檢討
《個人資料(私隱)條例》
的公眾諮詢報告

Report on
Public Consultation on
Review of the Personal Data
(Privacy) Ordinance

附件四 — 意見書
Annex 4 — Written Submissions

二零一零年十月
October 2010

目錄
Contents

1. 前言
   Foreword

2. 意見書索引
   Index of Written Submissions

3. 意見書
   Written Submissions

前言

政府在2009年8月28日發表檢討《個人資料(私隱)條例》的諮詢文件(“諮詢文件”)，進行為期三個月的諮詢。諮詢期於2009年11月30日結束。

2. 我們共收到178份[1]回應諮詢文件的公眾意見書。編印次序是根據收到意見書的先後次序排列。這些意見書包括以下三類：

(a) 發件人並無要求把身分或意見書保密的意見書，共有115份。這些意見書載列於本附件。

(b) 發件人要求把身分保密的意見書，共有32份。另有12份意見書，我們無法確認發件人是否同意把身分公開[2]。我們把這些意見書的發件人名字刪除後，載列於本附件。

(c) 發件人要求把意見書保密處理，共有19份。本附件並沒有載列這些意見書。

3. 在諮詢期間收到屬於廣告性質的傳真、垃圾電郵或懷疑帶有病毒的電郵，我們都不會作進一步處理。

4. 為了保障發件人的資料私隱，我們在編印意見書時，已將有關資料(例如：住址、電郵地址、身分證號碼和電話號碼等)刪除。

---

[1] 在收到的意見書中，其中兩份意見書按發件人的要求取代較早前提交的意見書。因此，雖然最後一份意見書的序號為 S0180，但實際數目為 178。

[2] 這些意見書未有提供有效的聯絡資料如通訊地址或傳真號碼。我們因而無法確認發件人是否同意在載列他們的意見書時把身分公開。

Foreword

The Government published the Consultation Document on Review of the Personal Data (Privacy) Ordinance ("the consultation document") on 28 August 2009 for a three-month consultation which ended on 30 November 2009.

2. We have received a total of 178[1] written submissions in response to the consultation document. They are arranged according to the order of receipt of the submissions. They comprise the following three categories:

(a) There are 115 submissions of which the senders have not requested anonymity or confidentiality. These submissions are included in this Annex.

(b) There are 32 submissions of which the senders have requested anonymity, and 12 which we are unable to ascertain whether the senders agree to make known their identities when their submissions are published[2]. The names of these senders have been deleted before the submissions are included in this Annex.

(c) There are 19 submissions of which the senders have requested confidentiality. The submissions are not included in this Annex.

3. Facsimiles received during the consultation period which were advertisements were not processed further. In addition, electronic mails which were spam mails or were suspected of being infected with virus were not processed further.

4. In order to safeguard senders' data privacy, we have removed senders' relevant data, such as residential addresses, email addresses, identity card numbers and telephone numbers, where provided, when publishing their submissions.

---

[1] Of the submissions received, two submissions have been replaced by subsequent submissions as requested by the senders. Therefore, though the last serial number of submission is S0180, the actual number of submissions received is 178.

[2] For these submissions, the senders have not provided any contact details such as correspondence address or fax numbers. We were therefore unable to ascertain whether they agree to make known their identities when publishing their submissions.

意見書索引
Index of Written Submissions

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0001	Lawrence Poon
S0002	見註 1 See footnote 1
S0003	未有署名 Anonymous
S0004	MS Ng
S0005	尹先生
S0006	見註 2 See footnote 2
S0007	見註 1 See footnote 1
S0008	Sharon
S0009	曾小姐
S0010	未有署名 Anonymous
S0011	見註 1 See footnote 1
S0012	見註 2 See footnote 2
S0013	未有署名 Anonymous
S0014	見註 1 See footnote 1
S0015	張朝鶴
S0016	阿 b
S0017	Lawrence Ma
S0018	見註 1 See footnote 1
S0019	徐曉杰
S0020	見註 2 See footnote 2
S0021	David Ma
S0022	見註 1 See footnote 1
S0023	見註 1 See footnote 1
S0024	阿 b
S0025	Sanny Chung

1 發件人要求不具名公開意見。The sender requested anonymity.

2 發件人要求以保密方式處理意見書。The sender requested confidentiality.

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0026	見註 1 See footnote 1
S0027	未有署名 Anonymous
S0028	見註 1 See footnote 1
S0029	見註 2 See footnote 2
S0030	見註 2 See footnote 2
S0031	見註 3 See footnote 3
S0032	見註 1 See footnote 1
S0033	Hong Kong Direct Marketing Association
S0034	見註 1 See footnote 1
S0035	Katherine
S0036	Stephen Chan
S0037	見註 3 See footnote 3
S0038	見註 3 See footnote 3
S0039	見註 1 See footnote 1
S0040	見註 1 See footnote 1
S0041	Margaret Lee
S0042	鍾澤偉
S0043	見註 1 See footnote 1
S0044	見註 1 See footnote 1
S0045	見註 2 See footnote 2
S0046	Tina Lau
S0047	江燦良
S0048	Swire Pacific Limited
S0049	Hong Kong Aircraft Engineering Company Limited
S0050	見註 3 See footnote 3
S0051	Nelson Lau
S0052	Hong Kong Federation of Insurers

1 發件人要求不具名公開意見。The sender requested anonymity.

2 發件人要求以保密方式處理意見書。The sender requested confidentiality.

3 未能確定發件人是否願意公開姓名。Unable to ascertain whether the sender agrees to make known his/her identity.

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0053	Hester
S0054	Hong Kong Institution of Engineers
S0055	港九勞工社團聯會
S0056	Hong Kong Investment Funds Association
S0057	見註 1 See footnote 1
S0058	見註 1 See footnote 1
S0059	見註 2 See footnote 2
S0060	見註 3 See footnote 3
S0061	見註 2 See footnote 2
S0062	The Hong Kong Institute of Chartered Secretaries
S0063	見註 3 See footnote 3
S0064	Archives Action Group
S0065	未有署名 Anonymous
S0066	PCCW Limited
S0067	Hong Kong Bar Association
S0068	The Hong Kong Association of Banks
S0069	見註 1 See footnote 1
S0070	見註 1 See footnote 1
S0071	香港珠寶製造業廠商會
S0072	Estate Agents Authority
S0073	The Law of Society of Hong Kong
S0074	見註 3 See footnote 3
S0075	見註 2 See footnote 2
S0076	見註 2 See footnote 2
S0077	蘇綺華
S0078	見註 2 See footnote 2
S0079	香港基督教服務處

1 發件人要求不具名公開意見。The sender requested anonymity.

2 發件人要求以保密方式處理意見書。The sender requested confidentiality.

3 未能確定發件人是否願意公開姓名。Unable to ascertain whether the sender agrees to make known his/her identity.

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0080	Hospital Authority
S0081	(此意見書按發件人要求被 S0163 取代) (This submission is replaced by S0163 as requested by the sender)
S0082	見註 1 See footnote 1
S0083	香港中華廠商聯合會
S0084	見註 1 See footnote 1
S0085	見註 2 See footnote 2
S0086	香港專業地產顧問商會
S0087	Freshfields Bruckhaus Deringer
S0088	見註 1 See footnote 1
S0089	AIDS Concern
S0090	The Real Estate Developers Association of Hong Kong
S0091	Vocational Training Council
S0092	丁毓珠
S0093	The Hong Kong Construction Association, Ltd
S0094	見註 2 See footnote 2
S0095	ZH
S0096	未有署名 Anonymous
S0097	Office of the Privacy Commissioner for Personal Data
S0098	見註 1 See footnote 1
S0099	Hong Kong Family Welfare Society
S0100	Kiwi Chan
S0101	Swire Properties Limited
S0102	見註 1 See footnote 1
S0103	Hong Kong Broadband Network Limited
S0104	見註 1 See footnote 1
S0105	愛護家庭家長協會

1 發件人要求不具名公開意見。The sender requested anonymity.

2 發件人要求以保密方式處理意見書。The sender requested confidentiality.

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0106	見註 3 See footnote 3
S0107	見註 2 See footnote 2
S0108	(此意見書按發件人要求被 S0149 取代) (This submission is replaced by S0149 as requested by the sender)
S0109	Hong Kong IT Alliance
S0110	Cheng Po-ling Polly
S0111	未有署名 Anonymous
S0112	見註 1 See footnote 1
S0113	Clifford Chance
S0114	見註 1 See footnote 1
S0115	Information Security and Forensics Society
S0116	Microsoft Hong Kong Limited and Microsoft Corporation
S0117	Blanche Leung
S0118	Ricky Wong
S0119	Hong Kong General Chamber Of Commerce
S0120	楊位醒
S0121	梁君彥
S0122	Federation of Hong Kong Industries
S0123	Yahoo! Hong Kong Limited
S0124	Baker & Mckenzie
S0125	明光社
S0126	Consumer Council
S0127	香港研究協會

1 發件人要求不具名公開意見。The sender requested anonymity.

2 發件人要求以保密方式處理意見書。The sender requested confidentiality.

3 未能確定發件人是否願意公開姓名。Unable to ascertain whether the sender agrees to make known his/her identity.

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0128	見註 3 See footnote 3
S0129	見註 3 See footnote 3
S0130	見註 3 See footnote 3
S0131	Society of Operations Engineers Hong Kong Region
S0132	香港社區組織協會
S0133	見註 2 See footnote 2
S0134	經濟動力
S0135	自由黨
S0136	香港中小型企業商會
S0137	PrimeCredit Limited
S0138	Hong Kong Information Technology Federation Ltd.
S0139	見註 1 See footnote 1
S0140	黎民
S0141	陳先生
S0142	JP Morgan Chase Bank, N.A.
S0143	香港小童群益會
S0144	見註 2 See footnote 2
S0145	民主建港協進聯盟
S0146	Urban Renewal Authority
S0147	見註 1 See footnote 1
S0148	Internet Professional Association & ISACA China Hong Kong Chapter
S0149	見註 3 See footnote 3
S0150	Hong Kong Computer Society
S0151	Hong Kong Doctors Union

1 發件人要求不具名公開意見。The sender requested anonymity.

2 發件人要求以保密方式處理意見書。The sender requested confidentiality.

3 未能確定發件人是否願意公開姓名。Unable to ascertain whether the sender agrees to make known his/her identity.

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0152	見註 1 See footnote 1
S0153	見註 2 See footnote 2
S0154	香港盲人輔導會
S0155	Allan G. Dyer
S0156	Working Group on Legal, Privacy and Security Issues of the Steering Committee on Electronic Health Record Sharing
S0157	香港人權監察
S0158	Elvis Law
S0159	見註 1 See footnote 1
S0160	Professional Information Security Association
S0161	Official Solicitor's office
S0162	The Hong Kong Medical Association
S0163	The DTC Association
S0164	見註 1 See footnote 1
S0165	The Hong Kong Institution of Engineers
S0166	IT Voice
S0167	見註 2 See footnote 2
S0168	Internet Society Hong Kong
S0169	香港社會服務聯會
S0170	Construction Industry Council
S0171	Graham Greenleaf
S0172	高永昊
S0173	The Hong Kong Institute of Housing
S0174	見註 3 See footnote 3
S0175	John Bacon-Shone
S0176	Mandatory Provident Fund Schemes Authority

1 發件人要求不具名公開意見。The sender requested anonymity.

2 發件人要求以保密方式處理意見書。The sender requested confidentiality.

3 未能確定發件人是否願意公開姓名。Unable to ascertain whether the sender agrees to make known his/her identity.

序號 **Serial No.**	姓名 / 名稱 **Name/Title**
S0177	Wharf T&T Limited
S0178	民主黨
S0179	未有署名 Anonymous
S0180	香港專業及資深行政人員協會

S0001

29/08/2009 11:33

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Answer: Public Consultation on Review of the Personal Data (Privacy) Ordinance August 2009

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear PDPO,

Attached is the answer of my View of the Public Consultation on Review of the Personal Data (Privacy) Ordinance for August 2009.

Regards,

Lawrence Poon

Public Consultation on Review of the Personal Data (Privacy) Ordinance August 2009.pdf

Public Consultation on Review of the Personal Data (Privacy) Ordinance August 2009

Major Proposal and Answer:

Sensitive Personal Data

• Should we subject sensitive personal data, such as fingerprints, to more stringent regulation?

Yes, I believe that only law enforcement should have the right to collect this kind of information. However, Bank should also allow collecting this kind of information in order to verify customer identity in some area of their business. For example, large amount wire transfer.

Data Security

• Should we regulate data processors entrusted with handling of personal data?

We should. They have to access data relate to personal information that can be very valuable to criminal. Therefore they should be regulated heavily.

• Should we require data users to notify the PCPD and affected individuals of personal data leakage incidents?

Yes, they need to inform PCPD and the individuals right aways, with in 24hours. This will give the victim time to notify bank that their personal information been leak and have the bank take precaution if ID thrift do happen.

Powers of the PCPD

• Should we give the PCPD criminal investigation and prosecution power?

This is the right ways to go. In many country that thrift of personal ID information is a major crime and should be punish with the full extend of the law allow. A person identity is those entire person has.

• Should we empower the PCPD to provide legal assistance to an aggrieved data subject who suffers damage by reason of a data user's contravention of a requirement under the Ordinance and intends to institute legal proceedings against the data user?

It should. Lay man don't know their right and hire a lawyer is very expansive. PCPD should provide legal assistance that involve international realest of personal information or company do not safe guard those information in order to cut cost.

• Should the PCPD be empowered to award compensation to an aggrieved data subject? *Offences and Sanctions*

It should, it will give some teeth to the PCPD and make offender unlikely to offend again.

• Should we make contravention of a Data Protection Principle an offence?

Yes.

• Should we make it an offence when a person discloses for profits or malicious purposes personal data obtained from a data user without the latter's consent?

It should, I don't like my phone company selling my personal information to the telemarketing company keep calling me during day time. I did not give many people my phone numbers and yet the telemarketer still able to know I change my cell phone number. So I guest my cell phone company sale information to them. Why should they allow to profit of the information that belongs to me??

• Should we make it an offence when a data user intentionally resumes the same contravening act shortly after complying with an enforcement notice issued by the PCPD against him?

It will serve as deterrence to those international to retaliating the people who report the offence. People report offence has to be protected in order for this to function.

• Should we empower the PCPD to impose monetary penalty on serious contravention of Data Protection Principles?

Yes, it will serve as deterrence for re-offence.

• Should we impose heavier penalty for repeated non-compliance with an enforcement notice?

Yes, it will make company less likely to not safe guard personal information as cost cutting measure.

• Should we raise the penalty for misuse of personal data in direct marketing? *Rights of Data Subjects*

We need to. Do not call list should also cover the live caller that as telemarketer. We can use the U.S. for example. Company have to give consumer option to opt out the information sharing between company or even department that with in a company for marketing purpose. Violator should face the same punishment as those leak information for profit.

• Should we empower a third party to give consent to the change of use of personal data of a minor or a mentally incapacitated person?

Only in case that the person can't be care for themselves or their action might be endanger the public or themselves. In those cases, court can appoint a third party to serve as power of attorney to deal with his/her personal business.

• Should we permit a data user to refuse a data access request made by parents on behalf of a minor when compliance with the request is not in the minor's best interests? *Exemptions from the PDPO*

This should only cover sexual orientation and some other most private information like communication between consol, mental professional, and attorney. We need to balance parental right and children right to privacy.

• Should we grant exemption to law enforcement agencies and rescue and relief agencies for handling personal data in emergency situations?

We should, this enhancement of law should not limited the government agency function in the case of emergency. But PDPO need to define what is the meaning of emergency or they will loophole it by decreeing all case as emergency when they want to get information that they are not in title.

• Should we allow data users to transfer personal data of minors that are relevant to parental care and guardianship to parents or guardians?

It is depending what is the information relate to. For example, do they have to right to know their children have STD or HIV positive? How about personal religion? If the knowledge of the information will endanger the children in the hand of their parents, I don't think they are in title to know.

It is happen in the U.S. that Muslim families kill their children after they convert to Christian as "honor killing" according to Muslim law. Hindus family send their daughter back to Indian so that their relative can have her kill for having sex with men before marriage. Muslim boy kill by family members for being homosexual. Do PDPO what this thing happen in Hong Kong?

Regards,

Lawrence Poon

S0002



To <pdpo_consultation@cmab.gov.hk>
cc
bcc
30/08/2009 18:25 Subject 個人資料（私隱）條例》的諮詢文件提交意見或建議
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啓者:

本人就個人資料（私隱）條例》的諮詢文件中有少許提交意見或建議.

就各私人機構申請職位所需填寫之個人資料中,求職者住住都需要填上配偶資料及"緊急事故通知者"之資料,這些資料當都包括姓名、電話號碼、關系甚至是私人住址.

本人清楚這些資料對員工是有一定的重要性,但可當求職者獲得聘請後才填報予公司(機構),不用把家人、親友之資料不必要地提供他人之私人資料予無關之公司(機構).

（來信人要求不具名公開意見）

S0003

30/08/2009 09:18

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject my views on the public consultation paper

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

I have attached my view on your consultation on the review of the privacy data. I strongly object to give the right to kids to disallow their parents to access their data!

My Views.doc

	My Views.
Major Proposals	
Sensitive Personal Data	
• Should we subject sensitive personal data, such as fingerprints, to more stringent regulation?	Yes, agree
Data Security	
• Should we regulate data processors entrusted with handling of personal data?	No need to further regulate data processors as the current guidelines are sufficient!
• Should we require data users to notify the PCPD and affected individuals of personal data leakage incidents?	Not necessary because PCPD can't help the situation.
Powers of the PCPD	
• Should we give the PCPD criminal investigation and prosecution power?	No, PCPD should not has the criminal investigation and prosecution power.
• Should we empower the PCPD to provide legal assistance to an aggrieved data subject who suffers damage by reason of a data user' s contravention of a requirement under the Ordinance and intends to institute legal proceedings against the data user?	Yes, PCPD can provide legal assistance for the victim who suffers damage.
• Should the PCPD be empowered to award compensation to an aggrieved data subject?	Depends on what sort of award compensation.
Offences and Sanctions	
• Should we make contravention of a Data Protection Principle an offence?	No comment
• Should we make it an offence when a person discloses for profits or malicious purposes personal data obtained from a data user without the latter' s consent?	No comment

• Should we make it an offence when a data user intentionally resumes the same contravening act shortly after complying with an enforcement notice issued by the PCPD against him?	How to distinguish between intentional or unintentional? Who make the judgement?
• Should we empower the PCPD to impose monetary penalty on serious contravention of Data Protection Principles?	No, the empowerment shouldn't go to PCPD
• Should we impose heavier penalty for repeated non-compliance with an enforcement notice?	No comment
• Should we raise the penalty for misuse of personal data in direct marketing?	No comment
Rights of Data Subjects	
• Should we empower a third party to give consent to the change of use of personal data of a minor or a mentally incapacitated person?	No comment
• Should we permit a data user to refuse a data access request made by parents on behalf of a minor when compliance with the request is not in the minor' s best interests?	Parents should have the right to access all their kids' data because these are the extremely useful for parents to give guidance
Exemptions from the PDPO	
• Should we grant exemption to law enforcement agencies and rescue and relief agencies for handling personal data in emergency situations?	No comment
• Should we allow data users to transfer personal data of minors that are relevant to parental care and guardianship to parents or guardians?	Parents should have the right to access their kids' data because these are the extremely useful to give guidance during brought-up
E-mail address: pdpo_consultation@cmab.gov.hk	

S0004

To pdpo_consultation@cmab.gov.hk

bcc

31/08/2009 12:18 Subject 私隱條例檢討諮詢公眾31.8.2009

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啓者:

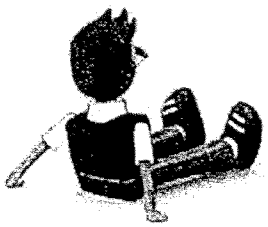
就以上題目,本人提議如下:

1. 有關街上/商場有銀行sale 咭 (road show), 申請人要於當時填上個人資料申請, 期間交出I.D 等個人証明作申請, 行動上未見政府有管制及執行, 我提議應每位申請人的資料副本上,蓋印鑑如"此証明文件用作申請xx銀行的VISA/MASTER CARD ...等字句, 另外獨立証明文件應用信封等入好,避免資料容易外洩等.

2.屋苑訪客登記, 填寫之表格應獨立一張, 不應所有都填同一張, 特別係一些單幢式樓宇, 管理欠妥善.

3.無論申請任何,都有須要呈交個人資料, 建議政府應提出制定,保障個人資料不會容易外洩.

4.到診所睇私家醫生時,入口登記護士往往只會問你身份証號碼,其實當時身邊正有其他病人坐著附近, 很易張自己的身份証號碼給別人知道. 這樣是否應提議醫生作改善.



MS NG

2009.8.31

Copyright © 2009 Yahoo! Inc. All rights reserved.

S0005



To <pdpo_consultation@cmab.gov.hk>

03/09/2009 14:27

Subject 我對諮詢文件的意見

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

您好！

以下是本人的意見：

敏感個人資料（如指紋）應否受更嚴格的規管？

不需要加規管。

應否規定資料使用者在發生個人資料外洩
事故時通知私隱專員及受影響的人士？

讚成。

應否賦予私隱專員刑事調查和檢控的權力？

讚成。

若有資料當事人因資料使用者違反私隱條
例的規定而蒙受損失並有意向資料使用者
提出法律訴訟，應否授權私隱專員爲受屈
的資料當事人提供法律協助？

讚成。

應否授權私隱專員向受屈的資料當事人判給補償？

讚成，但由法庭處理較佳。

應否把披露未經資料使用者同意下取得的
個人資料而從中取利或作惡意用途的行爲
訂爲罪行？

讚成。

應否授權私隱專員就嚴重違反保障資料原則的行爲施加罰款？

讚成。

應否將屢次違反執行通知的行爲處以更重的懲罰？

S0005

讚成。

應否將屢次違反執行通知的行爲處以更重的懲罰？

讚成。

應否授權第三者就更改未成年人或精神上無行爲能力的人的個人資料用途給予同意？

讚成。

如未成年人的個人資料與家長或監護人
履行照顧和監護責任有關，我們應否准許・
資料使用者把該等資料轉移給未成年人的・
父母或監護人？

讚成。
可參考本港保險業的現有的做法。現在爲未滿十八歲之人仕(如子女)，都是由父母或監護人作監管的，十八歲後監管權會自動轉給已成年之人仕。
這樣的做法較佳。

如有什麼需要或不清楚，請聯絡我。

謝！

尹先生

S0006

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)



To <pdpo_consultation@cmab.gov.hk>
cc
bcc
04/09/2009 19:36 Subject 有關工作證明文件的問題
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啓者：

本人是在有線電視維修工程部工作的，經常會接觸各大物業管理公司，但是我有一個疑問？有些管理處登記公司工作證便可以進入屋苑工作，但有些管理公司就一定要登記身份証資料才可以入內工作，這情況常發生在地鐵物業管理下的屋苑，這是地鐵公司的特權嗎？

本人覺得我們提供有效的工作證明文件已經很足夠了，因爲這證件已代表我所屬的公司，而且公司亦可證明我的身份！但管理公司就是這樣子，把我們的身份證資料登記在很多該公司的管理人員或保安人員都可以隨意翻閱記錄薄內！本人覺得這對個人資料的私隱有很大的譏諷！

所以本人希望貴處考慮立法改變這一不合理的做法，和確立公司委任工作證的法律有效地位！ 多謝！

祝工作愉快 九月四日

（署名來函）

（來信人要求不具名公開意見）



To pdpo_consultation@cmab.gov.nk
cc
bcc
11/09/2009 11:50 Subject 希望私隱可以納入埋外傭利用僱主資料去借$$為刑事
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

您好，

本人是外傭僱主， 發現現行條例只規管"商業機構"收集個人資料後, 濫用於非原本收集時的用途。
外傭僱主同外傭之間, 不屬"商業機構"關係, 即使僱主在不知情下被外傭用地址／僱主電話外出借貸／開電話服務， 僱主亦無從追究， 卻要受到外傭借貸／電話數的債主滋擾。

外傭僱主既要在法列上跟"商業機構"對待外傭， 私隱上卻毫無保障，公理何在？

身為外傭僱主， 聘請外傭原意為照顧家中老幼，自己可以外出掙錢，卻因此被滋擾。 現希望私隱條例可以納入， 因外傭利用僱主資料去借$$為刑事。

Sharon

S0009



To pdpo_consultation@cmab.gov.hk
cc
bcc
12/09/2009 14:21 Subject 《個人資料（私隱）條例》的意見
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

致 有關人士:

本人一直覺得在求職時, 雖然強調個人資料不會作其他用途, 但根本當事人是不會知道事實, 而申請物件時, 都要填上個人資料, 事後便會不知被什麼或相關公司拿去call客, 做生意了。

而且,相關公司,會否有連鎖效應? 一個大企業, 會經營不同類型的公司(飲食,娛樂, 銀行etc), 他們將當事人的資料給予"自己"的相關公司後 , 再給予自己公司的"相關"行業, 例如一個假設性的例, 申請銀行戶口卡, 個人資料其後便有可能被利用在信用卡, 再其後便到借貸公司, 再其後就落在與借貸公司任何有接觸/相關的公司手上,一直無止盡連鎖效應下去。所以應清楚寫明只限什麼職業種類, e.g 飲食只限飲食公司, 不會透露給娛樂公司 (最好當然是列明公司名) 而不是"相關"行業, 別人怎知道你是如何的"相關"法?

我認爲就是如此的效應, 手機雖然只申請了a電話公司, 但b,c,d公司不知爲何會有你的電話, 然後打來推銷, 這或許同業之間透露了吧。但最奇怪的是, 沒有申請任何信用卡, 竟然有人打來問:需要債務重組,借貸嗎? 是銀行透露?

我認爲當事人有權知道他們得知自己個人資料的來源, 既然報告上會有資料來源, 爲何來電者, 發email的人不來個資料來源? 而且,在填申請表/合約後, 一定要有副本! 讓當事人留底, 現在有些是有底單給予, 有些是要自己要求copy, 但在大街上申請信用卡的, 都不會有副本(以我所知)。這樣做是確保未來得知資料來源後, 可以查明該公司是否與單上所列的私人條例一樣。 要麼,每間公司都有一個個人資料私隱的部門,負責客戶查詢, 當事人可事後查明私隱資料到底透露了給哪些公司。

謝謝您的閱讀。希望能幫助到政府改善吧。

曾小姐 謹啓

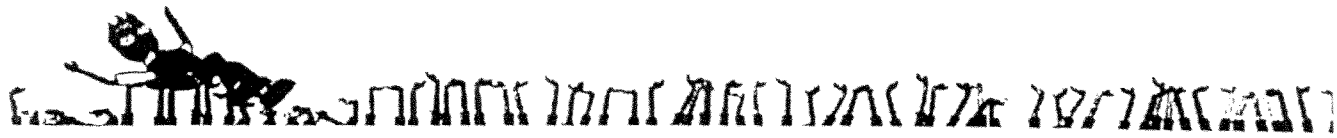
S0010



To pdpo_consultation@cmab.gov.hk
pdpo_consultation@cmab.gov.hk
cc
bcc
12/09/2009 10:13 Subject Consulation of personal data

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Privacy of personal data must including personal email address.



S0011

14/09/2009 13:53

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject On the Proposals for the Review of Person Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear the Correspondence,

Please find my opinions on the Proposals for the Review of PDPO in the attached file.

regards,

PDPO-Review-Comments.pdf

(Signed)

(The sender requested anonymity)

Comments on the Review of PDPO

My Opinion on the Proposals in the Consultation Paper on the Review of Personal Data (Privacy) Ordinance

by (name)

Date: Sept. 12, 2009

Proposal No. 1: Sensitive Personal Data

Differentiating Personal Data into "Sensitive" is essential to balance the piracy and public interests. However, it is difficult to set such a division. Sensitive Personal Data can be defined as those leading to improper purposes and improper application if leaked. For example, the credit card information of a person, if leaked, may lead to a faked card causing loss of that victim. Classifying biometric information as sensitive personal data seems improper, because those information can be easily acquired from a person without his/her prior to acknowledgement, which can be obtained via many means in daily lives. For example, personal fingerprints and DNA can be found on a mug used by a person; high definition digital photo can show iris as an art work. Of course, biometric information, especially DNA, may lead to illegal organs transplanting; but that would be another issue under other ordinances in the Law of Hong Kong.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

Regulating Data Processors and their sub-contractors are necessary. However, it is very difficult in practice due to technological limitation. Data Processors should refer to human levels and machine level because most information are keeping in computers and operating via computing systems in which every security profile is crackable. The regulation should be adjustable by an update-able standard and requirements. Perhaps, the easy way is to mark the moral obligation capable to force those Data Processors and Sub-contractors to improve to acceptable levels which should be defined by the current technology at that era.

Proposal No. 3: Personal Data Security Breach Notification

Privacy breach Notification is principally justifiable but difficult in practice. Before notification, there must be detection which is a part of the security profile. That means, detection may be failed under certain intrusion. In fact, some researchers have published their findings in Black Hat conference on how to mislead forensics and erase every trace of their intrusion. Although absolute cannot be achieve, notification must be done to victims if detected. However, if the notification is to public, it may lead to public panicky. For example, if HKBSC leaked some customers information, the whole public may totally withdraw their accounts leading to the liquidation of HKBSC.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

All persecution on criminal cases must go through Department of Justice. This is well defined in Hong Kong Legal System. Any modification would affect the legal independence and may even cause the collapse of HK legal system. However, PCPD can share the authority with Police on investigating some cases. However, obfuscation must be avoided and investigators in PCPD must be well trained as Police and in Digital Forensics.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

Providing legal assistance to an aggrieved data subject would be helpful, as long as it is within civil proceedings.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

It would be for a court to determine the appropriate amount of compensation payable. However, before going to the Law Court on a civil proceeding, there are two stages: arbitration and negotiation. PCPD can help both sides to settle their disputes outside the Law Court before conducting the civil proceedings.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

Making contravention of a Data Protection Principle should be an offense, if you can prove its malicious intend. In a criminal persecution, subjective factors (such as motive or malicious intension of the perpetrators) must be established. It is safe to keep "Contravention of the enforcement notice is an offense. " Since an enforcement notice has indicated the wrong doing, if the data user refused to follow, his/her malicious intend has been established.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

If the data leakage is among computers and internet, the Section 161 (Using Computers with Malicious Intend) , Criminal Damage and other related ordinances in the Law of Hong Kong are quite sufficient and such cases should be handled by Police and Department of Justice. The inadequacy is that buying and selling leaked personal data should be a crime. For other means of leaking personal data, there is necessary to consider such leakages leading to improper application with malicious purposes as an offense. (Note: reporting an affair of a minister in newspaper should not be considered as an offense.) Selling and buying those leaked personal data should also be a crime. For example, a person may get his friend's DNA and fingerprints via a mug; and then he may sell it to some underground economic groups leading to an illegal transplant; this is definitely a crime.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

If the solution in the enforcement notice was effective, it is an offense if a data user repeats such contravening act. However, if the enforcement notice was misleading or even a wrong solution, then the data user, repeating such contravening act, will not be an offense, but should have another chance for improvement with better solution.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

It would be for a court to impose monetary penalty and determine the appropriate amount of compensation payable. For a serious contravention of DPPs, it may be sufficient to be raised to a criminal case. If not, a civil proceeding should be taken.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

All depend on the technology. The supervision stated in Enforcement Notice may be outdated and insufficient to handle the situation. (Remark: there are more than 3millions pieces of malwares flowing in the internet and more than 200 new pieces of malwares being discovered daily; and, hacking skills are also evolved daily with technologies deployed.). Every outbreak should be considered as an independent case and a thorough investigation should be conducted. If there are

evidences to prove the intended negligence on the repeated offenders, they should be persecuted as a criminal case. (Section 161 on Malicious using Computers or even Criminal Damage).

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

Raising Penalty will be helpful. In direct marketing, their security in associating their software are normally sub-contracting to some software house which would charge a considerable amount of money. Hence, penalty should be above the amount of an average software house in providing security. Although this raising in penalty would cause some direct marketing companies to go liquidation, this is good for Hong Kong Citizens in preventing their loss.

Proposal No. 13 : Third Party to Give Prescribed Consent to Change of Use of Personal Data

All depend on the definition of "Third Party" and their operations. It should be guided by the validation of transferring duties and the principle of "Need-to-Know", which should comply the Children Human Right and Human Right Declaration.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

We should take the Rights of the Child (http://www.unhchr.ch/html/menu2/6/crc/treaties/crc.htm) as a whole. Parents (or persons bearing those duties), who are a part of the minor, should be copied on those personal data of a minor. However, if parents were abusing a minor before, they should have been re-educated and corrected before having their parental duties back. During that re-education period, it would be other responsible persons (or social welfare department) to bearing the duties of parents.

Proposal No. 15 : Access to Personal Data in Dispute

During the investigation, all can focus on items, say medical records, instead of content. This can reduce the demand on this proposal. However, there may be situation when the detail content is required. Then, PCPD will have its responsibility to safeguard those information and guided by this PDPO. Any failure would lead to the abuse of duties. That provision under PCPD must be well regulated.

Proposal No. 16 : Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

If Other Legislation forbids the access, then it is forbidden including PCPD. No further discussion is required.

Proposal No. 17 : Erasure of Personal Data

It is relatively easy to erase hard-copies. The problem is mainly in software copies. Todays, most information is handled by computers. In that case, erase is normally referring to delete and empty the "bin", which only changed the first character of the file name into "_" and the whole content of the file is recoverable in most cases. Nevertheless, taking practical steps are good enough to average data users.

Proposal No. 18 : Fee Charging for Handling Data Access Requests

It should be free of charge or included into monthly service charge. If you looks at a data center, all are in a computer system. Service charge is to cover the fixed cost in running that center and its benefit. Hence, all access are also included in that service charge.

Comments on the Review of PDPO

Proposal No. 19 : Response to Data Access Requests in Writing and Within 40 days

For an effective communication, it is good to have a written response whether the data user is holding such information or not. 40 days may be too long and data users may forget the request. Hence, the response should be done in 4 days or even 48 hours, via e-mails with its digital signature.

Proposal No. 20 : Circumstances for Issue of an Enforcement Notice

An enforcement notice should be issued in every case after the investigation or even the sentence by the Law Court. It may be about corporate operation procedure in improving the safeguard or as complex as a network system design if it is an electronic data center as in the case of Heartland Data Center in U.S.

Proposal No. 21 : Clarifying Power to Direct Remedial Steps in an Enforcement Notice

The PCPD has the power to direct the relevant data user in an enforcement notice to desist from doing an act or engaging in a practice. However, PCPD should take a constructive confrontation approach, especially in a complex situation.

Proposal No. 22 : Removing the Time Limit to Discontinue an Investigation

The Time Limit is not important and can be removed; but, the complaniant must be notified as soon as possible on the decision with reasons.

Proposal No. 23 : Additional Grounds for Refusing to Investigate

It is appropriate to include the following additional specific grounds for the PCPD to refuse to carry out or continue an investigation under Section 39(2) :

(a) the primary cause of the complaint is not related to personal data privacy;

(b) the complaint relates to any action which is currently or soon to be under investigation by another regulatory body; or

(c) the act or practice specified in the complaint relates to personal data or documents containing personal data which have been or will likely be or are intended to be used at any stage in any legal proceedings or inquiry before any magistrate or in any court, tribunal, board or regulatory or law enforcement agencies.

Proposal No. 24 : Transfer of Personal Data in Business Mergers or Acquisition

Merges or Acquisition are in corporate levels, little relates to the detail of personal data. It should be governed by the principle of "Need-to-Know" and thus only related data can be exempted.

Proposal No. 25 : Provision of Identity and Location Data on Health Grounds

To save lives, it is import to permit disclosure of any personal data where disclosure is necessary to prevent or lessen a serious threat to the life or health of an individual.

Proposal No. 26 : Handling Personal Data in Emergency Situations

For lives saving and effective communication, specific exemption from DPP 1(3) and DPP 3 of the PDPO should be granted in the handling of accidents or other life-threatening situations by LEAs

Proposal No. 27 : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

An exemption from DPP 3 should be provided to permit transfer of personal data of minors to their parents or guardians to enhance the protection of vulnerable minors and those at risk so that parents and guardians can properly discharge their responsibility on proper care and guardianship. This exemption should be guarded by the Right of Child.
(http://www.unhchr.ch/html/menu2/6/crc/treaties/crc.htm)

Proposal No. 28 : Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result

To relieve the PCPD's obligation to notify the complainant of the investigation result and related matters under Section 47(3) when the complainant has withdrawn his complaint.

Proposal No. 29 : PCPD to Disclose Information in the Performance of Functions

The PCPD and his staff should be able to disclose information reasonably necessary for the proper performance of the functions and powers of the PCPD, such as disclosure of information to statutory bodies like the Administrative Appeals Board which handles appeals against certain decision of the PCPD as stipulated in the PDPO and to overseas data protection authorities to facilitate cross-border privacy cooperation in the enforcement of personal data privacy rights. Some statutory bodies such as the Securities and Futures Commission and the Equal Opportunities Commission (EOC) are permitted under their respective legislation to disclose information in a number of situations associated with the proper discharge of the functions and the exercise of powers by them. Beyond this, it should be consider as the abuse of duties.

Proposal No. 30 : Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit

This would lead to the abuse of duties and should be limited and considered case by case.

Proposal No. 31 : Power to Impose Charges for Educational and Promotional Activities

Protecting privacy is a human right. Government authority, such as PCPD, should not impose any fee or charges for educational and promotional activities. In fact, it should be an undeniable responsibility of Government to educate and promote privacy in all cost.

Proposal No. 32 : Power to Obtain Information to Verify a Data User Return

This is a necessary step to enhance an effective communication.

Proposal No. 33 : Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings

The exemption from application of DPP 3 should be extended to cover the use of personal data required or authorized by or under law or court orders, or related to legal proceedings or for establishing, exercising or defending legal rights. It is reasonable and legitimate for data users to change the use of personal data in such circumstances.

Comments on the Review of PDPO

Proposal No. 34 : Transfer of Records for Archival Purpose

The necessary exemption from DPP 3 for the transfer of records containing personal data to GRS for archival purpose should be limited to a minimum level. Subsequent handling of the archival records containing personal data by GRS (including access to and use of records by members of public) will continue to be subject to the provisions of the PDPO.

Proposal No. 35 : Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

There should be any contradiction in against the Evidence Ordinance; and, this should not cause any obstruction of righteousness. That is, the refusal should be limited such that law enforcement can conduct its investigation and seize evidence.

Proposal No. 36 : Definition of Crime under Section 58

This should limited to empower law enforcement agencies under multilateral and bilateral cooperative agreements or arrangements providing personal data to their overseas counterparts for criminal investigations or detection of crimes overseas. It would also enable assistance to be provided to foreign jurisdictions in verifying personal data in connection with requests for legal assistance. In addition, law enforcement has its responsibility to ensure its counter-part to respect the human right in privacy.

Proposal No. 37 : Expand the Definition of "Relevant Person"

No Objection.

Proposal No. 38 : Exclude Social Services from the Definition of "Direct Marketing"

No Objection.

Proposal No. 39 : Exemption for Personal Data Held by the Court or Judicial Officer

No Objection.

Proposal No. 40 : Extend Time Limit for Laying Information for Prosecution

Two years are a reasonable time frame, but not for longer because the world is changing fast.

Proposal No. 41 : Duty to Prevent Loss of Personal Data

No Objection.

Proposal No. 42 : PCPD to Serve an Enforcement Notice together with the Results of Investigation

No Objection.

Proposal No. 43 : Contact Information about the Individual Who Receives Data Access or Correction Requests

No Objection

S0012

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

S0013



To pdpo_consultation@cmab.gov.hk
cc
bcc
20/09/2009 20:04 Subject 電訊公司
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

當你的手提電話臨近滿約的時段，多間電訊公司會主動介紹新plan給用戶，我的個人資料已被電訊公司公開搜查？

另，當我打自繼續續約該間電訊公司時，他們打電話來，叫我核對個人資料，例如：登記人全名，身份証號碼等，電話中確認才可以繼續享有這優惠，他們有時還說到門市可能未能得此優惠，他們的來電，多數是沒有來電號碼的。

我覺得這樣對我沒有保障，我覺得你們要監管他們！



20/09/2009 00:52

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Team 4
Constitutional and Mainland Affairs Bureau

Dear Sir/Madam,

I would like to give my comments on the Consultation Document on Review of the Personal Data (Privacy) Ordinance and wish to remain anonymous in the process.

I have the following views on Chapter Six: Offences and Sanctions.

For Proposal No.7, I agree to making contravention of a DPP an offence in order to deter contravention.

For Proposal No.9, I agree to making repeated contravention of a DPP on same facts an offence in order to deter repeated contravention.

For Proposal No.10, I agree to empowering the PCPD to impose monetary penalty on serious contravention of DPPs so that the PCPD can deal with such cases more effectively.

For Proposal No.11, I agree to imposing heavier penalty for repeated non-compliance with enforcement notice but I prefer to leave the appropriate penalty level decided by others.

For Proposal No.12, I agree to raising penalty for misuse of personal data in direct marketing but I prefer to leave the appropriate penalty level decided by others.

I have no comments on other proposals in other chapters. If necessary, you may reach me at the above email address.

Yours faithfully,

(Signed)

(The sender requested anonymity)

關於個人資料(私隱)條例建議：

建議人：張朝鶴(Cheung Chiu Hok),

建議 1： 敏感個人資料

8： 生物辯識資料應列爲敏感個人資料，身份證號碼也應列爲敏感個人資料。在我的個案中， 有人只用我的名字加上身份證號碼已經可以製造一張假身份證。

9： 很多時候申請會員卡時， 所填寫的資料往往被濫用於非會籍的用途， 其中以集團式經營尤甚。 有些申請表就列明所填寫的資料可用於集團其他聯所機構，實爲不當。

建議 2： 規管資料處理者及分判活動

10： 監於很多商業活動涉及外判， 個人資料遭受濫用的機會也大大提高。 應可考慮若由外判商引至個人資料外洩， 一但證實， 判出工程的公司也需負上責任， 以受阻嚇力。

11： 建議甚好。

12： 正确。

建議 3： 個人資料外洩通報機制

13： 關於個人資料通報機制， 原意很好， 但難於實施， 成本也昂貴， 未必符合成本效益。 以我的例子來說，我已向(刪除)購買一項服務，(因我的個人資料已外洩)， 若有人再用我的身份申請信用卡，(刪除)會傳電郵通知我。 但此項服務費用比較昂貴， 每年要 108 港幣， 而且不能單獨申請， 要和其他計劃使用，詳見附件。

私隱專員得執行權力

14： 此建議也屬合理， 但我認爲在調查的權力上， 應附予私隱專員更大的權力及權限， 至於罰款及其他罰則， 可交予律政司或法官。

15： 此建議十分好， 我贊成授權私隱專員爲受屈資料當事人提供法律協助，甚至可以 受害人提供法律援助， 向有關機構提出民事訴訟。 以我的個案來說，雖然我以委託(刪除)律師行發出律師信，但有關機構(刪除)及 (刪除) 并無動於衷， 拒絕更改我的個人信貸紀錄之餘(刪除) 更離譜，繼續向我發出騷擾電話。 我正在考慮是否向法律援助處申請法律援助向這兩家金融機構提出民事訴訟。

16： 我贊成應授權私隱專員判給受屈的資料當事人補償。 以我的個案， 我曾經向個人資料(私隱)條例專員公署提出投訴， 但由於担心此舉會影響(刪除)更改關

於我的錯誤的信貸紀錄的進度， 於是撤回投訴。

建議 7： 把違反保障資料原則訂爲罪行

18： 贊成把違反保障資料原則的行爲刑事化， 致於如何釐定違反保障資料原則可由個人資料(私隱)條例專員公署釐定或成立一個委員會來負責此項。

建議 8： 在未經授權下取得，披露和出售個人資料

19： 讚成此建議， 我的身份就是被盜用來申請信用卡， 并被追數公司騷擾。 就算把資料外洩的行爲刑事化，未必可以杜絕個人資料外洩，特別是經由互聯網，個人的身份往往難以追查。 但刑事化可以增加阻嚇力。

建議 9： 就同一事實重複違反保障資料已原則

20： 若資料使用者重複相同不符合原個人提供資料的原意的行爲或做法， 明顯有一挑戰私隱專員的權力， 應該訂爲罪行， 以鞏固私隱專員的權力。

建議 10： 就嚴重違反保障資料原則處以罰款

21： 讚成私隱專員應就嚴重違反保障資料原則的資料使用者繳付罰款， 可以由公署發出指引， 就何爲嚴重違反保障資料原則做出指引， 并由私隱專員決定。

建議 12： 提高在直接促銷中不當使用個人資料的罰則

23： 可以考濾提高罰款至 100,000 圓。

張朝鶴

（ 已簽署 ）

2009 年 9 月 19 日

（ 編者註：已刪除意見書中涉及來信人的個別個案的詳細資料及附件 ）

S0016

21/09/2009 22:46

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject 私隱政制

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啟者：

求職者要填表格，包括：姓名、身份證號碼、電話號碼、地址．．．．，但只要有這幾樣資料就可以打電話去一些機構申請一些收費服務，填一百次表可能都不獲聘用，為了求職，個人私隱就不斷揭露，極不安全。特別是身份證號碼，警訊都呼籲市民不要隨便透露。

我認為必要限制在聘用前的表格內容，例如：不確定聘用不能求取身份證號碼、地址只能以十八區作準，不能取ｘｘ樓ｘｘ單位．．．．．。

還有很多我想不到的陷阱，請為市民的安全而修正制度！

阿 b

S0017

To: Ms Christina Chong

From: Lawrence Ma, Barrister,
DAB professional affairs
committee member.

Re: Opinion on PDPO Reform

I suggest that sexual information should be included in the definition of sensitive personal data so as to deal with situations like posting nude celebrity photos on magazine front cover. This is an important social and cultural dilimena of Hong Kong.

Secondly, I support the ~~criminalisation~~ criminalisation of contravention in that serious contraventions should be punishable by terms of imprisonment. Thus, it is suggested that we make certain serious contravention as an indictable offence.

Thirdly, we need a specialist branch of prosecution. Be mindful that the conviction rate has been plainly low (see page 8 Consultation Document). That specialist prosecution branch can be within the Department of Justice or within the Privacy Commission.

Best Rgds,

(Signed)

22. September 2007.

檢討《個人資料（私隱)條例》

個人資料私隱專員公署：

本人十分感激個人資料私隱專員公署檢討《個人資料(私隱)條例》，可以比市民發動表一些意見，改善現今《個人資料(私隱)條例》不足知處。使《個人資料(私隱)條例》變得完善。

本人有以下一些意見比本署。

本人是殘疾人士，我不喜把自己的履歷表加入健康狀況。這是侵犯《個人資料(私隱)條例》，因爲自己健康問題及傷殘問題都是自己的事情，點解要比第三者知道這樣資料？這樣資料比公司老闆及人事部知道，他們不會聘用我們殘疾人士工作，有可能觸犯傷殘歧視。點解香港政府有一些部門要填寫我們殘疾人有關健康狀況在履歷表上？有什麼用途，是否真的可以幫助我們殘疾人士找工作？還是僱主會聘用我們殘疾人士工作？這樣不會請我們殘疾人工作，反而被僱主會覺得我們殘疾人士不能擔任這工種，影響我們殘疾人士面試及工作的幾會。這樣是嚴重侵犯《個人資料(私隱)條例》，我希望勞工處展能就業科、社會福利署及其他福利機構不要張我們殘疾人士的殘疾在任何情況下向第三者公開有資料。例如：尋找工作方面等。由期是我們殘疾人士不喜歡在勞工處展能就業科簽署一份《個人資料(私隱)條例》向第三者公開有關健康狀況。點解不是一年簽一次相關文件？一年簽一次有《個人資料(私隱)條例》向第三者公開有關健康狀況，可以自己在一年時間內想清楚。有關自己健康狀況是否直得公開？一但在勞工處展能就業科簽署一份《個人資料(私隱)條例》向第三者公開有關健康狀況。後悔莫及也太遲了，也不可以回頭！

最後，本人希望有以下兩點加強保護殘疾人士有關資料及改善有關《個人資料(私隱)條例》。

1. 希望可以加強保護殘疾人士的健康狀況及殘疾情況，不可以比第三者知道，不論在任何情況下不能給第三者知道有關資料。
2. 政府方面：勞工處展能就業科及有關機構可以比殘疾人士每年簽一次有關《個人資料(私隱)條例》向第三者公開文件，如果沒有簽不能向第三者公開，如履歷表上、口頭公開健康狀況及殘疾情況。
3. 希望可以比我們殘疾人士選擇有關公開《個人資料(私隱)條例》的健康狀況及殘疾情況，如可以口頭公開或履歷表公開等等。

多謝個人資料私隱專員公署比我發表意見。

(署名來函)

S0018

22/09/09

（ 來信人要求不具名公開意見 ）

S0019

P.01/01

意見：區議會候選人地址為何可以在互聯網輕易找到？政府在將候選人地址刊憲時應該好好保護其私隱。

有關檢討《個人資料(私隱)條例》地區諮詢會
回條

（請於二零零九年十月二日或之前回覆）

政制及內地事務局

請在適用的方格內填上✓號：

☐ 本人將出席第一場地區諮詢會
日期：二零零九年十月八日(星期四)
時間：下午七時至九時
地點：跑馬地黃泥涌道 133 號禮頓山社區會堂

☐ 本人將出席第二場地區諮詢會
日期：二零零九年十月十三日(星期二)
時間：下午七時至九時
地點：沙田源禾路 1 號 1 樓沙田大會堂展覽廳

☑ 本人未克出席諮詢會

姓名：徐曉杰　　簽署：（已簽署）

區議會：Kwai Tsing　　聯絡電話

傳真號碼：　　日期：22/9/08

S0020

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)



24/09/2009 12:53

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Consultation Document on Review of the Personal Data (Privacy) Ordinance (Proposal #8)

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing, Central Government Offices
Lower Albert Road, Hong Kong

Dear Sirs,

-

Re: Consultation Document on Review of the Personal Data (Privacy) Ordinance

-

I refer to Proposal #8 of the Consultation Document.- It is submitted that an offence for unauthorised obtaining, disclosure and sale of personal data should be created, in particular in the context of paparazzi activities.-

-

It has become a common malpractice for reporters to infiltrate personal lives of entertainment industry professionals and their spouses/children, to secretly take photographs of their personal activities without obtaining consent of the data subjects and then publish the same for profits.

-

It is trite law that "*depending on the circumstances, taking someone's photograph can be an act of personal data collection* " (**Eastweek Publisher v Privacy Commissioner for Personal Data CACV331/1999, para 30**).- Taking photographs of famous performers and their families, with full knowledge of their identities, constitutes personal data collection.- This is because such photographs contain information that relates directly to the data subject, and it is practicable to ascertain the identity of the data subjects from the photographs. -Indeed, magazines and newspapers would publish the photographs for their commercial value only if the readers can identify the data subjects in such photographs.

-

The Court of First Instance in that case considered "*fairness* " in DPP1(2) in **Eastweek Publisher v Privacy Commissioner for Personal Data HCAL 98/1998**:

-

> "*what rendered the taking of the photograph unfair was the fact that it was taken without the complainant's knowledge or consent at a time when (a) the photographer did not have reasonable grounds for thinking that he would be able to obtain her consent to its publication, and (b) the magazine did not have a policy of publishing someone's photograph (obtained without the person's knowledge or consent) in such a way that the person cannot be identified* " (Para 19) (emphasis added)
>
> -
>
> "*as one measure (amongst others) of the fairness of collection of the data, it was appropriate for the Commissioner to have regard to whether the data would be used fairly thereafter* " (Para 23) (emphasis added)
>
> -
>
> "*the complainant's consent to the taking of the photograph or to its subsequent*

publication was not something which could be taken for granted " (Para 24)

-

The consent of the data subject is invariably never obtained before or after the taking of these photographs, therefore such data collection is excessive and unfair. -

-

In relation to a defence, case authorities have provided guidelines of interpreting "news":-

-

a)---- In **Eastweek Publisher v Privacy Commissioner for Personal Data HCAL 98/1998**, where a reporter took photographs of people on the street for the purpose of commenting on their fashion sense, the Court of First Instance left the issue open whether "*lifestyle article* " falls under "*news activities* " or "*news gathering* " under section 61(3) of PDPO but commented that it was open for the Commissioner to conclude that the taking of the complainant's photograph to illustrate such an article was not news gathering (Para 18).

-

b)---- In **Associated Newspapers v News Group [1986] RPC 515** (a UK copyright case), it was decided that the reporting of the death of the Duchess of Windsor did not justify the publishing in the newspapers letters passing between the Duke and the Duchess.- Walton J commented that "*it does not seem to me that the actual publication of the letters is the sort of current event of which [the reporting current events defence] is speaking* ".

-

Therefore, paparazzi activities should not be covered under the section 61 "news" defence under PDPO, as there is no genuine news value in the personal lives of entertainment industry professionals, and more so, of their spouses/ children.-

-

In summary, it is submitted that:

-

------- there should be an offence for a person to disclose for profits or malicious purposes personal data which he obtained from a data user without the latter's consent, especially when such activities are undertaken with the aim to reap profits from violating personal data privacy of entertainment industry professionals;

-

------- defence provisions should not be too wide, and it should be made clear that paparazzi activities on the personal lives of entertainment industry professionals and/or their family do not qualify as "news"; and

-

------- -a high level of fine and/or imprisonment term should be introduced to achieve a deterrence objective.

-

Yours faithfully,
David Ma (Solicitor)



To <pdpo_consultation@cmab.gov.hk>
cc
bcc
24/09/2009 22:56 Subject 檢討《個人資料 (私隱)條例》

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt



檢討《個人資料 (私隱)條例》1.doc

檢討《個人資料（私隱)條例》

個人資料私隱專員公署：

本人十分感激個人資料私隱專員公署檢討《個人資料(私隱)條例》，可以比市民發動表一些意見，改善現今《個人資料(私隱)條例》不足知處。使《個人資料(私隱)條例》變得完善。

本人有以下一些意見比本署。

本人是殘疾人士。我好想問下個人資料私隱專員公署一個問題，也是一個一個的事實，請問公司的地址、公司電話號碼、公司傳真號碼、公司電郵及負責人是否在《個人資料(私隱)條例》下的保障？因爲我們殘疾人士在尋找工作時，經常出一些聽不清或聽不到的資料！這些聽不清或聽不到的資料就是我們自己申請一些工作，由於僱主打電話來，往往都聽不清楚地址、公司電郵等等。由期是對一些聽覺有問題的殘障人士來說影響十分大及嚴重！我們殘疾人士向勞工處展能就業科查詢以下的資料，勞工處展能就業科總是話這是（公司私隱），不能向我們殘疾人士公開，包括：公司的地址、公司電話號碼、公司傳真號碼、公司電郵及負責人。請問我們殘疾人士如何去面試及返工？沒有公司的地址、公司電話號碼等我們殘疾人士好難去公司面試及返工！也正事一個大問題的出現！舉兩個例子：第一個例子，我們殘疾人士去到公司面試才發覺公司沒有人在工作或外出工作及吃飯。我們殘疾人士沒有公司電話，沒有方法同公司僱主聯絡？這是叫我們殘疾人士回家？還是不斷地等公司開門？我們殘疾人士損失了時間及金錢，對坐輪椅的殘疾人士來說也是十分不便。第二個例子，我們殘疾人士沒有正確公司地址，好難找到公司來面試！我們殘疾人士在太熱氣溫下，如氣溫有三十一或三十三度左右，我們殘疾人士是否在街上走來走去找公司？你們應該有同情及關心我們殘疾人士！由於勞工處展能就業科的主任不是經常帶我們每一位殘疾人士去見工，所以產生以下的問題！

我們殘疾人士覺得勞工處展能就業科提出什麼的（公司私隱）是否玩弄的意味？其實我們殘疾人士好不滿勞工處提出的（公司私隱）。點解公司有（公司私隱），這是什麼的意思？公司是用來做生意，不是一個人。如果公司有（公司私隱）如何聘請人來工作？如何找到買家？這是否十分好笑的笑話！個人資料私隱專員公署可否回應我是否有（公司私隱條例）？

最後，本人有以下意見及解決方法。

1. 希望取消（公司私隱條例），勞工處本港就業科及勞工處展能就業科登記的

工，如有求職者申請這份工作，能夠公開公司的地址、公司電話號碼、公司傳真號碼、公司電郵及負責人，方便我們去面試及返工。

2. 如果真的有（公司私隱條例），希望勞工處登記的工，可以比勞工處展能就業科登記的殘疾人士得到括免，得公司的地址、公司電話號碼、公司傳真號碼、公司電郵及負責人的資料，方便我們去面試及返工。

多謝個人資料私隱專員公署比我發表意見。

（ 署名來函 ）

24/09/09

（ 來信人要求不具名公開意見 ）

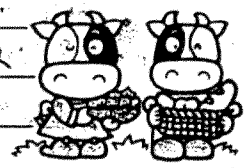
徵求建議如下：

《個人資料(私隱)條例》並不是知道對方消費力便公幫處理金錢不合理使用有些職員自行分類治動安排，做成分化隨意調整將予行通知。《個人資料(私隱)》不是用作表現給上司工作的評估標準。

甲乙丙說：你留給別人用吧？口應用則用心及善用別人的利理心態，為保註冊人仕的責是高級職人常看見很多別人私隱，當社會保障用平等的目光看法人同胞，在國際上看齊做個香港全面的整宣地，家庭(原師長)平均60歲普通高齡每月入息限額手機0在這個地方且子不生活，個案事主者、天在辦工時間被給聊聽(私隱)在某危險的後和別人談論職員五個事員個消息，財務公司 21345xx 減肥公司 31897xx 常在工作单位福利机構外洩個人資料。

公共事務機作職員也收集個人財務資料控制存款。

公務員、社工、護士、醫生、電腦資訊、記者、律師、保險、出納、局主管、判斷、用調北致一比九九個人工作態度保障私隱次重和談論送生活。(員徵員)





運用權力扣減殘障長期病者私支出可能加快她們的命治準。用已簽署的文件作證而机會不是以方直記錄的私隱證據。

隨鎮背景也採納資料要處，宮數查與開您角共生活很多妥多彩；請吃飲也向公衆仁佈的使用者私隱共識，經網絡傳送成實個人特可，齊達締造美好香港。

殘疾老弱人士包括：弱智、聽覺受損、視覺受損、肢体偏殘、言語障礙、精神病、自閉症、器官殘障、長期病患、注意力不足、過度活躍症、記憶力弱、特別學習困難引致工作損害已經私隱嗎？學位之仁設殘權當广東團華馬弟污名化賠，把個人資料宝報看輕果會的經濟學，殘廢如月60退休一個病人制造九九中屬工作庇蔭；透過支持社會大衆率擊學習政策發展經定香港福地我們也同工作。

以上是個人意高華為摘要，對不起(刪除)我練小姐請包融本公司用醫長病言氣粗了！抱歉。

請詢用途不用公開姓名可查閱。

私隱煙通是開源節流方向在家居所殘疾兒童及老弱者私隱如何平衡經醫生證明由其他專業組織人仕負對有否犯私隱呢

（來信人要求不具名公開意見）

S0023



To pdpo_consultation@cmab.gov.hk
cc
bcc
26/09/2009 12:53 Subject Re: 私隱政制

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啓者：

多謝回覆！我忽然想起，當我們打電話去收費機構查詢時，職員都要我們講出：客戶帳號、身份證號碼、電話、地址等等資料。聽聞有些人會把這些資料賣出，作其他謀利用途，包括非法勾當。－－我時常收到一些推銷電話(貸款、電話服務、等等)，但不知她們從何知道我的資料(電話號碼及姓名等等)。

另外，接受某些機構服務之後，她會電郵通知：如果你不作書面反對，本公司就會把你的資料作推廣用途等等。我覺得該公司必須在電郵中有一個「接受」及「不接受」的功能，讓客戶可以即時選擇，否則，很多人都怕麻煩，不作書面回應，而任由機構利用客戶的資料，不斷玩弄。例如：一些寬頻公司在合約中說明，你不書面提出終止合約，我們會幫你自動續約，你先要在兩個月前通知我們要終止合約，我們才寄一個表格給你，填寫及簽名，當中資料要完全無錯，在限時寄回或傳真，不可寄失或過時，否則無效！又要自己拆除全套解碼器及零件送到某單位，否則罰巨款！

一般市民要工作已經忙過不停，都懼怕這些無理的麻煩及刁難，希望可以有些條例及方法，與民方便，減少壓力，增加保障！

謝謝！

阿 b

--- 2009年9月21日 星期一，**pdpo_consultation@cmab.gov.hk** <*pdpo_consultation@cmab.gov.hk*> 寫道:

寄件人: pdpo_consultation@cmab.gov.hk <pdpo_consultation@cmab.gov.hk>
主題: Re: 私隱政制
收件人:
日期: 2009年9月21日,星期一,下午11:27

謝謝你就檢討《個人資料（私隱）條例》的諮詢文件提出意見。
政制及內地事務局
Thank you for your views on the Consultation Document on Review of the Personal Data (Privacy) Ordinance.
Constitutional and Mainland Affairs Bureau



27/09/2009 12:16

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Review of the Personal Data (Privacy) Ordinance - submission of opinion

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir/Madam,

Re: Sensitive personal data being unnecessarily accessed by registered phramacies

I would like to submit my opinion on the review of the personal data(privacy) Ordinance.

I am a patient who needs to buy prescribed medicine from registered phramacy shops on a regular basis. Doctor's reference letter is required to be submitted to the phramacy for filing upon the purchase of the medicine. Since there is a HKID card no. being shown on the doctor's letter in addition to the full name of the patient, I tried to strike out the HKID no. on the reference letter before passing it to the phramacy shop assistant. However, the phramacy shop assistant told me that by law, they must obtain the original doctor's letter with both the patient's name and HKID card no. printed in full.

I immediately felt that my personal data is unnecessarily exposed to anyone in the phramacy shop who can access these prescription letters.

I'm writing to suggest that the Government should amend the law to only indicate may be just the first 4 digits of the HKID card no. This practice had already adopted in many other usage of our HKID card no. However, this is not the case for medicine prescriptions policy.

In view of this, I'd like to urge the Government to review the policy and pass my opinion to the corresponding department for follow-ups.

Thank you for your attention.

Regards,
Sanny Chung
Hong Kong Resident

檢討<<個人資料(私隱)條例>>的意見書

本人現就諮詢文件作出意見。此意見書原則上以附件一A部建議十四作出意見。

"父母親查閱未成年人士個人資料的權利"此話題由諮詢文件一發佈時已引起各界人士廣泛回應。

廣泛的討論最主要擔心是太過著重未成年人士的私隱會導致父母親不如何去教導子女。但本人在想:當父母親去打(不論任可手法及程度)未成年子女時,子女會否去報警呢?即使去報警,去了法庭,法庭是否會受理呢?萬一法庭受理,刑罰又會否致於終身監禁,甚至死刑(部份國家)呢?詳細列明條例的用途,就是缩小法例的灰色地帶,即使立下條例,子女是否務必不給予成績表、健康報告(時下熱烈討論之驗毒計劃)。一般父母的想法就如本段頭一行"太過著重未成年人士的私隱會導致父母親不如何去教導子女",就如諮詢文件所列,如已離婚的父母親透過子女去了解他方之生活現況或現有資料的話,正是本人認為理應立例的原因之一。青少年的心理狀況往往深不可測的,即使有一些心事(可指一些不為人知的秘密)想去細訴給社工或師長等人知道,唯父母親要求理解,這可能令青少年更加憂鬱。縱使很多人抱著:父母親知道子女(包括成年或未成年)的近況理所當然的事這觀念,但此可引申伸到:丈夫或妻子了解配偶的個人資料等,因此,本人認為私隱條例不應只以本項為主去保障未成年人士的個人資料(私隱),應再加以條例。

個人資料部份:

本人先此聲明,本人不希望把本人的個人資料公開或經由不必需要者(準則只限有關當局:政制內地及事務局及個人私隱專處及其專員)查閱。及限制資料的用處只屬研究諮詢及作出回應的用途。

姓名:(刪除)

身份證號碼應與意見書無關

電話號碼:(刪除)/(手提)

住宅地址:(刪除)

聲明:

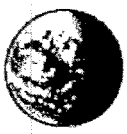
除個人資料部份,本人亦作出聲明。如上有任可資料或字眼及用詞上的錯誤,本人因此道歉,唯本人不會因此而負上任何責任。

本頁為第一頁,文件共有一頁。

二零零九年九月二十八日

(來信人要求不具名公開意見)

S0027



01/10/2009 18:41

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Public Consulatation on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sirs / Madam

Current :

All lucky draw at Mall, RTHK, Metro Radio and building security, they need to provide Name exactly in ID card, and the no.in first alphet with first 3 no. or 4 no.and mailing address.

Concern:

Internet UnSecurity and Unaccess people read the important info.

Suggest:

Not necessary the exactly name in ID card, but exactly the surename ;
No need the first alphet and random choosen from client the 4 no.in ID card
i.e. x3x4x5, etc..

Thank you for consideration

Happy Mid-Autumn Festival.



To pdpo_consultation@cmab.gov.hk
cc
bcc
02/10/2009 08:43 Subject 申請工作時的問題
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

你好嗎? 我想問一問在申請工作時,員工有什麼私穩權?
有時在填寫申請表時,差不多也需要提供由中學到10幾年後的工作經驗?
有無可能不公開員工本身的一世人的工作資料嗎?但又擔心公司不僱用這類員工,其實好頭痛.
有時只想好好地做一份文員,但又因為僱主知道我有多種技能而身兼多職,番下番工會由文員變成merchandiser and designer...
突然一身三職,僱主又想ｓａｖｅ　ｍｏｎｅｙ~
變了想找一份普通而安定的工時，好容易受到威脅~
（其實最關建是在填寫申請表時候，員工在填寫時決定是甚樣！）

麻煩可以提供一些意建給我們打公仔嗎？

謝謝你的寶貴時間！

（署名來函）

（來信人要求不具名公開意見）

S0029

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

S0030

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

(政府應該立法宮制網上資料，防止市民在網上犯法)
(政府應該立刻通知(警方商業及電腦罪案科同事，)
(和警方應該常常看網，防止市民在網上犯法的事情)
例如：在網上(誹謗別人)或者偷取(別人個人私隱資料)
在網上播，把別人(姓名，樣貌，年齡，身份証号码，和工作
地點，在網上播，都是犯法，(侵犯別人私隱罪)或者(偷拍別人
日常生活~~情形~~)在~~播~~網上播，然後收費，都是犯法，都是犯
法(侵犯別人私隱罪)，或者在網上播(作假新文報導)
(香港從來沒有發生這件案件，法庭沒有判決定罪)在網上播
說某人是(疑犯)或者(罪犯)都是犯法，犯了(誹謗別人罪)
(2009年5月6~~之間~~月之間，我曾~~經~~在網上看見有人(買別人~~(香港出世紙~~
(香港出世紙)~~來買~~，然後影印，買給非法入境，~~換取香港身份~~
換取(香港身份証)來港新方法。)看見信之後，立刻通知
(入境處的職員)市民取(什麼身份証明~~件件~~文件)
都要對取出(香港身份証)來(核對核實)是否(香港身份証持有人
才發放，(防止非法入境者來港)(買別人(出世紙)或(身份証)
和其他(香港身份証明文件)非法來港，的新方法。
(市民在網上看見有人犯法的事情，立刻通知警方，(警方在網
上看犯法的~~事~~事情，警方有權調查追究。網上犯法(如同現
實環境一樣，調查追究，捉那罪犯(市民不可濫用，新文自由
言論自由)直口，在網上犯法，(警方有權調查，追究捉那(罪犯
和(犯法網主)調查追究(嚴重的(網上犯法案件)警方有權叫
播主停播，接受警方調查。(所以市民要網上守法，做個好
公民。

（未能確定來信人是否願意公開姓名）

S0032

敬啟者：

本人因工作關係，需經常替公司老闆出外辦理私人事務，本人已持有老闆所發出之授權信並出示以作核對，但往往到達有關機構，例如銀行或其他機構辦理事務取文件，該機構卻要求本人出示身分証名文件及抄錄身分証號碼，甚至乎要求取得本人之身分證副本，這種要求實令本人之身分證資料會有被盜用或外洩的可能。本人深知若被抄錄身分証號碼或要求取得身分證副本時可向該公司或機構員工解釋有關個人資料(私隱)條例，甚至拒絕，這是否有其他更佳的方法提供本人日後再次遇上因工作關係，特別是替老闆辦理私人事務時，被抄錄身分証號碼或要求取得身分證副本。(請回覆)

現時香港無論電台、電視、報章及其他傳媒並沒有報導或宣傳有關個人資料(私隱)條例，而一般市民對私隱條例亦不明白更不關注。現貴處正資詢條例檢討期間，可否在大眾傳媒展開宣傳及教育香港市民有關條例細則，否則只有立法但在市民生活中未能真正實行出來，立法實屬空談，相信類似本人所遇到的情況只屬冰山一角。

第一頁

S0032

現懇請貴處盡快在香港立刻展開宣傳個人資料(私隱)條例，好使各人明白在自己的生活上或工作崗位如何保障或使用私隱條例，再次懇請貴處回覆本人以下之問題：

(一) 若銀行或公司機構若要求本人替老闆辦理私人事務時，被抄錄本人之身分證號碼或要求取得身分證副本是否違反了個人資料(私隱)條例，更鑑於當時本人已出示老闆之授權信並在信內已寫出本人之身分證號碼可作核實。

若沒有違反條例可否檢討和修訂這項條例以達市民在上述情況下得到保障。

(二) 懇請貴處立例監管香港各機構運作上有否違反了個人資料(私隱)條例。

此致

政制及內地事務局 （署名來函）

二零零九年九月三十日

抄送：香港個人資料私隱專員公署

本人地址：（刪除）

電郵：（刪除）

電話：（刪除） （來信人要求不具名公開意見）

第一頁

HKDMA

7th October, 2009

Team 4, Constitutional and Mainland Affairs Bureau,

Dear Sir / Madam,

After carefully reviewing the consultation document provided by your office, the HKDMA has only a few comments regarding some specific issues raised, but is in general agreement with the government position and recommendations regarding data privacy and security.

The HKDMA is a not-for-profit association dedicated to the interests of the direct marketing industry in Hong Kong, and modeled on the charter of the Direct Marketing Association headquartered in the US (an international association representing direct marketers worldwide). We believe that self-regulation is the most prudent and effective methods of ensuring compliance to best practices for both businesses and consumers across all forms of direct marketing. We further believe that this philosophy of self-regulation has been proven effective over decades in many countries and across many industries including direct marketing.

To that end, we strongly discourage the government from granting any additional authority or powers to the PCPD offices, and especially take exception to granting any enforcement to this agency. A glance at the caseload statistics supplied by the PCPD for the 2006-2008 time periods to gain insight into the current status of data security and privacy in Hong Kong would lead to the conclusion that the situation is actually quite good and under control. To put this into perspective, which is lacking in this presentation, it would be necessary to include a metric that included the total number of transaction from which these complaints had arisen. In that manner, one would have both a numerator and denominator and would see that the percentage of complaints when measured against total transactions is truly miniscule, certainly on the order of a fraction of a single percentage point. For example, we know that members of the HKDMA and HKCCA conduct millions upon millions of transactions annually, and using 2008 as a baseline, if those millions of transaction led to a grand total of 946 complaints (presumably not all even coming as a result of direct marketing), then the resulting percentage would be almost too small to measure.

This is not to excuse or dismiss any complaint, merely to provide some context to the overall situation, which the PCPD has consistently failed to provide. However, taking the PCPD's own numbers again, we can see that from 946 total complaints, only 96 resulted in compliance checks, and of those only 7 received enforcement notices, 5 were prosecuted, and only 2 were convicted. It seems to us that these numbers support our position, i.e. self-regulation is working, and the PCPD needs no further powers or authority.

With those comments as a background, we offer just a few further recommendations regarding specific issues.

Chapter 4 (B) 4.02: We believe that data processors should logically fall under the regulations applying to data users. We do not believe any separate direct regulation is necessary, and believe that the consultation paper presents arguments that support our position.

Chapter 4 (B) 4.19: We believe that internet based or related businesses, especially as identified whereby the data processor is differentiated from the data user, need no further direct or separate regulation.

Chapter 6 (G) 6.27: The writer of this document, or the PCPD, clearly does not understand the direct marketing business. Reference is made to "Direct marketing activities are prevalent in Hong Kong. Direct marketing calls are often a cause of complaint and nuisance to the data subjects." Firstly, direct marketing activities consist of a wide variety of media, usually integrated for maximum response. Outbound telemarketing calls, identified by the writer as "direct marketing calls" are only one part of the totality of direct marketing activities. This clear lack of any understanding of the business in question suggests that additional education is in order so that the PCPD can better execute their duties and responsibilities. We would be pleased to provide such education. Secondly, the second part of the statement is an expression of opinion, not fact, and it lacks any quantification whatsoever. To use the word "often" is a deliberately misleading attempt to create ammunition for additional penalties which are not needed. Again, referring to the PCPD's own numbers in this report, in actual fact, the number of complaints is extremely small already. Further penalties would not make a difference. The PCPD should know that responsible marketers DO NOT WANT to call people not interested in the product or service they offer, and want to take those people off their lists as quickly as they can. All responsible marketers already have definitive "opt out" options in place for such people wanting their names removed from lists. Contrary to the opinion of the PCPD, direct marketing is a business based upon cost-efficiencies, not a business based upon annoying people or becoming a nuisance.

Thank you for giving us the opportunity to provide commentary and feedback to this important work.

Cordially,

(Signed)

Eugene R. Raitt
Chairman
Hong Kong Direct Marketing Association

檢討《個人資料（私隱)條例》

個人資料私隱專員公署：

本人十分感激個人資料私隱專員公署檢討《個人資料(私隱)條例》，可以比市民發動表一些意見，改善現今《個人資料(私隱)條例》不足知處。使《個人資料(私隱)條例》變得完善。

本人有以下一些意見比本署。

本人是殘疾人士。我在勞工處展能就業科登記尋找工作，我知道勞工處展能就業科會將我們的學歷向第三者公開，這樣做我們殘疾人士覺得沒有問題，但是由於個人的學歷有高低之分，也有成功興失敗之分。高學歷及成功是所有人的理想及目標，但是有好多失敗者連會考試都不合格，他們都經過失敗的教訓都不喜歡別人講給有關自己失敗的考試成績。有一些人不斷向自己理想向前奮發，不論是否經過幾多次考試成績失敗，終於能夠達到自己理想目標，例如大學學位、高級文憑、副學士學位等等。點解勞工處展能就業科的就業主任要向僱主介紹我們殘疾人士，除了說我們有什麼殘疾外，連我們的學歷成績都向僱主介紹。但是勞工處展能就業科總是話你有什麼大學學位、高級文憑、副學士學位之外，也會說你會考什麼科目是拿的是 E、F、U 等等。其實點解不可以直接說最高學歷比較好一點？點解要由勞工處展能就業科的就業主任說這麼多的話？這樣我們好像再一次感受到失敗。這樣好像社會有不肯包容失敗者之心，是否可以幫助我們找尋工作？反而影響我們找尋工作，因爲我們加上了一些殘疾，是特別顯示出我們很困難找到工作面試！我們的苦，有唯共鳴？這是我們的(個人私隱)，我們不想自己不理想成績向外公開！只是希望公開自己的長處及最好成績，不理想成績由本人向僱主親自公開，這是十分理想的事。

最後，本人有以下意見及解決方法。

1. 如果要公開我們的會考成績及其他學歷成績，希望勞工處展能就業科可以比我們殘疾人士有選擇是否公開的字眼。
2. 希望在選擇公開成績及學歷方便，有讚成有反對的選擇。包括：(口頭、履歷表等)
3. 希望一年可以比我們簽一次，因爲都是我們的(個人私隱)。可以比我們評估一年的《個人資料(私隱)條例》是否對我們有益還是錯的選擇！
4. 希望勞工處展能就業科重量說我們高學歷及成功方便，失敗的不要公開！

多謝個人資料私隱專員公署比我發表意見。

S0034

(署名來函)

09/10/09

(來信人要求不具名公開意見)



To <pdpo_consultation@cmab.gov.hk>
cc
bcc
09/10/2009 13:46 Subject Opinion on Personal Data and Privacy Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

History: This message has been replied to.

Dear Sirs

I am emailing to express my opinion on the issue of personal data and privacy issues in Hong Kong. Being an expat, I feel the use and provision of personal data in Hong Kong is rather frequent that it actually provides the citizen with hardly any privacy whatsoever.

An example to point is the requirement to provide your ID number to consumer shops and its request by banks, even when you are an existing client and could easily just provide your ATM card and personal details eg date of birth, address etc.

I feel that the ID card is akin to my passport and should not be easily shown/disclosed/photocopied by a third party agent unless needed eg for account opening purposes etc. I remember going to IFC 2 offices for the first time and was required to provide my ID number. I was, initially, reluctant but was ordered to provide it or else I could not enter the premises for an interview. Again, once provided, who knows how such sensitive data could be used or obtained.

The ID card is just that, a means of identification for each HK citizen, which has been a long used item in Hong Kong. However, its provision/disclosure to third parties should be more closely guarded and provided only for pertinent uses.

Kind regards

Katherine

13/10/2009 10:19

To "pdpo_consultation@cmab.gov.hk" <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject the Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir / Madam,

I am Stephen Chan, working at the company handling the information for customers in HK, our company name is Confidential Materials Destruction Service Limited, established since 1984.

I would like to suggest the following about 'Data Security' to the board :

1. Personal Data (Privacy) Ordinance (PDPO) Chapter 486, rules 14 & 15 restrict the user to register for the usage of information, they should also set rules to restrict the information handler, the information handler should make registration to the PCPD, declare their ability, security process to handle & destroy the information.
2. Privacy Commissioner for Personal Data (PCPD) should responsible to monitor those information handlers' process; to verify their ability in handling information destruction process. If the handler is not capable or qualified, they cannot have the right to handle /destroy the information for customers. That is, they cannot be registered on the list of information handler.
3. PCPD should set the qualification requirement or grading to those information handlers, customers can check with this index list to choose the service provider.
4. There is an association named National Association of Information Destruction in USA, which setting AAA grade to information handlers or service providers. Customers can have a clear pictures of the service provider.
5. For those smallest service providers, monitoring system is much important, as they do not pay much responsibilities and care to their service standard.
6. It is better to set the punishment and penalty for those contravene with the rules

Please feel free to contact us at (deleted) for further information. Attached my name card for your good reference.

Thanks with best regards,

Stephen Chan cmds_stephen.pdf

TO..... DATE..... NO .....

私隱事員，你好，本人有些意見，希望能表達出來，本人希望能在見工的時候，假定如未聘請的時候，希望能取回填寫申請表格，取回個人的資料，能得到保障自己的資料。同時本人覺得很多時收到一些推銷電話，本人是用增值卡的，但是經常收到這些來電，本人懷疑是電訊公司，將本人的電話號碼買給其他公司，希望能立例保障，沒有本人同意下，不可將我的手提電話買給他人。

（署名來函）

祝你工作愉快
09-10-12

（未能確定來信人是否願意公開姓名）

我本人（刪除）應希望
私隱專員提供法律協助
應本人身上有政府盜聽器
希望抵下應盜聽器張本
人的私隱和資料外洩事
故影響生活和安全希望
私隱專員給救援和支援
法律協助能否回應私隱專
員的意見 本人（刪除）電話
（刪除）希望有回應和支援
法律協助

（未能確定來信人是否願意公開姓名）

·投訴 OGCIO 部門總部：

事關無其他政府部門將做滿二十，三十年的人名公開在 Lotus Notes，好無私隱條例，希望可以設有處理，因為不又一年，年年如事，政府應該查下此事。

不想公開身份。

（來信人要求不具名公開意見）

S0039

S0040

Our STRONG views on PD(P)O:

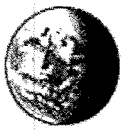
proposal	Pros	Cons
Sensitive personal data, such as employee id card and fingerprints, should be subject to more stringent regulation. But e-channel can be maintained status-quo	Clocking in and out do not reflect diligence of self-initiated and motivated employees performing outdoor work Such actions degrade employee-employer relation In accordance with guiding principles	
The PCPD should NOT be given criminal investigation and prosecution power	Privacy is not as severe as criminal offences In accordance with guiding principles	
The PCPD should NOT provide legal assistance	Public resources and finance should be better allocated and used elsewhere Privacy is not as severe as criminal offences In accordance with guiding principles	
If the PCPD is empowered to award compensation, it should not be from public resources	Public resources and finance should be better allocated and used elsewhere In accordance with guiding principles	
Contravention of a Data Protection Principle should NOT be an offence	Privacy is not as severe as criminal offences In accordance with guiding principles	
A person disclosed personal data should NOT be an offence	Privacy is not as severe as criminal offences In accordance with guiding principles	
A data user intentionally resumes the same contravening act should NOT be an offence	Privacy is not as severe as criminal offences In accordance with guiding principles	
The PCPD should NOT impose monetary penalty	Privacy is not so severe In accordance with guiding principles	
Penalty for repeated non-compliance should NOT be heavier	Privacy is not so severe In accordance with guiding principles	
Direct marketing penalty should be raised	penalty should be heavy to deter	

S0040

	In accordance with guiding principles	
Third party should NOT give consent to the change of use	Third party complicates cases In accordance with guiding principles	
Full-time students should NOT refuse a data access request made by education institute or parents	education institute or parents use data for benefits of full-time students Minor is not mature and experienced enough to decide best interests In accordance with guiding principles	
Law enforcement agencies, rescue and relief agencies should NOT be exempted unless life is endangered. They should never disclose to mass media without permission of affected individuals or family representative of deceased	mass media should not use right for public to know as illegal and unreasonable excuse to offend privacy In accordance with guiding principles	
Data of minors relevant to parental care OR guardianship should be allowed to transfer	parents use data for benefits of minor In accordance with guiding principles	

(name)

(The sender requested anonymity)



To pdpo_consultation@cmab.gov.hk
cc
bcc
23/10/2009 19:13 Subject 私隱條例檢討諮詢-my comments

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Hi,
just want to make two comments about the handling of ID cards.
1. I hate it when especially in the hotels in China, and also sometimes in the banks here even in Hong Kong, they take my ID card and leave it on the counter that is visible to everyone standing nearby, so people can read all details on my ID card. I think there should be a rule to protect this.
2. I have been to too many places where they photo copy my ID card. WHY? When I sign a contract for a phone service? And many many times at the banks! Even at the hotels in China, this copying of my ID card, along with my visa card info, phone numbers, e-mail address, and home address, they could do a lot with them! Please protect us.
Thank you very much.
Margaret Lee



To pdpo_consultation@cmab.gov.hk
cc
bcc
29/10/2009 12:53 Subject 有關個人資料條例意見
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

本人對個人資料私隱條例有以下意見

本人發覺有一個很嚴重的問題，現時所有用電話處理賬戶的方法，對方的接線生都會問及當事人的姓名身份證號碼等資料。
這完全是單方面核對資料，而當事人卻無從得知接線生是否在套取個人資料。

只是單方面接線生需要認證當事人是賬戶本人，而要求當事人提供資料來核對電腦記錄，但反過來當事人卻無法知道接線生是否該公司的服務員，而且有權力核對資料。

在這過程中，因爲當事人單方面提供資料，對方可以假借核對的名義而提抄下資料作其他用途。
例如: 這接線生根本不能進入公司系統，但因爲套取了資料而可進入系統偷個人其他資料作商業用途，甚至犯罪活動。

從不少的經驗中，這些電話處理的個案是沒有下文，要再三聯絡才有進展，在這些過程中，有可能資料被套取了。

這是一個很嚴重的漏洞，建議在這些驗證程序中，應該是雙方面核對資料。

並且要盡快立例禁止這種單方面套取資料的電話服務。

==========
Best regards
Rufus Chung 鍾澤偉



To "pdpo_consultation@cmab.gov.hk" <pdpo_consultation@cmab.gov.hk>

cc

29/10/2009 19:02

Subject my opinion to the pdpo

1. 本人想請問物業資料(即地址)為什麼不是个人私隱資料？為什麼打開本雜誌，名人手上的物業，無論是過去或現在持有，都可一覽無遺？

我本人認為每个人都有權為自己的地址保密的

2. 為什麼land registry的物業查察不是by一个物業去查察，而是可以容許物業代理去用某人身份証id或姓名去list out某人的所有物業資料。又或者容許download物業資料庫去support不合理利用物業資料

我的经歷如下:一天到xx物業代理找一名代理，他不在，我便坐下等他，期間聽到一班物業代理在討論某某先生委託他們出售单位的价钱，一名看着电脑的中年代理説："我check到某某先生都就快破產，他手上持有xx花園，xx大厦...现在放售的单位還不減价，可大幅壓价"

試問為什麼可以這樣利用別人的个人的物業資料去引至不公平交易。

（ 來信人要求不具名公開意見 ）

S0044

Our Reference 發文編號:
Your Reference 收文編號: CMAB/CR/7/22/40 Pt. 7
Telephone 電話:
Fax 傳真:

29 October 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong
(Attn : Miss Joanna C. H. Choi)

Dear Miss Choi,

Public Consultation on
Review of the Personal Data (Privacy) Ordinance

Thank you for your letter dated 28 August 2009 to the Chairman of ("the Organisation") on the review of the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486).

The "Org" fully supports affording adequate protection to personal data. In this regard, the "Org" has complied with the relevant provisions governing the handling of personal data. As the regulator of the broadcasting industry, the "Org" has promulgated in the Codes of Practice on Television and Radio Programme Standards that broadcasting licensees should observe the PDPO. In addition, the licences of domestic pay and non-domestic pay television programme services also stipulate that in addition to the obligation under the PDPO, the licensee has to ensure that subscriber data or information will not be disclosed to any other person without prior approval from the subscriber.

As for the details of the proposals made in the consultation paper, we have no particular comments to make.

Yours sincerely,

(Signed)

Secretary

(The sender requested anonymity)

S0045

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)



To pdpo_consultation@cmab.gov.hk
cc
bcc
01/11/2009 13:16 Subject 私隱 諮詢

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

你好!

我看過個人資料條例的諮詢文件後, 我認爲:
現在科技發達, 日常生活中, 真的好多時候會把個人資料給予別人處理!
例如: 網上登記, 電話登記, 經過朋友, 見工, 消費, 電話公司, 政府部門,

對我而言, 個人資料及私隱的定義是關於個人姓名, 電話, 地址, 電郵, 生日, 身份證, 教育程度, 學業, 工作, 家庭資料, 信用卡, 相片, 身體, 病歷, 等等.

其實我之前好奇地問過貴署, 原來投訴人要有證據證明發放資料者做過侵犯個人私隱的事! 貴署看到有證據才去調查事件, 所以成功檢控的個案每年只有2,3宗! 就像禁煙條例也需要改善! 聽說是控煙人員捉到違規者, 需要對方填很多資料, 通常未填完, 那人就走了! 所以政府推出這些法例, 爲了保護市民, 可是檢控程序, 仍然不夠完善!
因此本人很贊成貴署是次諮詢事宜!

以下舉幾個例子, 其實現在只是講信字, 很多時貴署真的保障不到市民!
日常生活中, 我時常收到電話, 電郵上的廣告, 的確很煩! 我想究竟誰人未經我同意把我的資料給予第三者?

很多求職者在尋找工作時, 需要把履歷表給予公司! 例如: 電話留下個人資料, 電郵履歷表到公司, 到公司見工時填個人資料! 假設有人心懷不軌把求職者的個人資料放上網或公開或派發給人或給予其他

公司, 或者透露給別人!

近年很多人爲了報仇, 一班人捉了一個人去拍短片, 要虐打或脫衣或強姦等等, 再把短片放上網上討論區, YOUTUBE, 電話! 爲什麼又不把公開此人的私隱身體的這班人當作是遺反私隱條例? 我清楚知道警方已有法例去檢控這班人, 不過可否雙重保障呢?

假設某人與某人結怨, 把對方的私事或個人資料亂唱, 或者把相片放上網! 爲什麼又不是違反私隱條例? 我清楚知道這是誹謗罪, 不過又可否雙重保障呢?

假設到診所看病, 需要出示身份證, 職員看到身份證的資料! 我怎樣確保職員會不公開呢? 所以就要加強及立法去保護個人私隱!

談到違反私隱條例是否需要等於犯法, 要坐監等刑罰? 我認爲自己是市民, 不敢說要判幾多年才夠! 不過的確需要用罰款及判監去杜絕這些違反者!
我建議可以向所有公司規定, 要求他們在(填寫個人資料)的文件上, 聲明: 本公司把你的個人資料只作求職用途, 一切資料會保密! 本公司如有違法, 你可致電私隱專員公署: XXXXXXX　另外, 可以規定公司, 在求職者要求下, 叫公司把填寫個人資料的影印本給予求職者, 如要收費, 0.5元! 此外, 僱員在僱主公司的個人資料, 也需要得到一份聲明! 另外, 可以像職業安全規例咁, 規定公司裏要最少有一人能去接受貴署的保護個人資料訓練, 而得到證書!
另外, 立法規定貴署可以抽籤形式去公司查他們處理個人資料的方法是否恰當? 就像海關抽查公司有沒有盜版! 另外, 也可以立法規定公司要呈交如何處理個人資料的聲明!

另外, 有些情況會被豁免! 我建議不能豁免! 要看違反者是否有動機? 及是否有公開個人資料! 我也贊成通報機制, 貴署可以通過郵寄, 及電話跟進去通知受害人!

另外, 我贊成授予私隱專員刑事調查及檢控權力! 也贊成把重覆違反者訂爲罪行, 以阻嚇作用!

最後, 我很欣賞貴署對香港市民的貢獻! 也衷心希望貴署做得更好!
謝謝!

TINA LAU

副本:

政制及內地事務局局長:

個人私隱條例資詢回應 S0047

個人私隱條例神化了「身分證」號碼,令香港各大小機構誤以為身分證號碼為「密絕機密」,以致誤用及濫用來核實「個人身份」!

試舉一例,致電「　　」熱線去操縱用戶個人戶口資料及服務,該公司需要致電者說出「身分證號碼」核實用戶身份,然後才可進行。如致電者在公眾場合不便說出,便得不到服務,此乃誤/濫用難病之一。

更嚴重者,身分證號碼跟着市民一生一世,絕不能更改。一生人中不止N次disclose, fill out, say out ..... 身分證號碼,洩露絕不為奇。如果有人得悉我「　　」身分證號碼,然後致電例如「　　」,便可操縱我戶口一切運作,如中門大開,有掩難籠,市民生命財產得不到保障!

** 所以我提議嚴禁以「身分證號碼」核實個人身份以運作個人戶口或可能令用戶有所損失的交易 **

而改以「用戶自訂」的密碼取而代之。

用戶自訂密碼，洩露後可以隨時更改；但「身分證號碼」跟着市民一生一世，就算死後也不能更改。

所以我有理由要求私隱專員考慮立法禁止用以上述本號內的運作。並要注宣傳各大小機構停止以「說出身分證號碼就核實為其本人」的胡混操作。再者，生物特徵跟身分證號碼同是「唯一」，以及「終生不可更改」，所以身分證號碼跟指紋、眼影等無異！

市民」

江燦良同應

18-10-2009

P.S. 請 立即停止
以本人身分證號碼在熱線核實本人身份。
因本人身分證號碼已非秘密。請以本人收聽留言密碼代之。以保障本人一切。

S0048

02/11/2009 14:09

To "'pdpo_consultation@cmab.gov.hk'" <pdpo_consultation@cmab.gov.hk>

cc

bcc

Subject Public consultation on the Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sirs,

We are pleased to submit the attached responses to the Consultation Document on Review of Personal Data (Privacy) Ordinance.

Best Regards,
David Fu

David Fu
Company Secretary
Swire Pacific Limited

2009.11.02 PPDO Consultation Response (SPAC).doc

SWIRE PACIFIC

S0048

2nd November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

By email: pdpo_consultation@cmab.gov.hk

Dear Sirs,

Responses to Consultation Document on Review of Personal Data (Privacy) Ordinance

We are pleased to submit the attached responses to the Consultation Document on Review of Personal Data (Privacy) Ordinance.

Yours sincerely,
For SWIRE PACIFIC LIMITED
David Fu
Company Secretary

Encl.

Responses to Consultation Document on Review of Personal Data (Privacy) Ordinance

Proposal No. 1: Sensitive Personal Data

Whether there is a need to accord better protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances; and

No. We do not consider that the additional cost and burden of complying with such a prohibition is justified by its apparent benefits.

If yes, whether the possible regulatory regime, including coverage of sensitive personal data, related regulatory measures, sanctions, and the need for grandfathering or transitional arrangement as set out in paragraphs 3.08 to 3.14, is appropriate.

If such a prohibition is imposed, the information covered should be limited to the biometric data referred to in 3.08 of the Consultation Document, there should be exceptions to the prohibition as described in 3.09 of the Consultation Document (but the medical exception should be broadened as described below), the prohibition should be subject to the existing enforcement regime (that is only breach of an enforcement notice should give rise to penalties) and the handling of existing biometric information should not be prohibited (that is there should be grandfathering arrangements not transitional arrangements). The medical exception should be broadened so that it applies to the handling of sensitive personal data for any purpose related to health or safety.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

Whether a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties;

No. It is inappropriate for data users, as private persons, to have a responsibility to police compliance with the law by other private persons (data processors). In any event imposition of contractual obligations will not necessarily result in compliance. The data processors may simply breach the contractual provisions.

Whether the activities of a data processor should be directly regulated under the PDPO or whether it is sufficient to indirectly regulate the data processor through the data user by contractual or other means; and

Having regard to the discussion in the Consultation Document (in particular in relation to the practical difficulties for data processors of compliance), we do not think that the activities of data processors should be directly regulated. We would also mention that direct regulation of data processors would risk

driving them offshore to jurisdictions where they were not regulated, to the detriment of the Hong Kong economy and Hong Kong's international competitive position. For the reasons given in the previous response, we do not think that activities of data processors should be regulated by contractual means.

If activities of data processors were to be directly regulated under the PDPO, what obligations should be imposed on data processors, and whether it is appropriate and practical to subject different categories of data processors to different obligations.

Not strictly applicable, in the light of our previous response, although we would not object to the suggestion in 4.19 of the Consultation Document that data processors should have a privacy policy (so long as no attempt was made in or through the legislation to describe what the elements of that policy should be).

Proposal No. 3: Personal Data Security Breach Notification

The need to institute a voluntary privacy breach notification system in Hong Kong.

We agree that a breach notification system should not be compulsory. We are not aware of evidence that timely and sufficient notification of material breaches is not being given (and this is unsurprising given that the two most likely sources of material breaches, government and the financial industry, have voluntary systems in place). This being so, we do not think that anything further needs to done by way of legislation or guidelines in this area.

The components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42, including:

(i) the circumstances under which notification should be triggered;

(ii) to whom the notice of breach should be sent;

(iii) timing of the notice;

(iv) by what means should the notice be sent;

(v) the content to be covered in the notice; and

(vi) the consequences of failing to give notification.

Not applicable in view of our previous response.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

Whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.

Having regard to the discussion in the Consultation Document, we agree that the status quo should be maintained, particularly in the light of the very small numbers of prosecutions actually undertaken and the general desirability of an objective assessment (by the Department of Justice) as to whether a prosecution is justified in any particular case.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

Whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under Section 66 of the PDPO, along the lines of the EOC model.

We do not support the conferring of this power. It seems to us that there is nothing peculiar to the privacy legislation which would justify taxpayers' money being made available to pursue a civil action under the legislation in circumstances where taxpayers' money would not be so made available under normal legal aid principles.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

Whether it is appropriate to introduce at this stage an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Having regard to the discussion in the Consultation Document (in particular the point made by the Law Reform Commission that conferring such a power would vest in a single authority an undesirable combination of enforcement and punitive functions), we do not support the conferring of such a power.

Proposal No. 7: Making Contravention of a DPP an offence

Whether we should make contravention of a DPP an offence.

Having regard to the discussion in the Consultation Document (in particular in relation to the impact on civil liberties and the original intention of the DPPs), we do not support making the contravention of a DPP an offence.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

Whether we should make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent; and

We have no objection to the creation of such an offence, so long as it is confined to disclosure for profit. Malicious purposes is too broad and uncertain a term. .

If yes, the need for defence provisions and the appropriate level of penalty.

If the offence is confined as proposed by us, we would not see the need for specific defences. If an offence along the UK lines is created, the UK defences should be applicable. We have no particular views on the level of penalty.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

Whether it is appropriate to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice; and

Having regard to the discussion in the Consultation Document (in particular the absence of repeat offences in practice) we do not consider it appropriate to create such an offence.

If yes, the appropriate penalty level for the offence bearing in mind that non-compliance with an enforcement notice is subject to a fine of $50,000 and to imprisonment for two years.

Not applicable, in the light of our previous response.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

Whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

Having regard to the discussion in the Consultation Document, we do not consider it appropriate to impose such penalties.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

Whether heavier penalty should be imposed for a second or subsequent conviction of Section 64(7); and

Given the lack of prosecutions for repeat offences referred to in the Consultation Document, we do not think such heavier penalties are necessary.

If yes, the appropriate penalty level, bearing in mind the existing enalty level for contravention of an enforcement notice which is a fine at Level 5 (up to $50,000) and imprisonment for two years, and in case of a continuing offence, a daily fine of $1,000.

Not applicable, in the light of our previous response.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

Whether the penalty for misuse of personal data in direct marketing (i.e. contravention of the requirement under Section 34(1)(ii)) should be raised; and

We have no views on this proposal.

If yes, the appropriate level of penalty.

Not applicable, in the light of our previous response.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

We support this proposal.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

We have no views on this proposal, save to say that, if the proposal is implemented, the legislation should impose no obligation on the data user (expressly or by implication) to form an opinion on whether the disclosure is in the interests of the minor.

Proposal No. 15: Access to Personal Data in Dispute

We support the proposal (as set out in paragraph 16 of Annex 1).

Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We support the proposal that the PDPO should be amended so that a data user need not comply with a data access request if the data user is entitled or bound by other legislation not to disclose the relevant information.

Proposal No. 17: Erasure of Personal Data

We support the proposal for the amendment of the PPDO set out in paragraph 23 of Annex 1.

Proposal No. 18: Fee Charging for Handling Data Access Requests

We do not think that the legislation needs changing, given what we assume is a relatively modest number of complaints about excessive charges. In addition, given the speed of technological change, any attempt to prescribe

particular maximum charges for particular items runs the risk of very rapid obsolescence.

Proposal No. 19: Response to Data Access Requests in Writing and Within 40 days

We think it undesirable to create a special regime for the police, though we understand that, if the legislation is amended as suggested, they will need a special regime. We think the better solution is not to amend the legislation.

Proposal No. 20: Circumstances for Issue of an Enforcement Notice

We have no views on the option in paragraph 39 of Annex 1.

Proposal No. 21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

We have no views on the option in paragraph 40 of Annex 1.

Proposal No. 22: Removing the Time Limit to Discontinue an Investigation

We have no views on the option in paragraph 43 of Annex 1.

Proposal No. 23: Additional Grounds for Refusing to Investigate

We have no views on the appropriateness of including the specific grounds referred to in paragraph 48.

Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

We support the exemption of such transfers. We think that the only condition necessary is that the transfer is required for the purposes of due diligence.

Proposal No. 25: Provision of Identity and Location Data on Health Grounds

We support changes to the legislation so that it operates along the lines described in paragraph 56 of Annex 1.

Proposal No. 26: Handling Personal Data in Emergency Situations

We support the proposed exemptions.

Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

We have no views on this proposal.

Proposals not to be Pursued

We agree that none of the proposals identified as not to be pursued need to be pursued.

Miscellaneous Proposed Amendments to the PDPO

We have no objection to the miscellaneous proposed amendments to the PDPO.

S0049

02/11/2009 14:10

To "'pdpo_consultation@cmab.gov.hk'" <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Public consultation on the Review of the Personal Data (Privac Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sirs,

We are pleased to submit the attached responses to the Consultation Document on Review of Personal Data (Privacy) Ordinance.

Best Regards,
David Fu

David Fu
Company Secretary
Hong Kong Aircraft Engineering Company Limited

20091102 PPDO Consultation Response (HAECO).doc

S0049

HAECO

2nd November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

By email: pdpo_consultation@cmab.gov.hk

Dear Sirs,

Responses to Consultation Document on Review of Personal Data (Privacy) Ordinance

We are pleased to submit the attached responses to the Consultation Document on Review of Personal Data (Privacy) Ordinance.

Yours sincerely,
For HONG KONG AIRCRAFT
ENGINEERING COMPANY LIMITED

David Fu
Company Secretary

Encl.

HAECO

Responses to Consultation Document on Review of Personal Data (Privacy) Ordinance

Proposal No. 1: Sensitive Personal Data

Whether there is a need to accord better protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances; and

No. We do not consider that the additional cost and burden of complying with such a prohibition is justified by its apparent benefits.

If yes, whether the possible regulatory regime, including coverage of sensitive personal data, related regulatory measures, sanctions, and the need for grandfathering or transitional arrangement as set out in paragraphs 3.08 to 3.14, is appropriate.

If such a prohibition is imposed, the information covered should be limited to the biometric data referred to in 3.08 of the Consultation Document, there should be exceptions to the prohibition as described in 3.09 of the Consultation Document (but the medical exception should be broadened as described below), the prohibition should be subject to the existing enforcement regime (that is only breach of an enforcement notice should give rise to penalties) and the handling of existing biometric information should not be prohibited (that is there should be grandfathering arrangements not transitional arrangements). The medical exception should be broadened so that it applies to the handling of sensitive personal data for any purpose related to health or safety.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

Whether a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties;

No. It is inappropriate for data users, as private persons, to have a responsibility to police compliance with the law by other private persons (data processors). In any event imposition of contractual obligations will not necessarily result in compliance. The data processors may simply breach the contractual provisions.

Whether the activities of a data processor should be directly regulated under the PDPO or whether it is sufficient to indirectly regulate the data processor through the data user by contractual or other means; and

Having regard to the discussion in the Consultation Document (in particular in relation to the practical difficulties for data processors of compliance), we do not think that the activities of data processors should be directly regulated. We would also mention that direct regulation of data processors would risk

driving them offshore to jurisdictions where they were not regulated, to the detriment of the Hong Kong economy and Hong Kong's international competitive position. For the reasons given in the previous response, we do not think that activities of data processors should be regulated by contractual means.

If activities of data processors were to be directly regulated under the PDPO, what obligations should be imposed on data processors, and whether it is appropriate and practical to subject different categories of data processors to different obligations.

Not strictly applicable, in the light of our previous response, although we would not object to the suggestion in 4.19 of the Consultation Document that data processors should have a privacy policy (so long as no attempt was made in or through the legislation to describe what the elements of that policy should be).

Proposal No. 3: Personal Data Security Breach Notification

The need to institute a voluntary privacy breach notification system in Hong Kong.

We agree that a breach notification system should not be compulsory. We are not aware of evidence that timely and sufficient notification of material breaches is not being given (and this is unsurprising given that the two most likely sources of material breaches, government and the financial industry, have voluntary systems in place). This being so, we do not think that anything further needs to done by way of legislation or guidelines in this area.

The components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42, including:

(i) the circumstances under which notification should be triggered;

(ii) to whom the notice of breach should be sent;

(iii) timing of the notice;

(iv) by what means should the notice be sent;

(v) the content to be covered in the notice; and

(vi) the consequences of failing to give notification.

Not applicable in view of our previous response.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

Whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.

Having regard to the discussion in the Consultation Document, we agree that the status quo should be maintained, particularly in the light of the very small numbers of prosecutions actually undertaken and the general desirability of an objective assessment (by the Department of Justice) as to whether a prosecution is justified in any particular case.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

Whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under Section 66 of the PDPO, along the lines of the EOC model.

We do not support the conferring of this power. It seems to us that there is nothing peculiar to the privacy legislation which would justify taxpayers' money being made available to pursue a civil action under the legislation in circumstances where taxpayers' money would not be so made available under normal legal aid principles.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

Whether it is appropriate to introduce at this stage an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Having regard to the discussion in the Consultation Document (in particular the point made by the Law Reform Commission that conferring such a power would vest in a single authority an undesirable combination of enforcement and punitive functions), we do not support the conferring of such a power.

Proposal No. 7: Making Contravention of a DPP an offence

Whether we should make contravention of a DPP an offence.

Having regard to the discussion in the Consultation Document (in particular in relation to the impact on civil liberties and the original intention of the DPPs), we do not support making the contravention of a DPP an offence.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

Whether we should make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent; and

We have no objection to the creation of such an offence, so long as it is confined to disclosure for profit. Malicious purposes is too broad and uncertain a term.

If yes, the need for defence provisions and the appropriate level of penalty.

If the offence is confined as proposed by us, we would not see the need for specific defences. If an offence along the UK lines is created, the UK defences should be applicable. We have no particular views on the level of penalty.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

Whether it is appropriate to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice; and

Having regard to the discussion in the Consultation Document (in particular the absence of repeat offences in practice) we do not consider it appropriate to create such an offence.

If yes, the appropriate penalty level for the offence bearing in mind that non-compliance with an enforcement notice is subject to a fine of $50,000 and to imprisonment for two years.

Not applicable, in the light of our previous response.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

Whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

Having regard to the discussion in the Consultation Document, we do not consider it appropriate to impose such penalties.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

Whether heavier penalty should be imposed for a second or subsequent conviction of Section 64(7); and

Given the lack of prosecutions for repeat offences referred to in the Consultation Document, we do not think such heavier penalties are necessary.

If yes, the appropriate penalty level, bearing in mind the existing enalty level for contravention of an enforcement notice which is a fine at Level 5 (up to $50,000) and imprisonment for two years, and in case of a continuing offence, a daily fine of $1,000.

Not applicable, in the light of our previous response.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

Whether the penalty for misuse of personal data in direct marketing (i.e. contravention of the requirement under Section 34(1)(ii)) should be raised; and

We have no views on this proposal.

If yes, the appropriate level of penalty.

Not applicable, in the light of our previous response.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

We support this proposal.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

We have no views on this proposal, save to say that, if the proposal is implemented, the legislation should impose no obligation on the data user (expressly or by implication) to form an opinion on whether the disclosure is in the interests of the minor.

Proposal No. 15: Access to Personal Data in Dispute

We support the proposal (as set out in paragraph 16 of Annex 1).

Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We support the proposal that the PDPO should be amended so that a data user need not comply with a data access request if the data user is entitled or bound by other legislation not to disclose the relevant information.

Proposal No. 17: Erasure of Personal Data

We support the proposal for the amendment of the PPDO set out in paragraph 23 of Annex 1.

Proposal No. 18: Fee Charging for Handling Data Access Requests

We do not think that the legislation needs changing, given what we assume is a relatively modest number of complaints about excessive charges. In addition, given the speed of technological change, any attempt to prescribe

particular maximum charges for particular items runs the risk of very rapid obsolescence.

Proposal No. 19: Response to Data Access Requests in Writing and Within 40 days

We think it undesirable to create a special regime for the police, though we understand that, if the legislation is amended as suggested, they will need a special regime. We think the better solution is not to amend the legislation.

Proposal No. 20: Circumstances for Issue of an Enforcement Notice

We have no views on the option in paragraph 39 of Annex 1.

Proposal No. 21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

We have no views on the option in paragraph 40 of Annex 1.

Proposal No. 22: Removing the Time Limit to Discontinue an Investigation

We have no views on the option in paragraph 43 of Annex 1.

Proposal No. 23: Additional Grounds for Refusing to Investigate

We have no views on the appropriateness of including the specific grounds referred to in paragraph 48.

Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

We support the exemption of such transfers. We think that the only condition necessary is that the transfer is required for the purposes of due diligence.

Proposal No. 25: Provision of Identity and Location Data on Health Grounds

We support changes to the legislation so that it operates along the lines described in paragraph 56 of Annex 1.

Proposal No. 26: Handling Personal Data in Emergency Situations

We support the proposed exemptions.

Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

We have no views on this proposal.

Proposals not to be Pursued

We agree that none of the proposals identified as not to be pursued need to be pursued.

Miscellaneous Proposed Amendments to the PDPO

We have no objection to the miscellaneous proposed amendments to the PDPO.

致：私隱專員公署：

本人就有關招聘時遞交個人資料，僱主或面試員工操守行爲，提出意見。

(1) 立法規定在未決定聘請有關職位員工時，不得擅自影印該個人資料，祇可核對。

(2) 立法聘請後影印該個人資料，必須再加蓋影印字樣。

(3) 立法要有關行政人員或人事部才可處理，有關個人資料不可隨便擺放及給第三者見到。

申訴人：(署名來函)

日　期：28-9-2009

(未能確定來信人是否願意公開姓名)

S0051



06/11/2009 17:14

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Consultation

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

I was one of the attendants to the Briefing Session: Consultation on the Review of the Personal Data (Privacy) Ordinance in HR perspectives organized by HKIHRM today. After reviewing the consultation paper, I would like to suggest that all senstive personal data (if adopted after the consultation) stored in electronic format should be requested to be encrypted. Given it do happens from time to time of data leaking through the internet / fringer device, the data collectors/users should have an obligtaion to ensure the data is always in encryted form which will minimize the exposure of personal data in case of leaking to the public.

Nelson Lau

S0052

HKFI
The Hong Kong Federation of Insurers
香港保險業聯會

Your Ref : CMAB/CR/7/22/40 Pt.7

BY FAX **AND BY MAIL**

5 November 2009

Ms Joanna Choi
Principal Assistant Secretary (4)
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong

Dear Ms Choi

RE: Consultation on the Review of the Personal Data (Privacy) Ordinance

Thank you for your letter dated 28 August 2009, inviting us to comment on the subject matter.

We have consulted our member companies, and their comments are set out as follows:

Proposal No. 1: Sensitive Personal Data

- Some clients cannot write and opt to use fingerprints as their signature specimen. In these circumstances it is necessary to allow collection of fingerprints as signature specimens of the clients and storage of fingerprints in the form of hardcopy and scanned copy in the imaging system as other personal data.
- We agree that protection is required for sensitive personal data. However, there is uncertainty on the definition of the sensitive personal data. The example of biometric data is considered as highly sensitive. The more information that is classified as sensitive personal data. The cost in supporting the operations will be increased substantially which may undermine the competitiveness of the business. We therefore suggest defining "sensitive personal data" clearly. From our experience, a clearer definition would help avoid potential contravention and possible abuse by concerned parties.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

- As data collectors and data users, some member companies currently impose on their service providers/business partners contractual obligations of confidentiality, including clients' personal data. However, it is not always practicable for our member companies to control possible breach of obligations by data processors. Therefore, imposing statutory obligations directly on data processors would be a more effective and pragmatic approach.

Ms Joanna Choi
Principal Assistant Secretary (4)
Constitutional and Mainland Affairs Bureau

- The use of contractual means also gives rise to another concern for group companies whereby the contract is signed between one company within the Group and the data processor (which provides service to the entire Group). Where the breach affects a company within the Group which is not the signing entity, the privity doctrine may prohibit the affected company which is not a party to the contract from acquiring and enforcing rights under the contract, and thereby failing to meet the proposed requirement.
- We agree to exercise tighter control over data processors. Data processors should be categorized so that different level of controls can be applied to different types of data processors. Detailed guideline can be developed in consultation with representatives from the industrial groups.
- We recommend that government / PCPD should directly regulate the data processor or sub-contractors by imposing obligations on them. If these subcontracted parties do not have the legal liability, it would be difficult for the data user to check that they have taken all practicable steps to ensure security and safekeeping of personal data, etc.
- Sub-contracting of data processing work is a rising trend in commercial environment. At the same time, it increases the risk of data misuse and leakage by subcontracted data processors. Currently, data users have been using contractual and indemnification provisions to make the subcontracted data processors liable in their handling, protecting and holding customers' data entrusted to them. Due diligence work on engaging new subcontracted data processors and audits of personal data handling process by them are also performed. However, the above measures may not effectively ensure complete security, proper use and retention of data handled by the subcontracted data processors. Practical difficulties are encountered in ensuring that the data processors perform satisfactory due diligence and procedures in compliance with PDPO data protection requirements. To ensure subcontractors are discharging the same level of compliance duties, we support the option of PCPD directly regulating data processors by imposing obligations on them.

Proposal No. 3: Personal Data Security Breach Notification

- Such notification could create excessive burden on business if this is an absolute duty without regards to the seriousness or scope of the implications. It is suggested that as an alternative, business shall maintain a log of data loss incidents for which PCPD shall be authorized to inspect under statutory provisions, if required. If notification is required, such obligations should be subject to specified criteria e.g. materiality, number of individuals affected etc. These should be clearly prescribed in guidelines to avoid ambiguities or possible non-compliance.

Ms Joanna Choi
Principal Assistant Secretary (4)
Constitutional and Mainland Affairs Bureau

- Voluntary notification is preferred as mandatory notification requirement is certainly too onerous. To implement voluntary notification, PCPD must issue very clear & practical guidelines for data users to follow; otherwise such requirement will likely impose undue burden on data users. It should also be applied equally to data processor who needs to notify cases of non-compliance pursuant to the guidelines to be constructed by PCPD.
- We need to review the guidelines about the "voluntary breach notification system". As an insurer, we are handling lots of customer data every day, the implementation of the notification system might create onerous burden on our business operations.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

- Criminal investigation and prosecution have been placed within the ambit of the Hong Kong Police and Department of Justice respectively. PCPD is a statutory body entrusted with the protection of personal data privacy of individuals. We concur that the overlap of the enforcement and punitive functions is not desirable.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

- We believe it would be more effective that the PCPD retain an independent role rather than providing legal assistance to an aggrieved data subject.
- Currently, the public can seek legal assistance if they are eligible. The public has already had source to seek for assistance.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

- We do not agree to this proposal because vesting power on a data protection authority to award compensation would result in an undesirable combination of enforcement and punitive functions in a single authority.
- It should be up to the court, not PCPD, to determine the amount of compensation payable; allowing PCPD to do so would vest in PCPD an undesirable merging of enforcement and punitive functions.
- We believe that the PCPD should retain an independent role to determine if there is any breach of the Data Protection Principles instead of being conferred with the authority to award compensation.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

- We do not agree to this proposal because the data protection principles are not prescribed in the PDPO; they are general guiding principles on data protection which are couched in generic terms and can be subject to a much wider range of interpretations.

Ms Joanna Choi
Principal Assistant Secretary (4)
Constitutional and Mainland Affairs Bureau

- We disagree with this proposal as it would have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability. Also, the idea of criminalizing the contravention of a DPP is a major departure from the original purpose of adopting the DPPs in the privacy ordinance.
- The DPPs are widely known to be in generic terms subject to different interpretations e.g. records should be kept 'no longer than necessary', 'appropriate security measures'. They are not specific as to what constitutes a 'contravention'. An enforcement notice is more specific and already empowers the PCPD to interpret and enforce such principles. We therefore consider that the current mechanism suffices and it is not appropriate or necessary to make a contravention of a DPP an offence.
- We believe that with the launch of the "voluntary breach notification system", public awareness will be further enhanced.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

- About the proposal of making it an offence if a person obtains personal data without the consent of data user and discloses the data to obtain profits or for malicious purposes, we are inclined to agree. However, we believe, first, a clearer definition about sensitive personal data should be worked out and properly communicated to the general public; and secondly, the focus on the intention behind the use of the data is important in order to avoid possible abuse.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

- We do not agree to this proposal and would like to counter propose that the PCPD can consider increasing the penalty together with an issue of enforcement notice upon repeated contravention of a DPP on same facts.
- With the "voluntary breach notification system" that will come into place, and with the view that no repeated contravention has occurred so far, we think the existing practice of issuing an enforcement notice is sufficient.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

- The DPPs are expressed in generic terms, whether it constitutes a 'serious' contravention is judgmental. Also, since it is uncommon for non-judicial bodies to have the statutory power to impose monetary penalties, we do not think the PCPD should be so empowered at this stage.

Ms Joanna Choi
Principal Assistant Secretary (4)
Constitutional and Mainland Affairs Bureau

- About empowering the PCPD to impose monetary penalty, our view is this will confuse the PCPD role whose main duty is to determine if there is any breach of the DPPs. Besides, the current DPPs are described in generic terms and can be subject to interpretation.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

- Heavier penalty shall have a greater deterrent effect, but consideration should be given to whether such contravention is unintentional or due to wilful disregard as well as the significance of the contravention.
- As advised in the document, since the launch of the PDPO, there has not been a problem with repeated offenders. Hence, we believe the existing mechanism (enforcement notice) is a sufficient deterrent.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

- The number of complaints is 59 in 2006, 87 in 2007 and 67 in 2008, which are minimal when compared to the direct marketing activities. It is suggested to maintain the existing penalty amount.
- Direct marketing is one of the key promotional activities adopted by most business in HK and elsewhere. A sensible balance must be struck between protecting individuals' personal data privacy on the one hand, and not fettering the normal functioning of business promotional activities on the other. We suggest keeping the status quo (i.e. not to raise the penalty) for the time being.

Proposal No. 17: Erasure of Personal Data

- We welcome this proposal. We suggest clarification or provision of more examples of what are being considered as reasonably practicable steps in erasures of personal data.
- Current duty to erase obsolete data is absolute, regardless of its practicality and reasonableness. We agree that "*the provision concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for fulfillment of the purpose of use*" because in some cases, it might be practically impossible to erase all such data as in the example quoted in the proposal.

Ms Joanna Choi
Principal Assistant Secretary (4)
Constitutional and Mainland Affairs Bureau

- The biggest issue for insurance companies is to make sure it is clear that personal data remains relevant from the time of underwriting through until a claim has been assessed and settled (or not settled). It is an unfortunate fact that some applicants deliberately do not disclose relevant information for the proper underwriting and conduct of insurance. This is often only evident at the time of claim assessment. Therefore personal data must be retained until 7 years after a policy is no longer in force or there is no possibility of a further claim against the insurer.

Proposal No. 18: Fee charging for Handling Data Access Requests

- It is difficult to consider the maximum amount of fees and to exhaust all fee types. The cost in handling data access requests shall depend on the cost in retrieving data and shall vary from company to company.
- The maximum amount can be determined after consideration of the difficulty in retrieving data and the amount of labor cost, regular review is required and thus frequent change to the schedule may result. However, if the maximum amount is too high to avoid frequent changing of the legislation, it will defeat the original purpose of setting this provision.

Proposal No. 20: Circumstances for Issue of an Enforcement Notice

- We propose that the PCPD may serve an enforcement notice under any of the following circumstances:
  - the act of contravention is continuing;
  - it is likely that the contravention will continue or be repeated; and
  - the contravention has caused damage or distress to the data subject.

Proposal A.1 Revamping Regulatory Regime of Direct Marketing

- Based on the rationale provided, we agree that it is appropriate not to pursue revamping regulatory regime regarding direct marketing.

Yours truly,

(Signed)

James Wong
Chairman

c.c. Governing Committee Members

JW/lw/sw

S0053



To pdpo_consultation@cmab.gov.hk
cc
bcc
10/11/2009 17:31 Subject Suggestions
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir,

I have the following comments on organizations collecting personal data.

1. When we enter a building e.g. HKJC office building, we are asked to present our I.D. card. Our names and the entier I.D. number are copied to the log book on the table of the reception. All names and numbers on the page are visible to anyone standing in front of the reception. I feel terribly uncomfortable about this arrangement. Name and I.D. number can be used to register mobile phone sim card, loans and etc.
I think the organization should be copying partially the I.D. number but not the whole one.
The handling of the data which is clearly visible on the logbook to anyone is also violating my privacy.

2. We don't know how the logbook will be handled when it is full. Will it be destroyed or will it be kept in their storeroom? Anyone having access to the used logbook can easily get the names and I.D. number of hundreds of people. Will they use these data in any illegal ways? We are never told how the logbooks will go when we are asked to present our I.D. card.-

3. Whenever we go to the mobile phone company to change a plan or change the address, our I.D. card will be photocopied once again, even when it was copied when we signed up with the company. All these extra copies will lead to the problem of mishandling of personal data, especially when there are hundreds of branches and thousands of staff and not every one and every branch could handle the personal data in an appropriate way.

4. We are receiving numerous calls from loan companies, beauty companies, banks and medical companies. Some of them know our names and numbers. Most outrageously, some are calling from a computer. Manyatimes, we receive the calls at the most inconvenient times. I really would like to protect my time and privacy and wish not to receive any of these calls again.

--
Best regards,
Hester

香港工程師學會
THE HONG KONG INSTITUTION OF ENGINEERS

S0054

Your reference: CMAB/CR/7/22/40 Pt. 7

11 November 2009

Miss Joanna CHOI
For Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong

Dear Miss Choi,

Review of the Personal Data (Privacy) Ordinance

Thank you for your letter of 28 August 2009 inviting the Institution to give views on the captioned subject.

Having reviewed the consultation document, we would like to inform you that the Institution does not have any specific comments on the consultation document.

Yours sincerely,

(Signed)

Monica YUEN (Mrs)
Secretary

港九勞工社團聯會
THE FEDERATION OF HONG KONG
& KOWLOON LABOUR UNIONS

S0055

本會檔號 OUR REF.:

政制及內地事務局：

對檢討《個人資料(私隱)條例》的諮詢文件之意見

有鑑於科技發展日新月異，本會擔心個人資料在現行的法例下是否得到足夠的保障，近期，經常有公營機構洩漏市民個人資料的事件發生，亦有不少市民投訴個人資料被利用在直接促銷活動中，本會對此表示關注，而個人私隱資料與公眾利益又應如何平衡亦是另一重要議題。本會對檢討《個人資料(私隱)條例》諮詢文件有以下意見：

把違反保障資料原則訂爲罪行恐會矯枉過正

本會擔心若把違反保障資料原則訂爲罪行，會造成矯枉過正的情況出現，由於科技發展日新月異，導致市民對私隱及個人資料的概念經常改變，加上在一些問題例如何謂「敏感資料」等尚未有定論時，恐怕實行刑事化會面對不少困難。許多違反條例的行爲都是在市民無心、不經意或不知情的情況下發生的，而當時人亦沒有從個人資料洩漏中獲取利益，若把該等情況定罪，將有許多市民被入罪，並有違「私隱權必須與其他權利以及某些公眾及社會利益取得平衡」及「避免商業活動和資料使用者承受沉重的負擔」等原則，將會使市民日常生活運作大受影響。而本會認爲把「未經資料使用者同意下取得及披露個人資料，並從中取利或作惡意用途的行爲」訂爲刑事罪行則較爲恰當，相信對侵犯私隱以從中取利的行爲能起阻嚇作用。

設立個人資料外洩通報機制

本會贊同設立個人資料外洩通報機制，讓私隱專員可以評估事件的影響，並監察機構跟進事件的情況，把事件的影響減至最低。然而，若果只訂立自願性通報機制，則可能會形同虛設，相信大部份機構亦不會主動通報，令有關當局難以評估及跟進事件，而諮詢文件中提到太多通知有機會造「通知疲勞」，這可能只是一種假設，本會擔心當局低估了資料

外洩事件對公眾人士的影響。政府已設立了電子個人資料外洩通報機制，規定各部門盡快呈報資料外洩事件，私隱專員可考慮把類似機制擴展至私營機構，相信通報機制能使相關人士所受的影響減至最低。

難以區分「敏感」資料及「非敏感」資料

諮詢文件提到可以考慮處理敏感個人資料應受到更嚴格的規管，現時的私隱條例亦無區分「敏感」資料及「非敏感」資料，本會認爲要劃分「敏感」與「非敏感」是相當困難的，同一項個人資料在不同情況下的「敏感」程度亦可能有所不同，因此難以一刀切的方式來區分，強行把每一項個人資料分類可能會引起更多的爭論。若把個人資料分成兩類，是否代表當「非敏感」個人資料遭外洩時，對當時人的影響很有限？本會對此有所保留。任何資料都有其重要性及特別的功能，一旦外洩時，也可能對當時人造成嚴重的影響，因此，本會並不建議區分「敏感」資料及「非敏感」資料。

對資料處理者作適當的監管

有鑑於把個人資料處理工序外判的情況日趨普及，本會明白建議對資料處理者作出適量的監管是有須要的，但如果以監管資料使用者的方法來規管資料處理者，相信是較爲困難的，部份資料處理者可能不知道其處理的個人資料之用途，亦可能有部份資料處理者甚至難以確定其處理的是否屬於個人資料，因此，強行要他們遵守與資料使用者相同的規例可能有欠公允，若要求資料處理者釐清資料的特性及用途，正如諮詢文件提及若向資料處理者施加廣泛的責任，可能會窒礙互聯網上資訊的自由流通。另一方面，若果資料處理者刻意利用個人資料而從中獲利，而私隱專員亦不能直接介入，則對資料當時人及資料使用者不利。本會建議向資料處理者施加適當的責任，例如要求資料處理者採取適當步驟，確保其處理的個人資料妥爲保存，私隱專員亦應保留介入及向資料處理者作出調查的權力。由於不同的資料處理者對個人資料的掌握程度也有不同，因此難以監管資料使用者的手法規管所有資料處理者，向資料處理施加適當的責任及有一個靈活富彈性的機制規管資料處理者是較爲適合的。

不應限制父母查閱未成年子女個人資料的權利

諮詢文件中另一個具爭議性的議題是應否准許資料使用者拒絕代表未成年人的「有關

人士」提出的查閱資料要求，以保障未成年人的利益，意味著資料使用者可以拒絕當時人的父母對其情況的查詢。此題目除了考慮實際操作問題外，亦涉及更大的家庭價值等問題，本會擔心若加入上述條文，會有矯枉過正的情況出現，同時亦會與政府強化家庭價值及鼓勵家庭成員多溝通的政策有所抵觸，父母作爲未成年人的監護人，有法律責任照顧未成年的子女，建議加入的條文可能會對此作出挑戰，繼以衍生其他家庭問題。

對建議授予私隱專員刑事調查及檢控權力有所保留

對於私隱專員的執法權力方面，本會對賦予私隱專員刑事調查及檢控罪行有所保留。本會擔心若賦予這些權力給私隱專員，會出現權力過大的情況，而諮詢文件亦未有提及私隱專員一旦賦予這些權力，將會怎樣行使？例如私隱專員是否會在未向涉嫌違反私隱條例者發出警告通知，便直接提出檢控，我們對此表示關注，因此對建議有所保留。文中提及此舉有助節省把個案轉介警方進行調查的時間，若私隱專員與警方加強溝通、簡化轉介程序，相信對縮短檢控時間會有所幫助，我們認爲此點並不是賦予權力給私隱專員的原因。

應爲受屈資料當時人提供適當的法律協助

本會贊同爲對受屈資料當事人提供適當的法律協助，現時，受屈的資料當事人可從民事程序申索，但因追討的成本太大，絕少市民會這樣做，部份公司可能針對此點，有恃無恐地進行一些侵害個人私隱的活動。若私隱專員能爲當時人提供適當的法律協助，將可對侵犯個人私隱的行爲起阻嚇作用。當然，私隱專員亦應評估當時人申索的成功機會，以免出現濫用及浪費公帑的情況。

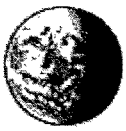
以上是本會對檢討《個人資料(私隱)條例》諮詢文件的一些意見，希望　貴局予以考慮！

港九勞工社團聯會　謹啓

2009 年 11 月 9 日

聯絡人：林振昇





16/11/2009 09:04

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Consultation Paper of the Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir/madam

Attached please find the comments of our members re the captioned.

If you have any questions, please feel free to contact me.

Thanks
Eric So
Hong Kong Investment Funds Association



HKIFA Members Comments On Review of Personal Data (Privacy) Ordinance.doc

HKIFA members' comments on the Consultation Paper of the Review of the Personal Data (Privacy) Ordinance

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities - Should we regulate data processors entrusted with handling of personal data?

- During the normal course of business, fund companies may be required to transfer personal data to 3rd parties for processing, e.g. updating of unitholder records, passing of unitholder information to their affiliates offshore for their fund range that is managed overseas but sold in Hong Kong, use of mailing houses for distribution of communications. The current practice of stipulating how to treat the confidentiality of such information in the contractual arrangement between the parties enables the parties themselves to put in place the necessary or relevant practical procedures to ensure that the personal data is handled appropriately. It may be difficult for legislation to be drafted widely enough to adequately cover the different business scenarios if direct regulation of data processors is opted for.

  Having said that, members do not agree that the data user should be the only party responsible under the Personal Data (Privacy) Ordinance ("PDPO") in the case of a breach by the data processor. Paragraph 4.20 suggests that in the case of a privacy breach by a data processor, the aggrieved party (data subject) seeks redress from the data user under the PDPO and following from that the data user then seeks back-to-back redress from the data processor under the contract between them. This approach would result in unduly involving the data user in a contentious matter where the data user itself has not breached the PDPO. Since data processors are likely to be third parties, no matter how tightly the contract is drafted, the data user never has ultimate or total control over the activities of the data processor. Accordingly, our members believe it would be inappropriate for the liability of a data processor's breach to always flow through the data user as this may cause undue reputational harm on the data user.

  It appears sensible that perhaps there should not be a distinction between data users and data processors (as per the Canadian and Australian jurisdictions). Our members agree that organisations, whether they are data users or data processors, should be required to comply with the relevant Data Protection Principles ("DPPs") generally, especially in the case where an organisation is aware (as stipulated in the contractual arrangements) that they will be handling/processing personal data.

Proposal No. 3: Personal Data Security Breach Notification - Should we require data users to notify the Commissioner for Personal Data ("PCPD") and affected individuals of personal data leakage incidents?

- Some members pointed out that the "Possible Notification Mechanism" set out at paragraphs 4.37 to 4.42 of the consultation document describes a mechanism which is not so "voluntary" in the sense of how that word is generally understood. In particular, paragraph 4.37 states: "The data user will be required to notify the PCPD when a personal data security breach may result in a high risk of significant harm to individuals or organizations. Notice of data security breach will have to be made to the PCPD within five business days of discovery of the breach." A mechanism based on the above-mentioned paragraph 4.37 can hardly be described as voluntary. Rather than being voluntary, the

possible mechanism involves mandatory requirements in relation to breaches which may result in "a high risk of significant harm" in the absence of any specification as to what might amount to "high risk" or "significant harm". It is, accordingly, submitted that the exact meaning of "voluntary" be elaborated upon in the course of the consultation. The experience of the UK, New Zealand and Australia which have promulgated voluntary guidelines should also be elaborated upon for consideration by the public.

- Members understand that the provision of breach notification will enable affected individuals to take measures to limit the consequences of such breach and also provide the PCPD with a means of monitoring breaches and organisational practices. However, members feel this should be weighed against the undesirable outcome of over-notification as this in itself may reduce the effectiveness of the notification. They also believe that breach notification should be given where there is a real usefulness to the affected individuals, i.e. where the breach carries a real risk of harm. Some feel that the system adopted by the UK, New Zealand, Australia and Canada appears reasonable where they have promulgated voluntary guidelines for organisations to follow in the event of a personal data breach and based on an assessment of whether the breach may give rise to a real risk of serious harm or cause substantial damage or distress to the affected individual.

- As the voluntary breach notification system is to apply to all organisations, public or private, it is expected that any guidelines promulgated to be flexible enough to be applied equally across different organisations types, in particular, that the guidelines would not be inconsistent with the current regulatory regime they are subjected to under the SFO.

  Given that the proposed regime is voluntary, it is expected that where an organisation can show that it has made a risk assessment of the breach and decided subjectively that there is no real risk of causing substantial damage or distress to the individual, that organisation should not be held accountable for choosing not to provide notification of the breach. If such an argument is not available to the organisation, the consequences would be that organisations might rather err on the side of caution and notify each and every breach to avoid contravening the notification guidelines.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD - Should we give the PCPD criminal investigation and prosecution power?

- The power to investigate criminal offences is generally vested in the police and the power to initiate criminal prosecution is generally vested in the Department of Justice. Given that offences carry with them significant impacts on the parties concerned, it does not appear that the reasons given for the proposal (as set out in paragraph 5.03 of the consultation document) amount to the "strong justifications" required for the delegation of the prerogative of initiating criminal prosecution (as referred to paragraph 5.04 of the consultation paper). This is particular so in view of the fact that there have only been a few cases of referral to the police over the past few years and the existing arrangement has been work smoothly. Also, rather than granting the PCPD with both powers of investigation and prosecution, it would be more appropriate for 2 separate government bodies (as is presently the case) to be separately vested with the respective powers to minimize the risk of over-concentration of power (and its possible abuse) and to ensure that justice is seen to be done. Accordingly, our members submit that the status quo should be maintained.

- As organizations that are regulated under the Securities and Futures Ordinance by the Securities and Futures Commission ("SFC"), our members believe that it is unnecessary for another regulatory authority to be vested with criminal investigation and prosecution power in relation to their activities as a regulated financial institution. If the government is concerned with the efficiency of the current system, it may consider setting up a system whereby the PCPD can liaise or coordinate its concerns or findings with the SFC and refer the matter to the SFC (as our primary regulator) for further handling.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66 - Should we empower the PCPD to provide legal assistance to an aggrieved data subject who suffers damage by reason of a data user's contravention of a requirement under the Ordinance and intends to institute legal proceedings against the data user?

- Members are not opposed to the PCPD providing legal assistance to aggrieved data subjects as they agree that an aggrieved party should not be inhibited from seeking recourse purely on a cost basis. However, they believe that such assistance should only be provided where the PCPD is of the view that there is a strong case to answer and the aggrieved data subject has shown that is incapable to bear such costs or that would be unreasonable for it to bear such costs. This is to ensure that there will not be an undue number of actions, frivolous or otherwise, to be brought against data users.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects - Should the PCPD be empowered to award compensation to an aggrieved data subject?

- Members believe that assessment of the compensation awarded to an aggrieved subject should be a matter for the courts to determine after hearing the case from both the aggrieved party and the data user in breach. The role of the PCPD should remain as a regulator in assessing whether a data privacy principle has been breached. The proposal to empower the PCPD to provide legal assistance to aggrieved data subjects should be sufficient in assisting those parties to seek the appropriate recourse through the court system.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence - Should we make contravention of a Data Protection Principle an offense?

- Contravention of a data protection principle may be caused by careless omissions or inadvertent acts without any intention of a criminal nature. It may not be in the interests of the public and would have significant impacts on the Hong Kong society as a whole if a mere contravention of a DPP, without any criminal intent, would attract criminal liability. This is particularly so as DPPs are couched in generic terms and are subject to wide interpretations. Instead, it would be more appropriate to single out particular acts of contravention of DPPs as committing summary offences or indictments having regard to the degree of severity, the seriousness of offence and harm or damage caused to the affected individuals.

- Members point out that it would be inappropriate to make contravention of a DPP an offense. DPPs are designed as a set of generic principles which embody upholding the spirit of privacy legislation. It is intended that data users should interpret these principles

and apply them to their respective businesses as they see fit in order to uphold this spirit of privacy. If contravention of a DPP is made an offense, the DPPs will need to be redrafted in much stricter terms so that data users will be absolutely clear what conduct will constitute an offense. Members believe this will have the undesirable effect of making the DPPs overly prescriptive and inflexible. They would suggest that the more appropriate approach would be for the legislation to specify particular types of conduct which would constitute a criminal offense, and for such conduct to be clearly and unambiguously described.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data - Should we make it an offence when a person discloses for profits or malicious purposes personal data obtained from a data user without the latter's consent?

- Members agree that making this an offence should further deter data users from engaging in such conduct and could lead to a more compliant culture. However, they query whether it is necessary to create such a new offence. It is not clear from the consultation paper if the creation of the new offence is in response to a large number of offenders engaging in such undesirable conduct or if the current regime is inadequate in dealing with such conduct. If the legislation is to include this new offence, members would also expect a number of appropriate defenses to be available to the offender where the conduct is not in breach of the spirit of the privacy legislation. They also expect guidance on what would constitute "profits" and "malicious purposes".

Proposal No. 9-12 – Questions on imposition of monetary penalties on serious contravention of DPPs and repeat offenders

- Although members understand that the PCPD would like to strengthen the enforcement of the PDPO and deter serious breaches of the DPPs (by imposing monetary penalties and making it an offence for intentional repeat offenders), they query if such increased measures are necessary. The consultation paper notes that there have not yet been any cases of repeat offenders since the enactment of the PDPO which suggests that this is not a problem area. Furthermore, our members agree that whether an act constitutes a "serious contravention" of a DPP is a matter of subjective judgment and therefore it may be unfair or inappropriate for the PCPD to issue monetary penalties based purely on its own assessment of the breach. If deterrence of particular conduct is the main objective, then our members agree that singling out particular acts or practices and making them offences (subject to a clear and unambiguous description of such acts or practices) may be more appropriate.

- Members would like to reiterate that as licensed financial institutions, they are subject to heavy regulation and supervision by the SFC. The SFC has wide powers to ensure that their conduct as a financial institution is appropriate. Accordingly, they suggest that if strengthening adherence to the DPPs is the key objective, then perhaps in respect of such entities which are already supervised by the SFC, the PDPC be empowered to refer matters of concern to the SFC for further handling.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data - Should we empower a third party to give consent to the change of use of personal data of a minor or a mentally incapacitated person?

- Subject to the conditions as set out in the consultation paper, members agree that a more flexible system whereby a designated third party who has been either appointed by the court or who has been appointed under a valid power of attorney is authorized to give consent on behalf of a data subject who is mentally incapacitated is useful.

Proposal No.17: Erasure of Personal Data

- Whilst timely erasure of obsolete personal data is important, any PDPO requirements should not be such as to pose an excessive burden to businesses. Section 26 and DPP2(2) imposes an absolute duty on a data user to erase obsolete personal data which, due to its absolute nature, may not be appropriate for all cases. Members agree that the PDPO should be amended so that the provisions concerning erasure of personal data would be regarded as having been complied with if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use. They also submit that the PDPO should be further amended to the effect that, in respect of personal data the erasure of which is not reasonably practicable, the said provisions would be regarded as fulfilled if reasonable means (and efforts) have been used (and made) to put the data in question in safe storage.

(End)

S0057



To pdpo_consultation@cmab.gov.hk
cc
bcc
13/11/2009 21:55 Subject 《個人資料 (私隱)條例》建議

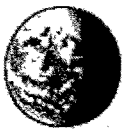
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

本人現爲一位中學生的家長,想就有關《個人資料 (私隱)條例》提出些少建議。

我發現很多學校的收費通告或回條上,設有一些學生資助及綜合援助的選項(同學若爲受資助類別,收費可減免),此措施原意是要幫助經濟有困難的學生,減輕他們的家庭負擔。但卻不能保障學生的私隱,當學生交出有關回條或通告時,其他人很容易就會知道他們的家庭經濟狀況,令學生的個人資料及私隱外洩。若同學之間有經濟差距的觀念,很容易會產生歧視及不和等情況,因此本人希望 貴部門能就此事,修訂《個人資料 (私隱)條例》保障學生及其家庭的私隱。

(來信人要求不具名公開意見)

S0058



13/11/2009 21:57

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Comment on the Consultation Document on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir/Madam,

I would like to make a suggestion of the restriction of "Cold Call" under the "Consultation Document on Review of the Personal Data (Privacy) Ordinance". As I have received around 5 to 10 Cold calls from my mobile phone per week, and the calls were made between 9 a.m. to 11 p.m from Monday to Sunday. I think it is a terrible issue which is effecting all Hong Kong residents. Some calls made from some companies which I do not know who they are or I do not use their services at all. Therefore, is there any possibilities to change this Ordinance to restrict the companies (or their employees) not allow to connect people, unless they have signed the agreement to let them do so?

To be honest, all people around me are also facing the same problem. Some companies do not care how you complain about it as well.

Beside, it costs once we receive the Cold Call. Therefore, I really hope that this problem can be fixed as soon as possible. Moreover, I have stayed in Australia for 4 years. I did not have this problem at all. I do not know why we have this issue in Hong Kong.

Million Thanks,

(name)

(The sender requested anonymity)

S0059

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

政制及內地事務局：你們好！

過去十年間，資訊科技迅速發展，互聯網變得普及，電子商貿快速增長，資訊和通訊科技的應用廣泛，祇此同時，提高香港的競爭和效率，并爲市民提供更多更方便的服務，興此同時，科技進步，并爲市民提供個人資料私隱的保障帶來新挑戰，爲此確定私隱條例是否應付這些發展，帶來挑戰，至爲重外，此外市民對個人資料私隱的保障日益關注，就此我們需要檢討，收緊個人資料的規管，我們也需要簡化私隱條例的運作和解決條例施行過程等問題。

1、我們建議如資料使用者離衆父母化其未成年子女提出查閱資料要求并不付給子婦的最佳利益，我們應當準許資料使用者拒絶該查閱要求。

2、應當授權第三者更改未成年或精神上無行爲能力人的個人資料用途給予同意。

3、應當提高違反執行通知資料原則行爲通知罰款。

4、應當提高直接促銷活動中不當使用個人資料關照。

5、應當對履次違反執行通知行爲處以最嚴重的懲罰。

6、應當把資料使用者已送行私隱專署發出執行通知規定從中取利但不久故意重犯行爲列入刑事罪行。

7、應當把握披露未經資料使用者同意下取得個人資料而從中取利或是惡意用途行爲列入刑事罪行。

8、應當把違反資料使用者原則訂爲刑事罪行。

9、應當授權私隱專員向受屈資料當事人判給補償。

10、若有資料當事使用者違反私隱一條例規定，而蒙受損失并有志向資料使用者提出法律訴訟。

11、對于警方正常檢查身份證行爲正常規管。

12、應當授于私隱專員刑事調查和檢控能力權力。

13、應當規管受托處理個人資料處理者嚴格規管。

14、對于敏感個人資料（如指紋）應當受到嚴格規管。

以上我們建議，希望你們咨詢立法後盡快立案通過。目前問題存在好多，需要立案通過才能受到助赫作用，如果咨詢它不立案使用等于白費心機，所以我們希望盡快立案通過。

安好!

(署名來函)

2009 年 11 月 9 日

（ 未能確定來信人是否願意公開姓名 ）

S0061

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

S0062

CHARTERED SECRETARIES 特許秘書
60 Years in Hong Kong

Natalia Seng
President

5 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Sirs,

Re: Consultation Document on the Review of the Personal Data (Privacy) Ordinance

We are pleased to enclose our submission in respect of the above consultation document.

Thank you for your attention.

Yours faithfully,

(Signed)

Natalia Seng FCIS FCS (PE)
President

Enclosure

THE HONG KONG INSTITUTE OF CHARTERED SECRETARIES

Submission on Review of Personal Data (Privacy) Ordinance

Key Proposals			
Proposal No. 1:	Sensitive Personal Data	Comments	
(a)	Whether there is a need to accord better protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances; and	Need more information	Since the perception of sensitive personal data is culture-bound, in the absence of a locally accepted definition of sensitive personal data, we have difficulties in responding to this question. The Consultation Document seems to treat biometric data as sensitive personal data by reference to two characteristics, i.e., being irrevocable and the grave privacy concerns if lost or mishandled. Once we agree on the meaning of sensitive personal data, we could then decide if they deserve better protection.
(b)	If yes, whether the possible regulatory regime, including coverage of sensitive personal data, related regulatory measures, sanctions, and the need for grandfathering or transitional arrangement as set out in paragraphs 3.08 to 3.14, is appropriate.	Not applicable	
Proposal No. 2:	Regulation of Data Processors and Sub-contracting Activities		
(a)	Whether a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties;	No	The proposal appears to use private law remedies to secure compliance of the PDPO obligations. Such practice could increase the compliance costs of data users.
(b)	Whether the activities of a data processor should be directly regulated under the PDPO or whether it is sufficient to indirectly regulate the data processor	No	The self-regulatory model described in paragraph 4.19 of the Consultation Document seems an attractive option. If some degree of government regulation of data processor is preferred, the

S0062

	through the data user by contractual or other means; and		government could consider the two-tier regulatory system currently practised in the travel agent industry. Regulating data processor through data user does not seem a viable option.
(c)	If activities of data processors were to be directly regulated under the PDPO, what obligations should be imposed on data processors, and whether it is appropriate and practical to subject different categories of data processors to different obligations.	Not applicable	
Proposal No. 3:	Personal Data Security Breach Notification		
(a)	The need to institute a voluntary privacy breach notification system in Hong Kong.		We support of idea of having voluntary guidelines for organisations to follow in the event of a personal data breach.
(b)	The components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42, including: (i) the circumstances under which notification should be triggered; (ii) to whom the notice of breach should be sent; (iii) timing of the notice; (iv) by what means should the notice be sent; (v) the content to be covered in the notice; and (vi) the consequences of failing to give notification.		These components could form part of the voluntary guidelines.
Proposal No. 4:	Granting Criminal Investigation and Prosecution Power to the PCPD		
	Whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.	No	We favour maintaining the status quo.

S0062

Proposal No. 5:	Legal Assistance to Data Subjects under Section 66		
	Whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under Section 66 of the PDPO, along the lines of the EOC model.	No	This is not good use of public funds.
Proposal No. 6:	Award Compensation to Aggrieved Data Subjects		
	Whether it is appropriate to introduce at this stage an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.	No	We support the views of the Law Reform Commission that it is undesirable to confer power on a data protection authority to award compensation as it could vest in a single authority a combination of enforcement and punitive functions.
Proposal No. 7:	Making Contravention of a DPP an offence		
	Whether we should make contravention of a DPP an offence.	No	We share the concerns set out in paragraph 6.04 of the Consultation Document.
Proposal No. 8:	Unauthorized Obtaining, Disclosure and Sale of Personal Data		
(a)	Whether we should make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent; and	Yes	We support the approach set out in paragraphs 6.09 and 6.11 of the Consultation Document.
(b)	If yes, the need for defence provisions and the appropriate level of penalty.		We support the need for defence provisions but have no views on the level of penalty.
Proposal No. 9:	Repeated Contravention of a DPP on Same Facts		
(a)	Whether it is appropriate to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally	No	We share the concerns set out in paragraph 6.15 of the Consultation Document: it is a departure from the original intent of adopting the DPPs in the PDPO.

S0062

	does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice; and		
(b)	If yes, the appropriate penalty level for the offence bearing in mind that non-compliance with an enforcement notice is subject to a fine of $50,000 and to imprisonment for two years.	Not applicable	
Proposal No. 10:	Imposing Monetary Penalty on Serious Contravention of DPPs		
	Whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.	No	We agree with the interpretation problems raised in paragraph 6.20 of the Consultation Document.
Proposal No. 11:	Repeated Non-compliance with Enforcement Notice		
(a)	Whether heavier penalty should be imposed for a second or subsequent conviction of Section 64(7); and	No	There does not appear to be a serious problem with repeated offenders.
(b)	If yes, the appropriate penalty level, bearing in mind the existing penalty level for contravention of an enforcement notice which is a fine at Level 5 (up to $50,000) and imprisonment for two years, and in case of a continuing offence, a daily fine of $1,000.	Not applicable	
Proposal No. 12:	Raising Penalty for Misuse of Personal Data in Direct Marketing		
(a)	Whether the penalty for misuse of personal data in direct marketing (i.e. contravention of the requirement under Section 34(1)(ii)) should be raised; and		We have no views on this proposal.
(b)	If yes, the appropriate level of penalty.		

S0062

Other Proposals			
(A) Rights of Data Subjects			
		Comments	
Proposal No. 13:	Third Party to Give Prescribed Consent to Change of Use of Personal Data		We have no views on this proposal.
Proposal No. 14:	Parents' Right to Access Personal Data of Minors		We have no views on this proposal.
Proposal No. 15:	Access to Personal Data in Dispute		We support the proposal as set out in paragraph 16 of Annex 1 of the Consultation Document.
(B) Rights and Obligations of Data Users			
Proposal No. 16:	Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation		We support the proposal as set out in paragraph 20 of Annex 1 of the Consultation Document.
Proposal No. 17:	Erasure of Personal Data		We support the proposal as set out in paragraph 23 of Annex 1 of the Consultation Document.
Proposal No. 18:	Fee Charging for Handling Data Access Requests		
(a)	Whether for the purpose of complying with Section 28(3), a data user should be required not to charge fees for complying with a data access request in excess of the prescribed maximum as set out in a fee schedule in the PDPO; and	No	We prefer self-regulation: the relevant professional bodies or trade associations could come up with a recommended scale of charges for handling data access requests for their members' reference.
(b)	If yes, the parameters for setting the prescribed maximum in respect of any proposed fee charging model.	Not applicable	
Proposal No. 19:	Response to Data Access Requests in Writing and Within 40 days		
(a)	Whether a data user should be required to inform a requestor in writing if he does not hold the requested personal data, save for a request related to criminal conviction record data which the Police		We have no views on this proposal.

S0062

	does not hold; and		
(b)	Whether a data user is required to inform a requestor within 40 days if he does not hold the personal data for which a copy of the personal data is requested, irrespective of whether the response is in written or verbal form.		
(C) Enforcement Powers of the PCPD			
Proposal No. 20:	Circumstances for Issue of an Enforcement Notice		
	To enhance the effectiveness of the PDPO in the protection of personal data privacy, one option is to allow discretion for the PCPD to serve an enforcement notice under any of the following circumstances:	No	If the practice has ceased and there is no likelihood of repetition, we do not see the need to empower PDPO to serve an enforcement notice.
(a)	Whether the act of contravention is continuing;		
(b)	Whether the contravention will continue or be repeated;		
(c)	Whether the contravention has caused or is likely to cause damage or distress to the data subject.		
Proposal No. 21:	Clarifying Power to Direct Remedial Steps in an Enforcement Notice		We support the proposal to clarify the power.
Proposal No. 22:	Removing the Time Limit to Discontinue an Investigation		We support the proposal as set out in paragraph 43 of Annex 1 of the Consultation Document.
Proposal No. 23:	Additional Grounds for Refusing to Investigate		
	Views are invited on whether it is appropriate to include the following additional specific grounds for the PCPD to refuse to carry out or continue an investigation under Section 39(2):		We agree with the concerns set out in paragraph 47 of Annex 1 of the Consultation Document and believe it is inappropriate to try to codify the various grounds for refusing to investigate a complaint.
(a)	The primary cause of the complaint is not related to		

S0062

	personal data privacy;		
(b)	The complaint relates to any action which is currently or soon to be under investigation by another regulatory body; or		
(c)	The act or practice specified in the complaint relates to personal data or documents containing personal data which have been or will likely be or are intended to be used at any stage in any legal proceedings or inquiry before any magistrate or in any court, tribunal, board or regulatory or law enforcement agencies.		
(D) Introducing New Exemptions			
Proposal No. 24:	Transfer of Personal Data in Business Mergers or Acquisition		
(a)	Whether an exemption from DPP 3 should be provided for the transfer or disclosure of personal data in intended merger, acquisition or transfer of businesses subject to the condition that the resultant organization will offer substantially similar service as the original data user; and	Yes	We support the proposal to introduce an exemption from DPP3 for the transfer or disclosure of personal data in intended mergers, acquisitions or transfer of businesses.
(b)	If yes, whether the option set out in paragraph 52 above is appropriate.		We believe the conditions set out in paragraph 52 of Annex 1 of the Consultation Document are reasonable.
Proposal No. 25:	Provision of Identity and Location Data on Health Grounds		
	To amend Section 59 of the PDPO to broaden the scope of application of exemption to cover personal data relating to the identity and location of the data subject where disclosure is necessary to		We have no views on this proposal.

S0062

	prevent or lessen a serious threat to the life or health of an individual.		
Proposal No. 26:	Handling Personal Data in Emergency Situations		
	Whether specific exemption from DPP 1(3) and DPP 3 of the PDPO should be granted in the handling of accidents or other life-threatening situations by LEAs and rescue and relief agencies.		We have no views on this proposal.
Proposal No. 27:	Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship		
(a)	Whether an exemption from DPP 3 should be provided to permit transfer of personal data of minors to their parents or guardians to enhance the protection of vulnerable minors and those at risk so that parents and guardians can properly discharge their responsibility on proper care and guardianship;		We have no views on this proposal.
(b)	If yes, what specific conditions should be attached to restrict the transfer to cases which are absolutely necessary.		
Proposals not to be Pursued			We have no views on these proposals.
(A) Scope of Regulation under the PDPO			
A.1	Revamping Regulatory Regime of Direct Marketing		
A.2	Internet Protocol Address as Personal Data		
A.3	Territorial Scope of the PDPO		
(B) Exemptions			
B.1	Public Interest Determination		
B.2	Public Domain Exemption		
(C) Powers of the PCPD			
C.1	Power to Search and Seize Evidence		

S0062

C.2	Power to Call upon Public Officers for Assistance		
C.3	Power to Conduct Hearing in Public		
C.4	Time Limit for Responding to PCPD's Investigation/ Inspection Report		
Miscellaneous Proposed Amendments to the PDPO			
(A) Statutory Powers and Functions of PCPD			
Proposal No. 28:	Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result		
	To relieve the PCPD's obligation to notify the complainant of the investigation result and related matters under Section 47(3) when the complainant has withdrawn his complaint.	Yes	We support the proposal.
Proposal No. 29:	PCPD to Disclose Information in the Performance of Functions		
	To amend Section 46 to allow the PCPD and his prescribed officers to disclose information reasonably necessary for the proper performance of his functions and exercise of his powers.	Yes	We support the proposal.
Proposal No. 30:	Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit		
	To protect the PCPD and his prescribed officers from being held personally liable for any act done or omission made in good faith in the exercise or purported exercise of PCPD's functions and powers under the PDPO.	Need more information	The public will need more information on this proposal.

S0062

Proposal No. 31:	Power to Impose Charges for Educational and Promotional Activities		
	To provide the PCPD with an express power to impose reasonable charges for undertaking educational or promotional activities or services.	Need more information	The public will need more information on this proposal.
Proposal No. 32:	Power to Obtain Information to Verify a Data User Return		
	To confer upon the PCPD the power to obtain information from any person in order to verify the information in a data user return filed under Section 14.	Yes	We support the proposal.
(B) Introducing New Exemptions			
Proposal No. 33:	Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings		
	To create an exemption from DPP 3 for use of personal data required or authorized by or under law, by court orders, or related to any legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights.	Yes	We support the proposal.
Proposal No. 34:	Transfer of Records for Archival Purpose		
	To create an exemption from DPP 3 for the transfer of information containing personal data of historical, research, educational or cultural interests to the Government Records Service ("GRS") for archival purpose.	Yes	We support the proposal.
Proposal No. 35:	Refusal to Comply with a Data Access Request on Ground of Self-Incrimination		
	To create a new exemption for data users from	Yes	We support the proposal.

S0062

	complying with a data access request on the ground of self-incrimination		
(C) Clarifying the Application of the PDPO in Certain Circumstances			
Proposal No. 36:	Definition of Crime under Section 58		
	To clarify the scope of application of the exemption provision under Section 58 by defining "crime" to mean a crime under Hong Kong law, or a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation.		We have no views on this proposal.
Proposal No. 37:	Expand the Definition of "Relevant Person"		
	To expand the definition of "relevant person" under Section 2 to include the guardian of data subjects with mental incapacity, who are appointed under Sections 44A, 59O, 59Q of the Mental Health Ordinance (Cap. 136).		We have no views on this proposal.
Proposal No. 38:	Exclude Social Services from the Definition of "Direct Marketing"		
	To amend Section 34 to exclude from the definition of "direct marketing" the offering of social services and facilities by social workers to individuals in need of such services and facilities.		We have no views on this proposal.
Proposal No. 39:	Exemption for Personal Data Held by the Court or Judicial Officer		
	To add a new provision so that the PDPO shall not apply to personal data held by the court or judicial officer in the course of the exercise of judicial functions.		We have no views on this proposal.

S0062

Proposal No. 40:	Extend Time Limit for Laying Information for Prosecution		
	To specify that the time limit for laying information for prosecution of an offence under the PDPO shall be two years from the date of commission of the offence.	Need more information	There must be compelling reasons for the 6-month statutory time limit when the PDPO was first enacted. In the absence of any evidence to support the change of circumstances, it is difficult for us to evaluate the proposal.
Proposal No. 41:	Duty to Prevent Loss of Personal Data		
	To amend DPP 4 in Schedule 1 to make it explicit that a data user is required to take all reasonably practicable steps to prevent the loss of personal data.	Need more information	The proposal appears to have extended the scope of DPP 4 and is likely to have an impact on data users. The public will need more information on this proposal.
(D) Clarifying Other Operational Matters			
Proposal No. 42:	PCPD to Serve an Enforcement Notice together with the Results of Investigation		
	To amend Section 47 to allow the PCPD to serve enforcement notice together with the results of investigation upon the relevant data user.	Yes	We support this proposal.
Proposal No. 43:	Contact Information about the Individual Who Receives Data Access or Correction Requests		
	To amend DPP 1(3) to permit a data user to provide either the job title or the name of the individual to whom data access or correction requests may be made.	Yes	We support this proposal.

S0062

敬啟者：

本人在醫院工作超過三十年，醫管局管理下其中一個文化是「院外候召」，有些情況下，即使不是醫生護士或專業人士，管方也喜歡給職員一個傳呼機帶回家，好讓管方「有需要時」找到該名員工。管方此舉可以是沒有任何津貼或補償的，其原意是希望員工「捱義氣」。

本來也沒有什麼問題的，私人時間時，不理會它便是了。但管方有條文(不知是出自何經何典？)是——如員工未能適時「應call」，則需要給予管方「合理解釋」。這就有問題了，我私人時間做什麼，干卿何事呢？為什麼要向管方交代呢？

不知醫管局管方這樣做是否違反保障個人私隱的精神呢？

對一般「打工仔」而言，確實是一個難題，因為一方面想維護個人私隱，另一方面也不好得罪「老細」，搞不好掉了飯碗，至少也可能被「劃花」個「file」，真是左右為難！

希望香港個人資料私人專員公署對於在職人士於職場中，能夠有相關法例保障個人私隱，對於僱主有明確的指引，以免僱主權力過大而侵犯個人私隱！

謝謝！

(署名來函)

2009/11/12

(未能確定來信人是否願意公開姓名)

ARCHIVES ACTION GROUP

Advocating Records Legislation for Hong Kong

S0064

12 November 2009

Team 4
Constitutional & Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Submission on Consultation Document on Review of the Personal Data (Privacy) Ordinance

1. The Archives Action Group is an informal body of concerned professionals reviewing and advocating the need for the enactment of archives legislation in Hong Kong for the effective and proper management of government records and the preservation of archives.

2. We have noted Proposal No. 34 in the Consultation Document that aims to create an exemption from Data Protection Principle 3 "for the transfer of information [*sic*] containing personal data of historical, research, educational or cultural interests [*sic*] to the Government Records Service...for archival purpose [*sic*]".

3. While we support this as a step forward in allowing the GRS to receive and preserve government records as archives, the consultation paper also states in relation to Proposal No. 34 that "the subsequent handling of the archival records containing personal data by GRS (including access to and use of records by members of [the] public will continue to be subject to the provisions of the PDPO". This is a matter of concern.

4. The extent to which control over, and access to, government archives is subject to privacy legislation rather than (in the absence of an archives law) the current administrative arrangements for access to archives requires clarification, and in particular whether "archival purpose" includes access and use as universally understood and practiced by professional archivists and historians.

5. We accept that the PD(P)O is necessary to protect privacy in Hong Kong but, given that the Ordinance was neither intended as, nor should be used as, a mechanism for the management of government records and archives, we would urge that the final report on the public consultation exercise contain a strong recommendation that the Administration take action to introduce legislation for that purpose.

For the
Archives Action Group

Filan Chua
Danny Chin
Simon Chu
Helen Swinnerton
Don Brech
William Waung
Stacy Gould

S0065



To pdpo_consultation@cmab.gov.hk
cc
bcc
18/11/2009 13:50 Subject 保安員不應將訪客的身分證號碼抄 錄在大廈入口處的登記冊內

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

為保安理由，管業經理有需要監察無權 進入大廈的人士進出大廈的情況。當大 廈保安員無法監察該些人士進入大廈後 的活動情況時，可能需要記錄他們的身 分資料，作為將來識辨他們的方法。在 此情況下，根據身分代號守則第2.3.4.2 段，保安員可以將訪客的身分證號碼抄 錄在大廈入口處的登記冊內。不過，依 據守則第 2.2 段，保安員應在可行的情 況下，讓訪客選用其他侵犯私隱程度較 低的方法，以代替提供身分證號碼。這 些方法包括接納要進入大廈某部分執行 職責的公共團體或相關機構或公共事業 公司僱員或送遞人員或工人的職員證或 工作證，或請受訪的住客辨識訪客。保 安員如對訪客到訪的目的有懷疑，可致 電發證機構核實，或取得有關業主及 / 或住客的確認。採取這些侵犯私隱程度 較低的方法，在保安方面可同樣有效地 阻止外人擅進大廈。

保安員應採取適當措施遮蓋訪客登記冊 上的記錄，以免其後的訪客看到這些資 料。訪客亦應獲告知可代替提供身分證 號碼的其他方法，以及保障資料第 1(3)原則所規定的事項，特別是包括收集訪 客姓名及身分證明文件號碼的目的，以 及該等資料可能會移轉予哪些人。物業管理團體除非獲得法律准許，否則 必須確保向訪客收集的個人資料只會用 於與原本收集目的相符或直接有關的目 的。在一般情況下，訪客登記冊內的資 料不應保留超過一個月。不過，有時會 需要將有關資料保留一段較長的時間，例如資料需用作舉證用途，或協助警方 調查不法活動。

本人極力反對保安員可以將訪客的身分證號碼完全抄錄在大廈入口處的登記冊內，事實上，抄錄四個字已足夠。

懇請跟進。謝謝。

S0066

To '"pdpo_consultation@cmab.gov.hk"' <pdpo_consultation@cmab.gov.hk>
cc
bcc
18/11/2009 15:42 Subject Submission by PCCW Limited

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sirs,

In response to the Consultation Document on review of PDPO, we attach hereof the comments of PCCW Limited for your consideration. Please feel free to contact the undersigned for any discussion on the issues concerning the PDPO review.

Best Regards,

Chris Cheng

Group Legal Adviser

PCCW Limited

pdpo consultation submission by PCCW Limited (18 Nov 2009).doc

PCCW®

S0066

SUBMISSION ON PUBLIC CONSULTATION

ON

REVIEW OF THE PERSONAL DATA (PRIVACY) ORDINANCE

November 2009

Introduction

This submission outlines the comments of PCCW Limited and its subsidiaries (collectively the "PCCW Group") in response to the Consultation Document on Review of the Personal Data (Privacy) Ordinance released in April 2009 ("the Consultation Paper").

In the Consultation Paper, we note that the Constitutional and Mainland Affairs Bureau proposes to expand the existing regulatory regime of personal data protection by various means including the imposition of more stringent regulations on data users, interpolating data processors into the regime of data privacy protection, criminalisation of certain acts of data users, making breach of data protection principles ("DPPs") an offence, increasing the penalty for breach of the provisions, etc. As a leading provider of telecommunication services in Asia, the PCCW Group handles a massive amount of personal data on a daily basis in its business operations. While we in principle support legislation which affords adequate protection to personal data, we would submit that such legislation should not be unduly burdensome to businesses. We have the following specific comments on the proposals in the Consultation Document.

Comments

Proposal 1: Sensitive personal data

The Privacy Commissioner for Personal Data (the "PCPD") proposes to impose more stringent controls on the processing of sensitive personal data by introducing the concept of "biometric data". The PCPD referred to various legislative documents including the *European Parliament's Directive 95/46/EC*, *UK Data Protection Act 1998* and *Australia's Privacy Act 1988*. However we note that such legislative documents do not themselves classify "biometric data" as being more sensitive than ordinary data. "Biometric data" is not defined in the PDPO or other ordinances of the HKSAR, however

the PCPD in various publications and speeches has suggested that fingerprint data or other data generated from biometric features are included as "biometric data".

It cannot be denied that fingerprint readers, retina scanners and other biological feature-related identification systems alike are widely used nowadays to record employee attendance and to control access to confidential areas. It is interesting to note that, unlike DNA profiling which could reveal other personal details such as racial or ethnic origins, records in fingerprint readers or retina scanners merely identify one individual from another. Such records usually appear in the form of a series of numbers which cannot be reverse-engineered to allow re-production of any biometric features or to reveal any other personal details concerning the individual. Taking the fingerprint reader as an example, the identification process is not a comparison between images of fingers scanned on the reader with those recorded in a database. The reader merely collects the geometric readings of a few spots on a fingerprint image and transforms them into a serial number which by itself does not reveal any biometric feature. The whole fingerprint recognition procedure does not even require storage of fingerprint images. As such, in an unfortunate case of leakage of information from a fingerprint scanning system, what would be lost is no more than staff names with corresponding serial numbers. Comparatively speaking, the potential harm resulting from such a case of leakage is much less damaging than leakage of ordinary information in staff profiles, such as staff numbers or telephone numbers.

We share the view that a higher degree of protection should be afforded to personal data which may inflict grievous harm on data subjects in the event of improper disclosure or leakage, e.g. biometric information that could reveal information such as health conditions, genetic information and ethnic origins. We however submit that the term "biometric data" should be carefully defined so as not to impede technological development nor to impose unnecessary burdens where the risk of inflicting grievous harm on an individual is extremely low.

Proposal 2: Regulation of Data Processors and Sub-contracting Activities

PCPD is proposing to add a new definition of "data processor" which means a person who holds, processes or uses personal data solely on behalf of a data user and who does not hold, process, or use such data for any of his own purposes, and to specify the obligation not to do an act or engage in a practice that contravenes DPPs2(2), 3 and 4.

In order to comply with DPPs2(2) and 3, we submit that it may be reasonable to expect data processors not to change the purposes for which the data is supplied by the person who engages their services and not to retain the data which is no longer necessary for fulfilling those purposes, even though the data processors may not even be aware whether the data entrusted to them is personal data or not. It is however not practicable not feasible to require data processors to comply with DPP4.

DPP4 requires data users to take all practicable steps to protect personal data from unauthorized or accidental access, processing, erasure or other use having regard to the kind of data and the harm that could result. However, it is impossible to devise such steps before comprehending the nature and quantity of the data concerned. Data processors, especially those in Internet-related businesses, are often unaware of the specific nature of the data passed to them. In fact, it is often the case that the data processor will not even know the contents of the data entrusted to him, and in order to find out the specific contents, he would need to intrude on the privacy of a data subject.

It is also important to note that data processors do not have any control over what data is received. Internet service providers (ISP), for example, are unable to inspect all data transmitted to their servers. As such, it is practically impossible for ISPs to incorporate into their business planning a data security system by reference to the kind of data they may process and the harm that could result upon data leakage.

Given the above, we submit that the issue of improvement of personal data security may be better addressed by PCPD forming a committee comprising of representatives from different business industries and issuing practical guidelines for data processors to follow. After all, direct regulation is unduly onerous on data processors, considering that they, unlike data users, do not compile any personal data for their needs and their business profit is not proportionate to the nature of data entrusted to them.

Proposal 3: Personal Data Security Breach Notification

We submit that the concept of security breach notification should be introduced as a voluntary reporting mechanism which encourages data users to notify the affected data subjects as soon as practicable to minimize any possible damage. A mandatory notification system at the present moment is not appropriate.

We understand that the rationale of the security breach notification is to allow the regulator to step in at an early stage of data leakage with a view to containing the damage. However, considering the technological complexity that may be involved, notifying PCPD would not necessarily contribute to the damage control. Data users should be encouraged to take immediate and effective actions to control damage, and the introduction of another bureaucratic step would only serve to consume resources more appropriately directed at containing data leakage.

It is also worth noting that the effectiveness of a breach notification mechanism would necessarily be compromised by the criminalization of DPP contravention (as per Proposal No.7). In the case of data leakage, the focus of data privacy compliance is whether the concerned data user has taken all practicable steps as DPP4 requires. If the breach of DPP4 is made an offence (which we do not support), a data user claiming the fundamental right of privilege against self-incrimination would have to be excused for

not revealing any information regarding the data leakage. As a result, the notification system would be rendered ineffective.

Furthermore, the proposed notification time of 5 business days is unrealistically inadequate for a data user to comprehend the situation, assess the risk and potential harm and prepare a detailed notice. In some incidents of data leakage, a considerable number of staff, overseas offices and/ or sub-contractors may be involved. To put a rigid time limit in the circumstances is undesirable and impracticable, especially in the case of considering whether to issue a public notification, for that would justify a more prudent examination and assessment of all the information.

Proposal 4: Granting Criminal Investigation and Prosecution Power to the PCPD

As pointed out in the Consultation Paper, some of the offences in PDPO are not technical in nature and involve imprisonment as penalty. We see it unnecessary and in fact undesirable for PCPD to take up the investigation and prosecution tasks. In addition, considering the trivial number of prosecution since the enactment of PDPO, it is uneconomical to exploit public resources to set up a prosecution team for PDPO offences.

Proposal 5: Legal Assistance to Data Subjects under Section 66

The PCPD intends to adopt the legal assistance scheme of the Equal Opportunities Commission ("EOC") empowered under the anti-discrimination ordinances. In principle, the EOC would only accede to a request for legal assistance if the case raises a question of principle or if it is unreasonable to expect the applicant to deal with the case unaided, having regard to the complexity of the case or the applicant's position in relation to the respondent or another person involved. According to the practice of EOC, applications for legal assistance are not entertained unless the complaints system and conciliation have proved to be unsuccessful.

In the case of the PDPO, it has been statistically proved that the invocation of section 66 of PDPO is extremely rare. Up to the moment of this submission, there is not a single court decision based on or relating to the application of section 66. As the anticipated demand for legal assistance in this area is very small, we believe that applications can simply be handled and approved by the Legal Aid Department which may seek assistance from the PCPD in due course.

Proposals 6 & 10: Award Compensation to Aggrieved Data Subjects and Imposing monetary penalty on serious contravention of DPP

DPPs are general principles of conduct which should not be transformed into something for which penalties can be imposed in the event that such principles are not absolutely abided by. The DPPs were not drafted with the intention that noncompliance result in the commission of an offence or the imposition of a penalty. We submit that in the event that DPPs are not abided by, the current regime in which the PCPD can direct data users to act or not to act by means of an EN is an adequate and more suitable means to protect the aggrieved data subjects. Moreover, the data subject is free to bring a civil action pursuant to section 66 to claim damages if the contravention is indeed very serious.

In this connection, we noted the invitation of views for Proposal No.6 on whether to introduce a redress avenue additional to section 66 by empowering the PCPD to award compensation to aggrieved data subjects. We submit that, while such additional avenue avails data subjects of a convenient means for seeking redress, it inadvertently involves, and so does the proposal to impose monetary penalty upon serious contravention, the consideration of how serious is the contravention. As previously stated, the DPPs are couched in generic terms and can be subject to wide interpretation. Thus, a defending data user could put forward various complicated arguments, and cite different pieces of legislation and case precedents, for consideration. It would therefore be most appropriate for the judiciary to retain jurisdiction of determining the seriousness of contravention, which could turn out quite legalistic and complicated.

The examples of imposing monetary penalties by non-judicial bodies mentioned in paragraph 6.19 of the Consultation Paper concern some well-defined offences, in contrast to the generic DPPs, and are therefore of little reference value.

Proposal 7: Making Contravention of DPP an offence

As explained in the Consultation Paper, DPPs, which were drafted as guidelines or principles, are couched in generic terms. Criminal provisions, on the contrary, are expected to be clear and unequivocal enough for one to tell what amounts to an offence. Given the fundamental difference in nature, it would be more appropriate to leave DPPs as mere guidelines and standards for data users to follow.

Proposal 9: Making repeated contravention of a DPP on same facts an offence

It should not be overlooked that upon balancing the costs and time involved in complying with an enforcement notice ("EN") with that needed to challenge an EN, some data users who disagree with the issuance of the EN may choose to comply with the directions in it rather than challenging it in the Administrative Appeals Board which could give rise to significant legal costs. If a data user is prosecuted for committing the same facts against which an EN had previously been issued, natural justice would still demand the prosecution to prove beyond a reasonable doubt that the EN was validly issued and would permit the data user to challenge the validity, legality and reasonableness of issuing the EN.

We are of the view that if a data user is prosecuted for committing similar acts against which an enforcement notice had been previously issued, the data user should not be estopped from challenging the decision of issuing the EN. The provision should also expressly state that the validity of the EN is an element to be proved beyond reasonable doubt by the prosecution.

Proposal 13: Third party to give prescribed consent to change of use of personal data

We agree that adopting the definition of "relevant person" under PDPO as the definition of a third party who can give prescribed consent on behalf of the data subject is appropriate.

We however note in the PCPD's Information Paper that it is proposed to allow a third party to give prescribed consent only if the proposed use of the personal data involves a clear benefit to the data subject. In this regard, one should note that the third party in the circumstance is the proper person to determine whether the proposed use could benefit the data subjects. The data user could by no means dispute the third party's decision in providing the prescribed consent. It is therefore suggested that the data user should be exempt from any liability under the PDPO for accepting the prescribed consent from the third party in the event that the consent is subsequently found invalid. For the avoidance of doubt, there should be provision in the PDPO which expressly provides that a data user, once reasonably satisfied that a prescribed consent is given by a third party as defined, can proceed on the basis that the proposed use is in clear benefit to the data subject.

Proposal 14: Parents' Right to Access Personal Data of Minors

We support the introduction of the right to refuse a data access request if the data user has reasonable grounds to believe that the compliance with the request would not be in the best interests of the minor. This however should be a right, rather than a duty, to refuse such data access requests. As with the submission made in respect of Proposal 13 above, a data user cannot conclude whether the parent's request is in the best interest of the data subject.

Proposal 15: Access to Personal Data in dispute

We fully support the introduction of the provision to prevent a data requestor from obtaining personal data by means of abusing the right to escalate the case to Administrative Appeals Board or Courts.

Proposal 16: Refusal to Comply with a Data Access Request on the Ground of Compliance with other Legislation

We welcome the introduction of the new ground for refusing data access requests in the event of a conflict with other ordinances. Consideration should however not be restricted to obligations under ordinances, but should be extended to rules and regulations imposed by regulators in different industries. For instance, data users in the telecommunications industry should be permitted to refuse data access requests that conflict with their licence conditions.

Proposal 17: Erasure of Personal Data

For data users who possess voluminous personal data in non-digital format, a clarification of the duty under section 26 and DPP2(2) concerning erasure of obsolete personal data is essential. We welcome provisions which are clear enough for data user to follow under different circumstances.

Proposal 18: Fee Charging for Handling Data Access Requests

The current criteria for assessing the excessiveness of DAR fees is arbitrarily imposed by the PCPD, as the term "excessive" in section 28(3) does not take into consideration practical business considerations. The PCPD arbitrarily assumes that the labour costs engaged in complying with DAR "*should only refer to the normal salary of a clerical or administrative staff who are able to handle the location, retrieval or reproduction work*". In the case of a large company, particularly one which adopts modern technology when

storing personal data, the data retrieval process could involve several security checks at different levels by various staff who may be more senior than a general office clerk.

We submit that it is essential to adopt a more flexible definition of what is considered to be excessive fees.

Proposal 20: Circumstances for Issuance of an Enforcement Notice

An enforcement notice serves to demand a data user to correct a wrong action. When an act is not continuing and there is no foreseeable likelihood of repetition, an enforcement notice in the circumstance is in fact otiose. We submit that the PCPD should not be empowered to demand a data user to alter any personal data systems or procedures unless such system or procedures have directly caused a contravention of the DPPs in the PDPO.

In order to enhance the protection of personal data privacy, the PCPD may consider providing professional recommendations and technical assistance to data users upon request so that they can improve their relevant systems and procedures.

Proposal 33: Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings

We support the introduction of this new exemption. Consideration should however be given to the difficulty faced by a data user in verifying whether the data is necessary for the legal proceedings as requested when the request is not made pursuant to a court order, considering that the data user would not have the required information to make the decision. To properly address the issue, it is recommended that the exemption should relieve the data user from any liability under the PDPO if the data requestor is a member of the judiciary or a legal practitioner from a recognised jurisdiction.

Proposal 38: Exclude Social Services from the Definition of "Direct Marketing"

We understand that the objective of this exemption is to ensure that the delivery of social services in the proper interests of society should not be hindered by the regulations of the PDPO. We support this proposal and at the same time suggest that the exemption should not be confined to social services offered by social workers, but should extend to social services offered or to be offered by any person or organization. This exclusion should apply by reference to the nature of the services rather than the persons who offered the services.

Conclusion

In summary, we submit that an effective regime for protecting personal data privacy should balance the rights of data subjects with business efficacy. Thank you for considering this submission. We would like an opportunity to clarify any questions you may have on the above.

November 2009

PCCW Limited

Consultation Document on Review of the Personal Data (Privacy) Ordinance

Submissions of the Hong Kong Bar Association

Preliminary

1. According to the Consultation Document (§4(a) refers), the first guiding principle for conducting the review of the Personal Data (Privacy) Ordinance (Cap 486) ("PDPO") is:

   "the right of individuals to privacy is not absolute. It must be balanced against other rights and public and social interests."

   This should not be the first guiding principle for the review. The first guiding principle – which is not included at all among the principles stated in the Consultation Document – should be that the right to privacy is a fundamental right guaranteed by Article 39 of the Basic Law, which provides for the continuation in force of the ICCPR wherein is enshrined both a general right to privacy and the right to protection of the law against arbitrary or unlawful interference with privacy, family or correspondence.

2. It is a matter of regret that the Consultation Document makes no reference to the fundamental status of the right to privacy. It is accepted that the right to privacy has to be balanced against other rights and public and social interests, but the balancing exercise must be done with the fundamental status of the right to privacy fully in mind.

3. In this Submission, the Hong Kong Bar Association sets out its response to the key proposals in the Consultation Document and also puts forward additional proposals not included in the Consultation Document.

Sensitive Personal Data

Proposal 1: Sensitive Personal Data

§8: *"At present, the PDPO does not differentiate personal data that are "sensitive" from those that are not. More stringent regulation of sensitive personal data is in line with international practices. However, there is no universally agreed set of sensitive personal data and perception of sensitive personal data is culture-bound. Given the challenges posed by the development of biometric technology on an individual's privacy, as a start we may consider classifying biometric data (such as iris characteristics, hand contour reading and fingerprints) as sensitive personal data."*

4. (a) Unrecognised by the Consultation Document, the Law Reform Commission ("the LRC") in its Report on Reform of the Law Relating to the Protection of Personal Data (August 1994) ("the LRC Report") considered, but rejected, a proposal for "*a specific restriction on the collection of specific categories of data*" (§§9.40 to 9.55). The LRC was of the view that the essential issue was whether the collection of the data was relevant to the data user's functions. It also considered that concerns about the use and abuse of sensitive data would be more efficiently addressed by "*the use of declarations and affording the individual an input prior to the implementation of adverse decisions.*" (§9.55)

(b) Addressing the LRC's arguments in turn. First, the fact that collection of a particular category of sensitive personal data must be relevant to a data user's functions does nothing to subject the processing of such data to stricter control in recognition of its greater potential to do harm. Second, the system of declarations proposed by the LRC, which was implemented (in modified form) by data protection principle 5 in Schedule 1 to the PDPO, does not serve to inform individuals that particular categories of sensitive information concerning them are being held by particular data users. Lastly, the only opportunity afforded to an individual for input prior to the implementation of an adverse decision is in relation to an adverse decision consequent on a "matching procedures" (s 30(5) of the PDPO refers), which covers a relatively narrow ambit of data processing.

(c) It follows that the rationale for the LRC's rejection of specific restrictions on the processing of sensitive data does not hold good.

(d) As the Consultation Document points out, the EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data ("the EU Directive") requires Member States to apply more stringent requirements to the processing of sensitive data.

(e) Specifically (by Article 8(1)) Member States are required to prohibit "*the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*". This requirement does not apply in five specified circumstances, including where the data subject has given his "explicit consent" (Article 9 refers).

(f) As the Consultation Document also points out, the application of greater restrictions to the processing of sensitive data is not confined to EU Member States. This is also the case in Australia under the federal Privacy Act, as well as, for example, Japan, Korea and Macau.

(g) In line with international practice, given the higher risks posed to individuals by the processing of sensitive data (and having considered and rejected the LRC's contrary arguments), the proposal that there should be more stringent control of the processing of such data is supported. (h) However, the proposal to "*start [by] ... classifying biometric data ... as sensitive personal data*" is too narrow. Other than pointing out that "*perception of sensitive personal data is culture-bound*" (§3.03), the Consultation Document does not address the issue of why none of the types of personal data defined as sensitive in the EU Directive (see above), or variations on them, should be included within any definition of "sensitive data" at the start.

§9: *"To provide a higher degree of protection to sensitive personal data, we have set out in the consultation paper a possible regulatory model to limit the handling of sensitive personal data by data users to specified circumstances in order to narrow down the scope of collection and use of such data."*
§3.09: *"The collection, holding, processing and use ("handling") of sensitive personal data would be prohibited except in the following circumstances:*
(a) the prescribed consent (i.e. express consent given voluntarily) of the data subject has been obtained;
(b) it is necessary for the data user to handle the data to exercise his right as conferred by law or perform his obligation as imposed by law;
(c) handling of the data is necessary for protecting the vital interests of the data subject or others where prescribed consent cannot be obtained;
(d) handling of the data is in the course of the data user's lawful function and activities with appropriate safeguard against transfer or disclosure to third parties without prescribed consent of the data subject;
(e) the data has been manifestly made public by the data subject;
(f) handling of the data is necessary for medical purposes and is undertaken by a health professional or person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional; or
(g) *handling of the data is necessary in connection with any legal proceedings."*

5. (a) There is no explanation in the Consultation Document as to why the proposed exceptions have been formulated in the way they have. While the justification for some of the proposed exceptions, such as (a) and (c), is obvious. The same cannot be said for others. It is not clear, for example, why proposed exception (g) should be necessary given proposed exception (b).

(b) There is some overlap between the proposed exceptions and the exceptions provided for in the EU Directive. For example, proposed exceptions (a), (c) and (e) are similar to exceptions (a), (c) and (e) under Article 9 of the EU Directive. However, proposed exception (b) is broader that its equivalent under Article 9, which is restricted to obligations and rights "*in the field of employment law in so far as authorised by national law providing for adequate safeguards*", and proposed exceptions (d), (f) and (g) have no equivalents at all under the EU Directive.

(c) Proposed exception (d) is of particular concern because it would render the proposal for special control on the processing of "sensitive data" close to being nugatory. Save for the addition of "*appropriate safeguard against transfer or*

disclosure to third parties without prescribed consent of the data subject", exception (d) is in fact the *status quo* under the PDPO pursuant to which there is no special control on the processing of "sensitive data". As a result, if exception (d) were adopted, data users could continue to collect, hold, process and use "sensitive data" as they did before *so long as* they did not transfer or disclose the data to third parties or only did so pursuant to exemptions to DPP3 as provided for in Part VIII of the PDPO (bearing in mind the recommendation to apply all the exemption provisions of Part VIII of the PDPO to "sensitive data": see §3.10 of the Consultation Document).

(d) The inclusion of exception (d) is objected to accordingly.

§3.12: "*We may consider making non-compliance with DPPs with regard to handling of sensitive personal data an offence.*"

6. For the same reason that this proposal should not be adopted generally (see below), viz. the DPPs are not precise enough to allow for sufficient certainty as to what they prohibit or permit to found criminal offences, so too should this proposal not be adopted in relation only to "sensitive data".

§§3.13 & 3.14: "*It may be advisable to apply the new requirements only to sensitive personal data collected after the relevant legislative provision comes into force ... Alternatively, we may specify a transitional period following the enactment of the new provision during which the processing of sensitive personal data will be exempted from the additional requirements.*"

7. (a) Sensitive personal data collected before the proposed new restrictions on the processing of such data come into force should not be excluded from the application of the new restrictions indefinitely. Accordingly, a transitional arrangement is preferred whereby such data will be made subject to the new restrictions upon the expiry of a specified period.

(b) For the avoidance of doubt, the transitional period should *not* apply to sensitive personal data collected after the new provisions come into effect.

Data Security

Proposal No 2: Regulation of Data Processors and Sub-contracting Activities

§§10-12: *"The rising trend of data users sub-contracting and entrusting data processing work to third parties has increased the risk to which personal data may be exposed. At present, the PDPO does not regulate processors which process personal data for data users. To strengthen security measures governing personal data entrusted to data processors, we have set out possible regulatory options.*
"Under such options, a data user who transfers personal data to a data processor for holding, processing or use, would be required to use contractual or other means to ensure that his data processor and any sub-contractors will take all practicable steps to ensure the security and safekeeping of the personal data, and to ensure that the data are not misused and are deleted when no longer required for processing.
"As part of the options, we can consider directly regulating data processors by imposing obligations on them. They would be required to exercise the same level of due diligence as the data user with regard to security, retention and use of the personal data thus entrusted. Recognising that compliance with certain requirements may pose problems for some data processors due to the operational constraints unique to specific industry sectors, we have also included the option of subjecting different categories of data processors to different obligations."

8. (a) The reason why the PDPO (by virtue of s 2(12)) does not impose obligations on persons who hold, process or use personal data solely on behalf of other persons and not for their own purposes is that many such persons have no knowledge of whether or not the data they hold, process or use are personal data and/or have little or no control over the processing of the data other than at the highest level. Operators of webmail services or social networking websites are two examples. On the other hand, there are data processors of the out-source and other types who are entrusted to carry out data processing with respect to data they know to be personal data (such as customer records) and which have full control over the processing of such data (within the terms of their contracts with the parties entrusting the data to them).

(b) Data processors of the former type are not in a position to ensure compliance with the requirements of the PDPO. Nor are their "users" generally in a position to require

them to do so. Accordingly, data processors of the former type should continue to be excluded from direct regulation under the PDPO and their "users" should not be made subject to any requirement to ensure they comply with the PDPO. For such data processors, it is sufficient that the "users" are themselves subject to the PDPO.

(c) There is no good reason why data processors of the latter type (i.e. out-source data processors and the like) should not be made subject to direct regulation under the PDPO subject to a satisfactory definition of what constitutes such a data processor.

(d) The proposal that a data user be required to use contractual or other measures to secure compliance with relevant obligations of the PDPO when contracting out the processing of personal data to third parties is *not* supported as an alternative to direct regulation (but is supported in conjunction with direct regulation). Given the doctrine of privity of contract, a data subject would not be able to enforce such a requirement; nor would a data subject have any remedy for its breach as against the data processor but may have a remedy against the principal via ss 65 and 66 of the PDPO.

Proposal No. 3: Personal Data Security Breach Notification

§13: "*Following the spate of personal data leakage incidents, questions have been raised on whether a personal data security breach notification ("privacy breach notification") system should be instituted to require data users to notify the PCPD and affected individuals when a breach of data security leads to the leakage or loss of personal data so as to mitigate the potential damage to affected individuals. A mandatory notification requirement could impose undue burden on business operations. Bearing in mind that a number of overseas jurisdictions adopt voluntary guidelines on privacy breach notifications, we consider it more prudent to start with a voluntary breach notification system so that we can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing onerous burden on the community. For this purpose, the PCPD can issue guidelines on voluntary privacy breach notifications.*"

9. Given the extent and size of the known data leakage incidents that have occurred in the last few years in Hong Kong, this problem is of sufficient seriousness to be

addressed by appropriate measures. A voluntary breach notification system under a framework provided by guidelines issued by the PCPD is a positive first step to take.

Enforcement Powers of the PCPD

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

§14. *"At present criminal investigations are conducted by the Police and prosecutions by the Department of Justice. We have considered if these powers should be conferred on the PCPD. Since some offences proposed in this review are not technical in nature and involve a fine and imprisonment, there could be concern if such powers are delegated to the PCPD. Moreover the existing arrangements have worked well. We do not see a strong case to give the PCPD the power to investigate into and prosecute criminal offence cases."*

10. (a) There is no good reason for granting the PCPD criminal investigation and prosecution powers.

(b) The lack of such powers may mean that in some cases 6 months will have elapsed before a complaint case has been considered for referral to the police for criminal investigation or to the Secretary for Justice for possible prosecution, thereby rendering any prosecution time-barred. This problem is best addressed by extending the time within which prosecutions under the PCPO may be brought (as proposed in proposal 40) rather than by granting criminal investigation and prosecution powers to the PCPD.

Proposal No 5: Legal Assistance to Data Subjects under Section 66

§15: *"Under Section 66 of the Ordinance, a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user in relation to his personal data is entitled to compensation from the data user. The PDPO does not empower the PCPD to provide assistance to aggrieved data subjects in respect of legal proceedings. To achieve greater deterrent effect on acts or practices which intrude into personal data privacy and enhance the overall effectiveness of sanctions provided for under the PDPO, views are invited on whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject."*

11. (a) Compared with the position with respect to the anti-discrimination ordinances, there has been a marked lack of claims for compensation for breaches of the PDPO. In fact, the Bar Association is aware of only one that has gone to trial and that claim was misconceived (Kwan Chi Shan v Yeung Yin Fong (關子山訴楊燕芳) (unreported, 4 December 1997, DCCJ 7812 of 1997)).

(b) One reason for the lack of such cases may be the fact that breaches of the PDPO are generally less likely to result in claims for substantial damages than in the case of breaches of the anti-discrimination ordinances, which often involve substantial claims for loss of income.

(c) Undoubtedly, however, the fact that the EOC has an express mandate to assist claimants making claims for breaches of the anti-discrimination ordinances has resulted in the development of the jurisprudence on the meaning and effect of those ordinances and encouraged claimants to bring cases without such assistance.

(d) In order to achieve a similar result, the proposal to empower the PCPD to provide legal assistance to claimants under s 66 of the PDPO along the lines of the EOC model is supported.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

§16. *"We have considered whether the PCPD should be empowered to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement by a data user, as an alternative to the existing redress avenue to seek compensation through the court as provided for under Section 66 of the PDPO. The appropriate body to determine compensation under the PDPO was thoroughly discussed in the Law Reform Commission ("LRC") Report on Reform of the Law Relating to the Protection of Personal Data issued in August 1994. The LRC opined that conferring power on a data protection authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions. The LRC recommended that the PCPD's role should be limited to determining whether there has been a breach of the Data Protection Principles ("DPPs"). It would be for a court to determine the appropriate amount of compensation payable. Views are invited on*

whether it is appropriate to introduce an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects."

12. (a) The reasons for the LRC's objection to granting the PCPD the power to award compensation still hold good.

(b) Two of the main reasons why claimants do not seek or obtain compensation for breaches of the PDPO at present are an under-developed jurisprudence on the meaning and effect of the PDPO (particularly in relation to claims for compensation) and the costs-risk for the "sandwich class" (in theory legal aid is available to claimants who pass the means and merits tests). Mandating the PCPD to assist claimants (see response to proposal 5 above) should go some way to addressing these obstacles to compensation claims under the PDPO.

(c) The proposal is accordingly not supported.

(d) As an alternative avenue for claimants to receive financial recompense for claimed breaches of the PDPO it is proposed that the PCPD be mandated (by amendment to the PDPO) to offer complainants and parties complained against the option of mediation in complaint cases he has decided to investigate (before commencing his investigation).

Offences and Sanctions

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

§§17&18: *"The PCPD is empowered to remedy contravention of a DPP by issuing an enforcement notice to direct the data user to take remedial steps. Contravention of the enforcement notice is an offence ... One option is to consider making contravention of a DPP an offence. Bearing in mind that DPPs are couched in generic terms and can be subject to a wide range of interpretations, to make contravention of a DPP a criminal offence would have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability. Moreover, this would be moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether we should make contravention of a DPP an offence."*

13. The DPPs are not precise enough to allow for sufficient certainty as to what they prohibit or permit in order to found a criminal offence. This is why breach of the DPPs was expressly excluded from the general offence provision of the PDPO (s 64(10) refers). The Proposal is accordingly not supported.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

§19: *"Incidents of blatant dissemination of leaked personal data on the Internet have aroused widespread concern in the community regarding the possible misuse of leaked personal data, such as fraud or identity theft. Unauthorised use of personal data may also intrude into personal data privacy and may cause damage to data subjects. To curb irresponsible dissemination of leaked personal data, we may consider making it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes."*

14. (a) The Proposal is supported.

(b) Any such offence should include an express *mens rea* element, e.g. obtaining or procuring the obtaining of personal data and disclosing the data with the intention of making a profit thereby and/or to cause harm to a subject of the data *knowing* the data user that is the source of the data has not given consent to their disclosure or being *reckless* as to whether such consent has been given or not.

(c) The appropriate level of penalty should be in line with the more serious offences provided for in s 64 of the PDPO which carry maximum penalties of a fine at level 3 and imprisonment for 6 months.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

§20: *"Under the PDPO, if a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently does the same act or engages in the same practice, the PCPD would issue another enforcement notice. Since the enactment of the PDPO, PCPD has not come across any such case of circumvention. To forestall possible circumvention of the regulatory regime, one option is to consider making it an offence if a data user repeats such contravening act. However, this would be*

moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether this is appropriate."

15. (a) It is not accepted that the proposal and the "*original intent of adopting the DPPs in the PDPO*" are in some way incompatible.

(b) Breach of the DPPs was not made an offence because the DPPs are too imprecise to afford reasonable certainty as to compliance for the purpose of imposing criminal sanctions. An enforcement notice issued by the PCPD, on the other hand, should state with particularity what a data user is required to do in order to comply with whatever DPP is in issue. (If the enforcement notice does not do this, it would be liable to be set aside on appeal to the Administrative Appeals Board.) Accordingly, the proposed new offence should not place data users in jeopardy of unwitting contravention unlike the position that would pertain if breach of the DPPs *simpliciter* was made an offence.

(c) The Proposal is accordingly supported.

(d) The penalty should be less than for a breach of an enforcement notice (fine at level 5 and imprisonment for 2 years: s 64(7) of the PDPO refers) because there would be no element of directly flouting a requirement imposed by the PCPD. On the other hand, the penalty should be greater than that for the general offence provision (fine at level 3: s 64(10) of the PDPO refers). The Bar Association proposes a penalty of a fine at level 5.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

§21: "*We have considered the option of empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. It is not common for non-judicial bodies to have the statutory power to impose monetary penalties. Under the PDPO, the DPPs are couched in generic terms and can be subject to wide interpretations. Although we may require the PCPD to issue guidance on the circumstances he considers appropriate to issue a monetary penalty notice, whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment. Views are invited on whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.*"

16. (a) For the reasons given in §§6.19 and 6.20 of the Consultation Document the proposal is not supported.

(b) The Bar Association is of the additional view that the imposition of a monetary penalty is a fine by another name. For the same reason that a breach of the DPP should not carry a criminal sanction (including a fine) so too should this not expose someone to a "monetary penalty". Adding the subjective element of "serious" does not make the risk of unwitting non-compliance any less.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

§22: *"The PDPO does not provide for heavier sanction for data users who repeatedly contravene an enforcement notice. Since the enactment of the PDPO, there has not been a problem with repeated offenders. We have considered the option to subject a repeated offender to heavier penalty to achieve greater deterrent effect. Views are invited on whether there is a need to impose a heavier penalty for such repeated offenders."*

17. (a) The penalty for contravention of an enforcement notice is a fine at level 5 ($50,000) and to imprisonment for 2 years: s 64(7) of the PDPO refers. In line with usual sentencing principles, if someone is proved to have contravened an enforcement notice more than once, this should (all other things being equal) result in a heavier penalty up to the maximum than would be imposed on someone who has done so only once.

(b) In any event, the lack of any incident of repeat contravention of an enforcement notice suggests that the deterrent effect of a higher maximum penalty in such a case (than is currently provided for in s 64(7)) is unnecessary.

(c) The Proposal is accordingly not supported.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

§23: *"Direct marketing calls are often a cause of complaint and nuisance to the data subjects. The PCPD is of the view that the existing level of a fine at Level 3 (up to $10,000) may not be sufficient to act as an effective deterrent to contain the problem and recommends the penalty level be raised. To curb misuse of personal data in direct marketing activities, we may consider raising the penalty level for misuse of personal data in direct marketing. Public views are invited on the appropriate level of penalty."*

18. The Proposal to raise the penalty (for contravention of s 34 of the PDPO) is supported.

(b) The Bar Association proposes that the penalty be increased to a fine at level 5 ($50,000).

Proposals not contained in the Consultation Document

To relieve data users from the obligation to redact the name or other information explicitly identifying another individual as the source of personal data that are the subject of a data access request when complying with the request if it is reasonable in all the circumstances for the data user to believe the requestor knows who the source is or would be able to infer this from a copy of the data from which the name or other information explicitly identifying the source have been redacted.

19. (a) Pursuant to s 20(1)(b) of the PDPO a data user *must* refuse to comply with a data access request if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject unless the other individual consents to such disclosure.

(b) The refusal obligation of s 20(1)(b) is subject to s 20(2) of the PDPO. There are two parts to s 20(2). The first part, s 20(2)(a), provides that where the "other individual" (as referred to in s 20(1)(b)) is the source of the personal data that has been requested, s 20(1)(b) shall not operate unless that other individual is *named* or *explicitly identified*. The second part of s 20(2), s 20(2)(b), provides that s 20(1)(b) shall not operate if the data user can comply with the data access request without disclosing the identity of the other individual by the omission of names, or other identifying particulars, or otherwise.

(c) The combined effect of ss 20(1)(b) and 20(2) is to require a data user to redact copies of personal data provided in compliance with a data access request in order to remove data that identify any other individual. In the case of an individual who is the source of the requested data, the requirement is met if the *name* or *other information explicitly identifying* the individual is redacted. In relation to any other individual it is necessary to remove all information that would identify him: see generally *Wu Kit Ping v Administrative Appeals Board* [2007] 5 HKC 450.

(d) In practice, compliance with this redaction requirement can be extremely onerous for a data user because each document containing personal data within the scope of the request must be reviewed for any references to any other individuals. Where a document contains such a reference, a decision must be taken as to what (if anything) must be redacted in order to comply with ss 20(1)(b) and 20(2) of the PDPO. This is often not obvious. Nor can this redaction obligation be taken lightly because non-compliance without reasonable excuse is an offence (s 64(10)).

(e) It is certainly accepted that the redaction requirement is necessary to protect the privacy of other individuals referred to in documents containing personal data that are the subject of an data access request. However, in the case of an individual who is the source of the requested personal data, redaction is often unnecessary because the requestor knows who the source of the data is or can infer this from the data remaining after the source's name or other information *explicitly identifying* him has been removed. For example, where a data access request is made to personal data in an employment performance appraisal, the data user is required to remove the name and title of the appraiser in order to comply with ss 20(1)(b) and 20(2). However, the requestor will usually either remember who the appraiser was or will be able to infer this from the period to which the appraisal relates. As a result, the redaction (in such a case) serves no meaningful purpose.

(f) In order to relieve part of the burden of the redaction obligation on data users in complying with data access requests, therefore, it is proposed that the PDPO be amended such that this obligation does not apply where the other individual referred to in the requested data is the source of the data and it is reasonable in all the circumstances for the data user to believe the requestor knows who the source is or would be able to infer this from a copy of the data from which the name or other information explicitly identifying the source have been redacted.

To publish or otherwise make available to the public and the legal profession all decisions of the Administrative Appeals Board on appeal from a decision of the PCPD.

20. (a) Judgments on the interpretation of the PDPO are few and far between. Apart from the single case of a claim for monetary compensation, there are only a handful of judgments from applications for judicial review of decisions of the PCPD. The vast majority of cases of persons aggrieved by the decisions of the PCPD are determined by administrative appeal to the Administrative Appeals Board which does not publish its decisions. A valuable source of jurisprudence is closed to the legal profession and appropriate advice cannot be given to lay clients. The summaries of selected Administrative Appeals Board decision are not adequate for the purpose giving appropriate advice since it is often necessary to consider the relevant decision in context with appreciation of the full submissions and reasoning.

(b) The Bar Association proposes that all decisions of the Administrative Appeals Board to date on an appeal from a decision of the PCPD be published or made available online.

Dated this 16th day of November, 2009
Hong Kong Bar Association

THE
HONG KONG
ASSOCIATION
OF
BANKS
香港銀行公會

S0068

20 November 2009

By e-mail: pdpo_consultation@cmab.gov.hk and post

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Sirs,

Consultation Document on Review of the Personal Data (Privacy) Ordinance

We refer to the Consultation Document on Review of the Personal Data (Privacy) Ordinance ("**PDPO**") published by the Constitutional and Mainland Affairs Bureau ("**Bureau**") in August 2009 ("**Consultation Document**"). On behalf of our members, we set out our views on various proposals in the Consultation Document.

1. General

1.1 We would like to begin by thanking the efforts of the Bureau and the Privacy Commissioner for Personal Data ("**PCPD**") in preparing the Consultation Document and the amendment proposals. We share the view that it is timely to review the provisions of the PDPO in light of the evolvement in technology and to take account of the experience since the PDPO became effective.

1.2 We fully support the guiding principles set out in paragraph 4 of the Executive Summary of the Consultation Document. In particular, there should be a balance between right to privacy and other interests. In deciding whether to implement any proposed changes or measures, the time, effort and resources which would be involved in compliance with those changes or measures need to be weighed against the benefits to be achieved. Further, where the existing provisions of the PDPO work satisfactorily or where the issues are currently addressed by other statutes or legal principles, they should be left undisturbed.

1.3 We strongly urge the Bureau to publish the consultation results and conduct further consultation on any draft amendments to the PDPO.

Chairman The Hongkong and Shanghai Banking Corporation Ltd
Vice Chairmen Standard Chartered Bank (Hong Kong) Ltd
Bank of China (Hong Kong) Ltd
Secretary Jennifer Cheung

主席 香港上海匯豐銀行有限公司
副主席 渣打銀行（香港）有限公司
中國銀行（香港）有限公司
秘書 張學欣

Incorporated by Ordinance, Cap. 364
根據條例第364章成立

1.4 Finally, we wish to put forward two issues set out as Additional Proposal (1) and Additional Proposal (2) in this submission for the consideration of the Bureau in its comprehensive review of the PDPO and related regulations.

2. HKAB's views

Proposal No. 1: Sensitive Personal Data
Invitation of Comments: *Whether there is a need to accord better protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances and, if yes, whether the possible regulatory regime, including coverage of sensitive personal data, related regulatory measures, sanctions and the need for grandfathering of transitional arrangement as set out in the Proposal is appropriate.*
Response: (a) From the banks' perspective and having particular regard to the nature of banking business and the purposes for which personal data are used by banks, our general view is that the existing regime under the PDPO provides sufficient protection. Accordingly, there is no need to distinguish between sensitive data and other personal data. (b) Having said that, sensitive data is a complex and evolving topic with far-reaching implications. Any proposed changes or measures should be thoroughly discussed and examined and subject to a separate consultation.
Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities
Invitation of Comments: *Whether a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties.*
Response: (a) We support the use by data users of contractual means to secure compliance with relevant PDPO obligations by data processors. (b) We would, however, emphasize that any requirements imposed on data users should be reasonable and practicable. Data users should not be required to secure data processors' compliance of the PDPO or performance of the contracts between them and the data users by any measures other than reasonably practicable

measures. In particular, data users should not be required to proactively and continuously oversee or monitor the operations of data processors to ensure compliance. Imposing such requirements will create an unduly burdensome administrative and operational obligation on data users. This will significantly reduce business efficacy and cost-effectiveness and, in turn, defeat the objective of the sub-contracting arrangement.

Invitation of Comments:

Whether the activities of a data processor should be directly regulated under the PDPO or whether it is sufficient to indirectly regulate the data processor through the data user by contractual or other means.

Response:

(a) As banks are one of the largest groups of outsourcer of personal data, we support in principle direct regulation of data processors under the PDPO. Our support is given on the basis that direct regulation will enhance and maintain the quality and standards of data processors and, in turn, facilitate the data users' selection and use of data processors.

(b) Any changes or measures should take account of the vast variety of data processors and their services.

Invitation of Comments:

If activities of data processors were to be directly regulated under the PDPO, what obligations should be imposed on data processors, and whether it is appropriate and practical to subject different categories of data processors to different obligations.

Response:

A logical approach would be to derive the data processors' obligations from the obligations imposed by the PDPO on data users. Subjecting different categories of data processors to different obligations may complicate the regulatory process and reduce efficiency. Any requirements to be imposed on data processors should be sufficiently general to address different industry sectors.

Proposal No. 3: Personal Data Security Breach Notification

Invitation of Comments:

The need to institute a voluntary privacy breach notification system in Hong Kong.
The components of a breach notification mechanism.

Response:

(a) Generally speaking, we do not have any particular concern with a voluntary privacy breach notification system under the PDPO.

(b) Having said that, we would emphasize that:

(i) any changes or measures should clearly specify the notification arrangement (including the circumstances triggering notification, the information to be provided in the notice and any timeline for providing the notice);

(ii) any notification should be subject to a materiality test (whether as to the relevant provision of the PDPO being breached or the severity of the breach);

(iii) given the voluntary nature of the notification system, failure to notify should not result in any sanction of any nature, statutory or otherwise; and

(iv) it is appropriate to specify the notification arrangement, given its voluntary nature, in a guideline to be issued by the PCPD rather than in the PDPO, and there should be a separate consultation on the relevant guideline.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

Invitation of Comments:

Whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.

Response:

The Bureau is of the view that there is not a strong case to give the PCPD the power to investigate and prosecute criminal offence cases. We share its view and rationale that the PDPO should not give the PCPD the power to investigate and prosecute criminal offence cases.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

Invitation of Comments:

Whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under Section 66 of the PDPO, along the lines of the EOC model

Response:

(a) We have great reservation on this Proposal.

(b) It is not appropriate to compare the PDPO regime to the EOC regime as they address issues of very different nature.

(c) In deciding whether to implement this Proposal, the following issues should be thoroughly considered and the interests of data subjects and data users should be carefully and fairly balanced:

(i) damages incurred by data subjects are often not substantial;

(ii) use of any public funding to provide legal assistance must be justified;

(iii) the risk of abuse by data subjects;

(iv) in the UK, the Information Commissioner may act on behalf of or in concert with a complainant. This power only applies where the case concerns data processed for "special purposes" and if the Information Commissioner is of the opinion that the case involves a matter of substantial public importance. This power covers proceedings brought by an individual for failure on the part of a data user which relate to personal data processed for "special purposes". The term "special purposes" is defined to mean any one or more of (1) purposes of journalism, (2) artistic purposes and (3) literary purposes; and

(v) in the US, there is no data privacy specific legal assistance mechanism available to data subjects.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

Invitation of Comments:

Whether it is appropriate to introduce at this stage an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Response:

The Law Reform Commission took the view that the role of the PCPD should be limited to determining whether there has been a breach of requirements under the PDPO whereas the determination of the appropriate amount of compensation should be left to a court. We share its view and rationale, in particular, that the appropriate amount of compensation should be determined by an impartial party.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

Invitation of Comments:
Whether we should make contravention of a DPP an offence.

Response:

We agree to the analysis set out in paragraph 6.04 under this Proposal in the Consultation Document. Criminal liability should not be imposed across the board to contravention of DPPs. The appropriate approach is to impose criminal liability having regard to the severity of the contravening acts or practices.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

Invitation of Comments:
Whether we should make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent; and if yes, the need for defence provisions and the appropriate level of penalty.

Response:

(a) We agree that those acts should be strongly discouraged. Therefore, in principle, we support the proposal to make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent.

(b) Having said that, we would emphasize that:

(i) what constitutes the criminal acts should be clearly defined, and inadvertent acts should be excluded;

(ii) any changes to the PDPO should only be required for closing loopholes under existing legislation. If criminal sanctions addressing those acts already exist under other statutes, there is no need to introduce further criminal sanctions under the PDPO unless it achieves additional results; and

(iii) it should be a defence for an employer if it has taken, in its capacity as employer, reasonably practicable steps to prevent contravention by its staff.

Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts
Invitation of Comments: *Whether it is appropriate to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice. If yes, the appropriate penalty level for the offence, bearing in mind that non-compliance with an enforcement notice is subject to a fine of $50,000 and to imprisonment for two years.*
Response: We note that the PCPD has not come across any case of circumvention as depicted in the Consultation Document. As the existing structure works well, we do not consider it necessary to adopt this Proposal or complicate the existing structure.
Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles
Invitation of Comments: *Whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.*
Response: We share the view and rationale of the Bureau set out in paragraph 6.20 under this Proposal in the Consultation Document. In particular, in view of the practical difficulty of defining what constitutes serious contravention, it is more appropriate to single out particular acts or practices of contravention of DPPs of a serious nature and make them an offence rather than giving the PCPD power or discretion to impose monetary penalties where the PCPD considers any contravention of DPP serious.
Proposal No. 11: Repeated Non-compliance with Enforcement Notice
Invitation of Comments: *Whether heavier penalty should be imposed for a second or subsequent conviction of Section 64(7); and if yes, the appropriate penalty level, bearing in mind the existing penalty level for contravention of an enforcement notice which is a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, a daily fine of $1,000.*
Response: We note from the Consultation Document that there has not been a serious problem with

repeated offenders. As the existing structure works well, we do not consider it necessary to adopt this Proposal or complicate the existing structure.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

Invitation of Comments:

Whether we should safeguard the vital interest of vulnerable classes of data subjects by devising a system which empowers a specified third party (the definition of which will be set out in the amendment legislation) to give consent to the change of use of personal data of such data subjects when it is in their best interests to do so.

Response:

(a) We respect the rationale of this Proposal. Nevertheless, protection of vital interests of vulnerable individuals in the nature described in this Proposal is not a privacy-related issue. There are various safeguards under existing law and legislation which are developed specifically with those interests in mind. It is not appropriate to create a separate framework on this subject under the PDPO.

(b) We are also concerned that the Proposal will impose unduly onerous and unreasonable obligations on data users. In particular, given the nature of banking business and transactions, it is often difficult in practice for banks (or indeed any data users) to determine whether the second condition specified in this Proposal is satisfied (i.e. the condition that the proposed use of the personal data involves a clear benefit to the data subject). We do not think it is fair to place that burden on the banks or data users.

Proposal No. 14: Parents' Right to Access Personal Data of Minors

Invitation of Comments:

(a) whether new provisions should be introduced to permit a data user to refuse a data access request made by a "relevant person" on behalf of a minor in order to protect the interests of minors taking into account the need for parents to exercise their rights and responsibilities over their children for the proper care of them; and

(b) if new provisions should be introduced, whether the possible option set out in paragraph 11 under this Proposal in the Consultation Document is appropriate; and whether some factors should be specified to enable the data user to assess if there are reasonable grounds in refusing such a data access request.

Response:

We repeat our comments in our response to Proposal No. 13.

Proposal No. 15: Access to Personal Data in Dispute

Invitation of Comments:

Whether we should add a provision under the PDPO that, where the lawfulness of a refusal to comply with a data access request is in dispute before the Administrative Appeals Board ("AAB"), a court of a magistrate, the relevant personal data should not be disclosed to the data requestor and other parties bound by the decision of the AAB, the court or magistrate, whether by discovery or otherwise, pending a determination in favour of the requestor.

Response:

(a) We support this Proposal.

(b) There are instances of abuse of the present loophole under the PDPO by data requestors. In those cases, the data requestor, using the appeal process, managed to obtain the requested data before the conclusion of the legal proceedings and thereby defeated the data user's objection to comply with the data access request in the first place.

Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

Invitation of Comments:

Whether to provide a new ground for a data user to refuse to comply with a data access request under Section 20(3) where the data user is obliged or entitled under any other ordinances not to disclose the personal data.

Response:

(a) We support this Proposal.

(b) With the removal* of section 3(2) of the PDPO, it is necessary to clarify the position where there are inconsistencies between the PDPO and other Ordinances.

* Section 3(2) was not adopted as the laws of the HKSAR by the decision of the Standing Committee of the National People's Congress on Treatment of the Laws Previously in Force in Hong Kong in accordance with Article 160 of the Basic Law of the HKSAR.

Proposal No. 17: Erasure of Personal Data

Invitation of Comments:

Whether we should amend the PDPO so that the provision concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use.

Response:

(a) We support this Proposal.

(b) The introduction of a "reasonably practicable" standard is also in line with the approach adopted with respect to other requirements under the PDPO including, section 19(4)(ii), DPP 1(3), DPP 2(1), DPP 4 and DPP 5.

Proposal No. 18: Fee Charging for Handling Data Access Requests

Invitation of Comments:

Whether for the purpose of complying with Section 28(3) of the PDPO, a data user should be required not to charge fees for complying with a data access request in excess of the prescribed maximum as set out in a fee schedule in the PDPO; and if yes, the parameters for setting the prescribed maximum in respect of any proposed fee charging model.

Response:

(a) It is only fair that a data user is allowed to charge fees for handling a data access request which are reasonable in the circumstances of the case. We support the principle that a data user should not charge excessive fee and this should continue to be observed by all data users.

(b) Apart from the practical challenge on designing the actual fee charging model proposed by this Proposal, we do not support implementing this Proposal for the following reasons:

(i) introducing a complicated fee charging model will increase the administrative or operational burden on data users in calculating the fees to be applied in each case;

(ii) the fee charging model should be simple and unambiguous to data subjects and a complicated fee charging model is likely to encourage arguments and disputes;

(iii) setting maximum fees may encourage abuse by data subjects - in our

members' experience, data access requests are often driven, not by privacy concerns, but other motives not relating to data privacy; and (iv) given that the existing fee mechanism is practicable and can be easily adapted by individual data users in setting and reviewing their own policies in such regard, any change or complication must be justified by what it can actually achieve.
Proposal No. 19: Response to Data Access Requests in Writing and Within 40 Days
Invitation of Comments: *(i) Whether a data user should be required to inform a requestor in writing if he does not hold the requested personal data, save for a request related to criminal conviction record data which the Police does not hold; and* *(ii) whether a data user is required to inform a requestor within 40 days if he does not hold the personal data for which a copy of the personal data is requested, irrespective of whether the response is in written or verbal form.*
Response: We support this Proposal.
Proposal No. 20 : Circumstances for Issue of an Enforcement Notice
Invitation of Comments: *Whether to allow discretion for the PCPD to serve an enforcement notice under any of the following circumstances:* *(a) whether the act of contravention is continuing;* *(b) whether the contravention will continue or be repeated;* *(c) whether the contravention has caused or is likely to cause damage or distress to the data subject.*

Response:

(a) We consider the existing provisions adequate from a personal data protection perspective whilst avoiding unnecessary administrative burden.

(b) If a data user ceases any act of contravention during the investigation by the PCPD, or if there is no likelihood of repetition, or if the data subject does not suffer any real damage, issuing an enforcement notice does not serve any useful purpose. More importantly, the objective of protecting personal data privacy is still achieved and at the same time keeping data subjects from abusing the complaint mechanism.

Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

Invitation of Comments:

Whether an exemption from DPP 3 should be provided for the transfer or disclosure of personal data in intended merger, acquisition or transfer of businesses subject to the condition that the resultant organization will offer substantially similar service as the original data user. If yes, whether the option set out in paragraph 52 under this Proposal in the Consultation Document is appropriate.

Response:

(a) We support this Proposal for adding an exemption from DPP 3.

(b) Whilst supporting this Proposal, we are of the view that:

(i) with a view to truly facilitating business mergers or acquisitions, it is worth considering extending the exemption beyond the due diligence stage and permitting the resultant organization or business transferee to continue to use the personal data after the merger or acquisition; and

(ii) we do not consider it necessary to impose the conditions specified in paragraph 52 except the first condition (i.e. the condition that the resultant organization or the business transferee will provide essentially the same or similar service to the data subjects as the original data user who holds the data). That condition will preserve use of personal data for the original purposes or essentially similar purposes in the hands of the resultant organization or business transferee, which will itself be subject to the PDPO with respect to the personal data provided by the original data user. As long as the resultant organization or business transferee is put in the same position (insofar as the PDPO) is concerned, the protection of personal data will not be prejudiced.

Proposal No. 29: PCPD to Disclose Information in the Performance of Functions
Invitation of Comments: *Whether to amend Section 46 to allow PCPD and his prescribed officers to disclose information reasonably necessary for the proper performance of his functions and exercise of his powers.*
Response: We do not agree to a general provision allowing the PCPD or his officers to disclose information in the performance of his functions and exercise of his powers. This concept is too vague and broad. Any exception to be introduced to the PCPD's obligation to maintain secrecy should be specified and limited, in particular, any exception to allow the PCPD to disclose information to overseas data protection authorities should be restricted to non-confidential data.
Proposal No. 32: Power to Obtain Information to Verify a Data User Return
Invitation of Comments: *Whether to confer upon the PCPD the power to obtain information from any person in order to verify the information in a data user return filed under Section 14 of the PDPO.*
Response: (a) We support the status quo and strongly object to this Proposal. Imposing the proposed requirement will likely result in significant increase on the administrative and operational burden of data users. (b) Under the existing section 64(1) of the PDPO, a data user commits an offence if he knowingly or recklessly supplies any information in a data user return which is false or misleading in a material particular. Balancing the principle of personal data protection and the principle to avoid onerous burden on business operations, we do not believe the benefit to be achieved by the proposed change justifies the burden it imposes on data users.
Proposal No. 33: Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings
Invitation of Comments: *Whether to create an exemption from DPP 3 for use of personal data required or authorized by or under law, by court orders, or related to any legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights.*

Response:

(a) We support this Proposal as it adds clarity.

(b) We are, however, concerned that the Invitation of Comments seems to imply that, at present, personal data cannot be used for establishing, exercising or defending legal rights without the prescribed consent of the data subject. DPP 3 allows use of personal data, without the data subject's prescribed consent, for purposes for which the data were to be used at the time of collection or DIRECTLY RELATED PURPOSES. It follows that, where the data user is a service provider, it may use a customer's personal data in connection with establishing, exercising or defending its legal rights on the basis that those purposes are directly related to provision of services by it to the customer.

(c) A similar exemption is available under common law with respect to the banker's duty of confidentiality regarding customer information.

Proposal No. 35: Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

Invitation of Comments:
Whether to create a new exemption for data users from complying with a data access request on the ground of self-incrimination.

Response:

(a) We support this Proposal.

(b) Under the existing PDPO, data users often find themselves in the unfortunate position where a data subject uses the relevant provisions as a tool of discovery. That goes beyond the objective and legislative intent of the PDPO which is protection of personal data privacy.

Proposal No. 41: Duty to Prevent Loss of Personal Data

Invitation of Comments:
Whether to amend DPP 4 in Schedule 1 to make it explicit that a data user is required to take all reasonably practicable steps to prevent the loss of personal data.

Response:

(a) It is not clear to us what is meant by "loss" of personal data for the purpose of this Proposal. Subject to clarification, we take the view that the existing regime offers sufficient protection and no change is required.

(b) More specifically:

(i) Any "loss" of personal data which results in access, disclosure or other use of data without the data subject's consent constitutes a breach of DPP 3 under the existing regime.

(ii) If the concern relates to "loss" of the device holding the personal data (e.g. a computer disc, USB or other device), the existing DPP 4 already requires a data user to take all reasonably practicable steps to ensure that personal data held by it are protected against unauthorized or accidental access or other use. If a data user complies with DPP 4 and the data holding device is installed with encryption or other safeguards which prevent access or use of data, loss of that device will not have any adverse effect on data subjects.

Proposal 43: Contact Information about the Individual Who Receives Data Access or Correction Requests

Invitation of Comments:

Whether to amend DPP 1(3) to permit a data user to provide either the job title or the name of the individual to whom data access or correction requests may be made.

Response:

We support this Proposal.

Additional Proposal (1): Investigation Period

There should be a time limit for the PCPD to conclude its investigation of any complaint or alleged contravention of the requirements of the PDPO by a data user, and issue its findings. In the absence of a time limit, the data user may encounter difficulty in properly defending its case due to lapse of time. In particular, difficulty may arise from departure of personnel or routine purging of related documents and materials. We also consider it reasonable for the PCPD to identify clearly the issues being investigated from the outset and keep the data user informed of the status of the investigation on a regular basis.

Additional Proposal (2): Use of Credit Data for Anti-Money Laundering (AML) Know Your Customer (KYC) Purposes

Under the current HKMA Guideline and Supplement on Prevention of Money Laundering, Authorised Institutions ("**AIs**"), including all our members, are required to verify the customer's identity (ID verification) using reliable, independent source documents, data or information. This will include both the personal customers and the relevant individuals of corporate customers, i.e. directors, principal shareholders, authorized signatories and beneficial owners of the corporate customers. It is also defined under the HKMA

guidelines that the identity of an individual includes the individual's name (including former or other name), residential address (and permanent address if different), date of birth and nationality.

Our members have encountered difficulties in obtaining reliable, independent source documents to verify the identity of the customers, especially in respect of the additional document to verify the current address and permanent address of the individuals. Furthermore, it is not uncommon nowadays for AIs to provide certain low AML risk products to the customers such as credit cards via non-face-to-face channels and under the HKMA Supplement, AIs are required to take specific measures to identify these customers, for examples, requisition of additional documents or obtaining a wide range of information capable of independent verification.

We are of the view that the Consumer Credit Data and Commercial Credit Data held by Credit Reference Agencies are reliable, independent source documents, data or information that can fulfill AIs' obligation on ID verification under the HKMA Guideline and Supplement. It is also noted that similar credit databases are opened to banks in other jurisdictions e.g. Australia for ID verification/AML KYC purpose. We therefore propose that AIs should be allowed to access data held at the Credit Reference Agencies for the purpose of conducting ID verification/AML KYC checks. Since amendment to the PDPO should not be required, we hope that the proposal will be accepted and implemented as soon as practicable to facilitate AIs in complying with the HKMA Guideline and Supplement.

If you have any further questions, please do not hesitate to contact us.

Yours faithfully,

(Signed)

Jennifer Cheung
Secretary

c.c. Hong Kong Monetary Authority (Chief Executive)



To '"pdpo_consultation@cmab.gov.hk"' <pdpo_consultation@cmab.gov.hk>
cc
bcc
23/11/2009 13:08 Subject 檢討《個人資料（私隱）條例》的公眾諮詢 建議

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

你好

請引入出生日期為私穩之一
現時的年齡歧視非常嚴重, 尤其尋找工作方面.
僱主多以養小朋友, 抱孫為由, 間接拒絕中年人仕之申請
這些中年人仕往往因而未能找到工作, 最後依靠社會福利繼續生存. 也成為社會眼中所謂的包伏
他們並非因為不肯工作, 也非殘缺, 他們還有能力工作, 甚至比年輕人更能幹
只因為年齡問題, 就比評為不能工作, 不適合申請培訓/職位.

如要證明該申請人是滿18歲的香港永久居民
身份證上的3粒星已經足夠吧

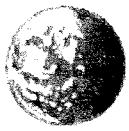
懇請貴 處可將出生日期/ 年份列入私穩之一

謝謝

Regards,

（ 署名來函 ）

（ 來信人要求不具名公開意見 ）



To "'pdpo_consultation@cmab.gov.hk'" <pdpo_consultation@cmab.gov.hk>
cc
bcc
23/11/2009 13:08 Subject 檢討《個人資料（私隱）條例》的公眾諮詢 建議

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啟

請引入出生日期為私穩之一
現時的年齡歧視非常嚴重, 尤其尋找工作方面.
僱主多以養小朋友, 抱孫為由, 間接拒絕中年人仕之申請
這些中年人仕往往因而未能找到工作, 最後依靠社會福利繼續生存. 也成為社會眼中所謂的包伏
他們並非因為不肯工作, 也非殘缺, 他們還有能力工作, 甚至比年輕人更能幹
只因為年齡問題, 就比評為不能工作, 不適合申請培訓/職位.

如要證明該申請人是滿18歲的香港永久居民
身份證上的3粒星已經足夠吧

懇請貴 處可將出生日期/ 年份列入私穩之一

謝謝

Regards,

（ 署名來函 ）

（ 來信人要求不具名公開意見 ）

香港珠寶製造業廠商會
Hong Kong Jewelry Manufacturers' Association

S0071

致：香港下亞厘畢道
中區政府合署東座 364 室
政制及內地事務局（第 4 組）

副秘書長何健華先生

尊敬的何健華副秘書長：

有關：回應《個人資料（私隱）條例》修訂重點

承蒙　何副秘書長撥冗親臨本會扼要地闡述關於《個人資料（私隱）條例》修訂重點的公眾諮詢，使本商會及部分會員能及時了解有關修訂事宜，不勝感激。

查閱有關《個人資料（私隱）條例》擬修訂的概要後，有感當中不少條文對本商會運作和珠寶業界營運息息相關，故特此來函反映初步意見，希望 貴局審慎考慮：

一．就敏感個人資料而言，鑑於現時並沒有一套國際公認的敏感個人資料規範，在缺乏標準的情況下，要釐訂一套區別敏感與非敏感個人資料的方案，未免有操之過急之嫌。本會認同需考慮規管敏感個人資料，但既然國際上亦暫時沒有清晰的界定方法，本港亦毋須急於釐訂區別敏感資料的方案。

二．在「資料保安」中「規管資料處理者及分判活動」方面，由於珠寶製造業者經常參與不同展覽和業務洽談活動，當中不乏行業間互相交換意見，商會認爲行業的現況和個別從業員認知的水平，目前尚未達到相當謹慎的程度，貿然修訂從嚴並不合符行業實際的環境，故在規管方面宜因應行業的特殊情況作彈性處理。

三．就「個人資料外洩通報機制」發出的指引，本會憂慮通報程序的複雜性及增加成本，盼 貴局能注意通報機制所牽涉的資源，特別是中小企的行政運作能力，以免帶來沉重的財務負擔。

四．至於「私隱專員的執法權力」方面，本會認爲現行由警方進行刑事調查，律政司負責檢控的機制運作暢順，並無充分理由賦予私隱專員進行刑事調查及提出檢控的權力，私隱專員亦無必要向受屈資料當事人提供法律協助。

五．關於私隱條例建議修訂之「罪行與制裁」，本會並不支持把違反保障資料原則訂爲罪行。我們重申非常尊重個人私隱，但採用一刀切式刑事化，未免過於嚴苛，偏離了私隱條例提供保障資料的原意，有必要審慎客觀地評估目前社會現狀，特別是公眾對法例認知的充足程度，以維護社會各界的平衡關係。

六．就應否向嚴重違反保障資料原則的資料使用者處以罰款，由於目前鮮有司法機構以外的機構獲賦予法定權力施加罰款，加上一種行爲是否嚴重違反保障資料原則純屬主觀判斷，授予私隱專員判處罰款的權力實有欠客觀性。

最後，本會認爲諮詢期訂於 11 月 30 日結束未免太倉猝，鑑於私隱條例對工商界的影響深遠，務請 貴局考慮延長諮詢期，好讓各界有較充分的時間深入理解，集思廣益，共謀一套既能滿足社會公眾利益、符合時代改變，又可提高專重個人私隱的全盤修訂方案。

敬頌鈞安

香港珠寶製造業廠商會

（ 已簽署 ）

總經理　張士昆 謹啓
2009 年 11 月 18 日

地 產 代 理 監 管 局
ESTATE AGENTS AUTHORITY

S0072

Your Ref: CMAB/CR/7/22/40 pt.7
Our Ref: EAA/DRA

17 November 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong
(Attn: Miss Joanna C.H. Choi)

Dear Miss Choi,

Public Consultation on
the Review of the Personal Data (Privacy) Ordinance

Thank you for your letter dated 28 August 2009 enclosing a copy of the "Consultation Document on Review of the Personal Data (Privacy) Ordinance".

The Licensing and Practice Committee of the Estate Agents Authority ("EAA") has considered the proposals set out in the Consultation Document and the views of the EAA on those proposals which have implications for the estate agency trade are set out below:

(a) *Regulation of Data Processors* (paragraphs 4.01 – 4.21 of the Consultation Document)

As in other professions or trades, estate agencies may outsource and entrust personal data processing work to third parties. The handling of personal data in electronic form increases the privacy risks to which such data are exposed. Any mishandling may lead to far-reaching damage to the affected data subjects. The EAA is of the view that a data user should be required to use contractual or other means to ensure compliance with relevant Personal Data (Privacy) Ordinance ("PDPO") obligations when contracting out the processing of personal data to third parties.

The EAA supports the proposal of directly regulating the activities of a data processor under the PDPO. It is considered that this would further enhance the protection of data subjects. The proposal is beneficial to the estate agency trade because without direct regulation

on data processors under the law, an estate agency as a data user may be held fully liable for the wrongdoings of data processors and also sub-contractors with whom it has no direct contractual relations.

(b) *Personal Data Security Breach Notification* (paragraphs 4.22 – 4.43 of the Consultation Document)

The EAA supports the proposal of instituting a voluntary breach notification system. The EAA is of the view that the estate agency trade should take the responsibility in an incident of personal data leakage. Thus, if the voluntary breach notification system is proven effective, it should be replaced by a mandatory one in future.

The EAA is also of the view that the proposal should clarify under what circumstances a leakage of personal data would be subject to notification. The extent of the data breach triggering notification should also be clearly stated.

(c) *Making Contravention of a DPP an offence* (Paragraphs 6.03 – 6.05 of the Consultation Document)

The EAA does not support the proposal to make the contravention of a Data Protection Principle ("DPP") an offence. Such a proposal would have significant impact on the estate agency trade.

(d) *Imposing Monetary Penalty on Serious Contravention of DPP* (paragraphs 6.17 – 6.21 of the Consultation Document)

The EAA supports the proposal to empower the Privacy Commissioner for Personal Data to impose monetary penalty for serious contraventions of DPPs, in order to deter serious contravention of DPPs.

(e) *Making Unauthorised Obtaining, Disclosure and Sale of Personal Data an offence* (paragraphs 6.06 – 6.12 of the Consultation Document)

Occasionally, the EAA receives complaints on unauthorized transfer of client's information to other estate agencies. Such incidents may involve gaining unauthorized access to, and collection of, customers' personal data by the staff of an estate agency for sale to third parties.

To deter cases of unlawful transfer of client's information and in view of the seriousness of the intrusion into personal data privacy and the gravity of the harm that may cause to the data subject as a result of the intentional or willful act of the person in flagrant disregard of the

personal data privacy of others, the EAA takes the view that the Government should make it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes.

(f) *Raising the Penalty for the Misuse of Personal Data in Direct Marketing* (paragraphs 6.26 – 6.31 of the Consultation Document)

The number of complaints on estate agents making direct marketing calls to consumers received by the EAA is not significant. Such direct marketing calls rarely bring about serious damage to the personal data privacy of the data subject concerned. The EAA is of the view that it may not be appropriate to raise the existing level of fine.

Should you have any question on the above, please do not hesitate to contact Ms Eva Lau, Director of Regulatory Affairs and General Counsel on .

Yours sincerely,

(Signed)

(Ms Eva Lau)
for Chief Executive Officer
Estate Agents Authority

c.c. Mr. Eugene Fung, Principal Assistant Secretary for Housing, Transport & Housing Bureau

Internal

Chairman, EAA
Chairman, Licensing & Practice Committee, EAA
CEO, EAA



25/11/2009 15:10

To '"pdpo_consultation@cmab.gov.hk"' <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Public Consultation on the Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Miss Choi,

Please find attached a reply letter with submissions from Ms. Joyce Wong of the Law Society of Hong Kong, the contents of which are self-explanatory.

Kind regards,
Lillian Chau
secretary to Ms. Joyce Wong



The Law Society of Hong Kong submissions on Review of the PDPO.pdf

THE LAW SOCIETY OF HONG KONG
香港律師會

Practitioners Affairs

Our Ref :
Your Ref :
Direct Line : CMAB/CR/7/22/40 Pt.7

President
會長
Huen Wong
王桂壎

Vice-Presidents
副會長
Junius K.Y. Ho
何君堯
Dieter Yih
葉禮德

Council Members
理事
Lester G. Huang
黃嘉純
Peter C.L. Lo
羅志力
Michael J. Lintern-Smith
史密夫
Ip Shing Hing
葉成慶
Billy W.Y. Ma
馬華潤
Sylvia W.Y. Siu
蕭詠儀
Cecilia K.W. Wong
黃吳潔華
Alex T.H. Lai
黎庭康
Kenneth S.Y. Ng
吳業
...phen W.S. Hung
熊運信
Ambrose S.K. Lam
林新強
Joseph C.W. Li
李超華
Amirali B. Nasir
黎雅明
Melissa K. Pang
彭韻僖
Thomas S.T. So
蘇紹聰
Angela W.Y. Lee
李慧賢
Brian W. Gilchrist
喬柏仁

Secretary General
秘書長
Raymond C.K. Ho
何志強

Deputy Secretary General
副秘書長
Heidi K.P. Chu
朱潔冰

25 November 2009

Miss Joanna C.H. Choi
for Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road, Hong Kong

Dear Miss Choi,

Re: Public Consultation on the Review of the Personal Data (Privacy) Ordinance ("PDPO")

I refer to our letter dated 3 September 2009 and attach the Law Society's comments on the Review of the PDPO for consideration by the Bureau and the Privacy Commissioner.

Yours sincerely,

(Signed)

Joyce Wong
Director of Practitioners Affairs

Encl.

THE LAW SOCIETY OF HONG KONG 香港律師會

Comments on Consultation Paper on "Review of the Personal Data (Privacy) Ordinance ("PDPO")"

The Law Society makes the following comments on the Proposals in the Consultation Paper:

Proposal No.1: Sensitive Personal Data

As the size of each organization and complexity for handling data access request in each case is different, it would be impractical to research into organizations / cases in order to determine an average or a reasonable administrative cost to be charged. We suggest that the administrative fee shall be absorbed into the non-refundable processing fee of HK$50.00 payable upon lodgment of a data access request, as suggested by the Commissioner, in addition to the fees chargeable under the proposed fees schedule.

It is also agreed that that the handling of sensitive personal data should only be permitted in the specific circumstances set out in paragraph 3.09 of the Consultation Paper. However, the exemptions should be amended as follows:

3.09 The collection, holding, processing and use ("handling") of sensitive personal data would be prohibited except in the following circumstances:

(a) the prescribed consent (i.e. express consent given voluntarily) of the data subject or a person authorised to act on the data subject's behalf has been obtained;

(b) it is reasonably necessary for the data user to handle the data to exercise his right as conferred by law or perform his obligation as imposed by law;

(c) handling of the data is necessary for protecting the interests of the data subject or others where prescribed consent of the data subject cannot be reasonably obtained in a timely manner;

(d) handling of the data is in the course of the data user's lawful function and activities with appropriate safeguard against transfer or disclosure to third parties without prescribed consent of the data subject;

(e) the data has been made public by the data subject or through other lawful means;

(f) handling of the data is reasonably necessary for medical purposes and is undertaken by a health professional or other person who in the circumstances

owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional; or

(g) handling of the data is reasonably necessary in connection with any legal proceedings.

We do not agree that a higher level of fine should be applicable for the contravention of these requirements. The existing sanctions are, in our view, adequate. It is not necessary that non-compliance with the DPPs should be considered an offence as this may have the consequence of making the regulatory regime too restrictive for businesses to carry out their normal functions without risking inadvertent breaches. In addition, such a step would increase the difficulty of establishing that an actionable breach has occurred.

It should be made clear that a data user should not be sanctioned for breach by a person to whom data processing etc. has been properly outsourced. Liability in such situations should be an unreasonable burden for businesses to assume in an international centre such as Hong Kong where offshore outsourcing is necessary in order to keep operational costs at internationally competitive levels.

Transitional arrangements should be implemented such that data handlers are given a certain period during which sensitive personal data is exempt from the new requirements, so that they may have time to adapt to the new regime. Given the extent to which data processing is outsourced, the transitional period should be at least 12 months. It is possible that a longer period may be necessary. Once this period is over all sensitive data must be processed in line with the new requirements. This is considered a preferable arrangement to grandfathering as it avoids the issue of sensitive personal data being processed differently depending on whether it was collected before or after these provisions come into force.

Proposal No.2: Regulation of Data Processors and Sub-contracting Activities

We agree there is a need for regulation of third party data processors given the rise in outsourcing data processing. However, imposing direct regulation upon the third party data processor is not a viable solution. Especially in light of the prevalence of overseas outsourcing (which is the norm for Hong Kong), it would be extremely difficult, if not impossible, to enforce these standards.

It is also hopelessly unrealistic to expect to be able to enforce either the PDPO or commercial contracts in all (or, in some cases, any) circumstances in the jurisdictions to which data is typically outsourced and it would place Hong Kong businesses at a competitive disadvantage if regulations were to make it impossible, impracticable or overly expensive to outsource to such countries.

It is also considered too burdensome and inflexible, given the difficulty in defining the purpose for which data is collected. Instead, the regulations should be imposed indirectly, via the data user. This approach is more in line with common international practice.

The regulations should impose an obligation on the data user to use contractual means to require the data processor and any other sub-contractors take all practicable steps to ensure the security and safekeeping of the data, to ensure the data is not misused and to delete it once it is no longer required. Contravention of this requirement would warrant enforcement

action by the PCPD, including serving an enforcement notice against the data processor. However, it is unrealistic to expect the data user to be responsible for breaches by the data processor or to have to take enforcement action at its own costs in most circumstances – the costs would be generally disproportionate to the benefits obtained (if any). This is a practicable solution as the flexibility of outsourcing data processing to third parties is retained whilst the organisation against whom an aggrieved data subject may claim redress is still the identifiable data user to whom they provided their personal data.

The blunt reality is that unless data users are able to outsource data processing etc offshore without being subject to unduly onerous restrictions or being held accountable for breaches by the data processors or subject to burdensome and expensive regulatory requirements, Hong Kong businesses will be placed at a competitive disadvantage. Accordingly, data subjects will continue to be exposed to certain risks (as at present) and appropriate risk disclosure to the effect that outsourcing/offshore transfer involves greater risk of unauthorised use or disclosure of personal data and that remedies may be limited should be provided.

Proposal No.3: Personal Data Security Breach Notification

We agree that given the widespread and increasing use of information, data users should be subject to a mandatory obligation to notify the data subjects concerned and the PCPD after becoming aware of a breach of data security which leads to the leakage or loss of personal data. This is necessary to mitigate the potential damage, including identity theft, which could result from such leakage or loss. Notification should be made as soon as possible so that data subjects may take steps to minimise potential damage. It is also important that the PCPD is notified in order to keep records up to date, to monitor organisation practices and to allow guidelines to be drawn up.

It is recommended that a system of notification should be introduced initially by voluntary guidelines issued by the PCPD. This is important in order to balance the need for notification with the costs that will be involved for businesses. These voluntary guidelines should be applicable to all industry sectors and should override any industry policies already in place to ensure a consistent approach. We note that most data users will have contact details for relevant data subjects (e.g. banks, phone companies, ISPs, insurance companies and most other businesses) and so it such not be too difficult to notify all affected data subjects of a breach. We consider the numerical approach toward notification is unnecessary.

The timing of these notifications should be as soon as possible following the breach or suspected breach, except where a delay is required by law enforcement agents. Notifications should be made individually in writing up to a certain number of data subjects but should then be made publicly, for example in a national newspaper, where the number of data subjects affected is above that threshold, e.g. 50, when it would no longer be practicable to notify each person individually. It is agreed that the notifications should include the content set out in paragraph 4.30 of the Consultation Paper. Finally it is recommended that no penalty be applied while the notification system is introduced on a voluntary guidelines basis but that once these guidelines are fine-tuned and the policy is finalised then an appropriate fine for contravention of such requirements should be implemented.

Proposal No.4: Granting Criminal Investigation and Prosecution Power to the PCPD

The question of whether the powers of criminal investigation should be granted to the PCPD will depend largely on whether some or all the offences set out in the proposals of this consultation document ultimately become law. If so, the nature of such offences are such that they are probably more suited to being investigated by the PCPD with attendant criminal investigation powers granted to it. However, if none of these offences become law, then there is no proper basis for granting the PCPD such powers for pre-existing offences with a privacy angle.

As for prosecution powers, it is not clear in the case of data privacy offences why there is a need for the PCPD to have such powers when the Department of Justice would likely be in a better position to make prosecution decisions based on wider considerations of public interest.

Proposal No.5: Legal Assistance to Data Subjects under Section 66

We agree.

Proposal No.6: Award Compensation to Aggrieved Data subjects

We agree, subject to the fact that any compensation notices are not automatically enforceable as if they were court orders, so that the PCPD would not be considered as seeking to exercise judicial power. Instead, they are treated as indicative compensation figures that are subject to being upheld and enforced by a court (with the PCPD being given statutory standing to make the necessary applications to uphold such notices) if the parties do not agree to their terms.

Care should be taken not to intake an element of punitive damages. However, we note the proposals in the latest consultation in England and Wales on breaches of the Data Protection Act[1]

---

[1] The Government has published its long awaited proposals on fines for serious breaches of the Data Protection Act 1998. The proposal is for a maximum fine of £500,000, with discretion for the information Commissioner's Office to assess the actual level of fines imposed on a case by case basis. The consultation period ends on 21 December, and the new fines could come into force as soon as April 2010.

The proposals are set out in consultation paper published on 9 November entitled "Civil monetary penalties: setting the maximum penalty".

The penalties will significantly boost the Information Commissioner's (currently very limited) enforcement powers. They are being introduced response to the seemingly endless tide of serious security breaches, which began to come to light almost two years ago with the HMRC debacle.

The new powers are to be found in the recently added section 55A of the DPA (introduced by section 144 of the CJIA 2008) and will apply to serious breaches of the Act which are likely to cause substantial damage or distress, and which are committed deliberately or recklessly.

The new provisions received Royal Assent in May 2008. However, the sanction is still not "live", as the amount of the penalties will need to be set by statutory instrument.

The MoJ has dropped the idea of fines based on a percentage of turnover model, similar to that used by other regulators, in favour of a fixed maximum fine which the ICO can then assess according to the seriousness of the breach and the resources of the data controller in question.

Proposal No.7: Making Contravention of a DPP an offence

Only deliberate breaches should be made an offence. Inadvertent breaches (including breaches resulting from recklessness or negligence) should not be an offence.

Proposal No.8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

We agree with the proposal provided that "obtain" is defined as such a way to mean obtained as a result of an act intended to obtain the personal data. Unsolicited or inadvertent receipt of personal data should not be included.

Proposal No.9: Repeated Contravention of a DPP on Same Facts

We agree with the proposal.

Proposal No.10: Imposing Monetary Penalty on Serious Contravention of DPPs

We disagree. The offensive mechanism in Proposal No 7 is sufficient.

Proposal No.11: Repeated Non-compliance with Enforcement Notice

We agree with the Proposal.

Proposed No.12: Raising Penalty for Misuse of Personal Data in Direct Marketing

We agree with raising the penalty for deliberate misuses of personal data (e.g. a fine at level 5). The enforcement of opt out/do not call regulators should be given greater priority.

Proposal No.13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

(a) We agree to impose the proposed conditions to allow third parties to give prescribed consent on behalf of a data subject. We suggest the PCPD consider issuing a code of practice or guidelines to guide data user on the necessary enquires required to be made before the data user could form a reasonable belief that the conditions are fulfilled, and to advise on the possible liabilities for failing to make necessary enquires leading to contravention of the PDPO. Please also consider the balance between protection of vulnerable classes of data subjects and business/organization interests as the code of practice should not impose excessive liabilities on business/organization or affect their normal operation.

(b) We agree to expand the definition of relevant person to include the guardians of data subjects whom meet the conditions specified under this Proposal.

The consultation document poses a single question, namely whether the fine of up to £500,000 provides the ICO with a "proportionate sanction" for serious DPA contraventions. The cap seems modest when compared with fines imposed by the FSA for data breaches in the financial services sector.

The MoJ and the ICO have both indicated that the plan is for the new fines to go live in April next year.

Proposal No.14: Parents' Right to Access Personal Data of Minors

(a) and (b) Inevitably there will be a judgement call when a data user decides what would constitute reasonable grounds in order to comply with a request by a relevant person on behalf of a minor. We are of the view that such power conferred to data users shall not be a statutory right. There would be more flexibility if comment is provided in the data user's code of practice or in guidelines issued by the PCPD which would have the benefit of avoiding ambiguity. The PCPD could therefore consider issuing guidelines.

Proposal No.15: Access to Personal Data in Dispute

We agree that when access to personal data is in dispute, the relevant personal data should not be disclosed to the data requestor and other parties whom would be bound by the outcome of the decision of AAB, the court or a magistrate.

Proposal No.16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We agree with the proposed amendment to the PDPO to allow a data user to refuse a data access request on grounds of compliance with secrecy requirements under other legislation.

Proposal No.17: Erasure of Personal Data

We agree with this proposal subject to clear guidelines being issued by the to be taken to meet the requirements of reasonable practicable steps to erase personal data.

Proposal No.18: Fee Charging for Handling Data Access Requests

As the size of each organization in each case is different, it would be impractical to research into organizations / cases in order to determine an average or a reasonable administrative cost to be charged. We suggest the administrative fee shall be absorbed into the non-refundable processing fee of HK$50.00 payable upon lodgment of a data access request, as suggested by the Commissioner, in addition to the fees chargeable under the proposed fees schedule.

Proposal No.19: Response to Data Access Requests in Writing and Within 40 days

(a) We agree.

(b) We agree.

Proposal No.20: Circumstances for Issue of an Enforcement Notice

We agree.

Proposal No.21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

We agree.

Proposal No.22: Removing the Time Limit to Discontinue an Investigation

We agree.

Proposal No.23: Additional Grounds for Refusing to Investigate

We agree.

Proposal No.24: Transfer of Personal Data in Business Mergers or Acquisition

We agree the transfer of personal data in mergers or acquisitions, or proposed mergers and acquisitions, is necessary to facilitate business and to promote Hong Kong as a centre for business. Therefore the conditions mentioned at paragraph 52 of the Consultation Paper should all be included.

Proposal No.25: Provision of Identity and Location Data on Health Grounds

We agreed the benefits of including location and identity of the data subject within this exemption would outweigh the risks that such inclusion may present to their data protection. Provided that the disclosure is restricted by certain conditions such as the threat of serious harm and the exemption is limited to being applied only for the purpose of lessening the risk of serious harm then sufficient protection of personal data would still be in place.

For the avoidance of doubt, neither this exemption nor any other provision of the PDPO should be used to disclose to the public (or any section of the public) the identities and addresses of persons who have been convicted of criminal offences. Such action typically makes it impossible for such persons to reintegrate with society.

Proposal No.26: Handling Personal Data in Emergency Situations

We agree that DPP 1(3) and DPP3 should not apply in cases of emergency or catastrophe but this exemption must only be employed for the purposes of lessening the threat or harm from such emergency or catastrophe. In other words, an emergency or catastrophe will not trigger a total disapplication of these principles for all users and processors for any purpose. Therefore it is important the drafting adequately limits the exemption by purpose and duration.

Proposal No.27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

We agree this exemption to DPP3 should be introduced for the purpose of protecting vulnerable minors and others who may be at risk. In order to ensure the personal data of minors is still adequately protected, the language should retain the need for input from the police or other authorities, although the threshold should be much lower than the previous "concrete proof": a reasonable basis for suspension should be sufficient.

Further, the condition that such disclosure should only be permitted if it is in the best interests of the minor should not be incorporated – such a provision will only add an unnecessary element of subjective uncertainty.

Proposal No.28: Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result

- **To relieve the PCPD's obligation to notify the complainant of the investigation result and related matters under Section 47(3) when the complainant has withdrawn his complaint.**

We agree.

Proposal No.29: PCPD to Disclose Information in the Performance of Functions

- **To amend Section 46 to allow the PCPD and his prescribed officers to disclose information reasonably necessary for the proper performance of his functions and exercise of his powers.**

We agree provided that, like corresponding provisions in legislation governing statutory bodies such as the Securities and Futures Commission and the Equal Opportunities Commission, the situations under which disclosure under this proposed ground may be made should be enumerated. Further, personal data may be disclosed to overseas data protection authorities to facilitate cross-border cooperation in the enforcement of personal data privacy rights only if the act being investigated by the overseas data protection authorities will constitute a violation of the DPPs or an offence under the PDPO if committed in Hong Kong.

Proposal No.30: Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit

- **To protect the PPCPD and his prescribed officers from being held personally liable for any act done or omission made in good faith in the exercise or purported exercise of PCPD's functions and powers under the PDPO.**

We agree.

Proposal No.31: Power to Impose Charges for Educational and Promotional Activities

- **To provide the PCPD with an express power to impose reasonable charges for undertaking educational or promotional activities or services.**

We agree provided that the charges are for covering expenses and reasonable time charge and not for profit, since PCPD is exempt from taxation.

Proposal No.32: Power to Obtain Information to Verify a Data User Return

- **To confer upon the PCPD the power to obtain information from any person in order to verify the information in a data user return filed under Section 14.**

We agree in principle, provided that it is clearly indicated in the legislation that for the purpose of verifying the information in a data user return, PCPD is exercising a general inspection power comparable to inspection powers under Section 36, rather than investigation powers under Section 38, which should only be invoked when complaints are received.

Proposal No.33: Use of Personal Data Required or Authorized by Law or Related to legal Proceedings

- **To create an exemption from DPP 3 for use of personal data required or authorized by or under law, by court orders, or related to any legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights.**

We agree that furthering legal rights is a legitimate exception to DPP3.

Proposal No.34: Transfer of Records for Archival Purpose

- **To create an exemption from DPP3 for the transfer of information containing personal data of historical, research, educational or cultural interests to the Government Records Service ("GRS") for archival purpose.**

The proposed exemption should extend only to materials already in the public domain.

Personal data collected by Government bureaux and departments which are not in the public domain should not be transferred to the GRS because:-

- It is contrary to the spirit of the PDPO for personal data to be used without consent of the data subject;

- The records kept in the GRS archive are, subject to a few exceptions, accessible to the public. Although it is proposed that after transferring the archival records to GRS, the subsequent handling of the archival records containing personal data (including access to and use of records by members of the public) will continue to be subject to the provisions of the PDPO, in the Code of Access to Information published by GRS it is provided that information about a person may be disclosed where the "public interest in disclosure outweighs any harm or prejudice that would result". There is concern that, while the PDPO does not empower the Government to make disclosure of personal data under "public interest", transferring the data to GRS will leave a door open for personal data to be disclosed to the public, without the data subject's consent, by the Government using "public interest" as a reason. The concern is aggravated by the fact that there is no mechanism under the Code of Access to Information for determination of whether or not public interest in disclosure outweighs any harm or prejudice that would result from disclosure of the personal data.

- Currently when government departments collect personal data, the stated purposes are usually limited in scope, and there is no sharing of personal data between government departments. There is concern that by allowing transfer

of personal data to GRS, data about a person can be aggregated at the GRS, contrary to the understanding of the data subjects when they first provided their personal data to the government departments.

Personal data not in the public domain has no historical, research, educational or cultural value and should not be transferred to the GRS without the data subject's consent.

Proposal No.35: Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

We agree that such an exemption should be introduced. However, it should not be applicable where the request is made by a data subject who should only be permitted to access their own personal data. A data subject's right to access his own personal data should not be conditional upon whether granting such a request would incriminate the user. The principle of privilege against self-incrimination should apply to general data access requests only.

Proposal No.36: Definition of Crime under Section 58

- **To clarify the scope of application of the exemption provision under Section 58 by defining "crime" to mean a crime under Hong Kong law, or a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation.**

We agree.

Proposal No.37: Expand the Definition of "Relevant Person"

- **To expand the definition of "relevant person" under Section 2 to include the guardian of data subjects with mental incapacity, who are appointed under Sections 44A, 59O, 59Q of the Mental health Ordinance (Cap.136).**

We agree.

Proposal No.38: Exclude Social Services from the Definition of "Direct Marketing"

- **To amend Section 34 to exclude from the definition of "direct marketing" the offering of social services and facilities by social workers to individuals in need of such services and facilities.**

We agree provided that a suitable definition of "social services" is added to Section 2 of the PDPO.

Proposal No.39: Exemption for Personal Data Held by the Court or Judicial Officer

- **To add a new provision so that the PDPO shall not apply to personal data held by the court or judicial officer in the course of the exercise of judicial functions.**

All the Exemptions contained in the PDPO are either very specific (stating which Section of the ordinance or which DPP is not to apply in what situation) or very limited in scope. This is so even for very serious issues such as safeguarding the security of Hong Kong. If a full scale exemption to the PDPO is to be given to the court or judicial officers, we expect to see more explanation or justification in the Consultation Document. Furthermore, some provisions in the PDPO should apply to all data users (such as DPP4 – security of personal data) and has nothing to do with judicial independence and immunity.

Absent appropriate justification, the Law Society objects to the proposed full scale exemption of the PDPO to the court or judicial officers.

Proposal No.40: Extend Time Limit for Laying Information for Prosecution

- **To specify that the time limit for laying information for prosecution of an offence under the PDPO shall be two years from the date of commission of the offence.**

The reasons given in the Consultation Document in support of Proposal No. 40 apply to all offences and there is no justification why the time limit should be increased from 6 months to 2 years. If from past experience of the PCPD has difficulty laying information for prosecution within the 6-month time limit, we suggest that the time limit be extended to one year rather than two years. There should be a balance between convenience to the PCPD and the anxiety to the party being investigated.

Given that breach of the PDPO may not be disclosed until some time after the event, the time period should run from when the PCDP becomes aware of the offence.

Proposal No.41: Duty to Prevent Loss of Personal Data

- **To amend DPP 4 in Schedule 1 to make it explicit that a data user is required to take all reasonably practicable steps to prevent the loss of personal data.**

We agree. Please see responses to Proposals No. 1 and 2 above for issues relating to outsourcing. Specifically, taking legal action should not be required given the expensive and, in many jurisdictions, the futility of taking such action.

Proposal No.42: PCPD to Serve an Enforcement Notice together with the Results of Investigation

- **To amend Section 47 to allow the PCPD to serve an enforcement notice together with the results of investigation upon the relevant data user.**

We agree.

Proposal No.43: Contact Information about the Individual Who Receives Data Access or Correction Requests

- **To amend DPP 1(3) to permit a data user to provide either the job title or the name of the individual to whom data access or correction requests may be made.**

We agree.

The Law Society of Hong Kong
24 November 2009

129061v5

檢討
《個人資料(私隱)條例》
公眾諮詢

重點

我的意見

（已簽署）

十一月 2009

二零零九年八月

引言

《個人資料(私隱)條例》("私隱條例")在1996年生效。政制及內地事務局在個人資料私隱專員("私隱專員")的協助下，就私隱條例進行了全面的檢討，研究隨着過去十年的發展，包括科技的進步，私隱條例的現有條文是否仍足以保障個人資料。

指導原則

在進行檢討時，我們以下述原則為依據：

- 個人的私隱權不是絕對的，必須與其他權利以及某些公眾及社會利益取得平衡；
- 需要在保障個人資料私隱與便利資訊及通訊科技持續發展之間取得平衡；
- 對私隱法例作出的任何修改，都不應削弱香港作為國際城市的競爭力和經濟效率；
- 需要避免商業活動和個別資料使用者承受沉重的負擔；
- 應充分考慮本地的情況；
- 私隱條例在科技轉變中應仍具彈性並且合時；
- 立法干預未必一定是最有效方法。在某些情況下，推行行政措施可達到保障個人資料私隱的效果；
- 社會對私隱課題有相當程度的共識至為重要。

我們就私隱條例提出了多項修訂建議，有關修訂或會對社會各界、公營部門、私營機構和市民有深遠影響。對於這些建議，我們持開放態度，歡迎市民就此提出意見。

主要建議

敏感個人資料

- 敏感個人資料(如指紋)應否受更嚴格的規管？

否

資料保安

- 應否規管受託處理個人資料的資料處理者？

否

- 應否規定資料使用者在發生個人資料外洩事故時通知私隱專員及受影響的人士？

私隱專員的權力

- 應否賦予私隱專員刑事調查和檢控的權力？
- 若有資料當事人因資料使用者違反私隱條例的規定而蒙受損失並有意向資料使用者提出法律訴訟，應否授權私隱專員為受屈的資料當事人提供法律協助？

S0074

- 應否授權私隱專員向受屈的資料當事人判給補償？

罪行及制裁

- 應否把違反保障資料原則訂為罪行？
- 應否把披露未經資料使用者同意下取得的個人資料而從中取利或作惡意用途的行為訂為罪行？
- 應否把資料使用者已遵行私隱專員發出的執行通知的規定，但不久又故意重犯的行為訂為罪行？
- 應否授權私隱專員就嚴重違反保障資料原則的行為施加罰款？
- 應否將屢次違反執行通知的行為處以更重的懲罰？
- 應否提高在直接促銷活動中不當使用個人資料的罰則？

資料當事人的權利

- 應否授權第三者就更改未成年人或精神上無行為能力的人的個人資料用途給予同意？
- 如資料使用者依從父母代其未成年子女提出的查閱資料要求並不符合子女的最佳利益，我們應否准許資料使用者拒絕該查閱要求？

豁免遵從私隱條例

- 應否向執法機關以及救援和支援機構給予豁免，以在緊急情況下處理個人資料？
- 如未成年人的個人資料與家長或監護人履行照顧和監護責任有關，我們應否准許資料使用者把該等資料轉移給未成年人的父母或監護人？

你的意見

諮詢文件可從各區民政事務處索取或從本局的網頁下載（網址：www.cmab.gov.hk）。請在**2009年11月30日或之前**，以郵寄、傳真或電郵方式提交意見或建議：

（未能確定來信人是否願意公開姓名）

S0074

S0075

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

S0076

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

S0077

致政制及內地事務局局長:

有關對於個人資料(私隱)條例的規定檢討咨詢文件

本人於2008年12月透過推廣活動，成功申請(刪除)銀行(下稱「銀行」)信用卡。在2009年約6-7月間，從本人之手機接獲一則推廣來電，本人感到驚訝是他們全面知道本人相關資料(例如:全名、身份證號碼及手機號碼)，聲稱是銀行附屬公司，因爲本人是幸運兒，如果不參與是本人之損失。其後，本人質疑該位職員不太專業時，他才和盤托出，稱有關資料是由銀行給予，後知是(刪除)保險公司((刪除))推銷保險，完全與銀行沒有關連。

後向銀行查詢得知，原先所申請信用卡之表格內一欄(即第5.ix)，本人所簽署已自動同意受權銀行(有機會)將個人資料交給相關之挑選公司(即第三者)；其目的是通知客戶銀行相信對客戶有利的服務，現提問? 如何「相信」及可謂「有利的服務」，這不外乎是保險推銷手段。過往各大發卡銀行會作擬辦內部推廣活動，本人不反對銀行業用此途徑尋找商機，但銀行利用了自己客人們對其之信任，沒有加以防禦下，作出違反誠信之行爲。

其職員們回覆時，聲稱此乃其本人之全部責任，本人應該清楚、明白及知道一切條款細則下才簽名。是否雷曼一事，不是一個大教訓嗎? 推廣員良莠不齊，有些還是外判公司聘請之短期員工，只要求有客人光顧，沒有清清楚楚——詳細說明有關條款及細則，是否凡事有涉及什麼條例的規定，全面需要錄音及見證人，雙方清楚明白後，才可立約，最方便有律師陪同，否則不可胡亂簽署。這個問題銀行間接稱本人愚昧，要有什麼充足證據支持本人之申訴，並分別在2009年8月至10月期間，覆函解釋此事 (附件共四份)。

本人受此侮辱的教訓下，如何尋找一些資產保障，是否無知或貪婪而種下禍根，本人只是一介草民，只是想申請一張電子貨幣的信用卡，方便作一般消費，何來無故要生事端。

現本人懇請局長閣下能就因此個案，不知是否有犧牲者發現情況下，更改現行之個人資料(私隱)條例的規定，免有些不法份子，從中取利，試問若無利可圖，那麼有慷慨的商人嗎?

祝 工作愉快!

不平人
(已簽署)
蘇綺華小姐

2009年11月25日

(編者註：已刪除意見書中涉及來信人的個別個案的詳細資料及附件)

S0078

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

香港基督教服務處
HONG KONG CHRISTIAN SERVICE
全人關心 卓越創新
care for all excel in all

香港
香港下亞厘畢道
中區政府合署東座 364 室
政制及內地事務局（第 4 組）

執事先生:

香港基督教服務處
對「檢討《個人資料（私隱）條例》的諮詢文件」的意見

香港基督教服務處（下簡稱「本處」）的服務單位遍佈港、九、新界及離島，共有50多種服務及70多個單位，包括長者社區服務、安老院舍、綜合家居照顧服務、青少年綜合服務、外展隊、駐學校社工、綜合家庭服務中心、寄養服務、兒童之家、弱能人士服務、社區發展服務、戒藥服務、診所、幼兒教育、青年及成人職業訓練課程、少數族裔服務、僱員支援服務、長者課程、內地社會服務事工、影音製作、度假中心及多項特別計畫，全年接受服務總人次超過100萬。在服務提供的過程中，我們每天都需要收取及處理大量的個人資料。因此，我們希望在這裡表達一下對「檢討《個人資料（私隱）條例》的諮詢文件」的一些意見。

1. 本處同意諮詢文件建議在新的條文中，准許資料使用者拒絕一位代表一名未成年人的 "有關人士" 提出的查閱資料要求，以保障未成年人的利益（附件 1，建議 14）。在本處過去的前線社會服務經驗中，我們偶爾會遇到未成年的服務使用者的父母提出的查閱資料要求。爲保障服務使用者的利益，我們均會以服務使用者的意願及福祉爲首要的考慮因素，決定是否把資料提供給有關人士。但是，以上的原則均建基於社工專業的手則，因此如政府能清晰加入有關條文，此不但能令社會服務界別能有更清晰的法規可依循，而且更能保障未成年人的利益。

2. 此外，本處建議如加入上述的新建議條文時，條文應附加一些因素，使資料使用者(例如社工)能夠衡量有否合理理由拒絕父母的查閱要求。本處建議的因素包括：甲) 未成年人的意願；乙) 提供資料給未成年人的父母會否危害當事人及他人的安全（例如把被虐子女現時居住的地址告之其施虐的父母知道或當事人拒絕接受治療而危害個人及他人的安全)；丙) 法庭的判決。

3. 本處更認爲不同類型的人士均應平等地受以上的新建議條文保障，因此本處反對諮詢文件建議「豁免易受誘惑及邊緣少年的父母遵從以上的規定，准許把未成年人的個人資料轉移給其父母或監護人，以加強對易受誘惑和邊緣少年的保護，以及使父母及監護人可妥善地履行適當照顧和監護兒童的責任」(附件 1，建議 27)。本處反對此建議，並不是否定父母及監護人應負起妥善地履行適當照顧和監護兒童的責任。相反，我們堅信爲服務使用者的長遠利益及福祉著想，父母及監護人的參與都是非常重要。但是，根據我們的前線社會服務經驗，所謂「父母及監護人的參與」是須有長遠的計畫及準備下才可進行。例如一名外展社工在街上遇上因家庭衝

突而離家出走的未成年人士，社工的首要工作是與個案建立關係及處理他的即時需要，如社工在認識該名未成年人後，便即時把資料告知其父母及監護人，此不但可能令個案不再信任社工而拒絕接受服務，而且更有可能把舊有問題擴大。另外，如一名受毒品毒害青少年因拒絕接受專業人士的協助而導致危害個人及他人的安全，資料使用者只需根據本處建議的 2.乙點附加因素，去衡量是否需要把資料提供給其父母及監護人，便可解決有關資料處理的問題。此外，新建議的條文中「易受誘惑及邊緣少年」的定義非常含糊及難於界定，因此爲保障及尊重未成年人的利益及權利，本處建議應把有關建議剔除。

4. 在附件 1 建議 13 的「第三者」定義方面，本處贊同把「有關人士」的定義擴展至包括根據精神健康條例 (第 136 章)第 44A 條、第 59O 條及第 59Q 條例被委任，精神上無行爲能力的資料當事人的監護人，此新建議條文能令有需要的人士獲得更全面的保障。除此之外，在本處多年的長者服務經驗中，我們發現現時在提供服務予"無能力處理其本身事務"之長者（如患有失智症者），一般由其家人作決定（如更改服務安排，申請院舍等），並非由法庭委任人士作處理；如實施有關建議，對服務提供或會造成重大影響，故需考慮有關條例之涵蓋範圍。

5. 在私隱專員的角色方面，本處同意授予私隱專員爲資料當時人提供法律協助 (第 5 章，建議 5)，此可加強保障資料當事人的權益，亦能夠加強阻嚇作用。但是「爲免私隱專員同時扮演法律協助及刑事調查和檢控罪行的雙重角色」及「確保本港的司法獨立」，本處不同意在新的條文下，私隱專員可授予刑事調查和檢控罪行的權力 (第 5 章，建議 4)。

6. 另外，本處同意附件 1 建議 26，執法機關、救援及支援組織在處理意外或其他危及生命的情況時，可獲得豁免遵守保障資料第 1(3)項原則及第 3 項原則，此可保障使資料當時人在危急時候獲得即時的救援。

7. 最後，作爲一間多元化的社會服務機構，本處不同意新建議條文中在「直接促銷」定義中剔除社會服務的建議 (附件 3，建議 38)。首先，本處尊重每個資料當時人自由選擇接受社會服務的權力，而且，在社會福利界的一筆過撥款下，越來越多社會服務團體參與涉及商業及直接促銷活動，例如社會企業，因此爲保障市場獲得公平競爭的機會，本處建議把附件 3 建議 38 剔除。

行政總裁吳水麗

(已簽署)

二零零九年十一月二十六日

S0080

醫院管理局
HOSPITAL AUTHORITY

HOSPITAL AUTHORITY'S COMMENTS ON CONSULTATION DOCUMENT ON REVIEW OF THE PERSONAL DATA (PRIVACY) ORDINANCE (PDPO)

Hospital Authority

24 November 2009

HOSPITAL AUTHORITY'S COMMENTS ON CONSULTATION DOCUMENT ON REVIEW OF THE PERSONAL DATA (PRIVACY) ORDINANCE (PDPO)

(A) **We have specific comments on the following proposals:**

(1) Proposal 1 – Sensitive personal data

We do not support this Proposal to create a further category of sensitive personal data because the existing system is well in place and the requirements of the proposed model will impose onerous operational and financial burden on HA bearing in mind collection of biometric data in the course of diagnosis and treatment is very common and in substantial volume in HA.

PDPO has an existing system well in place obliging data users to protect and safeguard all personal data of data subjects and to comply with the statutory requirements and the data protection principles (DPP) thereunder. It is questionable whether a further category of sensitive personal data with more stringent requirements over and above the existing system is necessary. We do not recommend a further category of sensitive personal data to be created.

If such a separate mechanism were introduced, data users will be subjected to additional operational and financial burden. The potential value and benefit from such a mechanism has to be weighed against the likely costs and resources to be expended in order to comply with such regime. Depending on what will be classified as sensitive personal data, it can potentially be onerous for the Hospital Authority (HA) to set up a new mechanism to handle this particular category. As a major health care provider in Hong Kong, HA handles substantial volumes of patients' personal data on a daily basis which are already subjected to the existing requirements of PDPO and under applicable law.

If a special category of 'sensitive personal data' is introduced, it is important that the legislation precisely define the scope of such data and the scope be limited at the outset. Data users need to be clearly guided as to its coverage and a narrower scope will enable data users and the administration to assess the practicalities of the mechanism. If

non-compliance with the new mechanism has potentially serious sanctions, it is all the more necessary that data users are facilitated by the legislative provisions and by administrative guidance on how to identify and handle such data.

The possible regulatory model imposes a general prohibition on the handling of sensitive personal data unless in specified exceptions. The burden lies on the data user to justify on each and every occasion that it can collect, hold, process and use sensitive personal data. If this model is to be adopted, it is important that the legislation should state and define such exceptions with clarity and precision. This is particularly so if the administration intends to impose sanctions or make it an offence for non-compliance with the new mechanism.

Under paragraph 3.09 in this proposal, the exceptions refer to situations where the data subject's prescribed consent has been (in subparagraph (a)) or cannot be obtained (in subparagraph (c)). The legislation should make clear how these exceptions apply particularly in the context of data subjects who are minors or who lack mental capacity.

The exceptions use the word 'necessary' on different occasions under subparagraphs (b), (c) and (g). The future model (if introduced) should give good guidance as to by what criteria this word is to be applied and interpreted.

Under paragraph 3.09(c), an exception is when the handling of the data is necessary for protecting the vital interests of the data subject or others where the data subject's prescribed consent cannot be obtained. Clear definition should be given as to what vital interests mean.

Under the model in paragraph 3.09(d), good and detailed guidance as to what amounts to appropriate safeguards should be given. Indeed, safeguards already exist under the present regime in PDPO against transfer or disclosure of personal data.

(2) **Proposal 2 – Regulation of data processors and sub-contracting activities**

We do not support this Proposal because the existing PDPO already imposes obligations on data processors and sub-contractors to protect personal data against unauthorized use etc.

The PDPO already imposes obligations on data users to take all reasonably practicable steps to ensure that personal data held by a data user are protected against unauthorized or accidental access, processing, erasure or other use. As the administration considers that the PDPO does not directly regulate the activities of an agent which processes personal data for its principal, the administration may wish to consider adjusting the definition of data user to include such data processors and subcontractors. This is particularly so in the context of Electronic Health Record Sharing.

(3) **Proposal 3 – Personal data security breach notification**

We support this Proposal.

The concept of a voluntary privacy breach notification system is supported but the specifics need to be worked on what needs to be notified and when. Clear guidance and adequate timing for such notification should be given. The voluntary mechanism should be limited to serious cases of personal data leakage or loss in the assessment of the data user. Being a voluntary mechanism, there should not be consequences for failing to give notification. Besides, to report the breach to PCPD within 5 business days is too tight for an organization to recollect the facts of the breach, analysis of the data lost and assessment of potential risks.

(4) **Proposal 13 – Third party to give prescribed consent to change of use of personal data**
Proposal 14 – Parents' right to access personal data of minors

We do not support these Proposals because it will be difficult for the HA to judge whether a request for a changed use or for disclosure of the personal data of the minor or a mentally incapacitated adult is or is not in his best interest or benefit.

Proposal 13 contemplates amending the PDPO to allow certain third parties to consent on behalf of data subjects who do not have sufficient understanding or intelligence to a change of use by the data user of the data subject's personal data if it is in the data subject's best interests or clear benefit to do so.

Proposal 14 is limited to a data access request situation in the context of a minor. It contemplates that a data user may refuse a data access request by a relevant person on behalf of a minor if the data user has reasonable grounds to believe that complying with the request would not be in the minor's best interests.

Under Section 18 of the PDPO, a relevant person (whether as currently defined in the PDPO or as may be expanded under Proposal 37) on behalf of an individual may request a data user to supply the individual's personal data that it holds. The data user is obliged to comply with such request unless otherwise permitted under the PDPO. There is no need for the relevant person to show and there is no need for the data user to know for what purpose the data requested is to be applied and whether such use is in the data subject's interests or benefit.

Following from this, the data user should not be laden with an additional burden to judge and determine whether a request for a changed use or for disclosure of the personal data of a minor or a mentally incapacitated adult is or is not in his best interests or benefit. Often, the request for a changed use or disclosure is not initiated by the data user but by some third party, and the data user is only responding to the request made.

Paragraph 8(a) describes a circumstance where a parent may abuse the data access mechanism to obtain the personal data of the child for the parent's own purpose rather than making it "on behalf of" the child. However, it can be very difficult to judge if there is an abuse. It may or may not be possible for the HA to judge the circumstance described in paragraph 8(b), ie, whether a parent is suspected to have committed child abuse.

Such a task to determine what is in a person's best interests or benefit can be difficult, especially for data users like HA which handles voluminous personal data of numerous data subjects. A data user may not have the information or ability to judge matters of clear benefit or best interests and it cannot be expected to embark on an investigation to check into or verify that. The data user may have little or no alternative but to place reliance on the assertions raised by the relevant person as to the benefit or best interests claimed. Indeed, what is 'clear' benefit can be hard to assess.

Furthermore, paragraph 6 under Proposal 13 raises a concept that other relatives or child care placement may be included as 'relevant person'. This calls into question how far the scope of relevant person should be extended. The practical logistics as to how this works need to be carefully canvassed especially when different persons claiming to be the 'relevant person' may object or consent to a changed use or disclosure and the data user is caught in the family dispute.

It would be helpful to take this opportunity to make clear what it means (in the context of a relevant person) to have parental responsibility and how it is applied in different situations such as divorced or separated parents, where a parent no longer has custody of the minor, where a parent has died or in a stepparent situation.

Lastly, if a minor is assessed to be of sufficient understanding and intelligence, his wishes as to his personal data privacy will need to be respected. There may be conflict in views between such a minor and the relevant person. If such a minor agrees or disagrees to a disclosure, it will be difficult for the data user to override his wish. Making clear the priorities will be helpful.

(5) Proposal 18 – Fee charging for handling data access requests

We support this Proposal provided there is adequate consultation as to the setting of the fee level and the maximum fees for chargeable items are set at a reasonable level.

The proposal aims to protect the public from being deterred from personal data access due to excessive fees charged for DAR. The intention of the

proposal is supported though a number of issues need to be addressed to ensure fair and successful implementation.

The maximum fee level should be reasonable and fair in terms of enabling the data users to recover their handling costs. As mentioned in the Consultation Document (Paragraph 25), there could be disparity in the operation costs between organizations, in particular between small companies and large statutory organizations. The handling costs could also vary greatly due to different complexity level of the personal data records.

HA's procedures in handling a data access request are explained below for better understanding of the complexity of HA's situation:

a. HA's procedures involved in the location, retrieval and reproduction of medical records are more complicated than those in other organizations. Medical records of patients comprise of the facts and findings related to the patients' conditions upon assessment by clinical staff, the self-reported history of illnesses and related information, the progress of patients conditions upon observation and interventions, including minute-to-minute recordings of patients specific physiological records, as well as information for clinical judgment and decision making, and all other relevant information related to the well-being of the patient, such as hand-over summaries and expert advice from other parties.

b. To make the complicated healthcare information recording and retrieval more complex, part of the information is recorded, stored and retrievable manually through paper record and hard copies while other part of the information is stored electronically, designed in a format and used via computerized interface for healthcare decision making purposes which could be difficult to be reproduced in paper format ready for dispatch to information requestor. Medical records of patients, especially for long stay patients or those with serious illness, are voluminous and complex. More time is required to extract the relevant information to meet the requestor's specific needs as well as to avoid copying irrelevant information and minimize the costs to the requestor.

c. A request often needs much clarification with the requestor before the scope can be determined. The extracted medical information needs to be reviewed by professional staff to ensure compliance with legal requirements (e.g. Mental Health Ordinance) and correctness as the information may often be used for clinical decision. To focus HA's limited resources on the provision of medical service to the public, HA has been providing copies of medical records under DAR on cost recovery basis. If the maximum fee is set at a level lower than HA's costs, the deficit in handling DAR will reduce the resources available for provision of medical service.

d. Higher labour costs are also incurred in duplication of x-Ray films and other radiological images which have to be performed by technical staff.

The maximum fee level is proposed to cover labour costs and actual out-of-pocket expenses. Quite often, the handling costs will be composed of fixed costs and variable costs. The former cover certain tasks that have to be done for each request while the latter vary with the complexity of the request and volume of records requested. The maximum fee level should reflect the nature of DAR and be composed of a lump sum covering the fixed costs plus an incremental charge covering the variable costs. This is similar to Proposal No. 26 in the Information Paper on Review of the PDPO issued by the Commissioner, under which, it is proposed to impose a non-refundable processing fee and charges for additional items.

The lump sum fee shall be levied upon lodgment of the DAR and should not be set too low so to prevent abuse of service by data subjects.

The principle of "not excessive" charge should be upheld for chargeable items covered in the fee schedule which is not explicitly stated in the Consultation Document. Otherwise, some data users may take the maximum level as the official approved charge irrespective of the actual costs in handling the DAR.

The maximum fee level needs to be reviewed from time to time to adjust for economic factors (e.g. inflation) and prevailing market price. A

mechanism needs to be set up for ongoing review.

(6) **Proposal 22 – Removing the Time Limit to Discontinue an Investigation**
Proposal 23 – Additional Grounds for Refusing to Investigate

We support these Proposals.

Section 38 of the PDPO sets out circumstances whereby the PCPD shall carry out an investigation. Before embarking on such an investigation, the PCPD would carry out "preliminary enquiry" to obtain information in order to decide whether to exercise its investigation power under Section 38. In the course of such preliminary enquiry, the PCPD may ask for disclosure of personal data of the complainant or other data subjects without furnishing consent from these individuals. For the sake of certainty, it will be beneficial to clarify that a data user is permitted to and will not contravene the PDPO or the DPP if and when it discloses such personal data to the PCPD in response to questions raised by the PCPD under the preliminary enquiry.

(7) **Proposal 27 – Transfer of personal data of minors relevant to parental care and guardianship**

We support this Proposal but it can be difficult for HA to judge whether a disclosure is for discharging the parent or guardian's responsibility on proper care and guardianship of the minor in the situation other than the provision of healthcare.

Proposal 27 seeks to deal with the restriction under the PDPO disallowing data users to transfer, of their own accord, the minor's personal data to his parents or guardian even if such transfer is to the minor's benefit. Proposal 27 contemplates introducing an exemption from DPP3 to permit data users to transfer a minor's personal data to his parents or guardian so that parents and guardian can properly discharge their responsibility on proper care and guardianship.

In the context of seeking consent for the provision of medical treatment to minors, the HA relies on the general law that consent can be obtained from

those with parental responsibility of the minor. To obtain consent from those with parental responsibility, it is inherent that information will need to be provided to them in order to enable them to make the decision. This process will involve disclosure of the minor's personal data to them. Such disclosure is necessary as part of the rendering of healthcare to minors.

In situations other than the provision of healthcare, it may be difficult for HA to judge whether a disclosure is for discharging the parent or guardian's responsibility on proper care and guardianship of the minor.

Nevertheless, if a data user makes such transfer or disclosure in the belief that it is to enable the parent or guardian to discharge his or her responsibility, but the minor or the parent or guardian disagrees, the data user should not be penalized for taking such a step.

Furthermore, data users will want to know whether it is necessary before applying such exemption to ascertain the views of the minor (especially if the minor is of sufficient intelligence and understanding). If such minor objects to the transfer or disclosure, then the priorities should be clearly set out.

(8) **Proposal 36 – Definition of Crime under Section 58 to mean a crime under Hong Kong law, or a crime or offence under the law of a place outside Hong Kong**

We do not support this Proposal because data users may not have the ability or knowledge to assess whether a situation amounts to a crime and offence overseas.

As the burden is on the data user to show it was justified to rely on a Section 58 exemption, data users may not have the ability or knowledge to assess whether a situation amounts to a crime and offence overseas. There can be practical difficulties to judge and determine the position under foreign law.

(9) **Proposal 37 – Expand the definition of "Relevant Person" to include the guardian of data subjects with mental incapacity appointed under Sections 44A, 59O and 59Q of the Mental Health Ordinance**

We support this Proposal.

The administration may consider whether to expand the definition to cover, for example, an attorney appointed under an enduring power of attorney.

Furthermore, applications for guardianship under Part IVB of the Mental Health Ordinance have to be supported by (amongst other matters) written reports of registered medical practitioners. In support of applications to the court under Part II of the Mental Health Ordinance, medical certificates are also required. As the data subject is mentally incapacitated, the party requesting for such reports or certificates from the HA is unable to furnish the data subject's consent to the HA for disclosure of the same. On the other hand, without these reports or certificates, the application will not be able to proceed. It would be beneficial to clarify that disclosure of personal data contained in such reports or certificates for the purpose of such applications under the Mental Health Ordinance will not be in breach of the PDPO or the DPP.

(10) **Proposal 38 – Exclude Social Services from the Definition of "Direct Marketing"**

We support this Proposal.

This proposal seeks to enable social workers in providing essential social welfare services for the benefit of target recipients to continue to use an individual's personal data without the need to inform the individual of an 'opt-out' right. In the HA, there may be circumstances where individuals may refer another person to the HA for psychiatric help and support and the person referred has not previously been treated in HA. The administration may consider extending the proposal to exclude from 'direct marketing' the provision of such needed services for the benefit of such persons being referred.

(B) **We believe that the status quo under PDPO should be adequate in respect of the following proposals:**

(1) Proposal 4 – Granting Criminal Investigation and Prosecution Power to the Privacy Commissioner for Personal Data (PCPD)

(2) Proposal 6 – Award Compensation to Aggrieved Data Subjects

(3) Proposal 7 – Making Contravention of a Data Protection Principle (DPP) an Offence

(4) Proposal 8 – Unauthorized Obtaining, Disclosure and Sale of Personal Data

(5) Proposal 9 – Repeated Contravention of a DPP on Same Facts

(6) Proposal 10 – Imposing Monetary Penalty on Serious Contravention of DPPs

(7) Proposal 11 – Repeated Non-compliance with Enforcement Notice

(8) Proposal 12 – Raising Penalty for Misuse of Personal Data in Direct Marketing

(9) Proposal 20 – Circumstances for Issue of an Enforcement Notice

(10) Proposal 21 – Clarifying Power to Direct Remedial Steps in an Enforcement Notice

(11) Proposal 40 – Extend Time Limit for Laying Information for Prosecution

(C) **We support the following proposals:**

(1) Proposal 16 – Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

(2) Proposal 17 – Erasure of Personal Data

(3) Proposal 19 – Response to Data Access Requests in Writing and Within 40 Days

(4) Proposal 24 – Transfer of Personal Data in Business Mergers or Acquisition

(5) Proposal 25 – Provision of Identity and Location Data on Health Grounds

(6) Proposal 26 – Handling Personal Data in Emergency Situations

(7) Proposal 43 – Contact Information about the Individual Who Receives Data Access or Correction Requests

(D) <u>We have no comment on the following proposals</u>:

(1) Proposal 5 – Legal Assistance to Data Subjects under Section 66

(2) Proposal 15 – Access to Personal Data in Dispute

(3) Proposal 28 – Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result

(4) Proposal 29 – PCPD to Disclose Information in the Performance of Functions

(5) Proposal 30 – Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit

(6) Proposal 31 – Power to Impose Charges for Educational and Promotional Activities

(7) Proposal 32 – Power to Obtain Information to Verify a Data User Return

(8) Proposal 33 – Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings

(9) Proposal 34 – Transfer of Records for Archival Purpose

(10) Proposal 35 – Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

(11) Proposal 39 – Exemption for Personal Data Held by the Court or Judicial Officer

(12) Proposal 41 – Duty to Prevent Loss of Personal Data

(13) Proposal 42 – PCPD to Serve an Enforcement Notice together with the Results of Investigation

(E) **We support the administration position on Annex 2 – Proposals not to be pursued.**

Hospital Authority
24 November 2009

S0081

(此意見書按發件人要求被 S0163 取代)

(This submission is replaced by S0163 as requested by the sender)

S0082

Reference:

Date: 26th November, 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

By email: pdpo_consultation@cmab.gov.hk

Dear Sirs,

Comments to Consultation Document on
Review of Personal Data (Privacy) Ordinance

We would like to put forward the views of [*"the Organisation"*] on the proposed amendments to the Personal Data (Privacy) Ordinance (PDPO).

[*"Org"*] supports the safeguarding of personal data and at all times follows the Data Protection Principles in collecting, using and handling personal data to ensure the compliance with the PDPO. Having being given the opportunity to comment, we would like to offer our views on specific proposals in the attached document.

We hope our comments would contribute to the Bureau's further deliberation of the review of the PDPO. We would be happy to discuss the issues in more detail if required so please do not hesitate to contact me at (deleted) or via email to (deleted)

Yours sincerely,

(Signed)

(The sender requested anonymity)

S0082

(The Organisation)'s

comments on

Consultation Document on

Review of the Personal Data (Privacy) Ordinance

Proposal No. 1: Sensitive Personal Data

From our reading of the proposal, it gives an impression that the concern lies on data leakage and therefore to implement a more stringent control on collecting, holding, processing and use of sensitive data, clause 3.01 referred. It is now proposed that if data is categorized as "sensitive personal data", it should then subject to the requirement of "prescribed consent" of data subject, clause 3.09(a) referred. While we support the principle to provide better protection to prevent data leakage, we do not see the introduction of a more stringent regulation of sensitive personal data would serve the purpose of preventing data leakage better. Moreover, we consider that the definitions of 'data' and 'personal data' are sufficiently wide to cover any personal data of an individual. Therefore, we do not consider that it is necessary nor appropriate to add a separate category of "sensitive personal" data. At the same time, we agree entirely that the term has many different perceived meanings and would only unnecessarily confuse and created uncertainties amongst the Hong Kong community at large what has been a well understood and implemented terms of 'personal data' under the Ordinance.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

It is inappropriate for data users, as private persons, to have a responsibility to police compliance with the law by other persons who process personal data for purpose of their own or others. In any event imposition of contractual obligations will not necessarily meet with the legislated objective of protection of individual's personal data which is imposed on all data users, regardless of whether a person may have been given possession of personal data following a contractual relationship or otherwise.

The legislative aim is to provide protection to personal data of individuals. In principle, all persons who would collect or process or in possession of personal data in general should be subject to the requirement of the law, regardless how they may have come into such possession. Therefore, we would support that proposal that activities of data processors should be directly regulated under the PDPO as that they would be subject to the same regulation as any other data users. As businesses are nowadays increasingly outsourcing their data processing activities, direct legal responsibility of the data processor could also improve the protection of personal data of individuals from leakage of data processor as the data processor, being likely experts in their field, would be in a better position to improve security measures to safeguard data leakage and provide better protection to personal data in their care.

Proposal No. 3: Personal Data Security Breach Notification

We agree that a breach notification system should not be compulsory. We are not aware of evidence that timely and sufficient notification of material breaches is not being given (and this is unsurprising given that the two most likely sources of material breaches, government and the financial industry, have voluntary systems in place). This being so, we do not think that anything further needs to done by way of legislation or guidelines in this area.

The components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42 are not applicable for a voluntary notification system.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

Having regard to the discussion in the Consultation Document, we agree that the status quo should be maintained, particularly in the light of the very small numbers of prosecutions actually undertaken and the general desirability of an objective assessment (by the Department of Justice) as to whether a prosecution is justified in any particular case.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

We do not support the conferring of this power. It seems to us that there is nothing peculiar to the privacy legislation which would justify taxpayers' money being made available to pursue a civil action under the legislation in circumstances where taxpayers' money would not be so made available under normal legal aid principles.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

Having regard to the discussion in the Consultation Document (in particular the point made by the Law Reform Commission that conferring such a power would vest in a single authority an undesirable combination of enforcement and punitive functions), we do not support the conferring of such a power.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

Having considered the original legislative intention of the DPP and the general nature of the DPP, we do not support making the contravention of a DPP an offence as it would have significant impact on civil liberties.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

We have no objection to make it an offence for a person who is confined to unlawful sale of personal data for profit. To make it offence for a person who discloses for malicious purpose, the term "malicious purposes" must be sufficiently and clearly defined. It should also be narrowed down the specific conducts so that uncertainty could be avoided. If a company is data user, it should not be held liable for such offence unless there is proven knowledge and connivance on the part of the company. In any event, such an offence must not have the effect of imposing an unnecessarily burden on businesses and the free throw of data for legitimate purposes in the community at large which would not be in the interest of Hong Kong as pointed out in the Consultation Paper.

If the offence is confined as proposed by us as above, we have no particular view on the level of penalty.

Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts

Having regard to the discussion in the Consultation Document (in particular the absence of repeat offences in practice) we do not consider it appropriate to create such an offence.

In the light of our preceding response, the penalty level for the offence is not applicable.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

Having regard to the discussion in the Consultation Document, we do not consider it appropriate to impose such penalties, especially by PCPD.

Whether there is any contravention of DPPs should remain a determination of the court. Similarly, the court, rather than the regulatory or executive branch, should be vested the power to impose a penalty. This reflects a well established tradition and principle of separate of power which has served Hong Kong well.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

Given the lack of prosecutions for repeat offences referred to in the Consultation Document, we do not think such heavier penalties are necessary.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

We do not consider it appropriate to raise the penalty for misuse of personal data in direct marketing under the provision of S.34(1)(ii) of the PDPO. We have not seen evidence or heard cases of misuse of personal data by direct marketing activities that warrants further or increase regulatory penalty.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

We support this proposal. However, the "third party" as a 'relevant person' shall be confined to:

- Where the individual is a minor, a person who has parental responsibility for the minor;
- Where the individual is incapable of managing his own affairs, a person who has been appointed by a court or otherwise has the legal authority to managing his affairs.

As there would be practically difficulty for a data user to verify the identity of such a third party being a "relevant person" of such a minor or incapacitated le person to give consent on behalf of a data subject, we do not consider it appropriate to expand the definition of "relevant person".

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

We have no views on this proposal, save to say that, if the proposal is implemented, the legislation should impose no obligation on the data user (expressly or by implication) to form an opinion on whether the disclosure is in the interests of the minor and no responsibility of data user to confirm or verify parental status in relation to the minor data subject.

Proposal No. 15: Access to Personal Data in Dispute

We support the proposal (as set out in paragraph 16 of Annex 1).

Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We support the proposal that the PDPO should be amended so that a data user need not comply with a data access request if the data user is entitled or bound by other legislation [or other legal obligation] not to disclose the relevant information. Similarly, there should be clarified in the legislation the exception to the use of the data to include disclosure in accordance or in compliance with any legal requirement or obligation.

Proposal No. 17: Erasure of Personal Data

We support the proposal for the amendment of the PPDO set out in paragraph 23 of Annex 1.

Proposal No. 18: Fee Charging for Handling Data Access Requests

We do not consider it appropriate to set a schedule prescribing maximum fees in PDPO set out in paragraph 28 of annex 1. We consider that the reasonable charges provision at present is sufficiently flexible to allow data users, taking into account of its circumstance but subject to objective standard, to recover the expenses incurred as a result of meeting the obligation imposed on them. At the same time, it also provides a balance against frivolous, excessive and irresponsible requests. Moreover, it has been our experience that many personal data requests have been used as fishing expedition for pre-litigation purpose to extract information which the data subject would not otherwise be entitled or obtained with ease in a litigation proceeding. Such purpose is clearly violating the legislative intent of PDPO and has not been supported by the court.

Setting a schedule prescribing maximum fees in PDPO will impose unnecessary financial burdens to data users and it is not fair.

Proposal No. 19: Response to Data Access Requests in Writing and Within 40 days

We think it undesirable to create a special regime for the police, though we understand that, if the legislation is amended as suggested, they will need a special regime. We think the better solution is not to amend the legislation.

Proposal No. 20: Circumstances for Issue of an Enforcement Notice

We do not consider it appropriate to create the circumstance set out paragraph 39(c) to allow discretion for the PCPD to serve an enforcement notice. Having considered the present provisions in the PDPO which give power to the Commission to serve enforcement notice to the data users concerned, we take the view that it is sufficiently wide to enable the Commission to enforce the law effectively and therefore unnecessary to create circumstances for enforcement notice to be served as proposed.

Proposal No. 21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

We have no views on the option in paragraph 40 of Annex 1.

Proposal No. 22: Removing the Time Limit to Discontinue an Investigation

We have no views on the option in paragraph 43 of Annex 1.

Proposal No. 23: Additional Grounds for Refusing to Investigate

We have no views on the appropriateness of including the specific grounds referred to in paragraph 48.

Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

We support the exemption of such transfers. We think that the only condition necessary is that the transfer is required for the purposes of due diligence.

Proposal No. 25: Provision of Identity and Location Data on Health Grounds

We support changes to the legislation so that it operates along the lines described in paragraph 56 of Annex 1.

Proposal No. 26: Handling Personal Data in Emergency Situations

We support the proposed exemptions.

Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

We have no views on this proposal, save to say that, if the proposal is implemented, the legislation should impose no obligation on the data user (expressly or by implication) to form an opinion on whether the disclosure is in the interests of the minor and no responsibility of data user to confirm or verify parental status in relation to the minor data subject.

~ End ~

S0083

香港中華廠商聯合會
The Chinese Manufacturers' Association of Hong Kong
(一九三四年成立 Established in 1934)

75 七十五周年誌慶 CMA 75th Anniversary

永遠名譽會長
Permanent Honorary Presidents
洪祥龍先生
Mr C P Hung JP
倪少傑先生
Mr Ngai Shiu Kit SBS OBE JP
朱祖涵先生
Mr Lawrence C H Chu
梁啟基先生
Mr Herbert Liang SBS MBE JP
陳永祺先生
Mr Chan Wing Kee GBS OBE JP
楊孫西博士
Dr Jose S S Yu GBS SBS JP
洪克協先生
Mr Peter H H Hung

[illegible]
[illegible]ident
尹德勝先生
Mr Paul T S Yin SBS BBS JP

立法會代表
Legco Representative
林大輝博士議員
Dr The Hon Lam Tai Fai BBS JP

副會長
Vice-Presidents
黃友嘉博士
Dr David Y K Wong
羅富昌先生
Mr Lo Foo Cheung JP
葉志光博士
Dr Yip Chi Kwong
倪錦輝博士
Dr Danny Ngai Kam Fai JP
施榮懷先生
Mr Irons Sze
劉文煒先生
Mr Joseph M W Lau BBS JP
李秀恆博士
[illegible]ddy S H Li BBS
[illegible]輝博士
Dr Lam Tai Fai BBS JP
羅榮鎰英女士
Mrs Ngan Ng Yu Ying Katherine JP

總務委員會主席
Chairman
General Affairs Standing Committee
黃友嘉博士
Dr David Y K Wong

財務委員會主席
Chairman
Finance Standing Committee
羅富昌先生
Mr Lo Foo Cheung JP

行政總裁
Chief Executive Officer
梁世華先生
Mr Paul S W Leung SBS

本會對「檢討《個人資料(私隱)條例》的諮詢文件」之意見

敬啟者：多謝　貴局於八月二十八日給本會尹德勝會長的來信。就檢討《個人資料(私隱)條例》的諮詢文件，本會經研究後，已擬具有關意見，現隨函附上意見書乙份，以資參考。如有查詢，請與本人(電話：2542 8668)或本會高級經理顏紅曉先生(電話：2542 8631)聯絡為荷。

此 致

政制及內地事務局局長
林瑞麟 GBS 太平紳士

附：本會意見書乙份

（已簽署）

香港中華廠商聯合會
行政總裁梁世華

二零零九年十一月二十七日

總辦事處 HEAD OFFICE
旺角辦事處 MONGKOK OFFICE
觀塘辦事處 KWUN TONG OFFICE
廣州代表處 GUANGZHOU OFFICE
廠商會檢定中心 CMA TESTING & CERTIFICATION LABORATORIES

S0083

香港中華廠商聯合會

對「檢討《個人資料(私隱)條例》的諮詢文件」的意見

1. 本會認同本港應為敏感個人資料提供較高程度的保障，故有需要訂明祇有在指定的情況下才可收集、持有、處理和使用敏感個人資料。本會亦贊成將生物辨識資料列為敏感個人資料以及採取諮詢文件中所建議的相關規管措施；但不認為須把在處理敏感個人資料時未能遵守保障資料原則的行為定為罪行。本會建議，本港可沿用現行的模式處理敏感個人資料的規管，並須採取不溯既往的豁免安排，允許在有關法例條文生效前已收集的敏感個人資料仍可繼續使用。
2. 鑑於把個人資料分判或委託給第三者處理的趨勢日益普遍，本港有必要引入間接規管模式，要求將個人資料轉移給第三方的使用者必須以合約形式或者其他方法，確保其承辦商或分包商會採取切實可行的程序，保證資料安全以及得到妥善的保管和處理。
3. 對個人資料外洩設立強制性通報機制可能會對商業活動帶來沉重的負擔，亦可能導致過度通報的現象。有見及此，本港暫無需訂立個人資料外洩的通報機制，但可鼓勵發生外洩事故的機構在自願基礎上兼且能力可及的範圍內，向私隱專員以及受影響的人士作出通報；私隱專員可就此制定無約束力的指引，供公眾參考。
4. 本港目前與私隱條例相關的檢控安排運作良好，並無需要再授予私隱專員刑事調查及檢控的權力。另一方面，為了避免把執法和處罰的職能歸於同一機構，私隱專員亦不宜獲授權向受屈的當事人判給補償以及為當事人提供法律協助。
5. 本會不贊成將違反保障資料原則訂為罪行，以免因為過份擴大刑責而影響公民自由。為了增強對嚴重違例行為的阻嚇作用，本會認為可考慮將就同一事實重複違反保障資料原則的行為訂為罪行；亦贊成《個人資料(私隱)條例》將未經授權下取得、披露和出售個人資料以從事牟利或作惡意用途的行為訂為罪行，並為此提供適當的抗辯理由條文以及罰則。
6. 本會認為，目前本港就違反保障資料的罰則整體上已行之有效，故無需授權私隱專員向嚴重違例者處以罰款或者對屢次違反條例者施以更重的懲罰；惟對於直接促銷的活動中不當使用個人資料的行為，可考慮將罰款的上限由 10,000 元提升至 50,000 元，以增強阻嚇力。

2009 年 11 月 27 日

27 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Sirs,

Consultation Document on Review of the Personal Data (Privacy) Ordinance

We are a credit reference agency pursuant to the Code of Practice on Consumer Credit Data issued by PCPD. We would like to thank you for the opportunity for us to comment on the Consultation Document. Our views on some of the Proposals contained are set out below.

Proposal No. 4	**Granting Criminal Investigation and Prosecution Power to PCPD**
Proposal No. 6	**Award of Compensation to Aggrieved Party**
Proposal No. 7	**Making Contravention of a Data Protection Principle an Offence**
Proposal No. 10	**Imposing Monetary Penalty on Serious Contravention of Data Protection Principles**

Our comments:

1. In general, we have concerns on expansion of power by PCPD under these Proposals and particularly in granting PCPD criminal prosecution and sanction power. We are concerned this may not be consistent with principles of separation of power in which executive, judiciary and legislative functions should be separated for check and balance.

In particular, the PCPD is empowered to approve Code of Practice. Although a breach is not a violation of law in itself, it is evidence of breach of Data Protection Principles. Currently, the Code of Practice on Consumer Credit Data which is drafted by PCPD applies to our business. If the Proposals are implemented, especially if contravention of Data Protection Principles is made direct criminal offences, the role of formulating the Code, interpreting and enforcing will be merged and vested in the same body.

2. Hong Kong already have one of the most developed privacy law regime in Asia and have the only independent privacy commission. While the effort to advance privacy rights for individuals in Hong Kong should be lauded, higher degree of privacy protection and ease of enforcement may make Hong Kong less competitive in Asia for businesses as costs of compliance will be higher. It may also discourage innovativeness as some commercially viable products or solutions beneficial to the economy involving personal data may not be feasible. For example, authentication of identity using credit data as a fraud solution generally is not permitted under current privacy law. Such solutions can have wide application to financial transactions, development of e-commerce, and in any situation where identity authentication is required (for example, authenticating electors upon voting) and can be widely beneficial to the economy.

3. Other than focusing on the enforcement side, we would like to respectfully suggest that upholding and promoting privacy rights should be a multi-dimensional task. On one hand, education of consumers on not just the extent but also the limitation of their rights is vital to maintain an environment conducive to our development of a healthy financial and economic system. On the other hand, continued expansion of role to give guidance including giving pre-case ruling to data users are in fact very helpful. Also, a reconciliatory approach by the creation of a mediation role for disputes on privacy issues may also be beneficial.

Proposal No. 18 Fee Charging for Handling Data Access Request

Our comments:

We are not supportive of setting a prescribed maximum on fee for data access request. The cost involved in data access depends on a variety of factors including

1) the nature of the data requested – is it something easily obtainable with little labour cost required eg copy of an application submitted, or something which needs to be retrieved, considered and processed

2) the cost structure of the data user

3) the nature of business of the data user- Is it in the business of information management as in the case of a credit reference agency or public record information company. In such cases, in addition to considering only the actual costs of disclosing the data, other costs like capital investment for collection of the data in the first place,

operating costs, the return on the investment for such companies must be taken into account. The question is who should dictate how much such return should be.

As the cost structure for each data user is so different, it is not practical from the data user's point of view to set a standard fee. No matter what basis is used to determine the prescribed maximum, setting it either too high or too low will obviously not work. If it is set somewhere in the middle, this will also have problems. Practically, it is likely that most data users will charge the maximum fee and therefore, the larger operations with higher cost will be subsidizing the profit of the smaller operators with lower costs for data access requests. This is not fair for the larger commercial enterprises.

We note that in the UK, a blanket maximum fee of 10 pounds is set except for credit reference records. However, the prescribed maximum for credit reference records is in fact only 2 pounds. Currently, a credit report charged by our company to the public is HK$180 and subject to review from time to time. If the intention to follow the UK practice in totality, the imposition of a drastically lower credit report fee would affect the viability of the business of our company which is based on our current credit report fee and which is also subject to revision in accordance with economic factors. This is also indirectly setting a limit on our revenue and pricing which is not in line with the Hong Kong economic or regulatory development.

Although we are not experts in specific UK legislation, we would also like to add that the legislative framework in the UK is very different from Hong Kong. We understand they have more developed consumer protection law and the credit reference agency is not just regulated by the Data Protection Act but also by the Consumer Credit Act. Both laws confer wide protection on consumer and privacy rights. They also have the Freedom of Information Act which ensures rights of personal data of citizens from government authorities and hence the atmosphere of data access seems very different. Note that in Hong Kong, our legislative environment has not evolved to the same extent and therefore adopting the UK model and setting a prescribed maximum fee may not be appropriate.

We also understand that the move to suggest a maximum fee is caused by complaints lodged by consumer for excessive fees charged. With due respect, we do not think any amendment to existing law should be complaint driven as this will sway the development of our legal system in the wrong way and not take into account other factors like effect on general competitiveness of our society and impact on other stakeholders. The key is rather more guidance and education on privacy rights.

S0084

In case you have any questions on our comments above, please contact (deleted) Director of Legal & Compliance, at (deleted) who would be most happy to discuss any issues further.

Yours faithfully,

(Signed)

(The sender requested anonymity)

S0085

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)



To pdpo_consultation@cmab.gov.hk
cc
bcc
27/11/2009 12:17 Subject 香港專業地產顧問商會對《個人資料(私隱)條例》的意見

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啓者：

有關《個人資料(私隱)條例》諮詢文件，本會商討後的意見如下：

1. 我們很同意公眾及個人資料的資料處理者是再進一步關注及重視有關資料上的處理。
2. 我們是同意將嚴重及多次違反保障資料原則的行爲，施加罰款。
3. 我們同意把披露未經資料使用者同意下取得的個人資料而從中取利或作惡意用途的行爲訂爲罪行。
4. 我們是不同意將違反資料原則的訂爲刑事罪行。

香港專業地產顧問商會會長
Lawrance Wong

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Central
Hong Kong

By Post & Email

27 November 2009

Dear Sirs

Personal Data (Privacy) Ordinance Public Consultation

We refer to the *Consultation Document on Review of the Personal Data (Privacy) Ordinance* (the ***Consultation Document***) issued by your offices on 28 August 2009.

In response to the Bureau's invitation for public views on the Consultation Document, we welcome the opportunity to submit our comments on the Bureau's proposals for revision of the *Personal Data (Privacy) Ordinance* (Cap 486) (the ***PDPO***).

By way of background, we are a leading international law firm with offices in twenty-seven locations around the world. We established our Hong Kong office in 1985, from where we provide a wide range of legal advisory services to businesses and individuals, including advice relating to the PDPO. We routinely make submissions and participate in public consultation exercises undertaken by the Hong Kong Government in relation to Hong Kong law reform initiatives and we believe this activity to be an important part of our role and our responsibility to the community.

As an international law firm, we draw upon on our experience of data privacy laws in other jurisdictions. The PDPO, of course, shares many elements in common with Directive

PARTNERS
Clive Rough Teresa Ko Richard Chalk Robert Ashworth Bruce Cooper Connie Carnabuci Ng Kay Ian Christopher Wong Peter Yuen Calvin Lai Grace Huang
REGISTERED FOREIGN LAWYERS
Simon Marchant (England and Wales) Perry Sayles (New York, USA)
Abu Dhabi Amsterdam Bahrain Barcelona Beijing Berlin Brussels Cologne Dubai Düsseldorf Frankfurt am Main Hamburg Hanoi Ho Chi Minh City Hong Kong London Madrid Milan Moscow Munich New York Paris Rome Shanghai Tokyo Vienna Washington

95/46/EC of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the ***European Data Protection Directive***). We have extensive experience advising on this directive and a number of the lawyers who have been involved in preparing this submission have advised clients both on the PDPO and on the national law enactments of European Community member states which have implemented the European Data Protection Directive. We have also advised on data privacy issues in a number of other jurisdictions in Asia and therefore have a good comparative understanding of data privacy laws and regulations across the region.

We have organised our submissions below using the numbering set out in the Consultation Document. We would be pleased to provide any clarification or further comment on our submissions at your request.

Proposal No.1: Sensitive Personal Data

We believe that the creation of a sub-category of sensitive personal data would, in principle, be an improvement to the PDPO. We support proportionality of regulation and where the loss or misuse of particular categories of data gives rise to more serious consequences for data subjects, it makes logical sense that the regulation is more rigorous and the consequences of non-compliance more substantial.

We fully appreciate the point made in the Consultation Document that perceptions as to what constitutes "sensitive" personal data draw on cultural considerations which may not be so readily transferable from the European Data Protection Directive or other laws and regulations from around the world. The proposal in the Consultation Document to limit sensitive personal data to biometric data would establish a very clear definition for this data but would leave the category of "sensitive" personal data very narrow in its conception.

We would suggest further discussion and debate on this subject with explicit consideration as to what the legislative objectives of the PDPO are in this respect. In particular, we think it prudent to consider whether the introduction of a category of sensitive personal data to the PDPO seeks to support the *Hong Kong Bill of Rights Ordinance* by imposing greater control over the misuse of data in a way which could contravene that ordinance. Alternatively, the objective may be more general, intending to enhance the PDPO's effect in relation to misuse

of data which generally causes more significant harm than other categories of data. We feel that clarity on the objectives of creating a category of sensitive personal data will help the development of the PDPO in this area.

Proposal No.2: Regulation of data processors and sub-contracting activities

The Consultation Document notes that the use of third party data processors is increasing in Hong Kong and that there have recently been some high profile security breaches involving leaks of personal data by such processors.

There is at present no explicit regulation of the processing of personal data by agents under the PDPO. Our understanding from the Consultation Document is that the Bureau is proposing two alternative regimes to fill the gap: (i) indirect regulation of data processors by means of imposing obligations on data users to procure data processors' compliance with the PDPO through contractual measures; and (ii) direct regulation of data processors under the PDPO.

We believe that there is good reason for the Bureau to seek to incorporate specific measures in the PDPO dealing with data processors. However, we strongly urge that the first proposed model of indirect regulation be adopted rather than the latter model of direct regulation.

We believe that direct regulation of data processors is likely to be harmful to Hong Kong's economy.

Imposing a direct regulatory burden on data processors will require data processors, IT service providers, business process service providers, internet service providers (***ISPs***) and other entities which process personal data on behalf of other businesses to take steps to assess the compliance risk that they face under the PDPO in agreeing to process the data. These steps will necessitate that the data processor make an assessment of the fairness of the processing of the data they have been asked to undertake by the data user. In practical terms, this means that the data processor will need to acquire an understanding of the nature of the data that they are processing, the circumstances under which the data was obtained by the data user and make an assessment as to whether the data is being processed in accordance with the purposes permitted under the PDPO.

The Consultation Document acknowledges that this would be a very heavy burden in the case of ISPs, who are typically "mere conduits" for data flow and who have little or no knowledge of the nature of the personal data processed on their equipment and networks. The Consultation Document raises the possibility that ISPs therefore be exempted from the regime for these reasons. However, we believe that the same lack of knowledge will apply to most other data processing entities. For example, an IT services company which manages a corporate data user's databases and IT infrastructure under an outsourcing arrangement will not be in a position to review the manner in which customer data in the database was initially obtained, nor will it be able to assess whether or not requests by the data user's employees for access to the data held in the outsourced database are compliant with the permitted purposes for processing the data under the PDPO. At best, the service provider would be "second guessing" the compliance assessments made by the data user, who will have far better information and therefore be in a far better position to reach a conclusion.

It should also be borne in mind that the compliance position in relation to personal data may change, for example, where new privacy policy terms are agreed or where a data subject has requested their removal from a marketing list. These changes are far more likely to be administered by the data user than the data processor and it will often be impracticable for data processors to remain current with this information.

For these reasons, we believe that the Bureau's concerns that direct regulation of ISPs under the PDPO would threaten Hong Kong's internet-related businesses apply more generally to business process outsourcing services providers, IT services providers and most other data processing businesses. Fewer businesses would offer these services if they bear a compliance risk. Those who continue in the data processing business would, if acting prudently, incur the cost of at least some degree of "second guessing" the data user's compliance position through legal due diligence. This would necessarily lead to price increases to cover the cost of the due diligence and a shifting of potential liabilities through indemnities.

We believe that these developments would put Hong Kong at a significant disadvantage as there is no comparable regulatory requirement anywhere in Asia. Industries which are particularly reliant on outsourced services such as banking and financial services would likely be hardest-hit, particularly local businesses competing with offshore entities whose outsourcing arrangements would not be bound by these requirements to the extent that they

rely on offshore data processing. Given the breadth of the proposal, even fairly mundane outsourced services such as company payroll would be impacted, with cost and efficiency implications for businesses of all sizes who benefit from specialist service providers in these areas.

The rise of outsourcing and other forms of data processing in Hong Kong (as noted in the Consultation Document) is consistent with developments elsewhere in the world. Businesses can benefit from outsourcing their non-core functions. In pursuing data processing and outsourcing initiatives, Hong Kong businesses are simply seeking to remain globally competitive. We do not believe that engaging third party data processors should perceived to be an inherent threat to data security. We do, however, believe that effective regulation is needed in this area, but that there is greater merit in the Bureau's first proposal to require data users to procure data processors' compliance with the PDPO through contractual measures. This approach would bring the PDPO in line with the position prescribed by Article 17 of the European Data Protection Directive, which provides:

Article 17

Security of processing

1. Member States shall provide that the [data user] must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the [data user] must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the [data user] and stipulating in particular that:

- the processor shall act only on instructions from the [data user],
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Article 17 of the European Data Protection Directive requires that data users enter into written contracts with their data processors. These contracts bind the data processor to process personal data only in accordance with the data user's instructions and in compliance with agreed technical and organisational measures which are appropriate for securing and preventing unauthorised use of the data.

The European Data Protection Directive places the onus on data users to judge the technical and organisational measures needed to achieve compliance with the directive. This is a sensible approach given that it is the data users who have full knowledge of the nature and sensitivity of the data and the circumstances under which it was obtained. Data users will therefore be best placed to determine appropriate measures needed to safeguard the data in accordance with the law and bear the consequences if improper processing takes place.

We believe that this approach will achieve the Bureau's objectives and provide an enforcement mechanism which will be acceptable to data processing businesses.

We would add that we have advised a number of corporate data users on large scale data processing and outsourcing contracts in Hong Kong. Following our advice on the point, our clients tend to ask that we incorporate terms along the lines of Article 17 of the European Data Protection Directive into the contracts we prepare to address the client's compliance with the fourth data protection principle under the PDPO and to safeguard confidentiality as an important business consideration. We have not encountered any difficulty on the part of IT service companies and other data processing businesses in accepting these terms. This approach provides a clear, consensual basis between the parties for managing compliance under the PDPO with explicit means of protecting data privacy through a written contract.

We also note that this approach has the advantage of being equally applicable to all data processors which process data collected, held, processed or used in Hong Kong or otherwise

controlled by a Hong Kong data user. If direct regulation of data processors were adopted under the PDPO, this would only apply to data processors based in Hong Kong, while the activities of off-shore data processors would continue to go unchecked.

In summary, we believe that there is greater merit in the Bureau's proposal to strengthen the obligations on data users in order to secure compliance of data processors' handling of personal data with the requirements of the PDPO, with a specific recommendation that Article 17 of the European Data Protection Directive be looked to as a proven approach which we hope would secure better PDPO compliance.

Proposal No.3: Personal data security breach notification

We are broadly in favour of the Bureau's proposal to implement a data privacy breach notification system. We agree that this should be introduced initially on a voluntary basis so as to avoid undue burden on the business operations of data users and to gain experience for the purpose of developing a mandatory procedure.

We note, however, that as is the case with many non-mandatory guidelines, the success of the notification system will rely on the judgment of data users to determine when a personal data security breach should be notified. Other factors, such as the costs of notifying data subjects and the reputational risk for the data user, may have an effect on the data user's decision whether or not to voluntarily notify the Privacy Commissioner for Personal Data (***PCPD***) and data subjects of data security breaches. It may be prudent for the guidelines to specify a non-exhaustive list of defined examples of personal data security breaches where notification to the PCPD and individual data subjects should be made. This could serve as a benchmark for data users to follow for voluntary notification of breaches in future.

Proposal Nos. 7 to 12: Offences and Sanctions

We regard the unauthorised use or misuse of personal data in breach of the PDPO to be a serious matter, and we agree that the current enforcement regime is perceived to be an inadequate deterrent against breaches of personal data security in Hong Kong. The consequence for Hong Kong is that in a number of areas of business activity, compliance with the ordinance is, regrettably, not taken as seriously as it should be. This undermines confidence in Hong Kong business.

We would note, in particular, the comments made by Magistrate Chan Yan-tong in his January, 2007 decision to fine a telecommunications company for continuing to make contact with data subjects for marketing purposes notwithstanding repeated requests that this contact cease. Mr. Chan commented that he did not feel that the fines, fixed to a maximum of HK$10,000, were a sufficient deterrent, particularly for large organisations which were likely to see such low fines as "a cost of doing business."

We agree that action must be taken to improve the PDPO's enforcement mechanics to make the ordinance a more effective deterrent, but we also agree with the Bureau's conclusion, set out in relation to Proposal 7, that a selective approach to characterising offences under the PDPO is preferable to the creation of a general offence of breaching a data protection principle. We do not believe that the data protection principles are sufficiently specific to form the basis for clear and justiciable criminal offences and that the aims of the PDPO will be better served in many cases by a co-operative administrative approach which encourages better compliance rather than an approach which is necessarily punitive.

We also agree with the Bureau's view set out in relation to Proposal 8, that there are clear areas of misuse of personal data which merit punishment as an offence. The Consultation Document refers (in paragraph 6.07) to section 55 of the United Kingdom *Data Protection Act 1998*, which creates the criminal offence for deliberate or reckless misuse of personal data. We believe that this would form a sensible basis for an analogous provision in the PDPO. The defences referred to in paragraph 6.08 of the Consultation Document should provide a means of clearly focus the offence on the abusive practices which it seeks to prevent.

We would also agree with proposals to enhance penalties for second or subsequent failures to comply with enforcement notices (Proposal 11). An enforcement notice will, like a tailored offence, give specificity to the unlawful conduct at issue and give advance written notice of an intention to prosecute the conduct should the remedial steps taken out in the notice not be taken. An offence crafted on this basis would therefore provide a fair, justiciable basis for bringing a prosecution.

In relation to the Bureau's review of the level of penalties imposed under the ordinance (Proposals 9 through 12), we would note that the United Kingdom's Ministry of Justice has

recently proposed the introduction of custodial sentences for misuse of personal data and that it intends to increase the maximum penalties for offences under section 55 of the *Data Protection Act 1998* (referred to above) to up to twelve months' imprisonment on summary conviction and up to two years' imprisonment on indictment.

In addition, the United Kingdom's Ministry of Justice has recently proposed that the Information Commissioner's Office would have the power to fine data user organisations up to GB£500,000 for serious breaches of data protection principles.

We believe that the former proposal to include the possibility of custodial sentences for the commission of an offence under the UK data protection legislation has merit, to the extent, at least, that monetary fines have proven to be inadequate deterrents and the approach remains limited to specific offences. For the reasons noted above, we do, however, have reservations about the second proposal to tie significant penalties to breaches of generally worded data protection principles, even if the offence is limited to material breaches.

In summary then, we would suggest that the Bureau consider the creation of a specific PDPO offence in line with section 55 of the UK *Data Protection Act 1998*, the creation of an offence of repeated non-compliance with an enforcement notice and consider increasing the penalties which may be imposed for misuse of personal data in direct marketing in breach of section 34 of the PDPO to a level which would clearly outweigh any commercial incentive to perpetrate the unlawful activities. The same enhanced levels of penalties should, in our view, apply proportionately to any new offences created as part of the reforms.

Proposal No.24: Transfer of personal data in business mergers or acquisitions

We believe that the exemption of personal data transfers as part of a merger or acquisition, conditional upon the provisions set out in the Bureau's Review, would bring the PDPO in line with the PCPD's code of practice. Merger and acquisition activity is, of course, important to the Hong Kong economy, as it provides opportunities for attracting investment capital and generating business efficiencies.

Disclosure of personal data to a potential acquirer during pre-sale due diligence may technically be use of personal data outside the scope of the original consent given by the data subjects and therefore may be inconsistent with the provisions of the PDPO. However,

obtaining consent from the data subjects for the transfer of their personal data for this purpose is usually impractical in the circumstances given the extent of such an exercise and the time constraints involved in the merger or acquisition process. In practice, most potential acquirers and their legal and financial advisers will be bound by confidentiality agreements with the seller for the protection of information disclosed to them during the sale process, which reduces the risk of any material effects or damage flowing from the seller's disclosure of personal data information.

We are in favour of the exemption from the PDPO for the transfer of personal data as part of a merger or acquisition, provided that it is the case that the personal data are acquired as assets of a going concern and the data would, following completion of the sale, continue to be used in manner and for substantially similar purposes for which it was collected.

Proposal No.25: Provision of identity and location data on health grounds

We believe that it makes practical sense to include disclosure of data subjects' identity and location information within the exemption under section 59 of the PDPO, which relates to the physical or mental health of data subjects.

There may be emergency circumstances in which the provision of identity and location personal data is vital to preventing serious harm to the physical or mental health of the data subject or other individuals, e.g. in the case of a global pandemic such as the recent swine flu outbreak. It may not be possible to obtain the prior consent of data subjects for disclosure of their identity and location personal data in the circumstances, due to incapacity of the data subject or time constraints, and without such consent the disclosure of identity and location personal data currently breaches the PDPO.

We believe that an extension of the exemption under section 59 to include identity and location data of a data subject is justified for the purposes of reducing the risk to the life or health of individuals.

Conclusions

We hope that you find our comments on the Consultation Document useful and we remain at your disposal to provide any clarification or further information which may assist the Bureau

in the evaluation of its proposals to amend the PDPO.

Yours faithfully

(Signed)

Freshfields Bruckhaus Deringer

S0088

27 November 2009

Team 4
Constitutional and Mainland Affairs Bureau

Re : Consultation on Review of Personal Data (Privacy) Ordinance

On behalf of *["the Organisation "]*

I am writing to submit our views in connection with the current review of the Personal Data (Privacy) Ordinance ("**PDPO**"). We hope that these will help the Bureau understand the concerns, in particular, of individual directors of companies registered under the Companies Ordinance in Hong Kong and that the Bureau would take them into account when finalizing the amendment(s) to the PDPO.

At present, there are more than one government agencies, for example the Companies Registry, the Transport Department and the Lands Registry, that are openly disclosing personal data, including name, complete ID number and residential address of individuals or directors of private companies registered in Hong Kong, to anyone who is willing to pay a small fee. These include:-

a) result of a company search that includes all individual directors' name, complete ID number and residential address;
b) Certificate of Vehicle Particulars provided by the Transport Department which shows the owner's name, complete ID number and residential address; and
c) copy of land registration record provided by the Land Registry which contains personal data of owners including complete ID number.

Given the concern for protection of personal data, the Government as a whole should probably consider how the above can be improved such that the result of these search are meaningful for their intended purpose while not compromising the protection of personal data, such as disclosing only part of the ID number and/or the residential address.

商界展關懷
caringcompany
Awarded by The Hong Kong Council of Social Service
香港社會服務聯會

S0088

27 November 2009

Should you have any questions or need any clarifications on the aforementioned examples, please do not hesitate to contact the undersigned at (deleted) or (deleted)

Yours faithfully

(Signed)

RL/

(The sender requested anonymity)

商界展關懷
caringcompany
Awarded by The Hong Kong Council of Social Service
香港社會服務聯會獲授

S0089



To <pdpo_consultation@cmab.gov.hk>
cc
bcc
27/11/2009 16:27 Subject AIDS Concern: opinion on Personal Data(privacy) Ordinance Consultation

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir,

Pls refer to the attached documents for the opinion from AIDS Concern on Personal Data(privacy) Ordinance Consultation.

Documents:
- Cover Letter
- Opinion

Should you have any enquiry, pls don't hesitate to contact Chan Fei at or through this email.
Thanks very much for your kind attention.

Best Regards,

Chan Fei
Campaign Officer (Anti-Stigma)
AIDS Concern

Our **MISSION** is to keep HIV prevelance in Hong Kong low through targeted prevention and care programmes for vulnerable communities, and to reduce the stigma attached to the disease and the communities most affected.



AIDS Concern Letter_PCPD Consultation.pdf



AIDS Concern comment_PCPD Consultation.pdf

AIDS concern
關懷愛滋

Established in 1990, AIDS Concern is a registered charity
關懷愛滋成立於一九九零年，爲一間註冊慈善機構

S0089

Patrons
贊助人

The Honorable Henry Tang Ying-yen, GBS, JP
唐英年先生

Ms. Anne B. Forrest
福爾絲小姐

Mr. James Haybyrne
賀智彬先生

Dr. Stanley Ho, GBS
何鴻燊博士

Ms. Christine Loh
陸恭蕙小姐

Mrs. Anne Marden MBE JP
馬晉夫人

Mr. Simon Murray CBE
馬世民先生

Ms. Michelle Yeoh
楊紫瓊小姐

Dr. Andrew S. Yuen
阮伊文博士

香港個人資料私隱專員公署：

個人資料(私隱) 條例諮詢

就個人資料(私隱)條例諮，「關懷愛滋」的回應載於附件一。

有關回應集結了個別愛滋病病毒感染者的意見，藉此向公署反映社群的關注，並期望日後「關懷愛滋」能與香港個人資料私隱專員公署就推動愛滋病病毒感染者的私隱保障合作。

如有查詢，請至電 （刪除） 或以電郵至 （刪除） 與 （刪除） 聯絡。

祝
工作愉快

行政總監

（已簽署）

黃慧筠敬上
二零零九年十一月二十七日

AIDS CONCERN 關懷愛滋

S0089

附件一：「關懷愛滋」就個人資料(私隱)條例諮詢的回應

以下是「關懷愛滋」就諮詢文件提出的主要建議的回應：

建議 1：敏感個人資料

諮詢問題

(a) 是否需要限定在指定的情況下才可收集、持有、處理和使用敏感個人資料，藉以爲該等資料提供更佳的保障；以及

(b) 若然，上文第3.08至3.14所載的可考慮規管制度，包括敏感個人資料涵蓋的範圍、相關的規管措施、制裁和不溯既往的豁免或過渡性安排的需要，是否恰當。

關懷愛滋意見

問題(a)

是。

建議一

修例列明愛滋病感染狀況屬於敏感個人資料。

建議二

愛滋病感染狀況等敏感個人資料的收集、持有、處理和使用，必須與其目的有適當的、必要的、合符比例的關係。

說明

我們認爲愛滋病感染狀況資料的涉露，極容易引起對愛滋病感染者的歧視性行爲。故此，愛滋病感染狀況等敏感個人資料的收集、持有、處理和使用，必須與其目的有適當的、必要的、合符比例的關係。

問題(b)

我們贊成在3.09指定的情況以外，禁止敏感資料的收集、持有、處理和使用。

愛滋病感染狀況資料的涉露所引起的歧視性行爲，在醫護環境中似乎十分普遍。很多時候除了主要負責某病例的醫護人員，其他不須負責該病例的醫護人員、負

責收費、清潔的工作人員都會從電腦、書面資料或口傳的情況下知道病人的健康狀況，我們收到多宗愛滋病病毒感染者因不必要的狀況涉露而受到歧視的個案。茲以實例說明：

實例一

一名愛滋病病毒感染者在街上暈了撞穿頭，由救護車送去去急症室，他告知救護員自己是感染者，傷口得到處理之後，醫院的收銀員只將收據放在坐著病人的腳旁，而當時唯獨他得到此待遇，令病人感覺到該收銀員似乎不願意和病人有直接接觸，有理由相信收銀員已由他人口中得知病人的身份。

實例二

一個感染者病發入院，在病床上時，有清潔人員在旁揶揄他有愛滋病，討論什麼是愛滋病，令到他有理由相信清潔人員也得知病人身份。

建議三

修例列明僱主不能要求求職者或僱員透露愛滋病感染狀況。

說明

事實上，愛滋病病毒並不影響工作能力，《國際勞動組織關於愛滋病與勞動世界的實施準則》指出，僱主不應該在招聘階段要求披露愛滋病病毒感染狀況（準則8.1）；僱主不能爲購買集體醫療保險而要求僱員進行愛滋病病毒測試，而僱員提供的感染狀況資料必須絕對保密（準則8.2）。我們曾收到一些愛滋病病毒感染者的個案，指求職時被要求以書面披露感染者狀況，簽寫同意書接受體檢或讓僱主查閱其醫療紀錄。這些求職者通常都不會被邀請參加第二輪面試或被錄用；有些僱員更被解僱。

建議2：規管資料處理者及分判活動

關懷愛滋意見

直接規管阻嚇性較強

建議3： 個人資料外洩通報機制

關懷愛滋意見

近來發生多綜病人資料外洩事件，關懷愛滋贊成訂立自願性的個人資料外洩通報機制。公署在4.39建議了發給受事件影響人士，我們認爲在通報中應加入當時資料使用者和公署已進行或將進行的跟進措施。

建議5：在第66條下爲資料當事人提供法律協助

關懷愛滋意見

贊成爲受屈資料當事人提供法律協助，同意公署5.11-13所列出的好處。

建議6：向受屈的資料當事人判給補償

關懷愛滋意見

贊成授權私隱專員以調解的方法處理私隱投訴。投訴人可要求被投訴人道歉、解釋或作出金錢/非金錢補償。

說明

調解是一個方便、能夠提高成本效益的機制。在香港民事司法制度改革下，法庭亦鼓勵訴訟雙方通過自願調解的方法解決爭議。賦予私隱專員調解的能力不會將私隱專員變成一個處罰機構，只會更加彰顯民事司法制度改革所推廣的精神。故此，並不存在法改會於1994年8月發出的《保障個人資料的法律改革報告書》中所說，賦予保障資料機構裁定給予補償的權力，並把執法和處罰的職能一併歸於單一機構的現象。

建議7：把違反保障資料原則訂爲罪行

關懷愛滋意見

同意6.04中建議把某些嚴重的違規行爲或做法，訂爲刑事罪行

建議8：在未經授權下取得、披露和出售個人資料

關懷愛滋意見

贊成把在未經資料使用者同意下，取得並披露個人資料，從中取利或作惡意用途的行爲，訂爲罪行。其他則沒有意見。

建議9：就同一事實重複違反保障資料原則

關懷愛滋意見

原則上同意對屢犯的資料使用者加強懲罰

建議11：重複違反執行通知

關懷愛滋意見

原則上同意對屢犯的資料使用者加強懲罰

完

S0090

香港地產建設商會

THE REAL ESTATE DEVELOPERS ASSOCIATION OF HONG KONG

By fax and post

27 November 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Central
Hong Kong
Attention: Miss Joanna C. H. Choi

Dear Ms. Choi

Public Consultation on the Review of the Personal Data (Privacy) Ordinance

We thank you for your letter of 28 August and wish to advise that we have no comment on the subject consultation.

Yours sincerely

(Signed)

Louis Loong
Secretary General



27/11/2009 16:54

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Comments from the Vocational Training Council on the Consultation Document on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir/Madam,

Comments from the Vocational Training Council on the Consultation Document on Review of the Personal Data (Privacy) Ordinance

On behalf of the Vocation Training Council (VTC), I wish to give our comments on the two proposals contained in the Consultation Document on Review of the Personal Data (Privacy) Ordinance as follows:

1. Re. Proposal No. 3: Personal Data Security Breach Notification

The VTC has no objection to the institution of a voluntary breach notification system in Hong Kong. We look forward to the issue of the relevant guidelines for implementation.

2. Re. Proposal No. 18: Fee Charging for Handling Data Access Requests

We agree it is desirable to have a fee schedule for handling data access requests. However, the fees charge proposed for processing the requests appears to only take into account the resources expended by clerical staff, when in fact such processing also requires input from staff above clerical grade. The resources of such involvements should be factored in when working out the proposed charge.

Please feel free to contact Mr. Evan Ho (deleted) , Human Resources Officer of Human Resources Division, VTC, if you need more information on our comments.

Regards

Kenny Woo

S0091

for Head/Human Resources Division
Vocation Training Council

S0092

丁毓珠 銀紫荊星章 太平紳士
東區區議會主席

Ting Yuk-Chee, Christina SBS, JP
Chairman
Eastern District Council

致：政制及內地事務局 (第4組)

傳真及電郵文件

檢討「個人資料(私隱) 條例」的諮詢文件之個人意見

「私隱條例」在香港已生效10多年，現行的私隱條例可以已不能滿足市民對個人私隱的保障要求，況且時代進步，科技日新月異，保障個人資料亦要面對好多挑戰。所以，檢討有關的條例，作出適時的修訂，以配合社會嘅的進步發展，我也同意是有需要的。

今次諮詢文件內提出40多項建議，檢討範圍包括，敏感個人資料、加強資料保安、擴大私隱專員職能，以及建議把惡意披露他人資料列爲刑事罪行等。本人就有關主要建議，提出一些個人意見。

1. ***敏感個人資料：***

a. 個人資料，例如DNA排序、瞳孔、掌紋及指模之類，獨一無二，不能隨意改變的特徵，當然要小心處理及受到嚴格規管。因爲無論收集這些資料有多少，或作任何特定用途，都係屬於個人資料，都應受到保護。 雖然，有專家話，所搜集嘅資料是無法回復的數據，但科技日日進步，難保他日能解破，市民的敏感個人資料會有機會外洩，及可能被一些不法分子作不正當用途。

b. 一般這些敏感個人資料，應該只會用作政府或國防系統。若是民用保安或考勤辨識系統，多爲提高管理效率。 這些用途，是需要提出證明，祇因沒有其他更好的資料作替代，並要給當事人自由選擇及同意，方能採用。

c. 近年洩露他人敏感個人資料或私隱的事件不斷增加，除上述之獨特資料外，有些市民亦希望將「病歷」、「住址」、「性傾向」等列入「敏感個人資料」範圍。由於不同國家及文化對『敏感資料』的定義不一，因此，個人資料的定義，不能把外國的法規照搬如宜，要根據香港情況作出修訂。 要分辨是否敏感資料，應要考慮有關資料一旦披露，會否令資料擁有者帶來極大損失，甚至聲譽，後果是否十分嚴重。 還有，病歷及一些特殊社會地位等資料，都可能會影響個人名聲，很多人都不想被彼露，亦需要留意。

d. 在現今文明法治的社會，市民對個人資料或私隱越趨關注。是有需要在應用生物辨識科技、私隱和發放方面取得平衡，保障公益之餘，亦要避免擾民，也不要防礙資訊自由等等。

2. *資料保安：*

a. 其實每個人都必須對個人資料的保安意識，時刻提高警覺。 因爲單靠現時收集資料的公司自律，做好保安措施，負上保護客人私隱的責任，未能完全確保資料受到保障。

b. 現時若遺失或泄露個人資料時，資料使用者未必會主動通知當事人，讓他們盡量減輕損失。所以，應設立個人資料通報機制，規定在個人資料外泄或遺失時，資料使用者必須通知私隱專員，應立即通知當事人及個人私隱專員。

3. *私隱專員的權力：*

就私隱專員的權力方面，我認爲刑事調查和直接檢控的權力，仍是由其他部門負責較好，可以發揮制衡之作用。比方現行之立法、執法及司法獨立進行，實有監察之效。

S0092

4. *罪行及制裁：*

a. 我贊成立法禁止資料使用者在未經同意下，將他人的個人資料在公開發放。例如：我相信很多市民都會認同的，就是「把直銷電話滋擾」之類的違規的1萬元罰則提高。現時電話推銷嘅滋擾情況可說極之嚴重，不理市民意願，繼續將個人資料作直銷用途。在自律不足及現行處罰條款太輕之下，我支持提高經營者在直銷活動中，不當使用個人資料罰則，以收阻嚇作用及保障市民權益。

b. 此外，當局還建議，將未經同意而披露他人私隱資料以牟取利益或作惡意用途，列爲刑事罪行，因爲這不但涉及個人利益，也可能對他人造成很大滋擾甚至傷害。如果發放者屬無心之失則不在刑事之列。但事實上，到底何謂惡意、何謂無心之失，根本難以定義，所以當局定要作出清晰界定、釐定相應罰則，否則便會引起更大的爭拗。其實，社會上對私隱的概念仍有很多模糊之處，不像偷竊或傷人，大家都有清楚明白犯法的界綫。而很多都是在生活小節和公司日常運作中不經意地發生，如果提出刑事化，就要先考慮會不會導致很多機構和市民在不知不覺中跌入法律陷阱，或大家顧忌多多，「斬腳趾避沙蟲」，疾礙正常運作。

5. *資料當事人的權利 及 豁免遵從私隱條例*

a. 還有，文件建議修例限制父母查閱未成年子女資料。就未成年人私隱所提出的，如父母代其未成年子女提出查閱要求乃不符合子女最佳利益，因而准許資料使用者拒絕有關要求，這一項卻不甚合邏輯，甚至有矯枉過正之嫌。一旦修訂付諸實行，持有資料的機構如認爲不符合當事人的最佳利益，可拒絕向當事人父母提供資料。 未成年的兒童和青少年，不僅未有法定行爲能力，心智也未成熟，其所作的判斷，隨時會有偏差，如是者，關係最密切的親人(父母親或監護人) ，所作的保護和輔導是最重要及有最大權責。就現時本港法例規定，所有涉及未成年人士的決定，皆須經過家長簽署同意。

b. 但我也認爲，政府可以修訂法例，允許社工或醫生等專業人士，在特定條件下，如爲了有效照顧未成年人的利益，協助父母或監護人盡早並確切了解其未成年子女的情況，交出有關資料。 若父母被懷疑虐待子女，或精神健康沒有足夠能力決定是否提供個人資料，學校和社會機構亦可拒絕提供。

S0092

總而言之，我認爲「保障個人資料私隱」，是十分敏感的課題，是需要詳細小心考慮，不能隨便謂有抗辯理由，就可取得或發放有關資料。在檢討時，應要保持文件所提的原則，即私隱權不是絕對的，必須與其他權利，以及公眾和社會利益取得平衡；也要平衡保障個人資料私隱和便利資訊，以及通訊科技持續發展。

同時，全球化亦對個人資料保障帶來挑戰，而且法律是有地域司法管轄權界限，不同地方有不同法律，若那些資料離境後便不再受本港法律保障。所以，有關保護條例的制定，不能祇看今天，也要考慮明天，因爲時代是不斷發展的，並要不時作出檢討。

在保障私隱資料方面，香港現時的做法，在亞洲區來說也算前列。所以，政府首要是加強教育宣傳；加強公民的道德意識。從根本做起，再配合法例修訂，相信會收到更良好效果。

（已簽署）

丁毓珠　謹上
2009年11月26日

S0093

27/11/2009 17:29

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject RE: Submission on the Consultation Document on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Mr. V. Chan

On behalf of HKCA we would like to submit the attached document in respond to the Review of the Personal Data (Privacy) Ordinance Public Consultation. Please do not hesitate to contact me at on issues related to the submission.

Kind regards

David Leong
Assistant Secretary General
The Hong Kong Construction Association, Ltd.

Submission on the Review of the Personal Data (Privacy) Ordinance Public Consultation.pdf

香 港 建 造 商 會
Hong Kong Construction Association

Submission on the Review of the Personal Data (Privacy) Ordinance Public Consultation

Over the past years the construction industry has implemented a series of measures aiming to enhance the safety and welfare of construction personnel. One of such measures known as Biometric Security Control System using HandKey Recognition System (HRS) has been developed and widely adopted by the industry for security control and provides attendance verification for wages payment of construction workers. The Handkey biometric data was selected over other biometric data such as fingerprints and retina because it was considered less privacy-invasive and would be least likely to cause any controversial issues. The multiparty development was extremely complex and the industry took well over 10 years to adopt the system that is currently providing site access security control for all of the 300,000 registered workers in Hong Kong. Realizing the benefits and contributions of the system, construction workers welcomed the system by engaging and accepting to use the system actively. Nowadays HRS becomes one of the standard administrative equipment in major construction sites in Hong Kong.

Security control for construction sites is important to prevent unauthorized or unqualified persons from entering into construction sites. Protection to public at large was no longer a nightmare for the Government, developers, consultants and contractors. Biometric security control provisions using HRS are now included as standard contract provisions in many public contracts. Previously many construction activities data requested by the Government were either hard to obtain or unavailable, but the system could now generate reports and information that are sought-after by many public administration departments such as Labour Department and Construction Workers Registration Authority.

The Commissioner's July ruling to disallowed the practice of using "Fingerprint Data for Attendance Purpose" has cast doubts over the legitimacy of HRS and has sparked off serious concerns on the use of HRS in construction sites. Subsequently, we have met with representatives of the Office of the Privacy Commissioner for Personal Data to explore the construction industry's practice in using biometric devices in particular the HandKey Recognition Systems that are commonly used in construction sites for security control of workers and personnel. Your office did not give any conclusion on

the legitimacy on HRS developed and used by the construction industry.

Based on the given advices, a number of feasibility studies are currently being carried out. Contractors would advise to modify the specifications of their existing hardware and software aiming to resolve the technical ambiguities that resulted from the Commissioner's rulings. However there is no guaranteed that the re-developed HRS could prevail under the scrutiny of the Personnel Data (Privacy) Ordinance.

Our views on the current consultation are:

1) HRS has been developed and widely adopted and accepted by construction workers for many years. This is a norm of the construction industry and should be "accepted practices" under the Ordinance.

2) The Ordinance needs to be very specific with sufficient detail to inform all stakeholders, in particular workers who should be aware of their own obligations and rights to avoid any unnecessary arguments and non productive administration procedures that have the potential of damaging the harmony between workers, their direct employers and Main Contractors.

3) The Ordinance must allow ample time for any proposed changes to the existing practice and system. Any modifications to the current way of working and site access control system will involve considerable financial and social costs.

We believe the construction industry has demonstrated commitments to foster safe and legitimate environments for construction practitioners and that infringement of privacy is not an issue. Considerable efforts by the industry have been devoted in the past years to tackle the problems of low volume of works and aging of construction workers in Hong Kong. The industry had already taken thoroughly steps to administrate and controls to protect privacy of construction personnel and therefore do not wish to engage in extended and unnecessary added measures for the Personnel Data (Privacy) Ordinance.

The Hong Kong Construction Association, Ltd.
15 November 2009

S0094

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)



30/11/2009 00:36

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject pdpo_consultation

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

就今次私穩條例的咨詢，我們有以下強烈要求立法:

(1)禁止稅務局使用市民的身份證號碼作為檔案編號的組成；

(2)禁止教統局使用學生的香港出世紙號碼、香港身份證號碼 或 簽證身份書號碼作為學生編號；因不少教育服務承辦商或網上學習提供者未得學童或家長同意，將學生編號成為登入編號或登入密碼；同時這些服務承辦商或網上學習提供者亦同時收集了學童的不少個人資料，如出生日期，住址，電話及電郵地址，成為一個身份證資料庫，缺乏有效之法律監管。另有情況是學童中有害群之馬，偷偷抄錄同學的手冊上的個人資料，用作不法(軌)之用，.....?!

(2) 現時不小NGO 、工會、私家醫生或商營醫療集團在未得市民的同意下，順手捻來亦濫用香港出世紙號碼、香港身份證號碼 或 簽證身份書號碼作為會員編號或診証編號。同時該等資料收集者亦同時收集不少服務使用者的個人資料，如出生日期，住址，電話及電郵地址，成為一個身份證資料庫，缺乏有效之法律監管。建議立法可讓樣服務使用者有權選擇在不影響生命尤關的情況—下，不提供完整的個人資料；例如只提供出生年份及立法不准使香港出世紙號碼、香港身份證號碼 或 簽證身份書號碼作為任何用途的編號！。

(3) 禁止任何人未得當事人同意下，在互聯網或任何電子媒體或傳訊工具散發某人的照片或個人資料，違者當受刑事檢控及監禁。

ZH
30-11-2009

S0096



29/11/2009 00:07

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject 檢討《個人資料（私隱）條例》的公眾諮詢

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

你好!本人工作是經常到客戶辦公室,每次當工廈保安員要求出示身份證時我都好合作出示登記,但久而久之,心想，他們登記後把我的資料會怎樣處理呢?一些有規模的大廈我還可放心，因爲我曾經去過一些大廈，保安員是一些外籍員工（尼泊爾）人，當然還有香港人，但我看見保安員爲入大廈的探訪者登記身份證時那本登記簿每個探訪者都能看見之前登記過的人的資料，還有，不是信不過那些外籍保安員，而是擔心我的資料會否被人偷取作其他用途，因政府宣傳都有提醒市民身分證是條鎖匙，不應除便透露別人，但工作關係-有辦法罷了，但本人想提出一點是，保安公司會怎樣確保探訪者的資料和有否立法保安公司處理登記後的資料呢?還有政府會有定期ｃｈｅｃｋ保安公司的處理手法呢？謝！

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

S0097

27 November 2009

By E-mail

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Central, Hong Kong

Dear Sirs,

Public Consultation on
Review of the Personal Data (Privacy) Ordinance

With reference to the Consultation Document on Review of the Personal Data (Privacy) Ordinance released on 28 August 2009, I enclose the ***PCPD's Submissions to the Consultation Document on Review of the Ordinance*** for your action.

Yours faithfully,

(Signed)

(Roderick Woo)
Privacy Commissioner for Personal Data

Encl.

S0097

PCPD's Submissions

To

Consultation Document on Review of the Personal Data (Privacy) Ordinance

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Contents:

		Page No.
I.	Purpose	1
II.	PCPD's Response to the Consultation Document	2
	Sensitive Personal Data	**2**
	Proposal No. 1 : Sensitive Personal Data	2
	Data Security	**10**
	Proposal No. 2 : Regulation of Data Processors and Sub-contracting Activities	10
	Proposal No. 3 : Personal Data Security Breach Notification	16
	Enforcement Powers	**20**
	Proposal No. 4 : Granting Criminal Investigation and Prosecution Power to the PCPD	20
	Power to Search and Seize Evidence	
	Power to Call Upon Public Officers for Assistance	
	Proposal No. 5 : Legal Assistance to Data Subjects under Section 66	24
	Proposal No. 6 : Award Compensation to Aggrieved Data Subjects	24
	Offences and Sanctions	**27**
	Proposal No. 7 : Making Contravention of a Data Protection Principle an Offence	27
	Proposal No. 8 : Unauthorized Obtaining, Disclosure and Sale of Personal Data	27
	Proposal No. 10 : Imposing Monetary Penalty on Serious Contravention of Data Protection Principles	27

Proposal No. 9 : Repeated Contravention of a Data Protection Principle on Same Facts 30

Proposal No. 11 : Repeated Non-compliance with Enforcement Notice 30

Proposal No. 12 : Raising Penalty for Misuse of Personal Data in Direct Marketing 31

Rights of Data Subjects..... 37

Proposal No. 13 : Third Party to Give Prescribed Consent to Change of Use of Personal Data..... 37

Proposal No. 14 : Parents' Right to Access Personal Data of Minors..... 43

Proposal No. 27 : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship..... 45

Enhancing the Effectiveness of Ordinance..... 47

Proposal No. 20 : Circumstances for Issue of an Enforcement Notice 47

Proposal No. 21 : Clarifying Power to Direct Remedial Steps in an Enforcement Notice 53

Proposal No. 22 : Removing the Time Limit to Discontinue an Investigation..... 53

Proposal No. 23 : Additional Grounds for Refusing to Investigate 54

Annex 2 to the Consultation Document – Proposals Not to be Pursued..... 60

Revamping Regulatory Regime of Direct Marketing..... 60

Internet Protocol Address as Personal Data..... 63

Territorial Scope of the Ordinance..... 65

Public Interest Determination..... 68

Public Domain Exemption..... 71

Power to Search and Seize Evidence..... 72

Power to Call Upon Public Officers for Assistance..... 72

Power to Conduct Hearing in Public..... 72

Time Limit for Responding to PCPD's Investigation/Inspection Report..... 73

Annex 3 to the Consultation Document – Miscellaneous Proposed Amendments to the Ordinance..... 74

Proposal No. 32 : Power to Obtain Information to Verify a Data User Return..... 74

Proposal No. 36 : Definition of Crime under Section 58..... 75

Other Proposals..... 78

III. Schedule..... 79

I. Purpose

1.1 On 28 August 2009, the Constitutional and Mainland Affairs Bureau (CMAB) released the Consultation Document on Review of the Personal Data (Privacy) Ordinance ("the Ordinance").

1.2 The review was initiated by the Privacy Commissioner for Personal Data (PCPD) in June 2006. An internal Ordinance Review Working Group was formed to assess the adequacy of protection of personal data privacy. After a year and a half's work, the Working Group completed its review and presented to the Government in December 2007 more than 50 amendment proposals and issues of privacy concern.

1.3 The Government has taken on board most of the proposals made by the PCPD. In order to let the public know more about the issues before making their submissions, the PCPD published a paper entitled "PCPD's Information Paper on Review of the Personal Data (Privacy) Ordinance" ("the Information Paper") on 9 September 2009. The Information Paper has been uploaded to PCPD's web-site[1].

1.4 This Submission sets out PCPD's response to various amendment proposals made in the Consultation Document. Where appropriate, specific references are made to the relevant materials contained in the Information Paper. In reading this Submission, readers are strongly encouraged to refer to the Information Paper for background materials.

Office of the Privacy Commissioner for Personal Data
November 2009

[1] http://www.pcpd.org.hk/english/review_ordinance/files/Odnreview_Information_Paper_e.pdf

II. PCPD's Response to the Consultation Document

2.1 Most of the proposals as set out in the Consultation Document had its origin in PCPD's 2007's proposals to the Government, which were intended to afford greater protection to personal data privacy. The Government's proposals even though more moderate and conservative than those made by the PCPD should still on the whole achieve the same objective. Some of these proposals deal with matters of significant privacy impact while others seek to strengthen the enforcement power of the PCPD and improve the efficacy of the regulation of the Ordinance. New mechanisms to deal with issues of public concern are also introduced. All these aim at bringing about an update piece of legislation that best suits the public in the protection of personal data privacy.

Sensitive Personal Data

Proposal No. 1 : Sensitive Personal Data

2.2 This proposal was originally made by the PCPD[2] to prohibit the collection, holding, processing and use of specific categories of personal data (to be defined as sensitive personal data) except under prescribed circumstances. The Administration has modified PCPD's original proposal by singling out only biometric data as sensitive personal data as a start.

Whether there is a need to accord better protection to sensitive personal data

2.3 Amending the Ordinance to give special treatment for sensitive personal data is in accord with Article 8 of the EU Directive 95/46/EC *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* thereby enabling the Ordinance to pass the EU adequacy test. It is a pre-requisite under the EU Directive that member states must ensure similar level of protection of personal data in the country to which the data will be transferred. Hence, adoption of the EU approach will enable uninterrupted exchange of personal data with the EU member

---

2 See PCPD's Proposal No. 1 at p.1 in the Annex to the Information Paper.

states. This is conducive to Hong Kong's prosperous growth in trade and business activities.

2.4 The PCPD therefore recommends that the protection level of special categories of personal data should be brought at par with the standard stipulated in the EU Directive 95/46/EC.

Coverage of sensitive personal data

2.5 Article 8 of the EU Directive provides that "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

2.6 The PCPD recommends the adoption of the categories specified in Article 8 with modifications. The PCPD suggests that "political opinion" and "religious or philosophical beliefs" be replaced by "political affiliation" and "religious beliefs and affiliations" respectively.

2.7 The PCPD is of the view that special care is warranted in the handling of special categories of personal data in view of the gravity of harm that may cause the data subjects if such data are mishandled. In anticipation of the eventual implementation of electronic health record sharing system where massive sensitive health records are kept in databases for use and access, the PCPD considers that more stringent control and prudent practice are required in relation to the handling of medical data.

2.8 The PCPD also supports the inclusion of biometric data as sensitive personal data. Biometric data can be considered sensitive since they are fixed and, unlike a password or a PIN, cannot be reset once they have been inappropriately released. They are very personal and private because they are information about an individual's physical self. Biometric data, such as fingerprints and genetic data, should be accorded higher protection. Biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent, and that biometric data could reveal other sensitive personal information, such as information about a person's health, racial or ethnic origin or religious beliefs. They can provide the

basis for unjustified discrimination.

2.9 Recently, as a result of advancement in technology, there has been a proliferation in the use of biometric devices, such as fingerprint scanners, for identification/verification purpose. In such a system, a biometric sample is taken from an individual. Data from the sample are then analyzed and converted into a biometric template, which is stored in a database or an object in the individual's possession, such as a smart card. Later, biometric samples taken from the individual can be compared to the stored biometric template to identify the individual or to verify the individual's identity.

2.10 In July 2009, the PCPD published a report[3] concerning the collection and recording of employees' fingerprint data for attendance purpose by a furniture company. In that case, the PCPD found that the collection of employees' fingerprint data by the company for monitoring attendance purpose was excessive and the means of collection was not fair in the circumstances of the case and consequently the company's practice was in contravention of Data Protection Principle ("DPP") 1(1) and DPP1(2) in Schedule 1 of the Ordinance.

2.11 In the light of the experience in handling complaints lodged with the PCPD involving the collection of personal data by fingerprint scanners, the PCPD arrived at the following general views:-

(a) First and foremost, if the act does not involve the collection of "personal data", it is outside the jurisdiction of the Ordinance. For example, there is a fingerprint recognition system that can convert certain features of the fingerprint into a unique value and store it in the smart card held by the employee (the employer does not hold a copy of the data). For verification, the employee needs to put his finger and the smart card on the recognition device. The system merely compares and matches the value in the smart card with the fingerprint features presented each time and the employer has no access to the personal data concerned. As the employer has not collected employees' fingerprint data or their value, he has not collected any "personal data" as defined in

---

3 Available at http://www.pcpd.org.hk/english/publications/files/report_Fingerprint_e.pdf

the Ordinance;

(b) If the fingerprint recognition system involves the collection of personal data, employers should be mindful not to collect fingerprint data purely for attendance purpose. In many other instances, there exist less privacy intrusive alternatives which can achieve the purpose of monitoring attendances. Whether or not features of the fingerprints are converted into value, such an act amounts to collection of excessive personal data and contravenes the requirements of DPP1(1), unless the genuine consent of the data subject has been obtained;

(c) If a data subject provides his fingerprint data voluntarily for a particular purpose, the application of the DPPs should not override the data subject's right to information self-determination. The PCPD will respect his consent if given voluntarily and explicitly;

(d) Fingerprint data should not be collected from children of tender age, regardless of any consent given by them, for reason that they may not fully appreciate the data privacy risks involved;

(e) Before collecting employees' fingerprint data for attendance purpose, employers must offer employees a free choice in providing their fingerprint data, and they must be informed of the purpose of collection and given other less privacy intrusive options (e.g. using smart cards or passwords);

(f) The means of collecting employees' fingerprint data must be fair. Employees should be able to give their consent voluntarily without undue pressure from the employers and should have the choice of other options; otherwise there may be contravention of the requirements of DPP1(1) and DPP1(2).

2.12 There are arguments that the data stored in a fingerprint recognition system are not personal data because:-

(a) the stored biometric data are just meaningless numbers, and

therefore are not personally identifiable information; and

(b) a biometric image cannot be reconstructed from the stored biometric template.

2.13 In relation to the argument in 2.12(a), while the numbers may not be able to identify an individual when considered alone, they are capable of identifying an individual when linked to other personal identification particulars. Similar examples are identity card numbers, credit card numbers and mobile phone numbers. The purpose of a fingerprint recognition system is to identify or verify the identity of an individual. The templates will ultimately be linked to identify a person. Hence, no matter how the templates are generated (in the form of numerical codes or otherwise), they will be considered "personal data" when combined with other identifying particulars of a data subject.

2.14 With respect to the claim that a fingerprint image cannot be reconstructed from the stored biometric template, Information and Privacy Commissioner of Ontario states in a paper entitled "Fingerprint Biometrics: Address Privacy Before Deployment"[4] issued in November 2008 the different view taken in some recent scientific works[5]:-

> *"Until recently, the view of non-reconstruction was dominant in the biometrics community. However, over the last few years, several scientific works were published that showed that a fingerprint can, in fact, be reconstructed from a minutiae template. The most advanced work was published in 2007 by Cappelli et al. The authors analyzed templates compatible with the ISO/IEC 19794-2 minutiae standard. In one test, they used basic minutiae information only (i.e. positions x, positions y, and directions). In another test, they also used optional information: minutiae types, Core and Delta data, and proprietary data (the ridge orientation field in this case). In all the tests, the authors were able to reconstruct a fingerprint image from the minutiae template. Very often, the reconstructed image had a striking resemblance with the original image. Even though this reconstruction was only*

4 Available at http://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf

5 See p.7 of the paper

approximate, the reconstructed image was sufficient to obtain a positive match in more than 90% of cases for most minutiae matchers."

2.15 The paper goes on to discuss the potential repercussions for security and privacy of fingerprint minutiae systems:-

"The potential repercussions of this work for the security and privacy of fingerprint minutiae systems are as follows:

The fingerprint image reconstructed from the minutiae template, known as a "masquerade" image since it is not an exact copy of the original image, will likely fool the system if it is submitted.

A masquerade image can be submitted to the system by injecting it in a digital form after the fingerprint sensor.

A malicious agent could also create a fake fingerprint and physically submit it to the sensor. The techniques of creating a fake fingerprint are inexpensive and well-known from the literature.

The ability to create a masquerade image will increase the level of interoperability for the minutiae template. The masquerade image can be submitted to any other fingerprint system that requires an image (rather than a minutiae template) as an input. No format conversion of the minutiae template would be required. Moreover, the minutiae template can be made compatible even with a non-minutiae fingerprint system (these systems are rare, however)."

2.16 The Australian Law Reform Commission ("ALRC") sees the need of extending the definition of "sensitive personal data" to cover biometric information. The ALRC made the proposal in its Report 108 – For Your Information: Australian Privacy Law and Practice[6] issued in August 2008. In recognizing that requiring consent to collect all

[6] Available at http://www.austlii.edu.au/au/other/alrc/publications/reports/108/6.html#Heading283

biometric information may be impracticable, the ALRC recommended to amend the Privacy Act to include the following in the definition of "sensitive personal data":-

(a) biometric information collected for the purpose of automated biometric verification or identification; and

(b) biometric template information.

2.17 The above are regarded as the most serious privacy concerns around the handling of biometric information and the recommendation is intended to address such concerns.

2.18 In October 2009, the Australian Government released its first stage response to the ALRC report[7]. The Australian Government recognized the importance of attributing a higher level of protection to personal information which is sensitive in nature and agreed that biometric information has similar attributes to other sensitive information and it is desirable to provide it with a higher level of protection. Given the broad nature of what can be considered biometric information, the Australian Government considered that the definition should make clear that the additional protections should only extend to that biometric information which is specifically being collected to identify or verify an individual through biometric processes.

Requirements in handling sensitive personal data

2.19 The PCPD supports the proposed exceptions to special treatment of sensitive personal data as stipulated in paragraph 3.09 of the Consultation Document.

Sanction for contravention of requirements

2.20 In view of the sensitive nature of the data and the degree of harm that could result in mishandling the data, a more stringent control should be imposed. The PCPD supports the proposal to make it an offence for any person who without reasonable excuse, fails to comply with the prescribed requirements governing the handling of sensitive personal

---

7 Available at http://www.pmc.gov.au/privacy/alrc.cfm

data. Since the proposed provision is new to the public, the PCPD suggests that any penalty should be restricted to the imposition of a fine but not a custodial sentence.

Grandfathering

2.21 The PCPD considers that a data user, who has collected any sensitive personal data before the commencement date of the new requirements, may continue to hold the data already collected. However, any subsequent use of the data should follow the new requirement by seeking the prescribed consent of the data subject.

2.22 To enable the public to become familiarized with the new requirements, the PCPD supports a transitional period for the implementation of the new requirements. It should however be borne in mind that fixing an unduly long transitional period will defeat the purpose of putting in place the new protection to sensitive personal data. The PCPD takes the view that the transitional period to be imposed should not be longer than twelve months.

Other comments

2.23 The PCPD urges the Government to reconsider its decision to single out biometric data from the seven types of "sensitive personal data" suggested by the PCPD. In particular, the PCPD asks the Government to seriously consider the inclusion of a person's physical and mental health condition as "sensitive personal data".

Data Security

3.1 With the rapid development of technology, the storage and disclosure of personal data often raise privacy concerns. Measures to ensure sufficient control and security are necessary in view of the increase of data losses and leakage incidents.

Proposal No. 2 : Regulation of Data Processors and Sub-contracting Activities

Whether a data user should be required to use contractual or other measures to secure its data processor's compliance with the relevant obligations under the Ordinance

3.2 This proposal was originally made by the PCPD[8] to the Administration. It is proposed to impose specific obligations on a data user, who transfers personal data to a data processor for holding, processing or use, to employ contractual or other means to require its data processor and any sub-contractors to take all practicable steps to ensure the security and safekeeping of the data, and to ensure that the data are not misused and are deleted when no longer required.

3.3 The PCPD expects a data user, in order to comply with the proposed specific obligation, to select a contractor of reasonable standard and quality that can provide adequate security of the personal data. The terms of the service agreement shall include the following provisions:-

(a) prohibition against any use or disclosure of the personal data by the contractor for a purpose other than the purpose for which the personal data are entrusted to it by the data user;

(b) security measures required to be taken by the contractor to protect the personal data entrusted to it, including imposing contractual obligations on the contractor to comply with the data protection principles of the Ordinance;

(c) timely return or destruction of the personal data when they are no

---

8 See PCPD's Proposal No. 2 at p.8 in the Annex to the Information Paper.

longer required for the purpose for which they are entrusted by the data user to the contractor;

(d) absolute or qualified prohibition on the contractor against sub-contracting the service;

(e) immediate reporting of any sign of abnormalities or security breaches by the contractor; and

(f) measures required to be taken by the contractor to ensure that its relevant staff will carry out the security measures and comply with the obligations under the service agreement regarding the handling of personal data.

3.4 It is normal business practice for a data user to enter into a contractual relationship with its data processors. Introduction of specific obligations on organizations to enter into the contractual terms for the protection of personal data with their contractors should not disrupt normal business activities. The contract may serve as evidence to show the data user's compliance with the requirements of the Ordinance in case a complaint is brought by a data subject against the data user for infringement of personal data privacy in relation to the act or practice of its data processing agent.[9]

3.5 It is important to note that the contractual requirement above is insufficient to effectively regulate the activities of the data processors. While the data processors may be liable to the data users under their contracts, their conduct may not be regulated by the Ordinance.

Direct or indirect regulation on data processors

3.6 It is unsatisfactory that the Ordinance does not regulate the handling of personal data by data processors as the definition of "data user" does not apply to them pursuant to section 2(12)[10]. Some of the data leakage

---

9 A data user may be liable for any acts done by its agent by virtue of section 65 of the Ordinance. According to section 65(2), any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated as done or engaged in by that other person as well as by him.

10 Section 2(12) of the Ordinance provides "*A person is not a data user in relation to any personal*

incidents show that very often the cause of the incidents was the lack of sufficient security safeguards on the part of the data processors[11]. Therefore, the PCPD finds that direct regulation on data processors is essential.

3.7 Paragraph 4.13 of the Consultation Document asserts the difficulties in defining the generic obligations for data processors because many Internet-related businesses will be unaware of the nature of the data, including the purpose for which they were originally collected. The PCPD wishes to point out that the proposal only requires these Internet-related businesses to ascertain the purpose for which they collected the data from the users of their Internet-related services. The proposal does not require them to ascertain the original purpose for which the data were collected by the users of the services.

3.8 The PCPD considers that, since the Internet-related businesses obtain personal data in the course of their business activities, the use of the personal data so obtained should be confined to the purpose of provision of the Internet-related services. Any use other than the original or a directly related purpose should be prohibited. To use the example of a social networking site given in paragraph 4.13 of the Consultation Document, the purpose for which any personal data were entrusted to the provider of the social networking site by its users should be the facilitation of the social networking. The provider does not have to ascertain the original purpose for which the users collected the personal data, even though the users may have posted up personal data in the social networking site for a different purpose.

3.9 The PCPD considers that the misunderstanding may be addressed by making appropriate amendments and/or additions to DPP3, so that the expression *"the purpose for which data were to be used at the time of collection"* in DPP3(a), in so far as it applies to the data processors, shall mean *"the purpose for which the data were entrusted to the data processor"*. The PCPD stresses that the concern can be addressed by

---

data which the person holds, processes or uses solely on behalf of another person if, but only if, that the first-mentioned person does not hold, process or use, as the case may be, those data for any of his own purposes".

[11] See PCPD's investigation report on the Independent Police Complaints Council, available at (http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf).

appropriate drafting of the amendments to the Ordinance instead of rejecting the whole idea of direct regulation.

3.10 Paragraph 4.15 of the Consultation Document also raises concerns that ISPs and web-based service providers might have problem to comply with the relevant DPPs as typically they have no knowledge of whether the data they are holding are personal data. The PCPD appreciates that inspection of each piece of communication processed by ISPs and web-based service providers may be technically and/or practically impossible. On the other hand, it is inevitable that personal data are being transmitted in those communication, and the risk of any data privacy breach on the part of the ISPs and web-based service providers is not merely hypothetical or remote.

3.11 The PCPD is of the view that the ISPs and web-based service providers are not required to examine each piece of information they process in order to find out whether it contains personal data, what kind of personal data they are, and to provide tailor-made security measures for each set of personal data. As responsible and prudent ISPs and web-based service providers, they should treat the information they obtained in the provision of the relevant services as containing "personal data". Similar to the example of a social networking site as discussed above, the purpose for which any personal data were entrusted to the ISPs and web-based service providers by their users should be the facilitation of the services, e.g. transmission of emails, rather than the purpose for which the users collected the personal data. As such, the ISPs and web-based service providers should be able to ascertain their obligations under the Ordinance, such as the restrictions on further use of the data, adequacy of data security, duration of data retention, etc.

3.12 Paragraph 4.16 of the Consultation Document raises a concern about uncertainty. It gives an example of an advertising-funded webmail provider who might transmit personal data on behalf of the sender, store, forward and index personal data on behalf of the recipient and process the data on behalf of third parties for the purpose of targeting marketing messages. It seems the concern is that the ISP is uncertain as to whether it has to consider the purpose for which the personal data were entrusted by the sender or the purpose for which they were entrusted by

the webmail provider. The PCPD appreciates that, like a data user, a data processor may process the same piece of personal data for multiple purposes. As far as the ISP is concerned, the entrusting of the personal data contained in an email by the sender and that by the webmail provider should take place within a split second. Besides, the purposes for which the data were entrusted by the sender and the webmail provider should be the same, i.e. transmitting the email to the recipients for the sender. As such, the ISP should have no practical difficulties in ascertaining the purpose for which the personal data are entrusted to it. To comply with the proposed obligations, the ISP shall not use the personal data for any purpose other than for the purpose of transmission and should erase the personal data after the transmission unless it has an obligation to retain the data.

3.13 Paragraph 4.17 of the Consultation Document raises a concern that many Internet-related businesses whose business purpose is to facilitate access to data, e.g. a search engine that caches data, may be left uncertain as to what constitutes unauthorized access to personal data. In the example, it seems that the provider of the search engine, which only caches data on its own initiative, is not entrusted with any personal data, hence, should not fall within the definition of "data processor." Additionally, in the PCPD's view, the requirement of DPP4 provides for safeguard of personal data against unauthorized or accidental access, etc. in the course of their transmission or storage. The example of a search engine should not be a matter of concern under DPP4 because access to the information or data concerned is authorized by the search engine.

3.14 The PCPD believes that paragraphs 3.8 and 3.9 above have also addressed the concern raised in paragraph 4.18 of the Consultation Document.

What obligations should be imposed on data processors?

3.15 The PCPD supports the option stated in paragraph 4.14 of the Consultation Document to require the data processors to:-

(a) ensure the personal data will be used only for the purpose for which such data were so entrusted or for directly related purpose;

(b) take all reasonably practicable steps to ensure the security and safeguarding of the personal data under its custody; and

(c) take reasonably practicable steps to erase personal data no longer required for fulfillment of the purpose for which the personal data were so entrusted.

Whether it is appropriate and practical to subject different categories of data processors to different obligations

3.16 Paragraph 4.19 of the Consultation Document mentions that the Internet environment is fast-evolving and it is important that privacy laws do not inhibit the development of desirable new Internet-related services. It is suggested that, instead of directly regulating data processors in the field of Internet-related business, their obligations should be limited to adoption and observance of their own privacy policy relating to the use, security and retention of personal data, and any failure to observe the policy will be subject to the PCPD's enforcement action. In PCPD's view, data protection does not depend solely on the formulation of a comprehensive privacy policy. Besides, it is the statutory obligation of the PCPD to monitor and supervise compliance with the Ordinance. In discharge of his statutory obligation, the PCPD shall not solely rely on the discipline and good governance of the data processors and enforce the terms of the privacy policies dictated by the data processors. The PCPD is still unable to see a convincing justification for relaxing the requirements of data processors for Internet-related businesses exclusively.

3.17 It must be stressed that the introduction of obligations on the data users in sub-contracting activities should not obviate or substitute the need for those obligations proposed for the data processors. These obligations are separate and essential to ensure protection at all levels. The PCPD does not consider it sufficient protection for the public in relation to their personal data to simply rely on data users to regulate their contractors because the existing section 65(2) of the Ordinance already provides that a principal can be liable for the act of its agent. The gravity and recurrence of data leakage incidents have shown that direct regulation on

the data processors may be more effective to curb data leakage incidents by data processors.

Proposal No. 3 : Personal Data Security Breach Notification

3.18 This proposal was originally made by the PCPD[12] in responding to the series of personal data losses and leakage incidents which arouse grave public concerns. The PCPD supports the proposal that data users should be required to give security breach notifications in certain situations. The Administration considers it more prudent to start with a voluntary breach notification system so that they can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing onerous burden on the community.

3.19 The PCPD observes that agencies and organizations are storing increasingly vast amounts of personal data electronically, some of which are sensitive in nature. The leakage of such data may allow identity theft of the affected individuals. It is evident that electronic leakage of personal data, e.g. through the Internet, is difficult, if not impossible, to contain. By the time a complaint is made to the PCPD, the personal data could have been downloaded and retained by countless unauthorized users on the Internet. Therefore, an early response to data leakage is crucial for protecting electronically stored personal data.

3.20 In the circumstances, serious consideration should be given to a containment plan which data users are required to adopt in order to mitigate or reduce the damages that may cause to the data subjects. Apart from other remedial measures, data users should be required under certain circumstances to notify the affected individuals of the security breach as soon as practicable after occurrence of the breach. This enables the affected individuals to take steps to prevent misuse of their personal data.

3.21 Security breach notification may not have a direct effect in preventing data leakage, it minimizes the exposure of the data subjects to possible

---

[12] See PCPD's Proposal No. 51 at p.136 in the Annex to the Information Paper.

damage. This is particularly so when a significant number of data subjects are affected by the breach and where sensitive personal data are lost or stolen. The Independent Police Complaints Council (IPCC) data leakage incident[13] is a good example where sensitive personal data were leaked on the Internet and the affected individuals have to be notified in order that they may take steps to prevent any misuse of their personal data. In that case, the IPCC gave the notification voluntarily.

3.22 The PCPD has received data users' voluntary notifications from time to time. During the period from 1 April 2008 to 31 July 2009, the PCPD received a total of 44 data breach notifications from data users in both private and public sectors. Concerning Government departments and public bodies, for the aforesaid 16 months period, the PCPD has received 33 incidents of security breach covering in total personal data of 16,303 individuals.

3.23 After receiving a notification of security breach, the PCPD will carry out a compliance check by enquiring with the relevant data users, pointing out the apparent insufficiencies in their data security system and inviting the data users, where appropriate, to take remedial actions. In many cases, the data users take the initiative and respond by undertaking immediate actions to remedy the data security breach. In other instances, the data users seek guidance and directions from the PCPD to step up security measures so as to avoid repetition of similar incidents in future.

3.24 To illustrate how PCPD reacts, below is a compliance check case which was prompted by a security breach notification:

> *The data user in this case is an insurance company in Hong Kong. By its letter of September 2008, the company informed the PCPD that an electronic file containing personal data of over 1,000 customers had been wrongfully sent to an unintended recipient by email. The company had contacted the wrong recipient who confirmed that the file had been deleted. The staff responsible for the wrongful dispatch*

---

[13] PCPD's investigation report available at http://www.pcpd.org.hk/english/publications/files/IPCC_e.pdf

was given a written warning.

In response to the compliance check initiated by the PCPD, the company formulated an action plan to strengthen the data transmission security by password protection, file automation and encryption. The company also informed the PCPD that its audit department would conduct a special review of the company's data transmission process focusing on data privacy.

In October 2008, the company provided a written undertaking to the PCPD agreeing to step up measures in respect of the security of the personal data held by it and provide the PCPD with a copy of its internal audit report on data transmission process.

3.25 Although many overseas jurisdictions have not made data breach notification a mandatory requirement, their privacy reforms all call for adopting a mandatory approach. Locally, the frequently reported incidents of data losses, particularly associated with the widespread use of portable electronic devices, call for tighter control. In addition, the feedback obtained from the recent consultative activities suggests solid support to making it a mandatory requirement.

3.26 The Government has already put in place a voluntary notification mechanism for personal data leakage incidents for a period of time. In view of the vast amount of personal data being held by the public sector and having regard to the expectation from the community, it will be desirable to impose mandatory breach notification on the public sector as a start.

3.27 There are concerns that it may cause the private sector undue burden to comply with the proposed requirements. It should be noted that under the proposed mechanism, a data user is not required to notify every security breach. It is only in those cases where the security breach may result in high risk of significant harm to individuals or organizations that notification is required. The PCPD will issue guidelines on the circumstances that would trigger the notification as well as the

particulars to be contained in the notice.

3.28 To facilitate smooth implementation of security breach notification, the PCPD recommends that, similar to data user return, the PCPD should be given the power to specify by notice in the Gazette the class of data users to which the notification requirement applies. In making the determination, the PCPD may consider a number of factors including the amount of personal data held by the specific class of data user, the degree of sensitivity of the data as well as the risk harm to the data subjects as a result of a security breach. The proposed mechanism ensures a gradual process and a selective approach that will balance different interests within the community.

Enforcement Powers

4.1 In order to strengthen the enforcement powers of the PCPD, various proposals were made by the PCPD to the Government. The purpose of the below proposals was to enhance efficiency of enforcement and to cause deterrence to infringements of the Ordinance.

Proposal No. 4 : Granting Criminal Investigation and Prosecution Power to the PCPD
Power to Search and Seize Evidence (C.1 of Annex 2 to the Consultation Document)
Power to Call Upon Public Officers for Assistance (C.2 of Annex 2 to the Consultation Document)

4.2 These proposals were originally made by the PCPD.[14] The PCPD advocated that specific power be conferred on the PCPD to carry out criminal investigation and prosecution. The power to search and seize evidence and to call upon public officers for assistance are incidental powers necessary for facilitating criminal investigation.

4.3 Paragraph 5.03 of the Consultation Document mentions three grounds which PCPD has put forward to support the proposal of granting PCPD prosecution powers. They are:-

(a) the PCPD possesses first-hand information obtained in the course of its investigations and can investigate into suspected commission of an offence speedily;

(b) as the regulator, the PCPD is proficient in interpreting and applying the provisions of the Ordinance, and can assess the weight and relevance of the evidence in any given situation with ease and confidence; and

(c) to save time on referring cases to the Police, hence to help meet the statutory time limit to lay prosecution which is set at six months from commission of an offence.

---

[14] See PCPD's Proposal Nos. 8, 14 and 16 at p.27, 44 and 48 in the Annex to the Information Paper.

4.4 Apart from the above reasons, granting prosecution power to the PCPD will help avoid criticism of favouritism where the Police or other government departments are involved in the case as data user. In addition, it will avoid the duplication of efforts of the PCPD and the Police. It is because usually the PCPD will carry out preliminary enquiries such as taking a statement from the complainant in order to satisfy that there is a *prima facie* case of commission of an offence before referring the complaint to the Police for criminal investigation. When the Police take over the case, they will take statement from the complainant again. The duplication of effort is a waste of both time and resources.

4.5 The Consultation Document states at paragraph 5.06 that there could be "community concerns" if prosecution power is delegated to the PCPD. However, there is no further elaboration as to what those concerns were. On the other hand, there are many examples where statutory bodies are empowered to carry out investigations and institute prosecutions on their own, such as, the Vocational Training Council, the Employment Compensation Assistance Fund Board, the Construction Workers Registration Authority and the Security and Futures Commission (paragraph 5.05 of the Consultation Document refers).

4.6 The power and function of prosecution entail the due presentation of facts to the Court. It does not place the PCPD in a position to decide or judge the culpability of any data user. That power is, as always, reserved for the judiciary.

4.7 The PCPD does not agree with the statement in paragraph 5.08 of the Consultation Document that *"whether the PDPO can afford effective protection to personal data privacy hinges on the adequacy of penalty sanction, rather than on who the party responsible for initiating prosecution is."* In PCPD's view, effectiveness in investigation and prosecution process is also an important contributing factor to the enforcement of the Ordinance. While the Administration states that it has put forth in Chapter Six of the Consultation Document proposals to step up the sanctions provided for in the Ordinance, it is noted that of the six proposals made in Chapter Six, the Administration has not shown

support to four of them[15].

4.8 Paragraph 5.04 of the Consultation Document mentions that strong justifications are required for the prerogative of initiating criminal prosecution to be delegated to the PCPD. In this respect, it should be borne in mind that a member of the community has the common law right to prosecute an offence. A feature of the early common law was the notion that it was not only the privilege but also the duty of the citizen to preserve the king's peace and to bring offenders to justice. Hence, under the common law every citizen has exactly the same right to institute any criminal prosecution as the Secretary for Justice or anyone else, although section 14 of the Magistrates Ordinance empowers the Secretary of Justice to intervene and assume the conduct of the proceedings at any stage of the proceedings before the magistrate.

4.9 The PCPD's proposal will not prejudice the Secretary of Justice's discretion to prosecute. It is because the granting of prosecution power to the PCPD entails only the carrying out of the prosecution work and the discretion whether or not to prosecute is always reserved for the Secretary for Justice. It will be made explicit in the law that the PCPD's power to prosecute shall be subject to the consent of the Secretary for Justice.

4.10 It has also been raised that the low number of referrals and successful convictions in the past years does not justify granting the power to the PCPD. It should be noted that whether or not to prosecute or whether a prosecution results in successful conviction is not in the hands of the PCPD after the referral. As for the number of referrals, the figures are 8, 9 and 5 for the years 2006, 2007 and 2008 respectively.[16] It rises to 9 cases in 2009 (as at 5.11.09). The following reasons may account for the low figures of referrals and prosecutions:-

(a) Many complaints are lodged after the time bar for prosecution

---

[15] The proposals not supported by the Administration are Proposal No. 7 (Making Contravention of a Data Protection Principle an Offence), Proposal No. 9 (Repeated Contravention of a Data Protection Principle on Same Facts), Proposal No.10 (Imposing Monetary Penalty on Serious Contravention of Data Protection Principles) and Proposal No. 11 (Repeated Non-compliance with Enforcement Notice).

[16] Paragraph 2.11 of the Consultation Document.

which is prescribed under the Magistrates Ordinance as six months[17];

(b) The complainants prefer the cases to be handled by the PCPD rather than the Police. It is the policy of the PCPD that consent should be sought from the complainant before any referral is made to the Police; and

(c) Cases of infringement of the Ordinance are generally not considered a priority in the array of offences within the purview of the Police both in terms of seriousness and urgency.

4.11 On the other hand, there is a strong likelihood that if the following proposals put forth by the PCPD are taken on board by the Administration, the number of cases for prosecution will increase significantly:-

(a) The proposal to extend the time limit for laying information for prosecution from 6 months to 2 years will certainly increase the number of cases suitable for prosecution;

(b) The proposal to widen the discretion of the PCPD to issue enforcement notices will certainly result in an increase in the issuance of enforcement notices, the breach of which is an offence;

(c) The proposals to create the following new offences will result in an increase in the number of cases for prosecution:-

(i) Contravention against the new provision for dealing with "sensitive personal data" (Proposal No. 1);
(ii) Knowingly or recklessly obtaining personal data without consent from the data user and the disclosure or sale of the data so obtained to third parties (Proposal No. 8);
(iii) Repeated contraventions of the Ordinance on the same facts where the first infringement has resulted in the issuance of an Enforcement Notice (Proposal No. 9);
(iv) Contravention against the requirement for

[17] Section 26 of the Magistrates Ordinance

destroy/return/use of data under the new "mergers, acquisition and transfer of business" exemption under Part VIII (Proposal No. 24).

Proposal No. 5 (Legal Assistance to Data Subjects under Section 66)
Proposal No. 6 (Award Compensation to Aggrieved Data Subjects)

4.12 These two proposals were originally made by the PCPD[18] in order to assist aggrieved data subjects to obtain compensation from the data users for any damages suffered by reason of the latter's infringement of the requirements of the Ordinance.

4.13 Paragraph 5.18 of the Consultation Document states that the LRC Report had thoroughly discussed the appropriate body to determine compensation under the Ordinance and the LRC opined that conferring power on a data protection authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions. Also, it is not appropriate to adopt the Australian model which advocates settlement by conciliation. The power to determine the amount of compensation is part and parcel of the investigation power of the Australian Privacy Commissioner. Besides, there has already been put forth proposal No. 5 to assist aggrieved data subjects in seeking redress through civil remedy.

4.14 The PCPD would like to point out that the LRC's recommendation at that time was premised on the assumption that the Court would determine the appropriate amount of compensation upon the PCPD's certificate of contravention but ultimately no such arrangement has been introduced under the current provisions.[19]

4.15 Under the Australian Privacy Act, if conciliation fails to resolve a complaint, the Australian Privacy Commissioner may make a determination. In the determination, the Australian Privacy Commissioner may (a) make a declaration directing the respondent to take steps remedying the contravention; and (b) award damages to the

---

18 See PCPD's proposals Nos. 54 and 53 at p.142 and 144 in the Annex to the Information Paper.

19 See paragraph 16.72 of the Law Reform Commission Report on Reform of the Law Relating to the Protection of Personal Data issued in August 1995.

complainant. The PCPD may carry out the similar settlement by conciliation. Indeed, many of the cases handled by the PCPD are resolved by mediation.

4.16 Section 66 of the Ordinance is rarely invoked in court proceedings, possibly due to lengthy and costly litigation process, and the risk of having to pay the defendant's costs. To PCPD's knowledge, there is no award ever made by the Court on damages suffered by a data subject as a result of infringement of personal data privacy. There has been international criticism that the Ordinance does not provide a genuine remedy to the aggrieved data subjects. Proposal No. 6 will provide an aggrieved data subjects an alternative choice of seeking remedy in a simpler, quicker and more effective way.

4.17 Proposal No. 5 is not a direct solution and cannot replace Proposal No. 6. Due to resources constraint, not all aggrieved party will be granted legal assistance. According to the model of the Equal Opportunities Commission ("EOC") quoted in the Consultation Document, the relevant legislation empowers the EOC to accede to a request for legal assistance only if:-

(a) the case raises a question of principle; or

(b) it is unreasonable to expect the applicant for legal assistance to deal with the case unaided, having regard to the complexity of the case or the applicant's position in relation to the respondent or another person involved or any other matter.

4.18 It should be noted that the opponent that an aggrieved data subject may face is usually an organizational data user who has ample resources (in terms of both manpower and monetary) to contest any civil action taken by the data subject. The PCPD considers that in order to provide adequate assistance to the aggrieved data subject, both proposals should be taken on board. In addition, these two proposals will serve direct deterrent effect on data users against infringement of the Ordinance.

Other comments

4.19 In conjunction with the power to be given under Proposal Nos. 5 and 6, the PCPD proposes that an additional power be conferred on the PCPD to carry out mediation of a complaint including settlement by a monetary sum. At present, there is no express power under the Ordinance for the PCPD to carry out mediation of a complaint. Through the mediation process, the parties to a complaint may, with the PCPD acting as a mediator, agree to settle the complaint in an amicable manner. If the mediation is not successful, the PCPD may consider granting an award or providing legal assistance to the aggrieved data subject to institute civil action. The proposal may bring to the quick settlement of a complaint which is conducive to privacy protection and is in general accord with the current judicial approach of mediating prospective litigations.

Offences and Sanctions

Proposal No. 7 : Making Contravention of a DPP an offence

Proposal No. 8 : Unauthorized Obtaining, Disclosure and Sale of Personal Data

Proposal No. 10 : Imposing Monetary Penalty on Serious Contravention of DPPs

5.1 Proposal No. 7 to make contravention of a DPP an offence was not made by the PCPD. Proposal No. 8 to create a new offence of unauthorized obtaining, disclosure and sale of personal data was originally made by the PCPD[20] and modified by the Administration. Proposal No. 10 to impose penalty on serious contravention of DPPs was originally made by the PCPD[21].

5.2 At present, contravention of a DPP *per se* is not an offence. Instead, certain acts or practices have been singled out as offences under the current legislation. Examples are non-compliance with a data access or correction request (sections 19 and 23), failure to erase personal data no longer required for the purpose of their use (section 26), carrying out matching procedures other than in accordance with any conditions specified by the Commissioner (section 30), and direct marketing made by a data user to an individual who has previously requested the data user not to so use his personal data (section 34).

5.3 Making contravention of a DPP *per se* an offence will no doubt impact on civil liberty given the imminent risk of criminal prosecution. Strong grounds are needed for such a legislative proposal. Factors that are relevant for consideration will include:

(a) whether the contravening acts or practices in question are so serious that they need to be controlled by imposing criminal sanction; and

(b) whether the element of culpable intent is present.

---

20 See PCPD's Proposal No. 41 at p.119 in the Annex to the Information Paper.

21 See PCPD's Proposal No. 52 at p.139 in the Annex to the Information Paper.

5.4 A selective approach is preferred. It is also recognized under international jurisprudence that effective means of ensuring the proper behaviour and attitude towards protection of personal data privacy is by regulation rather than criminal sanction.

5.5 To deter contravention of a serious nature, the PCPD supports the approach to introduce a monetary penalty for serious contravention of the DPPs, modeling on the approach recently adopted by the UK Data Protection Act.[22] It aims at dealing with breaches of which the risk of their causing substantial damage or distress is known or ought to have been known to the data users. It sanctions against data users who wilfully disregard or are grossly negligent in complying with the requirements of the DPPs.

5.6 In line with the selective approach mentioned above, the PCPD supports the introduction of a new offence modeling on section 55 of the UK Data Protection Act 1998 in order to deter intentional or wilful acts that seriously intrude into an individual's personal data privacy, e.g. downloading or disseminating of personal data leaked into the Internet. The objective is not to penalize leakage or unintentional or accidental dissemination of personal data by a person, but to protect data subjects whose personal data were leaked and to deter irresponsible acts of obtaining or disclosure of such leaked data without the consent of the data users. It is also intended to close the loophole that "theft" of personal data is not an offence at present. For example, if a staff of a telecommunications company copies customers' personal data from the employer's records for the purpose of selling them to debt collection agents or third parties for profits, the staff concerned will not be criminally liable for theft of property.

5.7 The PCPD disagrees with the view that the proposal may interfere with the normal and innocuous browsing activities of web-users. There should not be a concern that innocent individuals may be caught by the new offence because, under the proposal, the person downloading personal data from the Internet may have a defence if he had the

---

[22] Section 144 of the UK Criminal Justice and Immigration Act 2008 amends the UK Data Protection Act by inserting under section 55A the power of UK Information Commissioner to impose monetary penalty. A full version of section 144 of the Criminal Justice and Immigration Act 2008 can be found at (http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_16).

reasonable belief that he had lawful right to obtain the personal data or that the data user would have consented to the obtaining. Only those who act *"knowingly or recklessly"* will be affected by the offence. It should also be noted that the proposed new offence should not prevent any person from invoking the exemptions under Part VIII of the Ordinance. In particular, section 52 of the Ordinance provides for an exemption from the provisions of the DPPs where personal data are held by an individual and concerned only with the management of his personal, family or household affairs, or so held only for recreational purposes.

5.8 As additional safeguard for journalistic activities, a separate defence on journalistic activities may be introduced for the new offence modeled on the amendment made to section 55(2) of the UK Data Protection Act under section 78[23] of the Criminal Justice and Immigration Act.

5.9 The PCPD does not prefer the proposed confinement of the new offence only to *"disclosure of personal data so obtained for (i) profits or (ii) malicious purposes"* as it will largely limit the scope of protection. It will hardly cover the loophole of the existing legal framework unveiled in the recent acquittal of a Taxation Officer of the Inland Revenue Department (ESCC3331/07), who was charged with one count of misconduct in public office, contrary to Common Law, because the prosecution failed to prove the reasons for his collection of taxpayers' personal data and the intended purpose of use. In that case, the Taxation Officer recorded the particulars (names, identity card numbers, business registration numbers, addresses and telephone numbers) of 3,400 taxpayers for his future personal use. There was no evidence to prove that the collection of the personal data had brought the Taxation Officer any financial gain. Such act, though serious in nature will not be caught under the existing proposal which is restricted to obtaining the data for "profits" or "malicious purpose".

5.10 In conclusion, the PCPD does not support any proposal to make contravention of a DPP *per se* an offence. For serious contravention, a

---

[23] It is a defence for any person who acted for the special purposes, with a view to the publication by any person of any journalistic, literary or artistic material and in the reasonable belief that in the particular circumstances the obtaining, disclosing or processing was justified as being in the public interest.

monetary penalty may be imposed. It is only for those acts or practices which are so culpable that they should then be singled out as offences under the Ordinance.

Proposal No. 9 : Repeated Contravention of a DPP on Same Facts
Proposal No. 11 : Repeated Non-compliance with Enforcement Notice

5.11 Both proposals were originally made by the PCPD[24] to curb repeated contravention of the Ordinance.

5.12 Paragraphs 6.15 and 6.24 of the Consultation Document state that there does not appear to be a strong case to introduce the above offences as the PCPD has not come across any such case since the enactment of the Ordinance.

5.13 For Proposal No. 9, it is not uncommon for different complainants to complain against the same data user at different times on the same or similar facts. The series of data loss incidents are real example of repeated contraventions. As for Proposal No. 11, the restricted enforcement power under section 50 of the Ordinance could be the reason that the PCPD has not come across repeated contraventions of an enforcement notice. As proposal has been made to amend section 50 by granting wider discretionary power on the PCPD to issue enforcement notices (see Proposal No. 20), it is foreseeable that more enforcement notices will be issued if the proposal is adopted.

5.14 The imposition of heavier penalty on repeated offender is commonly found in other legislations.[25] The PCPD finds it justifiable to adopt a similar approach given the prevalence of direct marketing activities and that repeated offenders demonstrate their lack of remorsefulness for which higher penalty level is called for to prevent repeated infringement of personal data privacy.

---

[24] See PCPD's Proposal Nos. 39 and 40 at p.115 and 117 in the Annex to the Information Paper.

[25] For instance, section 39(1) of the Unsolicited Electronic Messages Ordinance (Cap. 593) provides that a person who contravenes an enforcement notice served on him under section 38 commits an offence. Section 39(2) states that a person who commits an offence under section 39 is liable on a first conviction, to a fine at level 6 (i.e. 100,000) and on a second or subsequent conviction, to a fine of $500,000, and in the case of a continuing offence, to a further daily fine of $1,000 for each day during which the offence continues.

5.15 While statistics are not available, the PCPD believes that a proactive and forward-looking attitude should be adopted in order to enhance data privacy protection at this electronic age. The principle that is behind these Proposals is to be supported.

Proposal No. 12 : Raising Penalty for Misuse of Personal Data in Direct Marketing

5.16 This proposal was originated from the PCPD[26] was made to increase the penalty level for misuse of personal data in direct marketing activities. The maximum penalty ($10,000 at present) under section 34 is hardly a deterrent. The relatively higher level of penalties imposed under the Unsolicited Electronic Messages Ordinance (Cap. 593) ("UEMO") which deals with unsolicited commercial electronic messages may be of some reference value.

5.17 The examples below show that the penalty level under the Ordinance at present is grossly insufficient:-

Case 1

In January 2007, a telecommunications company was convicted of breaching section 34(1)(ii) of the Ordinance. The case was heard at Kwun Tong Magistrates' Courts where four summonses were laid against the company for contravening section 34(1)(ii) of the Ordinance, which requires data users to cease to further contact the individual if he chooses to opt-out.

The company began contacting the complainant by phone to promote its IDD services in July 2005. The complainant asked the company several times to stop calling him for direct marketing purposes. Nonetheless, the company continued to call him on a number of occasions for direct marketing purposes despite his opt-out requests. In February 2006, the complainant

[26] See PCPD's Proposal No. 29 at p.85 in the Annex to the Information Paper.

lodged a complaint with the PCPD.

In July 2006, the PCPD issued a written warning to the company requiring it to cease making direct marketing calls to the complainant. In August 2006, the complainant received at least four marketing calls from the company. The PCPD concluded that the reoccurrence of the incidents was contrary to section 34(1)(ii) of the Ordinance and therefore referred the case to the Police for prosecution.

The company pleaded guilty to all summonses. The magistrate imposed a fine of $5,000 for the first summons, and $3,000 each for the 2nd to 4th summonses, making a total fine of $14,000 for the four summonses.

Case 2

In August 2007, a credit card company was convicted of two offences involving direct marketing activities in the Eastern Magistrates' Court.

The complainant was formerly a credit card holder of the company but cancelled the card account sometime in 2002/2003. Thereafter, the company sent several direct marketing mails to the complainant. In October 2005, the complainant made an opt-out request to the company by telephone. However, the complainant continued to receive direct marketing mail from the company. The complainant lodged a complaint to the PCPD in January 2006.

Having learned that the complainant had made a complaint to the PCPD, the company sent a letter of apology to him. The company also agreed to process the complainant's opt-out request by removing his data from their mailing list. Notwithstanding these actions taken, the complainant still received marketing mails from the

company on 15 January and 3 February 2007 respectively.

Consequently, the company was summonsed for two offences for breach of section 34(1)(ii) of the Ordinance. The company pleaded guilty to both summonses and the magistrate imposed a fine of $3,500 for each summon, which made a total fine of $7,000.

5.18 The Magistrate in Case 1, Mr. Chan Yan-tong, remarked that such direct marketing calls were "disgusting and annoying". He also commented that the maximum penalty of HK$10,000 hardly acted as a deterrent for large organizations.

5.19 The PCPD therefore supports that the penalty level for misuse of personal data in direct marketing be raised to a level of sufficient deterrent effect.

Penalty Level

5.20 Section 64 of the Ordinance sets out different levels of sanctions to be imposed in proportion to the gravity of the offence. The lowest level of sanction is found in section 64(5) and (10) at a maximum fine at level 3 ($10,000) for contravention of a condition of the PCPD's consent to a matching procedure and contravention of a requirement under the Ordinance. A higher level of punishment is imposed at a maximum fine at level 3 ($10,000) and imprisonment for 6 months for offences committed under section 64(1), (2), (3), (4), (6) and (9) which primarily relate to supply of false or misleading information in a data user return, data access or correction request, any matching procedure request, breach of duty of secrecy by the PCPD and his staff, and unlawful obstruction or non compliance with the lawful requirement of the PCPD. The highest level of punishment is found in section 64(7) for contravention of an enforcement notice, under which the offender is liable on conviction to a maximum fine at level 5 ($50,000) and imprisonment for 2 years and, in the case of a continuing offence, to a daily penalty of $1,000.

5.21 The PCPD recognizes that penalty levels should commensurate with the

adverse consequence of a breach, the harm caused to an individual, the relative importance of the rights to be protected and the seriousness of the offence as compared with other crimes. For existing offences, the PCPD proposes to increase the penalty level. As for proposed new offences, the PCPD proposes to keep pace with the penalty levels of similar offences in other legislation, thereby closing the gap of disparity of treatment. To facilitate the Administration to review the penalty level, the PCPD has prepared a ranking table at Table 1 below based on our assessment of the gravity of different offences.

5.22 The PCPD does not have strong views on whether a custodial sentence should be imposed on the proposed new offence of knowingly or recklessly obtaining personal data without consent. The UK Government is proposing to increase the penalty level to imprisonment for 2 years on indictment, and up to 12 months on summary conviction.[27] This is in addition to the fines not exceeding the statutory maximum (currently at £5,000) on summary conviction or unlimited fines on indictment. As for contravention of section 34(1)(ii), the penalty level of offences in the UEMO may be of reference value. The PCPD proposes that the levels of fines to be imposed on these two offences should be higher. In analyzing the assessment, readers should note that offence attracting custodial sentence is generally regarded as more severe punishment than a fine. The table below sets out how the PCPD ranks the offences.

Table 1 - Ranking of Existing and Proposed Offences (For ranking of penalty level purpose)

Section/ Proposal No.	Offence Details	Ranking (1 being the lowest, 6 being the highest)
Proposal No. 11	• Second or subsequent conviction for contravention of an Enforcement Notice	6

[27] See UK Ministry of Justice's Consultation Paper on "The Knowing or Reckless Misuse of Personal Data – Introducing custodial sentences" published on 15 October 2009, available at http://www.justice.gov.uk/consultations/docs/data-misuse-increased-penalties.pdf. The consultation will end on 7 January 2010.

Proposal No. 9	• Repeated contraventions of the Ordinance on the same facts where the first infringement has resulted in the issuance of an Enforcement Notice.	5
Existing 64(7)	• Contravention of an Enforcement Notice	4
Existing 64(1)	• Supply of false or misleading information in a material particular and in purported compliance of the notice under sections 14(4) (Data user return), section 14(8) (Prescribed information in the data user return) and section 15(3) & (4) (Prescribed information for the register or any change thereof)	3
Existing 64(2)	• Supply of information in a data access request or data correction request which is false or misleading in a material particular	3
Existing 64(3)	• Supply of false or misleading information in a material particular in a notice under section 15(6) (Cease to be data user)	3
Existing 64(4)	• Supply of false or misleading information in a material particular for the purpose of matching procedure	3
Existing 64(6)	• Contravention of section 44(3) (non-disclosure of identity under news immunity) or section 46(1) (duty to maintain secrecy)	3
Existing 64(9)	• Obstruction of performance of function by the Commissioner or failure to comply with the lawful requirement of the Commissioner, making a false or misleading statement to the Commissioner.	3
Proposal No. 12	• Contravention of section 34(1)(ii) for direct marketing activities	2

Proposal No. 8	• Knowingly or recklessly obtaining personal data without consent from the data user and the disclosure or sale of the data so obtained to third parties.	2
Existing 64(5)	• Contravention of conditions under a notice under section 30(2) (matching procedure) or 32(1)(b)(i) (matching procedure)	1
Existing 64(10)	• Contravenes a requirement under the Ordinance (other than a DPP) without reasonable excuse [Relevant acts covered by the offence being brought under this section:- - Section 23 (Data access request and data correction request), section 26 (Erasure of personal data), section 14 (Data user return) & section 34(1)(i) (Provision of opt-out choice).]	1
Proposal No. 1	• Contravention against the new provision for dealing with "sensitive personal data".	1
Proposal No. 24	• Contravention against the requirement for destruction/return/use of personal data under the new "mergers, acquisition and transfer of business" exemption under Part VIII.	1

Proposal No. 13 : Third Party to Give Prescribed Consent to Change of Use of Personal Data

6.1 This proposal was originated from the PCPD[28]. It aims to permit the parents or guardians of a vulnerable data subject to give consent on his/her behalf to the change of use of his/her personal data. It must be stressed that this proposal is designated to deal with specific cases where the use of an individual's personal data may need a change for his/her own benefit, but that individual lacks the capacity to give a voluntary and informed consent to such change of use under DPP3.

6.2 The PCPD's proposal seeks to allow a "relevant person" to give "prescribed consent" on behalf of that individual. The term "relevant person" under the existing Ordinance means (i) where the individual is a minor, a person who has parental responsibility for the minor; or (ii) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs. The PCPD did not propose the widening of the class of persons to be "relevant person".

6.3 A minor's capacity to give prescribed consent under DPP3 has drawn more attention from the general public. To begin with, it is important to note that specific right of privacy for children is recognized in Article 16 of the United Nations *Convention on the Rights of the Child 1989* which is applicable to Hong Kong:-

> "*1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to protection of the law against such interference or attacks.*"

6.4 A number of approaches may be considered in the assessment of the

---

[28] See PCPD's Proposal No. 5 at p.17 in the Annex to the Information Paper.

capacity of individuals under the age of 18, such as:-

(a) determination of a young person's capacity to understand on a case-by-case basis;

(b) by fixing an age over which the young person shall be taken as having the capacity;

(c) the combination of (a) and (b) above: i.e. by setting an age over which the minor shall be taken as having capacity, and setting another age under which the minor shall be taken as not having capacity. Capacity of minors between these two ages would require individual assessment.

(d) Setting certain ages of legal capacity for the particular context of the decision, e.g. by setting a particular maturity age in relation to certain sensitive issues such as information relating to pregnancy;

(e) according to specific group of young people, e.g. by deeming young people who are married, parents themselves or living independently to have legal capacity.

6.5 The person making the assessment of the minor's capacity may not be suitably qualified to make the assessment. While setting a minimum age should overcome the difficulties in making individual assessment, the oversimplified solution is arbitrary and may cause injustice. The PCPD's research on the decision-making capacity supports the approach of making individual assessment in the interest of fairness.

6.6 Individual assessment generally accords with the common law position of "Gillick competency" test introduced in the UK landmark decision of Gillick v West Norkfolk and Wisbech Area Health Authority and Another [1986] 1AC112. The case sheds light on the proper test to apply when assessing an individual's competency. It concerns the prescription of contraception by a medical doctor to a minor at her request. The test sets out the criteria for doctors and other health professionals to apply in ascertaining, where there is a conflict of interest between a child or young person and his/her parents, whether

medical advice or treatment can be given without the consent or knowledge of the parents. A child or young person who is judged after consideration of these criteria as having the capacity to consent is often referred to as being "Gillick competent". The House of Lords (by a majority of 3 to 2) held that parental consent was not required, and the following guidelines were established when a child or young person sought confidential medical advice:

(a) If a doctor was of the view that the procedure could be said to be in a child's best interests; and

(b) If that doctor could not persuade the child to tell his/her parents; then

(c) Provided that the child was able to understand the nature and consequences of the medical procedure,

the child was competent to consent without the knowledge and consent of his/her parents.[29]

6.7 The guidelines laid down in the case have been in use by professionals dealing with children and young people in other areas where consent is necessary.

6.8 The approaches adopted by overseas jurisdictions are set out in the table below:-

Jurisdiction	Approach
Privacy Act 1985 (Canada)	➢ An authorized person may exercise or perform on behalf of a minor rights or actions.
Data Protection Act 1998 (UK)	➢ An individual under the age of 16 may exercise any right conferred by the *Act* where he has a general understanding of what it means to exercise that right. Such understanding is presumed where the individual is 12 years old or above.[30]

[29] See p.91 of "Children's Databases – Safety and Privacy", a report for the UK Information Commissioner issued in November 2006.

[30] See section 66(2) of *Data Protection Act 1998 (UK)* and *"Data Protection Act 1998 Legal Guidance (2001)"* issued by the UK Information Commissioner.

Privacy Act 1993 (New Zealand)	➢ An organisation is entitled to refuse to disclose information requested by an individual under the age of 16 if the disclosure would be contrary to the individual's interest.[31]
Personal Health Information Protection Act 2004 (Ontario)	➢ A person aged 16 or above can consent to collection, use or disclosure of his/her personal information. ➢ A parent, children's aid society or other person with parental responsibility may provide consent on behalf of an individual who is under 16 *but not if* information relates to : (i) medical treatment about which the individual has made his or her own decision; or (ii) child and family services counseling in which the individual has participated on his/her own. • *However, if* the individual is considered to be capable of consenting on his/her own, then the individual's decision prevails over the conflicting decision of the parents or other substitute decision-maker.[32]
European Union Article 29 Data Protection Working Party Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)	➢ As a human, the child has a right to privacy. The core principle is that of the best interest of the child. ➢ If the processing of a child's data began with the consent of their legal representative, the child concerned may, on attaining majority, revoke the consent. But if he wishes the processing to continue, it seems that the data subject may need to give explicit consent wherever this is required. ➢ The principle of the best interest can have a double role. Situations may arise where the best interest of the child and his/her right to privacy appear to compete. In such cases, data protection rights may have to yield to the principle of best interest. This is particular the case for medical data. For example, a youth welfare service may require relevant

[31] See section 29(1)(d) of *Privacy Act 1993 (New Zealand)*.

[32] See section 23(2) and (3) of the *Health Information Protection Act 2004 (Ontario)*.

	information in case of child neglect or abuse. Similarly, a teacher may disclose a child's personal data to a social worker in order to protect the child, either physically or psychologically. ➢ Where consent is concerned, the solution can progress from mere consultation of the child, to a parallel consent of the child and the legal representative, and even to the sole consent of the child if he or she is already mature. ➢ The first level of the right to participate is the right to be consulted. ➢ The data protection needs of children must take into account two important aspects. Firstly, the varying levels of maturity which determine when children can start dealing with their own data. Secondly, the extent to which representatives have the right to represent minors in cases where the disclosure of personal data would prejudice the best interests of the child.
Privacy Act 1988 (Australia) *Australian Law Reform Commission Report issued on 11 August 2008*	➢ Currently, there is no provision for a child to give "consent". ➢ In relation to the question of capacity, the research conducted shows that an individual's capacity to make a decision cannot be determined by age alone.[33] ➢ It is also recognized that an individual approach to assess the capacity of a child or young person by way of the Gillick's test is the fairest and most appropriate way.[34] ➢ It is nevertheless acknowledged that the policy approach of setting a minimum age may have the advantage of clarifying the operation of the law and simplifying the process of determining capacity by data users.[35] ➢ Recommended model: • Where it is reasonable and practicable to make an assessment about the capacity of

[33] Paragraph 68.37 of the ALRC Report.
[34] Paragraph 68.102 of the ALRC Report.
[35] Paragraph 68.57 of the ALRC Report.

	an individual under the age of 18 to give consent, make request or exercise a right of access under the Act, an assessment about the individual's capacity should be undertaken. • Where an assessment of capacity is not reasonable or practicable, then an individual, (a) aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access; and (b) under the age of 15 is presumed to be incapable of giving consent, making a request or exercising a right of access. • Where an individual under the age of 18 is assessed or presumed to not have capacity under the *Act*, any consent, request or exercise of a right in relation to that individual must be provided or made by a person with parental responsibility for the individual.

6.9 While there is no uniform approach taken, the generally recognized approach is to assess the young person concerned on individual cases.

6.10 In deciding what is in the "best interest" to serve, the duty lies upon the person who gives such consent on behalf of the minor to show that it serves a clear benefit to the minor having regard to the extent of intrusion into personal data privacy of the minor and the benefits or privileges to be derived. For example, deciding the proper course of medical treatment to be received may be regarded as safeguarding the vital interest of the minor. Reasonableness and proportionality are the benchmarks to measure.

6.11 It should be borne in mind that this proposal is applicable only when there is a change of the use of the minor's personal data and does not apply in the ordinary course of personal data handling.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

6.12 The proposal was originally made by the PCPD[36] at the request of the social welfare sector to permit a data user, in exceptional circumstances, to refuse to comply with data access requests made by the parents on behalf of their children in order to protect the interest of the children.

6.13 Data users should be able in appropriate cases to refuse to comply with a data access request where disclosure would be contrary to the interest of the minors. The proposal models on the New Zealand approach laid down in section 29(1)(d) of the Privacy Act 1993 which provides a ground for refusal to disclose personal information of an individual under the age of 16 if the disclosure would be contrary to the individual's interest.

6.14 Paragraph 8 in Annex 1 of the Consultation Document lists the exceptional instances that a data user may refuse to comply with the data access request. They are:-

(a) where the parent may abuse the data access mechanism to obtain the personal data of the child for the parent's own purpose rather than making it "on behalf of" the child. For instance, an estranged parent may make a data access request to the school or social welfare organizations for his/her child's location data to trace the whereabouts of the child or the other parent of the child;

(b) where a parent is suspected to have committed child abuse on his/her child; and

(c) where the child has expressed to the data user (at the time when providing his/her personal data to the data user) his/her disagreement to the disclosure of the data to his/her parents.

6.15 It should be noted that the exercise of this proposed ground of refusal is only in exceptional and unusual situations and in most of the other situations, data users may not have justifications to refuse to provide the

---

[36] See PCPD's Proposal No. 20 at p.57 in the Annex to the Information Paper.

minor's personal data to the parents. Data users may run the risk of breaching the provisions of the Ordinance by unjustified reliance on this proposed ground of refusal. An aggrieved parent may lodge a complaint with the PCPD in such instances.

6.16 For the situation in 6.14(a) above, the PCPD has come across specific cases which show justification to cater for the situation. An example is given below:

> *In 2003, the ex-husband of the complainant lodged with a data user several data access requests as the relevant person of his daughter, who no longer lived with him, for information relating to the school in which the daughter was studying. The father claimed that he had no knowledge as to the daughter's whereabouts after divorce. Under DPP3, except with the prescribed consent of the data subject, the data user may not disclose personal data for such purpose other than a purpose which is the same as or directly related to the original purpose at the time of collection. In relation to one of the data access requests, the data user disclosed the personal data of the daughter with which the father managed to locate the daughter and caused nuisance to the complainant and the daughter. After investigation, the PCPD warned the data user that such disclosure of the daughter's personal data was not directly related to the original purpose at the time of collection of the daughter's personal data.*

6.17 As for the situation in 6.14(b) above, where a parent is suspected to have committed child abuse, disclosure of the minor's personal data may endanger the well-being of the child.

6.18 The reason for the inclusion of the situation in 6.14(c) is that some data users are concerned about the possibility of inhibiting the minors from seeking counseling or other professional services if their personal data are disclosed to their parents.

6.19 The proposal has drawn attention from the public. There has been concern that the proposal may deprive the parents the right to access the personal data of their children such as school records. The PCPD has

stressed that the proposal only seeks to deal with specific situations as outlined in the proposal and it has never been intended to deny the parents' right to access personal data relating to the minors' education and development. In the case of school records, one of the original purposes of the school in collecting the students' personal data (such as performance in school) is for education and development of the students. The release by the school to the parents such personal data of the students without the students' consent does not infringe the Ordinance.

6.20 Another concern raised is that the requirement of *"best interest of the minors"* should be clearly defined. It must however be noted that giving the phrase *"best interest"* a specific definition may be undesirable. In many instances, the case should be decided on its own facts after taking all the circumstances into consideration so as to assess the *"best interest of the minors"*. The PCPD does not object the approach suggested by the Administration to consider the appropriateness of specifying some factors to enable the data users to assess whether there are reasonable grounds in exercising the proposed right of refusal in dealing with such data access requests. It should however be borne in mind that giving the term too restrictive a meaning may defeat its original purpose.

Proposal No. 27 : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

6.21 This proposal did not originate from the PCPD. The Administration puts forward this proposal to provide for an exemption to allow data users to transfer personal data of a minor that are relevant to parental care and guardianship to the parents or guardian of the minor, so that the latter can fulfil their responsibility to exercise proper care and guardianship of their children under the age of 18. The PCPD appreciates the rationale behind the proposal which will facilitate parents to provide care and guidance to their children in time. In order that the transfer is justifiable, consideration should be given to the type of the exempted personal data, the degree of disclosure and the relevant circumstances at the material time. Also, a mechanism must be built in to guard against misuse. Moreover, it is imperative for Administration to consider allowing minors who attain certain age to make their own

decisions in relation to the disclosure of the personal data.

6.22 Apart from the option of providing specific exemption in the Ordinance, the Administration may consider whether the best solution to tackle the situation as identified in the proposal be by way of other child protection laws.

6.23 The PCPD has made enquires with overseas privacy regulators whether similar exemption is provided under their privacy legislation for the transfer of minors' personal data to the parents that are relevant to parental care and guardianship. The replies reveal that there is no equivalent or similar exemption under the overseas privacy legislation.

6.24 Take the situation in the UK for example, under section 29 of the Data Protection Act, an exemption is provided to allow disclosure of personal data if that will aid the prevention or detection of crime or the apprehension or prosecution of offenders. It covers situation where the police is of the view that the disclosure of the personal data about a minor to their parents might prevent a crime. However, in situation where there is far from "concrete evidence" of a crime (as mentioned in paragraph 65 Annex 1 of the Consultation Document), it will be covered by a wide range of local legislation in the UK which relates to ***child protection***. The relevant legislation lays emphasis on the experienced professionals empowered to make decisions which the child is unable to do so for themselves in circumstances where the child's overall well-being may be compromised. These decisions will at times include decisions to disclose personal data about the child. Unlike the police, the childcare professionals, social workers and teachers do not have to have "concrete evidence" before they may act. They simply have to show that in their professional opinion that it is in the child's best interests to disclose the relevant personal data.

Enhancing the Effectiveness of Ordinance

7.1 The PCPD supports all proposals raised in the Consultation Document that will enhance the effectiveness of the Ordinance.

Proposal No. 20 : Circumstances for Issue of an Enforcement Notice

7.2 This proposal was originally made by the PCPD[37]. It aims to relax the current overly restrictive criteria for issuing an enforcement notice by the PCPD. The option proposed by the Administration in paragraph 39 of Annex 1 of the Consultation Document, if adopted, will to a certain extent allow PCPD to exercise the right of issuing an enforcement notice in a more effective manner, thereby enhancing the protection to the individuals affected.

7.3 In addition to the option, the PCPD considers that its discretion will be more effectively exercised if a further option is provided to *consider other matters as the PCPD may think fit* when deciding whether to issue an enforcement notice. This option will enable the PCPD to consider also other relevant circumstances in the specific cases. In deciding whether to issue an enforcement notice, the PCPD wishes to be able to consider, amongst other things, the following:-

(a) whether it is in the interest of the public;

(b) the gravity of the contravention, including the number of individuals affected and the type of personal data involved;

(c) whether or not the data user has in place any data protection policy concerning the contravening act or practice;

(d) whether or not the act in question is deliberate or accidental or an isolated incident;

(e) the conduct of the data user during the incident in question, after being notified of the subject matter of the complaint (whether by the complainant, the media, PCPD, other regulators or other

[37] See PCPD's Proposal No. 19 at p.54 in the Annex to the Information Paper.

sources), and during the course of the investigation (whether co-operative, whether providing misleading information, whether remorseful, etc.);

(f) whether the data user has remedied the contravention during the course of investigation, whether or not the data user has unreasonably delayed the remedial action;

(g) whether or not the data user has offered to compensate the complainant;

(h) whether there are previous complaints against the data user and taking into account the circumstances of those complaints;

(i) whether or not the data user has previously found to have been in contravention of the Ordinance, irrespective of the nature of the act or practice concerned in the previous contravention.

7.4 The PCPD believes that to introduce more flexibility under section 50 to serve an enforcement notice will enhance data privacy protection in that data users in contravention of the Ordinance will be directed under the enforcement notice to take specific steps to remedy the contravention and failure to do so is a criminal offence.

7.5 Below are some case examples which the PCPD's discretion to issue an enforcement notice was restricted by the current section 50.

Case 1

The complainants (a couple) instructed a company to prepare their wills and they discovered that the company had adopted the wife's will as a template to draft the will of another client and forwarded a softcopy of the draft will for that client's approval. In the margin of the draft will, there were boxes printed with information of the wife's will as well as personal data of the husband. It was caused by the "check change" feature of the word processing software having been enabled during the process.

The company took remedial actions by (i) convening a meeting with all staff discussing the incident, running through the workflow again and explaining the consequences of not following the procedures (ii) devising a new workflow checklist to make sure that draft will was in correct format which has to be signed by the staff concerned and countersigned by the superior of that staff; (iii) giving a warning to the staff concerned who released the complainants personal data; and (iv) making an apology to the complainants.

In view of the remedial actions taken by the company, the PCPD found no evidence of likelihood of repetition of the contravention. Hence no enforcement notice was issued despite the serious intrusion of the complainants' personal data privacy.

Case 2

A complainant alleged that a telecommunications company had a practice of re-activating its customers' lockout account by automatically resetting his or her password to a fixed number of 123456, thus exposing the customer's personal information contained in its electronic billing system to the risk of infrusion by unauthorized third parties. Subsequently, the telecommunications company took remedial measures on password resetting. In view of the remedial actions taken, the PCPD found no evidence of likelihood of repetition of the contravention. Hence no enforcement notice was issued.

Case 3

The complainant alleged that a company had collected a copy of her Hong Kong identity card prior to the granting of a job interview. Upon intervention by the PCPD, the

company confirmed that they had destroyed all HKID copies of job applicants previously obtained, and undertook that they would not collect the HKID copies of job applicants unless and until the individual had accepted an offer of employment. In light of the above remedial actions taken by the company, the PCPD had not served an enforcement notice since no evidence of likelihood of repetition of the contravention could be found.

Case 4

The complainant had a dispute with a travel agent over the amount to be charged on cancellation of an air flight booking. The complainant later discovered that the travel agent had, without his consent, used the personal data collected during the booking transaction for lodging a complaint against him to his employer thereby disclosing the details of the dispute. Upon investigation by the PCPD, the travel agent confirmed that (i) she would not use the complainant's personal data for any purpose other than air flight booking and related matters; (ii) the information collected during booking transaction had formed part of internal document retained by employer of the travel agent and she had not retained a copy of the complainant's personal data. In view of the aforesaid, the PCPD did not issue an enforcement notice as no evidence of likelihood of repetition of contravention was found.

Case 5

The complainant opened an account with a ticket company for purchasing cinema and concerts tickets online by credit card. During online registration, the complainant chose not to receive direct email newsletter but he still received 3 marketing emails from the company at his email address. Subsequently, the company took remedial actions by (i) removing complainant's email address from

the mailing list (ii) amending the opt-out statement; and (iii) conducting manual check of mailing list to ensure no inclusion of subscribers who had opted out. In view of the remedial actions taken, there was no evidence of likelihood of repetition of the contravention by the company. Thus, no enforcement notice could be served on the company by the PCPD.

Case 6

In this case, the complainant borrowed from a bank a property mortgage loan. She later indicated to the bank that she intended to sell her property at a price less than the outstanding mortgage loan owed to the bank. The bank offered her a loan covering the shortfall balance to be repayable by 24 equal monthly instalments. The bank however treated the mortgage loan account as an account in default and notified the Credit Reference Agency of the above as a scheme of arrangement. The complainant complained that she had never been in default of the mortgage loan and the shortfall loan. Upon investigation by the PCPD, the bank asked the Credit Reference Agency to delete the purported default data, which the CRA had acted accordingly. In view of the remedial action taken by the bank, the PCPD opined that the contravention was not likely to be repeated and therefore no enforcement notice was issued.

Case 7

The complainant ceased to be a customer of a telecommunications company. Later, he discovered that the telecommunications company debited his credit card for a service fee. As the complainant had never provided his credit card number to the company, he lodged a complaint with the PCPD. Investigation by the PCPD revealed that the telecommunications company had made a clerical mistake by wrongly debiting the complainant's

credit card account for a fee incurred by another customer. The telecommunications company stated that they had a policy in place requiring their staff to verify the accuracy of customers' personal data and in order to avoid recurrence of similar incident in future, they had advised their staff to double-check the credit card account number before transferring the same to the bank. In view of the remedial action taken by the company, the PCPD opined that the contravention was not likely to be repeated and therefore no enforcement notice was issued.

Case 8

The complainants complained that a company provided online service to their subscribers for retrieval of individuals' ownership of properties. The PCPD's investigation revealed that the personal data contained in the database of the company were purchased from the Land Registry and the company had used the data for a purpose outside the purpose of use as stipulated by the Land Registry. To remedy the situation, the company ceased providing the service to their customers. Given the remedial action taken by the company, the PCPD did not issue an enforcement notice since there was no likelihood of repetition of the contravention.

7.6 In each of the cases above, had the PCPD not been tied by the restrictions under section 50, it could have served enforcement notices on the parties complained against directing them to cease doing any act or engaging in any practice which caused the infringement. It will have a deterrence effect on the parties concerned since any breach of the directions of an enforcement notice is a criminal offence.

7.7 Added to those cases is the situation that the PCPD is not able to issue an enforcement notice directing a data user to destroy personal data collected by unfair means where the contravening act of collection had ceased and there is no evidence suggesting that the contravention will

continue or be repeated[38]. This is undesirable as the protection of personal data privacy has been compromised by the overly restrictive criteria for issuing an enforcement notice.

7.8 There should not be concerns that the additional option will confer unfettered discretion on the PCPD. It is because pursuant to the current provision of the Ordinance[39], a data user who has been served with an enforcement notice may lodge an appeal to the Administrative Appeals Board (AAB) against the PCPD's decision. Hence, if PCPD's discretion is not reasonably exercised, his decision will not stand before the AAB.

7.9 The PCPD therefore urges the Administration to consider adding *"such other matters as the Commissioner may think fit to consider"* as paragraph (d) to the option raised in paragraph 39 of Annex 1 of the Consultation Document.

Proposal No. 21 : Clarifying Power to Direct Remedial Steps in an Enforcement Notice

7.10 This proposal originated from the PCPD[40] was made for the purpose of stating explicitly the PCPD's power to direct the relevant data user in an enforcement notice to desist from doing an act or engaging in practice. This will clear up the grey area currently found in the Ordinance.

Proposal No. 22 : Removing the Time Limit to Discontinue an Investigation

7.11 This was a proposal originated from the PCPD[41] to remove the time limit imposed under section 39(3) of the Ordinance with regard to a decision to discontinue investigation. It is not effective use of the limited resources of the PCPD to continue to pursue unwarranted investigations. Hence, the PCPD supports this proposal to amend the Ordinance to make this clear.

---

38 See section 50(1) of the Ordinance

39 See section 50(7) of the Ordinance.

40 See PCPD's Proposal No. 19 at p.54 in the Annex to the Information Paper.

41 See PCPD's Proposal No. 13 at p.41 in the Annex to the Information Paper.

Proposal No. 23 : Additional Grounds for Refusing to Investigate

7.12 This proposal was originally made by the PCPD[42] to add the following grounds under section 39(2) of the Ordinance for refusal to carry out or continue an investigation initiated by a complaint:-

(a) where the primary cause of the complaint is not related to personal data privacy;

(b) the complaint relates to any action which the complainant has a remedy in any court or tribunal or is currently or soon to be under investigation by another regulatory body, unless the PCPD is satisfied that in the particular circumstances it is not reasonable to expect the complainant to resort or to have resorted to that right or remedy; or

(c) where the act or practice specified in the complaint relates to personal data or documents containing personal data which have been or will likely be or intended to be used at any stage in any legal proceedings or inquiry before any magistrate or in any court, tribunal, board or regulatory or law enforcement agencies.

7.13 As for the ground (a) *"where the primary cause of the complaint is not related to personal data privacy"*, a comprehensive study of the following complaint cases received by the PCPD will help to clarify the reasons why such a proposal was made.

Case 1

The daughter of the complainant posted a notice with the headline "The present chairman xxx arrogates all powers to himself" in the public area of the building.

In response to the notice, the chairman of the Incorporated Owners ("IO") xxx issued a memo, which contained the name of the complainant. In this connection, the complainant complained that the

---

42 See PCPD's Proposal No. 12 at p.37 in the Annex to the Information Paper.

chairman of the IO had disclosed his personal data, and the IO "criticized owners with big-character poster of the Cultural Revolution".

The PCPD opined that from the nature of the incident (scolding and libel), the complaint was not related to personal data privacy.

Case 2

The complainant sent a letter to the owners of his building with respect to the re-election of the management committee of the building. The name and address of the complainant were stated in the letter.

In response to the letter, the Incorporated Owners ("IO") of the building issued a memo, which contained information of the complainant, such as name. In this connection, the complainant complained that the IO had disclosed his personal data.

The PCPD opined that the complaint mainly involved the expression of opinions to owners on the re-election of the management committee by the complainant and the IO. The complainant had disclosed his identity to the owners at the beginning. The cause of the complaint was not related to privacy.

Case 3

The complainant was a customer of a telecommunications company.

The telecommunications company intended to call the complainant to promote its service, but the call was picked up by the complainant's son, who accepted the service on behalf of the complainant. The complainant then complained that the telecommunications company used his

personal data to promote sales to his son.

The PCPD opined that the case mainly concerned the manner in which the telecommunications company's salesman promoted its service. It was not related to personal data privacy.

Case 4

The complainant was a customer of a telecommunications company and used credit card autopay to settle the bills.

Later, the complainant stopped using the credit card autopay service, but the company continued to use his credit card account to settle the bills. The complainant lodged a complaint with the PCPD.

The PCPD opined that the case mainly involved the settlement of bills between the service provider and the customer. It was not related to privacy.

Case 5

The complainant was an online game customer of an electronic game manufacturer.

The complainant was rejected to log in the game because he had wrongly registered as a minor.

After amending the date of birth, the complainant still could not log in. In this connection, the complainant complained that the manufacturer had retained and used the data which were not updated.

Enquiry with the manufacturer revealed that it had recorded the correct date of birth of the complainant. The PCPD took the view that the incident was caused by the setting of system of the manufacturer. It was not

related to personal data privacy.

7.14 It is self-evident from the above cases that the primary causes of the complaints are not related to personal data privacy.

7.15 There are also complaints caused by personal feud. In this connection, the AAB in AAB Appeal No.24 of 2001 stated as follows:-

> *"The Board wish to make it known that we deprecate any attempt by persons to use the Board as a forum for the pursuit of personal vendetta or to vent their anger. The Ordinance must be interpreted and applied sensibly, reasonably and practicably so that it is not used as a tool of oppression or revenge."*

7.16 The PCPD agrees with the observation made by the AAB. Very often, it is found that some complainants have utilized the complaint channel provided under the Ordinance for personal feud rather than being motivated by a genuine concern for protection of one's personal data privacy. The PCPD considers that the complaint channel under the Ordinance should not be used as a forum for the pursuit of personal dispute not related to personal data privacy.

7.17 The Administration has expressed reservations in respect of ground (b) *"if the complaint relates to an action for which the complainant has a remedy in any court or tribunal"* because it would deprive an aggrieved party of a redress alternative. The PCPD considers that in some cases, the PCPD may not be an appropriate forum for the aggrieved individual to seek redress, when compared with the sanction imposed under other laws or ordinances. For example, where a complaint involves a disgruntled employee seeking redress against the employer's termination of his employment, the PCPD finds it proper for the matter to be dealt with in the Labour Tribunal. In order to provide further safeguard to the aggrieved individual, the PCPD has considered and did make proposal for a saving clause. This is when in the particular circumstances it is not reasonable to expect the complainant to resort or to have resorted to the right or remedy in court or tribunal. In addition, the Ombudsman Ordinance also contains similar ground of refusal under

section 10(1)(e)(ii). This shows the Legislature's readiness to accept similar ground as valid refusal of a complaint.

7.18 With regard to ground (c), i.e. where personal data in question have been or will likely be or intended to be used at any stage in any legal proceedings or inquiry, the common example is where the complainant is engaging in a fishing expedition to obtain documents and data (through the lodging of a data access request) which he would otherwise only be entitled to under discovery procedures taken in legal proceedings. In a judicial review application[43], the Judge took the view that where the data subject had obtained or could have obtained copies of his personal data through legal proceedings, it would be meaningless and a waste of public funds for him to lodge a complaint with the PCPD on non-compliance with a data access request and for the PCPD to investigate the matter. In a judicial review application[44] made against the AAB's decision concerning compliance with a data access request lodged by the Appellant, the Court states in paragraph 34 of the judgment as follows:-

> *"It is not the purpose of the Ordinance to enable an individual to obtain a copy of every document upon which there is a reference to the individual. It is not the purpose of the Ordinance to supplement rights of discovery in legal proceedings, nor to add any wider action for discovery for the purpose of discovering the identity of a wrongdoer under the principles established in Norwich Pharmacal v Commissioners of Customs and Excise [1974] AC 133. That conclusion is entirely in accord with the decision of Deputy Judge Muttrie in Gotland Enterprises Ltd v Kwok Chi Yau [2007] HKLRD 236, at 231-2."*

7.19 The proposal to include three additional grounds of refusal aims to make good use of the PCPD's limited resources in handling complaints and

---

[43] 徐冠華 訴 個人資料私隱專員 [2004] 2 HKLRD 840
http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=39465&QS=%28%7Bhcal94%2F2003%7D%7C%7BHCAL000094%2F2003%7D+%25caseno%29&TP=JU

[44] Wu Kit Ping v Administrative Appeals Board, HCAL60/2007
http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=58956&QS=%28%7Bhcal60%2F2007%7D%7C%7BHCAL000060%2F2007%7D+%25caseno%29&TP=JU

should therefore be supported.

General comments

7.20 The critical success factor involved in the handling of complaints is that the PCPD should be permitted to utilize its limited resources by not having to investigate complaints where the general good of the public is not manifestly served. To achieve the goal of following up on every complaint in a painstaking manner is not the practice in overseas privacy or data protection authorities. PCPD simply has to be allowed to be selective in order to be effective having regard to the size of its organization.

Annex 2 to the Consultation Document - Proposals Not to be Pursued

8.1 Annex 2 to the Consultation Document contains 9 proposals that the Administration is not inclined to pursue after deliberating on the implications of the proposals. The PCPD's stance on each of the proposals is set out below.

Revamping Regulatory Regime of Direct Marketing

8.2 The Administration does not consider it appropriate to make further amendments to the regulatory regime of direct marketing under section 34 of the Ordinance.

8.3 The PCPD has, however, suggested the Administration to consider reviewing the regulatory regime with particular attention to the following aspects[45]:-

(a) whether to introduce an "opt-in" regime in place of the current "opt-out" regime;

(b) whether a territorial wide central "Do-not-call" register be established; and

(c) whether a data user shall disclose the source of the data upon the data subject's request.

8.4 The "opt-in" approach requires a data user to obtain the express consent of the data subject for the use of the latter's personal data. Such approach is in alignment with the "prescribed consent" under the use limitation principle expounded under DPP3. A territorial wide central "Do-not-call" register will serve as a clear notice and caveat to data users which intend to make telemarketing calls, not to use the personal data contained in the register for such purpose. As a further step to enhance protection to personal data, consideration may be given to require the data user, on request by a data subject, to disclose the source of his personal data collected by it. This suggestion was made to address the concerns raised by complainants on how organizations

[45] See PCPD's Information Paper, Issue No. 2 to the Annex at p.155-156.

obtained their personal data for making the unsolicited direct marketing communications to them.

8.5 The PCPD considers that conferring a right on the individuals to know the source of data will enhance transparency in how individuals' personal data is handled and promote the handling of personal data that accords with individuals' reasonable expectation over the use of their personal data. The Australian Law Reform Commission in its Report 108 – For Your Information: Australian Privacy Law and Practice[46] issued in August 2008 made a similar recommendation. In response to the recommendation, the Australian Government has recently accepted such recommendation and agreed that individuals should have the right to be so informed by the organization if they have not had a customer relationship with the organization[47].

8.6 Paragraph 5 of Annex 2 (p.72) of the Consultation Document states that the Administration is monitoring the situation of using person-to-person calls for telemarketing purpose and will consider the possibility of regulating such activities under UEMO if the problem grows in future. In a recent paper[48] prepared by the Office of the Telecommunications Authority ("OFTA's Paper") to the Legislative Council Panel on Information Technology and Broadcasting, it stated that the use of personal data for direct telemarketing had already been regulated under the Ordinance and there was no clear need to contemplate further legislative measures for such calls. From this paper, it appears that no change will be made to UEMO to regulate person-to-person telemarketing activities. It is therefore necessary for the Administration to reconsider revamping the regulation of direct marketing activities involving the use of personal data in this opportune moment of reviewing the Ordinance.

8.7 OFTA's Paper contains the results of a public opinion survey and an industry survey commissioned by the Administration in respect of person-to-person telemarketing calls. It is noted from the summary of

---

46 Available at http://www.austlii.edu.au/au/other/alrc/publications/reports/108/26.html#Heading386

47 Recommendation 26-6 Australian Government First Stage Response to ALRC Privacy Report, p.59, available at http://www.pmc.gov.au/privacy/alrc.cfm

48 LC Paper No. CB(1)240/09-10(04), available at http://www.legco.gov.hk/yr09-10/english/panels/itb/papers/itb1109cb1-240-4-e.pdf

the public opinion survey that the respondents had not been asked about whether there was any need for the Government to expand the scope of the UEMO to cover person-to-person telemarketing calls involving the use of personal data. Nevertheless, the results of the survey reflected clearly the community concerns about direct marketing activities. It is revealed from the public opinion survey that:-

(a) Out of 967 respondents, 766 were always sure whether callers had their personal data or not. Among these 766 respondents, 55% reported that more than 40% person-to-person telemarketing calls received by them involved the use of their personal data.

(b) Out of the 806 respondents who had ever received person-to-person telemarketing calls in which callers had their personal data, only 35% of them had ever requested the callers not to call them again. Among those respondents who had ever made unsubscribe requests to callers, only 21% said that callers would honour their request. On the other hand, 30% said that callers would continue to call even though they had promised not to call again.

(c) About 81% of 967 respondents said that person-to-person telemarketing calls had caused inconvenience to them. When being asked to rate the level of inconvenience, over 30% considered such calls caused a lot of inconvenience to them, while almost half of them reported moderate inconvenience. The most often quoted inconveniences included wastage of time, being called when respondents were working or busy, and being called repeatedly.

(d) 57% of 1,157 respondents in the survey considered that the Government should regulate person-to-person marketing calls not involving the use of personal data. 42% of the total respondents supported regulation by legislation while 15% of the respondents supported to regulate such calls by a voluntary code of practice[49].

8.8 It is noted that there is no majority view to support regulation of

[49] Quoted from the OFTA's Paper.

person-to-person marketing calls not involving the use of personal data by legislation. However, it is totally different from the case of using personal data for direct marketing. The PCPD takes the view that the Administration should reconsider the need to tighten up the regulation of direct marketing activities involving the use of personal data under the Ordinance given the clear voice reflected in the community.

Internet Protocol Address as Personal Data

8.9 This proposal was originated from Yahoo's case[50] where heated debates had been raised on whether IP address should be viewed as "personal data". The Administration does not consider it appropriate to deem IP address *per se* as personal data under the Ordinance. The PCPD is open-minded as to the proposal but would like to set out the information below for consideration.

8.10 The existing three-limb definition of "personal data" gives general guiding principles on what constitutes "personal data" without singling out any particular kind of data to be so classified. The definition is of pretty straight forward application save for the concept of "indirect" identification and relevancy. In the past, the PCPD, in interpreting the meaning of what is "reasonably practicable" for the data user to ascertain the identity of the individual, has taken into account of other information that is readily obtainable by the data user.

8.11 The Yahoo's case raised concern on whether IP address falls within the definition of "personal data" as it can give useful hints for tracing the identity of the actual user of the computer. In the Yahoo's case, the PCPD took the view that an IP address *per se* does not meet the definition of "personal data". However, "personal data" can include an IP address when combined with, for example, identifying particulars of an individual.

8.12 The Yahoo's case went before the AAB[51]. The Appellant relied on *Cinepoly Records Co Ltd and others v Hong Kong Broadband Network*

---

50 See PCPD's investigation report, available at http://www.pcpd.org.hk/english/publications/files/Yahoo_e.pdf

51 AAB No. 16/2007, available at http://www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf

Ltd and others [2006] 1 HKLRD 255 to illustrate how an IP address might be used to track down the identity of a certain data subject. Having considered the evidence before it, the AAB dismissed the appeal and decided that on the facts of the case, the IP log-in information provided by Beijing Yahoo! even when coupled with other information disclosed, did not constitute "personal data" as defined under the Ordinance.

8.13 The public sentiment at the material times was very much concerned about the protection of IP address and questions were raised in the Legislative Council relating to disclosure of IP address without consent.

8.14 In view of the public concern, it is necessary to review whether IP address should be afforded the same protection of "personal data" under the Ordinance. The PCPD sets out below the pros and cons for deeming IP address as personal data.

Pros

- it gives certainty on its classification;
- it imposes obligations on persons, such as ISPs, webmail service providers and IT system administrators, etc to comply with the requirements of the Ordinance; and
- the disclosure of IP address to third parties, such as law enforcement bodies, would have to comply with DPP3 or otherwise the application of the relevant Part VIII exemption.

Cons

- IP address can be dynamic instead of static and there may be multiple users to a computer, e.g. in an office or cyber café environment. It may not be practicable to ascertain the identity of the user of the computer;
- IP address appears at the header of an email, affording it with the protection under Ordinance may have practical difficulties;

- onerous burden may be imposed on the ISPs and webmail service providers, particularly in situation when they have no intention to compile information about any individual when IP address is randomly allocated.

- If IP address is specifically defined as personal data, then email address, mobile phone number, car registration number, Autotoll tag number, Octopus card number etc. should logically be considered for inclusion on the ground that they are capable of "indirectly" identifying a particular individual by tracing. It would appear difficult to have an exhaustive list.

8.15 Added to the above complications is that new IP address standards (IPv6) have already been applied in some network segments (less than 1% of the WWW). Unlike the current IP addresses (IPv4), there is no "public" or "private" but universally unique IP address within IP v6 operations (while "static" and "dynamic" concepts would still apply). When compared to IPv4, an IPv6 address always represents a uniquely numbered computing device (usually operated by a person) in the WWW (even if such device is working behind a router or within a LAN). Unlike the situation in IPv4 (that identifying a device hosting a private IPv4 address could only be done by the LAN owner/operator), identifying an IPv6 host device may be possible on most of the data recipient's sides.

8.16 The question as to whether IP address alone shall be deemed as "personal data" is very controversial and the rights and interests of different classes in the society shall be fully and carefully considered before a decision should be made. PCPD is open-minded with regard to the proposal.

Territorial Scope of the Ordinance

8.17 This proposal was originated from PCPD[52] to exclude from the application of the Ordinance any act or practice involving personal data the collection, holding, processing and use of which occur wholly

[52] See PCPD's Proposal No. 6 at p.21 in the Annex to the Information Paper.

outside Hong Kong. The Administration is not inclined to pursue the proposal.

8.18 As it presently stands, the Ordinance is unclear as to whether it applies to cases where the act of collection, holding, processing and use of personal data take place wholly outside Hong Kong.

8.19 Section 39(1)(d) provides that where none of the conditions specified is fulfilled in respect of the act or practice complained of, the PCPD may refuse to carry out or continue with an investigation initiated by a complaint. One of the conditions specified under section 39(1)(d)(i)(B) is where *"the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned"*.

8.20 Where personal data are "wholly collected, held, processed and used" by an organization or a person outside Hong Kong, the act or practice is likely to be subject to the applicable laws at the place that the act takes place or the practice is engaged in. By the operation of the territorial principle, certain territorial link with Hong Kong should exist in order for the Ordinance to apply.

8.21 It is however commented by the AAB in AAB No.16/2007[53] that section 39(1)(d) is not a provision dealing with extra-territorial application of the Ordinance and *"it does not provide the answer as to whether the Ordinance may have extra-territorial application"*. It was also decided that insofar as the person satisfies the definition of *"data user"* under the Ordinance exercising control over the personal data *"in or from Hong Kong"*, the Ordinance shall apply notwithstanding that none of the acts of collection, holding, processing or use of the personal data takes place in Hong Kong.

8.22 It would be unfair to the data user if the Hong Kong law and overseas law both govern the handling of the data not originated from Hong Kong, particularly where there is a conflict of laws situation. It then follows that a data user will face the dilemma of either breaching the Ordinance if it authorizes disclosure of the personal data to a foreign law

[53] Available at http://www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf

enforcement authority or faces the legal consequence (sometimes involving criminal sanction) under the applicable foreign law if it fails to comply with the lawful order issued under that law. The PCPD will also face practical difficulty to gather evidence on such overseas act or practice.

8.23 To deal with the anomaly, the Ordinance should be amended to exclude from its application personal data the collection, holding, processing and use of which occur wholly outside Hong Kong.

8.24 In paragraphs 12 to 13 in Annex 2 of the Consultation Document, the Administration states that the LRC considered it important that data protection law in Hong Kong should apply to a data user within the jurisdiction, even where the data have been transferred to or are being processed in another jurisdiction. The Administration is concerned that it might create a loophole in the proposed regime as a company in Hong Kong can arrange offshore collection of personal data by an agent and outsource the holding, processing and use of such data outside Hong Kong and it would make Hong Kong a data haven.

8.25 The PCPD does not see from the example given by the Administration that Hong Kong would become a data haven. According to the proposal, if any part of the data cycle of the personal data in question takes place in Hong Kong, the relevant data would still be protected under the Ordinance even if they are subsequently transferred outside Hong Kong. A Hong Kong company uses an offshore entity to collect personal data in Hong Kong, the company would still be caught by the proposed regime if the collection took place in Hong Kong. For those personal data that are collected, held, used and processed wholly outside Hong Kong, the PCPD does not see why they should be protected under the Hong Kong law. It should be noted that the LRC report was prepared 15 years ago. The situation should be reviewed in light of the economic development of the society during the last decade. Particularly, the PCPD is mindful of the proliferation of Hong Kong people establishing businesses outside Hong Kong, such as in the Mainland. For example, a person in Hong Kong owns a toy manufacturing business in the Mainland. The employees of the business are all employed in the Mainland and personal data of the

employees are collected, held processed and used wholly in the Mainland. The owner could not have expected that he had to comply with the Ordinance, being a Hong Kong law, in protecting the personal data of his employees in the Mainland. Nor could he have expected that the PCPD would have jurisdiction to deal with complaints made by his employees in the Mainland. It is also illogical to expect that, with so limited resources, the PCPD would be able to deal with complaints raised by complainants all over the world whose employers are in Hong Kong.

8.26 The PCPD therefore considers that it is highly desirable to consider the realistic proposition that the Ordinance should not apply to any act or practice involving personal data the collection, holding, processing and use of which occur wholly outside Hong Kong.

Public Interest Determination

8.27 This proposal was originally made by the PCPD[54] for the purpose of empowering the PCPD to make a public interest determination, with conditions, if any, imposed on a case-by-case basis upon application by the relevant data user. The Administration does not consider it appropriate to pursue such a proposal.

8.28 It is mentioned in paragraph 16 in Annex 2 of the Consultation Document that the proposal if instituted will undermine the certainty of personal data privacy protection afforded to data subjects. The PCPD does not agree with the view taken by the Administration. Many overseas jurisdictions have provisions in their data privacy legislations the public interest exemption.[55] Contrary to the Administration's view, the proposal, under which a data user who wishes to invoke public interest exemption shall apply to the PCPD for public interest determination, will provide for greater certainty by enabling a data user to release the relevant data in the public interest without contravening DPP3 where the circumstances require a timely disclosure.

---

[54] See PCPD's Proposal No. 33 at p.94 in the Annex to the Information Paper.

[55] See the relevant provisions of UK Data Protection Act, New Zealand Privacy Act and Australian Privacy Act as set out in paragraphs 14.2 to 14.5 of the Information Paper.

8.29 The Administration further states in paragraph 16 in Annex 2 of the Consultation Document that if there is justification to grant exemption on specific grounds, it is more appropriate to address them by way of specific public interest exemption. In PCPD's view, it is impracticable to provide an exhaustive list of public interest exemptions for or a public interest exemption that encompasses all appropriate situations. On the other hand, a general public interest exemption would provide for flexibility to accommodate all appropriate cases. The proposed public interest determination mechanism, which is operated on *ad hoc* basis upon application of the concerned data user, will enable the PCPD to determine whether there is justifiable overriding public interest that outweighs data privacy protection.

8.30 At the meeting of the Panel on Constitutional Affair of Legislative Council held on 15 December 2008, Legislative Council members queried on the deficiency of the Ordinance in enabling disclosure of personal data in the public interest. This proposal serves as a possible solution for the Administration's consideration.

8.31 The below examples show clearly the problems faced by data users when no such exemption exists:-

Example 1

In early February 2007, there were reports of incidents of failed Octopus EPS add-value transactions where Octopus cardholders failed to add value to their cards although monies were deducted from their bank accounts. Following the incidents, the Octopus Card Company identified a number of affected transactions and sought assistance from EPS Company (Hong Kong) Ltd to make the necessary refund. It was however discovered that the bank aecounts of some of the affected cardholders have been closed and the cardholders could not be located. While some other banks may have the new contact information of the affected persons, it would be in breach of DPP3 to disclose the information to the Octopus Card Company. Should the PCPD be conferred with the power as proposed,

it would be a justifiable case for making a determination.

Example 2

In 2006, the Secretary for Health, Welfare and Food decided to develop an organ donation computer database by the Central Organ Donation Registry to facilitate people registering as organ donors and to boost up the number of registered donors in Hong Kong. The Hong Kong Medical Association (HKMA) since 1994 had kept some 40,000 registered organ donors in its database. It would therefore be necessary for HKMA to release its own database to the Central Organ Donation Registry. In order to comply with DPP3, it would be necessary for the HKMA to seek consent from the relevant registered donors. However, it might not be practicable to seek their consents as contact details of the registered donors were not up to date. Should the PCPD be conferred with the proposed power to make public interest determination, it will be a justifiable case for the PCPD to exercise his discretion.

8.32 A practical advantage of adopting this approach than a general public interest exemption is that the PCPD may impose controls on the act or practice to be conducted or engaged in so as to tailor-made the case to maintain public interest at the minimal scarification of personal data privacy. For instance, a decision to allow the disclosure of personal data may saddle the data user with a prohibition in disclosing certain kind of data, such as identity card number or name. Instead of making a blanket public interest exemption, the proposed scheme represents a gradual process whereby the PCPD is charged with the function to determine in each and particular case whether there is justifiable overriding public interest that outweighs the data privacy right of individuals.

8.33 On the basis of the above, the PCPD urges the Administration to take on board the proposal.

Public Domain Exemption

8.34 This proposal[56] originated from the PCPD concerns the creation of a new exemption from DPP3 in respect of personal data available in the public domain. While the PCPD is open-minded to the proposal, the Administration does not see a case to take this proposal forward.

8.35 Currently, personal data gathered or obtained from the public domain by a data user are treated no differently from other personal data under the current provisions of the Ordinance. Personal data can be made known in the public domain by various means, such as by being contained in public records and obtainable through public search or inspection, e.g. court documents filed, records kept by public registries, etc. Another means is by way of publication in the media, such as a journalistic report or a public announcement. Question arises as to whether a data user is still required to observe the requirements under DPP3 where the personal data are available in the public domain.

8.36 The PCPD acknowledges that there are problems of using publicly available information for secondary purposes, such as the use of property owners' records from the Land Registry to provide a search of an individual's property ownership, the use of personal data contained in public register for direct marketing activities. Added to this is the improper use of personal data available on the Internet arising from data leakage incidents. On the other hand, there may be legitimate purposes to serve in checking an individual's financial status, such as property ownership, before deciding whether to institute legal proceedings or pursue a judgment debt against him.

8.37 It is therefore timely to consider whether personal data available in the public domain should be exempted from the data protection principle3.

---

[56] See PCPD's Proposal No. 36 in the Annex to the Information Paper.

Power to Search and Seize Evidence
Power to Call upon Public Officers for Assistance

8.38 These two proposals are bundled with Proposal No. 4 to confer power on the PCPD to carry out criminal investigation and to institute prosecution. Readers are invited to refer to PCPD's submissions made in paragraphs 4.2 to 4.11 above.

Power to Conduct Hearing in Public

8.39 This proposal to conduct hearing in public[57] was originated from PCPD but the Administration does not see there is a need to pursue.

8.40 Section 43(2) of the Ordinance provides that any hearing for the purpose of an investigation shall be carried out in public unless the PCPD considers otherwise or the complainant requested that the hearing be held in private. If the complainant's request is so received, under the current provision, the PCPD has no alternative but to accede to the request.

8.41 The PCPD finds the provision too restrictive that hinders public hearing. In cases when issues of public interest and importance are involved, members of the public should have a right to know and to be informed.

8.42 It is raised in paragraph 26 in Annex 2 of the Consultation Document that the LRC was concerned that the prospect of a public hearing could act as disincentive to the lodging of a complaint. Besides, the PCPD is already empowered to publish a report on the result of investigation under section 48(2) of the Ordinance.

8.43 In PCPD's view, the LRC's concern can be addressed by making it a proviso in the proposed amendment that the PCPD is required to consider all the circumstances of the case including the request from the complainant for the hearing to be conducted in private. Moreover, the PCPD considers that, while section 48(2) of the Ordinance enables the

[57] See PCPD's Proposal No. 15 at p.46 in the Annex to the Information Paper.

PCPD to publish a report after completion of an investigation, a requirement under section 43(2) of the Ordinance that a hearing shall be carried out in public is to ensure that the proceedings are conducted in an open and fair manner. In the PCPD's opinion, the concerns to be addressed by sections 43(2) and 48(2) are different.

8.44 The PCPD therefore considers that there is a need to review the current provision to enhance the right of the public to know and be informed.

Time Limit for Responding to PCPD's Investigation/Inspection Report

8.45 This proposal to shorten the data user's response period to a report to be published under the Ordinance from 28 days to 14 days was originally made by the PCPD.[58] The Administration does not consider it appropriate to take forward the proposal.

8.46 Generally speaking, the PCPD will choose to publish a report when he considers the case involving an issue of significant social or public interest, sometimes on matter which has already been widely reported by the media. The effectiveness of sending out the message through the report will be hampered or diminished if it is not being reported timely.

8.47 The length of the notice period to respond to a report to be published by the PCPD under section 48 was prescribed when the Ordinance was first enacted. The notice period of 28 days should be reconsidered in light of the rapid development in technology and telecommunication which has profoundly enhanced efficiency in the decision making process.

8.48 Since the right of the relevant data user to comment on the draft report extends only to advising on any exempted matter contained in the report but not the contents of the report in general, it is considered that the period of 28 days to be excessively long. The PCPD therefore finds it necessary to shorten the period to 14 days.

---

[58] See PCPD's Proposal No. 31 at p.90 in the Annex to the Information Paper.

Annex 3 to the Consultation Document - Miscellaneous Proposed Amendments to the Ordinance

Proposal No. 32 : Power to Obtain Information to Verify a Data User Return

9.1 This proposal was originally made by the PCPD[59] in order to confer power on the PCPD to obtain information from any person in order to verify the particulars in a data user return filed under section 14 of the Ordinance.

9.2 Pursuant to section 14 of the Ordinance, the PCPD may, by notice in the Gazette, specify a class of data users to submit data user returns. The data user return shall be in a specified form and shall contain the prescribed information sets out in Schedule 3 of the Ordinance. The prescribed information now covers name and address of the data user, the kind of personal data collected, the purposes of collection, the classes of transferees of the data, the places to which the data will be transferred outside Hong Kong and the name and address of the individual to whom data access request may be made. The particulars in the data user return are made available for public inspection pursuant to section 16 of the Ordinance.

9.3 At present, there is no express power conferred under the Ordinance on the PCPD to obtain information from any person to verify the particulars stated in the data user return. The PCPD therefore proposes that such express power be provided under the Ordinance so that when there are reasonable grounds for believing that any particulars stated in the data user return are not true or accurate, the PCPD may exercise the power to obtain any information from any person to verify the particulars.

9.4 Apart from this proposal, the PCPD has also proposed to empower the PCPD to specify, from time to time, the "prescribed information" required to be submitted by a data user in a data user return. It will give more flexibility to the disclosure mechanism in a data user return, taking into account the changing needs and aspiration of privacy protection. Take the recent series of data security breaches as an

[59] See PCPD's Proposal No. 44 at p.126 in the Annex to the Information Paper.

example, if the proposal is taken on board, the PCPD may by notice in the Gazette, require a data user to include in the data user return information relating to data security breach. The proposal will increase the transparency of the data protection policies and practices adopted by data users and provide effective and efficient dissemination of the information to the general public. Individuals' trust and confidence on data users' determination to protect personal data privacy will be much enhanced which will ultimately benefit the data users in building up their reputation. Nowadays, transparency and accountability of data users are the focus of privacy governance. In order to face the challenge to personal data privacy in this electronic age, data protection must be robust, yet flexible. The PCPD therefore urges the Administration to pursue this proposal.

Proposal No. 36: Definition of Crime under Section 58

9.5 This was a proposal originated from PCPD[60] for the purpose of clarifying the scope of application of the exemption provision under section 58 by defining the word "crime". The Administration has made modification to the definition proposed by PCPD.

9.6 The Ordinance as it currently stands does not define the words "crime", "offenders" or "unlawful conduct" which are found in the exemption provision of section 58 of the Ordinance. Doubts were cast on the ambit of the exemption provision under section 58 of the Ordinance as to whether it is wide enough to cover overseas crimes and offences so that a data user can properly invoke the exemption in disclosing personal data to an overseas law enforcement agency for investigation of a foreign crime. It is therefore the aim of the proposal to clarify the scope of the application of the exemption.

9.7 In Hong Kong, the Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525 ("MLAO") regulates the provision and obtaining of assistance in criminal matters between Hong Kong and places outside Hong Kong. Section 5(1)(g) of the MLAO provides that "a request by

[60] See PCPD's Proposal No. 3 at p.12 in the Annex to the Information Paper.

a place outside Hong Kong for assistance under this Ordinance shall be refused if, in the opinion of the Secretary for Justice, the request relates to an act or omission that, if it had occurred in Hong Kong, would not have constituted a Hong Kong offence".

9.8 The PCPD finds important public policy consideration when construing "crime", "offenders" or "unlawful conduct" in section 58. Having regard also to the territorial principle of the Ordinance, the PCPD considers it sensible, prudent and reasonable to interpret the words "crime" or "offenders" under section 58(1)(a) and (b) to mean "(i) an act or omission that is punishable as an offence under the laws of Hong Kong or (ii) an act or omission for which legal assistance under the Mutual Legal Assistance in Criminal Matters Ordinance, Cap 525 has been sought and obtained". And the criminal aspect of the meaning of "unlawful conduct" should be construed accordingly. The Administration's proposal modifies the PCPD's original proposal by replacing the meaning in (ii) by "a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation".

9.9 In this respect, the PCPD notes that under the MLAO, a territory will have to enter into an agreement with the Government of the HKSAR in relation to legal or law enforcement cooperation on criminal matters. By an order made by the Chief Executive in Council, the MLAO shall be made applicable as between the HKSAR and such territory subject to modification. A request for legal assistance in criminal matters has to be made to the Secretary for Justice and should satisfy the requirements specified under the provisions of the MLAO.

9.10 On careful examination of the wordings proposed by the Administration in the definition, the PCPD notes that there is no express reference to the request for assistance being made and obtained under the MLAO. This raises the concern that it may leave rooms for a local data user to rely on the relaxed exemption to disclose personal data to overseas authorities irrespective whether a request has been made to the Secretary for Justice for legal assistance under the MLAO. Such relaxation is not desirable from the perspective of personal data protection. In order to strike a proper balance between personal data privacy and investigation of crime,

the PCPD recommends the Administration to modify their proposal so that the definition will expressly refer to a request for assistance sought and obtained under the MLAO.

Other Proposals

10.1 The above submissions are made in respect of proposals which are more controversial in nature. The PCPD supports other proposals stated in the Consultation Document as listed in the Schedule attached. References to the corresponding proposals originally made by the PCPD are stated in the footnotes. Readers may refer to the relevant PCPD's original proposals in the Information Paper to better understand the underlying reasons for proposals.

- END -

III. Schedule

The PCPD supports the below proposals:-

Proposal No.	Brief Description
15	Access to Personal Data in Dispute[61]
16	Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation[62]
17	Erasure of Personal Data[63]
18	Fee Charging for Handling Data Access Requests[64]
19	Response to Data Access Requests in Writing and Within 40 Days[65]
24	Transfer of Personal Data in Business Mergers or Acquisition[66]
25	Provision of Identity and Location Data on Health Grounds[67]
26	Handling Personal Data in Emergency Situations[68]
28	Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result[69]
29	PCPD to Disclose Information in the Performance of Functions[70]
30	Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit[71]

---

61 See PCPD's Proposal No. 25 at p.70 in the Annex to the Information Paper.
62 See PCPD's Proposal No. 23 at p.65 in the Annex to the Information Paper.
63 See PCPD's Proposal No. 43 at p.124 in the Annex to the Information Paper.
64 See PCPD's Proposal No. 26 at p.73 in the Annex to the Information Paper.
65 See PCPD's Proposal Nos. 21 and 55 at p.61 and p.146 respectively in the Annex to the Information Paper.
66 See PCPD's Proposal No. 38 at p.111 in the Annex to the Information Paper.
67 See PCPD's Proposal No. 32 at p.92 in the Annex to the Information Paper.
68 See PCPD's Proposal No. 34 at p.99 in the Annex to the Information Paper.
69 See PCPD's Proposal No. 48 at p.131 in the Annex to the Information Paper.
70 See PCPD's Proposal No. 30 at p.87 in the Annex to the Information Paper.
71 See PCPD's Proposal No. 18 at p.52 in the Annex to the Information Paper.

31	Power to Impose Charges for Educational and Promotional Activities[72]
33	Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings[73]
34	Transfer of Records for Archival Purpose[74]
35	Refusal to Comply with a Data Access Request on Ground of Self-Incrimination[75]
37	Expand the Definition of "Relevant Person"[76]
38	Exclude Social Services from the Definition of "Direct Marketing"[77]
39	Exemption for Personal Data Held by the Court or Judicial Officer[78]
40	Extend Time Limit for Laying Information for Prosecution[79]
41	Duty to Prevent Loss of Personal Data[80]
42	PCPD to Serve an Enforcement Notice together with the Results of Investigation[81]
43	Contact Information about the Individual Who Receives Data Access or Correction Requests[82]

72 See PCPD's Proposal No. 9 at p.30 in the Annex to the Information Paper.
73 See PCPD's Proposal No. 35 at p.103 in the Annex to the Information Paper.
74 See PCPD's Proposal No. 37 at p.109 in the Annex to the Information Paper.
75 See PCPD's Proposal No. 22 at p.63 in the Annex to the Information Paper.
76 See PCPD's Proposal No. 4 at p.15 in the Annex to the Information Paper.
77 See PCPD's Proposal No. 28 at p.83 in the Annex to the Information Paper.
78 See PCPD's Proposal No. 7 at p.24 in the Annex to the Information Paper.
79 See PCPD's Proposal No. 17 at p.50 in the Annex to the Information Paper.
80 See PCPD's Proposal No. 56 at p.149 in the Annex to the Information Paper.
81 See PCPD's Proposal No. 49 at p.133 in the Annex to the Information Paper.
82 See PCPD's Proposal No. 42 at p.122 in the Annex to the Information Paper.

S0098

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
30/11/2009 10:03 Subject Consultation Document on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

To whom it may concern,

Attached our comments for your consideration.

Thanks

(name)

CONFIDENTIAL NOTE: The information contained in this email is intended only for the use of the individual or entity named above and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, please immediately notify the sender and delete the mail. Thank you.

12 major proposals to the review of PDPO with comments 2 with no suggestions.DOC

(The sender requested anonymity)

onsultation Paper - Review of the Personal Data (Privacy) Ordinance (Deadline : 30 Nov 2009)
2 Major Proposals

Sensitive Personal Data

oposal No. 1 **Sensitive Personal Data**

sues

At present, the PDPO does not differentiate personal data that are "sensitive" from those that are not. There is a need to consider whether the processing of sensitive personal data should be subject to more stringent data protection requirements to better protect the personal data privacy of individuals.

Nil

Data Security

oposal No. 2 **Regulation of Data Processors and Sub-contracting Activities**

sues

Handling of personal data in electronic form increases the privacy risks and is particularly the case when sensitive personal data in electronic form are transmitted to an outsourced agent or contractor for handling. Data security measures would need to be stepped up, particularly where outsourcing is involved, as a preventive measure. On the remedial front, measures would need to be mapped out to contain the damage to individuals affected by data leakage incidents.

At present, the PDPO does not directly regulate the activities of an outsourcing service provider (agent / data processor). However the data user who engages the agent to process the personal data is to be held liable for any acts done by data processor and also sub-contractor. As this would be unfair and pose onerous burden to data users if we solely rely on the data user to ensure privacy protection by data processor. And, it is inevitable that we, as a data user, need to outsource certain functions to sub-contractors due to business and operational needs. We also understand that in the process of which may involve transfer of personal data to sub-contractors. However, regarding such personal data provided by us to the sub-contractors, since the sub-contractors are under no regulatory requirements to comply with PDPO and data users are solely liable for such compliance, the only way to ensure compliance is by contractual means, and we believe that all data users who engage sub-contractors in this regard would in fact have similar contractual means to safeguard their own interests. However, as contractual obligations are merely of a commercial nature, regardless of how well we have conducted our due diligence in identifying the competent sub-contractors, it may still be possible for sub-contractors to choose not to comply with contractual obligations based on commercial reasons, and at the end the data users may be in breach of PDPO requirements despite having contractual obligations in place, thus the rights of the data subjects are impaired. In this regard, we are in support of the proposal that direct obligations of regulatory nature on sub-contractors are preferable, and depending on the functions they carry out on behalf of the original data users, and the type of industry that the original data users are in, different obligations may be necessary. In addition, this direct regulation will need to have a clear definition, guidelines with clear processes and communications to put it in full force.

oposal No. 3 **Personal Data Security Breach Notification**

sues

At present, there is no requirement under the PDPO for a data user to notify the PCPD or individuals affected by a data leakage incident. We need to consider whether a personal data security breach notification ("privacy breach notification") system should be instituted to require organizations to notify the PCPD and affected individuals when a breach of data security leads to the leakage or loss of personal data so as to mitigate the potential damage to affected individuals.

We agree with the voluntary notification mechanism which would require a data user to notify the PCPD on those with significant impact, and to

S0098

consider whether individuals should be notified, taking into account the potential harm caused by the breach. However, such voluntary notification should be generically applicable to all data users and / or data processors of all industries to ensure level playing field. There should be a clear guideline on voluntary breach notifications clearly stating under what conditions notification is required, and consequences to data users for late notification. And, if voluntary notification to both PCPD and data subjects is to be imposed, PDPO should also indicate whether there are other reporting requirements under law or requirements by industry associations for the same or for more stringent purposes, whether compliance of those would prevail over compliance with PDPO.

Enforcement Powers of the PCPD

oposal No. 4 **Granting Criminal Investigation and Prosecution Power to the PCPD**

sues The PCPD cannot conduct search for or seize evidence, carry out criminal investigation or initiate prosecution on his own. Criminal investigations are conducted by the Police and prosecutions, where necessary, are initiated by the Department of Justice.

We prefer status quo. The Authorities under existing arrangement should be adequate for carrying out investigations, and believe that criminal investigation and prosecution powers currently vested with the police and DOJ are sufficient. By changing the current framework, it will also create confusion and duplication of effort and wasting of resources.

oposal No. 5 **Legal Assistance to Data Subjects under Section 66**

sues At present, the PDPO does not empower the PCPD to provide assistance to aggrieved data subjects in respect of legal proceedings under Section 66. These individuals would have to bear all the legal costs themselves unless they are qualified for and have successfully obtained legal aid.

We prefer status quo. Existing practice should be followed and to avoid double standard of legal aid system, if any.

oposal No. 6 **Award Compensation to Aggrieved Data Subjects**

sues The PDPO is considering the option of empowering the Privacy Commissioner to determine the amount of compensation, so as to provide a quick and effective redress to the aggrieved party through mediation.

Disagree with the proposal, and might create conflict of interest between proposal 5 & 6.

Offences and Sanctions

oposal No. 7 **Making Contravention of a Data Protection Principle ("DPP") an Offence**

sues At present, contravention of a DPP by itself is not an offence under the PDPO. Instead, the PCPD is empowered to remedy the breach by issuing an enforcement notice to direct the data user to take specified remedial steps within a specified period. It is only when the data user contravenes the enforcement notice will he commit an offence under Section 64(7), and be liable on conviction to a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

We oppose to making contravention of a DPP an offence. The fact that the DPPs are listed as "principles" in the schedule and not even as specific provisions under the PDPO indicate that these DPPs are meant to be as general guiding principles only, so to make them to become criminal offences seem inconsistent with the original legislative intention. Besides, it is particularly impractical for certain DPP e.g. DPP5, which requires a data user to ensure openness and availability of his personal data policies, the contravention can simply be rectified without the need to increase the deterrent effect by making it an offence.

oposal No. 8 **Unauthorized Obtaining, Disclosure and Sale of Personal Data**

S0098

sues

At present, use of personal data is regulated by DPP 3, and contravention of any DPPs per se is not an offence. In view of the seriousness of the intrusion into personal data privacy and the gravity of harm that may cause to the data subjects as a result of the intentional or willful act of the person in flagrant disregard of the personal data privacy of others, the PCPD has to seriously consider whether such blatant acts should be subject to criminal sanction.

If in general contravention of DPPs is not an offence, we do not agree that particular acts out of these DPPs should be made as offences.

·oposal No. 9 **Repeated Contravention of a Data Protection Principle on Same Facts**

sues

It is possible that a data user, may resume the same contravening act or practice shortly after compliance with an enforcement notice issued against him. Under the existing provisions, the enforcement action at the disposal of the PCPD will be to issue yet another enforcement notice.

Again, if in general contravention of DPPs is not an offence, we do not agree that repeated contravention of a DPP on same facts should be made as offences. And existing mechanism is considered sufficient to achieve a deterrent effect.

·oposal No. 10 **Imposing Monetary Penalty on Serious Contravention of Data Protection Principles**

sues

Considered empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs so as to strengthen the enforcement of the PDPO and to deter serious contravention of DPPs.

Disagree with the proposed. There seems no segregation of duties among proposals 4, 5, 6 and 10. Besides, there is no independent review of the process and over empowering PCPD, and existing arrangement is considered as sufficient. On the other hand, if monetary penalty is to be imposed for serious contravention of DPPs, PDPO should indicate clearly what is considered as "serious contravention" which may be different between data users in different industries; the type of personal data; and the exceptions / defences, etc. But overall, we oppose the imposing of monetary penalty on contravention of DPP.

·oposal No. 11 **Repeated Non-compliance with Enforcement Notice**

sues

At present, it is an offence under Section 64(7) of the PDPO for a data user to contravene an enforcement notice issued by the PCPD. On conviction, the data user is liable to a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, a daily fine of $1,000. The PDPO does not provide for heavier sanction for repeated offenders of Section 64(7), thus considering the option to subject a repeated offender to heavier penalty to achieve greater deterrent effect.

Nil

·oposal No. 12 **Raising Penalty for Misuse of Personal Data in Direct Marketing**

sues

Direct marketing calls are often a cause of complaint and nuisance to the data subjects. The PCPD is of the view that the existing level of penalty may not be sufficient to act as an effective deterrent to contain the problem and recommends the penalty level be raised. There were also calls within the community to raise the penalty level to curb these annoying direct marketing calls. In a case brought before the court concerning the making of direct marketing calls by a telecommunications company, the Magistrate remarked that the maximum penalty of $10,000 under the PDPO can hardly act as an effective deterrent for large companies.

Disagree. Some misuse of personal data may be caused by misconduct of individuals who may have been working (in current employment or in prior employment) in sub-contractor of data processors. It is unfair to final data users where those misbehaved individuals are not under the

governance system. In general, existing arrangement is considered as sufficient.

S0098

香港家庭福利會

(Incorporated with Limited Liability)

HONG KONG FAMILY WELFARE SOCIETY

S0099

Patron: The Honourable Donald Tsang, GBM, Chief Executive of the Hong Kong Special Administrative Region
贊助人：香港特別行政區行政長官曾蔭權GBM

President
Dr. Eric Li Ka-cheung, GBS, OBE, JP
Chairman
Mr. Christopher Law
Vice-Chairman
Mrs. Betty Cheng
Hon. Treasurer
Mr. Patrick S.S. Cheng
Executive Director
Mrs. Cecilia Kwan

since 1949

By Fax & By Post

27 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Sir/Madam,

Views towards " Review of the Personal Data (Privacy) Ordinance"

Attached please find the views of Hong Kong Family Welfare Society towards the review of the captioned Ordinance, for your consideration.

Any enquires please do not hesitate to contact our Senior Manager (Enhancement & Facilitation), (deleted)

Thanks for your attention.

Yours faithfully,

(Signed)

Cecilia Kwan (Mrs.)
Executive Director

60th Hong Kong Family Welfare Society
Love for Family · Passion to Serve

S0099

Hong Kong Family Welfare Society

Views towards "Review of the Personal Data (Privacy) Ordinance"

The following are our views towards the proposed amendment to the Personal Data (Privacy) Ordinance (PDPO), for your consideration:

Proposal No. 1: Sensitive Personal Data

1. Subsection 3.09 (f): For the removal of any doubt, we suggest that the handling of data for social welfare purposes by social work professionals should enjoy the same exemption as the handling of data for medical purposes by health professionals.

   Thus, we suggest subsection 3.09 (f) should read as follows: "Handling of the data is necessary for medical or social welfare purposes and is undertaken by a health or social work professional or person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health or social work professional."

Proposal No. 3: Personal Data Security Breach Notification

2. We support that the affected individual of a leakage or loss of personal data incident should be early notified if there is an assessment of possible risk or harm to the individual concerned, for the sake of protection. A personal data security breach notification system should be introduced under the requirement of the Ordinance.
3. We recommend that the Privacy Commissioner for Personal Data ("PCPD") should propose general criteria for the risk assessment, yet allow data users in different industry and profession to propose their specific criteria.
4. We propose that PCPD should provide guidance to organizations regarding "best practice" to prevent and handle the loss of personal data incident. To ensure the compliance to the best practice guide, we support the reporting of the incident to PCPD if it is assessed to have serious harm to the affected individual.

Proposal No. 14: Parents' Right to Access Personal Data of Minors

5. For the avoidance of domestic violence, we regard it as essential that a parent suspected of abuse of a child should not be able to use the "machinery" of PDPO either in person or by an agent to ascertain the whereabouts of such a child and/or the other parent. This could be brought about by amending the definition of "relevant person" in Section 2 of the Ordinance to exclude such a suspected abuser from access to the type of information just referred to.

6. In the same way that parents have rights, so do the children. We think that one of the factors which should be taken into account wherever possible before granting a parent or a relevant person access to a child's personal data is the attitude expressed by the child towards the disclosure of his personal data. This can only apply to children of sufficient understanding and intelligence to know the nature and significance of the application. The older the child is, the more important it is to know his/her attitude towards such disclosure.

7. However, there are no objective criteria to assess whether a child has sufficient understanding or intelligence to fully understand the disclosure. Thus, we propose that the PCPD should provide guidance on the objective criteria.

8. Furthermore, we support your proposal for the introduction of a new provisions to permit a data user to refuse a data access request made by a "relevant person" on behalf of a minor, if the data user has reasonable grounds to believe that the relevant person may abuse the data access mechanism to obtain the personal data of the minor.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

9. If the definition of "relevant person" in PDPO is amended in the way we have suggested in Proposal No. 14, there ceases to be a need for any "third party". Therefore, we propose to allow "relevant person" to give prescribed consent to change of use of personal data.
10. Before consenting to any change of use of personal data in relation to a minor, the "relevant person" should wherever possible ascertain the attitude expressed by the minor towards the proposed change of use of such data.

Proposal No. 25: Provision of Identity and Location Data on Health Grounds

11. We support the extent of the scope of application of exemption to cover personal data relating to the identity and location of the data subjects since it facilitates Social Welfare Agency to provide timely support for those in need of assistance. However, it should be restricted to extreme circumstances, where public bodies such as the Police, Social Welfare Agency or Immigration Department become involved to deal with emergencies or crisis.

Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

12. With a family perspective, we are committed to support "relevant person" to carry out their responsibility effectively, for the benefits of the child. Disclosure of the children's personal data is one of the effective means to facilitate them to fulfill their responsibilities.

13. In principle, we support the provision of an exemption from Data Protection Principle 3 to permit transfer of personal data of minors to a "relevant person".

14. However, such exemption should be restricted to the situation, with specific conditions which are absolutely necessary. And we suggest the following conditions for the transfer:
    - It is for the best interest of the minor, AND
    - For the protection of the minor when there is sufficient ground to raise serious concern about the safety of the minor

    Before deciding to the transfer of personal data in relation to a minor, the "relevant person" or the data user should wherever possible ascertain the attitude expressed by the minor towards the disclosure of such data.

- End -



To pdpo_consultation@cmab.gov.hk
cc
bcc
30/11/2009 02:02 Subject 檢討《個人資料（私隱）條例》的公眾諮詢
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Date: Nov 30, 2009

香港下亞厘畢道
中區政府合署東座364室
政制及內地事務局（第4組）

檢討《個人資料（私隱）條例》的公眾諮詢

資料保安

本人發覺有某些商業機構的前僱員，例如地產代理，帶同客戶資料離職。本人相信前僱主定不會將有商業價值之資料拱手讓予競爭者，故該等資料便是盜取及非法轉移，應定為刑事罪行

個人資料外洩通報機制

因通訊資料不全或已变，資詢文件內之通報機制建議，很多時可能不能履行

罪行及制裁

如上述地產代理的例子，本人同意咨詢文件之建議8：在未經授權下取得、披露和出售個人資料，訂為罪行

檢討時中的原則

對於在進行檢討時，貴方以下述原則為依據：(c) 對私隱法例作出的任何修改，都不應削弱香港作為國際城市的競爭力和經濟效率。 本人強烈反對這項原則。 因為七百萬市民之私隱，較為重要，不能為了經濟利益，而放棄對人的尊重。就如美國以往有很多人反對環保，認為會削弱經濟

敏感個人資料

3.03 海外司法管轄區普遍認為，敏感個人資料包括種族或民族本源、政治意見、宗教或哲學信仰、工會會籍、健康狀況及性生活。我認為，政治意見可以被第三者有意無意錯誤詮釋，

信仰、工會會籍、健康狀況及性生活。我認為，政治意見可以被用二有用意無意錯誤詮釋，或有目的地作轉述。 所以應受到約束

違反規定的制裁

3.12 目前，違反保障資料原則本身並非犯罪。本人認為這項原則欠缺效率，應該改變

為資料當事人提供法律協助

(a) 有關個案涉及一個原則問題

意見: 即涉及社會整體利益，便應提供法律協助

(b) 在顧及有關個案的複雜程度、申請人相對於答辯人或受牽涉的其他人的位置或任何其他事宜下，期望該名申請人，在沒有協助的情況下處理該個案並不合理

意見: 就如消委會的案件一樣，現實中申請人多為個人，相對多為公司機構的答辯人一定勢弱。 貴方建議的結果會引致大多數案件都會有協助。 故此本人對這有保留

刪除個人資料

本人發覺，某些資料使用者會將他人個人資料保持非常長的時間，甚至似是無了期。 就算客戶已一直沒有與之交易，公司的銷售電話亦不斷。 所以本人建議要立刪除期，e.g. 訂明五年為限

Yours faithfully,
Kiwi Chan



SWIRE PROPERTIES

S0101

30th November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

By email: pdpo_consultation@cmab.gov.hk

Dear Sirs,

Responses to Consultation Document on Review of Personal Data (Privacy) Ordinance

We are pleased to submit the attached responses to the Consultation Document on Review of Personal Data (Privacy) Ordinance.

Yours sincerely,
For and on behalf of
Swire Properties Limited

Doris Chu
Head of Human Resources & Administration

Encl.

Responses to Consultation Document on Review of Personal Data (Privacy) Ordinance

Proposal No. 1: Sensitive Personal Data

Whether there is a need to accord better protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances; and

No. We do not consider that the additional cost and burden of complying with such a prohibition is justified by its apparent benefits.

If yes, whether the possible regulatory regime, including coverage of sensitive personal data, related regulatory measures, sanctions, and the need for grandfathering or transitional arrangement as set out in paragraphs 3.08 to 3.14, is appropriate.

If such a prohibition is imposed, the information covered should be limited to the biometric data referred to in 3.08 of the Consultation Document, there should be exceptions to the prohibition as described in 3.09 of the Consultation Document (but the medical exception should be broadened as described below), the prohibition should be subject to the existing enforcement regime (that is only breach of an enforcement notice should give rise to penalties) and the handling of existing biometric information should not be prohibited (that is there should be grandfathering arrangements not transitional arrangements). The medical exception should be broadened so that it applies to the handling of sensitive personal data for any purpose related to health or safety.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

Whether a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties;

No. It is inappropriate for data users, as private persons, to have a responsibility to police compliance with the law by other private persons (data processors). In any event imposition of contractual obligations will not necessarily result in compliance. The data processors may simply breach the contractual provisions.

Whether the activities of a data processor should be directly regulated under the PDPO or whether it is sufficient to indirectly regulate the data processor through the data user by contractual or other means; and

Having regard to the discussion in the Consultation Document (in particular in relation to the practical difficulties for data processors of compliance), we do not think that the activities of data processors should be directly regulated.

We would also mention that direct regulation of data processors would risk driving them offshore to jurisdictions where they were not regulated, to the detriment of the Hong Kong economy and Hong Kong's international competitive position. For the reasons given in the previous response, we do not think that activities of data processors should be regulated by contractual means.

If activities of data processors were to be directly regulated under the PDPO, what obligations should be imposed on data processors, and whether it is appropriate and practical to subject different categories of data processors to different obligations.

Not strictly applicable, in the light of our previous response, although we would not object to the suggestion in 4.19 of the Consultation Document that data processors should have a privacy policy (so long as no attempt was made in or through the legislation to describe what the elements of that policy should be).

Proposal No. 3: Personal Data Security Breach Notification

The need to institute a voluntary privacy breach notification system in Hong Kong.

We agree that a breach notification system should not be compulsory. We are not aware of evidence that timely and sufficient notification of material breaches is not being given (and this is unsurprising given that the two most likely sources of material breaches, government and the financial industry, have voluntary systems in place). This being so, we do not think that anything further needs to done by way of legislation or guidelines in this area.

The components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42, including:

(i) the circumstances under which notification should be triggered;

(ii) to whom the notice of breach should be sent;

(iii) timing of the notice;

(iv) by what means should the notice be sent;

(v) the content to be covered in the notice; and

(vi) the consequences of failing to give notification.

Not applicable in view of our previous response.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

Whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.

Having regard to the discussion in the Consultation Document, we agree that the status quo should be maintained, particularly in the light of the very small numbers of prosecutions actually undertaken and the general desirability of an objective assessment (by the Department of Justice) as to whether a prosecution is justified in any particular case.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

Whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under Section 66 of the PDPO, along the lines of the EOC model.

We do not support the conferring of this power. It seems to us that there is nothing peculiar to the privacy legislation which would justify taxpayers' money being made available to pursue a civil action under the legislation in circumstances where taxpayers' money would not be so made available under normal legal aid principles.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

Whether it is appropriate to introduce at this stage an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Having regard to the discussion in the Consultation Document (in particular the point made by the Law Reform Commission that conferring such a power would vest in a single authority an undesirable combination of enforcement and punitive functions), we do not support the conferring of such a power.

Proposal No. 7: Making Contravention of a DPP an offence

Whether we should make contravention of a DPP an offence.

Having regard to the discussion in the Consultation Document (in particular in relation to the impact on civil liberties and the original intention of the DPPs), we do not support making the contravention of a DPP an offence.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

Whether we should make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent; and

We have no objection to the creation of such an offence, so long as it is confined to disclosure for profit. Malicious purposes is too broad and uncertain a term. .

If yes, the need for defence provisions and the appropriate level of penalty.

If the offence is confined as proposed by us, we would not see the need for specific defences. If an offence along the UK lines is created, the UK defences should be applicable. We have no particular views on the level of penalty.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

Whether it is appropriate to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice; and

Having regard to the discussion in the Consultation Document (in particular the absence of repeat offences in practice) we do not consider it appropriate to create such an offence.

If yes, the appropriate penalty level for the offence bearing in mind that non-compliance with an enforcement notice is subject to a fine of $50,000 and to imprisonment for two years.

Not applicable, in the light of our previous response.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

Whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

Having regard to the discussion in the Consultation Document, we do not consider it appropriate to impose such penalties.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

Whether heavier penalty should be imposed for a second or subsequent conviction of Section 64(7); and

Given the lack of prosecutions for repeat offences referred to in the Consultation Document, we do not think such heavier penalties are necessary.

If yes, the appropriate penalty level, bearing in mind the existing enalty level for contravention of an enforcement notice which is a fine at Level 5 (up to $50,000) and imprisonment for two years, and in case of a continuing offence, a daily fine of $1,000.

Not applicable, in the light of our previous response.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

Whether the penalty for misuse of personal data in direct marketing (i.e. contravention of the requirement under Section 34(1)(ii)) should be raised; and

We have no views on this proposal.

If yes, the appropriate level of penalty.

Not applicable, in the light of our previous response.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

We support this proposal.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

We have no views on this proposal, save to say that, if the proposal is implemented, the legislation should impose no obligation on the data user (expressly or by implication) to form an opinion on whether the disclosure is in the interests of the minor.

Proposal No. 15: Access to Personal Data in Dispute

We support the proposal (as set out in paragraph 16 of Annex 1).

Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We support the proposal that the PDPO should be amended so that a data user need not comply with a data access request if the data user is entitled or bound by other legislation not to disclose the relevant information.

Proposal No. 17: Erasure of Personal Data

We support the proposal for the amendment of the PPDO set out in paragraph 23 of Annex 1.

Proposal No. 18: Fee Charging for Handling Data Access Requests

We do not think that the legislation needs changing, given what we assume is a relatively modest number of complaints about excessive charges. In addition, given the speed of technological change, any attempt to prescribe

particular maximum charges for particular items runs the risk of very rapid obsolescence.

Proposal No. 19: Response to Data Access Requests in Writing and Within 40 days

We think it undesirable to create a special regime for the police, though we understand that, if the legislation is amended as suggested, they will need a special regime. We think the better solution is not to amend the legislation.

Proposal No. 20: Circumstances for Issue of an Enforcement Notice

We have no views on the option in paragraph 39 of Annex 1.

Proposal No. 21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

We have no views on the option in paragraph 40 of Annex 1.

Proposal No. 22: Removing the Time Limit to Discontinue an Investigation

We have no views on the option in paragraph 43 of Annex 1.

Proposal No. 23: Additional Grounds for Refusing to Investigate

We have no views on the appropriateness of including the specific grounds referred to in paragraph 48.

Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

We support the exemption of such transfers. We think that the only condition necessary is that the transfer is required for the purposes of due diligence.

Proposal No. 25: Provision of Identity and Location Data on Health Grounds

We support changes to the legislation so that it operates along the lines described in paragraph 56 of Annex 1.

Proposal No. 26: Handling Personal Data in Emergency Situations

We support the proposed exemptions.

Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

We have no views on this proposal.

Proposals not to be Pursued

We agree that none of the proposals identified as not to be pursued need to be pursued.

Miscellaneous Proposed Amendments to the PDPO

We have no objection to the miscellaneous proposed amendments to the PDPO.

S0102

Our Ref :

Your Ref :

香港下亞厘畢道
中區政府合署東座 364 室
政制及內地事務局(第四組)

敬啓者：

關於「個人資料(私隱)條例建議」諮詢文件意見

就政制及內地事務局於二零零九年八月發出的檢討「個人資料(私隱)條例建議」諮詢文件，本會十分關注，並就文件之內容諮詢本會同工之意見及整理了有關建議。

現隨函附上本會對諮詢文件的意見，以供參考。祈盼　貴局在搜集各方意見後，能制定出完善的方案，以確保條例足以保障個人資料。如有任何查詢，歡迎致電 (刪除) 與本會服務總監 (刪除) 聯絡。

副總幹事

(已簽署)

二零零九年十一月二十六日

「檢討<個人資料(私隱)條例>諮詢文件」意見

協會已就關於檢討<個人資料(私隱)條例>諮詢文件鼓勵同工作出討論，對諮詢文件的主要建議，現將意見撮要如下：

建議 1： 敏感個人資料(如指紋)應否受更嚴格的規管，即需要限定在指定的情況下才可收集、持有、處理和使用敏感個人資料，藉以爲該等資料提供更佳的保障。

意見： 大部份同工表示同意此項建議，並認爲應嚴格執行。

由於敏感個人資料通常是個人獨有的，如沒有妥善監管及保存，容易被人盜用，對於資料擁有人可帶來極大的傷害，故認同收集過程中，要確保有健全嚴管政策及保障制度讓資料持有人可以清楚了解收集用途，當然，如收集原因涉及出入境及保安等用途，則政府應有權向需要人士收集。

另有同工建議個人資料應該因應敏感程度予以不同處理方法，至於何者該納入「敏感資料」則需透過諮詢以達成共識。此外，有同工認爲除生物辨認資料外，病歷及個人財政狀況亦屬較敏感類別。

建議 2.1： 應否規管受託處理個人資料的資料處理者?
應否規定資料使用者在把個人資料判予第三者處理時，以合約方式或其他方法確保對方履行私隱條例所訂的有關責任?

意見： 大部份同工均表示應該，認爲目前之條例並不能有效地監管資料處理者之操守。所有資料提供者在有私隱條例保障的情況下提供自己的個人資料，故當資料使用者在把個人資料判予第三者處理時，爲保障資料提供者的權益，資料使用者理應以合約方式或其他方法確保對方履行私隱條例所訂的有關責任。

建議 2.2： 應否在私隱條例下直接規管資料處理者的活動，抑或透過資料使用者以合約方式或其他方法間接規管資料處理者已足夠?

意見： 部份同工認爲應該直接規管資料處理者的活動，會對資料擁有者較有保障。

部份同工則認爲透過資料使用者以合約方式或其他方法間接規管資料處理者已足夠。因當資料處理者承諾履行合約的內容時已表示其行爲已受到私隱條例的監管。

建議 2.3： 如在私隱條例下直接規管資料處理者的活動，應向資料處理者施加什麼責任，以及向不同類別的資料處理者施加不同責任是否恰當及切實可行?

意見： 大部份同工認爲應向資料處理者施加的責任是按照私隱條例處理個人資料。資料處理者於處理前應明確知道保密是非常重要，未經當事人書面同意，不得將資料交予第三者，並確保資料提供者的個人資料得到恰當的處理或只限作爲處理某些事件的用途。此外，認爲向不同類別的資料處理者施加不同責任是公平和合適的做法，因要視乎涉及事件的類型。

少部份同工認爲向不同類別的資料處理者施加不同責任並不恰當及未必切實可行，難以追查。

建議 3： 應否規定資料使用者在發生個人資料外洩事故時通知私隱專員及受影響的人士?

意見： 大部份同工均認爲應該在發生資料外洩時通知私隱專員及受影响人士，因爲可以盡早讓受影響的人士有所準備，以致損失及受影響的程度減至最低，以及可讓各相關人士討論如何善後及商討解決及補救的方法。

另有同工認爲因有關機制運作未成熟，故建議現時之通報應爲自願性質，待確立有關的指引及程序後才考慮進一步之方案。此外，有同工認爲要視乎情況的嚴重性，如只是個別人士的一般資料而未有任何對其構成影響，可通知受影響人士已經足夠。

建議 4： 私隱專員應否獲賦權進行刑事調查及提出檢控或應否維持現狀?

意見： 大部份同工認爲應維持現狀。由於現時由警方進行刑事調查及由司法部門提出檢控的機制行之有效，本港亦不宜有過多機構擁有調查權力，以減少重疊工作和功能，避免造成混亂及浪費資源及公帑。雖然如此，專員亦需定期與警方及司法部門交換資訊及了解最新有關私隱之社會動向。

少部份同工同意私隱專員應獲賦權進行刑事調查及提出檢控。另有同工認爲私隱專員可賦權進行刑事調查，但提出檢控則由警方或法庭處理。

建議 5： 若有資料當事人因資料使用者違反私隱條例的規定而蒙受損失並有意向資料使用者提出法律訴訟，應否授權私隱專員爲受屈的資料當事人提供法律協助?

意見： 大部份同工認爲應該。一般市民對私隱條例及法律認知有限，加上法律訴訟費用不菲，如授權私隱專員爲受屈的資料當事人提供法律協助，除有助提高公眾對私隱的意識外，亦有助保障一般市民的權利。

根據諮詢文件表示應否參照平機會的模式，授權私隱專員爲有意根據私隱條例第66條向資料使用者提出法律訴訟，以申索補償的受屈資料當事人提供法律協助。按照平機會的現有授權模式，強調授權爲「有意透過法律程序索取補償的個別人士提供協助」，故同意只需提供協助予以上人士，因私隱專員可以使用其他方式協助受屈的資料當事人，例如提供調解服務。

另同意5.13的考慮因素，在未正式透過法律申請索償，就違反根據私隱條例之損害前，對其民事申索的成功機會多少作一個合理評估，這樣對受屈人士提供一個合理的心理準備及適當參考資料，作一個決定是否起訴。

由於授權私隱專員之權限，只作協助者之角色，故此不是在法律上有行使權，相信不會混淆爲一個執法機關，並且在協助受屈的資料當事人過程中，更強化受屈人士之自主性及獨立性，根據以上的原則同意授權私隱專員爲受屈的資料當事人提供法律協助。

少部份同工不同意，並建議應由法律援助處協助，以減少角色上的衝突。

建議 6： 是否應授權私隱專員判給受屈的資料當事人補償，以提供多一個補救途徑?

意見： 大部份同工認爲執法機關不應擁有判決權力，索償及調查不應由同一私隱專員執行。角色難免有混淆。但明白所有裁決交於法庭審理需時很長，故建議可成立一名私隱(調解) 專員，專責執行所有交予法庭審理前的調解；與私隱(調查) 專員專責作出調查和執法的角色分開。最終的補償條款均需交由法庭劃一釐定或最終修訂。另有同工認爲私隱專員應與有關司法部門訂立補償指引予公眾參考。

少部份同工同意此建議，認爲能簡化程序，使補償加快。

建議 7： 應否把違反保障資料原則訂爲罪行?

意見： 由於公眾對保障私隱的意識不足，過往違反保障資料的原則並不構成罪行，以免市民誤墮法網。但隨着社會發展，侵犯個人資料的個案越來越多，對社會影響亦越來越大，現時一些違反保障資料原則的行爲，不但是蓄意，更會對個人及社會造成重大損失。這些行爲若根據現時條例，只會被列爲民事訴訟，對當事人的保障並不足夠，亦未能產生阻嚇作用。因此大部份同工認爲應該訂爲罪行，使資料處理者更能嚴守保密原則。

另有同工建議要考慮有關違反保障之資料對個人、社會影響構成負面影響之重要性、覆蓋面，及是否蓄意違反保障資料原則而衡量是否訂爲罪行。

少部份同工不同意，認爲有關意識仍未提高，若定爲罪行，會令非蓄意遺漏人士招致刑責。

建議 8： 應否把在未經資料使用者同意下，取得並披露個人資料，從中取利或作惡意用途的行爲，訂爲罪行?

意見： 大部份同工認爲應該。被披露的個人資料可作非法用途，牽連甚廣，而披露者的動機是有意圖地作出此行爲，從而達到目的，所以應訂爲罪行。

由於現時未經資料使用者同意下，取得並披露個人資料而從中取利的問題愈見嚴重，不少國家已有清晰條文將上述行爲列爲罪行，以保障私隱，因此同意香港亦需訂立類似條文，但隨着互聯網的普及，不少網絡使用者可能在瀏覽或下載檔案時誤觸法紀，故建議在草擬條例時先從阻止利用未經資料使用者同意下取得並披露個人資料以從中取利的行爲入手。

少部份同工認爲訂爲罪行刑罰太重。

建議 9： 應否把資料使用者已遵行私隱專員發出的執行通知的規定，但不久又故意重犯的行爲訂爲罪行？若然，有關罪行適當的罰則。現時不遵行執行通知，可處罰款50,000元及監禁兩年。

意見： 大部份同工認爲應該訂爲罪行，認爲現時的罰則已具阻嚇作用。並建議所謂「短期內重覆」之「短期」可能需要定下時間線，例如兩年內。

少部份同工建議維持現狀。

建議 10： 應否授權私隱專員就嚴重違反保障資料原則的行爲施加罰款？

意見： 大部份同工認爲應該授權私隱專員就嚴重違反保障資料原則的行爲施加罰款。

少部份同工不同意，建議將某些嚴重違反保障資料原則的行爲定爲罪行，因爲某些情況是否嚴重違反保障資料原則可能爲主觀判斷，故適宜由法庭裁決，以免屆時由私隱專員施加罰款而易引致爭論。另有同工認爲罰款不一定起阻嚇作用。

建議 11： 應否將屢次違反執行通知的行爲處以更重的懲罰，以加強阻嚇作用？若然，適當的罰則。現時違反保障資料原則的刑罰爲第5級罰款(最高可達50,000元)及監禁兩年；如屬持續犯罪，每日罰款1,000元。

意見： 大部份同工同意加重刑罰，建議可將每日罰款提高，例如每日罰款建議爲$5,000以加強阻嚇作用。

少部份同工認爲既然條例自頒布以來，未有人士被檢控一次以上，反映情況並不太嚴重，建議在情況轉差時才再考慮。另有意見認爲現時罰則已具阻嚇作用，但執法及檢控方面則需加強，以免給予市民「有法不執」的負面印象。

建議 12： 爲遏止在直接促銷活動中不當使用個人資料的情況，應否提高在直接促銷活動中不當使用個人資料的行爲的罰則?若然，適當的罰則。

意見： 大部份同工認爲應該，因現時罰則未能阻止不當使用個人資料的行爲。有關罰則建議最高罰款可定爲$100,000元及監禁三年或參照刑罰第5級罰款（最高可達$50,000元）。另有同工建議若重覆再犯，可公開該不良公司名單予公眾。

少部份同工不同意提高罰則。

建議 13： 應否授權第三者就更改未成年人或精神上無行爲能力的人的個人資料用途給予同意?

意見： 大部份同工認爲應該，但建議只限授權予該名未成年人或精神上無行爲能力的人之合法監護人，就更改其個人資料用途給予同意。同工表示授權第三者更改以上人士的個人資料用途會使中心運作更爲方便及有效率，甚至可能會對當事人所接受之醫療、教育和社會服務等必要服務有深遠影響。但須確保該項更改爲上述人士之意向，同時要有適當監管。有同工建議可訂立一套制度以確保當事人之個人資料不會被授權之第三者濫用或疏忽處理。授權之第三者既授予使用當事人個人資料之權力，亦需有規則遵守，如能確保於當事人有需要時授權之第三者能作出適時與適切的回應。此外，可透過有關制度作出授權轉移之申請，以免當事人之福利受到影響。

少部份同工表示不同意。

建議 14： 如資料使用者依從父母代其未成年子女提出的查閱資料要求並不符合子女的最佳利益，我們應否准許資料使用者拒絕該查閱要求?

意見： 大部份同工認爲若父母的要求並不符合子女的最佳利益，同意此項建議。同工認爲任何情況下都以子女的最佳利益爲優先，除資料擁有者外，其他人並不能決定資料擁有者之最佳利益，故除涉及刑事及公眾利益外，資料使用者應有權拒絕查閱要求。

父母作爲未成年子女的家長及監護人，應有權索閱與未成年子女相關的資料，以作出最符合該未成年子女的最佳利益，由於題目內指父母索閱資料要求並不符合子女最佳利益時的情況，服務提供機構未必有客觀準則或標準，去判斷或界定何謂不符合該未成年子女之最佳利益，如服務提供機構拒絕其要求，須根據清楚及具體的定義及機制去執行，監護人及子女在提出反對時，可有申訴程序。因此應由政府或有關方面建立有效之評核機制，以評估是否符合子女的最佳利益才容許資料使用者使用查閱。

有同工表示由於父母對未成年子女有監護權，而不符合子女的最佳利益較難界定，此建議應詳加考慮。

建議 15： 應否向執法機關以及救援和支援機構給予豁免，以在緊急情況下處理個人資料?

意見： 大部份同工均贊同建議，認爲在涉及市民安危及公眾利益情況下，執法機關及救援機構可獲豁免，但須就「緊急情況」作進一步的界定。此外，有同工表示安老院舍與醫療機構之間的查傳訊息，應可考慮豁免。

建議 16： 如未成年人的個人資料與家長或監護人履行照顧和監護責任有關，我們應否准許資料使用者把該等資料轉移給未成年人的父母或監護人?若然，應該附加甚麼特定條件，限制轉移個人資料的做法只適用於絕對有需要的個案。

意見： 大部份同工認爲應該，以加強對易受誘惑的未成年人和邊緣少年的保護，以及使父母及監護人可妥善地履行適當照顧和監護兒童的責任。但情況是以該未成年人的最佳利益爲依歸，並同意附加特定條件。建議家長或監護人可以書面提出申請，詳述照顧內容，並由有關法律機構或私隱專員審核後才可以批核使用該等資料。或由相關認可機構(例如：社會福利署)作出評估，證明其父母或監護人合宜照顧和監護該名未成年人，以該名未成年人的成長及日後發展得到最大好處爲目的。

部份同工建議在准許資料使用者將未成年人的個人資料轉移給其家長或監護人前，應通知資料擁有者，並由其決定將什麼資料轉移給其家長或監護人。

(完)

S0103



To <pdpo_consultation@cmab.gov.hk>
cc

30/11/2009 14:49

bcc
Subject Submissions on Consultation Paper to Personal Data (Privacy) Ordinance

☒ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

This refers to the Consultation Document on Review of the Personal Data (Privacy) Ordinance. On behalf of HKBN, I submitted here in the attached Word Document that sets out our concerns on the likely impact which the Proposals made in the Consultation Document will have on the development of the IT industry.

Best Regards,
S. L. Lo



HKBN Submission – PDPO Review.doc

Submissions of Hong Kong Broadband Network Limited To The "Consultation Document On Review of The Personal Data (Privacy) Ordinance" August 2009 ("the Document")

We, Hong Kong Broadband Network Limited ("**HKBN**") are a fixed telecommunications network service provider. Our Submissions sets out our concerns on the likely impact which the Proposals made in the Consultation Document will have on the development of the IT industry, bearing in mind the Guiding Principles for conducting the Review as stated in the executive summary of the Document.

Proposal 1

Prohibiting the collection, holding, processing and use of sensitive personal data and introduction of sanctions for contravention of such requirements.

Comments

As recognized by the PCPD, there is no universally agreed definition of sensitive data beyond the general standard that such sensitive data must be

(a) intimate data about an individual and
(b) data likely to be utilized in discriminatory decisions.

Biometric systems capturing behavioral and physiological attributes are seen as cause for particular concern where used for commercial or human resource management purposes. . However, the use of biometric information as a means of identification and as an alternative to signatures has been around for centuries. In the past, it was necessary to collect the complete information eg a whole finger or whole set of finger prints to identify the individual. These days, biometric information can be collected only in part. Often, such part is not sufficient for identification of an individual, and hence is not sensitive personal data. Meanwhile, with the advances in technology, such part collected biometric information is sufficient to allow verification of identity. Despite that there is chance for incorrect verification, as not the whole biometric information is captured and used for verification the use of biometric data is still well received because it is convenient, speedy, at relatively low costs to the user.

If the PDPO is meant to regulate data relating directly or indirectly to a living individual, from which **it is practicable to ascertain** the identity of the individual and which are in a form in which access to or processing of is practicable. Therefore, the data to be regulated must lead to identification of an individual.

Incomplete biometric information does not allow for the data subject to be positively identified and consequently, does not fall within the general ambit of PDPO regulation.

Further, such incomplete biometric data also does not fall within the general standard of sensitive data as recognized by the PCPD in that such incomplete biometric data is neither unique nor intimate to an individual.

The use of such data is convenient and effective and should not be unnecessarily over regulated. It is unnecessary because the risk that such data allows for identification of an individual leading to discriminatory decisions against such individual is probably non existent as discussed above.

If a separate concept of sensitive personal data is introduced, we are concerned that there would be no clear definition of "sensitive personal data" and therefore many types of data that would be caught by any definition is potentially, not easy to ascertain.

Submissions

(a) Not all biometric data are sensitive personal data. Use of biometric data for verification of identity and not identification of an individual should be distinguished.

(b) Collection, holding or processing of biometric data which is not sufficient to identify a person should not be subject to stringent protection requirements under the Ordinance. For example, a data user may capture only a percentage of data relating to a finger print or an iris to enable identity to be verified. This allows the captured data to be matched against data records, often *voluntarily* provided by the data subject in the first place, to enable his/ her identity to be verified. Even if there is a system breach, the captured data on its own is not sufficient to enable the data subject to be identified.

(c) The danger of identity theft or discrimination against a data subject for human resource management or maintenance of security reasons is far outweighed by the benefits to a data user in terms of increasing efficiency and costs. Biometric data matching technology has enabled security to be enhanced in various situations at relatively low costs, quickly and accurately.

Proposal 2

Regulation of data processors and sub-contracting activities.

Comments

In principle, we agree that data processors, meaning, any party other than an employee who holds, processes or uses personal data solely on behalf of a data user and not for its own purposes should be subject to the same requirements imposed on a data user. However, the nature of the telecommunications business and internet in particular poses

unique challenges on policing and enforcing any requirements. We are extremely concerned as to how proposed new requirements by way of direct regulation will be carried out in practice.

In particular, a telecommunications operator is different to an internet service provider ("ISP"). It so happens that most telecommunications operators are also ISP but not necessarily vice versa. Telecommunications operators are carriers, providing telecommunications connection between different physical locations. They are required to hold a Unified Carrier License (UCL) or equivalent to operate their business in Hong Kong. Meanwhile, ISP is an entity who holds a Public Non-Exclusive Telecommunications Service (PNETS) license, providing Internet access service. In most case, an ISP may also provide other internet related businesses, for example, email service, data storage service etc. In this discussion, an ISP should strictly refer to the provision of Internet Access Service.

For the reasons stated below, both a fixed network operator and an ISP should not both be responsible for protecting the privacy of an individual for information carried in the system as long as the system is reasonably secure. It is impossible to ensure that the system cannot ever be hacked into or physically tampered with.

First, as an ISP or telecom operator, a huge amount of data passes through our system per second. We have no means of ascertaining if such data are personal or sensitive in nature, let alone establish for what purpose the data was collected.

Second, most of the data passes through our system in temporary transit, in terms of millisecond. Such data are not collected by us but may be considered entrusted to us for processing in the sense of sorting out certain types of data which are then re-transmitted onwards. Such data would not remain in our custody or possession.

Third, there is no fool proof method to stop such data from being illegally tapped during transit. . Being a fixed network operator, we have hundreds of kilometers of cables all over the Territory of the HKSAR and it is not possible to monitor security at all times over every inch of the cables. Reasonable steps may be taken to minimize such risks but a data processor would be subject to very onerous judgment calls if there is no consistent and standard safety system imposed. However, we consider that a standard safety system is neither practical nor desirable in the interests of developing internet related businesses and next generation data centers. We have the necessary software to ensure that the information passing through our network system is secure but we are unable to ensure that the information cannot be hacked or tapped. To give an analogy, a VIP (the data protected) may be conveyed in a bullet proof vehicle but it is impossible to bullet proof the road system.

Fourth, under the Telecommunications Ordinance, we are under existing statutory obligations not to interfere or intercept messages passing through our network system. We are concerned that new obligations to be imposed on data processors would

inadvertently put us in conflict with existing obligations under the Telecommunications Ordinance or the conditions of our Licence.

For other internet related services and not Internet Access Service, we agree that the operator should be responsible for the security of the information passed to them by a data subject or a data user.

An undesirable effect of imposing liability on data processors may be that foreign companies collecting data which they know are personal or sensitive as defined by the Ordinance and stored in our secure drives for their own use are unlikely to be subject to any enforcement action whilst on the other hand, liability may very easily attach to us, as data processors even though we would not be in the position to identify if such data is subject to the PDPO in the first place.

Submissions

(a) The definition of a "data processor" should be narrow and should not include entities with merely split second possession of the data nor with reasonable efforts on its part, are still unable to identify whether the data is personal or sensitive in nature.

(b) Any new regulations to be imposed on a data processor should ensure that there is a level playing field for all so that data users whether local or foreign should be under similar or more onerous duties than a data processor to protect such data.

(c) Direct regulation may not be practical for reasons stated in the comments. Securing data processors compliance with the obligations by means of contractual requirements is preferable because data processors refusing to enter into such agreements would eventually receive no work.

Proposal 3

Granting criminal investigation and prosecution power to PCPD

Comments

We are concerned that the power to investigate and to prosecute being vested in one entity, the PCPD, will lead to over zealous prosecutions. Under the Basic Law, the control of prosecutions is vested with the Department of Justice ("DOJ"). Direct prosecutorial power is usually delegated when highly technical knowledge is required.



28/11/2009 22:48

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject 私隱條例意見

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

本人不願意公開個人資料。

一、為了依從私隱條例第28(3)條的規定，應否規定資料使用者依從查閱資料要求所徵收的費用，不得高於私隱條例內收費附表列出的訂明最高收費

本人認為此附表是必須的。

本人認為除了為實質的物品訂出最高的收費，同時亦必須為查閱資料定最高人工的收費，每次收費，如果每次要查閱多項資料亦只可定出一個收費。高昂的收費，會為查閱個人資料的人士止步。何謂「超乎適度」？只有訂出查閱資料定最高的收費才能解決。政府多個部門都只收取實質費用（如紙張影印，每張一元）。

如果查閱資料只需一人工作即可，但機構為令人止步，可能會使用多人，令一個步驟變成百個步驟，這亦解釋了為何英國會定出十英磅的法例，香港應該效法。

舉個例子，香港考試及評核局在設定查閱個人資料收費時，包括了郵遞的費用，但假若考生親自前往該局拎取資料，費用仍然沒有減去郵資。對於考生而言，三百八十五元的首科收費會令考生卻步（大學生薪金大約四千元），這個價錢在申訴專員調查之前一樣，考生未能查閱試卷副本時亦一樣，但之後沒有為查閱試卷資料而定出一個新收費。

人工收費每次（無論有多少項資料）最高收費：一百元。

二、收費模式，用以訂明最高收費的參數

紙張（A4，F4　及定明長闊）：每張一元
CD/DVD：每張碟二元
其他：購買的成本

三、應否規定資料使用者如無持有要求查閱的個人資料，須以書面回覆要求者，但如查閱的資料涉及個人刑事犯罪紀錄而警方並未持有該資料則屬例外

我認為必須規定資料使用者如無持有要求查閱的個人資料，須以書面回覆要求者。因為作為資料使用者，持有甚麼資料，查閱者無可能完全知悉，只有通過查詢才知道。

但如查閱的資料涉及個人刑事犯罪紀錄而警方並未持有該資料則屬例外。

四、應否規定資料使用者如無持有資料當事人的個人資料，因而無法應要求提供有關資料的複本，須在40日內回覆要求者，不論有關回覆是以書面或口頭方式作出。

我認為這是必須的。四十日內回覆要求者，可減去無了期的等候，防止有人為令他人止步而在一年內「使用資料後，保密銷毀資料」，阻止查閱。

S0105

To pdpo_consultation@cmab.gov.hk
cc
Subject 回應《個人資料（私隱）條例》的諮詢文件

28/11/2009
17:47

敬啟者：

愛護家庭家長協會是本地一群有心維繫和推廣傳統一夫一妻家庭制度及相關的家庭價值及幸福的家長組織，本會得悉**政制及內地事務局**已發出檢討**《個人資料（私隱）條例》的諮詢文件**，邀請公眾就條例的修訂建議發表意見。

現特函 閣下，以提出本會的意見和關注。首先，作為市民和家長，我們認為相關的私隱條例應以**社會倫理和法治精神作為首要考慮和原則**，現代社會注重法治和私隱等觀念，原因不外乎是現實中人類社會仍存在著不同程度的矛盾、不公義、危機和威脅人類個體以至群體生存和發展的實況和因素，相關因素又不利於人類生活的安穩性以至持續良性發展。又或者說：「現今人類的狀況距離理想中的大同世界或所謂的烏托邦還有明顯的差距。」

從歷史來說，香港是承襲了英國的普通法和因回歸中國而制定的基本法為憲章，其中的一個基本假設，就是現行的制度是基本乎合香港的現實需要，並且有利於本港的繁榮和穩定發展。所以，在法治和公義的基礎上，所有建制和措施都應以有利社會的健康和良性發展為大前題，不能喧賓奪主或無限上綱的成為一個超然建制，否則，香港很易會變成一個只知政治正確而不知自力更新的社會，若是這樣，香港的前途必然灰暗！

本會尊重法治，同時強調倫理道德是人類社會良性發展的不可或缺的基礎。基於上述的前題，本會謹此進見：

（一） 我們同意「私隱」或其相關法定建制不是至高無上的事物，當然，「私隱」是應當被尊重，特別是考慮到私隱被不當的張揚和使用時很可能會對被張揚者構成損害或不必要的威脅或壓力。

當然，「私隱」是應當被尊重，特別是考慮到私隱被不當的張揚和使用時很可能會對被張揚者構成損害或不必要的威脅或壓力。

（二）

-1-

今天香港的倫理道德是香港社會在過往發展中的一種累積和承傳，雖然不是絕對，但相關的倫理和道德都是本於維護和促進香港的良性發展，不是不能改，**但應透過一正規和合理過程，包括通過各方持分者的討論，政府的研究和承擔，才可修改**。因此，我們反對把一些未經歷史印證或足夠考核的觀念〔如私隱是個人的絕對權利[1]〕被神化成一些所謂「普世價值」。

（三） 就青少年與其家長或監護人間的「私隱」權衡，我們認為家長既有養育他們的責任，必須被賦予對子女的**知情權**及為未成年子女接受何種教育的選擇權。否則，家長便難以合理和有效地履行養育的工作和責任；如此一來，青少年和社會問題必然氾濫，而社會要付出高昂的代價！

（四） 家長/監護人的知情權應受保障，除非相關家長或監護人因為精神或病理因素失去養育和監護相關青少年的能力，又或者其子女的私隱一旦被他們揭露時，我們有足夠理由相信可能會導致其子女身心受創或生命受威脅，在這些處境下，政府或其他合法受受應當被尊重的托人應介入和暫代家長/監護人之職，以預防不幸事情發生，並維持代父母(surrogate parents)之職職年人之職，以預防不幸事情發生直至他們的家長/監護人能重新承擔父母的天職為止。

（五） 以近期氾濫於青少年間的吸毒問題題surrogate parents)以至在網上設立所謂「自殺群組」的問題，青少年因身心成長因素，並因缺乏足夠的人生經驗來自我保護和糾正，家長的知情權更不可被剝奪。若有機構/人士以私隱為名來剝奪相關的知情權，相關機構/人士應對後果負上全面責任，而政府亦責無旁貸，或是糾正相關歪風，或是對可能出現的傷害作出全面承擔和補償！

（六） 當青少年的個人資料與其家長或監護人履行照顧和監護責任相關時，有關當局應規定及時把相關資料通知和送達他們的家長或監護人，以便相關家長作出適切的跟進和處理。

（七） 同理，執法機關以及救援和支援機構**在緊急情況下**應有權處理相關人士的個人資料，只要相關機關/人員能信守對相關資料的官方保密承諾，若相關的私隱一旦被洩漏，否相機構或官方負責人

官方保密承諾，若相關的私隱一旦被洩漏，否相機構或官方負責人應負上民事補償責任。

此致
香港政制及內地事務局

愛護家庭家長協會 上

愛護家庭家長協會(PARENTS FOR THE FAMILY ASSOCIATION)

[1] 一個明顯的反證是針對謀殺犯或恐怖份子的犯罪意圖不應受私隱保護。

S0106

致政制及內地事務局第四組收：

本人反對醫生有權查閱客人的家族病歷史，

因為這是客人的私隱。

(署名來函)

30/11/09.

(未能確定來信人是否願意公開姓名)

S0107

（ 來信人要求以保密方式處理意見書 ）

S0108

(此意見書按發件人要求被 S0149 取代)

(This submission is replaced by S0149 as requested by the sender)



香港資訊科技聯盟

HONG KONG IT ALLIANCE

S0109

30th November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert road
Hong Kong

Dear Sir

Re: Consultation Document on
Review of the Personal Data (Privacy) Ordinance (PDPO)

We are writing in response to the Consultation Document on Review of the Personal Data (Privacy) Ordinance (PDPO). On behalf of Hong Kong IT Alliance, we would like to submit our comments on specific proposals as below:

Proposal No.1: Sensitive Personal Data

We do not think there is a need to introduce this new category at this stage, and in particular, we disagree that "biometrics" should be singled out under the proposed new category and subject it to more stringent regulation. Technology is rapidly evolving, and legislation is never the best way to deal with technology. Furthermore, in the absence of a clear definition of "biometrics" and a set of relevant operational guidelines, any step causing prejudice to "biometrics" is considered detrimental to the development of local IT industry, thereby affecting Hong Kong's competitiveness as a whole.

Proposal No. 2: Regulation of Data Processors and Sub-contracting activities

It is in our opinion that the existing practice of regulating only the data users is sufficient. Outsourcing is widely adopted in the current business environment, especially with the emergence of cloud computing. It will be onerous to exercise direct regulation over the numerous subcontractors who may situate outside Hong Kong's jurisdiction with respect to a specific project. Leaving the responsibility to the 1st tier contractors who will deal with their outsourced parties would be appropriate. After all, any action that is perceived to be constraining our IT operating environment is not welcome.

Proposal No. 3: Personal Data Security Breach Notification

Imposing a security breach notification system would result in considerable compliance burdens on businesses. We trust it is appropriate to confine the practice of serving soonest notice, upon leakage of personal information, to the Privacy Commissioner and data subjects among the Government departments, companies in the financial sector, and hospitals (the best practice which is already in place for the entities). For other companies, we believe notification should only be made on a voluntary basis.

S0109

香港資訊科技聯盟
HONG KONG IT ALLIANCE

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD
Our response is a definite "NO". We do not see there is a need for PCPD be associated with more tangible power. Instead, the Commissioner should engage more resources in educating the public and the industry about privacy, and instilling a sense of self-discipline among those involved or affected.

Proposal No. 5: Legal Assistance to Data Subjects
The use of public funding to assist individuals in pursuing civil claims cannot be justified, especially in most cases where the damages involved in the security breaches are far from substantial. We do not want to open the floodgates to abuse legal assistance.

Proposal No. 6: Awards Compensation to Aggrieved Data Subjects, and Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles
There is absolutely no need to give the Commissioner such additional power or responsibilities.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence
We do not see there is a need to change the existing regulations. The ease of use and application of IT would make many of us fall victim unwittingly to the contravention of the DPPs. Making it an offence would leave many uncertainties in our operating and business environment.

As a conclusion, we are of the view that there is no compelling reason to review the PDPO at this stage for tightening the regulation. Hong Kong is a sophisticated city and our IT practitioners and participants are in general well-disciplined. The pursuit of a more protective and stringent legislative framework will only be possible at the expense of innovation and creative development.

Yours faithfully,

(Signed)

Leo KAN
Vice-Chairman and
Hon. Chairman of Personal Data (Privacy) Ordinance Committee

CITICEN : CHENG PO LING POLLY
CONTACTS : (deleted)
ADDRESS : (deleted)

Introduction

S0110

Economic downturn in the past ten years has driven job requirements more and more demanding. Against this backdrop, employers are seeking every opportunity to maintain headcounts level by upgrading staff, instead of increasing number of staff. Nowadays, high qualification job applicants are sought after with lower pay and rank. Over-paid, title-inflated but under-qualified supervisors are under serious threat. These supervisors are keen on protecting their own interest by means of setting up recruitment traps through mis-represented job description.

Mis-leading Job Description

Very often, job description misleads job applicants by stating that the candidate would eventually report to senior management, e.g. the board of directors. The reporting line forms a lure to applicants, implying that there will be promising future. High caliber, over-qualified applicants are attracted in false hope. Personal particulars are then collected for perusal by someone (the "authorized persons") in fairly similar capacity as the job applicants without prior notice. The whole practice deprives the job applicants of their privacy rights, especially when the persons authorized to read their personal particulars are actually the job applicants' direct competitors in the job market.

Abuse of personal information during recruitment process is as follows:

Job Application Discloses High Volume of Personal and Business Information

1. Authorized persons can have the full picture of how their job searching direct competitors are fixing their expected salary.
2. Because of the popularity of job searching engines and Internet portals, they can easily copy format, phrasing and selling points of the C.V. and cover letters of the job applicants at a click.
3. If disclosed in the C.V., authorized persons can learn about department structure, size and how many subordinates the incumbents of similar position have. This opens to them better future, because different company assign totally different number of staff to the same position. E.g. a sales director can have 5 to 50 subordinates.
4. If disclosed in the section on work experience of the C.V., authorized persons can get business intelligence e.g. client list, project details and budget size.
5. If reference is given, authorized persons can locate who those easy going, reasonable supervisors are. This opens easy access for their own selves to cold approach these potential employers, because the job applicants are leaving their jobs sooner, offering them golden opportunity to leapfrog to better positions.
6. They might even copycat part-time study path of their job searching direct competitors in a bid to advance in career. E.g. license type of bankers.

MON 30 PM 2:30

1. Interviewers are hungry to ask for current strategies and tactics of their business competitors. If declined to disclose these information, the applicants are doomed to fail.
2. Alternatively, interviewers might ask job applicants for suggestions on how the company could improve their existing strategies. They seek only to tap the applicants' business knowledge.
3. If written test is conducted, authorized persons turn out to be "free riders", reaping others' harvest of creative ideas offered in proposal writing and even the use of wordings in speech writing.
4. Interviewers, having previous personal encounters with someone in the job applicants' current employers, sometimes ask for insider information or status of key personnel (e.g. directors) of the companies. They do this in order to pave their way to approach them, or there is other indecent hidden agenda.

Real Life Examples

1. *(A company)* advertised in April 2009 to recruit a "Senior Vice President – Investor Relations & Corporate Communications", who will report to the company's Deputy Chief Executive Officer. The company invited me by phone two months later on 22 June for an interview, saying that there will be "different arrangements": I shall report to a Senior V.P. in Investor Relations & Corporate Communications instead. Details of email correspondence related to this recruitment trap are attached in Appendix I on pp.5-10. Upon my rejection, the company issued another recruitment advertisement on 3 July 2009, opening a far junior position. This means that the recruiter wanted both to save advertising cost and forcing qualified but under-paid staff to fill up junior positions.

2. *(A company)* advertised on 30 October 1999 to recruit a "Senior Communication Resources Officer" salaried HK$500K up p.a. The advert stated clearly that it required a university degree holder with seven years of experience. Actually, the position was not a replacement, it was the filling of a vacancy left by a form-five graduated clerical officer, sacked suddenly by the company after working there for over 16 years. As the clerical officer was responsible for posting recruitment adverts on the company website regularly, recruitment of her successor could not be done via a job description of her own. This was why an over-stated, misrepresented advert was used. Recruitment adverts before (Appendix II on p.11) and after the employment (Appendix III on p.12) are attached for comparison. My past experience matches perfectly well with the job requirements of the 30 October 1999 advert. Copy of three reference letters attached to Appendix II serves as iron evidence.

Effect: Undermining Job Applicants' Competitiveness

If applicants' privacy cannot be protected whenever seeking jobs, then personnel or human resources department is simply not doing its job. It is absolutely unfair to the job applicants.

1. Recruitment process can never be level playing field because "authorized persons" are taking full advantage of the job applicants, who are direct competitors in the same industry sector of the job market.

   E.g. the authorized persons then have better knowledge of salary to ask for when applying jobs
   E.g. for small businesses, the authorized persons can snatch job applicants' customer accounts
   E.g. the authorized persons can copy project details and apply for their own use

2. The authorized persons can use others' C.V. and application letters as "canned food" template for self use.

3. Career path is full of twists and turns originally. Learning others' study path or getting referees' contacts enables the authorized persons to have quick access to higher levels, reaping others' hard earned harvest.

4. In the short run, the use of mis-represented job description wasting time of job applicants and the company. It is because even job interview has been conducted, the company would normally not hire the applicants because the interview questions uncover the true intention of the authorized persons, showing serious conflict of personal and business interest. The authorized persons are the only winning party because they steal ideas without cost.

5. Even hired, the conflict of interest prevails. In the long run, hatred grows and will eventually end up with unfair job performance comments internally and externally. Again, only the authorized persons are the winner. The job applicants are not easy to find jobs thereafter, they give but can never take.

Legal Principle

Mis-represented job description breaks contract law principle. Recruitment advert, although only the very first step of the whole recruitment process, is an integral part of the job contract duly signed between employers and employees. Wordings therein almost serve as an invitation to treat. It can create false hope. In essence, misrepresentation means a set up to the job seekers. It wastes their time, disgraces them and ruins their future. Unfairly, it feeds over-paid but under-qualified supervisors with first-hand job market and business information at the expense of career prospects of the job applicants.

Possible remedy for the above situations:

1. Only personnel or human resources staff is allowed to read job applications. "Authorized persons" should be narrowly defined. Independence must be maintained to avoid conflict of interest during recruitment stage, employment period and after employment. If under-qualified supervisors were to read through applicants' C.V., prior consent has to be sought from the job applicants. E.g. personnel staff should call job applicant first, asking "if your supervisor is a diploma holder, while you are a master's degree holder, do you mind if s/he could read your C.V. ?" It is at the job applicants' discretion to disclose their personal particulars or privacy cannot be protected.

2. If tragedy took place, title-inflated, under-qualified supervisors were assigned to oversee over-qualified, under-paid experienced subordinate. Then, reference check after such employment should allow written disclaimer to be issued by the "victims", making clear that the supervisors are having poorer education, experience than they are. The two persons were in serious conflict of interest at work. Which is to say, the supervisors' comments COULD BE TOTALLY UNFAIR. After all, would anyone want to be taken over by someone far less paid but are better qualified than they are? This explains the whole conflict of interest.

(Annexes not attached)



30/11/2009 13:18

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject 人資料(私隱) 條例公眾諮詢提出之意見

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

至有關人事:

以下是本人對個人資料(私隱) 條例公眾諮詢提出之意見:

1. 個人資料當事人在法定下有權在任何情況下填寫之個人資料后, 可即時有權要求該機構把其些個人資料保密, 不能在以后被某些機構索取其個人資料時披露(例如, 新更改之地址或電話號碼), 及資料當事人可索取已填寫之個人資料之影印本作紀錄保存. 如該機構有影印並在影資料當事人之身份證, 則該機構必須在身份證影印本上寫上或在上面蓋印・列明該影印本只供該機構內部作紀錄用.以避免該機構擁有他人個人資料之人員可私下把他人個人資料去查詢他人之私隱. (因本人曾聽聞某些機構會私下用員工之個人資料去查詢該員工之信貸紀錄及稅務紀錄等). 而亦得知索取個人信貸紀錄之表格上之索取紀錄人之簽署, 亦不需跟任何銀行戶口上之簽署模樣一樣才能取得該人之信貸紀錄.

2. 機構與機構之間如索取某人之個人資料時, 我應爲該被索取某人個人資料的機構, 應自動把被索取某人的個人資料影印本寄交或通知個人資料當事人其那些個人資料已傳至那一機構.

3. 我應爲就某機構向另一機構在口頭上對某人之個人資料傳述亦應納入某人之個人資料. 亦合法地可被個人資料當事人有權索資料. 被索取資料之機構亦應如實向資料當事人披露所有經某一機構口頭上傳述之個人資料. 因不實之口頭上傳述亦對資料當事人有很深遠之影響及傷害. 並對刻意抹黑及作惡意之中傷亦應以法例定罰, 警告.

4. 某人把他人在未經.同意下的相片上載於網上並刻意抹黑及作惡意之中傷亦應以法例定罰, 警告. 及對當事人之影響及傷害作賠償

5. 應諮詢文件內p.13, 敏感個人資料中, 對他人之身體特徵在未經當事人同意下作刻意抹黑及作惡意之中傷並以口頭上傳述, 亦應以法例定罰, 警告 及對當事人之影響及傷害作賠償.

6. 應諮詢文件內p.17 之 3.13 及 3.14 , 我應爲就算在豁免過渡期后及在法例生效后, 在之前已收集的敏感個人資料 (口頭上及文件上的資料) , 如在法例生效后有對當

, 在之前已收集的敏感個人資料 (口頭上及文件上的資料) , 如在法例生效后有對當事人做成損害 (在情感及精神上受到傷害), 仍應視爲違反私隱條例, 以法例定罰, 警告. 及對當事人之影響及傷害作賠償. 否則我應爲對資料當事人很不公平.

我很希望私隱委員會能夠細心考慮本人以上之意見, 並在檢討定例后, 請大力向市民宣傳, 例如: 在無線電視節目上向市民宣傳有關法例及提高人們對私隱安全之保障及對他人私隱尊重之意識.)

RGDS.



30/11/2009 12:32

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir/madam,

My feedback to Proposal No. 8: Unauthorized Obtaining, Disclosure and sale of personal data

I agree to make such unauthorized obtaining, disclosure and sale of personal data an OFFENCE if a person obtains personal data without the content of the data user and discloses the personal data so obtained for profits or malicious purposes.

Technology advances in a very fast pace that one can hardly imagine how personal privacy can be infringed to such extent. I am one of the victims that some GPS tracking tools has been placed in my belongings. My whereabouts are checked by others and my information is passed to others without my consent.

Morality is not their concerns. Only making it an criminal offence can help.

The following links are about some GPS tracking tools.Please a look.

http://gps.toptenreviews.com/recreation/gps-clothing-you-wear-it-where-.htm

http://tech.slashdot.org/article.pl?sid=05/05/29/1547234&from=rss

http://findarticles.com/p/articles/mi_m0CYP/is_1_111/ai_98539810/

http://www.thefreelibrary.com/Positioning+through+play+clothes:+wearable+GPS+devices+track...-a098539810

http://news.cnet.com/8301-10784_3-9764275-7.html

Regards,

(name)

(The sender requested anonymity)

C L I F F O R D
C H A N C E

CLIFFORD CHANCE
高偉紳律師行

BY HAND AND BY EMAIL
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

30 November 2009

Attention: Team 4
Email: pdpo_consultation@cmab.gov.hk

Dear Sirs,

Response to Consultation Document on the Review of the Personal Data (Privacy) Ordinance (the "Consultation")

This is a submission by Clifford Chance in response to the Consultation on the review of the Personal Data (Privacy) Ordinance ("**PDPO**").

We are grateful for the opportunity to comment on the proposals and are appreciative of the efforts of the Privacy Commissioner for Personal Data ("**PCPD**") to update the PDPO in light of technological advances and changes in business practices with a view to balance the interests of individuals, businesses and the needs of the Hong Kong economy.

We are generally supportive of and welcome the PCPD's proposals. We have several specific comments we would like to make. The proposal references correspond to those in the Consultation. We make no specific comments in relation to the proposals not discussed in this letter.

PARTNERS
S.R. BACHE
C.S.K. CHAN
E.Y.L. CHEN
R.M. DENNY
M. FELDMANN
B.W. GILCHRIST
C. HENG
A.E. HO
L. HO
G.O. HUGHES
A.D. HUTCHINS
H.R. JENKINS
C.W.M. KAN*
A.S.H. LO
M.D. ROGERS
M.G. SHIPMAN
C.F.M. TANG
D. WACKER
J.R. WADHAM
J.A. WALKER
A. WANG
A.M. WHAN

FOREIGN LEGAL CONSULTANTS
P.J. CHARLTON (ENGLAND AND WALES)
S.J. COOKE (ENGLAND AND WALES)
P.C. DARE BRYAN (ENGLAND AND WALES)
J.R. FADELY (NEW YORK, USA)
GAO P.J. (PRC)
P.C. GREENWELL (ENGLAND AND WALES)
H.S. KIM (NEW YORK, USA)
A.E. LLOYD (MARYLAND, USA)
D.K. MALIK (ENGLAND AND WALES)
M.W. TRUMAN (ENGLAND AND WALES)

CONSULTANTS
N. BUDHWANI
L.P. CHEN
C.D. HASSALL
K.K.C. LEUNG
A.P. OAKES
P.S. O'CONNOR
C.J.G. ROBINS
A.W.Y. SHUM

*CHINA-APPOINTED ATTESTING OFFICER

1. Proposal No. 1: Sensitive Personal Data

We are of the view that any regulation of sensitive personal data should be carefully considered. Although we agree that generally, specific regulation of sensitive personal data is in line with international practice and standards, as recognised in the Consultation, the coverage of what constitutes sensitive personal data and the ways in which such data are regulated vary widely from jurisdiction to jurisdiction. Where the coverage of sensitive personal data is widely defined (such as in the case for Europe), we note that this has created practical difficulties in subjecting data users to stringent regulations where in certain circumstances may not be justified.

We note that the Consultation proposes in paragraph 3.08 that one option is to only classify biometric data as sensitive personal data, and we agree to the adoption of this more restrictive and narrow coverage of sensitive personal data as it is likely that biometric data would in most circumstances be considered information that would be sensitive in nature.

In relation to the regulation of sensitive personal data, we are not supportive of imposing a very strict regime in relation to the regulation of sensitive personal data that may prevent or hinder legitimate processing of such data. We generally agree with the list of circumstances where data user may collect, hold, process and use sensitive personal data as set out in paragraph 3.09. In particular, we agree with the inclusion of paragraph 3.09(d) provided that this should not include a right of the data user to disclose sensitive personal data to third parties.

In relation to sanctions for contravention of the requirements relating to sensitive personal data, we consider that it would be appropriate to extend the existing regulatory regime governing contravention of DPPs involving personal data to sensitive personal data. We also agree to the grandfathering or transitional arrangement as set out in paragraph 3.14 which is an approach adopted by other jurisdictions including Europe.

2. Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

We do not consider that it would be necessary to include specific provision in the PDPO to require data users to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties. Under the current regulatory regime, data users are already subject to the data protection principles that would make them directly accountable for their holding and processing of personal data. It would be the duty of data users to ensure that any act of sub-contracting to data processors or third parties would be in compliance with the existing data protection principles. We consider that there is no additional need to impose further statutory obligations to require data users to do so.

In addition, we do not consider that the activities of a data processor should be directly regulated under the PDPO. We consider that the existing regime (whereupon a data processor who holds, processes or uses personal data solely on behalf of another person and does not hold, process or use those data for any of his own purposes, would not be regulated as a data user) should be maintained.

Paragraph 4.14 of the Consultation sets out the proposed means of direct regulation. We consider that proposal (a) and (c) would not be necessary given that any data processor who breaches (a) or (c) (i.e. who uses personal data for purposes outside the purpose (or directly-related purpose) for which such data were so entrusted; or who does not take reasonably practicable steps to erase personal data no longer required for the entrusted purposes) would then be considered to be holding, processing or using personal data for its own purposes and not solely for and on behalf of a data user. In other words, the data processor would, in these circumstances, be subject to the same obligations as a data user instead and there should not be any need to impose direct obligations on them as data processors. In relation to proposal (b), we consider that it should be the obligation of a data user to decide the appropriate level of security, and to decide whether it would be necessary to contractually oblige data processors to do so, or to make the appropriate assessment as to whether the data privacy policies of data processors would be sufficient (as suggested in paragraph 4.19 of the Consultation).

Accordingly, we are supportive of maintaining the current indirect regulation of data processors as set out in paragraph 4.20 of the Consultation. Instead of direct regulation of data processors, and in addition to the current regime whereupon data users may contractually impose obligations upon data processors, we consider that it may also be an option to consider imposing a statutory indemnification obligation on data processors to indemnify a data user in relation to any loss or damages suffered by a data user arising from the holding, processing or use of personal data by data processors.

3. Proposal No. 3: Personal Data Security Breach Notification

We agree with the proposal that any personal data security breach notification obligation should, at least at the current stage, be voluntary - to impose mandatory security breach notifications without sufficiently clear and objective standards required for making notifications would result in unduly burdensome obligations to notify in circumstances that may not justify the cost and efforts of notification.

We generally agree to the components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42 of the Consultation on the basis that the notification requirement will be voluntary, including the proposed list of information that should be included in a notification as set out in paragraph 4.39 of the Consultation.

4. Proposals No. 4 to 6: Enforcement Powers of the Privacy Commissioner for Personal Data

We consider that the existing scope of powers of the Privacy Commissioner is working well and should be maintained, and we make no specific comments in relation to proposals 4 to 6 of the Consultation.

5. Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

The proposal to make contravention of a data protection principle a direct offence for reasons set out in paragraph 6.04 of the Consultation needs further consideration. The data protection principles are broadly drafted and it may in certain circumstances be difficult for data users to make a correct assessment as to their main obligations relating to the data protection principles. Making a contravention of a data protection principle a direct offence would, in our view, create unreasonable burden on data users. We consider that the current regulatory regime (where a contravention of an enforcement notice would amount to an offence) should be maintained.

6. Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

We believe that, provided the proposed offence is drafted such as to catch manifest wrongdoing and not inadvertent breaches, it would be appropriate to make it an offence for a person who obtains, discloses or sells for profit or malicious purposes personal data which he obtained from a data user without the latter's consent. The approach taken in the UK under Section 55 of the UK Data Protection Act (as set out in paragraph 6.07 of the Consultation) may be used. We consider that the defences listed in paragraph 6.08 of the Consultation which are defences set out in the UK legislation are generally appropriate although we would note that the defences set out in (e) and (f) relating to justification for reasons of public interest should be carefully considered to determine whether these are similarly applicable in the Hong Kong context.

7. Proposals No. 9 to 12: Other Proposals Relating to Offences and Sanctions

We consider that the regulatory regime relating to offences and sanctions is working well and should be maintained, and we make no specific comments in relation to proposals 9 to 12 of the Consultation.

8. Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We agree that under the current regulatory regime, if a data user is bound by a statutory duty to maintain secrecy, such data user may face a dilemma of either breaching a data access provision of the PDPO or a relevant secrecy provision in another ordinance. Accordingly, we agree with the proposal to include a new ground for a data user to refuse to comply with a data access request under Section 20(3) of the PDPO where the data user is obliged or entitled under any other ordinances not to disclose the personal data. As with other grounds for refusal to comply with a data access request, a data user should be required to follow the current procedures set out in the PDPO in relation to their response to data access requests.

9. Proposal No. 17: Erasure of Personal Data

Contrary to some other data protection principles, under Section 26 of the PDPO and data protection principle 2(2), the duty to erase personal data that are no longer needed is a strict requirement (for example, the standard required of data users in some other data protection principles are only to take "all practicable steps"). We believe that the current provisions relating to the erasure of personal data can create an onerous burden on data users and agree with the proposal to amend the PDPO so that the provisions concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfilment of the purpose of use.

10. Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

We agree with the proposal to include an exemption from DPP3 for the transfer or disclosure of personal data in intended merger, acquisition or transfer of businesses, subject to conditions. We believe that the conditions for this exemption should be on the basis of fairness and transparency as opposed to consent obtained from data subjects, given that in most cases involving merger, acquisition or transfer of businesses, obtaining the data subjects' prescribed consent may be a sensitive issue. Accordingly, the conditions set out in paragraph 52 of the Consultation are generally appropriate although further consideration should be given to (b) (where "it is not practicable to obtain the data subjects' prescribed consent for such a use") – in certain circumstances, it may be practicable to obtain the data subjects' prescribed consent but it may not be desirable for business reasons to do so, in which case condition (b) would not be satisfied. We believe that if the other conditions set out in paragraph 52 are satisfied, then it would not be necessary to include (b) as a condition.

If you have any questions on the above or would like to discuss further, please contact Kenneth Leung at (deleted)

Yours faithfully

(Signed)

Clifford Chance

S0114

27 November 2009

Your ref.: CMAB/CR/7/22/40 Pt. 7

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong

Attn: Miss Joanna C. H. Choi

Dear Sir

Public Consultation on
The Review of the Personal Data (Privacy) Ordinance

We thank you for your letter dated 28 August 2009, inviting *"the Organisation"* to give its views on the subject consultation. Please be informed that the Hong Kong Institute of Surveyors do not have any comments on the Review of the Personal Data (Privacy) Ordinance.

Yours faithfully

(Signed)

(name)

(The sender requested anonymity)



To pdpo_consultation@cmab.gov.hk
cc

30/11/2009 14:25

bcc
Subject ISFS comments on the "Consultation Document on Review of the Personal Data (Privacy) Ordinance"

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Assistant Secretary (Constitutional and Mainland Affairs) 4B
HKSAR

November 30, 2009

Dear Secretary,

Consultation Document on Review of the Personal Data (Privacy) Ordinance

In view of the "Review of the Personal Data (Privacy) Ordinance" consultation document by the CMAB, our society (Information Security and Forensics Society) would like to express our view in respect to the key proposals discussed in the document (attached).

Regards,
KP Chow
Vice Chairman,
Information Security and Forensics Society



ISFS_PDPO_20091130.pdf

INFORMATION SECURITY AND FORENSICS SOCIETY
資訊保安及鑑證會

In view of the "Review of the Personal Data (Privacy) Ordinance" consultation document by the CMAB, the Information Security and Forensics Society would like to express his view in respect to the key proposals discussed in the document as follow:

There is no question that identity (ID) data can be stolen using a multitude of technologies and techniques – e.g. by obtaining unauthorised access to computers (eg hacking), through electronic interception or the outright theft of disks, printer outputs, smart ID cards, PDAs, mobile phones, laptops or home computers – and the list of techniques and technologies involved in the theft of IDs is growing both in number and sophistication. Finally, there is the possibility that ID data can be lost, through improper handling, then employed for criminal purposes.

Yet does a victim of ID theft have adequate remedies under local law?

Current limitations of the PDPO

Hong Kong's current approach to tackling the problem of ID theft primarily stresses prevention through the application of the PDPO which is intended to govern the collection and use of personal data and thereby prevent imprudent disclosure of personal data that might lead to ID theft.

However, this approach has limitations. The PDPO is limited to data 'users who control the collection, holding, processing or use of the data'. Though this may cover cases for which a thief has obtained IDs through unauthorised interception of mail or trespass or without the requisite statutory power to make such collection, there would be no 'collection' of data' where a thief obtains information by memorising comments or conversations.

Secondly, the PDPO applies only to living individuals and is specific in the forms of data covered. Thus it would not apply in cases where thieves stole IDs of dead persons.

Thirdly, the PDPO contains exceptions through which data users might escape regulation. For instance, s 65 does not apply to criminal proceedings. Section 64 excludes the use of statistics and research from the ambit of Principle 3, s 33 governing the transfer of data out of Hong Kong and is not in effect. And Principle 4 of the PDPO does not require data users to give absolute guarantees of security.

Finally, though the PDPO imposes criminal sanctions for failure to comply with enforcement notices, actually applying this sanction to a data thief who could rapidly acquire IDs and quickly run up bills for large amounts is, in fact, impractical. [1]

[1] Ronald Yu, 'Is Hong Kong ready for ID Theft in the 21st Century?' Hong Kong Lawyer *Hong Kong Lawyer*, May 2004, available at: http://www.hk-lawyer.com/2004-5/May04-cover.htm

Other legislation

There are other laws a victim might successful invoke including: Ss 16A, 17, 18, 18A, 18D, 22(d) of the Theft Ordinance (TO), ss 68, 71 and 73 of the Crimes Ordinance where forgery is involved, and if multiple parties are involved in the theft of IDs and subsequent crimes to defraud, s 159A (1) of the Crimes Ordinance could be applied for the crime of conspiracy while s 4(2) of the Criminal Jurisdiction Ordinance broadly extends the criminal jurisdiction of the courts of Hong Kong to cover such conspiracies - as long as a relevant event occurs in Hong Kong. A criminal who physically breaks into his victims' homes and steals data directly from their computers could be charged under s 11 of the TO and if the criminal hacked into a victims' computer from a remote machine, s 27A of the Telecommunications Ordinance could be invoked.

However, these laws have limitations of their own. For example, if a criminal bought data from a reputable online site, there would have been no 'theft' regardless of the property issues (though he might still be charged under s 161 of the Crimes Ordinance for accessing a computer with dishonest intent to cause loss to another or with a view to dishonest gain) and a victim of an ID theft who suffers from a subsequent identity fraud is precluded from invoking the tort of fraud by the wording in s 16(A) of the TO.[2]

In addition, there are limited sanctions in the case where data is lost through careless handling. Moreover, unlike American consumer protection legislation, the PDPO does not actually offer a comprehensive framework for a victim of ID theft to expunge erroneous records nor does the PDPO offer a victim much in the way of compensation and investigations of ID theft must, for all practical purposes, now be undertaken privately which can be an expensive exercise.

Thus with the growing danger and increasing sophistication of ID theft, the legislation should be amended to upgrade investigative powers of an appropriate organization (e.g. the Privacy Commissioner), offer victims of ID theft better remedies, compensation or both, and grant broader powers to a victim of ID theft to ensure that erroneous records are removed.

In short, Hong Kong should strengthen its Personal Data Privacy regime to establish a comprehensive and effective legal framework not only to discourage criminals from using Hong Kong as a haven for ID theft, but also grant the appropriate bodies greater investigation of ID theft and strengthen the protections, remedies and rights of victims of ID theft.

[2] Ibid

Microsoft

Submission in response to the Consultation Document on Review of the Personal Data (Privacy) Ordinance

1 Executive summary

Microsoft Hong Kong Limited and Microsoft Corporation (together "**Microsoft**") welcome the opportunity to make this submission in response to the *Consultation Document on Review of the Personal Data (Privacy) Ordinance* ("**Consultation Document**") issued by the Constitutional and Mainland Affairs Bureau ("**CMAB**") , with the support of the Privacy Commissioner for Personal Data ("**PCPD**").

Microsoft's key submissions are as follows:

- Microsoft strongly supports retaining the principles-based, technologically neutral approach to privacy regulation as currently provided for in the Personal Data (Privacy) Ordinance ("**PDPO**") and the Data Privacy Principles ("**DPPs**");
- Microsoft supports the principle that data protection obligations should vary in proportion to the sensitivity of the personal data, but believes that this principle can be better achieved by tailoring the existing DPPs rather than creating a separate regime to define and protect sensitive personal data,
- Microsoft supports the staged implementation of a breach notification scheme;
- Microsoft supports indirect regulation of data processors and sub-contractors, but does not support direct regulation; and
- Microsoft does not support granting criminal enforcement powers to the PCPD or making the contravention of a DPP an offense.

2 Introduction

This submission sets out Microsoft's views on key issues relating to the regulation of privacy in Hong Kong. Each of the following sections sets out a response to one or more of the proposals in the Consultation Document (the relevant proposal number(s) are indicated in brackets at the end of each heading).

Microsoft Hong Kong is the local subsidiary of Microsoft Corporation and has operations throughout Hong Kong. In the privacy sphere, Microsoft Hong Kong's activities are principally regulated by the PCPD. To address these obligations and those that Microsoft is subject to in other jurisdictions

around the world, Microsoft has implemented a single, global privacy policy. Under Microsoft's global privacy policy, Microsoft makes the same privacy commitment to all of its customers irrespective of the approach to privacy regulation in their country of residence.

Microsoft believes that effective privacy and data protection can be built on a foundation of four core principles:

(a) A consistent and workable standard, across all organizations and industries, for offline and online data collection and storage. Laws and regulations should be consistent from industry to industry, and compatible with privacy laws around the world.

(b) Increased transparency regarding the collection, use and disclosure of personal data. This includes a range of notification and access functions, as well as simplified, consumer-friendly privacy notices and features that permit individuals to access and manage their personal data collected online.

(c) Meaningful levels of control over the use and disclosure of personal data. Individuals' right to consent before companies use or disclose their personal data should be balanced with the need for business flexibility, while avoiding bombarding consumers with excessive and unnecessary levels of choice.

(d) A minimum level of security for personal data in storage and transit. Standards should require organizations to take reasonable steps to secure and protect critical data against unauthorized access, use, disclosure or modification.

These principles inform Microsoft's views on privacy regulation in Hong Kong and around the world.

3 Sensitive Data (Proposal No. 1)

3.1 Separate regulation of sensitive personal data

Microsoft understands that certain types of personal data are more sensitive than other types, and that the degree of sensitivity should be a crucial factor in determining the appropriate level of regulation for personal data.

However, Microsoft does not support the creation of a separate statutory regime for "sensitive personal data", because Microsoft believes that differential treatment based on different personal data types is more effectively achieved by incorporating the differential treatment concept into the DPPs, rather than by creating a separate regime. For example, in relation to DPP4 (Security of personal data), Microsoft supports the approach adopted in the corresponding APEC Principle,[1] where data controllers are required to implement *appropriate safeguards* that are *proportional* to:

[1] See APEC Principle 7 (Security Standards): Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [22].

(a) the likelihood and severity of the harm threatened;

(b) the sensitivity of the information; and

(c) the context in which it is held.

In Microsoft's view, the degree of flexibility afforded by this kind of test cannot be matched by a statutory scheme that arbitrarily partitions personal data into "sensitive" and "not sensitive". This kind of test also reduces the risk of data users adopting measures to artificially move data from "sensitive" to "not sensitive", since it requires a consideration of all of the circumstances surrounding the data, rather than just the application of a single statutory definition.

If the Constitutional and Mainland Affairs Bureau is interested in pursuing the model described above, Microsoft would be happy to discuss the concept in greater detail.

3.2 Classification of biometric information as sensitive personal data

Microsoft's strongly believes that technological neutrality promotes the adequacy and effectiveness of the PDPO and should be maintained wherever possible, and is concerned that the classification of biometric information as sensitive personal data inappropriately focuses on the methods of data collection and storage, rather than the inherent characteristics of the data. Indeed, as paragraph 3.06 of the Consultation Document states (emphasis added):

> *"Biometric data **could reveal** sensitive personal information such as health, genetic information, or ethnic origin."*

In Microsoft's view, defining biometric information as sensitive information would also be inconsistent with international practice, since there is no internationally accepted test for "sensitivity" or definition of "sensitive personal data". In this context, if Hong Kong were to impose its own standard, then this would impose an additional Hong Kong-specific compliance burden for companies like Microsoft where Hong Kong is just one of the jurisdictions where the company's products and services are offered.

From a broader perspective, Microsoft is also concerned that a trend of adopting a separate statutory regime for "sensitive personal data" will inevitably result in cross-jurisdictional uncertainty, as different countries adopt different tests for partitioning "sensitive" and "not sensitive" data. Such a consequence would be detrimental for data users that operate in multiple jurisdictions (because of the increased regulatory burden) as well as data subjects (because of the difficulty in identifying the relevant test to apply in a given circumstance).

Microsoft does not, however, advocate inaction in this area, and appreciates that there is a legitimate public concern, and need for consideration of legislative responses, in relation to the fraudulent use of personally descriptive data (such as in the case of identity theft and impersonation). So, while Microsoft does not believe that privacy legislation is the appropriate

place to address this concern, Microsoft does support raising fraudulent use of personally descriptive data in the context of a review of Hong Kong's existing criminal laws in order to establish their adequacy to meet the increasing threats that are posed by cybercrime.

4 Regulating Data Processors and Sub-contracting Activities (Proposal No. 2)

4.1 The benefits of indirect regulation

Microsoft understands that data is increasingly mobile, and that it is now common for data to be collected and then transferred to another entity, to another country, or both. Microsoft supports a mechanism that ensures that data protection obligations are preserved at each link in this chain of custody, but also believes that any such mechanism should be sufficiently flexible to ensure that excessive regulation is avoided, and that innovation is not inhibited.

In Microsoft's view, indirect regulation allows the interests of consumers to be preserved without sacrificing flexibility, since the data user and data processor in each instance can adopt suitable measures to regulate the transfer and processing of customer data. Of course, such agreed arrangements should be subject to minimum statutory protections, and Microsoft therefore supports the proposal that data users be placed under an obligation to take measures, contractual or otherwise, to ensure compliance with the PDPO.

Microsoft notes that the indirect regulation model is also consistent with the model described in Principle 9 (Accountability) of the APEC Privacy Framework, which requires personal information controllers remain *accountable* for the protection of personal information they collect, use or hold even if that data is transferred from one jurisdiction to another. Importantly, as with the indirect regulation model in the Consultation Document, the accountability principle allows data users to tailor their compliance method to a given context.

4.2 Indirect regulation is preferable to direct regulation

Microsoft is concerned, however, that the flexibility and consistency benefits associated with indirect regulation will be lost if data processors are directly regulated. One example of this outcome is in situations where personal data is transferred to a data processor, but remains under the control of the data user (such as when a data processor is providing "cloud computing" services).[2] When this is the case, it would be unreasonable to deem the data processor as being equivalent to the data user, since clearly the user and processor do not have the same ability to ensure the security and lawful use of the data.

Microsoft is also concerned that the protections given to personal data in agreements between data users and data processors will become less rigorous

[2] In this context, Microsoft has recently released a position paper entitled *Privacy in the Cloud Computing Era: A Microsoft Perspective*. Microsoft's Chief Privacy Stategist, Peter Cullen, and Senior Direct of Privacy Strategy, Brendon Lynch, have also blogged in this area.

as a consequence of direct regulation, since there will be a tendency for all parties to rely upon the statutory safety net rather than negotiate situation-specific obligations. Even if the consumer ends up with rights against the data processor that are equivalent to those it would have had against the data user under the indirect regulation model (and this will depend upon the manner in which statutory obligations are imposed on the data processor), Microsoft's view is that this outcome is inconsistent with general consumer expectations, since the consumer will not be able to take action under its existing established relationship with the data user.

As noted in the Consultation Document, it has become commonplace for personal data of Hong Kong citizens to be processed in other jurisdictions (particularly mainland China). In Microsoft's view, this fact further supports an indirect regulation model in preference to direct regulation, since it will be difficult if not impossible for Hong Kong consumers to exercise their rights directly against offshore data processors. An indirect model, with Hong Kong data users setting up appropriate legal relationships with offshore data processors, will be more likely to result in actual changes to the practices of offshore data processors, as data users are able to assert their rights against the data processors in response to consumer complaints.

Finally, in relation to the mechanism for imposing privacy obligations on data processors, Microsoft does not support the proposal a data processors need only comply with its own, self-adopted, privacy policy.[3] Microsoft believes that privacy regulation should facilitate two objectives: giving data subjects meaningful privacy protections that promote confidence in e-commerce, and creating obligations that are clear, reasonable, and not unduly burdensome. Allowing data processors to rely upon a privacy statement would not facilitate either of these objectives, since a data processor could implement a privacy statement which does not contain meaningful privacy protections, or act at any time to remove existing protections.

4.3 International consistency

The issue of consistency, and Microsoft's preference for regulatory regimes that are consistent across jurisdictions, is referred to in section 2 above. In the context of direct versus indirect regulation, Microsoft believes that the fact that direct regulation is less flexible means inevitably that there will be higher associated compliance costs. As has been previously noted, this is likely to have a cumulative detrimental effect on companies like Microsoft that offer products and services across many jurisdictions - each with their own, specific, compliance requirements - as well as the general effect of making business more onerous to conduct in Hong Kong.

4.4 Regulation by category of data processor

The Consultation Document also requests comments in relation to the proposition that different types of data processors should be made subject to different categories of regulation. Microsoft's view on this proposal stems from its overall view, expressed above, that privacy regulation should be phrased in terms of outcomes and principles, and that implementation is a

[3] See Consultation Document paragraph 4.19.

matter best left to data subjects, data users and data processors. Consequently, Microsoft does not support the categorisation of data processors in the PDPO, as Microsoft is not convinced that such categories could be drafted sufficiently generically and in a technology-neutral manner to ensure that the categories remain relevant in the future. Microsoft's instead believes that a suitable general obligation, along the lines of the indirect model discussed above, is a more effective regulatory strategy.

5 Breach Notification (Proposal No. 3)

5.1 Introduction of breach notification

Microsoft supports the introduction of a voluntary breach notification obligation in the PDPO, as Microsoft believes that an appropriately structured mechanism of this kind promotes public confidence in the data custody practices of data users.

Microsoft supports the staged implementation process for the breach notification obligation, and agrees with the Consultation Document conclusion that implementing a mandatory scheme as an outcome of the current consultation process would be premature.[4] The voluntary notification regime will provide crucial data which can then guide subsequent changes to the PDPO, and the voluntary notification period will promote public awareness of, and confidence in, the notification process, and give Hong Kong businesses time to adapt to the new requirements.

The voluntary notification period will also give Hong Kong time to monitor international developments in relation to breach notification. Currently, there is not a consistent international approach in this area. With the benefit of a voluntary breach notification period, Hong Kong will be able to move quickly once an international consensus emerges to implement a mandatory notification regime that is appropriate for the citizens of Hong Kong, as well as being in harmony with the breach notification regimes of other jurisdictions.

5.2 Guidance on when to issue breach notifications

As recognised in the Consultation Document, one of the key issues associated with the introduction of a breach notification obligation is identifying the types of data breaches where a breach notification would be an appropriate step for a data user to take.

Microsoft's view is that an individual should be informed of a security breach if that breach results in, or could reasonably result in, the misuse of that data subject's unencrypted sensitive financial information for the purposes of fraud or identity theft. However, Microsoft does not believe that a breach notification obligation should extend to:

(a) data that has been rendered unusable, unreadable or indecipherable to an unauthorized third party through practices and/or methods, such as encryption, redaction, access controls and other such mechanisms,

[4] See Consultation Document paragraph 4.34.

which are widely accepted as an effective industry practice or an industry standard; or

(b) situations where the data subject is unable to take any protective or remedial measures in relation to the breach (ie no self-help is available).

Microsoft considers that this structure implements an appropriate balance between empowering data subjects to minimise the more serious consequences that might flow from a security breach involving their personal information, and avoiding a situation whereby security notifications are so frequent that data subjects disregard them or are unable to differentiate between those that indicate a significant risk and those that do not. In Microsoft's view, this structure is also consistent with the principle that breach notification should focus on empowering the data subject, rather than being a punitive measure against the data user.

Microsoft considers that, in the context of a voluntary notification regime, it would be useful if the PCPD were to publish guidance on the factors that data users should take into account when deciding whether to issue a breach notification to data subjects.

5.3 Form and timing for notification

In Microsoft's opinion, data users should be afforded discretion as to the method by which they provide breach notifications to affected data subjects. Data users should be able to take into account factors such as:

(a) the size of their organisation;

(b) the relative cost of different methods of providing the notification; and

(c) the ways in which the data user typically communicates with its customers; and

(d) whether or not a delay in notification is reasonable (such as in the case where a law enforcement agency requests a delay),

when determining when and how to notify data subjects of a data breach.

Microsoft recommends against mandating any particular form for notification, as in Microsoft's view a single mandated form in unlikely to be appropriate for all industry sectors. For example, if a data user normally communicates with its customers via email, then breach notification via email would generally be the preferable form of notification, as an email is likely to come to the data subject's attention much faster than a notification by physical mail.

More generally, Microsoft considers that the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and

Customer Notice[5] (which interprets s 501(b) of the United States' *Gramm-Leach-Bliley Act*) provides a useful model for fleshing out a breach notification obligation. The Interagency Guidance considers matters such as how to identify data subjects affected by a regulated security breach, the timing and content of any breach notification, and the manner in which any breach notification should be delivered.

6 Criminal Sanctions (Proposals No. 4 - 12)

6.1 Criminalisation of PCPD provisions

Microsoft's position in relation to the criminalisation-related proposals in the Consultation Document is based on its belief that principle-based drafting of privacy obligations is generally inconsistent with the imposition of criminal penalties, because of the necessity for outcomes in privacy obligations to be stated in general terms. Criminalising such obligations would create significant uncertainty, as businesses will not necessarily know when particular behaviour becomes criminal, and Microsoft is particularly concerned about the adverse effect that criminalisation would have on the IT industry, where businesses are often engaged in new or innovative activities. Where criminalisation is appropriate (and Microsoft agrees that there are instances of intentional conduct such as fraud where this will be the case),[6] the legislative response should be by way of cybercrime legislation rather than via amendments to the PDPO.

In relation to the DPPs, Microsoft agrees with paragraph 6.04 of the Consultation Document, and particularly the statement that the *"DPPs are couched in generic terms and can be subject to a wide range of interpretations"*. Microsoft agrees with the Consultation Document that criminalising non-compliance with the DPPs would be counter-productive (see Proposal No. 7), and consequentially recommends that contravention of the DPPs not be made an offence.

6.2 Amendments to PCPD's functions and powers

Microsoft agrees with the Law Reform Commission and the Consultation Document that combining enforcement and punitive functions in a single entity is generally undesirable. Microsoft therefore does not support Proposals No. 4 (Granting Criminal Investigation and Prosecution Power to the PCPD), 6 (Award Compensation to Aggrieved Data Subjects) and 10 (Imposing Monetary Penalty on Serious Contravention of DPPs).

7 Microsoft's demonstrable commitment to privacy

Microsoft is committed to helping individuals and organisations realise the benefits of technology while preserving control over how personal

[5] Issued by the Office of the Comptroller of the Currency (Department of the Treasury), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision (Department of the Treasury). Available at: http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf.

[6] See also Microsoft's submission in section 3.2 above in relation to the fraudulent use of personally descriptive data.

information is used and protected. Microsoft delivers on this commitment in a number of ways, including by making investments in technology, leading and partnering with industry, and providing guidance and education. Set out below are some examples of Microsoft's initiatives in these areas.

7.1 Technology investments

In 2002, Microsoft's Chairman Bill Gates signalled a major shift in the way Microsoft develops software when he launched the Trustworthy Computing Initiative, a long-term, collaborative effort to provide more secure, private, and reliable computing experiences for all computer users.

The depth and breadth of Microsoft's commitment to security and privacy protection can be clearly seen in Windows 7, Microsoft's newest client operating system. From Windows Firewall with Advanced Security, which provides the first line of defence against malicious attacks, to Windows Defender, which scans a PC for potentially unwanted software, Windows 7 offers multiple layers of protection against intrusions and unauthorized access to user data.

The newest version of the Microsoft Web browser, Internet Explorer 8, also features major advances in privacy protection, including features that help detect suspicious Web sites and prevent users from unintentionally divulging personal information while communicating and shopping online.

7.2 Leadership and partnership

Microsoft provides leadership in establishing industry standards that help give users control over how their information is used, collected, and shared. For example, Microsoft established a corporate privacy policy that applies to the collection and use of all customer and partner information, providing business units and employees with a clear and simple framework to help ensure privacy compliance companywide. To help software developers build solutions and applications that address customers' privacy concerns and reflect worldwide privacy legislation, Microsoft has made available a set of Privacy Guidelines for Developing Software Products and Services.[7] At the technology level, Microsoft strives to make privacy management simpler and more secure by developing products with intuitive controls for configuring privacy options and encouraging the entire software industry to develop products that give users more choice about how their personal information is used.

To address growing concerns about data breaches and the collection and use of personal information, Microsoft partners with other industry leaders, governments, and law enforcement in a number of areas. For example, as a member of the Consumer Privacy Legislative Forum, Microsoft actively promotes federal privacy legislation in the United States that provides a uniform standard for organizations and strong protection for consumers. Microsoft has also worked with Canadian law enforcement to develop the Child Exploitation Tracking System, a tool that helps police thwart online child predators. Microsoft was among the first companies to embrace the Safe

[7] See http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en

Harbor privacy principles developed by the U.S. Department of Commerce and the European Commission, which meet the strict EU standards governing the collection, use, and retention of data.

Regionally, Microsoft is also an active participant in APEC's Data Privacy Subgroup and Electronic Commerce Steering Group, is a member of the East Asia Privacy Leadership Project and recently sponsored the International Association of Privacy Professionals' (**IAPP**) foray into Asia through KnowledgeNet workshops conducted in Australia, Singapore and Japan.

7.3 Guidance and education

In the area of consumer education, Microsoft is funding a worldwide privacy education campaign that includes free product updates, articles, and tools on www.microsoft.com. We have also joined with organizations including the Federal Trade Commission, AARP, the National Centre for Missing & Exploited Children, iSAFE, and the U.S. Chamber of Commerce to offer a series of Get Net Safe seminars to educate consumers on how to protect themselves and their children from computer viruses, spyware, identity theft, scams, and online predators. In Hong Kong, Microsoft also works with schools under its Partners in Learning program and NGOs (e.g. Hong Kong Federation of Youth Group) to raise awareness of students and other internet users on online safety and security as well as privacy concerns.

Microsoft's privacy-related guidance to organizations starts with essential training for IT professionals and developers in privacy and security best practices. Microsoft has already trained more than 750,000 IT professionals and developers through security summits, webcasts, e-learning clinics, and online training materials. This training includes fundamental tools and techniques for building products using Microsoft's Security Development Lifecycle processes, including threat-modelling tools and techniques for writing more secure code. Microsoft also sends out Worldwide Chief Security Advisors ("CSAs"), who act as trusted advisors to customers, governments, industry groups, and academia to help them face the challenges of privacy and security in a connected world. More than 30 CSAs are currently working in 20 countries with local governments.

8 Further consultation

Microsoft thanks the Constitutional and Mainland Affairs Bureau and the PCPD for considering its views on the regulation of privacy in Hong Kong, and would welcome the opportunity to further discuss any of the points raised in this submission. To do so, please contact Ms. Winnie Yeung, Director of Legal & Corporate Affairs on (deleted), email at (deleted).



30/11/2009 15:18

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Response to Consultation Document on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sirs

The challenge in data privacy is to balance the need for sharing data with protecting personally identifiable information, and it is compounded by the rapid development of technology e.g. spyware, social networking and sharing sites. Here are some of my thoughts:

1. Proposal Nos.8-11

1.01 Breach of data privacy is very common nowadays, and in some cases this could cause substantial harm, financial and otherwise, to the victims. As it now stands, the law does not provide a good deterrent for those who intend to act in breach or an effective remedy for the victims. It is very artificial for the police (as evident in the nude photos cases) to have to resort to some other laws to charge the suspect for what, clearly, is a violation of data privacy.

1.02 I support Proposal 7 and agree that contravention of a DPP should constitute an offence. Proposal 8 is also necessary.

1.03 Further, it is not unheard of that a regulatory body is given powers to impose monetary penalty, e.g. Securities and Futures Commission. I believe that with appropriate review or appeal channels, it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

1.04 I also agree that repeated contraventions should attract more serious penalties. In other areas, the courts will definitely take into account the behaviour of a repeated offender during sentencing.

1.05 An award of damages is a more realistic help for the victims, avoiding the need for them to resort to the more complicated and costly litigation process.

2. Proposal No. 1

2.01 I support the proposed protection for sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances.

2.02 I believe that the difficulty lies in properly defining "sensitive personal data". Care should be taken in working out what the term "sensitive personal data" intends to cover. Biometric information should clearly be included. It remains unclear whether information such as credit file, financial transactions, ID card/travel document number, credit card information and photographs of truly private moments are covered under the proposed regime for sensitive information. Abuse of such information could subject a victim to serious harm and losses.

2.03 Information about a person's financial transactions, including the amount of assets, positions held in stocks or funds, outstanding debts, and purchases can be just as sensitive as his biometric data. If criminals gain access to information such as a person's accounts or credit card numbers, that person could become the victim of fraud or identity theft. Information about a person's purchases can reveal a lot about that person's history, activities, habits and contacts. It is not easy to draw a line between what is sensitive and what is not. I will prefer the Government to err on the side of caution, while the corporate people will suggest the opposite. In any event, I would urge the Government to give some thought to inclusion of important financial information in the protection of sensitive personal data.

3. Revamping Regulatory Regime of Direct Marketing

3.01 I am very disappointed to note that the proposals for revamping this area have not been adopted. As a victim of such calls on almost a daily basis, and three of those at the time of writing this e-mail, I must say that this form of invasion and harassment is clearly getting out of control and unacceptable.

3.02 It has always been my view that this is more intrusive and disturbing than any other forms of marketing, for which, a Do-Not-Call register has already been maintained. I have expressed the same view to the OFTA when commenting on the anti-spam legislation back in 2006. But my views went unheeded and I continued to suffer such calls.

3.03 The very fact that the marketing agents possess information relating to a data subject in the first place is per se problematic and scary. Stricter enforcement in this regard is clearly required.

3.04 I strongly urge the Government to re-consider the proposals relating to revamping the regulatory regime for direct marketing activities under the PDPO.

I hope the Government can give some thought to the above. Thank you for your kind attention.

Best regards
Blanche Leung (Ms.)

S0118

To <pdpo_consultation@cmab.gov.hk>
cc

30/11/2009 15:14

bcc
Subject Submissions on Consultation Paper to Personal Data (Privacy) Ordinance

☒ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

This refers to the Consultation Document on Review of the Personal Data (Privacy) Ordinance. On behalf of Ricky Wong, I submitted here in the attached Word Document that sets out our concerns on the likely impact which the Proposals made in the Consultation Document will have on the development of the IT industry.

Best Regards
Maggie Leung
Executive Secretary to Ricky Wong
City Telecom (HK) Ltd/Hong Kong Broadband Network Ltd



RW Ltr-PCPD(2) (2).doc

S0118

Consultation Document On Review Of
The Personal Data (Privacy) Ordinance August 2009

Submissions of Ricky Wong

I write specifically in relation to "Proposal 3" regarding a proposed personal data security breach notification.

I believe that in principle, a breach notification mechanism should be introduced. However, the circumstances which trigger such notification must be clearly identified to avoid accidental contravention of such provisions.

The need to identify circumstances which trigger notification may be obvious but is difficult to identify in practice. It would be logical to relate notification with the consequences of breach but the consequences following breach is not easy to identify in advance.

By way of example, a breach affecting only one data subject may have very serious consequences to that data subject whilst a single breach affecting many data subjects may have little consequence to each of them or breach of the same data may have different effect on the data subject at different points in time. Likewise, many separate breaches of data security may have little or no cumulative effect on a data subject. Therefore, how would the mechanism for voluntary and mandatory notification be set and who is to decide the consequence of breach?

I do not believe that setting a mechanism of notification based on the number of data subjects affected or the number of breaches committed is likely to address the object of notification, which is to provide advance warning to an individual. As recognized by the Consultation Document, an individual may become de-sensitized after receiving numerous notices but in fact, only the data subject is able to assess to what extent the consequence of security breach will be. For the reasons above, I take the view that the breach notification should be on a mandatory basis.

HKGCC

Hong Kong General Chamber of Commerce

香港總商會

Hong Kong General Chamber of Commerce

S0119

Helping business since 1861

30 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Sirs

Consultation on Review of the Personal Data (Privacy) Ordinance

The Chamber has considered the Consultation Document on Review of the Personal Data (Privacy) Ordinance and our response is detailed in the enclosed paper.

Yours sincerely

(Signed)

Alex
CEO

Encl.

Consultation on Review of the Personal Data (Privacy) Ordinance

Comments by the Hong Kong General Chamber of Commerce

27 November 2009

1. Guiding Principles

It is important that the Review of the Personal Data (Privacy) Ordinance (PDPO) be guided by the principles listed in the Consultation Document (para 1.06), especially with respect to adequately protecting personal data privacy, and at the same time protecting other interests. Hong Kong's competitiveness, the development of information and communications technologies, and business operations will be adversely affected if an onerous burden and excessive restrictions are imposed on businesses that collect and use customer data.

As a matter of principle, the Government should refrain from adding extra compliance costs on businesses, unless the benefits clearly outweigh the burden. This is particularly important at this time as many companies are still struggling to cope with a difficult economic environment. On the whole, the PDPO has served Hong Kong well. As such, any amendment should only be introduced if there is strong justification for doing so.

A substantial section of the review is dedicated to examining whether the Privacy Commissioner for Personal Data (PCPD) should be given new powers to prosecute and impose penalties, in addition to making certain actions offences. We advise extreme caution on both matters. Expansion of government powers, in addition to the creation of new offences often results in imposing new limits on civil liberties. Consequently, these should only be considered if their need is widely agreed and deemed necessary. Any new offence created under the PDPO will invariably impact the free flow of information. We present our detailed comments addressing this proposal below, but emphasize that the Government should always adopt a prudent approach in contemplating new offences and new powers that may restrict the flow of information. Upholding civil liberties should be a guiding principle in the review.

As noted in the *Information Paper on Review of the PDPO*, it is recognized internationally that ensuring proper conduct and attitude in the use and protection of personal data privacy best achieved through regulation and education rather than criminal sanctions. The preference for education, rather than criminal sanctions, should therefore also be another guiding principle in the review.

We also do not believe that entrusting prosecution and penalizing powers with the Office of the PCPD is warranted. Nor will increasing the powers of the Office of the PCPD solve all the major problems relating to personal data protection in Hong Kong. The present division of labour between the PCPD and the Police has proven to work well. We cannot see any compelling reason for transferring prosecution powers from the Police to the PCPD. It is also doubtful whether the public would have greater trust in the PCPD than in the Police when it comes to criminal investigation and prosecution. Moreover, recent judicial precedents in Hong Kong have reaffirmed the constitutional principles that the powers to determine criminal liabilities should rest with the courts. We therefore cannot see any justification or possibility for transferring to the PCPD the powers to penalize data users who violate the PDPO.

2. Specific Comments on "Key Proposals"

Proposal No. 1: Sensitive Personal Data

In seeking to afford more protection to data subjects, we should tread carefully in attempting to define what constitutes sensitive personal data. As mentioned in the consultation document, the perception of sensitive personal data is culture-bound and there is no universal agreement on what constitutes sensitive personal data.

The option of classifying biometric data as sensitive personal data may not be the best first step to take towards enhancing protection for data subjects. Technologies are evolving very quickly and it is not easy to define the boundaries of biometric data. An over-generalized definition of biometric data will frustrate or even inhibit innovative applications of biometric technologies in business operations. There have been instances in which technology firms disagreed with the view of the PCPD on whether the use of certain finger feature recognition systems amounted to collecting fingerprints, hence constituting excessive collection of personal data. As a first step, the Government should seek to gain a clearer understanding about the technological and business landscape to avoid making hasty decisions on bringing in additional regulations.

The collection of biometric data, such as fingerprints, iris characteristics and hand contours is not widespread in Hong Kong. By and large, the proposed additional requirements for the handling of sensitive personal data have already been embedded in the PDPO. There is no urgency to introduce new regulations on biometric data and any proposed changes should be the subject of a separate consultation, with full technological and legal analysis to assist stakeholders' discussions.

Although heath-related information is not a subject of this consultation, there are concerns in the business community that more regulations may be imposed in the future on collecting information on employees' health. It is necessary for some businesses to ensure that their employees are in good health in order to protect their customers and the wider public. The processing of health information in the recruitment and ongoing staff management process is therefore a necessary procedure. A High Court decision in 2008 also upheld that a company did not breach the PDPO when it required employees to submit medical records for managing attendance and sick leave. The PDPO has prescribed clear principles on the collection and processing of personal data, and we do not see a strong case for adding extra requirements by classifying health information as sensitive personal data, even if the latter is to become a new category under the PDPO.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

If greater regulation on data processors as subcontractors is needed, we are of the view that the Government should consider imposing specific duties and obligations directly on data processors.

Data subjects expect the same protection of their personal data irrespective of whether their data is held and handled by the primary data user or its processing agent. The law, therefore, should not distinguish between data users and outsourced data processors, and all should be required to comply with the same privacy principles.

Imposing direct legal obligations on data processors will be far more effective than relying on data users to impose obligations on their subcontractors through contractual measures. It would be an onerous requirement for primary data users to proactively and continuously monitor the operations of their subcontractors in order to ensure compliance, as it is not uncommon that there are further subcontracting activities along the supply chain.

We appreciate that the Government recognises the potential impact of direct regulation on the fast-evolving Internet-related businesses and the need to avoid inhibiting new services and frustrating the free flow of information on the Internet. In view of the need to maintain flexibility for Internet-related businesses, para 4.19 in the Consultation Document has suggested that as long as Internal-related businesses have adopted a privacy policy, then the obligations under a direct regulation regime should be construed as a requirement to honour the relevant policy terms. While the Chamber supports the broad direction of allowing sufficient flexibility under a direct regulation regime, doubts remain as to what businesses would be classified as "Internet-related." Further clarifications are needed.

Proposal No. 3: Personal Data Security Breach Notification

Introducing a security breach notification system would impose considerable compliance burdens on businesses. As mentioned in the Consultation Document, the impact of a mandatory privacy breach notification on businesses cannot be underestimated. Voluntary guidelines, on the other hand, would also in effect become mandatory, because businesses would be obliged to join the system to avoid the adverse reputational effects of not signing up. In practice, many companies would promptly take pre-emptive action in the case of a major security breach by notifying data subjects in order to protect their reputation. Reputational pressure has already achieved the effect of driving corporations to behave responsibly. Therefore, we believe there is no urgent need for further guidelines or mandatory requirements.

Prescribing in detail the timing, form, means and contents of breach notifications would be unnecessarily restrictive. It would also be costly for the authorities to monitor and enforce the compliance of the detailed notification requirements.

Proposal No. 4: Granting Criminal Investigation Power to the PCPD

Under the present system, the Police conduct criminal investigations into breaches of the PDPO. As mentioned in the Consultation Document, the present system has been working smoothly and there is no strong case for change.

The PDPC performs two main functions: enforcing the PCPO and helping data users to comply with the PCPO. Giving the PDPC the power to prosecute will confuse PDPC's important role as an enabler of data protection. If the PDPC has the power to prosecute, it will also have the adverse effect of making data users wary of seeking assistance from PDPC.

It has been suggested that the powers of prosecution should be transferred to the PCPD in order to avoid conflicts of interests in case the Police or a Government department is the data user involved in an alleged infringement of the PDPO. We do not agree with this line of argument. The Police Force is organized in such a way that investigation can be conducted properly and impartially, even when a case

involves its own officers or other government employees, and that any complaints on alleged partiality will be dealt with according to set procedures.

Proposal No. 5: Legal Assistance to Data Subjects

The PDPO does not empower the PCPD to provide assistance to aggrieved data subjects in respect of civil claims proceedings. Comparison has been made with the Equal Opportunities Commission (EOC) which is empowered by the relevant legislation to assist individuals who want to pursue compensation through legal proceedings. But we do not agree that it is appropriate to compare the PDPO regime with that of the EOC's as they address issues of a very different nature. The use of public funds to assist individuals in pursuing civil claims could only be justified with a strong case, and there has been no strong call in the community for public assistance to aggrieved data subjects, probably because in most cases of security breaches, the damages were not substantial.

Proposal No. 6 Awards Compensation to Aggrieved Data Subjects, and
Proposal No. 10 Imposing Monetary Penalty on Serious Contravention of Data Protection Principle

The two proposals touch on the PCPD's powers in respect of determining civil and criminal liability, and awarding compensation to aggrieved data subjects or imposing monetary penalty on serious contravention of DPPs. The proposals touch on the fundamental principle of separation of powers enshrined in the Basic Law.

We are of the view that, as first recommended in the Law Reform Commission Report in 1994, it is more appropriate for the courts, not the PCPD, to determine compensation. Combining the enforcement and punitive functions of the PCPD is not desirable.

On the other hand, it has been settled in the Final Court of Appeal judgment in *Koon Wing Yee* that under the doctrine of separation of powers in the Basic Law, only the courts can determine criminal liability. Empowering the PCPD to impose a monetary penalty on serious contravention of DPPs would amount to determining criminal liability by a non-judicial body. And as noted in the Consultation Document, the generic nature of the DPPs also gives rise to questions on whether it is appropriate to empower PCPD to apply fixed penalties on the contravention of DPPs (also see comments on Proposal No. 7 below).

Proposal No. 7 Making Contravention of a Data Protection Principle an Offence

We do not support Proposal No. 7. The Consultation Document has clearly, and rightly, pointed out that the Data Protection Principles (DPP) are couched in generic terms which can be subject to a wide range of interpretations. To make contravention of a DPP an offence would have a significant impact on civil liberties if an inadvertent act or omission could attract criminal liability.

The Consultation Document goes on to suggest a "selective approach" by singling out particular acts or practices as offences, having regard to the severity of such contravening acts or practices. We do not object to this approach as certain activities have already been singled out as offences under current legislation. But we would caution that because every new offence represents a restriction of civil liberties and expansion of government power, criminalization should only be considered when the

contravening acts are indisputably serious, and that criminalization is the only and most effective means of tackling the problem.

We do not support the suggestion of introducing a monetary penalty for "failure to comply with the DPPs but limited to breaches that are avoidable and that give rise to a serious data protection risk" (Para 7.4, PDPC's Information Paper on Review of the PCPO), for the same reasons as those stated in our objection to Proposals No. 6 and 10. The courts - not the PCPD -- should impose fines according to the established constitutional principles in the Basic Law.

Proposal No.8: Unauthorized Obtaining, Disclosure and Sale of Personal Data
While we have no objection to this proposal in principle, the Government should look into two issues.

First, it should examine other existing legislation that tackles this issue. One such example is the offences under the Crimes Ordinance related to gaining access to a computer with criminal or dishonest intent. Amendments to the PDPO should only be made for closing loopholes under existing legislation. Amending the PDPO to tackle a problem that is adequately covered by other legislation is a waste of public resources and will create confusion.

Secondly, it is important to ensure that criminal liability will not be imposed on employers or organizations for unauthorized handling of personal data by their employees. A defence should be provided for employers where they have taken reasonable steps to prevent contravention by their staff.

Proposal No. 12 Raising Penalty for Misuse of Personal Data in Direct Marketing
In determining the appropriate penalty for misuse of personal data, the Government should carefully considering how much higher a penalty would need to be set at in order to be a sufficient deterrent. While a maximum penalty of $10,000 may not be an effective deterrent for large companies, a heavier penalty might disadvantage SMEs. However, it may still be insufficient to deter larger enterprises.

Another crucial question, as noted in the Consultation Report, is whether such calls bring serious and material damages to data subjects. Unsolicited marketing calls can be a nuisance, but the material damage may not be substantial. Imposing a heavy fine would therefore be disproportionate.

Last, but not least, if a draconian regime is imposed on direct marketing calls, this could lead to companies scaling down related business activities, which would result in some people losing their job.

Unless the Government can effectively address the above issues, the Chamber does not support raising the penalty.

Direct marketing calls are also regulated by the Office of the Telecommunications Authority (OFTA). We notice that a recent OFTA survey has found that although many people found such calls a nuisance, 13% of respondents said they had benefitted from the calls, and 21% said they had made a transaction as a result of the call. The Government has suggested that nuisance calls should be reduced by voluntary

measures, such as a code of practice for major sectors that make frequent use of direct marketing calls. We agree that a voluntary code of conduct is an appropriate measure for the next step.

3. Specific Comments on "Other Proposals" in Annex 1

We wish to comment on a few "other proposals" discussed in Annex 1 of the Consultation Document.

Proposal 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

While we support the proposal to permit a person to give consent on behalf of a data subject to the change of use of the latter's personal data, we are of the view that "third party" should be strictly defined according to the definition of "relevant persons" in Section 2(1) of the PDPO, as follows:

- Where the individual is a minor, a person who has parental responsibility for the minor;
- Where the individual is incapable of managing his own affairs, a person who has been appointed by a court or otherwise has the legal authority to managing his affairs.

We do not consider it appropriate to expand the definition of "relevant person" as it would be difficult for businesses as data users to verify the identities of a wide variety of third parties.

Proposal 18: Fee Charging for Handling Data Access Requests

We do not consider it appropriate that a maximum fee to access data be set. Presently, data users are charged a fee based on the operation costs of different data users. This also provides a deterrent against frivolous, excessive and irresponsible requests. Setting an across-the-board maximum fee will remove this flexibility of the PDPO and impose additional burdens on businesses. There is already a safeguard in the PDPO against excessive fees for accessing data. The PCPO may take action should the fee be deemed to infringe upon DPP 6.

- End -

對「檢討個人資料（私隱）條例公眾諮詢」的意見

香港東區區議員楊位醒

《個人資料》（私隱）條例》於 1996 年生效，距今已有十多年，由於社會的發展和科技的進步，本人同意，現有條文確實有需要作適當修改以保障個人資料。

據諮詢文件顯示：特區政府政制及內地事務局在個人資料私隱專員的協助下，就有關條例進行了全面檢討，提出了多項建議。

以下是本人的意見：

（1）就我們看到的建議中，有多項是關於擴大私隱專員的權力，例如：賦予私隱專員刑事調查和檢控的權力，授權私隱專員向受屈的資料當事人判給補償，授權私隱專員就嚴重違反保障資料的原則施加罰款等等。

本人認爲，私隱專員的權力其實已經足夠，與其無必要地把應屬法庭或警方的工作都包攬上身，倒不如切切實實做好本份的工作，精益求益，確立專業精神。其實，回看私隱公署一直以來的工作表現，包括最近審計署就私隱公署提出的多項意見，可以看到私隱公署其實大有改善的空間，與其急急忙忙擴大權力而容易出現更多流弊，倒不如認認真真地一步一個腳印做好工作。不過，就授權私隱專員爲受屈的資料當事人提供法律協助，這反而是可以考慮的。當然，要檢討私隱公署是否有足夠的資源，若否，政府可適量增加資源，以協助公署設立訴訟基金，協助受屈者進行民事申索。

（2）修改建議中提到：敏感個人資料，如指紋等應受到更嚴格的規管，這點本人非常贊同。至於敏感資料是否還包括病歷、住址等多項，政府應繼續諮詢及聽取市民的意見，以作界定，並在不影響公民自由的前提下，將未經授權而惡意披露的各項敏感個人資料的行爲定爲刑事罪行。

（3）本人認爲，應設立個人資料通報機制，規定在個人資料外泄或遺失時，資料使用者必須通知私隱專員，經有關方面評估後，再決定是否發出指引通知受影響人士。

（4）目前條例，如資料使用者違反保障資料原則，私隱專員可發出執行通知，要求資料使用者在指定時限內採取指定的補救措施，藉以糾正違規情況。本人認爲，若發生資料使用者屢次違反執行通知的行爲，應對之處以更重的懲罰。

（5）本人同意應提高在直接促銷活動中不當使用個人資料的罰則，而金額可考慮從現在的一萬元提高至五萬元，與其他法例看齊。

（6）本人認爲，應立法規管在未經他人同意下，取得個人資料並將之在互聯網上公開的行爲。

（7）修改建議中提到有多項就未成年子女與家長的關係問題，我們認爲，應充分考慮中國人家庭的觀念，而個人私隱亦非絕對，必須尋求與其他權利以及某些公眾和社會利益取得平衡，故在這方面的修訂要慎重，不可草率，例如在父母查閱其子女個人資料的權利不應被無理限制以及兒童個人資料私隱權利亦應受到尊重這兩方面要取得平衡。

（8）本人認爲，向執法機關及救援和支援機構給予豁免，以在緊急情況下處理個人資料，這是合理的。而資料使用者在確知兒童的個人資料是與家長或監護人履行照顧和監護責任有關的，應可獲准將此等資料轉移給未成年人的父母或監護人。

經濟動力
ECONOMIC SYNERGY

梁君彥議員就檢討《個人資料(私穩)條例》諮詢文件的回應

前言

過去十年間，資訊科技迅速發展、互聯網普及、電子商貿快速增長等原因，爲個人資料私隱保障帶來新挑戰。因此，政府於本年八月發表檢討《個人資料(私隱)條例》的諮詢文件（下稱「諮詢文件），諮詢公眾有關敏感個人資料、資料保安、私隱專員的執法權力、罪行及制裁等各方面的意見，目的是希望完善條例，更有效地保障香港市民的個人私隱。對於這份諮詢文件，本人有以下回應：

敏感資料立例不宜過急

諮詢文件表示，資訊科技的發展爲現時規管個人資料私隱的制度帶來挑戰。誠然，隨着資料以電子方式儲存、傳輸及處理，個人資料外洩的後果，所造成的損害遠比過往嚴重。尤其是某些個人的隱密資料，當不幸被洩及經互聯網傳播，會給當事人無法估量的傷害。但同時，我們亦要明白，香港作爲一個外向型經濟體，立例時宜多參考外國例子，如操之過急，則有可能影響香港將來發展，因此，我認爲有關敏感資料所包括的範圍亦應多考慮外國做法。

歐盟95/46/EC指令第八條第一款列明，種族或民族本源、政治意見、宗教或哲學信仰、工會會籍、健康狀況及性生活爲需要特別限制處理的個人資料。而歐盟成員國英國及德國，亦有相類限制。英國《1998年保障資料法令》及德國《聯邦資料保護法令》，亦分別使用「敏感個人資料」（sensitive personal data）及「特殊組別個人資料」（special categories of personal data），指出某些資料需要特別留意。而澳洲《1988年私隱法令》有關敏感資料（sensitive information）的內容，亦與歐盟、英國及德國相若。

我認爲，香港可參照歐盟、英國、德國及澳洲的做法，把種族或民族本源、政治意見、宗教或哲學信仰、工會會籍、身體及精神狀況、性生活及犯罪紀錄定爲敏感個人資料。

至於生物辨識資料，如瞳孔特徵、掌紋及指模等，外國還未有先例列爲敏感個人資料，香港絕不宜走在外國前頭，以嚴厲方式規管這類資料，以免窒礙生物辨識科技的研究，局限了這門新興產業的發展。

事實上，自諮詢文件推出以來，從事開發生物辨識系統的資訊科技企業及有關設備的生產商，已即時受到打擊，業務大不如前。由於未清楚將來生物辨識資料的規管程度和模式，用戶已紛紛暫停向開發商採購新設備和系統。若政府最終決定實行嚴厲規管，恐怕這門原來有大好前景的產業，發展空間會急劇收縮，大大影響業內的企業和員工。

基於以上原因，我不贊同把生物辨識資料列爲敏感個人資料。

對資料處理者先行間接規管再檢討成效

由於所採集資料往往不是由資料使用者保管，而是外判予其他機構處理，而現有法例卻沒有規管那些資料處理者，因此我亦同意修例，對資料處理者加強監管，以保障資料使用者及資料當事人。但另一面，正如諮詢文件所言，我們亦須在保障個人資料私隱與正常商業運作之間，取得適當平衡，以免顧此失彼。

作爲平衡，我認爲現階段不須直接規管資料處理者，以免突然增加業界的壓力及成本。我們可先行間接規管，依靠資料使用者確保其資料處理者儘一切合理方法保障個人資料安全。即使資料處理者有過失，私隱專員亦不能直接介入。但資料使用者仍可根據合約法尋求補償，而資料當事人亦可向資料使用者尋求補救。此外，政府可制定指引，訂明那些措施爲合理措施，以便業界「有所適從」，政府也可劃定3至5年後檢討，再視乎當時情況，考慮是否需要改爲直接規管。

只有敏感資料洩密才須通報

現行的自願性通報機制，比較適合社會現況，亦較爲業界接受。若硬性通報，會對機構造成沉重負擔，有違平衡保障私隱與商業運作的原則。此外，正如澳洲法律改革委員會所言，太多的外洩通知可能會令大眾難以判斷那些事故涉及重大風險，造成「通知疲勞」，於社會亦非好事。因此，我建議，除非事件涉及敏感個人資料，須硬性規定通知私隱專員，否則其他事件可繼續實施自願性通報機制。

私隱專員權力不宜過大

雖然私隱專員提出3個理由，要求得到刑事調查和檢控罪行的權力，以及搜查和檢取證據等附帶權力，但我認爲，理據並不算充分。首先是現行安排運作暢順，實毋須改變。其次，其他相類似組織，如平機會等，亦沒有這些權力，但私隱專員所提的3個理由：擁有第一手資料、熟悉相關條例、及節省檢控時間，均是其他相類似組織所有的條件。如果因這3個理由讓私隱專員得到這些權力，恐怕會

引起連鎖反應，其他類似組織亦會提出同樣要求，屆時，香港的司法系統難免會受到震盪。

鑑於法律訴訟既費時又昂貴，且民事索償的結果又未可預知，很多資料使用者即使受屈，亦沒有申索補償，因此政府建議私隱專員有權判給受屈的資料當事人補償。針對這個問題，當初法改會已表明，把執法和處罰的職能歸於同一機構，並不可取。我十分同意法改會的意見，認爲應維持現狀，即私隱專員負責裁定保障資料原則是否遭違反，而法庭負責釐定補償額。**我希望在有關司法的分工上，除非有必要的原因，否則應維持原狀，以免造成任何不必要的影響。**

雖然我反對建議4及6，但卻支持建議5，認爲私隱專員可爲資料當事人提供法律協助。正如私隱專員所提，他們有第一手資料，又熟悉相關條例，是一般市民沒有的條件。如得到私隱專員協助，當受屈一方可以更準確評估民事索償的勝訴機會，亦不會因費用問題而對法律訴訟卻步，那麼政府建議6的原因便不再存在了。

規管過嚴將致惡果

雖然保護個人資料是文明社會應當做的事情，但現今資訊科技發達，很多時市民都會不小心或不自覺洩露其他人的資料。**如果規管過嚴，有可能會影響香港市民珍而重之的資訊及言論自由。**

我對有關「罪行及制裁」，即建議7至12都原則上同意。但有關建議7：把違反保障資料原則訂爲罪行；建議8：在未經授權下取得、披露和出售個人資料；及建議9：就同一事實重複違反保障資料原則，**我則認爲必須給予被控方申辯權，並在非惡意、非故意及有合理辯解的情況下可豁免刑責。**這樣做可以平衡保障個人私隱及保障言論自由兩方面，是一個比較可行的辦法。

總結

科技發展一日千里，優化條例以適應時代變遷，保護市民的個人私隱實有所必要。但同時我們亦須平衡營商成本，以及對其他方面的影響。敏感資料內容，我們宜參考外國規定及個案，以免偏離國際標準。而對資料處理者的監管，亦應循序漸進，以平衡保護個人私隱及商業運作。有關私隱專員的權力，在現行體制運作良好的情況下，根本沒有必要作出大改動。最後，我亦希望政府修例時不應只看到保護私隱，亦要顧及言論及資訊自由之可貴。只有如此，才可顧及社會的整體利益。

香港工業總會
Federation of Hong Kong Industries

香港工業總會
FHKI

S0122

香港資訊科技業協會 Hong Kong Information Technology Industry Council

香港工業總會轄下 Under the auspices of the Federation of Hong Kong Industries

Dr Paul Kan, Chairman

30 November 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong

Dear Sir / Madam,

Response to Public Consultation on
the Review of the Personal Data (Privacy) Ordinance submitted by
Hong Kong Information Technology Industry Council

We refer to your letter of 28 August 2009 inviting our Council to submit our views on the subject, we have discussed the Consultation among our members and compiled a Response as attached, with a focus on IT-related aspects.

HKITIC urges the Government to exercise extreme prudence when contemplating to introduce new laws to the existing regulatory regime, especially as Hong Kong has started to recover from the devastating financial tsunami. While IT continues to play a critical role in transforming the society and the economy, technology players and developers must be given sufficient latitude and a free and friendly operating environment to facilitate continued innovation and development.

IT will contribute greatly to Hong Kong's sustainable development as it is a central facilitator to the six new growth areas set forth in this year's Policy Address. Amendments to the legislations might be perceived with a negative impact on technology development with an unduly onerous regulatory environment, thus affecting Hong Kong's competitiveness.

The Council, with a readiness to contribute to the advancement of technology and help industries move up the value chain, requests the Government to refrain from introducing amendments that are beyond "reasonable", and to provide clear guidance and remove any uncertainties in the operating environment, to ensure that the IT sector and Hong Kong's competitiveness can continue to sustain and flourish in a free and friendly community.

Yours sincerely,

(Signed)

Shirley Ha
Vice-Chairlady
Hong Kong Information Technology Industry Council

Response to Consultation Document on Review of the Personal Data (Privacy) Ordinance
By Hong Kong Information Technology Industry Council

Proposal No.1: Sensitive Personal Data

Hong Kong's existing PDPO does not define sensitive data. As many developed countries such as UK, and Australia have introduced sensitive personal data regulations, Hong Kong may refer to them to determine if we need a "sensitive data" category at this stage. We are neutral to the proposal to classify and differentiate sensitive personal data from the non-sensitive, however the choice of data should be judicious. We suggest that we should first start with a minimal set of sensitive personal data, which are really considered important, and may then add to the list only when necessary.

Recently, there have been concerns about companies collecting employees' biometric information for use in commercial application purposes such as access control identification and authorization. ***HKITIC is strongly opposed to making biometric information sensitive personal data, as by doing so, PDPO would deter, if not prohibit, the collection of such information for further development and usage of new technologies and applications.*** We must realize that as technologies advance, our routine life-style may have to change and adapt to new technologies. Many countries are developing applications using biometric data, and some of them are very advanced in the adoption of biometrics technology. If at this stage we take a broad brush approach to classify biometrics as sensitive personal data and subject them to more stringent regulations, this would amount to a wilful act of interfering with and adding burden to local research and development.

The singling out of "biometrics" in the Consultation as a potential candidate for sensitive data has already left the vendors and developers in biometrics very unsettled, resulting in major losses of business. Uncertainties abound, and it's difficult to reach a consensus on how biometrics should be defined and treated. ***As such, we strongly advocate that Guidelines are more appropriate in dealing with biometrics than legislation.***

Date of birth and location information could be categorized as sensitive, but age and gender are subjective, even though people argue that such information may be discriminative in nature. The point is making such information sensitive personal data does not eliminate discrimination.

The making of non-compliance with Data Protection Principles (DPPs) with regard to handling of sensitive personal data an offence is not recommended because, as mentioned in the consultation paper, an inadvertent act or omission would leave data users to face criminal liability. This will scare data users, increase their administrative cost, or force them to consider moving their business outside Hong Kong. Instead, we suggest PDPO to facilitate the collection of sensitive personal data by providing clear and comprehensive procedures and guidelines in collecting, handling, and

protecting such data as well as any remedial actions that data users need to take in case of data leakage. *We agree with the view to revise the existing level of fine and accept the proposal of increasing the monetary fine value. However, we 're opposed to a longer term of imprisonment. A heavy fine should serve quite effectively as a deterrent.* PDPO should provide clear definitions of the different levels of penalty and the conditions under which data users are considered to have violated the principles.

As far as the sensitive personal data are concerned, we do not object if the existing regulatory regime governing contravention of DPPs involving personal data is extended to sensitive personal data, provided enough education, promotion and publicity are made to the public, with clear guidelines and code of practices given to data users, and full preparatory work to be in place for the PCPD to take up the challenges.

Both grandfathering and transitional arrangement have their shortcomings. Grandfathering does not demand additional administrative work and costs but it is unfair to data subjects who have their sensitive personal data previously collected by data users. On the other hand, transitional arrangement creates confusion and impose extra administrative burden and costs on data users. We think the former is more practical.

Proposal No. 2: Regulation of Data Processors and Sub-Contracting Activities

In considering the regulation of data processors and sub-contracting activities, we believe that there are difficulties in defining generic obligations for data processors. Besides, there are difficulties for PCPD to directly intervene with faults committed by a data processor, for instance, when the data processor is not constituted locally in Hong Kong where HKSAR Law cannot be applied.

We think that a data user should be held responsible for any contravention of data privacy. Data user should be prudent in protecting data and should be judicious in choosing a reliable data processor. *We disagree with direct regulation of the activities of data processor under the PDPO because there are difficulties in drafting law that is appropriate for the variety of data processors.* Besides, many data users outsourced their work to foreign data processing companies, who are not bound by local regulations. So directly regulating data processors may only increase their costs and impact their competitiveness against foreign data processors. Instead, we agree with the view of indirect regulation on data processors through the data users by contractual and other means; PCPD could devise a code of conduct for data users and data users could refer to this code of conduct or data privacy guidelines to draft their contracts and to choose their sub-contractors in accordance with the guidelines.

Proposal No.3: Personal Data Security Breach Notification

We support the view of PCPD that a requirement to notify all affected parties of each and every personal data leakage incident is costly to organizations and individuals. In addition, those same recipients who receive too many breach notices may have difficulty to assess which ones carry a real risk of harm and which ones are minor in nature and consequence. Or they may become desensitized to the notices and ignore some of the notices. Therefore, the impact of mandatory privacy breach notification on businesses cannot be underestimated. Considering that a number of overseas jurisdictions adopt voluntary guidelines on privacy breach notifications, we agree with PCPD to start with a voluntary breach notification system so that we can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing undue burden on the community. We highly appreciate that the PCPD would issue clear guidelines on voluntary privacy breach notification.

On the issue of which circumstances that notification should be triggered, we think that the primary concern of the public is whether their sensitive information may allow criminals to take advantage and cause them to suffer financial loss. In this sense, we suggest if the leakage of personal data that involves any identity information, such as hkid number, passport number, and financial information such as credit card numbers, bank statements or transaction information, or insurance details etc., then the notification should be triggered; such notification should be sent to the PCPD and data subject; the time of notification should be right after the organization's risk assessment which has determined to trigger notification; the means of notifications could be mail, email, sms or phone calls, allowing different means of notification to mitigate the notification cost incurred by the organizations; the content of the notifications should include the leakage information, when and what to be alerted as well as the organizations' remedial actions. The consequences of failing to give notification may give rise to customers' complaints, claims, and damage of brand name, which are intangible but important to the organizations' business.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

We see no compelling reason to give the PCPD the power to investigate into and prosecute criminal offence cases because, as mentioned in the consultation, effective protection to personal data privacy hinges on the adequacy of penalty sanction, rather than on who the party responsible for initiating prosecution is. Besides, the number of cases referred to for prosecution every year is manageable and do not see any trend of acute increase. However, we do not support the extension of time limit for laying information for prosecution of an offence from six months to two years as it would take too long to handle a case and it is unfair to the affected subject.

Proposal No.5: Legal Assistance to Data Subjects under Section 66

We do not think that it is necessary to confer the PCPD with the power to provide legal assistance

to aggrieved data subject because many cases of the contravention of personal data protection are not urgent in nature. Conferring the power to the PCPD may lead to inefficient use of government resources; and when there is an easy path to request compensation, some people would try their luck and abuse the system. We need to strike a good balance between providing legal aid for people with real needs and avoiding other people who just want to try their luck.

Proposal No.6: Award Compensation to Aggrieved Data Subjects

We are against award compensation to aggrieved data subjects directly by the PCPD because firstly, we are concerned that awarding compensation would vest in a single authority an undesirable combination of enforcement and punitive functions as mentioned in the consultation paper. Secondly, we are concerned about the complexity and credibility in determining the judicious compensation amount, and any dispute on the amount will have to be settled in court eventually. Besides, if the PCPD have the power to determine the amount of compensation, it may lead to abuse since many people may just try their luck if there is no need to go through the court process, as a result of which the PCPD would have to handle many more cases that may not originally be eligible for compensation. Furthermore, the PCPD would have to expand its scale in investigation and enforcement activities; the expenditure budget of the PCPD would increase as a result.

Proposal No.7: Making Contravention of a Data Protection Principle an Offence

We agree with the view of not making contravention of a DDP a criminal offence to avoid many cases of inadvertent act or omission attracting criminal liability. We however support increasing the existing penalty levels to reinforce the deterrent effect.

Proposal No.8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

We resist making unauthorized obtaining and disclosure of personal data an offence because it is very difficult to define if the person knowingly or mistakenly obtains or discloses personal data without consent. Instead, we would prefer data users to be contractually bound with their employees or sub-contractors, such that these parties clearly know their obligations towards others' personal data; and that disclosure and sale of personal data would become a commercial crime and should be handled by police.

The penalty of Unauthorized Obtaining, Disclosure and Sale of Personal Data could be increased to double or triple the current level as a deterrent.

Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts

As PCPD has not come across any case of circumvention of resuming the same contravening act or practice shortly after compliance with an enforcement notice issued against him, there is no compelling argument to make such act an offence. Instead, the penalty level could increase if there

are repeated enforcement notices being issued.

Proposal No.10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

Empowering the PCPD to determine monetary penalty on serious contravention of DPPs would involve the complexity of granting PCPD both the power of legislation and enforcement within a single department. This may not be welcomed. Apart from this complexity, we agree with the view of empowering PCPD to require data users to pay monetary penalty for serious contravention of DPPs, provided that a comprehensive guidline on the circumstances where PCPD considers appropriate to issue a monetary penalty notice is well prepared and both data subject and users are well educated on this.

Proposal No.11: Repeated Non-compliance with Enforcement Notice

We think that doubling the penalty level for repeated non-compliance with Enforcement notice would be suitable, which would mean a fine of up to $100,000, and in the case of a continuing offence, a daily fine of $2,000. However, we do not agree to increase the sentence, which should stay at two years.

Proposal No 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

We agree with the view of raising Penalty for Misuse of Personal Data in Direct Marketing subject to a comprehensive guidance on how such penalty is imposed on direct marketing companies. Every business requires promotion and follow-up services, and direct marketing plays an important part, which should not be unduly restrained. The penalty level can be raised to $50,000.

Proposal No 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

We agree to adopt the definition of "relevant person" under the PDPO and include the guardians of data subjects with mental incapacity as the definition of third party to give consent to the change of use of personal data of vulnerable classes of data subjects.

Proposal No 14: Parent's Right to Access Personal Data of Minors

It is the role of parent to take care of their children, and that includes having access to their data if necessary. We do not agree to introduce new provisions to permit a data user to refuse a data access request made by a "relevant person". It is inappropriate for data user to make the decision on whether refusing the access really would protect the interest of the minors. In case of suspected child abuse, the data user should report to the authority and let the court make the decision. After all, Hong Kong has a sound law enforcement and legal system in place, and there is no need for everybody to try and play judge.

Proposal No 17: Erasure of Personal Data

We agree with the view that PDPO requirements should not be such as to pose an excessive burden on businesses. We are neutral to the proposal on amending the PDPO so that the provisions concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use.

-end of Response-

YAHOO!

S0123

BY POST AND EMAIL

30 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, 3/F East Wing
Central Government Offices
Lower Albert Road
Hong Kong
pdpo_consultation@cmab.gov.hk

Consultation Document on Review of the Personal Data (Privacy) Ordinance ("Ordinance")

Yahoo! Hong Kong Limited is pleased to have the opportunity to respond to the above consultation.

Background about Yahoo! Hong Kong

Yahoo! Hong Kong is operated by Yahoo! Hong Kong Limited, which is a wholly-owned subsidiary of Yahoo! Inc., a leading provider of comprehensive online products and services to consumers and businesses worldwide. Yahoo! is a prominent Internet brand globally and the most trafficked Internet destination worldwide. Launched in January 1999, Yahoo! Hong Kong is a Chinese-language site of the Yahoo! network tailored to meet the needs of local audience of Hong Kong. Yahoo! Hong Kong is consistently ranked No. 1 in audience reach in monthly Nielsen//Netratings Reports since April 2001.

Overview

The Ordinance has been in force since 1996. It is our view that the Privacy Commissioner for Personal Data ("**PCPD**") has been effectively enforcing the Ordinance to protect the privacy of the Hong Kong people. While we do not see any need to substantially amend the Ordinance, we welcome and appreciate the Government's proposal to review and improve it.

We would agree with the guiding principles stated in the Consultation Document that privacy is not an absolute right and there needs to be a balance between the interests of different stakeholders in protecting personal data. Any change to the Ordinance should not undermine Hong Kong's competitiveness and economic efficiency as an international city. Bearing in mind that most Asian countries (such as Singapore, another major regional business hub) do not have privacy laws, any increase in the burden on businesses to comply with the Ordinance would undoubtfully discourage or drive away foreign investment.

Comments on the Proposals

We set forth our comments on the individual proposals below.

<u>Proposal No. 1: Sensitive Personal Data</u>

We do not see the need to create a sub-classification of personal data considered "sensitive data" within the Hong Kong legal framework. Though the Consultation Document correctly mentioned that certain jurisdictions like the EU and Australia do have such provisions in their laws, in Hong Kong, there have not been particular cases or requests from the general public/business sectors to define this new category of data.

YAHOO!

Furthermore, as mentioned in the Consultation Document, there is no universally agreed definition for what should constitute sensitive data. If the term "sensitive data" is to be defined, then we would suggest that its definition must be inclusive, specific and unambiguous and only include specific data that warrants more stringent rules and additional protection. We would oppose to any reference to some vague and general principles or criteria in defining "sensitive data", which would only introduce uncertainty in the law for both the general public and business sectors alike. The Consultation Paper contemplates the prospect of higher level fines for those who contravene the newly defined "sensitive personal data category", any uncertainty on the scope of "sensitive data" will undoubtedly increase the operational and financial burden of the business sector, without a clearly articulated benefit for the public. In this connection, taking stock of the specific language suggested, we do not agree that "data likely to be utilized in discriminatory beliefs" should be classified as distinct sensitive data, because in theory, various types of even less sensitive data could nevertheless be misused for improper discriminatory purposes (consider for example misuse of gender, age or even residential address).

With respect to the specific issue of use of biometric data for various purposes, if the Government and the community consider that biometric data are both commonly collected in Hong Kong and require additional privacy rules, for legislative purposes, it would be acceptable to define "sensitive data" as meaning "biometric or similar data". Such narrow definition could address the concerns of the Government and the public, without being overreaching in impact on the community or on the business sector.

Finally, it is also our view that reducing the prospect of impermissible use of data for improper discriminatory purposes will not be achieved through "defining" data as sensitive or non-sensitive, but instead would be furthered by focusing on permissible and impermissible uses of all types of data.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

The current DPP 4 provides that with respect to data held by a user, all practical steps must be taken by that user to protect against unauthorised or accidental access, processing, erasure or other use having particular regard to any measures taken for ensuring (1) the integrity, prudence and competence of persons having access to the data and (2) the secure transmission of the data. In our view, this DPP already effectively stipulates that the data user is at times responsible for the security of the data, whether the data is held by himself or his contractors and agents. We therefore do not see distinct value in explicitly imposing additional duties on the data users with respect to security (as per paragraph 4.09). The Government could consider, however, a minor amendment to DPP4 to clarify that personal data is deemed held by the data user himself if held by his agents or contractors to further clarify the intent of the law today to avoid possible gaps in responsibility.

If the Government and the community consider that direct regulation of "data processors" is a necessary enhancement, we would agree with paragraph 4.19's proposals that the law has to address specific issues for specific types of Internet-related business. As stated, the Internet environment is fast-evolving and it is important that privacy law does not inhibit the development of desirable new Internet-related services. We would support the proposal that if the data processor has adopted a privacy policy, which sets out its policy regarding the use, security and retention of personal data, then the obligations in paragraph 4.14 should be construed as a requirement to honour the relevant terms of such privacy policy. Such proposal will provide sufficient flexibility to the data processor of internet-related businesses to adopt privacy policies appropriate to their businesses and also provide regulatory certainty around personal data privacy obligations.

Proposal No. 3: Personal Data Security Breach Notification

We would agree that data users should be encouraged to properly disclose data leakage incidents. However, we are of the view that voluntary notification schemes can be adopted rather than relying on mandatory requirements, recognizing the importance that the format of consumer communications should be entirely voluntary and discretionary and may require a degree of flexibility depending on business type, and what information is available to the business about its consumers. Incidents justifying disclosure inevitably would vary and any stipulated or compulsory notification could prove too rigid and impracticable commercially. Furthermore, mandatory notification might cause abuse of notice to the public which will then forfeit the original intent. By abuse, we are focusing on the harms to consumers that can result from over-notification, or notification for technical breaches that do not result in substantial consumer harms.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

We are of the view that the present scheme is working properly and do not see any urgent need to confer new criminal investigation powers on the PCPD.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

We would agree with the LRC Report that conferring power to the PCPD to award compensation would vest in it an undesirable combination of enforcement and punitive functions. It should remain the province of the Hong Kong courts to determine the appropriate amount of compensation payable.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

The PCPD is empowered to remedy contravention of a DPP by issuing an enforcement notice to direct a data user to act.

The DPPs are couched in generic terms and can be subject to a wide range of interpretations – this is appropriate to afford good flexibility to the PCPD in performing his functions. On the other hand, legislation imposing criminal liability should be tightly worded and narrowly construed. As such, a DPP contravention should not be made an offence. The proposal to make a DPP contravention a criminal offence will definitely create significant amount of risk for members of the business community that may unintentionally, inadvertently or mistakingly violate the DPPs. Moreover, the Ordinance currently provides that in case of contravention, the PCPD may issue enforcement notices whereby a failure to obey them would constitute a criminal offence, with the possibility of imprisonment of 2 years. We are of the view that the existing penalty already provides a more than sufficient deterrent against DPP's violations.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

We would agree with the acts described in paragraph in 6.06(a) of the Consultation Document should constitute criminal offences. As regards the acts described in paragraph 6.06(b), they should constitute criminal acts only when the disclosure was intentional (ie, excluding inadvertent disclosure). We need to be cautious about the risk to the public in the case of internet-browsing under the proposal. With the advent of advanced internet technology and the inability of end users to fully comprehend the risks involved in the use of computer software, personal data may be disseminated unintentionally through the use of a computer software by the user himself, and such act could be caught as "reckless

YAHOO!

disclosure" under the proposed offence. We would support the view that "reckless disclosure" of personal data without the consent of the data user will be an offence only when it is for profit or malicious purpose. Such clarification will help relieve the concern of general public and provide deterrent effect as well.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

Consistent with our rationale in response to Proposal 7, we do not agree that Proposal 9 is necessary at this time.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

Section 66 of the Ordinance provides for compensation to be paid to the person who suffers damage by reason of a contravention of any DPP. The compensation includes injury to feelings and by its very nature is directly proportional to the seriousness of the contravention. Hence, we do not see the need to impose additional penalties for "serious contravention", as proportionality is already implied in Section 66. In addition, we do not agree that power should be conferred to the PCPD to require data users to pay monetary penalties for serious contravention of DPPs as it could vest in the PCPD an undesirable combination of enforcement and punitive functions.

If, however, this proposal were to be implemented, we would opine that the definition of a "serious contravention" under the UK Data Protection Act is too vague to provide enough clarity to data users and is therefore subject to arbitrary interpretation by the enforcer. Terms such as "substantial damage or distress" should be quantified. For example, it could be defined that a contravention is serious if it affects more than a certain number of data subjects or directly causes substantial financial loss of more than HK$1,000,000.

Moreover, under the current provisions of the Ordinance, a person who is dissatisfied with the decision of the PCPD may appeal to the Administrative Appeals Board, whose decision is final and not subject to further appeal, except, in theory, for judicial review on limited grounds. We would suggest that additional grievance redress channels should be created to ensure due process and justice. We would also suggest that the Ordinance should have provisions to clearly define the level of penalty to be imposed in relation to each type of contravention. This will help to give clarity to the data user and also provide deterrent effect.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

As stated in the Consultation Document, there has not been a problem with repeated offenders, we are of the view that there is no need to impose a heavier sanction for data users who repeatedly contravene an enforcement notice.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

Our view is that the current level of punishment already provides sufficient deterrent as there were not many cases since the implementation of the Ordinance. Furthermore, this proposal might increase the burden of business sector especially those that rely on personal data information for proper and legal direct marketing purposes and there is no sufficient rationale to impose a higher punishment level for "Direct Marketing" per se. Accordingly, we do not see the necessity to raise the level of punishment for misuse of personal data in direct marketing.

YAHOO!

Proposal No. 16 : Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We would strongly agree with and support the suggestion of adding a new recognized basis upon which data users may refuse to comply with a data access request under section 20(3), where the data user is either obliged or entitled not to disclose personal data. This will provide much needed clarity that data users need not breach either the data access provision or the relevant secrecy provisions contained in other ordinance through the very act of complying with one of them.

Proposal No. 20 : Circumstances for Issue of an Enforcement Notice

We are of the view that the current provision on the circumstances for issue of an enforcement notice is operating smoothly and thus we do not see the need to expand the scope of circumstances as proposed on the Consultation Document.

Proposal No. 36 : Definition of Crime under Section 58

We do support the clarification of the scope of exemption provision under Section 58 but we would suggest that the term "law enforcement agencies" should be clarified as meaning "law enforcement agencies in Hong Kong" only. This will ensure that Hong Kong data users will only have to deal with law enforcement agencies in Hong Kong, which may or maybe not providing assistance to foreign jurisdiction under multilateral and bilateral cooperative agreements or arrangements.

Conclusion

The review of the Ordinance gives rise to a lot of complex and controversial issues, involving various stakeholders in the society. It will take considerable time and effort for our society to come to a consensus on how the law should be reformed. We would expect that after this initial consultation exercise, further and more focused consultation will be conducted with specific legislative draftings. We look forward to continue working closely with the Government in its next-round consultation.

Again, thank you for the opportunity to give our comments above. Should you have any questions, please do not hesitate to contact the undersign at (deleted)or (deleted)

Yours faithfully

(Signed)

Ms Noelle Tai
General Counsel
Yahoo! Hong Kong Limited

Hong Kong | BAKER & McKENZIE

Consultation Document on Review of the Personal Data (Privacy) Ordinance

Response by Baker & McKenzie

November 2009

Contents

1.	Key to Abbreviations	3
2.	Introduction and General Comments	4
3.	Sensitive Personal Data	5
4.	Data Security	7
5.	Enforcement Powers of the Privacy Commissioner for Personal Data	11
6.	Offences and Sanctions	14
7.	Summary of Proposals for Comments	19

KEY TO ABBREVIATIONS

Administrative Appeals Board ("**AAB**")

Constitutional and Mainland Affairs Bureau ("**CMAB**")

Consultation Document on Review of the Personal Data (Privacy) Ordinance dated August 2009 ("**Consultation Document**")

Data Protection Principle ("**DPP**")

Department of Justice ("**DOJ**")

Equal Opportunities Commission ("**EOC**")

Office of the Privacy Commissioner for Personal Data ("**PCPD**")

Office of the Telecommunications Authority ("**OFTA**")

Personal Data (Privacy) Ordinance ("**PDPO**")

PCPD's Information Paper on Review of the Personal Data (Privacy) Ordinance dated 9 September 2009 ("**Information Paper**")

Unsolicited Electronic Messages Ordinance ("**UEMO**")

1. Introduction and General Comments

1.1 Baker & McKenzie is a leading global law firm with 68 offices in 38 countries across the world. Experienced privacy practitioners in these offices form part of our Global Privacy Group.

1.2 Our Hong Kong office has significant experience advising on privacy and data protection issues. Our team has assisted domestic and multinational clients devise practical and strategic privacy compliance solutions. We advise on issues specific to the workplace, the internet and individual industry sectors, such as banking, telecommunications, financial services, entertainment, retail, insurance, information technology, marketing, outsourcing and healthcare.

1.3 We are grateful for the opportunity to provide our comments on the Consultation Document on Review of the Personal Data (Privacy) Ordinance which was published for public consultation in August 2009.

1.4 The primary purpose of the PDPO is to protect the privacy of individuals in relation to personal data and to set out the duties and powers of the PCPD.

1.5 The PDPO has been in force since 1996 and, since then, changes in the information and technological environment in which we operate have presented new challenges in relation to the protection of personal data. In addition, the increasing number and severity of data leakages and the increasing focus of regulators on privacy and data protection issues have raised awareness as to the need to safeguard personal data.

1.6 We agree that there are a number of issues concerning the PDPO which are due for review and many of these have been considered as part of this consultation. We consider, however, that the fundamental way in which the PDPO operates, that is by providing data protection principles for fair information practices, should not change.

1.7 Whilst a large number of issues were covered in the Consultation Document, our view is that the Consultation Document should have also given further consideration to how the transfer of data to overseas jurisdictions is to be dealt with. Section 33, providing a prohibition against the transfer of personal data to places outside Hong Kong except in limited circumstances, has been part of the PDPO since its inception but has yet to come into force. We consider that this review process is the opportune time to review the need for the provision and how it should operate if it is to be enacted.

1.8 We provide below our specific comments on the Consultation Document following the order of the sections and paragraphs as they appear in the Consultation Document.

2. Sensitive Personal Data

Proposal No. 1: Sensitive Personal Data

2.1 Proposal No. 1 proposes providing a higher degree of protection to sensitive personal data and confining the scope of collection and use of such data in line with international practices. Comments are specifically invited on:

(a) whether there is a need to accord better protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances; and

(b) whether the proposed regulatory regime, including coverage of sensitive personal data, related regulatory measures, sanctions and the need for grandfathering or transitional arrangements as set out in the Consultation Document, is appropriate.

2.2 In our view, it is appropriate to apply stricter regulation to sensitive personal data, that is, by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances.

Coverage of Sensitive Personal Data

2.3 In general, we consider the proposed regulatory regime, as set out in paragraphs 3.08 to 3.14 of the Consultation Document, to be appropriate. However, we note that the Consultation Document does not put forward a proposed definition of "sensitive personal data". It discusses the fact that sensitive personal data may include biometric data, but does not explicitly state whether other intimate data, such as physical attributes, health or personal beliefs will also be subject to tighter regulation.

2.4 In our view, the definitions of "sensitive personal data" as set out in the in the UK Data Protection Act 1998 and the Privacy Act 1988 of Australia are helpful. The Annex to the Information Paper sets out a proposed definition of "sensitive personal data", which largely reflects the definitions in the overseas legislation. We agree that it is appropriate that "sensitive personal data" be defined as personal data consisting of information as to: (a) the racial or ethnic origin of the data subject; (b) his/her political affiliation; (c) his/her religious beliefs and affiliations; (d) membership of any trade union (within the meaning of the Trade Unions Ordinance, Cap 332); (e) his/her physical or mental health or condition; (f) his/her biometric data; or (vii) his/her sexual life.

2.5 We note, however, that the proposed definition of "sensitive personal data" does not include any reference to criminal records, the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any Court in such proceedings. In our view, this is a significant omission: it is important that a reference to criminal records (or the past commission of any offence etc) be included in the definition of "sensitive personal data". In our view, the relevant exemptions to the statutory protection of "sensitive personal data" will strike the necessary balance between the rights of individuals to privacy and the protection of the public interest to be informed.

2.6 One final point in relation to the definition of "sensitive personal data" relates to the reference to "biometric data". Given that the term "biometric data" is a relatively new and developing concept, if the definition of "sensitive personal data" is to include "biometric data", we recommend that "biometric data" be separately and clearly defined.

Related Regulatory Measures

2.7 It is proposed in the Consultation Document that the collection, holding, processing and use of sensitive personal data be prohibited, except in prescribed circumstances such as where the prescribed consent of the data subject has been given or where the collection, holding, processing or use of the data is necessary for the purposes of exercising or performing any right which is conferred or imposed by law on the data user. In our view, the proposed regulatory model is generally appropriate in that the strict prohibition combined with the limited exemptions strikes the right balance between the interests of the individual and the public.

2.8 It is not clear, however, how the exemptions would apply in practice. For example, it is not apparent whether a data user would need to obtain consent at the point of collection as well as when handling and again when disclosing, or whether a blanket consent would be acceptable. In addition, the proposed wording of the revised Section 4A(1)(d) set out in the Information Paper, which provides an exemption to the prohibition on collecting, holding, processing and use of sensitive personal data if the data user does so "in the course of [its] lawful function and activities with appropriate safeguard against transferring or disclosing to third parties without prescribed consent", is very broad. We recommend that this exemption be more specific to avoid ambiguity.

Sanctions

2.9 Rather than creating a specific offence for the unlawful handling of sensitive personal data an offence, we consider it more appropriate to maintain the current legislative framework and to add a separate DPP dealing with sensitive personal data. However, we agree that an exception should be made for intentional or reckless disclosures of sensitive personal data. As discussed at paragraphs 5.7 to 5.18 below, we recommend that any unauthorized obtaining, disclosure and sale of any personal data should be an offence which carries a significant penalty (see paragraphs 5.15 to 5.18 below for specific suggestions) as this will provide a more effective deterrent. In addition, we recommend that, in fixing the penalty, the Court should be required to consider a number of relevant factors as prescribed by the PDPO. Such factors may include, amongst other things, whether the contravention involved any sensitive personal data.

Grandfathering or Transitional Arrangement

2.10 Comments are invited on whether there is a need to include grandfathering or transitional arrangements in relation to any new requirements concerning sensitive personal data. From a practical perspective, it would be very difficult for a data user to obtain specific consent to continue to hold, use or process sensitive personal data. We therefore recommend that the data subject's consent to the continued holding, processing and use of sensitive personal data not be required. Any penalty for intentional or reckless disclosure, however, should take immediate effect without regard to the time when the sensitive personal data was collected.

3. Data Security

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

3.1 Proposal No. 2 sets out possible regulatory models for:

(a) data users when sub-contracting out the handling or processing of personal data; and

(b) the regulation of those agents handling the processing of personal data ("data processors") on behalf of the data user.

In relation to (b), the term "data processor" would need to be defined in amendments to the PDPO as it is not currently a defined concept in the PDPO. (We agree with the definition proposed in paragraph 4.08 of the Consultation Document). A direct and indirect regulatory model is outlined in the Consultation Document for data processors.

3.2 With respect to data users, comments are invited on whether a data user should be required to use contractual or other measures to secure compliance with the PDPO obligations when contracting out the processing of personal data to data processors. Data users are currently liable for the acts of data processors by virtue of Section 65(2) of the PDPO. Therefore, it is already in a data user's interests to take steps to ensure compliance with the PDPO in order to avoid liability for a data processor's acts.

3.3 If additional obligations were to be placed on a data user with respect to ensuring compliance, then the taking of such steps may be incorporated into a "leniency" regime to excuse the data user from liability for the breaches of the data processor or limit liability for the same. Doing so would counterbalance data users' additional administrative burden of having to take such steps.

3.4 This leniency regime could be adopted in the following ways:

(a) incorporating the obligations on a data user into the relevant DPPs (perhaps DPP3 and/or DPP4) and compliance with the DPPs would provide relief to the data user from liability under Section 65(2) of the PDPO; or

(b) simply providing that a data user will not have liability under Section 65(2) of the PDPO if he has taken all reasonably practicable steps to ensure the data processor complies with certain obligations under the PDPO (see discussion in paragraph 3.5 below).

We prefer the latter approach because it does not put additional burdens on a data user but provides an incentive for data users to take such steps. We note, however, that such a leniency regime may not be appropriate where the data processor is overseas and beyond the reach of the PCPD.

3.5 With respect to the steps to be taken by data users, regardless of which approach is taken, we do not agree that the means used by data users to take such steps should be specifically prescribed in the PDPO (i.e. contractual means) although these could be suggested in non-mandatory guidelines. Instead, we prefer that the requirement should be phrased in more general terms such as "reasonably practical steps". These steps should be appropriate for the kind of data involved, the harm that may result from inadequate security of such data and the nature of the processing of the data to be

conducted. We agree that the steps should relate to the security and safekeeping of the data, to ensuring that data are not misused and data are erased when no longer required.

3.6 With respect to the proposed regulatory regime for data processors, we have been asked to comment on whether their activities should be directly or indirectly regulated. We are in favour of direct regulation of data processors within certain limits. We consider that indirect regulation is not the correct model as it places an additional burden on data users to undertake enforcement action against data processors. We consider this to be the role of the PCPD.

3.7 The Consultation Document also calls for comments on the scope of obligations to be imposed on data processors in a direct regulation model. We agree with the scope of proposals set out in paragraph 4.14 of the Consultation Document. We note the concerns set out in the Consultation Document about data processors in Internet-related businesses who may process data for multiple uses. To address this concern, we do not agree that different categories of data processors be subjected to different obligations. Instead, we suggest that limb (a) of paragraph 4.14 be expanded as follows:

(a) ensure the personal data will be used only for the purpose for which such data were so entrusted or for directly related purposes or for purposes that the data processor has reason to believe are within the reasonable contemplation of the data user.

This addition (underlined) gives the data processor some flexibility as to the purposes for which it may use the data. It may be useful if the PCPD issued some guidance as to purposes reasonably contemplated for use of personal data in certain industries.

Proposal No. 3: Personal Data Security Breach Notification

3.8 Proposal No. 3 sets out a notification regime with two elements where a personal data security breach has occurred:

(a) a data user would be required to notify the PCPD when a personal data security breach may result in a high risk of significant harm to individuals or organisations; and

(b) a data user would decide whether notifications should also be sent to affected individuals based on an assessment of the level of risk of harm on a case by case basis.

The type of information to be set out in a breach notice to individuals is also set out in the proposal.

3.9 We are invited to comment on the need to institute a voluntary breach notification system in Hong Kong. We agree that a voluntary regime is the right approach for Hong Kong. The introduction of a mandatory data breach notification regime would impose an increased administrative burden on businesses and may also lead to "notification fatigue" amongst data subjects.

3.10 We consider, however, that unlike the current proposal, the regime should be truly voluntary. The current proposal requires the data user to notify the PCPD of serious breaches. However, our view is that both notifications to the PCPD and individuals

should be provided on a voluntary basis. Guidelines in relation to circumstances where the PCPD and/or individuals should be notified of breaches should be issued by the PCPD.

3.11 In order to encourage data users to voluntarily report breaches to the PCPD and/or individuals, we suggest that a leniency regime be considered. For example, where a data user has self-reported a breach to the PCPD and has demonstrated that is has notified affected individuals and implemented sufficient remedial measures, consideration should be given by the PCPD as to whether an enquiry or investigation is needed. The discretion not to make enquiries or to conduct an investigation based on the evidence provided will also help to free up the PCPD's resources for handling more serious cases.. We also consider that notifications made to the PCPD should be kept confidential by the PCPD.

3.12 We are also invited to comment on the components of the breach notification mechanism set out in paragraphs 4.37 to 4.42 of the Consultation Document. Our other specific comments are as follows:

(a) the content of the notice (paragraph 4.39) – we consider this information to be adequate.

(b) timing of the notice – the proposal is 5 business days from discovery of the breach for notifications to the PCPD (paragraph 4.37) and as soon as possible and without unreasonable delay for notifications to affected individuals (paragraph 4.40). We have no objection to these proposals.

(c) means of notification to affected individuals – the proposal is for notification by regular mail, or by electronic notice if the affected individual has expressly consented (paragraph 4.41). We do not agree that regular mail should be the default means of sending notices or that express consent should be required for sending electronic notices for the following reasons:

(i) sending of notices by regular mail may result in significant time in preparing the notices and cost in sending the notices, both of which may place a heavy burden on businesses;

(ii) electronic notices will be delivered to affected individuals in a much shorter period of time than a notice by regular mail, allowing affected individuals to deal with the breach more quickly;

(iii) many businesses, particularly online businesses, may not collect the postal addresses of individuals and therefore sending of notices by regular mail may not be feasible; and

(iv) requiring businesses to obtain express consent to deliver such notices electronically imposes a heavy administrative burden on businesses and may interfere with the delivery of notifications.

Our view is that data users should be able to deliver the breach notification by whichever means it usually uses to communicate with the affected individuals. No consent should be required for data users to communicate with data subjects in this way. The potential gravity of a breach should outweigh the data subject's consent to be notified of the breach by specific means.

The notification regime should also specify whether notifications will be required to be given to affected individuals located outside Hong Kong in order to avoid any misunderstandings as to the data user's obligations.

4. Enforcement Powers of the Privacy Commissioner for Personal Data

Proposal No. 4: Granting Criminal Investigation and Prosecution Powers to the PCPD

4.1 Proposal No. 4 considers whether the PCPD should be granted the power to investigate and prosecute offences under the PDPO, as well as incidental powers of search and seizure of evidence. The PCPD takes the position that the granting of such powers is justified on the basis that:

(a) this will save time and will assist the DOJ in commencing prosecutions within the six-month statutory limitation period;

(b) the PCPD will have first-hand information from its investigations and can quickly determine whether an offence has been committed; and

(c) the PCPD is capable of interpreting and applying the provisions of the PDPO and can assess the relevance and weight of the evidence.

4.2 The proposal appears to be disproportionate to the needs of the PCPD at the present time for the following reasons:

(a) We are not aware of any evidence that demonstrates that the DOJ has failed to prosecute any claims within the statutory limitation period. The concern regarding the DOJ's ability to prosecute claims within the limitation period may not therefore be well-founded.

(b) According to the Consultation Document, the PCPD has referred only 22 cases to the police for prosecution between 2006 and 2008. We are not aware of any evidence that the DOJ caseload demands a change in the way cases are prosecuted under the PDPO.

(c) The DOJ is an independent body appointed to prosecute criminal offences. In the absence of compelling grounds justifying the proposed amendment, we see no reason to depart from the present arrangement or for the powers of the Secretary for Justice to be delegated to the PCPD for the prosecution of cases under the PDPO.

(d) We share the community concern about vesting too much power in one body. The granting of prosecution powers to the PCPD is not in consonance with the intended spirit of the legislation which includes empowering the PCPD to educate the public on the PDPO and to monitor and supervise compliance with the PDPO. Under the present regime, data users are more likely to make voluntary disclosures to the PCPD and to work with the PCPD to improve their systems and to enhance protections for personal data. We consider that the granting of prosecution powers to the PCPD will dramatically reduce the number of voluntary disclosures and will materially alter the relationship between the PCPD and the public.

4.3 With regard to the proposal to grant to the PCPD powers of search and seizure of evidence for criminal prosecutions, we understand that this proposal is not being pursued (Annex 2, C.1 of the Consultation Document). Since there is no compelling reason for granting powers of prosecution to the PCPD, it would appear unnecessary in any event for it to be granted powers of search and seizure for such prosecutions.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

4.4 Proposal No. 5 considers whether the PCPD should be empowered to provide legal assistance to aggrieved data subjects. This is akin to the EOC's power to grant legal assistance to complainants under Hong Kong's anti-discrimination legislation. In considering whether to grant legal assistance, the EOC considers a number of factors, including:

(a) whether the case raises a question of principle;

(b) the complexity of the case (it may be unreasonable to expect the applicant for legal assistance to deal with the case unaided where the case is complex);

(c) whether the case can establish a useful legal precedent; and

(d) whether the case can effectively enhance public awareness on equal opportunities issues.

4.5 It is our view that the granting of legal assistance helps to ensure that a body of case law is built up in Hong Kong with useful precedent value so that the public understands how the relevant legislation is to be interpreted and implemented. It also enables aggrieved persons to institute meritorious claims which would not otherwise be commenced due to the lack of funds.

4.6 We therefore agree, in principle, with the proposal to empower the PCPD to provide legal assistance to aggrieved data subjects where similar criteria to those considered by the EOC are satisfied.

4.7 Having said this, we consider that such legal assistance should be granted only in a limited number of cases where the criteria, such as those listed above, are fulfilled. This appears to be the situation under the anti-discrimination legislation. Taxpayers' money should not, for example, be expended on assisting aggrieved persons to pursue damages in cases where the prospect of succeeding are not considered by the PCPD to be reasonably high and where the above and other similar criteria are not satisfied.

4.8 We wish to add that the ability for aggrieved data subjects to seek legal assistance under the PDPO should not preclude data subjects from, alternatively, being able to seek legal aid from the Legal Aid Department in proceedings against data users, since we do not anticipate that legal assistance under the PDPO would be granted in the majority of cases.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

4.9 Proposal No. 6 considers whether the PCPD should be given the power, after the conclusion of an investigation, to determine the amount of compensation payable to an aggrieved data subject through a process of mediation. We are concerned that this may lead to confusion as to the PCPD's role in an investigation. It is also unclear how this proposal would be implemented. We highlight below some of our concerns:

(a) The purpose of the investigation process is to determine whether, in the PCPD's opinion, the data user has contravened a provision of the PDPO. The question of damages or compensation to the data subject is dealt with as a separate issue under the PDPO.

(b) It is not clear how the PCPD can determine the amount of compensation to be awarded to the data subject through a process of mediation. In a true mediation, the mediator adopts a neutral position and his/her role is to facilitate communication between the parties so that they themselves determine the result. A mediation where the PCPD determines the result is arguably ultimately an adjudication and not a mediation.

(c) Currently, a data user has the right of appeal against a decision of the PCPD to issue an enforcement notice. That avenue of appeal is the Administrative Appeals Board which hears appeals only in respect of administrative decisions. However, if either the data user or the data subject disagrees with an award of compensation, there is no clear avenue of appeal under the PDPO. The AAB does not review decisions on the civil damages (including damages for injury to feelings) payable to aggrieved persons. If the award is characterised as a mediated settlement, there may be no avenue of appeal at all. If the award is characterised as an adjudicated sum, consideration will need to be given to the forum and grounds for an appeal.

(d) Even if a true mediation is intended, with the parties determining the amount of compensation paid, members of the public may find the role of the PCPD confusing. In an investigation, the role of the PCPD is not to mediate between the parties. The PCPD has the power to determine whether, in its opinion, a contravention of the PDPO has occurred and, if appropriate, to issue an enforcement notice. A respondent to a complaint, which has been investigated by the PCPD and the PCPD considers that a contravention has occurred, may be uncomfortable with the PCPD also acting as a mediator on the question of damages. The PCPD should arguably not play the role of both enforcer and mediator.

4.10 Enabling the PCPD to act as mediator (not adjudicator) on the question of damages may also be inconsistent with the PCPD's proposed power to grant legal assistance to aggrieved parties. Where, for example, a mediation fails and a sum cannot be agreed upon, it would be incongruous for the PCPD to step out of its neutral mediator shoes and to adopt a partisan position by granting legal assistance to one of the parties.

5. Offences and Sanctions

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

5.1 Proposal No. 7 invites comments on whether a contravention of a DPP should be an offence. Currently, contravention of a DPP is not an offence. A breach of a DPP is remedied by the issuing of an enforcement notice by the PCPD. Breach of the enforcement notice is an offence.

5.2 Proposal No. 7 was not put forward in the Information Paper, nor does it appear to be supported by the CMAB. However, the Consultation Document notes that it is considered in response to a series of recent personal data leakage incidents which raised questions as to whether existing sanctions in the PDPO are sufficient.

5.3 The Consultation Document notes that the current provisions of the PDPO are in line with international jurisprudence governing personal data privacy legislation. It is also noted that there is a need to strike a careful balance between the protection of personal data and other competing rights and interests such as freedom of information and the civil liberty of individuals. Any proposed new offences should be circumscribed so that unintended activities are not caught within an offence with an unnecessarily wide scope.

5.4 We agree with the comments in the Consultation Document and do not support making contravention of the DPPs an offence.

5.5 The DPPs are cast in generic terms and are therefore subject to a wide range of interpretations. The risk of inadvertently offending is therefore unacceptably high. Accordingly, it is not appropriate to criminalise a contravention of the DPPs.. In addition, Proposal No. 7 cuts across the original intent of the DPPs which was to provide guidance to data users rather than specific procedures to be followed.

5.6 We further agree with the statements in the Consultation Document that it is more appropriate to adopt a selective approach and single out specific acts or practices as offences, consistent with the current structure of the PDPO.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

5.7 Proposal No. 8 seeks comments on whether an offence should be created for a person who discloses, for profits or malicious purposes, personal data obtained from a data user without the data user's consent. In addition, comments are sought on the need for defence provisions and the appropriate level of penalty.

5.8 We understand this proposal is also put forward in response to public concern regarding leakages of personal data and, in particular, the unauthorised use of personal data causing damage to data subjects including:

(a) unauthorised access and collection of personal data for sale to third parties for profit; and

(b) unauthorised disclosure of patient's sensitive data, particularly health records, to third parties.

5.9 Currently, the unauthorised use of data in this manner is a breach of DPP 3 and contravention is not an offence. This is in contrast to the position in the UK, for example, where it is an offence to knowingly or recklessly, without the consent of the

data controller, obtain or disclose personal data or procure the disclosure, subject to certain defences, or to sell or offer to sell the obtained personal data.

5.10 We agree that the creation of an offence for personal data that is misused in this way is an appropriate attempt to deter blatant intrusions on privacy and contraventions of the PDPO. However, in our view the wording of the offence should be more closely based on the UK offence, in particular that it should be an offence to knowingly or recklessly disclose.

5.11 It appears that the CMAB's proposed narrowing of the UK definition, to refer to disclosure for profits or malicious purposes, is to address the concern that normal or innocuous activities may be caught by the provision. However, in our view, this risk is mitigated by creating a two-level approach to the offence such that it is an offence to either:

(a) obtain or disclose or procure the disclosure of personal data knowingly or recklessly and without the consent of the data controller, unless a defence applies; or

(b) sell or offer to sell the personal data so obtained.

5.12 We recommend the defences should mirror the UK defences; however, a "reasonable belief" standard should apply to each defence. Following this approach, it would be a defence to the act of knowingly or recklessly obtaining or disclosing or procuring the disclosure of personal data where:

(a) the person acted in the reasonable belief that it was necessary for preventing or detecting a crime;

(b) the person acted in the reasonable belief that he/she was required or authorised by any enactment, rule of law or order of a Court;

(c) the person acted in the reasonable belief that he/she had, in law, the right to obtain, disclose or procure the disclosure;

(d) the person acted in the reasonable belief that he/she would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring or such disclosure;

(e) the person acted in the reasonable belief that, in the particular circumstances, the obtaining, disclosing or procuring such disclosure was justified as being in the public interest; or

(f) the person acted with a view to the publication by any person of any journalistic, literary or artistic material and in the reasonable belief that such act was justified as being the public interest.

5.13 In our view, there should be no requirement for a defendant to prove the defences, only to prove that they held the relevant belief and it was reasonable to hold such belief.

5.14 Adopting a definition closer to the UK definition, with the defences applicable to the first limb of the offence, achieves the aim of not catching unintentional or innocuous acts and removes the difficulty of proving that the defendant acted for "malicious purposes". Moreover, the second limb of the offence, catches the blatant act of

making a profit from personal data obtained in such a knowing or reckless way and there are no defences which apply to such act.

5.15 With respect to the appropriate level of penalty, we agree that the penalty level should be increased in order to impose the desired deterrent effect and that a fine commensurate with the gravity of the misdeed would be appropriate.

5.16 While the penalty level should be increased, it is our view that the actual level of penalty should be left to the discretion of the magistrate, rather than a fixed schedule of penalties. However, guidance should be given in the PDPO as to the factors that should be taken into account in fixing a penalty, such factors to include:

(a) the type and amount of data involved;

(b) the extent of disclosure;

(c) whether the data was obtained and/or disclosed with malice (although malice need not be proved);

(d) whether the data was disclosed for profit and the extent of the profit; and

(e) whether the data was sensitive data or not.

5.17 If Proposal No. 1 regarding sensitive personal data is adopted, a two-tier penalty regime may be appropriate. The penalties should be increased to Level 5 for all offences, and for those involving sensitive personal data, the available penalties should increase.

5.18 Where a defendant has disclosed the personal data for profit, the disgorgement of profits may be an appropriate remedy to be made available to the Court in certain cases. By requiring the profit from such offence to be paid back, the incentive to profit from disclosure of data in this way is reduced. While the number of data subjects who may be entitled to be paid by the offender may be large, depending on the data disclosed, there is a precedent for dealing with such penalties. For example, such a penalty may currently be imposed in relation to insider dealing offences.

Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts

5.19 Proposal No. 9 invites comments on:

(a) whether it is appropriate to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice; and

(b) if so, the appropriate penalty level for the offence, bearing in mind that non-compliance with an enforcement notices is subject to a fine of HK$50,000 and to imprisonment for two years.

5.20 In our view, there is no compelling reason to introduce a new offence of this nature.

5.21 We note that the current regime means the PCPD has no option other than to issue another enforcement notice if a data user intentionally and repeatedly contravenes a DPP on the same facts, having complied with an enforcement notice. However, given there have been no cases of data users repeatedly contravening the DPPs in this

manner since the enactment of the PDPO, it does not appear to be an issue which requires additional penalties to be imposed.

5.22 Should the CMAB still consider this to be an issue which requires addressing, we recommend that:

(a) it is clearly set out in the relevant provision what is meant by "same act" or "same practice". Given the DPPs are broadly drafted, there is a need to ensure that any such offence would not catch unintentional breaches of the DPPs where the data user is otherwise complying with the enforcement notice; and

(b) such offence should be limited to situations where the data user is acting knowingly or recklessly in intentionally doing the same act. "Intentionally" is a term open to interpretation and the offence should not be unduly wide in its interpretation.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

5.23 Proposal No.10 is concerned with whether monetary penalties should be imposed by the PCPD for serious contraventions of the DPPs.

5.24 The Consultation Document notes that in the UK there is an amendment to the UK Data Protection Act that is not yet in force, which allows the UK Information Commissioner to serve a data controller with a monetary penalty notice for (a) a serious contravention of the data protection principles; (b) which is likely to cause substantial damage or distress and; (c) where the data controller knows or ought to have known a risk of contravention of a kind likely to cause substantial damage or distress but failed to take reasonable steps to prevent the contravention.

5.25 In Hong Kong, it is noted that it is not common for non-judicial bodies to have a statutory power to impose monetary penalties. Where they do, it is in relation to fixed penalty schemes (such as those which authorise public officers to impose penalties for traffic offences, smoking and other public acts) or clearly defined offences (such as those specified in the UEMO for failure to comply with a direction issued by the Telecommunications Authority).

5.26 We do not support the introduction of monetary penalties for serious breaches of the DPPs. In our view, there is a risk that such a penalty would create an arbitrary hierarchy of DPPs between serious breaches and non-serious breaches and it is a matter of subjective judgment as to what constitutes a "serious" breach. In addition, the DPPs are generic in nature and are not a suitable basis upon which to create monetary penalty sanctions, for the reasons given in response to Proposal No. 7.

5.27 We agree with the Consultation Document that it is more appropriate to single out particular acts or practices as offences.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

5.28 Currently there are no heavier sanctions in the PDPO for repeated contraventions of an enforcement notice. Proposal No.11 invites comments on:

(a) whether heavier penalties should be imposed for a second or subsequent contravention of an enforcement notice, in breach of Section 64(7) of the PDPO; and

(b) if yes, the appropriate penalty level, bearing in mind that the existing penalty level for contravention of an enforcement notice is a fine at Level 5 (up to HK$50,000) and imprisonment for up to two years, along with a daily fine of HK$1,000 for a continuing offence.

5.29 We agree with the principle set out in Proposal No.11, that it is consistent with other pieces of legislation to impose a heavier penalty for repeated offences.

5.30 While no data user has been prosecuted more than once for contravention of an enforcement notice, in our view it is still appropriate to introduce heavier penalties for repeated contraventions as part of the broader review of the PDPO. However, the further contravention must be sufficiently similar with the terms of, or the offence referred to in, the enforcement notice.

5.31 We support a penalty regime consistent with the UEMO, where a data user who commits a second or subsequent offence as set out in the enforcement notice is liable to a fine of HK$500,000 and a further daily fine of HK$1,000 for each day the offence continues. We also support a similar provision to the UEMO that provides the data user with a defence if he/she can prove that he/she exercised all due diligence to comply with the enforcement notice.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

5.32 Section 34 of the PDPO regulates the use of personal data in the carrying out of direct marketing activities. Section 34(1)(ii) prohibits a data user from using any personal data for the purpose of carrying out direct marketing activities if the individual who is the subject of the data, has previously requested the data user to cease to use his/her personal data. Contravention of this section without reasonable excuse is an offence, punishable by a fine of up to HK$10,000.

5.33 Proposal No.12 invites comments on whether the penalty for misuse of personal data in direct marketing should be raised and on the appropriate level of penalty.

5.34 While we do not object to the principle behind this proposal, we query whether raising the penalty is the best approach. Under the current regime, the DOJ may issue a separate summons for each offence and the Court has the flexibility to impose the current penalty in relation to each offence. Given, in most cases, that the conduct that will be the subject of such proceedings will be on a large scale, rather than a single instance of misuse of data, the aggregation of such penalties could be very high.

5.35 In our view, approaching the issue in this way is a better approach. Increasing the penalty may impose too high a risk for legitimate marketing activities to be carried out and frustrate the creation of new economic activity.

6. Summary of Proposals for Comments

Annex 1: Other Proposals : Invitation for Comments

(A) Rights of Data Subjects

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

6.1 Proposal No. 13 intends to give the right to a "relevant person" (as defined in the PDPO) to consent to the change of use on behalf of a data subject who does not have capacity to give consent. Such data subjects would include minors and those incapable of managing their own affairs (i.e. due to mental incapacity).

6.2 The proposal is that "prescribed consent" (as defined in the PDPO) can be given by a relevant person where the data subject does not have sufficient intelligence or comprehension to understand the proposed change of use and the proposed use has a clear benefit to the data subject.

6.3 In principle, we have no objection to this proposal, subject to the following comments:

(a) the proposal seems to create an anomaly in the law, as consent or guidance of relevant persons is not required to ensure that minors and those incapable of managing their own affairs are capable of understanding a Personal Information Collection statement at the time of collection of their personal data; and

(b) guidance should be given as to what is meant by a "clear benefit" for the data subject. Similarly, prescribed consent should also be required where the use of data may be to the detriment of the data subject such as the situation in Example 1 in Proposal No. 5 of the Information Paper.

6.4 Views are also invited on whether the definition of "relevant person" should be expanded to cover the situation described in paragraph 6 of Annex 1 of the Consultation Document where the minor is in the care of relatives or child care placement. If these parties are assuming "parental responsibility" for the minor, then they should fall within the definition of "relevant person". For clarity, the definition of "relevant person" could be expanded to include the data subject's legal guardian.

Proposal No. 14: Parents' Right to Access Personal Data of Minors

6.5 Proposal No. 14 seeks to provide a data user with the right to refuse a data access request made by a "relevant person" on behalf of a minor, when such a refusal is to protect the interests of the child. Examples of circumstances where a data access request may be refused include situations where:

(a) an estranged parent is seeking location data regarding a child;

(b) the parent is suspected of child abuse; or

(c) the child has requested his or her data not be disclosed.

6.6 Views are invited on whether such a right of refusal should be introduced. In principle, we have no objection to the introduction of a right for a data user to refuse

requests if it is in the interests of child. Additionally, such right of refusal must not imply that the data user has a duty to make such an assessment in all cases where a data access request is made on behalf of a minor. Guidance as to "reasonable grounds" would be welcomed by data users such as schools to avoid placing them in an untenable situation.

6.7 Views are also invited on whether the grounds for refusal should be expressed in general terms (i.e., "reasonable grounds to believe that compliance with the request would not be in the best interests of the child") or whether specific grounds should be stated. Two alternative proposals are set out in the Information Paper in Proposal No. 20. The latter proposal is the more general approach. We support the more general approach as this gives data users more flexibility in their determinations.

6.8 As a side note, consideration should also be given to whether a similar right of refusal should apply to data subjects with mental incapacity and to carers who are suspected of abuse.

Proposal No. 15: Access to Personal Data in Dispute

6.9 Proposal No. 15 seeks to include a provision in the PDPO that, when the refusal to comply with a data access request is in issue before the AAB or a Court , the personal data should not be disclosed to the data requestor by discovery or otherwise.

6.10 The purpose of this proposal is to close a loophole whereby a party could abuse the appeal process to obtain documents to which it is not otherwise entitled. On this basis, we have no objection to the proposal.

(B) Rights and Obligations of Data Users

Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

6.11 We agree with the proposal to permit a data user to refuse to comply with a data access request on the ground that there is a competing statutory obligation requiring the data user not to disclose the personal data.

Proposal No. 17: Erasure of Personal Data

6.12 We agree that the PDPO should be amended so that obsolete personal data are regarded as having been erased if a data user can prove that it has taken all reasonably practicable steps to erase it.

Proposal No. 18: Fee Charging for Handling Data Access Requests

6.13 Given the uncertainty of both data users and data subjects as to the appropriate fees for complying with data access requests, we consider it prudent to prescribe a fee schedule for certain types of documents when complying with data access requests under the PDPO; for example, for photocopies, DVDs, CDs, etc. However, we recommend a proviso which permits a data user to charge higher fees where it can demonstrate that its reasonably incurred out-of-pocket expenses are greater than those set out in the schedule. This may, for example, be necessary if the prescribed fee schedule is out-of-date or no longer reflects the actual cost of certain media.

6.14 The Consultation Document suggests that a fee schedule be published in the PDPO. An alternative is to grant the PCPD the power under the PDPO to publish a fee schedule which may be amended from time to time. This obviates the need to amend the legislation each time the schedule is to be amended or updated.

6.15 The fee schedule should, however, be limited to prescribing fees for common types of media. It should not prescribe limits for processing costs. Some data access requests require a data user to retrieve files going back many years, to physically review those files and to redact unrelated data or the personal data of other data subjects. Many data subjects do not appreciate the time spent on processing their requests. The ability to charge reasonable processing fees not only ensures that data users do not suffer too much of a detriment by complying with the PDPO, but assists in reducing the number of unreasonable or oppressive data access requests.

Proposal No. 19: Response to Data Access Requests in Writing and Within 40 Days

6.16 We agree with the proposal to amend the PDPO to require a data user to inform a data subject in writing within 40 days that it does not hold the requested personal data of the data subject. We also agree with the proposed exemption permitting the police to inform a data subject orally within 40 days that he or she has a clear criminal record.

(C) Enforcement Powers of the PCPD

Proposal No. 20: Circumstances for Issue of an Enforcement Notice

6.17 At present, the PCPD is empowered to issue an enforcement notice where the act of contravention is continuing or where a contravention has occurred and is likely to continue or be repeated. However, in deciding whether to serve an enforcement notice, the PCPD must also consider whether the contravention has caused or is likely to cause damage or distress to the data subject. According to the Consultation Document, as well as the PCPD's interpretation of Section 50 of the PDPO as illustrated in the Information Paper, if the contravening act or practice has ceased and there is no likelihood that it will be repeated, the PCPD is unable to issue an enforcement notice even if the act has caused harm or damage to a data subject.

6.18 It is our understanding that the PCPD wishes to have the power to issue an enforcement notice where damage or distress has been caused to a data subject, regardless of whether the contravention has ceased or is likely to be repeated. The Consultation Document does not indicate what the enforcement notice would state in a situation where the contravention has ceased, since there would be nothing to enforce. An enforcement notice normally sets out the remedial action to be taken by the data user. Where appropriate remedial action has been taken, it is not necessary to issue an enforcement notice.

6.19 If the intention is that the PCPD would be permitted in the enforcement notice to require the data user not to repeat the same activity, we agree with this proposal, provided that the prohibited activity is clearly defined. The enforcement notice should not be drafted too widely to cover activities which extend beyond the contravention which has occurred.

6.20 The Information Paper states that the issuance of an enforcement notice has a deterrent effect. We agree. However, we consider that it is not the fact of an enforcement notice having already been issued that deters a data user from continuing to contravene the PDPO, but it is the threat of an enforcement notice that has this effect. In our experience, when data users are being investigated by the PCPD, this gives them the opportunity to examine their practices and policies and to take appropriate action to remedy any contravention, to the satisfaction of the PCPD. The purpose of doing this is to avoid the issue of an enforcement notice. The fact that an enforcement notice can be avoided through their own positive behaviour therefore gives an incentive to data users to modify and continue to monitor their practices to ensure compliance with the PDPO.

6.21 However, if an enforcement notice can be issued once a contravention has been found to have occurred, regardless of any remedial action taken by the data user, the message is sent that data users are simply penalised for errant behaviour. There is no reward as such for having made the effort to remedy their practices (which often arises from ignorance or a misunderstanding of their obligations) and hence the incentive is removed for making such efforts. A data user may, in such a case, simply wait for the enforcement notice to be issued before taking any remedial action. This diminishes the educational value and effect of the enforcement notice and imposes a different regime of strict liability, enforcement and penalties.

6.22 The relevance of damage or distress to a data subject in deciding whether to issue an enforcement notice is not clear under Section 50(2) of the PDPO. The section does not state that an enforcement notice cannot be issued where no damage or distress has been caused to a data subject. Amendments to Section 50(2) would help to clarify this.

6.23 Because Section 50 is ambiguously drafted and because the Consultation Document does not explain in detail the meaning of the proposed amendments, it is not clear to us what is being proposed. For example, it is not clear whether the proposal is that the PCPD will be empowered to issue an enforcement notice where a contravention of the PDPO has occurred but has ceased, is continuing or may be repeated, but where a data subject has suffered *no* damage or distress. This needs to be clarified to avoid uncertainty.

6.24 The Consultation Document does not specify the proposed wording of any amendment to Section 50 of the PDPO. We note from the Information Paper that the PCPD proposes to amend the wording of Section 50 so that the PCPD need only have *"due regard"* to whether a contravention is continuing, or will continue or be repeated, or whether the data user has caused or is likely to cause harm to the data subject. We take the view that the PCPD must be confined to issuing enforcement notices in specified circumstances. To provide the PCPD with the discretion only to have "due regard" to a variety of circumstances is likely to create uncertainty and disagreement as to the proper application of the section and this may result in an increased number of appeals to the AAB.

Proposal No. 21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

6.25 We agree that the PCPD should be empowered to state in an enforcement notice that the data user is required to cease and desist from doing or continuing an act or engaging in a practice which the PCPD has found to be in contravention of the PDPO.

Proposal No. 22: Removing the Time Limit to Discontinue an Investigation

6.26 We agree with the proposal to remove the current time limit imposed on the PCPD to inform a complainant of its decision not to investigate a complaint or to discontinue an investigation into a complaint. We note that the EOC is not subject to any time restriction for informing a complainant of such a decision. We agree that the decision and reasons for the decision must continue to be provided to the complainant in writing.

Proposal No. 23: Additional Grounds for Refusing to Investigate

6.27 We agree in principle to the inclusion in Section 39(2) of the PDPO of further specified grounds on which the PCPD may refuse to investigate, or continue to investigate, a complaint. This may assist in providing more clarity and minimising unmeritorious complaints being lodged with the PCPD. However, we do not agree with the proposed additional grounds for refusing to investigate a complaint, i.e.:

(a) Where the primary cause of the complaint is not related to personal data privacy;

(b) Where the complaint relates to an action for which the complainant has a remedy in any Court or Tribunal, or which is currently or soon to be under investigation by another regulatory body; or

(c) Where the act or practice specified in a complaint relates to personal data or documents containing personal data which have been or will likely be used at any stage in legal proceedings or an inquiry.

We respond below to each of the above grounds.

Ground (a)

6.28 In the Information Paper, the PCPD has provided examples of situations where it considers that the primary reason for the relevant complaint does not relate to personal data privacy. We can envisage situations where it may not be clear cut as to whether a complaint is predicated primarily on data privacy issues or other issues. The data subject may have a number of very valid concerns resulting from actions taken by the data user. The exercise of this ground may involve the PCPD putting itself in the shoes of the complainant to decide what the primary basis for the complaint is. It would be wrong for a complainant to have to justify to the PCPD that his or her complaint is genuinely based on data privacy concerns.

6.29 In addition, data privacy issues may be a secondary but still very valid concern. If a contravention of the PDPO has clearly occurred, but this is linked with a much more serious complaint by a data subject against the data user, we do not see why the data subject should be precluded from seeking the PCPD's assistance in investigating and restraining the activity prohibited by the PDPO.

Ground (b)

6.30 We do not agree that data subjects should be precluded from pursuing their rights under the PDPO merely because a remedy is available to them in Court or Tribunal proceedings or as a result of an investigation by another regulatory body.

6.31 Where data subjects have suffered loss as a result of a contravention of the PDPO, and they wish to claim civil damages under Section 66 of the PDPO, a decision in their favour from the PCPD may assist them in demonstrating their entitlement to damages. They should not therefore be deprived of the ability to have their complaint to the PCPD investigated merely because there are alternative remedies available to them. In addition, these alternative remedies are unlikely to include damages for injury to feelings which are available under Section 66(1) of the PDPO.

Ground (c)

6.32 If the act or practice specified in a complaint is that the data user has failed to properly comply with a data access request, the fact that documents containing the personal data are being, or are likely be, used in legal proceedings or in an inquiry should not preclude the data subject from having his/her complaint investigated.

6.33 The proposed amendment assumes that all data users fully comply with all their discovery obligations in legal proceedings without data subjects having to apply for specific discovery or further and better discovery, procedures which can be a drain on financial resources. Data subjects should be entitled to obtain copies of documents containing their personal data through the less costly route of data access requests under the PDPO if they consider it appropriate to do so.

(D) Introducing New Exemptions

Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

6.34 Proposal No. 24 intends to exempt personal data provided in the context of a merger or acquisition from DPP3. This is because there is often a genuine need to disclose personal data as part of a transaction but it may not be practical to obtain consent from data subjects for reasons such as time or deal sensitivity.

6.35 In general, we are in favour of this exemption being added to the PDPO. However, we are of the view that some of the conditions suggested in paragraph 52 of the Consultation Document in relation to the exemption are too restrictive. In particular, we have concerns with the following conditions:

(a) 52(b) – that the exemption will apply where it is "not practicable" to obtain consent. This introduces a subjective element to the exemption. We are of the view that consent should not be required at all for this exemption as the other conditions provide adequate protection for this limited purpose. As such, the condition should not be included.

(b) 52(c) – the data are necessary but not excessive for the due diligence purpose. Again, this introduces a very subjective element into what can be disclosed. We do not consider this to be a workable condition because information which is not "necessary" in one party's mind may be considered necessary in another's. This condition may be burdensome for sellers by requiring them to go through data and determine what is "necessary".

(c) 52(d) – this condition should restrict use of the data for the purpose of effecting a merger, acquisition or transfer of business. To restrict use only for the purpose of due diligence further narrows the scope of the exemption.

(d) 52(e) – if disclosures can be made to legal or other advisors (see below), then any obligation to return/destroy should be subject to any professional/legal obligation to retain the data.

6.36 Our view is that the exemption should apply not only to parties to the transaction but also their legal, financial and other advisors.

Proposal No. 25: Provision of Identity and Location Data on Health Grounds

6.37 Proposal No. 25 would allow for the disclosure of location or identity data of a data subject where it is required for health purposes. This could be done by way of an additional exemption in Section 59 of the PDPO. We have no objection to this proposal.

Proposal No. 26: Handling Personal Data in Emergency Situations

6.38 Proposal No. 26 would allow for personal data to be handled in emergency situations where immediate assistance is required. It would provide an exemption from DPP 1(3) (collection) and DPP 3 (use). We have no objection to this proposal.

Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

6.39 Proposal No. 27 would allow a data user to transfer the personal data of a minor to the parent or guardian where the data user considers the transfer will benefit the minor. Examples given are where the minor is using drugs or is likely to commit a crime.

6.40 We note that this proposal was not included in the PCPD's original amendment proposals made in 2006.

6.41 We do not support this proposal as we do not find that there is any basis for it. It infringes greatly on the personal data rights of minors given the lack of definition of the circumstances in which their personal data could be transferred. There are specific exemptions in the PDPO (or proposed in the Consultation Document) which allow for personal data to be used in limited circumstances outside the original purpose for which it was collected. These should be adequate to cover specific circumstances where data needs to be transferred to the parents or guardians. Parents or guardians have the right to access their children's personal data should they have any specific concerns. The proposal also puts certain data users (such as schools) in a difficult position because they may not be able to make an accurate assessment in respect of every minor data subject, which could lead to (a) errors; and (b) inconsistent treatment amongst (for example) students.

Annex 2: Proposals not to be Pursued

(A) Scope of Regulation under the PDPO

A.1: Revamping Regulatory Regime of Direct Marketing

6.42 This proposal considered revamping the regulatory regime of direct marketing (as set out in Section 34 of the PDPO) including introducing the following:

(a) obtaining the data subject's explicit consent to use his data for direct marketing ("opt-in"); and

(b) setting up a "do-not-call" register against direct marketing activities.

6.43 The UEMO was introduced in 2007 with respect to direct marketing via electronic messages. The UEMO sets out a number of rules for sending electronic messages and provides for do-not-call registers (maintained by OFTA for SMS, fax and pre-recorded messages. The UEMO does not regulate person-to-person direct marketing.

6.44 The proposal considers an "opt-in" regime whereby data users would need to consent to use of their personal data for direct marketing. The UEMO, however, is an "opt-out" regime. We believe that the introduction of an opt-in regime in the PDPO will conflict with the opt-out regime in the UEMO. In addition, an opt-in regime will create a greater burden for businesses in undertaking direct marketing activities, which are often vital to their operations. We consider that the introduction of an opt-in regime for some direct marketing while there is an opt-out regime for electronic messages will be confusing and difficult to understand.

6.45 The introduction of a do-not-call register "against direct marketing activities" would be difficult to administer and enforce. Any do-not-call register should be with respect to a specific means of communication, like those currently set up under the UEMO. Also, splitting the administration of do-not-call registers between regulatory authorities may lead to confusion for both data subjects and data users. We consider that the introduction of further do-not-call registers should be considered together with OFTA and in the context of the UEMO.

6.46 We agree that this proposal should not be pursued.

A.2: Internet Protocol Address as Personal Data

6.47 This proposal considers whether an Internet Protocol address ("IP address") by itself should constitute personal data.

6.48 As correctly set out in the Consultation Document, an IP address is a number which identifies an electronic device and allows the device to communicate with other devices. Combined with other information (such as a telephone number or user name), it may identify an individual. In this case, it would be considered personal data and fall within the current scope of the PDPO.

6.49 However, as the IP address alone identifies the device rather than the user or users, we agree that it does not constitute personal data and the proposal should not be pursued.

A.3: Territorial Scope of the PDPO

6.50 This proposal considers whether the PDPO should apply where none of the acts of the data processing cycle takes place in Hong Kong. Although practical from an enforcement perspective, there is a risk that exempting data users in such circumstances will create a loophole where a person in Hong Kong can by-pass the PDPO simply by arranging for offshore collection and outsourcing the holding, processing and use of data. The CMAB is not inclined to follow this proposal.

6.51 We consider the proposal to be practical and workable provided that certain safeguards are put in place to avoid the potential loophole identified by the CMAB. The exemption can be stated not to apply where, for example, the offshore collection or use of the data can be shown to be done under the direction or control of a Hong Kong data user.

(B) Exemptions

B.1: Public Interest Determination

6.52 This proposal considers whether the PCPD should be empowered to make public interest determinations with regard to the disclosure of personal data without the consent of the data subject.

6.53 In the Information Paper, the PCPD has set out a number of international examples but prefers the Australian approach. This approach empowers the Privacy Commissioner in Australia to exempt an act that would otherwise infringe a privacy principle after balancing the interest in doing the act against adherence to the relevant principles. The Privacy Commissioner also has the power to issue temporary determinations in an emergency or urgent situation.

6.54 We do not object to this proposal as it seems that such determinations will be made by the Privacy Commissioner only on a case by case basis after weighing up the public interest against privacy protection. We do not agree with the position in the Consultation Document that the mechanism will undermine the certainty afforded to data subjects. We would assume that the power would not be used lightly but only in the case of genuine public interest. We believe that this proposal should be pursued as per Proposal No. 33 in the Information Paper.

B.2: Public Domain Exemption

6.55 This proposal considers a new exemption to DPP 3 (use of personal data) for data available in the public domain.

6.56 We agree with the position in the Consultation Document that this proposal should not be pursued. A great deal of personal data is in the public domain, not only in public registers but also on the Internet. In fact, in many cases, personal data on the Internet is posted without the data subject's knowledge or consent. The mere fact that data are in the public domain should not put it outside the rules for using, handling, processing and storing data set out in the PDPO.

6.57 We agree that this exemption may lead to the abuse of personal data, particularly in the course of direct marketing, and should not be pursued.

(C) Powers of the PCPD

C.1: Power to Search and Seize Evidence

6.58 We do not agree with the proposal to give the PCPD the power to search for and seize evidence without the data user's prior consent, particularly given that the reason for this proposal is to enable the PCPD to prosecute data users. Since we object to the proposal to grant to the PCPD powers of prosecution, the power to search for and seize evidence is unnecessary.

C.2: Power to Call upon Public Officers for Assistance

6.59 We agree with the proposal to provide the PCPD with an express power to call upon public officers to assist in the performance of its functions under the PDPO. The Consultation Document suggests that Section 64(9) of the PDPO already provides this power to the PCPD. However, Section 64(9) does not confer a positive power on the PCPD to request assistance from public officers. It merely makes it an offence for a person to obstruct or fail to cooperate with the PCPD and is principally aimed at data subjects and witnesses. The Consultation Document also suggests that public officers *have* been providing assistance to the PCPD when a request is made. If that is correct, there is no reason why conferring an express obligation to public officers to assist the PCPD would be objectionable.

C.3: Power to Conduct Hearing in Public

6.60 We do not agree with the proposal to permit the PCPD to hold a public hearing for the purpose of an investigation, notwithstanding a request by the complainant for the hearing to be held in private. Complainants will ordinarily expect that investigations involving their personal data will be conducted privately. Most investigations do not require a hearing unless, for example, the PCPD wishes to hear oral evidence, such as where the PCPD wishes to test the truth of the evidence given. There is no compelling reason for such a hearing to be conducted in public, particularly given that potentially sensitive privacy issues may be involved. We do not therefore agree that the PCPD should be empowered to override a request by the complainant to have such a hearing held in private.

C.4: Time Limit for Responding to PCPD's Investigation/Inspection Report

6.61 We disagree with the proposal to shorten the period from 28 days to 14 days for a data user to inform the PCPD whether it objects to the disclosure in a report on an inspection or investigation of personal data which are exempt from disclosure under Part VIII of the PDPO.

6.62 For some data users, it may be necessary for the report to be circulated and discussed amongst different departments and management personnel before a response can be provided to the PCPD. There is no compelling reason to put pressure on a data user to respond within 14 days. The detriment to a data user by shortening the response period will likely outweigh any benefit to the PCPD and to the public by doing so.

Annex 3: Miscellaneous Proposed Amendments to the Personal Data (Privacy) Ordinance

6.63 In our view, the proposals in Annex 3 are generally appropriate. We have therefore confined our comments to those proposals which we believe are contentious and worthy of comment.

(A) Statutory Powers and Functions of PCPD

Proposal No. 31: Power to Impose Charges for Educational and Promotional Activities

6.64 It is proposed under Proposal No. 31 that the PCPD should be expressly empowered to impose charges for educational and promotional activities. There does not appear to be any reason put forward in support for this proposal, other than pointing out that other statutory bodies are provided with the power to charge fees.

6.65 In our view, the educational and promotional role played by the PCPD is of vital importance, particularly following legislative change. We therefore consider that charges should not be imposed. To impose fees for such a service may mean that smaller or less well-resourced organisations are placed at a disadvantage as compared to their larger counterparts and may be more exposed to legal risk simply because they have less capacity to pay.

(B) Introducing New Exemptions

Proposal No. 35: Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

6.66 Proposal No. 35 is intended to "uphold the common law principle of privilege against self-incrimination" by creating a new exemption for data users from complying with a data access request on the ground of self-incrimination. While it is appropriate to invoke this principle in respect of natural persons who are facing criminal sanctions, it is not as clear that this exemption should apply to a data user which is a body corporate. It is widely accepted that the primary rationale for the privilege against self-incrimination (e.g. protection of personal freedom and dignity) is weak when applied to an artificial entity such as a corporation. In our view, the scope of any exemption based on the ground of self-incrimination must be adequately defined; that is, it must be clear whether a corporation can rely on this exemption to refuse to comply with a data access request. Assuming that the exemption does not apply to corporations, we strongly recommend that officers of the corporation are adequately protected.

Proposal No. 36: Definition of Crime under Section 58

6.67 DPP 3 states that a data user must not use data for a purpose which is different from the purpose for which it was collected without the data subject's express voluntary consent. Currently, Section 58 exempts a data user from the requirement to obtain this consent in certain situations. One of those situations is where the personal data are needed for the prevention or detection of a crime and, if that personal data are not provided, this is likely to prejudice the prevention or detection of the crime.

6.68 The term "crime" is not currently defined under the PDPO and it is unclear whether the exemption has extra-territorial effect. For example, if an overseas enforcement agency requests information for the investigation of a crime outside Hong Kong, it is not clear from the legislation whether this exemption will apply. The issues arising

from this lack of clarity were borne out in the Yahoo! case involving the journalist Shi Tao who was imprisoned in the PRC for having leaked state secrets.

6.69 These issues appear to have prompted Proposal No. 36 which is intended to provide clarification of the meaning of the word "crime" so that a data user can invoke the exemption in disclosing personal data to an overseas law enforcement agency for investigation of a crime.

6.70 In its Information Paper, the PCPD proposed a two-pronged definition of "crime", which is broader in scope than the definition of "crime" proposed by the CMAB in the Consultation Document. The PCPD definition of "crime" appears to provide that, even if the crime is committed outside HK, if it would constitute an offence if committed in Hong Kong, then it would come within the definition of crime. However, the CMAB definition appears to limit the definition of "crime" to those crimes committed under Hong Kong law, most of which do not have extra-territorial effect.

6.71 In our view, the broader definition is preferable as the narrower definition proposed by the CMAB does not address the issues highlighted in the Yahoo! case. In other words, if "crime" is limited to those crimes committed under Hong Kong law, a data user would be placed in a position of having to decide whether to withhold personal data that may be needed for the prevention or detection of a crime or whether to disclose such information in breach of the PDPO and DPP 3. This could prove to be an impediment for multinational organisations who seek to assist in legitimate investigations.

6.72 In contrast, the second-limb of the proposed definition of "crime" is broader in the Consultation Document than in the Information Paper. In particular, the CMAB has proposed that "crime" also refer to a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation. In comparison, the PCPD has proposed that "crime" refer to an act or omission for which legal assistance under the Mutual Legal Assistance in Criminal Matters Ordinance ("MLA") has been sought and obtained.

6.73 The proposal in the Consultation Document is arguably wider than the PCPD's proposal which only refers to assistance under the MLA, so it permits other forms of "legal or law enforcement cooperation". It is not clear what "legal or law enforcement cooperation" means, and it would be useful to obtain clarification on whether that could include requests by entities which are not law enforcement agencies for information to assist in the investigation of crimes.

(C) Clarifying the Application of the PDPO in Certain Circumstances

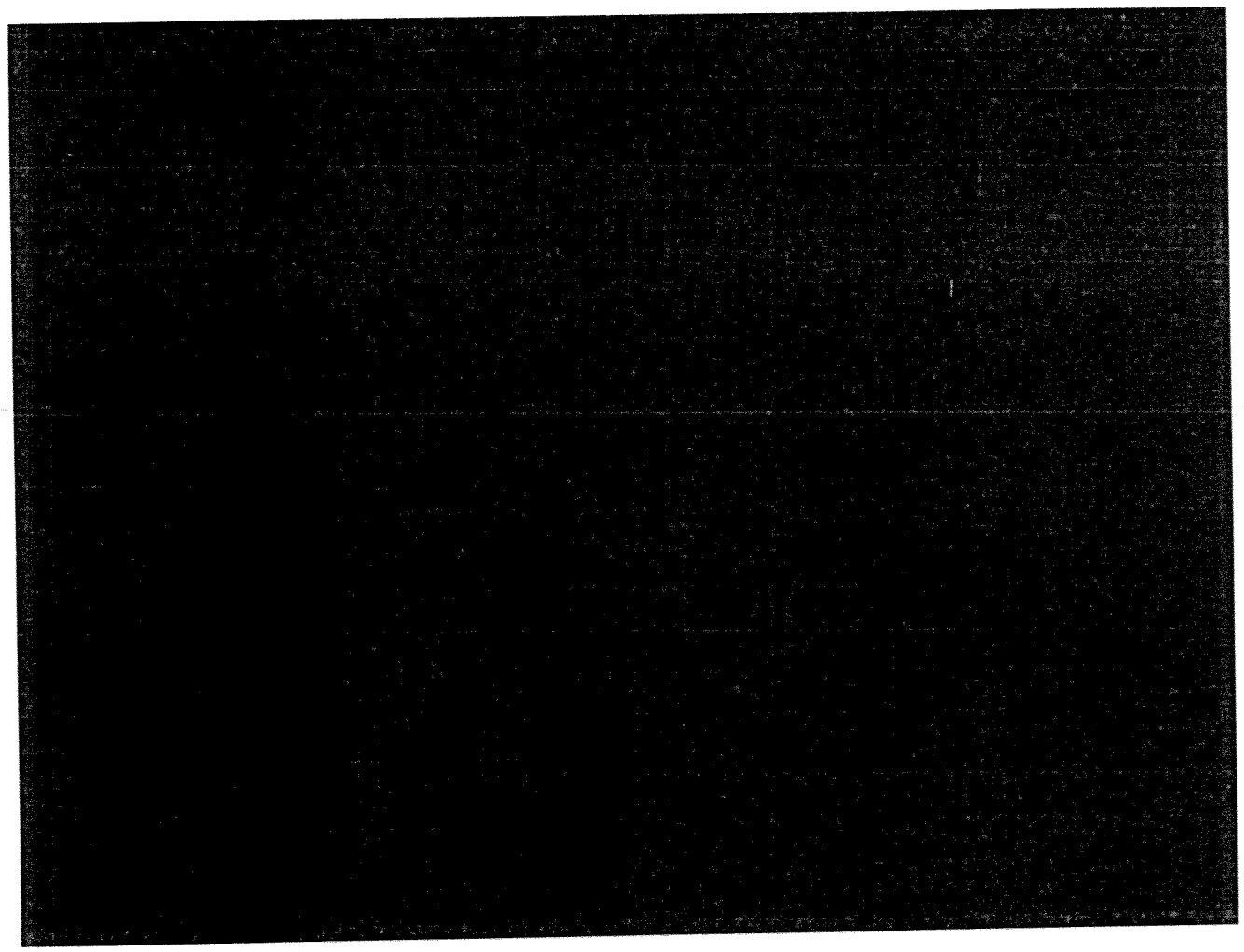
Proposal No. 40: Extend Time Limit for Laying Information for Prosecution

6.74 The current statutory time limit for laying an information to prosecute an offence under the PDPO is six months from the commission of the offence. The Consultation Document proposes that the time limit for laying informations for prosecution of an offence under the PDPO should be extended to two years from the date of commission of the offence.

6.75 While the PCPD considers that this timeframe is too tight given the number of agencies involved, in our view, this does not serve as sufficient justification for extending the limitation period. The current statutory time limit safeguards data users against the possibility of prejudice from excessive delays. We also consider that the passage of time will weaken the justification for a criminal prosecution in these circumstances.

Baker & McKenzie

30 November 2009



Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

©2009 Baker & McKenzie
All rights reserved.

明光社

《個人資料(私隱)條例》檢討
明光社意見書

政府現正就《個人資料(私隱)條例》進行全面檢討，諮詢公眾意見，市民可於 2009 年 11 月 30 日前將意見提交政府。[1]本社關注諮詢文件第(14)項(父母親查閱未成年人士個人資料的權利)中的建議，在下列三項情況中，資料使用者應否向兒童的父母提供該兒童的個人資料，包括：

a)) 有關資料可能被已離婚但不擁有該兒童監護權的一方濫用
b) 父親或母親懷疑虐待子女；以及
c) 子女向資料使用者表明，不同意該使用者向其父母透露個人資料

對於 a 及 b ，爲了充分保障兒童的權益及安全，拒絕向父親或母親透露兒童的資料是可以理解的。但 c 的情況就非常令人憂慮，有兩個問題值得思考：
一) 年齡，應容許那個歲數的兒童擁有這個自決權？即可以拒絕父母查閱他的個人資料，不論設定的年齡是 13、14、15...，都會有爭議，何不繼續現有的做法，到子女年齡達 18 歲成年時，才可擁有這自決權；
二) 誰最有資格爲兒童做決定？是社工、醫護人員、教師、警方，還是政府？他們的決定一定比父母的決定更符合兒童的最大利益嗎？

此外，有關做法亦可能令現有多條法例不能執行，根據《警察通例》(第 34 章)〈婦孺〉，提及當警方發現一名被遺棄或虐待的未滿 16 歲人士時，警方須根據《保護兒童及少年條例》(第 213 章)第 34 條向少年法庭提出申請。並

1) 須通知該名少年的父母或監護人在審訊日期和時間出庭。
2) 如須由法醫科進行身體檢查，警方須安排其家長或監護人在場，除非該家長乃案件所涉及的人物，否則，未經家長或監護人同意，法醫官不應替該名少年檢查身體[2]。

有些案件更牽涉到一些違規青少年的刑罰，如警司警誡[3]，當一名未滿 18 歲的少年人，因犯案而被拘捕及有足夠證據被起訴時，警方可以照一般案件處理，將少年犯人起訴交由少年法庭處理。另一種做法是由一名警司或以上職級的警務人員行使酌情權，向該名少年人施行警誡，而無須交由少年法庭審理。

[1] 政制及內地事務局網頁 www.cmab.gov.hk
[2] http://www.police.gov.hk/hkp-home/chinese/pgo/Cpgo034.pdf
[3] http://www.police.gov.hk/hkp-home/chinese/faqs/index.htm#10

案件是否適合進行警司警誡須考慮8項因素，其中2項是：
...少年犯及其父母或監護人同意接受警誡；
犯案人的家長或監護人的態度等因素；...

假如該名未成人士向警方(資料使用者)透露，拒絕家長查閱他的案件，他可能會因此失去以警司警誡方式彌補他做錯事的刑罰，大大影響該兒童的前途。

政府今次的檢討重點應集中如何保障市民的私隱及個人資料得到適當的保障，不會被第三者用作商業上的宣傳推廣用途，甚至被不法之徒作爲犯罪的工具。由於父母有親情及法律責任妥善照顧其18歲以下的子女，除個別非一般的家長外，照常理家長應會以子女的最大利益出發，爲子女的撫養、教育和健康等問題做最適當的決定，家長有實際上的需要向資料使用者取得子女的個人資料，包括成績，校內表現，校外情況，醫療報告，甚至違規行爲及犯罪記錄等等。

除非政府有非常充分及合理的理由，否則，不應無故剝奪父母查閱未成年子女個人資料的權利，而將有關權利交由一名與該未成年人士沒有關係的人士(資料使用者)或他本人，去衡量甚麼對該名未成年人士最好。因爲子女未必有足夠的知識作適當的決定，假如不幸子女做錯決定時，承擔後果的很多時不獨他/她們自己，還有他/她們的父母，並非資料使用者，這樣不但對父母非常不公平，亦未必有益於兒童的長遠福祉。

基於以上原因，本社認爲應維持現有的做法，容許家長有權查閱未成年子女的個人資料。

明光社
二零零九年十一月二十六日

CONSUMER COUNCIL

S0126

By post & email
Pdpo_consultation@cmab.gov.hk

30 November 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland and Affairs Bureau
3rd Floor, Main and East Wing
Lower Albert Road
Hong Kong

Attn: Miss Joanna C.H. Choi

Dear Miss Choi,

Re: Public Consultation on
the Review of Personal Data (Privacy) Ordinance

Thank you for your letter of 28 August 2009. Attached please find the Council's views on the captioned Ordinance for the consideration of the Bureau.

Should you have any queries, please feel free to contact me at 2856 8585 or Mr. Simon CHUI, Senior Legal Counsel, at 2856 8544.

Yours sincerely,

(Signed)

Connie LAU
Chief Executive
Consumer Council

Encl.

Public Consultation on Review of the Personal Data (Privacy) Ordinance ("PDPO")

1. The Consumer Council welcomes the opportunity to offer its comments in response to the said Consultation seeking views of the public on the review of the Personal Data (Privacy) Ordinance.

Sensitive Personal Data

2. Apart from biometric data, personal data such as identity card number, medical data, bank account number, credit card number and sex orientation are also vital information which leakage may put the data subjects at real risk of substantial loss; and therefore warrant further protection.

3. As such, while agreeing that additional requirements were needed for handling sensitive personal data, the Council is of the view that the new regulatory regime should not be merely limited to biometric information but should be extended to other types of sensitive personal data which leakage may put data subjects at real risk of substantial damage.

4. Nevertheless, new criminal offence for breach of mishandling of sensitive personal data was not required for the time being unless it was justified further by strong reasons.

5. As regards the question of when the new statutory requirements for handling sensitive personal data should take effect, the Council would prefer the "transitional period" option to the "grandfathering" option since the former would ensure that data users will meet the new requirements for all the sensitive data they possessed regardless of when these data were collected.

Data security

Data processor's obligations

6. As regards the 3 possible regulatory models set out in paragraph 4.07 of the Consultation Document, Members preferred a model imposing direct obligations on data processors to ensure security of the data entrusted to them, while also placing specific obligations on data users to ensure the security of the data transferred to the data processors they engaged.

7. The Council supports that the data processors would be required, as proposed, to "take all reasonably practicable steps to ensure the security and safeguarding of the personal data under their custody". When determining what the reasonably practicable steps were, the court has to take into account the particular circumstances of the data processors, which would include the types of data processing they engaged in. For this reason, it is not necessary to subject different categories of data processors to different obligations for the purpose of regulation.

Personal data security breach notification

8. The Council finds it necessary to have a mandatory requirement for data users to issue personal data security breach notification to the affected individuals as soon as possible after leakage of personal data for which substantial number of affected individuals or substantial loss or damage to the affected individuals is reasonably anticipated.

9. In other words, the notification should be triggered where the leakage was likely to pose a real possibility in causing serious harm or damage to the individuals. The Council would suggest that the Privacy Commissioner for Personal Data ("the Commissioner") should give clear guidelines to the data users on how the risks should be assessed.

10. It is further suggested that the notice should be served by any practical means in the circumstances.

11. The Council deems that the information to be contained in the notice as mentioned in paragraph 4.39 of the Consultation Document would be sufficient.

Enforcement Power of the Commissioner

Extension of enforcement power

12. It is an important principle that control of criminal prosecution be vested with the Department of Justice. Therefore, the Council does not support the proposed extension of enforcement power of the Commissioner as mentioned in paragraph 5.03 of the Consultation Document.

Legal Assistance to Aggrieved Data Subjects

13. The Council has reservation over the proposal of empowering the Commissioner to offer legal assistance to aggrieved data subjects for recourse to civil remedy under s.66 of PDPO. If there was really such a need to give legal assistance to aggrieved data subjects, the Administration should explore the possibility of extending Legal Aid to s.66, rather than creating an anomaly by giving the Commissioner the power to grant legal assistance.

Offences and sanctions

Whether contravention of a Data Protection Principle ("DDP") should be made an offence

14. There appears no evidence justifying a change from the existing

"rectification approach" in the form of enforcement notice mechanism to the proposed punitive approach of making contravention of a DPP an offence. Therefore the Council does not support the proposed criminalization measure against contravention of a DPP.

Unauthorized obtaining, disclosure and sale of personal data an offence

15. Nowadays data were so often transmitted through or downloaded from the internet. If unauthorized obtaining and disclosure of personal data are made an offence as proposed, it would be easy for people to break the law unknowingly. The Council is not shown any evidence that the current situation regarding unauthorized obtaining and disclosure of personal data should warrant such draconian sanction. Therefore the Council has reservation over making unauthorized obtaining and disclosure an offence.

16. However, sale of personal data is made for the purpose of monetary gains and must be a deliberate act. For this reason, the Council opines that it should be made an offence for a person who knowingly sold personal data without the consent of the data user.

Repeated contravention of a DPP on same facts

17. As there is no evidence that repeated contravention has become an issue, the Council does not support the proposal of making it an offence for lack of justification for such a need.

Imposing monetary penalty on serious contravention of DPPs

18. Nor does the Council support the proposed empowerment of the Commissioner to impose monetary penalty on serious contraventions of DPPs. Instead, the Council is of the view that the Government should consider singling out particular acts or practices of contravention DPPs of a serious nature and making them an offence. And, for the sake of clarity, a clear definition of "serious contravention" should be given.

Repeated non-compliance with enforcement notice

19. The Council opines that there is no need to impose heavier penalty for repeated non-compliance with an enforcement notice. Such conduct could be defined as the act or practice of serious nature that would attract criminal sanction as proposed; and the court might take into account repeated non-compliance when sentencing.

Direct marketing

20. Regarding the issue of misuse of personal data in direct marketing, the Council fully appreciates the nuisances caused by unsolicited direct marketing and re-iterates that the "opt-in" approach should be adopted to address the problem. But if the "opt-out" approach remains, the

existing penalty of $10,000 will be inadequate.

Third party to give prescribed consent to change of use of personal data

21. The Council opines that if the existing law has already allowed a relevant person to access or correct the data on behalf of the data subject, there is no reason for disallowing him/her to change on behalf of the data subject the use of the data subject's personal data.

22. Furthermore, the Council supports the proposal that specified relevant persons should be empowered to give consent to the change of use of personal data on behalf of vulnerable classes of data subjects, such as minors and mental disabled. But they have to demonstrate that the consent is so given for the benefit of the data subjects concerned.

23. As to the definition of "relevant person", the Council agrees that certain classes of person should be added to the definition if it can be demonstrated that it is done for the benefit of the data subjects concerned.

Parents' right to access personal data of minors

24. The Council supports the proposal that a data user should be permitted to refuse a data access request made by a "relevant person" on behalf of a minor if the data user had reasonable grounds to believe that compliance with the request would not be in the best interests of the minor.

25. As to the factors that the data user should assess for establishing reasonable grounds for the refusal of data access, the Council would suggest that the Commissioner should devise a set of guidelines in consultation with various classes of data users.

Transfer of personal data in business mergers or acquisition

26. The Council is supportive of the proposal that an exemption from DPP3 should be provided for the transfer or disclosure of personal data in intended merger, acquisition or transfer of businesses subject to the condition that the resultant organization will offer substantially similar service as the original data user.

27. It seems that protection of the data subject affected by the exemption can be furthered by making it a condition that personal information transferred in connection with a prospective merger or acquisition is anonymised.

28. There may be some uncertainty over whether disclosure of sensitive personal data is unnecessary and excessive, and therefore should be

disallowed under paragraph 52 (c) of the Consultation Document. It seems that there is a need to make it clear that sensitive personal data will not be exempted. This is consistent with the Administration's proposal that handling of sensitive personal data would be prohibited except, inter alia, that the prescribed consent of the data subject has been obtained.

29. Last but not lease, except for the contravention of the conditions under paragraph 52 (d) and (e) mentioned in paragraph 53 of the Consultation Document, there is no mention of the sanction for the breach of other conditions for the exemption. The Council calls for further proposal or clarification in this regard.

Consumer Council
November 2009

S0127

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
30/11/2009 17:31 Subject 有關檢討《個人資料（私隱）條例》諮詢文件的意見
☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

香港研究
Hong Kong Research

香港下亞厘畢道
中區政府合署東座364室
政制及內地事務（第4組）

執事先生：

有關檢討《個人資料（私隱）條例》諮詢文件的意見

你好， 貴局於2009年8月就《個人資料（私隱）條例》修訂展開爲期三個月的公眾諮詢，本會就此於2009年11月21日至27日，進行了「市民對檢討《個人資料（私隱）條例》諮詢文件的意見調查」，以分別了解成年人士及未成年人士對該份諮詢文件的意見。本會就上述調查所得之結果，進行深入分析，並整理成一份詳細的調查報告（詳見附件）。現根據本會的調查結果分析所得，對諮詢文件作出以下建議：

1. 調查發現，在「立法規管生物辨識資料如瞳孔特徵、掌紋及指紋等敏感個人資料的使用範圍」、「設立自願性通報機制」及「將未經授權下取得、披露及出售個人資料，從中取利或作惡意用途的行爲訂爲刑事罪行」三項建議上均能取得大部份成年人士的認同。

2. 在是否賦予私隱專員刑事調查和檢控權力的問題上，較多成年人士認同賦予私隱專員刑事調查和檢控權力，但亦有部份成年人士則較認同維持現有安排，反映建議未獲得大部份成年人士的共識。本會建議當局應向市民進一步闡釋賦予私隱專員更多權力的利弊，讓市民可進一步對此進行深入探討。

3. 在涉及父母使用子女個人資料權利的建議上，多數成年人士表示贊成授權父母可更改未成年子女個人資料用途，但未成年人士在此問題上意見分歧，結果反映未成年人士對此問題未達共識。

4. 對於是否贊成若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許警方將其有關資料告知父母，大部份成年人士對此表示贊成，但較多未成年人士對此卻表示不贊成，反映在此問題上兩者立場迥異。

5. 此外，大部份成年人士及未成年人士贊成除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發查閱子女的個人資料，反映建議得到大多數市民的支持。

6. 未成年人士在是次諮詢中是其中一個持份者，從部份調查結果所得（第3、4及5點），未成年人士對部份建議與成年人士持相反立場，本會建議當局積極吸納未成年人士對諮詢文件的意見，透過溝通和闡釋，爭取更多未成年人士對建議的認同及支持。

本會希望上述建議有助　貴局條訂相關條例，進一步加強本港對個人資料私隱的保障。

香港研究協會
二〇〇九年十一月三十日

附件：「市民對檢討《個人資料（私隱）條例》諮詢文件的意見調查」調查報告



「市民對檢討《個人資料（私隱）條例》諮詢文件的意見調查」調查報告.pdf

S0127

香港研究協會
Hong Kong Research Association

市民對檢討《個人資料（私隱）條例》諮詢文件的意見調查

調查報告

二〇〇九年十一月

1 研究背景

1.1 香港研究協會爲一個非牟利的學術機構，於二〇〇四年六月創立。協會將透過調查研究，爲市民提供一個發表意見、關心香港的平台，並加深市民對社會各方面的認識。

1.2 宗旨

1.2.1 以獨立和客觀的角度對香港社會各方面進行調查及研究，提出有建設性的方案或建議，扮演民間智庫的角色；

1.2.2 凝聚市民力量，共同關心社會，推動香港可持續發展。

1.3 主要工作

1.3.1 對社會各方面進行調查、研究，範圍包括政治、經濟、民生、國際熱點、國情等；

1.3.2 就香港不同範疇的社會政策展開專題研究，並提出建議及方案，供政府及社會各界人士參考；

1.3.3 凝聚青年義工共同參與研究調查工作。

1.4 二〇〇九年八月，政府展開檢討《個人資料（私隱）條例》的公眾諮詢。本會特此進行電話訪問調查，以了解市民對諮詢文件的意見。

1.5 調查結果曾在二〇〇九年十一月二十九日發送至各大傳媒。由於篇幅所限，未能全面反映結果。本報告旨在就是次調查結果，作出系統性的整理和分析，以較深入及全面地反映香港市民對檢討《個人資料（私隱）條例》諮詢文件的意見。本報告亦將就調查結果提出具針對性的建議，供政府及社會各界參考。

2 調查設計

2.1 本調查題目爲：市民對檢討《個人資料（私隱）條例》諮詢文件的意見調查。

2.2 本調查以隨機抽取電話號碼的電話訪問系統進行。

2.3 電話號碼抽樣方法是首先用電腦以隨機方法抽取「種籽」數字，再以電腦程式進行多次混合算術的方法產生另一組號碼，然後在混合後再過濾重覆號碼，成爲最後訪問樣本號碼。

2.4 本會有一套嚴謹的監測機制，定期對整個調查系統進行測試，以確保系統正常運作。

2.5 調查於 11 月 21 日至 27 日進行，成功訪問了 1408 名市民，其中 1081 名爲成年人士，佔七成七；327 名爲未成年人士，佔兩成三。

3 調查結果

3.1 諮詢文件建議立法規管生物辨識資料如瞳孔特徵、掌紋及指紋等敏感個人資料的使用範圍。調查發現，逾五成半受訪成年人士對此表示「贊成」（56%），表示「不贊成」的佔兩成半。此外，亦有一成九受訪成年人士對此表示「無意見」（表一）。

表一：諮詢文件建議法規管生物辨識資料如瞳孔特徵、掌紋及指紋等敏感個人資料的使用範圍，受訪成年人士是否贊成？（樣本=1081）

規管生物辨識資料	百分比
贊成	56%
不贊成	25%
無意見	19%
合計	100%

3.2 現時私隱條例沒有規定資料使用者於發生個人資料外洩事故時須通知私隱專員或受影響人士，諮詢文件建議設立自願性通報機制，逾六成受訪成年人士對此表示「贊成」（64%），表示「不贊成」的佔一成六。另有兩成受訪者對此表示「無意見」（表二）。

表二：現時私隱條例沒有規定資料使用者於發生個人資料外洩事故時須通知私隱專員或受影響人士，諮詢文件建議設立自願性通報機制，受訪成年人士是否贊成？（樣本=1081）

設立自願性通報機制	百分比
贊成	64%
不贊成	16%
無意見	20%
合計	100%

3.3 有意見認爲應賦予私隱專員刑事調查和檢控權力以提升執法效率；亦有意見認爲現行警方與律政司分別進行調查及檢控的安排運作暢順，近五成受訪成年人士較認同「賦予私隱專員刑事調查和檢控權力」的意見（47%），有三成受訪成年人士則較認同「維持現行安排」。另外，近一成受訪成年人士表示「其他」意見（9%），亦有一成四受訪成年人士對此表示「無意見」（表三）。

表三：有意見認爲應賦予私隱專員刑事調查和檢控權力以提升執法效率；亦有意見認爲現行警方與律政司分別進行調查及檢控的安排運作暢順，受訪成年人士較認同哪一種意見？（樣本=1081）

應否賦予私隱專員刑事調查和檢控權力	百分比
賦予私隱專員刑事調查和檢控權力	47%
維持現行安排	30%
其他	9%
無意見	14%
合計	100%

3.4 諮詢文件建議將未經授權下取得、披露及出售個人資料，從中取利或作惡意用途的行爲訂爲刑事罪行，大部份受訪成年人士（88%）對此表示「贊成」，表示「不贊成」及「無意見」的則各佔百分之六（表四）。

表四：諮詢文件建議將未經授權下取得、披露及出售個人資料，從中取利或作惡意用途的行爲訂爲刑事罪行，受訪成年人士是否贊成？（樣本=1081）

訂爲刑事罪行	百分比
贊成	88%
不贊成	6%
無意見	6%
合計	100%

3.5 對於授權父母可更改未成年子女個人資料用途的建議，逾五成受訪成年人士對此表示「贊成」(53%)，而表示「不贊成」的則佔兩成半。另表示「無意見」的受訪成年人士佔兩成二（表五）。

表五：諮詢文件建議授權父母可更改未成年子女的個人資料用途，受訪成年人士是否贊成？（樣本=1081）

建議授權父母可更改未成年子女的個人資料用途	百分比
贊成	53%
不贊成	25%
無意見	22%
合計	100%

3.6 現行法例不容許警方主動把未成年子女的個人資料告知其父母；諮詢文件建議若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許將其有關資料告知父母，逾八成受訪成年人士對此表示「贊成」(84%)，表示「不贊成」的佔百分之九。另有不足一成受訪成年人士表示「無意見」(7%)（表六）。

表六：現行法例不容許警方主動把未成年子女的個人資料告知其父母；諮詢文件建議若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許將其有關資料告知父母，受訪成年人士是否贊成？（樣本=1081）

容許警方主動把未成年子女的個人資料告知其父母	百分比
贊成	84%
不贊成	9%
無意見	7%
合計	100%

3.7 諮詢文件建議除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發，查閱子女的個人資料，逾七成受訪成年人士對此表示「贊成」(71%)，表示「不贊成」的佔一成六。此外，有逾一成受訪成年人士對此表示「無意見」(13%)(表七)。

表七：諮詢文件建議除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發，查閱子女的個人資料，受訪成年人士是否贊成？（樣本=1081）

容許父母查閱以未成子女的個人資料	百分比
贊成	71%
不贊成	16%
無意見	13%
合計	100%

3.8 鑑於社會上對諮詢文件中一些涉及父母使用子女個人資料權利的建議表示關注，調查亦進一步了解未成年人士對文件中使用其個人資料建議的意見。

3.9 調查結果顯示：三成七受訪未成年人士表示「贊成」授權父母可更改未成年子女的個人資料用途，亦有三成八受訪未成年人士對此表示「不贊成」。另外，表示「無意見」的受訪未成年人士佔兩成半（表八）。

表八：諮詢文件建議授權父母可更改未成年子女的個人資料用途，受訪未成年人士是否贊成？（樣本=327）

授權父母可更改未成年子女的個人資料用途	百分比
贊成	37%
不贊成	38%
無意見	25%
合計	100%

3.10 至於若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許警方將其有關資料告知父母，近三成受訪未成年人士對此表示「贊成」(28%)，另有逾四成受訪未成年人士對此表示「不贊成」(44%)，而表示「無意見」的則佔兩成八（表九）。

表九：現行法例不容許警方主動把未成年子女的個人資料告知其父母；諮詢文件建議若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許將其有關資料告知父母，受訪未成年人士是否贊成？（樣本=327）

容許警方主動把未成年子女的個人資料告知其父母	百分比
贊成	28%
不贊成	44%
無意見	28%
合計	100%

3.11 調查亦問及受訪未成年人士對除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發，查閱子女的個人資料建議的意見，逾六成受訪未成年人士對此表示「贊成」(63%)，表示「不贊成」的佔兩成。另有近兩成受訪未成年人士表示「無意見」(17%)(表十)。

表十：諮詢文件建議除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發，查閱子女的個人資料，受訪未成年人士是否贊成？（樣本=327）

容許父母查閱以未成子女的個人資料	百分比
贊成	63%
不贊成	20%
無意見	17%
合計	100%

3.12 按人口變項的交叉分析結果顯示：不同社會階層的成年人士皆傾向贊成立法規管生物辨識資料如瞳孔特徵、掌紋及指紋等敏感個人資料使用範圍的建議。收入愈高者則愈贊成建議；相反，收入愈低者不贊成建議的比率則愈高（表十一）。

表十一：受訪成年人士的社會階層與其是否贊成規管生物辨識資料之交叉分析（樣本=1081；顯著性=0.000<α=0.05）

	受訪成年人士的社會階層			
	低收入人士	中產人士	高收入人士	整體
規管生物辨識資料				
贊成	49%	61%	66%	56%
不贊成	26%	24%	23%	25%
無意見	25%	15%	11%	19%
合計	100%	100%	100%	100%

3.13 就受訪成年人士的年齡組別來看，年齡介乎 41 至 65 歲的受訪者對授權父母可更改未成年子女個人資料用途表示贊成的比率較其他的爲高（表十二）。對於有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許警方將其有關資料告知父母，年齡介乎 41 至 65 歲的受訪者表示贊成的比率較其他的爲高（表十三）。同樣地，年齡介乎 41 至 65 歲的受訪者對除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發查閱子女個人資料表示贊成的比率較其他的爲高（表十四）。整體而言，不同年齡組別受訪者均傾向贊成上述三項建議。41 至 65 歲年齡組別的成年人士較其他年齡組別成年人士明顯贊成諮詢文件中有關父母使用子女個人資料權利的建議。值得留意的是，在 18 至 30 歲、31 至 40 歲及 41 至 65 歲三個年齡組別中，年齡愈大的組別對建議表示贊成比率愈高，其比率於 41 至 65 歲組別達到高點後，65 歲以上組別贊成比率均出現回落。

表十二：受訪成年人士的年齡與其是否贊成授權父母可更改未成年子女的個人資料用途之交叉分析（樣本=1081；顯著性=0.000<α=0.05）

	受訪成年人士的年齡				
	18 至 30 歲	31 至 40 歲	41 至 65 歲	65 歲以上	整體
授權父母可更改未成年子女的個人資料用途					
贊成	49%	53%	56%	30%	53%
不贊成	31%	26%	23%	24%	26%
無意見	20%	21%	21%	46%	22%
合計	100%	100%	100%	100%	100%

表十三：受訪成年人士的年齡與其是否贊成容許警方主動把未成年子女的個人資料告知其父母之交叉分析（樣本=1081；顯著性=0.000<α=0.05）

	受訪成年人士的年齡				
	18 至 30 歲	31 至 40 歲	41 至 65 歲	65 歲以上	整體
容許警方主動把未成年子女的個人資料告知其父母					
贊成	77%	84%	88%	70%	84%
不贊成	16%	8%	6%	13%	9%
無意見	7%	9%	6%	18%	8%
合計	100%	100%	100%	100%	100%

表十四：受訪成年人士的年齡與其是否贊成容許父母查閱以未成子女的個人資料之交叉分析（樣本=1081；顯著性=0.000<α=0.05）

	受訪成年人士的年齡				
	18 至 30 歲	31 至 40 歲	41 至 65 歲	65 歲以上	整體
容許父母查閱以未成子女的個人資料					
贊成	65%	69%	76%	67%	71%
不贊成	22%	18%	12%	6%	15%
無意見	13%	13%	12%	27%	13%
合計	100%	100%	100%	100%	100%

3.14 就受訪家長而言，在是否贊成「授權父母可更改未成年子女的個人資料用途」（表十五）、「若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許警方將其有關資料告知父母」（表十六）及「除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發，查閱子女的個人資料」（表十七）三項建議的意見上，受訪家長表示贊成的比率均較非家長的爲高；但整體而言，受訪成年人士（包括家長及非家長）皆傾向贊成上述建議。

表十五：受訪成年人士是否父母與其是否贊成授權父母可更改未成年子女的個人資料用途之交叉分析（樣本=1081；顯著性=0.001<α=0.05）

	受訪成年人士是否父母		
	是	不是	整體
授權父母可更改未成年子女的個人資料用途			
贊成	57%	46%	53%
不贊成	22%	30%	26%
無意見	21%	24%	22%
合計	100%	100%	100%

表十六：受訪成年人士是否父母與其是否贊成容許警方主動把未成年子女的個人資料告知其父母之交叉分析（樣本=1081；顯著性=0.002<α=0.05）

	受訪成年人士是否父母		
	是	不是	整體
容許警方主動把未成年子女的個人資料告知其父母			
贊成	87%	79%	84%
不贊成	7%	12%	9%
無意見	7%	9%	8%
合計	100%	100%	100%

表十七：受訪成年人士是否父母與其是否贊成容許父母查閱以未成子女的個人資料之交叉分析（樣本=1081；顯著性=0.000<α=0.05）

	受訪成年人士是否父母		
	是	不是	整體
容許父母查閱以未成子女的個人資料			
贊成	78%	61%	71%
不贊成	11%	22%	15%
無意見	11%	17%	13%
合計	100%	100%	100%

4 結果分析及建議

4.1 調查發現，在「立法規管生物辨識資料如瞳孔特徵、掌紋及指紋等敏感個人資料的使用範圍」、「設立自願性通報機制」及「將未經授權下取得、披露及出售個人資料，從中取利或作惡意用途的行爲訂爲刑事罪行」三項建議上均能取得大部份受訪成年人士的認同，相信相關條例可順利通過修訂。

4.2 在是否賦予私隱專員刑事調查和檢控權力的問題上，較多（47%）受訪成年人士認同賦予私隱專員刑事調查和檢控權力，但亦有爲數不少（30%）的受訪成年人士則較認同維持現有安排，反映建議未獲得大部份成年人士的共識。本會建議當局應向市民進一步闡釋賦予私隱專員更多權力的利弊，讓市民可進一步對此進行深入探討。

4.3 在涉及父母使用子女個人資料權利的建議上，多數受訪成年人士（53%）表示贊成授權父母可更改未成年子女個人資料用途，但受訪未成年人士在此問題上意見分歧（贊成：37%；不贊成：38%），結果反映未成年人士對此問題未達共識。對於是否贊成若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許警方將其有關資料告知父母，大部份（84%）受訪成年人士對此表示贊成，但較多（44%）受訪未成年人士對此卻表示不贊成，反映在此問題上兩者立場迥異。此外，分別有七成一及六成三受訪成年人士及受訪未成年人士贊成除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發查閱子女的個人資料，反映建議得到大多數市民的支持。未成年人士在是次諮詢中是其中一個持份者，從部份調查結果所得，未成年人士對部份建議與成年人士持相反立場，本會建議當局積極吸納未成年人士對諮詢文件的意見，透過溝通和闡釋，爭取更多未成年人士對建議的認同及支持。

4.4 在人口變項分析方面，年齡介乎 41 至 65 歲的受訪成年人士較其他年齡組別明顯贊成「授權父母可更改未成年子女個人資料用途」、「若有證據顯示未成年子女有可能干犯罪行，並相信父母得悉此事有助防止罪行時，容許警方將其有關資料告知父母」及「除父母涉嫌虐兒或者父母已離異外，容許父母以未成年子女的利益出發查閱子女的個人資料」三項建議。就受訪家長而言，表示贊成上述三項建議的比率均較非家長的爲高；但整體而言，成年人士皆傾向贊成上述建議。

政府及內地事務局個案提寫政策第四組:

S0128

檢討個人資料私人條例，本人有以下三個情況要求的敬望接納。

第一是實例: 因每次見工僱主總會要全部個人資料的負本包括個人身份証一定要比他們的，但從不在個人身份証負本上印上COPY 的字眼，有事逗不抽空面試立刻說等通知，並本人是過見過幾個不同男女老幼，和不地方不同公司不同行業的僱主，大意見過他們的這班僱主，番見但說以入了在電腦內和一樣等通知，我當時以過了 6 個月以上，我立刻問僱主爲何不請還保留本人見工者的個人資料還沒取消，僱主當時沒有回應，只說等通知。後來我曾問勞工處爲何不請人，也要太多個人資料特別是個人身份証資料，但勞工處說以向每一位僱主一早說明要請某人開工，才要個人身份証負本的，但大部分僱主不跟勞工處法例去做，照收個人資料特別是個人身份証資料負本沒印上 COPY 的字眼。

本人希望政府收緊屬法例如超過一個月不能留下任何見工者的個人資料一定要取消，並且一定用這位員工才要，身份証負本和上面印上 COPY 的字眼，否則罰款 5 萬港幣入獄 5 年。

第二是實例: （刪除）本人的家人性名在 2000 年某日在這公司申請的商業電話服務至到 2005 年某日才停用（刪除）公司商業電話服務，本人性名同年 2000 年也在（刪除）公司申請了家居電話服務，至到 2005 年同時某日也取消（刪除）公司這家居電話服務，並且一早在（刪除）公司申請用的上網服務和電視服務，某日我打去熱線查詢，當日電視收得差才打去，後來發現有線熱線錄音說本人有三個登記資料是
(1)（刪除）電視服務帳戶號、(2)（刪除）上網服務帳戶號、(3)（刪除）電話家居服務帳戶號(3)（刪除）電話家居服務帳戶號。
我不知爲何多了一個（刪除）電話家居服務帳戶號，雖然沒有收多我這個（刪除）電話家居服務費，但當時我只管電視收得差問題，沒有去跟進這件事的，並且 （刪除）公司屈我家人比新的家居電話號碼，她們找本人的家人性名，並用口才騙取家人的手提電話資料，來推銷電話服務，當時我不比困聽到有問題?
如真的是找他點會不知他手提電話資料，，我不知爲何多了一個（刪除） 家居服務帳戶號，雖然沒有收多我這個（刪除）電話家居服務費，但當時我只管電視收得差問題，沒有去跟進這件事的，並且 （刪除）公司屈我家人比新的家居電話號碼，她們同中打來找本人的家人性名，並用口才騙取家人的手提電話資料，來推銷電話服務，當時我不比困聽到有問題? 如真的是找他點會不知他手提電話資料，我也問過家人有否比 （刪除）公司任何一個職員知轉了新公司的家居服務，家人說無的，本人知是（刪除）電話電訊公司的因當時用過（刪除）電視服務並通知比新的家居電話號碼，他們是兄弟班機構。

本人希望政府收緊屬法例不倫任何公司，一定不要買賣任何客戶所有個人資料外漏出去，如發現有此事，一定要罰款 5 萬港幣和入獄 5 年。

第三是實例: （刪除） 用 MK17 的自製產品這公司是黑店她班女人或男人不倫是僱主或員工一樣無良心行騙手法包含誤導銷售騙財，我識有位朋友她被騙去幾萬元港幣並且以一早收集很多個人資料有手提電話、有住屋地址、有身份証內所有資料、並將個人身份証號碼代替客戶號碼，最過份是這客戶以停用這間公司的任何美容服務療程，也超過了 5 年有多過不斷用電話惡作劇煩人，我朋友也曾主動打去要求不好在找她並且要求在它們的公司電腦取消所有個人資料但到現在是沒有做到的。

本人希望政府收緊屬法例任何一間美容機構一定要合法注冊，並且不倫任何一間美容機構不准收個人資料太多，例如個人身份証資料只能在前面 3 個號字和住屋地址不能比的以有手提電話，可以用手提電話寄短，電話留言等多方面給客戶信息，否則罰 6 萬港幣入獄 6 年。 希望政府及內地事務局個案提寫政策第四組能幫助我們平民百性心聲。

祝你們工作愉快和身心健康

(署名來函)

11 月 30 日 2009 年

(未能確定來信人是否願意公開姓名，並已刪除
意見書涉及來信人的個別個案的詳細資料)

政策及內地事務局：見信好！

由于一連串事情發生，市民對個人資料私隱保障日益關注，就此我們非常需要檢討個人私隱收緊個人資料規管，我們要簡化私隱條例規管，進行施行争取相關措施。

現應不應當反映一些問題，我們無辦法到目前爲止，無辦法忍受日夜受到困擾聲音。這些聲音不知道發生在什麽地方，幾年來太過分：根據我們幾年的從無綫電廣播聽到的聲音，這種聲音是發生在哪個地區，哪個屋村自由黨分部頭目，濫殺無辜人聲音，同時也有在爲市民主持公道社區中心主持公道，護法制聲音，自由黨分部頭目仗着自由黨名義和力量，冤枉、侮辱、抹黑長者夫婦和一些無辜人，廣大市民聽清楚，我想你們應當也聽到了，這種惡意用途民憤極大。自由黨分部頭目挑戰法紀，抓起石頭砸自己脚太可惡，無中生有，捏造事實，制造矛盾，制造是非，祇許州官放火，不許百姓點燈作法，自己可以講，就不讓他們反駁，唯恐天下不亂，濫殺無辜人，企有此理，惡意中傷，實在氣人。强詞奪理，欺人大甚，迫害長者（24 小時打壓包圍無辜人）憑什麽資料來打壓市民，太過份了。從無綫廣播聽到，無論走到哪都聽到這種聲音，太可恨了，真是惡意中傷，整整這麽多年了，太可怕了，目前香港雖然是法治社會，但是惡勢力正向弱勢群體開刀，太頑固，太不講道理，仗着自己是自由黨分部頭目可以無法無天，今日在證據面前還要冤屈市民，民憤極大，自由黨這個民聲已經使市民去地這個政黨希望，估計下屆選擇可能會流失票數。如此濫殺無辜人，他自己作錯事情，冤屈別人

反而誤賴別人，剥奪他人自由和言論自由凌駕法律之上，點解我們會知道，都是以無綫電廣播聽到，久而久之聽清楚，今日我們爲受氣的市民而寫，在未發表個人意見同時，我們要求政府和有關部門快快解決（纏擾）無辦法休息，他 24 小時全力打壓，他的行爲還没有解决了，點解警方應采取措施呢。他破壞社會秩序使市民無辦法開工，無辦法得到休息，侵犯他人私隱，今日迫着我們就個人私隱問題我們發表個人意見：請你們采取有關措施，盡快解决這個（纏擾）問題。解决私隱問題。

我們建議：1、把私隱規管受托個人資料處理者，應當嚴格規管。

2、對敏感個人資料（如指紋）應當受到更嚴格地規管。

3、應當規定資料使用者在發生個人資料處理者，外泄事故通知私隱專員及受影響人士。

4、應當授權私隱專員刑事調查和檢控權力。

5、授權私隱專署爲法定機構。

6、若有當事者因資料使用者違反私隱條例規定而蒙受損失并已向資料使用者提出法律訴訟，應當授權私隱專員爲受屈的資料當事人提出法律協助。

7、應當授權私隱專員向受屈資料當事人判給補償，有必要這樣做。

8、應當把違反保障資料原則訂爲刑事罪行。

9、把披露未經資料使用者同意下取得個人的資料從中取得惡意行爲用途行爲訂爲刑行。

10、應當把資料使用者已送行私隱專員發出的執行通知規定，但不

久又故意重犯的行爲訂爲刑事罪行。

11、應當授權私隱資料嚴重違反保障資料原則訂爲施加罰款。

12、應當將履次違反執行通知行爲處以更重罰則。

13、應當提出直銷法律中不當使用個人的資料罰則。

祝

安好!

(署名來函)

2009 年 11 月 17 日

(未能確定來信人是否願意公開姓名)

政制及內地事務局：見信好！

研究過去十幾年的私隱資料條例和私隱專署協助不作好，尤爲重要，主要你們作爲政府要緊部門非常感謝你們，爲市民作這麼多事情。目前非常重要事情是盡快解決香港目前與在看問題，1、嚴重的網上侵權，2、嚴重侵犯板權，3、嚴重侵犯私隱權，4、嚴重侵犯人生自由權，5、嚴重侵犯言論自由，就以上情況講解香港是一國二制社會，高度自治社會，依法制法，天下之事不難于之法，而難于法，必之行，不難于聽言，難于言之必效，要言行一致，誠信于民。在我們未發表個人意見，我們[redacted]市民，無辦法承受日夜維扶聲音，幾年來不斷傳來有人冤屈市民聲音，我們也是送貨要經常從九龍塘坐車到深圳，然後返回等車，經常聽到這樣聲音，久而久知，全面聽到好清楚，出于好奇心，把他全部録下來，我們幾個人都會背下，整個侵犯私隱作法過程，我們也經常去深圳還貨，有時開車到福建邊關時也聽到這種聲音，實在無可忍地步。我們[redacted]非常同時安中無故人處境困境，恨自由黨給市民帶來精神痛苦和人格侮辱，名譽傷害，但我們不知道發生什麼地方，來自哪個地區和屋村，我們也了解到三年 6 個月 27 天，某地區，某屋村會輔導合作中心，他們風雨無阻，放弃假日，没有得到休息，24 小時替市民申冤，主持公道，爲社區服務幾十年的好，可以講全香港的市民服務中心最好一個，日日夜夜爲民解冤枉，足足用了 3 年 6 個月時間，與不法分子作鬥争，今日把我們所録言下來情況先告訴你們，你們了解發生在這裏市民是多麼痛苦，精神相當煩腦的，正因爲這樣把我們聽到事情告訴你們，受害者是內地國家幹部，一級教

師，有二十幾年榮譽證書，她老公是政府高官，廉潔奉公，守法好官，05 年 6 月份以後，自由黨分部頭目，無中生有制造受害當事人，6 個月日日夜夜把當事人兩公婆腦人，根本都没有腦人，他什麽花招都出來了，人地兩公婆在休養，兩人開大刀，雙雙入院，在休息睡覺，死死説他們腦入，在這樣情況有人替他報不平，好像我們寫信給你們同理可證，根本與她無關。當時在鄰捨輔導會和有關部門主持公道下，定爲腦人是假，但是上訴并不是她，在没有辦法情況走投無路返回福建去，而她前走後追到福建，又在人地當地工作單位挑起是非，然後又把兩地的私隱部暴露出來，光天化日之下，挑起中港兩地私隱事情，使冤情深如海，并且到屋村所在地有關部門收集當事人私隱，起至當事人銀行好多少款都收集一清二楚，然後又暴露出來大把錢，根本在内地没有貪污硬要冤枉人貪污的百幾元款問題，貪污是犯法行爲，内地與香港法律已經接軌會開除，在内地政府及各部門官方文件根本證明公安局證明二十幾年遵紀守法好市民，根本没有犯法，也没有貪污百幾元問題，好市民，講解香港 89 年到香港他冤枉當事人是 98 年來，痴死 29 年，明明是遵紀守法，没有犯法，香港 19 年身份證三顆星，是香港納税好市民，硬要冤枉人地犯法，唔通身份證有得假，無得假，硬要冤枉人兩公婆騙人，與她老公連理 46 年，有各種證據付給有關處理事件中心，正式，硬要冤枉人地婚前不貞，同時還要冤枉人地偷耶，身爲人民教師着嚴教育下一代，幾時人地偷耶，證據面前光明磊落作風正派好市民，并且冤枉人地打擾是鷄，幾時人地有作過鷄，同時他自己打冤枉學生（BB 作鷄）反而冤枉學生（BB 作鷄），根本人地都没

有碰到學生，硬要冤枉人地講，在休息室裏從來没有碰過學生一起過。好煩，作有事情都是他自己一手挑起，青天白日講大話，教唆他人，和煽動他人，24 小時包圍當事人和鄰捨中心，惡勢力已經犯侵校園 3 年 6 個月天，日日夜夜，相當難爲鄰捨服務中心，相當難爲當地警方，和各個部門；忙得團團轉，在大把證所，證明打錯，但是他死不承認，公開認錯，拒絶認錯，還教唆他人向報上登道德及其他，11 月 23 日報道太可惡，侵犯私隱三翻四次，讓人再去，收集侵犯人身由自，違反基本規定，剥奪居民他人自由是犯法，天光打底天暗，周而復始，死死糾纏，3 年 6 個月 27 天，我們天天聽慣了，都會背下來這個過程，我們録音，左右爲難，目前困境，没有辦法解决，惡勢力手下有一百多人，在法制的社會根本不存在輸贏問題，存在着能不能侵犯問題，人家都没有錯，在大把證據面前，講人家騙人，我們聽了都很氣，眼泪都流下來，世間上有這麽壞的人，企有此理，無中生有，捏造事實，不讓來人反駁，不許反駁，既使人家是啞巴，啞巴也有發言權，不講道理，廣大市民對這個惡意用途，惡意扶黑早已經忍無可忍，如于他用電話困擾内地一個工作人員，致使她撞車而死，經常打電話困擾，他自己可以打電話，别人就不可以打電話，什麽自由都給他剥奪了，他條條是犯法的，講話自由都給他剥奪了，也剥奪了鄰捨服務中心的一切自由，太可惡了，他自己一手打爛，嫁禍當事人，嫁禍中心，太可惡了，請你們收到我們的信以後，就存在着這個問題轉告政府，有必要對就這個侵犯私隱盡快立案通過，起到助哧作用，24 小時打壓包圍，情節太嚴重了，對市民的纏擾，我們根本就没辦法休息，望政府

快快咨詢文件，解決纏擾方法：

1、 應當提高直銷促銷活動中不當使用個人的懲罰；

2、 應當對于履次違返執行重要懲罰；

3、 應當授權就嚴重違反保障資料原則行爲施加罰款；

4、 把資料使用者未經同意下取得個人起到了惡意用途，類爲刑事罪行；

5、 應當把違反保障資料定爲刑事罪行；

6、 應當授權私隱專員向受屈補給補償；

7、 若有資料當事人用資料違反資料條例規定，而蒙受損失，并有意向資料使用者提出法律訴訟，當授權私隱專員爲受屈的資料當事人提供法律援助。

8、 應當授權給麽隱專署刑事檢控的權力。

9、 應當規定資料使用者，在發生資料外泄事故時，通知私隱專署及受影響的人士。

10、 應當規管受手處理個人資料處理者。

11、 對敏感的資料（如指紋）應當受更嚴格規管。

12、 對于警方檢查身份證列入正常規管。

安好！

(署名來函)

2009 年 11 月 27 日

（ 未能確定來信人是否願意公開姓名 ）

S0131

Society of Operations Engineers (Hong Kong Region)

Date: 28 November 2009 Our Ref.:SOEHKR-20091129-01

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Sir/Madam,

The Society of Operations Engineers in Response to the Public Consultation on Review of the Personal Data (Privacy) Ordinance

As one of the Professional Engineering Society in Hong Kong , The Society of Operations Engineers Hong Kong Region (SOEHK) would like to express our comment on some issues of the Personal Data (Privacy) Ordinance as follows for your kind consideration.

Sensitive Personal Data

- *Should we subject sensitive personal data, such as fingerprints, to more stringent regulation?*

Our comment: In terms of provide better security on protecting personal data against misuse of personal data particular the biometric data, we are totally agree to stringent regulation to be set but certain degree of flexibility is preferred and to be reserved to the data subjects. If stringent regulation is enforced in future, we believe more operation cost will be necessary for uplifting our data operation and management system and it will be one of our concerns on the financial burden to be added on the non-profit making society like SOEHK. Some of the general personal data for basic identification of our members is required and the security control to comply the future requirements should be simple and not require high technology to support, such as some sophisticated and proprietary software or system.

INVESTORS IN PEOPLE

Data Security

- *Should we regulate data processors entrusted with handling of personal data?*
- *Should we require data users to notify the PCPD and affected individuals of personal data leakage incidents?*

Our comment: As a responsible society, we are endeavor to protect all our members' personal data in a save and controllable environment. However, as mentioned in the Clause 10 of the consultation document, the risk of exposing personal data by illegal method is increasing with the trend of new information technology. To certain extend, big investment on catching up the new technology may be required to upgrade or even to maintain the same degree of current protection, but we are unable to afford such investment and it may not be fair to our members as well. Please consider your proposal to balance this foreseeable conflict before finalize the new regulation.

Powers of the PCPD

- *Should we give the PCPD criminal investigation and prosecution power?*
- *Should we empower the PCPD to provide legal assistance to an aggrieved data subject who suffers damage by reason of a data user's contravention of a requirement under the Ordinance and intends to institute legal proceedings against the data user?*
- *Should the PCPD be empowered to award compensation to an aggrieved data subject?*

Our Comment: We have the same point of view as Clause 14 to 16 in the consultation document, the authority of PCPD can be remain unchanged at the moment and some offences proposed in this review are not technical in nature and involve a fine and imprisonment, there could be concern if such powers are delegated to the PCPD. Moreover the existing arrangements have worked well. We do not see a strong case to give the PCPD the power to investigate into and prosecute criminal offence cases.

Offences and Sanctions

- *Should we make contravention of a Data Protection Principle an offence?*

Our Comment: We have the same concern on this issue as stated in the Clause 18. If the indicant is caused by an inadvertent act or omission, we should not consider it is a making contravention of a DPP an offence.

- *Should we make it an offence when a person discloses for profits or malicious purposes personal data obtained from a data user without the latter's consent?*
- *Should we make it an offence when a data user intentionally resumes the same contravening act shortly after complying with an enforcement notice issued by the PCPD against him?*
- *Should we empower the PCPD to impose monetary penalty on serious contravention of Data Protection Principles?*
- *Should we impose heavier penalty for repeated non-compliance with an enforcement notice?*
- *Should we raise the penalty for misuse of personal data in direct marketing?*

Our Comment: If the intention is to obtain profits or malicious purposes, it should be a contravention of an offence we have the same observation on incidents of blatant dissemination of leaked personal data on the Internet have aroused widespread concern in the community regarding the possible misuse of leaked personal data. Please also consider an exception/flexibility to be offered to the non-profit making society when imposing heavier penalty for the repeated non-compliance with an enforcement notice as they may lack of comprehensive data control tools or resources.

Rights of Data Subjects

- *Should we empower a third party to give consent to the change of use of personal data of a minor or a mentally incapacitated person?*
- *Should we permit a data user to refuse a data access request made by parents on behalf of a minor when compliance with the request is not in the minor's best interests?*

Our Comment: We agree the principle of the suggestions as stipulated Proposal no.13 and all detail procedures on assessing the right should be carefully determined and grace period shall be applied to review the actual implementation.

Exemptions from the PDPO

- *Should we grant exemption to law enforcement agencies and rescue and relief agencies for handling personal data in emergency situations?*

Our Comment: Exemption should only be confined in emergency situations of accident or emergency rescue was envisaged at the time of their collection.

Should you have any queries on our comment, please do not hesitate to contact our Hong Kong Region Office or the undersigned.

Thank you for your kind attention.

(Signed)

Yours faithfully,

Ir Jeffrey Yung
Chairman
Society of Operations Engineers
Hong Kong Region

S0132

To <pdpo_consultation@cmab.gov.hk>
cc

30/11/2009 16:43

bcc
Subject 香港社區組織協會民權法律中心 回應檢討《個人資料(私隱)條例》諮詢文件意見書

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

香港社區組織協會民權法律中心
回應檢討《個人資料(私隱)條例》諮詢文件意見書

1. 引言

香港特別行政區政府在個人資料私隱專員的協助下，決定全面檢討現行《個人資料(私隱)條例》(下稱「私隱條例」)，並展開為期三個月的公眾諮詢。私隱條例自1996年生效，至今已有十三年，當局遲至2009年8月才展開諮詢，實在遠遠追不上市民對私隱的關切及社會發展步伐。然而，現時諮詢雖姍姍來遲，但本會亦希望當局能撥亂反正，在公眾諮詢後儘快修訂法例，以免與國際社會人權標準及文明脫節。

除了資料科技迅速發展、互聯網的使用變得普及外，市民對個人資料的保障及私隱意識亦日益提升。再者，外國對私隱權利的立法，以至實行普通法地區對涉及私隱權的判決，亦對本港修訂私隱條例，提供莫大的參考。因此，本會將從過往十多年條例執行的問題及外國的經驗，回應諮詢文件各項的建議。

2. 就諮詢文件各項建議回應

2.1 敏感個人資料

建議1：敏感個人資料

敏感個人資料涵蓋的範圍

現行私隱條例並沒有區別“敏感”個人資料與“非敏感”個人資料。由於不同種類的個人資料涉及不同程度對個人的描述或紀錄，資料外洩所造成的傷害及損害遠比過往深遠；若涉及的屬敏感資料，其洩漏或向第三者意外披露有關資料可能對資料當事人造成更重大損害。因此，本會認同有必要在定義上更清晰及仔細地區分“敏感”和“非敏感”個人資料，以強化對個人私隱的保障。

至於何謂“敏感”個人資料，本會認為應有關資料必須具備下列特點：

- 有關個人的隱密資料，例如身體特徵、健康狀況或個人信念；以及
- 極可能用以作出歧視性決定的資料。

參考海外國家經驗，敏感個人資料應包括：生物特徵(如：瞳孔特徵、掌紋、指模、基因資料)、種族或民族本源、政治意見、宗教或哲學信仰、工會會籍、健康狀況、性生活情況、刑事記錄等。本會認為，諮詢文件只建議首先考慮把生物辨識資料列為敏感個人資料，顯示政府對保障私隱的取態非常保守；本會強烈建議，敏感個人資料須定義為全面包括有關個人的隱密資料及極可能用以作出歧視性決定的資料。

由於敏感的定義或隨著時代轉變而有所改變，在強調保障個人資料私隱的大原則下，本會認為除有關定義應採取寬鬆的立法模式，法例亦應容讓日後藉附屬立法方式增加屬敏感個人資料的範圍及內容，從而為個人資料私隱提供更佳保障。

有關處理敏感個人資料的規定

由於敏感個人資料涉及較深度的私隱，因此，在收集、持有、處理和使用敏感個人資料時，需要有更嚴格的規定。本會認同除非符合下述情況，否則禁止收集、持有、處理和使用（統稱“處理”）敏感個人資料：

(a) 獲得資料當事人的訂明同意(即自願而明確的同意)；
(b) 資料使用者為行使法律所授予的權力，或履行法律訂明的責任而必須處理有關資料；
(c) 雖未能取得資料當事人的訂明同意，但為保障資料當事人或其他人的重要利益而必須處理有關資料；
(d) 資料使用者在履行其合法職能和進行合法活動時處理有關資料，並已採取了適當措施，防止資料在未得資料當事人的訂明同意而轉移至或洩漏給第三者；
(e) 資料當事人已明顯地公開了有關資料；
(f) 為醫療目的而必須處理有關資料，而處理資料的是一個專業醫護人員，或是一個在該情況下負有保密責任的人（等同專業醫護人員的

保密責任）；或
(g) 因涉及法律程序而必須處理有關資料。

違反規定的制裁

目前，違反保障資料原則本身並非犯罪。私隱專員獲授權向資料使用者發出執行通知，以糾正違規事項。違反執行通知則屬犯罪，一經定罪，可處第5級罰款（最高可達50,000元）及監禁兩年；如屬持續罪行，可處每日罰款1,000元。然而，有關刑罰往往被批評為過輕，既未能反映過錯的嚴重性，實際執行上亦缺乏阻嚇力。

本會認為，為突顯敏感個人資料的重要性，在考慮法例中保障資料原則的原意下，若有人在處理敏感個人資料時，因疏忽而違反遵守保障資料原則，則私隱專員可發出執行通知，不遵從執行通知者會接受較因披露非敏感個人資料的為重刑罰。

此外，若有人在惡意或蓄意損害個人資料，不論是敏感或非敏感個人資料，均應定為刑事罪行予以檢控。為反映嚴重性，若涉及敏感個人資料，並惡意或蓄意下違反保障資料原則，被告人將要面對較高的刑罰。(見下表)

	因疏忽而 違反保障資料原則	惡意或蓄意下 違反保障資料原則
敏感個人資料	發出執行通知，不遵從者會接受**較重**刑罰。	**訂立刑事罪行**予以檢控，最高刑罰**較重**。
非敏感個人資料	發出執行通知，不遵從者會接受**較輕**刑罰。	**訂立刑事罪行**予以檢控，最高刑罰**較輕**。

不溯既往的豁免或過渡性安排的需要

雖然新修訂的法例理應對法例實施以後的行為產生約束力，然而，若有關行為(即收集、持有、處理和使用個人資料)屬持續進行，為突顯私隱權及個人資料的重視，本會認為在制訂新規定後，指明一個過渡性時期，期間敏感個人資料的處理可獲豁免，不受新規定的規管；在過渡性時期之後，資料使用者在處理敏感個人資料時，則需符合新的規定。這樣既可避免現時絕大部份的資料使用者避開新法例規管，同時亦促使資料使用者主動地檢視過去搜集的是否屬敏感個人資料，是否有必要繼續收集或使用，以符合新法例的要求。

2.2 資料保安

建議2：規管資料處理者及分判活動

根據私隱條例第2(12)條的規定，如某人純粹為另一人，而並非為其任何本身的目的而持有、處理或使用個人資料，則該人不算是資料使用者。在現行法例下，資料當事人憑藉私隱條例第65(2)條獲得保障。根據該條的規定，委聘代理處理個人資料的資料使用者，須就該獲其授權（不論是明示或暗示，亦不論是事前或事後授權）的代理所作出的任何行為承擔責任。

本會認為，不論是資料使用者，或其委託的資料處理者，他們均有責任確保個人資料獲得適當處理。由於在日常生活中，很多個人資料均會交由第三者處理，因此，法例應強化且列明資料使用者及資料處理者的法律責任。特區政府應參考英國的保障資料法令，規定資料控制者/使用者需實施適當技術及機構層面的措施，以保護交託給處理者的個人資料，有關措施包括挑選可充分保證在處理資料方面採取技術及機構層面保安措施的處理者。

此外，法例應訂明資料處理者的特定法律責任，直接規管資料處理者，包括：

(a) 確保個人資料只會用於在受託處理資料時所述明的用途，或與其直接有關的用途；
(b) 採取所有合理可行的步驟，確保由其保管的個人資料安全及妥為保存；以及
(c) 採取所有合理可行的步驟，刪除無須再為貫徹其受託目的而持有的個人資料。

資料處理者若不遵行上述(a)至(c)項任何一項規定，私隱專員可採取執法行動，包括送達執行通知。與此同時，若資料處理者惡意或蓄意下違反保障資料原則，亦需負上刑事責任。

建議3：個人資料外洩通報機制

過去數年，個人資料外洩事件屢有所聞，每次事件均引起社會廣泛關注。然而，個別政府部門或公營機構均未有在切實可行的範圍內，向受影響的資料當事人或社會大眾通報事件。不少外洩事件的消息亦是在傳媒報導事件後，政府當局或有關的機構才急忙回應，令人質疑是否有需要加強規管通報外洩情況。

個人資料外洩嚴重威脅個人私隱，後果可以非常嚴重。只有儘早通知當事人及向社會大眾通報，並採取補救措施，才有助將過錯帶來的損害減至最低。因此，有效的個人資料外洩通報機制極為重要。本會認為，當局應修訂法例，立法訂立個人資料外洩通報機制，規定資料使用者或資料處理者均需在事發後向私隱專員公署通報情況，並向受事件影響的資料持有人。

有論者認為或可採取選擇性或自願性的通報機制，避免出現太多通知下所謂「通知疲勞」，本會並不認同。因為若屬自願性質，外洩個人資料的部門或機構，便極有可能因著避免損壞形象或其他原因而不願報導，甚至錯誤評估外洩個人資料的嚴重性，結果適得其反，無助減低受影響人士可能的損失。再者，若通知數字眾多，亦可藉此讓公眾及社會人士得悉問題的嚴重程度，從而讓當局加強公眾私隱教育及加強執法工作。

法定通報機制包括的資料

面對以上立法建議，法例應列明通報機制應包括以下資料，同時應容讓私隱專員有權要修訂通報個案的資料詳情，以配合社會發展：

(a) 事件的概況；
(b) 外洩日期及時間；
(c) 發現事故的日期及時間；
(d) 外洩的源頭（機構本身或代機構備存個人資料的第三者）；
(e) 所涉及的個人資料類別一覽表；
(f) 對外洩事件導致身分遭假冒的風險評估；
(g) 為防止個人資料在未經許可下更廣泛地被取閱而採取或將採取的措施；
(h) 有關受影響個別人士可獲得更多資料及協助的聯絡資料；以及
(i) 個別人士可如何保障自己的身分不被盜用或被假冒的資料及指引。

2.3 私隱專員的執行權力

建議4：授予私隱專員刑事調查及檢控權力

為加強保障個人資料私隱權，以及提升在私隱條例下的規管效率，私隱專員建議賦予他更多權力來執行私隱條例，本會深表認同。根據現行私隱條例，私隱專員擁有檢察權及調查權，但沒有檢控權力。有關檢控的工作主要由律政司負責及決定是否檢控。

根據《基本法》第六十三條，刑事檢控工作由律政司主管。然而，如在

私隱條例明文規定，根據條例提出的檢控，把檢控權授予私隱專員，並不違反《基本法》的規定。事實上，正如諮詢文件所述，現時亦有不少法定機構被賦權提出檢控，例如：職業訓練局、僱員補償援助基金管理局，建造業工人註冊管理局、證券及期貨事務監察委員會等。

因此，除私隱專員公署外，當局亦應同時檢討現行的平等機會委員會的權力，考慮立法授予其直接檢控的權力。

一如諮詢文件第5.03段所述，建議私隱專員應獲授予刑事調查和檢控罪行的權力，以及搜查和檢取證據等的附帶權力，有以下的原因：

(a) 私隱專員掌握在調查中取得的第一手資料，可以迅速對涉嫌干犯的罪行展開調查；
(b) 身為規管者，私隱專員擅於詮釋和引用私隱條例的條文，故此可以在任何特定的情況下，輕易地評估證據的分量和是否與案件相關；以及
(c) 節省把個案轉介警方進行調查的時間，有助在法定時限內，即由干犯罪行當日起計六個月內，提出檢控。

事實上，私隱專員作為保障市民個人資料私隱的守護者，其亦屬人權監察機制的一重要部份，專員公署應獲賦予超然獨立的地位，以履行保障個人資料的法定職責。公署的職能強調執行法例，有別於其他以提供公共服務為主的政府部門。若然專員缺乏任何刑事調查權及檢控權力，只會被公眾視為欠缺實權的「無牙老虎」，既不利執行法例，亦無助於私隱推廣工作。再者，若律政司、警務處或其他政府部門等出現涉嫌違反私隱條例的指控，律政司在檢控過程中便出現角色衝突的問題。以英國為例，當地的資訊專員辦公室(Information Commissioner's Office (ICO)) 便獲法例賦予獨立的刑事調查及檢控權力。

對於賦予刑事調查及檢控權力或誘發龐大公共資源的需要，這要視乎社會違反《個人資料(私隱)條例》的普遍性。在賦權後的首數年，當局必然要投放更多資源予公署就執行法例為公署人員提供相應的培訓工作。長遠而言，由於公署人員已熟悉了刑事調查的工作及檢控程序，在累積一定經驗後，相信需時亦大大縮短。

同理，為使私隱專員更有效地履行其執法及檢控工作，私隱專員亦應獲授權搜查及檢取證據，為檢控程序搜證。否則其刑事調查及檢控工作將難以全面進行。此外，當局亦應修訂私隱條例，賦予私隱專員在執行調查及視察工作時召喚公職人員提供協助。因此，若特區政府確實持開放態度，就建議4(即是否授予私隱專員刑事調查及檢控權力)進行公眾諮詢，則需同時就諮詢文件附件二第C.1及C.2項涉及私隱專員建議新增的權

力，一併納入建議部份諮詢市民大眾。

再者，持續的評估及評核，亦有助公署建立其專門能力，同時亦有助發掘執法和條例當中的不足之處，從以提出改善建議。諮詢文件第5.07段亦提出延長檢控的時限，目的就是回應因律政司檢控工作繁重，檢討時間緊迫的問題，本會同意延長檢控時限，亦相信在充份資源的配合下，由私隱專員公署進行檢控亦有助縮減提出檢控的時間。

建議5：在第66條下為資料當事人提供法律協助

根據現行私隱條例，任何資料當事人因任何資料使用者，就關乎他的個人資料違反條例下的規定而蒙受損害，有權根據條例第66條就該損害向有關的資料使用者申索補償。然而，私隱條例並無授權私隱專員在受屈資料當事人根據第66條提出訴訟方面，為其提供協助。這些個別人士除非合資格並成功取得法律援助，否則須自行承擔全部的訴訟費用。此等安排有欠妥善，因為法律援助署人員在考慮是否批出法律援助時，除進行經濟審查及案情審查外，亦會考慮申索人在訴訟中能否獲得一定可觀的利益。

因此，個別申索人可能因為在訴訟中所得利益甚微，而不獲批出法律援助。申索人不僅難以獲得法律救濟，同時一些涉及重大公眾利益的原則問題，亦未能透過法院裁決而得以釐清。

本會認為私隱條例應參考平機會根據反歧視條例的情況，私隱專員公署應獲授權為有意透過法律程序索取補償的個別人士提供協助，包括：(a)提供意見；(b)安排律師或大律師提供意見及協助；(c)安排由律師或大律師作代表；以及(d)提供平機會認為適當的任何協助。

另外，若有關個案涉及一個原則問題；或在顧及有關個案的複雜程度、申請人相對於答辯人或受牽涉的其他人的位置或任何其他事宜下，期望該名申請人，在沒有協助的情況下處理該個案並不合理，私隱專員公署亦應獲賦權提供法律協助。

建議6：向受屈的資料當事人判給補償

資料當事人若因資料使用者就關乎的個人資料違反私隱條例下的規定而蒙受損害，有權根據私隱條例提出申索補償。為簡化程序及減輕法庭的工作量，有建議認為應否授權私隱專員釐定補償額的方案，本會反對此項建議。一如法改會1994年8月發出的《保障個人資料的法律改革報告書》中的討論，賦予保障資料機構裁定給予補償的權力，會把執法和處罰的職能一併歸於單一機構，做法並不可取。

訓的職能一併歸於單一機構，做法並不可取。

因此，本會認為私隱專員的職責應只限於裁定有沒有保障資料原則遭違反。至於補償的適當款額，已屬法院管轄的範疇，應由法庭釐定。這亦有助制衡私隱專員公署的權力。當然，若受屈的資料當事人主動希望與投訴人作出調解，公署亦可協助調解進行，但最終補償的金額亦由雙方協商，而非由私隱專員判定。

2.4 罪行及制裁

建議7：把違反保障資料原則訂為罪行

目前，違反保障資料原則本身並非罪行。設立保障資料原則及執行通知的機制，目的是希望平衡個人資料私隱與維護其他人權和利益(包括公民自由和資訊自由)。然而，根據過往十多年私隱條例實踐的經驗看來，僅僅在違反發出執行通知，難收阻嚇之效。因此，法例應詳細就何種情況下違反保障資料原則，訂立刑事罪行以增加阻嚇力，從而反映問題的嚴重性。

如前文提及，若有人在處理敏感個人資料時，因疏忽而違反遵守保障資料原則，則私隱專員可發出執行通知(非刑事罪行)，若不遵從執行通知者，則始接受較重刑罰。若所涉及屬非敏感個人資料，刑罰將較輕，若屬敏感個人資料，刑罰將較重。

此外，本會認為，若有人因惡意或蓄意損害個人資料，則不論那是屬於敏感或非敏感個人資料，均應將有關行為定為刑事罪行予以檢控。為反映嚴重性，若涉及敏感個人資料，並惡意或蓄意下違反保障資料原則，被告人將要面對較高的刑罰。

建議8：在未經授權下取得、披露和出售個人資料

個人資料(不論屬敏感或非敏感)屬個人私隱，在未經授權下而取得、披露或作出售用途，明顯對資料當事人私隱的侵害，極有可能造成莫大傷害。現行私隱條例對以上行為主要以保障資料的第3原則(即個人資料的使用)作規管，卻未有將違反有關規的立入刑事管制。

事實上，傳媒不時亦有報導有市民的客戶個人資料被其他公司盜用，因此，為強化公眾教育及對個人資料使用方面的保障，本會認為有必要將未經授權下取得、披露和出售個人資料列作為刑事罪行。在罪行的意圖方面，若被告人理應只有知情或罔顧下取得、披露和出售個人資料，因此不涉及在疏忽下發生以上情況。對於因涉及意外而外洩個人資料，亦

不屬此罪行的範疇，有關立法條文可仿傚英國保障資料法令第55條的規定。

此外，由於在某些情況下或需在資料當事人沒有同意下披露有關個人資料，因此，法例亦應同時引入以下抗辯的理由：

(a) 為防止或偵查罪行而必須的；
(b) 任何成文法則、法律規則或法庭命令所規定或經有關法則、規則或命令授權；
(c) 該人有理由相信他獲法律賦與權利取得、披露或促使披露有關個人資料；
(d) 該人有理由相信假如資料控制者得知他取得、披露或促使披露有關個人資料，資料控制者會同意該些行為；
(e) 取得、披露或促使披露有關個人資料的行為在特定情況下符合公眾利益；
(f) 該人為了特別目的取得、披露或促使披露有關個人資料，供任何人用作任何新聞、文學或藝術材料的發布，他並有理由相信有關舉動符合公眾利益。

互聯網應用方面，有論者或擔心新的罪行阻礙正常的網上瀏覽或資料傳播，本會認為，若互聯網使用者將個人資料放在網站上，則有關個人資料的使用目的，使要視乎該網站的性質(例如：社交網站、討論區等)，資料當事人對其私隱的合理期望理應有所不同。然而，儘管如此，若有人主動地在下載個人資料，即可被視為知情下下載，若因電腦軟件自行運作地無意中發放了個人資料，即不屬建議罪行中範疇。

建議9：就同一事實重複違反保障資料原則

若有人或機構違反保障資料原則，並按私隱專員的執行通知指示更正，但其後又故意重複執行通知所涉及的行為或做法，現行法例並未有將有關情況訂為刑事罪行。本會認為，縱使自私隱條例頒布以來，私隱專員未有遇到類似的迴避規管情況，但這並不代表問題的嚴重性不高。事實上，若有人或機構是以在短期內重複違反有關通知，儼如早前的執行通知未能有效獲得遵從。本會認為有必要將有關情況訂為刑事罪行，重複就同一事件違反保障資料原則有別於僅一次違反原則的情況，因此可以增加刑罰。

然而，有關情況必須涉及同一事實違反保護資料原則，再者，若同一事實違反保護資料原則的事件兩次事隔太久，或對被資料使用者或資料處理者帶來不公，因此，建議亦引入時效條款(例如：一年、兩年等)，避免有人或有機構因可多前違反保護資料原則，數年或十多年後因同一事實

違反有關原則而需負上刑事責任。

建議10：就嚴重違反保障資料原則處以罰款

另一方面，諮詢文件討論應否授權予私隱專員就嚴重違反保障資料原則判處罰款；對此，本會並不贊成有關建議。首先，私隱專員主要責任是執行私隱條例的實施，肩負執法者的角色，若果賦予罰款的權力，私隱專員便需兼任司法機關的審判角色。換言之，私隱專員既有執法者亦是審裁者的雙重身份，明顯出現角色衝突，安排上有違程序公義，亦難以有其他部門加以制約及監察其權利。

再者，定義如何屬「嚴重」違反保障資料原則亦十分困難，當中涉及頗為主觀的判斷，就是私隱專員認為事件對個別受影響人士影響不深，惟對資料當事人而然亦可能影響深遠。因此，若以「嚴重」與否來區分是否處以罰款，執行上難顯公平，當中亦涉及原則性問題，因此，本會反對引入嚴重違反是處以罰款的建議。

建議11：重複違反執行通知

目前，根據私隱條例第64(7)條，資料使用者違反私隱專員發出的執行通知，即屬犯罪。一經定罪，資料使用者可被處以第5級罰款（最高可達50,000元）及監禁兩年；如屬持續罪行，可處每日罰款1,000元。對於重複違反執行通知的資料使用者而言，本會認同需處以更重的懲罰，以制裁違反執行通知的規定。本會建議若有人或有機構屢次違反條例，法例應賦予法庭更大的自由裁量權，處以法庭認為合適的刑罰，量刑參考因素包括：違反執行通知的持續時期、被告人/機構在發出執行通知後所採取的措施、違反有關原則對受影響的資料當事人的影響嚴重程度等。

建議12：提高在直接促銷中不當使用個人資料的罰則

私隱條例第34條規管資料使用者，把個人資料用於直接促銷活動。依據該條例第34(1)(ii)條，如資料當事人曾要求資料使用者，停止把其個人資料用於直接促銷，則資料使用者不得將任何該等資料用於直接促銷。任何資料使用者無合理辯解而違反第34(1)(ii)條的規定，即屬犯罪，一經定罪，根據第64(10)條可處第3級罰款（最高可達10,000元）。

過去三年(2006年至2008年)，私隱專員每年分別接獲不足100宗的投訴，而成功檢控的數字亦偏低。隨著直銷活動在市場日漸普及，相信有關投訴會有增無減。再者，現行最高刑罰僅一萬元，對大公司阻嚇力不大。

因此，本會認同需加重刑罰，法例亦應賦予法庭更大的自由裁量權，處

以法庭認為合適的刑罰，量刑參考因素包括：違反執行通知的持續時期、被告人/機構在發出執行通知後所採取的措施、違反有關原則對受影響的資料當事人的影響嚴重程度等。

2.5 其他建議

(A) 資料當事人的權利

建議13：由第三者給予訂明同意更改個人資料用途

現行私隱條例並沒有條文准許一名人士，代一名資料當事人同意更改其個人資料的用途。若干資料當事人，例如未成年人或精神上無行為能力的人，未必具有智力與能力明白和理解資料使用者更改其個人資料用途對其私隱的影響。本會認為有關建議有助維護資料當事人的重要利益，同意當局可訂立一套制度，賦予第三者更改該資料當事人的個人資料的用途。

然而，第三者在決定更改該資料當事人的個人資料的用途之前，其必須採取以下的程序，包括：向資料當事人通報有關決定、向資料當事人查詢其意見(如有能力理解)、向私隱專員公署通報以紀錄備忘等。

法例亦應訂立評核機制，定期覆檢(例如：每一年)該第三者是否仍然適合代表資料當事人同意更改其個人資料(例如：參考未成年人的年齡及心智成熟程度、精神上無行為能力的人的復康進度等)。此外，若資料當事人不滿有關第三者的安排，當事人亦可向私隱專員公署或法庭等機制提出上訴申請，以檢測有關第三者的安排是否合適。

建議14：父母親查閱未成年人士個人資料的權利

父母有法律責任妥善照顧其18歲以下的子女，包括照顧兒童健康、教育及其他兒童或青少年事務。現行私隱法例亦規定「有關人士」包括未成年人負有作為父母親的責任的人。然而，父親或母親亦有可能濫用查閱子女個人資料機制的可能。由於未成年人與父母涉及其個人資料的問題千變萬化，本會認為私隱條例應加入新的條文，准許資料使用者衡量有否合理理由下，決定拒絕一位代表一名未成年人的「有關人士」(例如：其父母)提出的查閱資料要求，以保障未成年人的利益。

條例亦應規定資料使用者在決定是否向「有關人士」提供所需的個人資料時，需考慮以下因素，建議包括：

(a) 父親或母親查閱資料的目的是否符合管教、照顧子女的目的；
(b) 父親或母親是否懷疑曾虐待子女；
(c) 未成年人士有否向資料使用者表明，不同意使用者向其父母親透露其個人資料；
(d) 查閱該項的個人資料是否存有合法目的(legitimate aim)；
(e) 查閱的個人資料是否有合理關係(rationally connected)；
(f) 查閱的個人資料是否合乎該目的比例(proportionate)，查閱的是否不多於需要達致的目的(no more than necessary)；
(g) 查閱資料會否損害未成年人士的最大利益(the best interest of the minor)。

建議15：查閱受爭議的個人資料

一名資料當事人可向私隱專員投訴一名資料使用者，指後者未能依從他查閱其個人資料的要求。當感到受屈的人士申請司法覆核時，與該司法程序有關的人士亦享有獲得披露該等文件的權利。但是私隱條例卻沒有條文禁止在上訴或司法覆核時，出示要求的資料。

為此，本會同意香港仿傚英國保障資料法令修訂現行私隱條例，將由行政上訴委員會、法庭或裁判法院進行聆訊時，在要求資料一方被判得直前，不得以披露或其他形式向資料要求者或其他受行政上訴委員會、法庭或裁判法院的決定所約束的人士披露案件所涉的個人資料。

(B) 資料使用者的權利及義務

建議16：為遵從其他條例而拒絕依從查閱資料要求

私隱條例第19條規定，資料使用者須在收到查閱資料要求後依從該項要求，惟可按第20條所載的各項理由及第28(5)條拒絕依從要求。可是，拒絕理由沒有包括資料使用者根據其他條例，有義務或有權不披露資料的情況。

為此，本會同意諮詢文件建議，本港可仿傚澳洲、新西蘭及英國的個人資料私隱法例，訂定豁免條款，遇有其他條例訂明法定要求，不得披露資料時，資料當事人毋需依從有關查閱個人資料要求的規定。然而，由於在某些情況下，披露要求的個人資料的利益或較法例賦予的責任(例如：保密法定責任、不披露資料責任等)更為重要，因此，法例亦應訂明有關爭議最終可由法庭裁決定斷。

建議17：刪除個人資料

根據私隱條例第26條，凡資料使用者持有的個人資料已不再因為原有使用目的(包括任何直接有關的目的)而有需要保留，資料使用者須刪除該等資料，除非任何法律禁止刪除該等資料，或不刪除該等資料符合公眾利益(包括歷史方面的利益)。

本會同意參考其他海外司法管轄區(包括澳洲、加拿大、新西蘭及英國)，如資料使用者已採取合理可行的步驟，刪除過時的個人資料，使用者一般被視作已履行類似的要求，而不會被視作為觸犯私隱條例。

建議18：處理查閱資料要求所收取的費用

私隱條例第28(2)條規定，資料使用者可為依從查閱資料要求，就需要提供的個人資料副本向要求者徵收費用。第28(3)條規定，所徵收的費用不得超乎適度。事實上，不少市民亦曾投訴有資料使用者，就按查閱資料要求提供所需要的資料而徵收的費用差別很大，更投訴人表示收費過高。

因此，本會認為應否規定資料使用者依從查閱資料要求所徵收的費用，不得高於私隱條例內收費附表列出的訂明最高收費，另建議訂明最高收費參數如下：

	$/每張最高收費
影印本	2
電腦打印本	2
錄音或錄像的CD-ROM/DVD+R光碟副本	50
放射診斷造影記錄副本 (例如：X光片、磁力共振掃描、電腦斷層掃描、正電子放射斷層掃描、超音波)	100
錄音的謄抄本	80
郵費	按實際支出而定
速遞費	按實際支出而定
人手和找出、檢索和複製所要求的個人資料	按實際支出而定

建議19：在40日內以書面回覆查閱資料要求

現時私隱條例並無明文規定，資料使用者如沒有持有要求的個人資料，須以書面通知要求者。這安排明顯不符合私隱條例的立法意圖。縱使查閱的資料涉及個人刑事犯罪紀錄，而警方並未持有該資料則屬例外；警

方亦應以書面回覆。警方不可因擔心發出的無犯罪紀錄證明書遭人偽造/擅自塗改而不發出書面文件，因此偽造/擅自塗改屬刑事罪行，干犯者需負上刑責，況且，若所言屬實，莫非所有書面文件均應以口頭處理？再者，若書面文件回覆的接收者改由僱主，亦可減少偽造/擅自塗改書面文件的情況。

因此，本會認為應規定資料使用者如無持有要求查閱的個人資料，須在40日內以書面回覆要求者，以配合私隱條例的立法目的。

(C) 私隱專員的執法權力

建議20：在何種情況下發出執行通知

私隱條例第50條規定，私隱專員在完成調查後，可向資料使用者發出執行通知，指示資料使用者按通知所指明的步驟，糾正導致發出該通知的違反行為或事宜。然而，即使有關作為已對資料當事人造成傷害或損害，如資料使用者已停止有關作為或行為，而有關作為或行為不可能重複發生，私隱專員則不能向資料使用者發出執行通知。

為此，本會同意，在以下任何情況，私隱專員可向資料使用者發出執行通知：

(a) 資料使用者正違反私隱條例下的規定；
(b) 違反行為將持續或會重複發生；
(c) 違反行為已對或相當可能對資料當事人造成損害或困擾。

建議21：澄清在執行通知中指示糾正違規行為的權力

私隱條例第50(1)條規定，私隱專員須在執行通知內，指明資料使用者須在期限內，採取步驟糾正違規事項。據了解，私隱專員認為，有關資料使用者應停止作出某項作為或行為，在通知內指明依從的期限，並不恰當。本會認為以上僅為字眼表達問題，儘管不修訂第50(1)條，私隱專員仍可在執行通知內指令資料使用者停止作出某項作為或行為。

建議22：取消中止調查的時限

私隱條例第39(3)條規定，如私隱專員拒絕繼續進行一項由投訴引發的調查，他須於收到該項投訴後的45日內通知投訴人。雖然現行平機會、申訴專員公署及海外私隱機構均不受類似的法定規定所限，即無須在指定期間內，把拒絕進行或繼續進行某項調查的決定通知投訴人。然而，本會認為現存規定明確，讓投訴人可在預期的時限內清楚私隱專員的決定，因此建議繼續保留有關規定，其他人權監察機構亦應考慮仿傚以上

規定。

建議23：拒絕調查的新增理據

在私隱條例第38條下，私隱專員接獲投訴後，除第39條另有規定下，會對有關資料使用者進行調查，確定投訴所指的作為或行為，是否有違私隱條例的規定為更好地限制私隱專員行使其酌情權，諮詢文件建議將私隱專員以往通常拒絕進行或拒絕繼續進行調查的依據，引入法例中，包括

(a) 投訴的主因與個人資料私隱無關； (b) 另一規管機構正就或即將就投訴關乎的行動展開調查；或(c) 如投訴所指的作為或行為與個人資料或載有個人資料的文件有關，而所涉及的資料已在或相當可能在任何裁判法院、法庭、審裁處、委員會、規管或執法機構的法律程序或研訊的某個階段使用。

本會同意引入(a)項，但反對引入(b)項。因為縱使另一規管機構展開調查，其調查重點並不是與私隱有關係，因此私隱專員公署沒有必要而拒絕調查。另外，為尊重其他司法或類司法機構的法律程序，本會亦同意引入(c)項，惟有關資料必須已經(而不包括相當可能)被該等機構使用。

(D) 新增豁免條文

建議24：商業併購過程中個人資料的轉移

商業合併、重組、轉讓或業務買賣在盡職辦理之時，一方或須向另一方披露或轉移所持內含個人資料的業務資料，以供核查評估。再者，一如諮詢文件所言，併購行動分秒必爭，要在轉移有關資料前取得資料當事人的訂明同意，會對併購造成障礙。再者，有關方面或確有需要在盡職辦理之時對交易嚴加保密。為此，本會同意本港私隱條例引入特定條文，容許因應業務買賣、合併或重組轉移個人資料，惟須符合諮詢文件第52段列出的條件：

(a) 組成後的機構或業務承讓方向資料當事人所提供的服務，基本上應與原資料使用者所提供者相同或類似；
(b) 要取得資料當事人的訂明同意，把其個人資料作有關用途，並不切實可行；
(c) 所披露的個人資料對盡職處理來說是必要而非過多的；
(d) 承讓方只限在盡職處理指明範圍內，使用及處理有關個人資料，除非已取得資料當事人的訂明同意，或使用有關個人資料是私隱條例所容許或豁免；
(e) 如交易並沒有進行或並無完成，所轉移的個人資料須妥為銷毀或

退還轉讓方；以及
(f) 若有關商業交易的主要目的、目標或結果是購買、售賣、租用、轉讓、處置或披露個人資料，則有關豁免並不適用。

建議25：基於健康理由提供身分和所在地資料

私隱條例第59條規定，與資料當事人的身體健康或精神健康有關的個人資料，若按使用個人資料原則（第3原則）和查閱個人資料原則（第6原則）的規定處理，可能對資料當事人或任何其他人士的身體健康或精神健康造成嚴重損害，可獲豁免不受管限。不過，有關豁免不適用於提供資料當事人的所在地和身分等其他類別的個人資料。

本會同意修訂私隱條例第59條，將豁免的適用範圍，擴大至包括資料當事人的身分和所在地的個人資料。

建議26：在緊急情況下處理個人資料

如同建議25，由第三者向有關機構提供的個人資料的限制不利進行與救援工作有關的個人資料，因此，遇有執法機構、救援及支援機構執行救援及支援工作時，建議豁免這些機構遵從保障資料第1(3)項原則及第3項原則：(a) 尋找牽涉或有理由相信可能牽涉在意外或其他危及生命的情況的人；(b) 通知(a)項所指人士的家人有關人士遇上意外等；以及(c) 便利提供救援予(a)項所指人士。

建議27：為了履行監護責任和家長照顧責任而把未成年人的個人資料轉移

教養兒童和協助他們成長是父母及監護人的基本責任。如父母及監護人無法合理查閱其子女／監護兒童的個人資料，便未必能有效地履行他們的責任。然而，社會並不可隨意地忽略未成年人的個人私隱。

現行私隱條例第18(1)條容許未成年人的父母或監護人，查閱有關未成年人的個人資料，但條例<u>並無容許資料使用者主動</u>把未成年人的個人資料轉移給其父母或監護人。

為此，本會同意可在私隱法例中，訂明未成年人的個人資料與家長和監護人分別履行照顧及監護責任有關，容許資料使用者把該等資料轉移給未成年人的父母或監護人，以便他們可以更好地履行本身的責任，適當地照顧和監護其18歲以下的兒童。值得注意的是，有關規定必須適用於所有未成年人，而不應劃分所謂邊緣青年或高危青少年，否則只會做成負面標籤，亦有損這些所有未成年人均應享有相同私隱保障的原則。

然而，一如建議14分析所言，條例亦應規定資料使用者在主動向父母親或監護人提供有關未成年人的個人資料時，亦需考慮以下因素，包括：

(a) 父親或母親查閱資料的目的是否符合管教、照顧子女的目的；
(b) 父親或母親是否懷疑曾虐待子女；
(c) 未成年人士有否向資料使用者表明，不同意使用者向其父母親透露其個人資料；
(d) 查閱該項的個人資料是否存有合法目的(legitimate aim)；
(e) 查閱的個人資料是否有合理關係(rationally connected)；
(f) 查閱的個人資料是否合乎該目的比例(proportionate)，查閱的是否不多於需要達致的目的(no more than necessary)；
(g) 查閱資料會否損害未成年人士的最大利益(the best interest of the minor)。

3. 其他建議

3.1 改革私隱專員公署以加強問責

私隱專員公署作為法定組織，是執行私隱條例及維護市民私隱權益的重要機制。然而，過去十多年，這關乎人權保障的機制不單缺乏足夠權力以履行私隱權保障的責任，而且私隱專員這重要職位的任命全掌握在政府手中令公眾難以監察，因而專員與公署完全沒有向公眾問責，凡此種種不但違反國際公認的保護人權國家機構的設立原則，也令私隱專員公署（以及平機會）等法定人權機構容易變成獨立王國，在行政以至財政使用上都容易出現弊病。

聯合國大會於1994年通過了《促進和保護人權的國家機構》的決議，確認了“關於（促進和保護人權的）國家機構的地位的原則”（俗稱“巴黎原則”）。該原則規定促進人權機構的組成及其成員的任命，“不論是通過選舉產生還是通過其他方式產生，必須按照一定程序予以確定，這一程序應提供一切必要保障，以確保參與促進和保護人權的社會力量的多元代表性”；然而，現時私隱專員公署由私隱專員一人作主要決策，而其任命完全由行政長官一人決定，這在公署組成以至專員人選決定過程均完全缺乏應有的社會多元代表力量參與。

為此，本會強烈認為，要令私隱專員公署有效保障人權、加強問責及加強其獨立性，當局必須全面修訂私隱條例以改組公署，透過民間社會的多元參與以加強私隱專員公署的代表性、問責性和獨立性。

3.2 儘快實施私隱條例第33條

諮詢文件附件2第A.3部份提及，目前，資料使用者在香港或從香港控制資料的處理，即使整個資料處理過程在香港以外地方進行，均受私隱條例規管。然而，有關規定完全不足以保障香港市民的個人資料不被不合理地移轉至香港以外地方。根據現行私隱法例，有關移轉個人資料至香港以外地方，主要由該條例第33條規定。條例第33條禁止個人資料移轉至沒有類似香港保障個人資料的地區，然而，該條在私隱法例生效十多年後，至今仍未實施。因此，縱使資料使用者或資料處理者，在香港以外地方以不合乎個人保障資料原則的方式處理個人資料時，私隱專員亦極難監管。

按照條例第33條規定，條文一旦生效，專員便可藉憲報公告，為本條的施行指明該地方。有見很多企業及跨國公司均將其業務移轉至海外，當中涉及收集、持有、處理、使用個人資料，當局有必要儘快公佈實施條例第33條，以完善保障個人資料。

另一方面，現時條例第33條並沒有要求資料使用者或資料處理者，在移轉個人資料至香港境外後必須通知私隱專員。有見私隱專員缺乏足夠資源在境外監管，本會同時建議訂立法定責任，規定資料使用者或資料處理者在轉移個人資料時需向私隱專員通報，以強化公署的監管。這也有利日後個人資料外洩或遺失的調查工作。

3.3 儘快落實各項保障私隱權立法

事實上，現行私隱條例僅保障個人資料免受侵害，涵蓋範疇極為有限；個人私隱權所涉範圍甚廣，包括：免受纏繞、秘密監視、監察或偷聽等，甚至個人私隱受侵害時，能否獲得充分的民事救濟途徑亦極為重要。法律改革委員會過去十多年先後推出多份報告書[1]，建議立法機關儘快完善涉及保護私隱權的立法。因此，當局若然決心保障個人私隱，除了儘快落實修訂保障個人資料方面的私隱條例以外，更應將法改會各項立法建議納入日程上，儘快制訂立法時間表，以求對私隱權有更全面的保障。

《香港人權法案》第十四條規定："(一)任何人之私生活、家庭、住宅或通信，不得無理或非法侵擾，其名譽及信用，亦不得非法破壞。(二)對於此種侵擾或破壞，人人有受法律保護之權利。"有關的人權法明確規定了政府有需要透過立法以全面保障當地人民的私隱不受任何（包括政府及私人）的無理及非法侵擾，因此政府更有法律責任全面立法保障港人的私隱權。

4. 本會主要建議一覽

(1) 訂立“敏感個人資料”類別，並對敏感資料提供較高程度的保障；
(2) 加入規管資料處理的分判活動；
(3) 設立資料外洩通報機制，強制要求外洩資料者必須向私隱專員公署及受害人通報；
(4) 授予私隱專員刑事調查及檢控權；
(5) 授權私隱專員公署為資料當事人提供法律協助；
(6) 把惡意或蓄意損害個人資料列為刑事罪行；
(7) 把未經授權下取得、披露和出售個人資料列為刑事罪行；
(8) 修訂法例以加強私隱專員公署組成的民間代表性、問責性及獨立性；
(9) 實施私隱條例中有關規管不得隨意將個人資料移轉至外地的條文；及
(10) 儘快跟進法改會過往報告的建議，全面立法加強對市民各方面私隱權的保障。

5. 結語

以上分析簡要地回應諮詢文件各項主要建議。本會強調，隨著市民及國際社會對私隱權的意識及訴求日益提高，修訂《個人資料(私隱)條例》的工作實刻不容緩。本會促請當局在公眾諮詢期屆滿後，儘快展開立法工作。與此同時，特區政府亦應訂立時間表，落實其他涉及保障私隱權的立法建議，讓個人私隱受侵害時，可獲得法律救濟，否則私隱權只會淪為空談，徒具實質意義。

二零零九年十一月

聯絡： 何喜華(主任) 電話： (刪除) 傳呼： (刪除)

蔡耀昌 (社區組織幹事) 電話： (刪除)
王智源 (社區組織幹事) 電話： (刪除)

[1] 法律改革委員會自1993年開始，就涉及私隱課題進行諮詢及研究，並先後發出以下報告書，包括：纏擾行爲(2000年10月)、侵犯私隱的民事責任(2004年12月)、傳播媒介的侵犯私隱行爲(2004年12月)。然而，以上三份報告書中所有立法或修訂法例的建議均未有落實。
此外，法改會在2006年3月發出《私隱權：規管秘密監察報告書》，當局亦在同年提交《截取通訊及監察條例草案》（即其後立法制定的2006年第20號條例），內容反映了法改會的部分建議；然而，有關條例僅規管執法部門進行截取通訊及監察的程序，卻未有規管私人之間截取通訊及監察行爲。



SoCO privacy ordinance review_position paper_2009_11.doc



privacy survey summary report_2009_11.doc

(此附件與電郵內容相同，因此不重覆連載)

香港社區組織協會 民權法律中心

S0132

市民對個人私隱及私隱法例認識調查報告

(2009 年 11 月)

1. 前 言

香港特別行政區政府在個人資料私隱專員的協助下，決定全面檢討現行《個人資料(私隱)條例》(下稱「私隱條例」)，並展開為期三個月的公眾諮詢。為此，進一步了解市民對現存個人私隱及私隱法例的認識，本會於 2009 年 9 月至 10 月期間進行問卷調查，搜集市民對諮詢文件的意見，結果簡要如下：

2. 調查結果

2.1 對私隱條例的認識

是次問卷調查共訪問了 213 名本港市民，被問及有否聽過《個人資料(私隱)條例》時，絕大部份受訪者(94.7%)均表示曾聽過《私隱條例》。(表 1)然而，受訪者普遍對《私隱條例》中的個人資料的定義並不太掌握。最多受訪者(85.4%)認為電話號碼屬個人資料、五成多(56.5%)的受訪者認為姓名及受僱紀錄屬個人資料。此外，只有不足一半(47.3%)受訪者認為相片屬個人資料，表示其餘類別屬個人資料的受訪者亦僅四成多或以下，工作表現評核(44.9%)、職業(37.7%)、宗教信仰(23.7%)。(表 2)在《個人資料(私隱)條例》保障人士方面，超過一半受訪者(53.7%)條例保障在世及去世人士，四成多(44.8%)表示只保障在世人士，極少數(1.5%)受訪者認為法例只保障去世人士。(表 3)

2.2 侵犯個人私隱經歷

在個人私隱受侵犯的經歷方面，七成多(72.5%)受訪者表示沒有曾經遇到懷疑被侵犯個人私隱，但亦有二成多(27.5%)受訪者表示曾遇到懷疑個人私隱受侵犯的情況。(表 4)被問及曾懷疑被侵犯私隱的受訪者時，不足一成(9.4%)表示有就以上經歷向公署作出投訴。(表 5)而在曾向私隱專員公署投訴的人士當中，亦僅一成多(18.6%)投訴個案表示投訴成立。(表 6)此外，其餘曾遇到懷疑私隱受侵害的受訪者，他們不向公署投訴的最主要原因是不想小事化大(41.2%)、不知道有此投訴渠道(33.3%)、表示沒有錢投訴(28.9%)、甚至認為沒有幫助(23.7%)或浪費時間(14.9%)。(表 7)

2.3 對諮詢文件建議的意見

調查亦訪問受訪者對政府當局擬備的諮詢文件之意見，他們對各項建議意見如下(表 8)：

- 九成以上的受訪者(91.4%)認為現行法例沒有區別「個人資料」是否屬敏感(例如：指紋、血型、基因資料等)或非敏感(例如：姓名、地址等)，認為法例應就敏感個人資料作更嚴格的規管；
- 絕大部份受訪者(95.2%)認為若發生個人資料外洩事故時，法例應規定必須通知私隱專員及受影響人士；
- 近九成受訪者(87.3%)認為法例應賦予私隱專員搜查及檢取證據權力，以便進行刑事檢

控；並賦予私隱專員刑事檢控的權力(90.1%)；

- 絕大部份受訪者(94.7%)認為私隱專員應為受影響的資料當事人提供法律協助，並有權向受影響的資料當事人判處補償(88.8%)；
- 受訪者均普遍認為(92.3%)，若披露未經資料使用者同意下取得的個人資料而從中取利或作惡意用途的行為，應將之訂為罪行。此外，近九成(88.7%)亦認為，假若資料使用者已遵行私隱專員發出的執行通知的規定改正，但不久又故意重犯，則應訂定為罪行；
- 另方面，超過一半(53.1%)受訪者認為法例應授權予第三者，讓第三者有權更改未成年人或精神上無行為能力的人的個人資料用途，四成多(46.9)受訪者認為不應該；
- 另外，近六成(59.8%)受訪者表示，若有父親或母親向持有未成年子女的第三方，要求代其子女查閱資料，但要求並不符子女最佳利益，法例亦應准許第三方拒絕該查閱要求，但亦有四成多(40.2%)受訪者表示反對。

2.4 受訪者資料

是次調查受訪者八成(80.8%)為女性，其餘則為男性(19.2%)(表 9)；最多受訪者年齡介乎 26 至 40 歲(40.9%)，其餘則為 41 至 60 歲(22.8%)、11 歲或以下(10.9%)、18 至 25 歲(10.4%)、12 至 17 歲(8.8%)及 60 歲以上(6.2%)(表 10)。職業方面，近半受訪者(48.8%)職業為家庭主婦、三成多(30.6%)為學生、在職人士(11.8%)、其餘則屬待業(4.1%)或退休人士(4.7%)等(表 11)。

3. 研究分析及建議

3.1 市民對私隱權及私隱條例認識不深

是次調查發現，受訪市民普遍對《私隱條例》的條文並不認識。也許近年市民對個人私隱問題的關注有所增加，然而，這並不代表市民真正掌握個人私隱的概念。舉例來說，調查曾詢問受訪者對個人資料定義的認知，惟超過一半受訪者均誤以為相片、工作表現評核、職業、宗教信仰不屬於個人資料，更有過半數受訪者表示私隱條例保障在世及去世，或只有在世人士，可見公眾對條例的認識仍停留在極低階段，當局有必要加強私隱教育及推廣。

此外，政府亦應將有關涉及人權及公民權利的相關法例及概念，列入各中、小學的教育課程大綱，規定學校需向學童灌輸私隱、反歧視及平等機會等人權概念，藉以提高公民對人權的認識。另外，當局亦應規定任職公務員及公營部門的職位的申請人，在投考時必須通過有關人權教育的考核，以確保公職人員對個人私隱及其他人權概念的認識和關注。

3.2 加強私隱專員法定權力、優化現行投訴機制

雖然大部份受訪者表示未曾遇到懷疑被侵犯個人私隱，惟觀乎他們對私隱概念的掌握，極有可能曾被侵犯卻不自知，因此所謂未曾遇到的回應不一定盡然反映實況。另外，在表示曾遇到懷疑個人私隱受侵犯的個案中，普遍亦沒有公署投訴，究其原因，當中包括市民不想小事化大或不知道有此投訴渠道，然而，有效而便捷的投訴機制，亦有助鼓勵懷疑受侵犯的市民作出投訴。這不僅需要簡化投訴程序，更要修訂法例，容讓私隱專員具有實權執行保障私隱的職責及投訴工作。

事實上，處理投訴的效率亦直接影響市民的投訴意欲。舉例而言，近日審計署報告批評私隱專員公署的處理投訴日數太長，發現超過 180 天的法定期限(截至 2009 年 6 月，案齡超過 180 天的逾期個案有 33 宗，平均案齡達 426 天)。[1]這既反映現行投訴機制效率不高，但同時亦揭示私隱專員缺乏充足調查權力，從而儘早完成投訴調查工作。因此，除了要加強公署的工作效率外，亦要檢討如何加強私隱專員的調查權力，這亦回應是次當局展開公眾諮詢的內容。

3.3 儘快落實諮詢文件各項建議

當局發出的諮詢文件，當中提出多項修訂法例的建議，受訪者大多對各項建議表示支持，當中包括：區分敏感個人資料以作更嚴格規管、個人資料外洩事故時需依法通知私隱專員及受影響人士、賦予私隱專員搜查及檢取證據權力，以便進行刑事檢控、為資料當事人提供法律協助、將利用個人資料從中取利或作惡意用途訂為罪行、將屢次違反專員通知的行為訂為罪行。

此外，較大爭議的建議包括應否授權予第三者更改未成年人或精神上無行為能力的人的個人資料用途、以及若父或母親向持有未成年子女的第三方，要求代其子女查閱資料，但要求並不符子女最佳利益，法例應否准許第三方拒絕該查閱要求，較多受訪者表示有所保留。雖然以上兩項建議賦予第三者較大的法定權力，有論者亦擔心會影響父母教育子女的天職，但為顧及未成年人士或精神上無行為能力的人最大利益之前提下，有關修訂亦屬必須。(詳細修訂法例建議參見本會的意見書)[2]

2009 年 11 月 30 日

聯絡： **何喜華 (主任)** **電話：** (刪除) **傳呼：** (刪除)
蔡耀昌 (社區組織幹事) **電話：** (刪除)
王智源 (社區組織幹事) **電話：** (刪除)

[1] 審計署署長第五十三號報告書(2009 年 10 月) 第 9 章：個人資料私隱專員公署 http://www.aud.gov.hk/chi/pubpr_arpt/rpt_53.htm
[2] 香港社區組織協會 民權法律中心 (2009 年 9 月) 回應檢討《個人資料(私隱)條例》諮詢文件意見書

調查圖表

S0132

表 1 你有沒有聽過《個人資料(私隱)條例》？

	選擇人數	百分比
有	197	94.7
沒有	11	5.3
合計	208	100.0

遺失個案: 5 個

表 2 據你所知，根據個人資料(私隱)條例規定，下列那些屬個人資料？ (可選擇多於一項)

	認為屬於個人資料的 選擇人數(百分比)	認為不屬於個人資料的 選擇人數(百分比)
姓名	117 (56.5%)	90 (43.5%)
電話號碼	176 (85.4%)	30 (14.6%)
性別	52 (25.1%)	155 (74.9%)
職業	78 (37.7%)	129 (62.3%)
宗教信仰	49 (23.7%)	158 (76.3%)
相片	98 (47.3%)	109 (52.7%)
受僱紀錄	117 (56.5%)	90 (43.5%)
工作表現評核	93 (44.9%)	114 (55.1%)

表 3 據你所知，那些人士受《個人資料(私隱)條例》保障？

	選擇人數	百分比
在世人士	91	44.8
去世人士	3	1.5
在世及去世人士	109	53.7
合計	203	100.0

遺失個案: 10 個

表 4 你有沒有曾經遇到懷疑被侵犯個人私隱的情況？

	選擇人數	百分比
有	53	27.5
沒有	140	72.5
合計	193	100.0

遺失個案: 20 個

表 5 有沒有就以上經歷向私隱專員公署作出投訴？

	選擇人數	百分比
有	5	4.3
沒有	110	95.7
合計	115	100.0

遺失個案: 98 個

表 6 投訴結果為何？

S0132

	選擇人數	百分比
成立	8	18.6
不成立	6	14.0
未有結果	28	65.1
其他	1	2.3
合計	43	100.0

遺失個案: 170 個

表 7 為何不向私隱專員公署投訴？ (可選擇多於一項)

	選擇人數	百分比	總回應人數
不知道有這渠道	38	34.2%	111
不想小事化大	47	41.2%	114
認為沒有幫助	27	23.3%	116
浪費時間	17	14.8%	115
沒有錢投訴	33	28.7%	115

表 8 近日政府就檢討《個人資料(私隱)條例》進行公眾諮詢，我們想問問你的意見：

	應該 (%)	不應該 (%)	總回應人數
1. 現行法例沒有區別「個人資料」是否屬敏感(例如：指紋、血型、基因資料等)或非敏感(例如：姓名、地址等)，你認為法例應否就敏感個人資料作更嚴格的規管？	192 (91.4%)	18 (8.6%)	210 (100%)
2. 若發生個人資料外洩事故時，法例應否規定必須通知私隱專員及受影響人士？	199 (95.2%)	10 (4.8%)	204 (100%)
3. 應否賦予私隱專員搜查及檢取證據權力，以便進行刑事檢控？	178 (87.3%)	26 (12.7%)	202 (100%)
4. 應否賦予私隱專員刑事檢控的權力？	182 (90.1%)	20 (9.9%)	202 (100%)
5. 私隱專員應否為受影響的資料當事人提供法律協助？	196 (94.7%)	11 (5.3%)	207 (100%)
6. 私隱專員應否有權向受影響的資料當事人判處補償？	183 (88.8%)	23 (11.2%)	206 (100%)
7. 披露未經資料使用者同意下取得的個人資料而從中取利或作惡意用途的行為應否訂為罪行？	191 (92.3%)	16 (7.7%)	207 (100%)
8. 你認為應否把資料使用者已遵行私隱專員發出的執行通知的規定，但不久又故意重犯的行為訂為罪行？	181 (88.7%)	23 (11.3%)	204 (100%)
9. 你認為應否授權第三者，讓第三者有權更改未成年人或精神上無行為能力的人的個人資料用途？	110 (53.1%)	97 (46.9%)	207 (100%)
10. 如果有父或母親向持有未成年子女的第三方，要求代其子女查閱資料，但要求並不符子女最佳利益，法例應否准許第三方拒絕該查閱要求？	122 (59.8%)	82 (40.2%)	204 (100%)

表 9 受訪者的性別

	選擇人數	百分比
男	40	19.2
女	168	80.8
合計	208	100.0

遺失個案: 5 個

表 10 受訪者的年齡

	選擇人數	百分比
11 歲或以下	21	10.9
12 至 17 歲	17	8.8
18 至 25 歲	20	10.4
26 至 40 歲	79	40.9
41 至 60 歲	44	22.8
60 歲以上	12	6.2
合計	193	100.0

遺失個案: 20 個

表 11 受訪者的職業

	選擇人數	百分比
學生	52	30.6
在職人士	20	11.8
家庭主婦	83	48.8
待業	7	4.1
退休	8	4.7
合計	170	100.0

遺失個案: 43 個

S0133

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

經濟動力
ECONOMIC SYNERGY

經濟動力就檢討《個人資料(私穩)條例》諮詢文件的回應

前言

過去十年間，資訊科技迅速發展、互聯網普及、電子商貿快速增長等原因，爲個人資料私隱保障帶來新挑戰。因此，政府於本年八月發表檢討《個人資料(私隱)條例》的諮詢文件（下稱「諮詢文件），諮詢公眾有關敏感個人資料、資料保安、私隱專員的執法權力、罪行及制裁等各方面的意見，目的是希望完善條例，更有效地保障香港市民的個人私隱。對於這份諮詢文件，經濟動力有以下回應：

敏感資料立例不宜過急

諮詢文件表示，資訊科技的發展爲現時規管個人資料私隱的制度帶來挑戰。誠然，隨着資料以電子方式儲存、傳輸及處理，個人資料外洩的後果，所造成的損害遠比過往嚴重。尤其是某些個人的隱密資料，當不幸被洩及經互聯網傳播，會給當事人無法估量的傷害。但同時，我們亦要明白，香港作爲一個外向型經濟體，立例時宜多參考外國例子，如操之過急，則有可能影響香港將來發展，因此，我們認爲有關敏感資料所包括的範圍亦應多考慮外國做法。

歐盟95/46/EC指令第八條第一款列明，種族或民族本源、政治意見、宗教或哲學信仰、工會會籍、健康狀況及性生活爲需要特別限制處理的個人資料。而歐盟成員國英國及德國，亦有相類限制。英國《1998年保障資料法令》及德國《聯邦資料保護法令》，亦分別使用「敏感個人資料」（sensitive personal data）及「特殊組別個人資料」（special categories of personal data），指出某些資料需要特別留意。而澳洲《1988年私隱法令》有關敏感資料（sensitive information）的內容，亦與歐盟、英國及德國相若。

我們認爲，香港可參照歐盟、英國、德國及澳洲的做法，把種族或民族本源、政治意見、宗教或哲學信仰、工會會籍、身體及精神狀況、性生活及犯罪紀錄定爲敏感個人資料。

至於生物辨識資料，如瞳孔特徵、掌紋及指模等，外國還未有先例列爲敏感個人資料，香港絕不宜走在外國前頭，以嚴厲方式規管這類資料，以免窒礙生物辨識科技的研究，局限了這門新興產業的發展。

事實上，自諮詢文件推出以來，從事開發生物辨識系統的資訊科技企業及有關設備的生產商，已即時受到打擊，業務大不如前。由於未清楚將來生物辨識資料的規管程度和模式，用戶已紛紛暫停向開發商採購新設備和系統。若政府最終決定實行嚴厲規管；恐怕這門原來有大好前景的產業，發展空間會急劇收縮，大大影響業內的企業和員工。

基於以上原因，我們不贊同把生物辨識資料列爲敏感個人資料。

對資料處理者先行間接規管再檢討成效

由於所採集資料往往不是由資料使用者保管，而是外判予其他機構處理，而現有法例卻沒有規管那些資料處理者，因此我們亦同意修例，對資料處理者加強監管，以保障資料使用者及資料當事人。但另一面，正如諮詢文件所言，我們亦須在保障個人資料私隱與正常商業運作之間，取得適當平衡，以免顧此失彼。

作爲平衡，我們認爲現階段不須直接規管資料處理者，以免突然增加業界的壓力及成本。我們可先行間接規管，依靠資料使用者確保其資料處理者儘一切合理方法保障個人資料安全。即使資料處理者有過失，私隱專員亦不能直接介入。但資料使用者仍可根據合約法尋求補償，而資料當事人亦可向資料使用者尋求補救。此外，政府可制定指引，訂明那些措施爲合理措施，以便業界「有所適從」，政府也可劃定3至5年後檢討，再視乎當時情況，考慮是否需要改爲直接規管。

只有敏感資料洩密才須通報

現行的自願性通報機制，比較適合社會現況，亦較爲業界接受。若硬性通報，會對機構造成沉重負擔，有違平衡保障私隱與商業運作的原則。此外，正如澳洲法律改革委員會所言，太多的外洩通知可能會令大眾難以判斷那些事故涉及重大風險，造成「通知疲勞」，於社會亦非好事。因此，我們建議，除非事件涉及敏感個人資料，須硬性規定通知私隱專員，否則其他事件可繼續實施自願性通報機制。

私隱專員權力不宜過大

雖然私隱專員提出3個理由，要求得到刑事調查和檢控罪行的權力，以及搜查和檢取證據等附帶權力，但我們認爲，理據並不算充分。首先是現行安排運作暢順，實毋須改變。其次，其他相類似組織，如平機會等，亦沒有這些權力，但私隱專員所提的3個理由：擁有第一手資料、熟悉相關條例、及節省檢控時間，均是其他相類似組織所有的條件。如果因這3個理由讓私隱專員得到這些權力，恐怕會

引起連鎖反應，其他類似組織亦會提出同樣要求，屆時，香港的司法系統難免會受到震盪。

鑑於法律訴訟既費時又昂貴，且民事索償的結果又未可預知，很多資料使用者即使受屈，亦沒有申索補償，因此政府建議私隱專員有權判給受屈的資料當事人補償。針對這個問題，當初法改會已表明，把執法和處罰的職能歸於同一機構，並不可取。我們十分同意法改會的意見，認爲應維持現狀，即私隱專員負責裁定保障資料原則是否遭違反，而法庭負責釐定補償額。**我們希望在有關司法的分工上，除非有必要的原因，否則應維持原狀，以免造成任何不必要的影響。**

雖然我們反對建議4及6，但卻支持建議5，認爲私隱專員可爲資料當事人提供法律協助。正如私隱專員所提，他們有第一手資料，又熟悉相關條例，是一般市民沒有的條件。如得到私隱專員協助，當受屈一方可以更準確評估民事索償的勝訴機會，亦不會因費用問題而對法律訴訟卻步，那麼政府建議6的原因便不再存在了。

規管過嚴將致惡果

雖然保護個人資料是文明社會應當做的事情，但現今資訊科技發達，很多時市民都會不小心或不自覺洩露其他人的資料。**如果規管過嚴，有可能會影響香港市民珍而重之的資訊及言論自由。**

我們對有關「罪行及制裁」，即建議7至12都原則上同意。但有關建議7：把違反保障資料原則訂爲罪行；建議8：在未經授權下取得、披露和出售個人資料；及建議9：就同一事實重複違反保障資料原則，**我們則認爲必須給予被控方申辯權，並在非惡意、非故意及有合理辯解的情況下可豁免刑責。**這樣做可以平衡保障個人私隱及保障言論自由兩方面，是一個比較可行的辦法。

總結

科技發展一日千里，優化條例以適應時代變遷，保護市民的個人私隱實有所必要。但同時我們亦須平衡營商成本，以及對其他方面的影響。敏感資料內容，我們宜參考外國規定及個案，以免偏離國際標準。而對資料處理者的監管，亦應循序漸進，以平衡保護個人私隱及商業運作。有關私隱專員的權力，在現行體制運作良好的情況下，根本沒有必要作出大改動。最後，我們亦希望政府修例時不應只看到保護私隱，亦要顧及言論及資訊自由之可貴。只有如此，才可顧及社會的

整體利益。

－ 完 －

自由黨
LIBERAL PARTY

致：政制及內地事務局（第4組）

由：自由黨

頁數：8頁 (連此頁)

自由黨就「檢討《個人資料(私隱)條例》的諮詢文件」的回應

謹附上自由黨就「檢討《個人資料(私隱)條例》的諮詢文件」的回應。如有查詢，請致電吳小姐(電話：（刪除）)或繆小姐(電話：(刪除)

自由黨
2009年11月30日

S0135

自由黨

LIBERAL PARTY

自由黨就「檢討《個人資料(私隱)條例》的諮詢文件」的回應

一、前言

保障私隱是體現保障個人權利的一項重要表現，尤其是近年本港屢次發生大規模的個人資料外洩事件，更大大提高了社會對此議題的關注。故此，對於當局發出「檢討《個人資料(私隱)條例》的諮詢文件」，全面檢討條例及提出修訂建議，以回應社會發展及科技進步為條例帶來的新挑戰，自由黨表示歡迎，並有具體意見如下：

二、具體回應

1. 有關規管敏感個人資料（建議一）

隨着科技發展，生物辨識系統在本港社會的應用亦越來越廣泛，不少大企業，以致學校、醫院等都分別有收集個人的指模、瞳孔特徵等資料，以作考勤或保安用途，但正如諮詢文件所指出，生物資訊是獨一無二，且不能改變的，可揭示敏感的個人資料，例如健康狀況、基因資料或種族本源等，如有關資料處理失當，可以對當事人造成重大損害。故此，我們認同諮詢文件所建議，把個人資料劃分為敏感及非敏感兩個類別，並把生物資料納入前者，作出更嚴格的規管，並輔以相應的懲罰，以加強保障個人權益。

不過，為免窒礙社會應用各種新科技，我們認為當局不宜以「一刀切」的模式，禁制涉及敏感資料處理的技術使用。我們認為應該容許資料使用者根據例如保安等特定的理由，並在得到私隱專員的批准，才可依照規定收集、持有、處理和使用敏感的個人資料。至於未來敏感個人資料的範圍或規定，則可隨科技及社會發展按需要作出檢討。

諮詢文件建議在指定情況下，方可收集、持有、處理和使用敏感

個人資料，而首項條件為要「獲得資料當事人的訂明同意（即自願而明確的同意）」。對此，自由黨認為何謂「自願而明確的同意」定義有欠清晰，勢將會令社會無所適從。例如僱主如果已在招聘廣告或招聘合約中，把「需要收集指模」列作聘用條件，向將來受僱的應徵者收集指模，算否已得到僱員「自願而明確的同意」呢？為免有關規管令社會人士誤墮法網，當局應先釐清各項相關概念細節。

至於現時有提供生物辨識系統服務的業界，指稱現時的民用指模採集系統基於技術問題，資料根本不能還原為指模影像，故不涉及收集個人資料等，我們盼望當局與業界多作溝通，嘗試找尋一條既可加強保障個人敏感資料，又不礙新科技應用及發展的方法。

2. 有關資料保安方面的建議

2.1 規管資料處理者及分判活動（建議二）

縱使個人資料處理的分判活動已經十分普遍，但是目前的私隱條例只規管資料使用者，卻未有直接規管資料處理者，亦即代其處理個人資料的分判商，情況殊不理想。近年便接連發生一些資料處理者外洩個人資料的大型事故，其中零六年警監會二萬名投訴人機密資料在網上外洩，洩密源頭為其電腦承辦商，更令社會震驚。為了加強保障市民私隱，我們認為條例必須與時並進，當局應該對所有資料使用者處理者，都作出嚴格規管，以保障個人私隱。

例如，當局亦應該協助業界制訂清晰的守則，讓委託人（資料使用者）委託分判商（資料處理者）代其處理、持有或使用個人資料時，雙方都知所遵從，這樣不但可以釐清彼此的責任，亦可給予這些個人資料最佳保障。當局並應與業界積極研究制訂不同的處理方法，讓分判商獲得的資料已經事先過濾，減去可供識別個人的部分，令到資料縱使外洩，他人亦無法憑此連繫上個別人士，從而減低個人資料外洩的風險。

2.2 個人資料外洩通報機制（建議三）

目前，政府內部已設立電子個人資料外洩事故通報機制，規定各政策局及部門須盡快向私隱專員呈報外洩事件，以及通知受影響人士。為了加強保障個人私隱，諮詢文件建議引進

自願性的個人資料外洩通報機制，要求政府、公營機構及私營機構按照私隱專員的指引，在適當情況下啟動通報機制，以盡早通知可能受外洩事件影響的人士，讓他們可以採取措施盡量減低損失，而有關的指引必須清晰、符合實際情況及易於遵從，從而發揮最大效用。

3. 有關私隱專員的賦權

3.1 授予私隱專員刑事調查及檢控權力(建議四)

鑑於現行私隱專員把個案轉交警方負責刑事調查及檢控的安排，行之有效，而且運作順暢，我們認為無需作出重大更改。

3.2 在第66條下為資料當事人提供法律協助(建議五)

面對法律訴訟費用高昂，加上對私隱條例未必有足夠的認識，可能會令一些欲根據私隱條例作出申索的資料當事人因而卻步，未能尋求公義。為了解決此問題，我們認為，私隱專員應先就侵犯私隱的問題，向資料當事人提供法律協助，包括對當事人提供法律意見，及協助他們評估申索的成功機會。

此外，當局還可考慮參照平機會的有關機制，賦權私隱專員在申索個案涉及重大原則問題或公眾利益等情況下，為有意透過法律程序的申索人安排律師或大律師作代表，協助其興訟。此舉亦可為不符法律援助資格的中產申索人士，增加一條申訴途徑，為涉及私隱的問題討回公道。

3.3 給受屈的資料當事人判給補償(建議六)

基於我們在回應「建議五」時，已建議私隱專員可按情況，向受影響的資料當事人提供適切的法律協助，如涉及補償亦應由法庭釐定，故不認為有需要按諮詢文件建議，為申索人提供多一個補救途徑，授權私隱專員判給個人私隱受侵的當事人作出另外補償。

4. 有關罪行及制裁

4.1 把違反保障資料原則訂為罪行（建議七）

對於諮詢文件建議，把某些嚴重的違反保障資料原則的嚴重違規行為或做法，訂為刑事罪行，以提升條例的阻嚇力，我

們原則上並不反對，但是前提是當局須要就何謂「嚴重違反」保障資料原則，作出清晰的定義及指引，特別是這六項保障資料原則用辭涵義廣泛，可作多種不同的詮譯，當局必須詳加闡釋，避免因為定義不清，或市民因非蓄意的行為或遺漏都誤招刑責，嚴重影響公民自由。

4.2 在未經授權下取得、披露和出售個人資料（建議八）

為了加強規管個人資料在互聯網上肆意發放的事故，諮詢文件建議「在未得資料使用者的同意下，知情或罔顧後果地取得個人資料，再把所得的個人資料披露，並從中取利或作惡意用途」訂為罪行，並施以相應的懲罰。就此我們原則上認為可以接受，但是文件未有對「惡意」作出清晰定義，有欠妥當；為免引起公眾疑慮使用互聯網時會因此誤墮法網，以至網上正常的資訊流通亦受影響，我們認為當局在制訂有關條文前，必須先釐清有關定義，廣泛諮詢公眾並取得共識。

4.3 就同一事實重複違反保障資料原則（建議九）

正如諮詢文件所指，由私隱條例實行至今，未有出現是項建議所指的資料使用者在遵從執行通知後，短期重複該違反保障資料原則的行為或做法，故我們認為文件建議防範此行為而新訂罪行既無需要，亦過於瑣碎，故不予贊同。

4.4 就嚴重違反保障資料原則處以罰款（建議十）

基於現時受屈的當事人已可經由民事途徑索償的方式，而我們在回應建議五時亦已提出可賦權私隱專員按情況對申索人提供適切的法律援助，我們認為當局並沒有必要如此項建議般，再賦權私隱專員向嚴重違反保障原則者處以定額罰款。

4.5 重複違反執行通知（建議十一）

基於本地不少法例對屢犯者都處以更重的懲罰，以阻嚇重犯，按此原則我們亦同意諮詢文件的建議，對重複違反私隱專員所發執行通知的人士，訂定更高的懲罰。

4.6 提高在直接促銷中不當使用個人資料的罰則（建議十二）

鑑於部分市民對他們的個人資料被他人在促銷活動中不當使用，而不勝煩擾，但是現時有關罰則最高罰款只為一萬元，沒有足夠阻嚇力，我們認同諮詢文件的建議，應適度提高有

關的罰則。

5. 有關資料當事人的權利

5.1 由第三者給予訂明同意更改個人資料用途（建議十三）

目前，某些資料當事人，例如智障或殘障的人士，縱使未必具有足夠的智力或能力決定個人資料的使用，但是他們的家長或監護人卻沒獲賦權更改當事人的個人資料用途；這種狀況，對當事人獲得醫療、教育或社會服務，均會構成不必要的阻礙。故此，我們是十分贊同諮詢文件是項建議，賦權「第三者」，例如是未成年子女的父母，在資料當事人因為不能理解，或沒有足夠智力完全理解向其提出的更改資料用途建議，因而沒有能給予訂明同意；以及涉及的個人資料擬作的用途對資料當事人有明確的好處的情況下，更改當事人的個人資料用途。

為了照顧特殊的個別情況，我們認為「第三者」的定義還可以擴闊至包括當事人的其他直系成年親屬，以確保即使未能聯絡其父母，仍有其他成年家庭成員可代當事人作出適切的更改個人資料用途的決定。此外，對於諮詢文件提到「第三者」的定義可擴展到「各種託兒班」，我們認為在個別緊急及特殊情況下，可指明僅託兒中心校長方有權力更改弱勢當事人的個人資料用途，以釐清權責。

5.2 父母查閱未成年人士個人資料的權利（建議十四）

我們認為，家長既有照顧子女的責任，亦應該有相應的權利，包括可獲得未成年子女的個人資料，他們方可以有效地履行全面照顧子女生活起居、醫療、教育等需要之責，助其身心健康發展。正如在現行私隱條例下，未成年子女的父母是有權向資料使用者要求查閱其子女的個人資料的。

諮詢文件為保障兒童權利，建議加入新的條文，准許資料使用者在一些情況下，可以拒絕向父母發放其未成年子女的個人資料，包括：

i. 父或母可能為其個人目的，而濫用查閱資料機制；

ii. 父或母懷疑虐待子女；以及

iii. 子女向資料使用者表明，不同意向其父母透露其個人

資料。

對於前兩項新增的限制條件建議，我們沒有異議，但是對於第三項建議則表示強烈反對。

事實上，如任由未成年子女可自行決定向父母隱瞞重要的個人資料，不但會令本港的親子倫理關係，增添無謂隔閡，更將有礙為人父母者及時察知子女的異常情況，及早協助子女回頭是岸，因為未成年子女的心智尚未成熟，他們的意願亦未必合乎自己的最大利益。舉例說，一名染有毒癮的未成年人士就可以利用是項條文，對社工表示不欲其個人資料讓父母知悉，以免被父母親迫其戒毒，實不可取。

6. 就豁免遵從私隱條例的意見

6.1 在緊急情況下處理個人資料（建議二十六）

對於諮詢文件建議容許執法機構和醫療機構，在緊急情況下獲得豁免遵從私隱條例以方便救援，我們認為可以接受，惟基於不少涉及救援工作的個人資料，例如個人病歷均極為敏感，故有關豁免的適用情況應該加以限制，例如僅容許涉及意外或生命安全的情況，才能獲得上述的豁免，以杜絕濫用。

6.2 為了履行監護責任和家長照顧責任而把未成年人的個人資料轉移（建議二十七）

如我們回應建議十四所言，家長是應有接觸未成年子女個人資料的權利，以令他們有效履行責任照顧子女的責任的。諮詢文件是項建議容許資料使用者，例如警方或社福機構等在未成年人士惹上麻煩，例如受毒品毒害時，主動把未成年人士的資料交與家長，正是一項有助家長履行照顧責任的配套措施，可以讓家長能夠適時為其未成年子女提供支援，值得支持。我們更認為有關個人資料的轉移不應如諮詢文件所建議般，只限於「邊緣少年」，而應該適用於所有未成年人士。

7. 有關把互聯網地址視為個人資料

對於互聯網地址(IP 地址)是否應該列作個人資料的問題，社會是存有不同意見的。其實，單憑 IP 地址是不能顯示用戶身份的，但 IP 地址若連同可供識別個人的其他資料，如互聯網服務供應

商分配該 IP 地址的紀錄及其客戶資料，可識別個人，亦可獲私隱條例保障。基於上述考慮，我們認為現時並無需把 IP 地址維入個人資料範圍，但是隨着科技發展例如發展到個人的 IP 地址時，當局亦應作出適時檢討。

三、總結

我們期望當局透過廣泛的公眾諮詢，對《個人資料(私隱)》條例作出全面檢討，並提出適切的修訂，令條例能夠與時並進，在加強保障個人私隱資料、社會發展，資訊流通與科技應用之間，取得一個適當平衡。

香港中小型企業商會
The Hong Kong Chamber of Small and Medium Business Ltd.

S0136

何健華先生, JP
政制及內地事務局
副秘書長
香港下亞厘畢道
政府合署東座 364 室
傳真：2523 0565

先傳真，後郵遞

尊敬的何秘書長：

有關中小企業界對檢討《個人資料(私隱)條例》的建議

承蒙　閣下早前在百忙中抽空出席本會舉辦的活動，就檢討《個人資料（私隱）條例》（下稱「條例」）的公眾咨詢向本會會員闡述有關重點，令本會會員更確切地了解有關檢討的事宜，謹此致以衷心感謝！

經過本會仔細研究就檢討有關「條例」的資料後，特致函　閣下以反映本會對「條例」關注的地方，現分爲以下數點：

1/ 關於建議就同一行為重複違反保障資料原則構成罪行的問題，本會十分關注。有別於大企業，中小企業力量薄弱、難以聘用專人處理個人資料事宜，若中小企業不慎觸犯私隱條例，他們難有足夠人手處理以避免再誤墮法網。故建議應為何謂「重複違反」作清晰定義。並應爲企業提供有力的支援。

2/ 本會認同考慮規管個人敏感資料的大方向，但唯國際上目前並未有一套界定何謂敏感個人資料的標準，在欠缺此基礎的情況下，本港實沒有急切需要制定一套區分敏感與非敏感個人資料的準則。

3/ 對於檢討「條例」中建議私隱專員被賦予刑事調查和檢控的權力、以及授權私隱專員，規定嚴重違反保障資料原則的資料使用者判處罰款，我們深表關注。目前分別由警方及律政司負責刑事調查及檢控的機制運作良好，故此我們並不贊同公署擁有刑事調查及檢控的權力。至於判處罰款方面，如本文第二點內所述，現時國際上並未有一套界定敏感個人資料的標準，爲避免在欠缺客觀標準的情況下造成主觀判決，罰款事宜應交由法庭處理，賦予公署有關權力並不恰當。



To <pdpo_consultation@cmab.gov.hk>
cc

30/11/2009 17:39

bcc
Subject PDPO Consultation-PrimeCredit Limited

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

PDPO Consultation –PrimeCredit Limited

Proposal No. 2: Data Processors

Current legislation does not regulate acts of an agent processing personal data for a data user. We agree with the direct regulatory model proposed in the consultation where data processors e.g. direct mailing companies themselves would be responsible for ensuring data is only used for the purpose for which it was provided to them, secure and safeguarded and erased once no longer required. Although the above are usually bind by contractual agreements between the principals and agents, the latter would be more cautious in handling the personal data provided by the former should they be also subject to direct regulation.

Proposal No. 3: Personal data security breach notification

The consultation proposes a voluntary regime for notification of loss or leakage of personal data. The voluntary notification mechanism would require a data user to notify the PDPO within 5 days of a breach and to consider whether individuals should be notified, taking into account the potential harm caused by the breach.

This however does not apply to authorized institutions whose reporting to the HKMA is compulsory for the loss or leakage of customer data (HKMA Circular dated 10 July 2008). It would be very helpful if similar guideline can be issued to other industries assisting them in making the judgment. In addition, suggestions on the definition of high risk information e.g. name & email address, address & account information should be given to industries so that the latter will not be over-burdened on issuing notices to individuals.

In case of data processors (agents), they should inform their principals of such breaches and further guidance should be given as to whom, the agents or principals, should notify the affected individuals.

Proposal 8: Unauthorized obtaining, disclosure and sale of personal data

Disclosing personal data for profits without obtaining the data subject's consent or for malicious purposes has become increasingly serious recently. Making it an offence would heighten the public awareness on the seriousness of the breach.

Besides, regarding the unauthorized "disclosure" of personal data, we agree with the Office that the proposed provisions should not impose liabilities on data users for accidental leakage not resulting in substantial harm. Only those acting intentionally, knowingly or recklessly with a purpose for "profits" or "other malicious purpose" should be captured by the proposed provisions.

More detailed guideline should be given on the reporting party i.e. whether it would be the data subject or the data user whose client information were sold for profits by its employee to report the incident, or both. The current legislation encourages reporting by data subject but not usually the data users.

We suggest considering the penalty level for such breach by making reference to other countries' privacy acts e.g. UK and Australia

S0138

30/11/2009 17:46

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Re: HKITF's submission to government on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

To: CMAB (pdpo_consultation@cmab.gov.hk)

Enclosed please find HKITF's submission to government on Review of the Personal Data (Privacy) Ordinance for your perusal. Thanks.

Best regards,

Francis Fong
President
Hong Kong Information Technology Federation Ltd.
On behalf of the Council

HKITF - Privacy law review submission -11 30 09.pdf

Submission in response to the Consultation Document on Review of the Personal Data (Privacy) Ordinance

Executive summary

HKITF's key submissions are as follows:

- HK should retain the principles-based, technologically neutral approach to privacy regulation as currently provided for in the Personal Data (Privacy) Ordinance ("**PDPO**") and the Data Privacy Principles ("**DPPs**");
- Data protection obligations should vary in proportion to the sensitivity of the personal data, and this principle can be better achieved by tailoring the existing DPPs rather than creating a separate regime to define and protect sensitive personal data,
- A voluntary breach notification scheme with clear and effective guidelines is appropriate for a city like HK;
- Indirect regulation of data processors and sub-contractors is preferred;
- Proposals to grant criminal enforcement powers to the PCPD and to make the contravention of a DPP an offense not supported; and
- HKG to engage key stakeholders in order to identify and implement the best methods of advancing health privacy.

Proposal No. 1 - Sensitive Data

1.1 Sensitive personal data

HKITF appreciates that certain types of personal data are more sensitive then other types, and that the degree of sensitivity should be a crucial factor in determining the appropriate level of regulation for personal data.

However, the creation of a separate statutory regime for "sensitive personal data" may not be the best solution, and may even cause greater confusion and higher compliance costs for businesses in HK, that are mainly SMEs. We believe that differential treatment based on different personal data types is more effectively achieved by incorporating the differential treatment concept into the DPPs, rather than by creating a separate regime. As discussed in the APEC Privacy Framework 2005, data controllers should be required to implement ***appropriate safeguards*** that are ***proportional*** to:

(a) the likelihood and severity of the harm threatened;

(b) the sensitivity of the information; and

(c) the context in which it is held.

With technology advancement and changing market conditions, the degree of flexibility afforded by this kind of test is critical and cannot be matched by a statutory scheme that arbitrarily partitions personal data into "sensitive" and "not sensitive". This flexibility also avoids the risk of data users adopting measures to artificially move data from "sensitive" to "not sensitive", since it requires a consideration of all of the circumstances surrounding the data, rather than just the application of a single statutory definition.

1.2 Biometric information

HKITF advocates that technological neutrality promotes the adequacy and effectiveness of the PDPO and should be maintained wherever possible, and is concerned that the classification of biometric information as sensitive personal data inappropriately focuses on the methods of data collection and storage, rather than the inherent characteristics of the data. Indeed, as paragraph 3.06 of the Consultation Document states (emphasis added):

> *"Biometric data **could reveal** sensitive personal information such as health, genetic information, or ethnic origin."*

As far as HKITF is aware, there is no internationally accepted test for "sensitivity" or definition of "sensitive personal data". If HK were to define biometric information as sensitive information and impose its own standard, this may have the unintended impact of stifling innovation and R&D efforts in the area of bio technology. This is contrary to the HKG policy of encouraging innovation and technology, and to have HK as the IT hub for the region. Any local standards that are inconsistent with international practice will further discourage MNCs to invest in HK.

One alternative to address the public concern for protecting HK citizens data against fraudulent use of personally descriptive data (such as in the case of identity theft and impersonation) may be to review HK's existing criminal laws. The risks we are concerned about may be better dealt with under cybercrime legislation rather than privacy laws.

Proposal No. 2 - Regulating Data Processors and Sub-contracting Activities

2.1 Indirect regulation preferred

With the explosion of Web 2.0, data is incredibly mobile, and that it is now common for data to be collected and then transferred to another entity, to another country, or both. HKITF urges HKG to exercise caution in establishing a mechanism that will ensure that adequate data protection obligations are preserved at each link in this chain of custody, while avoiding excessive regulations that would discourage e-commerce and inhibit innovation.

The current indirect regulation regime allows the interests of consumers to be preserved without sacrificing flexibility. We support the proposal that require the data user and data processor in each instance to adopt suitable measures to regulate the transfer and processing of customer data, contractual or otherwise, to ensure compliance with the PDPO.

The indirect regulation model is also consistent with the model described in Principle 9 (Accountability) of the APEC Privacy Framework, which requires personal information controllers remain *accountable* for the protection of personal information they collect, use or hold even if that data is transferred from one jurisdiction to another. Importantly, as with the indirect regulation model in the Consultation Document, the accountability principle allows data users to tailor their compliance method to a given context.

On the contrary, direct regulation of data processors fails to offer the flexibility and consistency benefits associated with indirect regulation. With the popularity of social network and cloud computing services, personal data is frequently transferred to a data processor, but remains under the control of the data user. Under such circumstances, it would be unreasonable to simply deem the data processor as being equivalent to the data user, since clearly the user and processor do not have the same ability to ensure the security and lawful use of the data.

HKG should also be mindful of the practical challenges in enforcing direct regulation against data processors. The commercial reality is that many data processors that serve data users in HK are off-shore and not subject to HK jurisdiction. Given that HK privacy law has no extraterritorial effect on those off-shore entities, having direct regulation on data processors will only create additional burdens for those providing data processing services in HK, but fail to offer the kind of control and protection it intends to achieve.

2.2 Regulation by category of data processor?

The Consultation Document also requests comments in relation to the proposition that different types of data processors should be made subject to different categories of regulation. HKITF believes that privacy regulation should be phrased in terms of outcomes and principles, and that implementation is a matter best left to data subjects, data users and data processors. Consequently, we do not support the categorisation of data processors in the PDPO, as HKITF is not convinced that such categories could be drafted sufficiently generically and in a technology-neutral manner to ensure that the categories remain relevant in the future. A suitable general obligation, along the lines of the indirect model discussed above, is a more effective regulatory strategy.

Proposal No. 3 - Breach Notification

3.1 Introduction of breach notification

HKITF supports the introduction of a voluntary breach notification obligation in the PDPO, as an appropriately structured mechanism of this kind promotes public confidence in the data custody practices of data users. However, to be effective and offer protection to consumers, such voluntary

breach notification system should be supported with clear guidelines from the PCPD.

On the other hand, the introduction of a mandatory breach notification at this time may have unknown and potentially significantly detrimental impact on data users.[1] HKITF considers that the policy goals associated with breach notification can be effectively achieved by a voluntary scheme, and agrees with the Consultation Document conclusion that implementing a mandatory scheme as an outcome of the current consultation process would be premature.

There is not a consistent international approach in the area of breach notification, and in particular there is no agreement on the whether breach notification requirements should be tied to the citizenship of the affected data subjects, or to the location of the breach, or to some combination of both. In this context, a mandatory regime imposed by Hong Kong may potentially conflict with the regimes of other jurisdictions, and that this would place multinational companies in a difficult, and potentially costly, compliance position.

3.2 Guidance on breach notifications

As recognised in the Consultation Document, one of the key issues associated with the introduction of a breach notification obligation is identifying the types of data breaches where a breach notification would be an appropriate step for a data user to take. HKITF believes that an individual should be informed of a security breach if that breach could reasonably result in the misuse of that data subject's unencrypted sensitive financial information. This threshold marks an appropriate balance between empowering data subjects to minimise the more serious consequences that might flow from a security breach involving their personal information, and avoiding a situation whereby security notifications are so frequent that data subjects disregard them or are unable to differentiate between those that indicate a significant risk and those that do not.

If the HKG were to introduce a voluntary notification regime, it would be useful if the PCPD were to publish guidance on the factors that data users should take into account when deciding whether to issue a breach notification to data subjects.

3.3 Form and timing for notification

In HKITF's view, data users should be afforded discretion as to the method by which they provide breach notifications to affected data subjects. Data users should be able to take into account factors such as:

(a) the size of their organisation;

(b) the number of recipients of the notification;

(c) the relative cost of different methods of providing the notification; and

[1] See Consultation Document paragraph 4.34.

(d) the ways in which the data user typically communicates with its customers,

when determining when and how to notify data subjects of a data breach.

- More generally, the HKG may draw reference from the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[2] (which interprets s 501(b) of the United States' *Gramm-Leach-Bliley Act*), which provides a useful model for fleshing out a breach notification obligation. The Interagency Guidance considers matters such as how to identify data subjects affected by a regulated security breach, the timing and content of any breach notification and the manner in which any breach notification should be delivered.

Proposals No. 4 – 12 - Criminal Sanctions

4.1 Criminalisation of PCPD provisions

In general, HKITF opposes to the criminalisation-related proposals in the Consultation Document, as the principle-based drafting of privacy obligations is generally inconsistent with the imposition of criminal penalties. Criminalising such obligations would create significant uncertainty, as businesses will not necessarily know when particular behaviour becomes criminal. HKITF is particularly concerned about the adverse effect that criminalisation would have on the IT industry, where businesses are often engaged in new or innovative activities.

In relation to the DPPs, as pointed out in paragraph 6.04 of the Consultation Document, the *"DPPs are couched in generic terms and can be subject to a wide range of interpretations"*. We agree with the Consultation Document that criminalising non-compliance with the DPPs would be counter-productive (see Proposal No. 7), and consequentially recommends that contravention of the DPPs not be made an offence.

HKITF believes that civil remedies in general should provide adequate protection to citizens affected by any non-compliance. There may be exceptions in cases of identity theft or malicious dealing of personal data, but again we feel those situation may be better dealt with under cybercrime law regime.

Others

5.1 Health Privacy

The current consultation does not cover health related information in general. The health sector presents unique and complex privacy issues, many of which have only recently emerged due to the relatively recent update of technology in this sector.

---

[2] Issued by the Office of the Comptroller of the Currency (Department of the Treasury), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision (Department of the Treasury). Available at: http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf.

The plan of HKG to launch a SAR-wide electronic health record (eHR) system presents a number of privacy concerns. HKITF considers it critical that there be control by patients over tiered access to his/her health data. A privacy-sensitive approach to the development of the eHR system is needed to ensure that the system is designed with built-in checks and balances to lower the risk (both in terms o the likelihood and magnitude) of data security breaches. HKITF urges HKG to engage as early as possible in consultation with government, industry and other key stakeholder groups in order to identify and implement the best methods of advancing health privacy.

By Hong Kong Information Technology Federation

November 30, 2009

Established in 1980, the Hong Kong Information Technology Federation is a nonprofit, non-political trade association that acts as a forum in which the IT-related businesses in Hong Kong can work together for the benefit of the industry and to maintain a high level of business practice amongst the members.



30/11/2009 17:55

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Consultation Document on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir/Madam,

On behalf of *"organisation"* which is one of famous discussion forum in Hong Kong. We would like to provide our comment to below Personal Data Privacy:

建議4：授予私隱專員刑事調查及檢控權力
　私隱專員應否獲賦權進行刑事調查及提出檢控或應否維持現狀。 -> 私隱專員不應獲賦權進行刑事調查及提出檢控，應維持現狀。

建議5：在第66條下爲資料當事人提供法律協助

應否參照平機會的模式，授權私隱專員爲有意根據私隱條例第66條向資料使用者提出法律訴訟，以申索補償的受屈資料當事人提供法律協助。
-> 不應

建議6：向受屈的資料當事人判給補償

是否應授權私隱專員判給受屈的資料當事人補償，以提供多一個補救途徑。
-> 不應

建議7：把違反保障資料原則訂爲罪行
　應否把違反保障資料原則訂爲罪行。 -> 不應

建議10：就嚴重違反保障資料原則處以罰款
　應否授權私隱專員就嚴重違反保障資料原則判處罰款。 -> 不應

Regards,

(name)

(The sender requested anonymity)

S0140

致香港特別行政區政府

政制及內地事務局

關於檢討《個人資料（私隱）條例》的意見書

（共4頁）

日期：公元二零零九年11月30日

（一）基本立場

1. 作為市民，本人認為相關的私隱條例應以**社會倫理和法治精神作為首要考慮和原則**，現代社會注重法治和私隱等觀念，原因不外乎是現實中人類社會仍存在著不同程度的矛盾和不公義，以至危害或威脅人類個體以至群體生存和發展，這又跟人類對理想中的大同世界的訴求有關。

2. 香港既是承襲了英國的普通法和奠基於回歸中國後的基本法，其中的一個基本假設，就是原有制度的延續性和注入基本法的解釋或調節規範，延續性主要針對回歸前制度是基本可行和乎合香港的現況，基本法作為香港的小憲法則賦予這法治基礎的一個主體性，並承認中國作為主權國的體現和規範，如中英聯合聲明所指出的有助於維持香港的繁榮與穩定，所以，在法治和公義的基礎上，所有建制和措施都應有利於社會的和諧及良性發展，若過分執著於「政治正確性」而忽略了社會的良性發展，則可能有違反聯合聲明以至基本法之嫌！

3. 本人尊重法治，同時強調倫理道德是人類社會良性發展的不可或缺的基礎。

（二）具體意見

1. 我同意「私隱」或其相關法定建制不是至高無上的事物，當然，「私隱」是應當被尊重，特別是考慮到私隱被不當的張揚和使用時很可能會對被張揚者構成損害或不必要的威脅或壓力。

2. 今天香港的倫理道德是香港社會在過往發展中的一種累積和承傳，

雖然不是絕對，但應受尊重，直至相關的標準或價值透過公眾廣泛討論後，**才可修改**。因此，我反對把一些未經歷史印證或足夠考核的觀念〔如私隱是個人的絕對權利[1]〕被神化成一些所謂「普世價值」。

3. 就青少年與其家長或監護人間的「私隱」權衡，我認為家長既有養育他們的責任，必須被賦予對子女的**知情權**及為未成年子女接受何種教育的選擇權。否則，家長便難以合理和有效地履行養育的工作和責任；如此一來，青少年和社會問題必然氾濫，而社會要付出高昂的代價！

4. 家長/監護人的知情權應受保障，除非相關家長或監護人因為精神或病理因素失去養育和監護相關青少年的能力，又或者其子女的私隱一旦被他們揭露時，公眾有足夠理由相信可能會導致其子女身心受創或生命受威脅，在這些處境下，政府或其他合法受托人應介入協調和處理，以預防不幸事情發生，又應向有關當事人提供適切的公民協助。

5. 若因為私隱而剝奪了家長的知情權和與監護相關的選擇權〔例如近期氾濫於青少年間的吸毒問題以至在網上設立所謂「自殺群組」的問題〕，則政府是責無旁貸，或是糾正相關歪風，或是對可能出現的傷害作出全面承擔和補償！

6. 當青少年的個人資料與其家長或監護人履行照顧和監護責任相關時，有關當局應規定及時把相關資料通知和送達他們的家長或監護人，以便相關家長作出適切的跟進和處理。

7. 同理，執法機關以及救援和支援機構**在緊急情況下**應有權處理相關人士的個人資料，只要相關機關/人員能信守對相關資料的官方保密承諾，若相關的私隱一旦被洩漏，相關機構或官方負責人應負上民事補償責任。

[1] 一個明顯的反證是針對謀殺犯或恐怖份子的犯罪意圖不應受私隱保護。

（三） 其他意見

3.1 關於個人資料外洩通報機制(諮詢文件建議 3)，本人同意可先推行自願性通報機制，以更準確地評估遵行外洩通報對各界別的影響，再調校通報規定，使有關規定既合理又切實可行，但在過渡至一較嚴格的規管或立法以前，有關當局應同時設立一協助相關當事人，在其個人資料被不當或不法洩露時，可快捷及不需花費昂貴的費用來調解或索償。

3.2 根據私隱條例第 66 條為資料當事人提供法律協助：有關當局不防考慮成立一個中介訟裁專員/機構，以協助有關雙方調解，在調解失效時，才正式授權私隱專員為受屈資料當事人提出訴訟。至於具體罰則，則應交由法庭判定。如當事人在相關案件判決後，仍然感到不公平，則可向私隱專員提出協助覆核或上訴的申請，若私隱專員認為案件值得跟進，可出任為當事人的合法代理人，進行相關申索，若是這樣，亦應按當事人的承擔能力，訂定其合理的訟費分擔水平〔如當事人財產/年收入的 5%〕。

3.3 至於應否把違反保障資料原則訂為罪行，本人建議可以先易後難的方式，先為一些刻意違反私隱指引或法定規範的行為定為罪行，以便評審這類安排的可行性和適切性。

3.4 直銷電話經常令資料當事人受到滋擾，如因而引起投訴和被定罪，初犯可以處以第 3 級罰款（最高可達 10,000 元），再犯者則理當提高至 100,000 元和連續犯例期間的按日罰款〔如每日 5000 元〕，並應加上監禁條款。

3.5 至於因現今社會趨向一體化，在立法、訂定罰則和制定訟裁機制的同時，有關當局應注意互換原則〔Principle of Reciprocity〕，因為諸如透過互聯網或其他電子渠道而發放私隱一事，國與國，甚至區與區之間的管制常有差異，這些差異除了可構成跨區不公平的管制與處罰外，亦可能出現外區犯法，本區難管，或同一區域人士可能就同一涉嫌違例事件，會在不同區域得到顯著不同的看待，在這些情況下，立法前應先做好跨區評估和協商，以求達至一均衡合

理和有效的管制方法。

此致
香港政制及內地事務局

進見者：黎民〔筆名〕，獨立時事觀察員

==========本文完結 (End of Document)==========

敬啓者：

就<<個人資料(私隱)條例>>("條例")的諮詢文件作出回應

有關第 6 章：罪行及制裁：建議 8：在未經授權下取得、披露和出售個人資料 及 建議 12：提高在直接促銷中不當使用個人資料的罰則

須處理的問題

現時未經直接授權下取得及披露個人資料情況普遍 以及 市民受直接促銷活動滋擾情況嚴重，是基於條例寬鬆，而以上提及的罪行及制裁(包括新建議)均未能理由充分地控制上述問題。

背景

現時大部分銀行及財務機構("該些機構")均在取得客戶個人資料前給予客戶或要求客戶簽名確認該些機構擬訂的有關於個人資料(私隱)條例的客戶通知("該通知")，而該通知間接或直接令該些機構獲得客戶同意該通知的內容，包括一些涵義極廣的條文，例如：

客戶的資料可能會作下列用途：

- 爲本行及 /或*特選公司*推廣服務或產品；

基於現時並未有對這類通知有任何規管，致使這些涵義極廣的條文，令該些機構理由充分地披露客戶的個人資料給予*任何*一間機構作推廣服務或產品，致使 "有關第 6 章：罪行及制裁：在未經授權下取得、披露和出售個人資料" 的條例在推廣服務或產品的涵概授權下形同虛設，更令市民受直接促銷活動滋擾情況日益嚴重，而建議 12：提高在直接促銷中不當使用個人資料的罰則 在這情況下只是治標不治本。

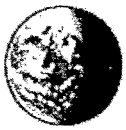
可考慮的規管模式

任何機構在取得客戶個人資料前給予客戶或要求客戶簽名確認的有關於個人資料(私隱)條例的客戶通知內容，須包括以下內容：

1. 要清楚列出個人資料可能會給予用作推廣服務或產品的機構清單("清單")
2. 提供清單包括的機構的資料保護主任聯絡資料 (讓市民可以在日後聯絡取消授權)

如對以上回應有任何查詢，請聯絡陳先生，電話 (刪除)，傳真號碼 (刪除)
電郵地址 (刪除)

S0142



To "pdpo_consultation@cmab.gov.hk" <pdpo_consultation@cmab.gov.hk>

30/11/2009 17:47

Subject Consultation Document on Review of the Personal Data (Privacy) Ordinance

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sirs,

We refer to the Consultation Document on Review of the Personal Data (Privacy) Ordinance and would like to provide our comments on Proposal No. 7 entitled "Making Contravention of a Data Protection Principle an Offence".

We note your comments in paragraph 18 of the Executive Summary, "that data protection principles (DPPs) are couched in generic terms and can be subject to a wide range of interpretation". **We strongly object to making contravention of a DPP an offence.** DPPs are high level principles, and do not refer to specific acts; it would not be appropriate to impose criminal liabilities on a breach of DPP, in particular if it is due to an inadvertent act or omission.

We also believe that the effective means of ensuring the proper behaviour and attitude towards protection of personal data privacy is by regulation and education rather than criminal sanction. The Consultation Document rightly notes the need to strike carefully a balance between protection of personal data privacy and other competing rights and interests, such as the civil liberty of individuals and freedom of information.

We believe it would be more appropriate to adopt a selective approach by singling out particular acts or practices such as a wilful disregard to complying with the requirements of the Ordinance or a grossly negligent act, as an offence, having regard to the severity of such contravening acts or practices.

We also welcome using a selective approach to introduce a monetary penalty for failure to comply with the DPPs, but limited to breaches that are avoidable or intentional, and that give rise to a serious data protection risk. It would address behaviour that reveals either a wilful disregard for the requirements of the Ordinance or a grossly negligent approach to complying with the requirements.

In summary, we do not consider there are strong grounds of justification for making contravention of a DPP an offence.

We note the Guiding Principles include:-
(i) the right of individuals to privacy is not absolute. It must be balanced against other rights and public and social interests;

(ii) any changes to the privacy law should not undermine Hong Kong's competitiveness and economic efficiency as an international city.
We believe without certainty in the law especially as regards potential criminal charges, Hong Kong may be put at a disadvantage.

If you have any questions on the above, please feel free to contact our Mr Dennis Chan at (deleted) or Ms Linly Chiu at (deleted)

Yours sincerely,

JPMorgan Chase Bank, N.A.
Hong Kong

香港小童群益會
The Boys' & Girls' Clubs Association of Hong Kong

敬啟者：

「個人資料（私隱）條例」諮詢意見書

本會多年來致力兒童及青少年服務，積極推動社會建構一個健康、安全和有利兒童成長的環境。個人資料(私隱)條例的內容能直接影響兒童的權利及利益，因此本會對此條例甚爲關注。

現隨函附上本會就此條例諮詢的意見，以作參考。如有任何進一步的查詢或意見，歡迎與本人聯絡。(　(刪除)　)

此致

政制及內地事務局

香港小童群益會總幹事

(已簽署)

羅淑君女士

二零零九年十一月二十五日

副本抄送：立法會政制事務委員會

香港小童群益會
The Boys' & Girls' Clubs Association of Hong Kong

「個人資料（私隱）條例」諮詢意見書

個人資料（私隱）條例（第 486 章）在 1996 年生效，隨著社會發展及轉變，個人權利以至兒童權利都更受關注及重視，如何在維護兒童權利與公衆利益，包括家長的照顧權之間取得平衡是社會各界值得討論的議題。本會多年來致力於兒童及青少年服務，推動社會大衆重視兒童的權利及利益，因此對諮詢文件中所提及與兒童特別有關連的建議尤其關注，以下將就諮詢文件建議第三項、十三項、十四項及二十七項提出有關意見。

建議 14：父母親查閱未成年人士個人資料的權利

現時條例容許兒童的父母親向資料使用者查閱其子女的個人資料，即使當中有濫用查閱資料機制的成分。我們同意如有合理理由（一）懷疑兒童的父母親為達到個人目的而拿取其子女的個人資料或（二）證實兒童的父母親曾有虐待兒童的紀錄的情況下，資料使用者有權拒絕父母的查閱要求。

至於當兒童在保密的情況下向資料使用者如社工透露某些個人資料，而同時該兒童已作出不同意該社工向其父母透露有關資料的明顯要求時，我們認爲應以尊重兒童的個人資料私隱權利為原則，配以社工的專業判斷，在不構成重大事故的環境下適當地拒絕父母的查閱要求。與此同時，我們理解到社會對於父母對兒童的照顧責任的關注，我們絕對肯定父母及家庭的照顧角色對兒童成長的重要性，但兒童與父母之間的溝通應建基於兩者之間的互信，而並不是透過第三者的私下查閱，這不單破壞兒童與父母之間的信任，也破壞了兒童與社工之間的信任，長遠地將影響兒童的個人利益。

建議 27：為了履行監護責任和家長照顧責任而把未成年人的個人資料轉移

現時條例並沒有容許資料使用者主動把兒童的個人資料轉移給其父母。我們認爲，社工應以尊重兒童的意願為原則，不應主動把該兒童的個人資料轉移給其父母。但與此同時，若社工認爲讓兒童的父母得知兒童的個人資料有助其父母履行他們的責任，並對兒童有著較佳的利益時，社工會利用專業判斷及專業手法鼓勵或勸導兒童主動將資料告知其父母，這亦是社工一向的處理手法，亦是較符合兒童利益的做法。

相反，假若容許社工主動把兒童的個人資料轉移給其父母，有可能牽起社工與家長之間很多不必要的爭拗，而最終的受害者就是兒童。其實，家長要得知子女的資料，使其有效地及適當地照顧子女，必須從建立良好的家庭及親子關係入手，建立彼此的互信，加強溝通，使子女視父母為其傾訴對象，才是最適切的關心方法。

建議13：由第三者給予訂明同意更改個人資料用途

如諮詢文件中所述，容許由第三者給予訂明同意更改個人資料用途的建議影響深遠，包括對醫療、教育、社會服務等重要服務的提供。因此，我們希望當局能進一步具體詳細地闡明當中的細節及影響，讓公衆能夠更深入討論並給予意見。

建議3：個人資料外洩通報機制

除了討論實施個人資料外洩後的通報機制外，個人資料外洩前的預防措施更爲重要。不少個人資料外洩個案均涉及互聯網、搜尋軟件、可攜式電子儲存裝置等以電子方式大量儲存的資料，外洩原因屬個人不慎使用多於外界惡意入侵，大多是可避免的。當局應加強有關預防方面的教育，讓公衆了解個人資料的重要性及保管個人資料的責任，並為各機構提供度身指導，幫助他們選擇較合適及有效的資料儲存方法及預防資料外洩的措施等，減低資料外洩事故的發生。

二零零九年十一月二十五日

S0144

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

民建聯 DAB

檢討《個人資料（私隱）條例》的諮詢文件

民建聯意見書

2009 年 11 月 30 日

一．背景及立場

《個人資料（私隱）條例》實施已超過十年，資訊及通訊科技的應用，及保障個人私隱的概念及要求，都較訂立法例的時期轉變不少。而自訂立私隱條例至今，亦發生了不少侵犯個人私隱的行為，但礙於法例未有規管，因而欠缺適當的制裁，而社會各界對此亦有相當的共識，就是要盡快修例堵塞漏洞。因此，民建聯歡迎政府在現階段就私隱條例進行檢討，以適應社會及時代的變化。

對於諮詢文件所提出的建議，民建聯的考慮原則是希望能於鼓勵資訊及通訊科技的持續發展，以及保障個人資料私隱之間，取得平衡；其次，便是以小心謹慎的態度去考慮任何違反保障資料原則的行為，訂為罪行的建議，以免嚴重影響到公民自由。

二． 具體意見

1. 敏感個人資料

諮詢文件建議立法訂明何謂“敏感個人資料”，並將收集或使用一些生物辨識的資料如瞳孔、掌紋及指模等的行為，作出更嚴格限制。民建聯對此持保留的態度。由於現時收集及使用生物辨識資料的通常做法，只會採取較少量的資料如收取面部或指模的數點數據，縱使被其他人偷取，亦無法將資料還原及重組成原有的面容或指模，故此，個人私隱不會因而受到損害。即使政府認為有確切需要對生物辨識資料的收集或使用作出規管，我們亦認為應以實務守則方式，由業界與私隱專員共同磋商，而據民建聯的理解，業界現正與專員就制訂指引方面，進行商討。

至於是否訂立“敏感個人資料”以及包括的範圍為何，我們認為，宜多諮詢及聽取市民的意見。對於公眾而言，何謂敏感資料的最直接決定，便是資料外洩後的結果，包括會否對當事人帶來極大

的損失或損害其嚴重，故不少市民認為應將一些如病歷、住址或性取向等資料列為“敏感個人資料”，政府因而可就此作出探討。更重要的是，無論是否劃分敏感或非敏感的個人資料，政府都應增撥資源，讓私隱公署能就如何正確使用及保障個人資料，推動更多宣傳及教育等的工作。

2. 規管資料處理者及分判活動

對於諮詢文件建議制訂“資料處理者”的定義，並對有關資料分判的行為作出規管。民建聯認為，既然不少資料使用者均會外判其資料處理工作予其他人，那些能夠接觸到個人私隱資料的人士，便應同樣遵守現有法例，因此，我們支持規管這些資料處理者。至於應採取甚麼規管模式，由於現行業界的分判模式極為細緻，基本上難以透過法律條文作出規管，故建議私隱專員應與業界商討，並制訂實務守則或指引，從而達致規管資料處理者的活動的目的。

3. 個人資料外洩通報機制

諮詢文件建議設立個人資料通報機制，民建聯認為是正確的一步，亦符合社會的期望。但對於諮詢文件傾向採用“自願性”的通報機制，則有所保留。我們認為，諮詢文件不贊成強制性的通報機制，是為免各機構因每次外洩事故都需通知所有受影響人士，因而承受沉重的負擔，然而，根據諮詢文件的建議，若要求各機構自行評估及衡量因外洩或遺失個人資料事故的影響性及損失程度，才決定是否通報，其後果只有兩種，一就是自行評估的做法同樣地對機構造成沉重的負擔，第二就是機構便索性不作任何通報，最終令到通報機制無法運作。

我們因此建議採用混合模式的做法：當出現資料外洩或遺失的情況，所有資料使用者都應“強制性”通知私隱專員；至於其後應否通知受事故影響的人士，則由私隱專員在接獲通知並經評估後，再決定是否發出指引，要求機構作出通知。由於專員對於外洩等事故的影響及損害程度，具有更專業的評估能力，故讓專員作出指引，將較各機構自行評估的做法，更具保障性；此舉亦可避免要求資料使用者無論外洩事故的影響性有多大，都要通知所有受影響人士，因而承受沉重的負擔。

民建聯 DAB

4. 在第66條下為資料當事人提供法律協助

個人資料私隱一旦受到侵害，市民現時只能透過民事訴訟去作出索償。但現實情況是，面對繁複的民事訴訟程序，以及被告往往是財雄勢大的資料使用者，受損失的當事人因而極少透過民事方式追討賠償。故此，我們贊成私隱專員可為有意提出法律訴訟的人士，提供相關的法律協助，讓受屈的一方能有更多資源去評估提出民事申索的機會。此外，由於專員過去曾投訴沒有足夠的資料，因而未能全面履行巡查工作的問題，為確保私隱公署能有效協助受影響人士，故建議政府應增加並確保公署具備足夠的資源，去履行此項新增的權力。

5. 向受屈的資料當事人判給補償

現時民事索償的費用高昂及程序繁複，令到受損失的人士極少透過民事方式追討賠償，諮詢文件建議授權專員就違反私隱條例的行為，釐定補償額，藉此為當事人提供多一個補救途徑。對於應否讓專員具有釐定補償額的權力，我們認同法改會的關注，即私隱專員的職責應只限於裁定任何行為有否違反保障資料原則，而不應具備釐定補償額的權力，有關權力應由法庭行使。

6. 把違反保障資料原則訂為罪行

民建聯認為，將違反保障資料原則的行為訂為罪行，必須小心謹慎地考慮，以免嚴重影響到公民自由。其實，不輕言以刑事手法去處理違反保障資料原則的行為，亦是在某個程度上保護資料當事人。原因是一旦涉及刑事檢控，便會將資料使用者與當事人置於對立面，使用者往往為了保障自己，只會集中精力於推卸刑責，而不會在發生事故時，立即作出補救措施，此將不利於經已受到影響的當事人，盡量減輕因資料外洩而受到的損失。

7. 在未經授權下取得、披露和出售個人資料

為維持本港的資訊自由，我們需要小心謹慎地考慮應否以刑事方式去規管一些侵害個人資料的行為，但對於一些傷害性較大的行為，確實需要依靠立法，才能確保受害人受到足夠的保障，以及對侵權者具相當性的阻嚇力。由於過去經常出現未經授權下取得、披露及出售個人資料的行為，有關情況亦證明造成的影響性及傷害性極大，要求立法已是社會的共識。我們因此支持對於未經授權而披

露個人資料，從中取利或作惡意用途的行為，訂為罪行。

至於何謂“惡意用途”，為免解釋流於主觀，容易令市民誤墮法網，最終影響到資訊交流及言論自由，我們建議可參考英國的做法，即引入明確的抗辯理由，相信做法已適當地在保障個人私隱與公眾利益之間，取得平衡。

8. 提高在直接促銷中不當使用個人資料的罰則

市民不時都受到不當直接促銷的騷擾，情況更達致令人煩燥的程度。然而，根據現時的法例，最高一萬元的罰款相對於大公司而言，確實難具阻嚇力，故此，我們建議提高有關罰款至五萬元，此罰則與違反專員發出執行通知的最高罰則相同，令處罰違法個人私隱的行為的所有罰則，具有一致性。

9. 由第三者給予訂明同意更改個人資料用途

諮詢文件針對現時法例只准許資料當事人自行更改其個人資料的用途，但基於部分當事人如未成年人或精神上無行為能力的人士未能充份了解更改用途的必要性，從而影響其使用醫療、教育或社會福利等服務，故建議授權“第三者”如父母或法庭委任的人，可代表資料當事人更改其個人資料的用途。我們認為，准許父母或監護人等為未成年人的重要利益，而代為更改其個人資料的用途，是值得探討的做法，但前提是必須確保用途的更改不會影響到未成年人的利益，故有必要制訂相關保障機制。

我們建議資料使用者在准許“第三者”更改未成年人的個人資料的用途時，必須考慮“在更改個人資料的用途後，不能令該資料當事人承受任何的刑事或民事上的責任”。此做法參考了“免受自我入罪”的基本人權概念，充分保障資料當事人的權利，以及確保父母有妥善照顧其子女的法律責任。

10. 父母親查閱未成年人士個人資料的權利

父母作為子女的監護人，毋論是基於履行照顧和監護子女的法律責任，又或出現父母本身的愛護子女之心，都會不時向資料使用者查閱其子女的個人資料。但隨着保障個人資料私隱的要求日漸提高，未成年子女的私隱能否毫無條件地被父母查閱，已受到社會的

民建聯 DAB

關注，諮詢文件探討此議題，有其必要性，特別是落實有關建議，或會破壞家庭成員間的信任。

另一方面，假若父母查閱子女的個人資料的最根本出發點，是基於子女的利益的話，要求父母提出一些合理理由，而非隨意地作出查閱，亦是某程度上保障未成年人的利益；再加上現實生活中，確曾出現有父母只為個人的目的而非子女的利益而查閱資料的個案，故適當地保障未成年人的利益，亦無不妥。在平衡子女的個人私隱與父母的查閱責任，我們建議，父母作出查閱要求時，資料使用者只需記錄查閱要求的理由即可，而非如諮詢文件的建議，資料使用者有權審核父母查閱的理由，甚至作出拒絕的權利。

11. 為了履行監護責任和家長照顧責任而把未成年人的個人資料轉移

在照顧未成人的利益的方面，協助父母或監護人盡早並確切地了解未成年人所面對的處境及狀況，相信有一定的幫助。現時，盡管社工或醫生等專業人士知道某青少年受到毒癮影響，但卻不能主動通知家長，讓他們多留意其子女，勸導及協助戒毒，此外，警方即使接獲內地移交的北上吸毒者，亦不能告之其父母，導致家長未能及時跟進曾北上吸毒的青年人。我們因而認同諮詢文件在有關方面的建議，訂定一定的豁免規定，讓未成年人的個人資料可轉移給父母或監護人，藉此保護未成年人和邊緣少年，以及使父母及監護人可妥善地履行適當照顧和監護兒童的責任。至於豁免的範圍或應具甚麼特定的條件，我們建議可考慮若青少年的行為涉及吸毒或嚴重罪行時，資料使用者便准許將未成年人的資料轉移給其父母或監護人，讓他們能及早知悉。我們相信此舉將有助打擊青少年吸毒問題。

- 完 -

S0146

市區重建局
URBAN RENEWAL AUTHORITY

Your Ref.: CMAB/CR/7/22/40 Pt. 7

30 November 2009

Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong

BY FAX & BY POST

Attn: Miss Joanna C. H. Choi

Dear Sirs,

RE: Public Consultation on the Review of the Personal Data (Privacy) Ordinance

Thank you for your letter dated 28 August 2009.

We are pleased to note that the Government with the support of the Privacy Commissioner of Personal Data (Privacy) Office has conducted a comprehensive review of the Personal Data (Privacy) Ordinance to cope with the changes brought to the Hong Kong economy due to the repaid advancement in information technology, prevalence of the internet and communications technology.

In general, we support your views described in the Consultation Paper. However, we also set out below our views to some proposals that you have invited for comments for your consideration:

1. Proposal No.2 : Regulation of Data Processors and Sub-contracting Activities
   We are of the view that direct regulations on the activities of data processors are more appropriate. Enforcement action taken by the Commissioner against data processors who are in breach of the PDPO is much more efficient than legal action on breach of contract initiated by data users against data processors.

2. Proposal No.7 : Making Contravention of a Data Protection Principle an Offence
   We do not agree to this proposal. We think that the present measure for the PCPD to issue an enforcement notice to a data user if the data user is in breach of a DDP

is sufficient to have a deterrent effect on the data user in breaching DDPs. Further, if the data user contravenes the enforcement notice, he will commit an offence under Section 64(7) of the PDPO. Hence, it is not necessary to make contravention of a DDP an offence.

3. Proposal No.9 : Making of Repeated Contravention of a Data Protection Principle after Enforcement

We do not agree with the proposal. We opine that the penalty, i.e. fine and imprisonment, for contravention of enforcement notice under Section 64(7) of the PDPO is sufficient. If a data user persistently contravenes a DDP after complying with an earlier enforcement notice, he should be issued another enforcement notices for compliance. To make the repeated contravention of DPP after compliance with earlier enforcement notice is too harsh.

We hope our views will be helpful to you.

Yours sincerely,

(Signed)

Pius K W Cheng
Director, Legal Services

30-NOV-2009 19:41 URBAN RENEWAL AU 99% TOTAL P.02
P.02

S0147

By Email and by Fax
Total 89 pages

30 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong
(Fax: 2523 0565)
(Email: pdpo_consultation@cmab.gov.hk)

Dear Sirs

Views and Comments on the Public Consultation on Review of the Personal Data (Privacy) Ordinance

I am writing to cordially request that the following Proposed Considerations be made on reviewing the Personal Data (Privacy) Ordinance ('**Ordinance**'):

Summary of Proposed Considerations

1. In considering any **contravention** under the Ordinance, the following considerations on the personal data concerned must be made (please refer to *Michael Noel James Hosking and Marie Angela Hosking v Simon Runting and Others* (CA101/03, 25 March 2004, New Zealand Court of Appeal Judgment, para. 15, **enclosed**):

    a. **That the disclosure of the private facts must be a public disclosure and not a private one.**

    b. **Facts disclosed to the public must be private facts and not public ones.**

    c. **The matter made public must be one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.**

    d. **The nature and extent of legitimate public interest in having the information disclosed must be weighed.**

Above Judgment also provides proper and useful information on reviewing the Ordinance.

S0147

2. The Ordinance must require that **the personal data concerned be clearly stated** in any investigation, enforcement notice, or notice of offence (if applicable). In a letter dated 16 August 2006 issued by the Privacy Commissioner for Personal Data ('**Commissioner**') that contained a Result of Investigation and an Enforcement Notice ('**EN**' copy **enclosed**) it was merely stated that the personal data of the data subject "including his name and other identifying particulars" without stating what "other identifying particulars" were.

3. That **the burden of proof must be laid on the Commissioner**. In the EN, the data user was requested to remove a forum (http://www.hkedcity.net/mediaEd/forum) in the internet that did not exist (**enclosed** copy of Exhibit D1 of the court case TMS12120/2007). Furthermore, in the appeal no. 46/2006 to the AAB against the EN, the Commissioner did not produce the major piece of evidence, namely the Recorded Conversations, to the AAB, and the AAB refused to consider the contents of the Recorded Conversations (para. 43 of AAB's decision dated 17 April 2007, **enclosed**). In the EN, the Commissioner directed the data user to remove said Recorded Conversations in the internet. It also stated in the EN that there were no personal data in the Recorded Conversations (para. 11 of EN).

4. That the **jurisdiction and power of the Commissioner** conferred under the Ordinance must be **confined to personal data**. In the EN, the Commissioner directed the data user to remove the Recorded Conversations even though the Recorded Conversations did not contain any personal data as stated in the EN (para. 11 of EN). In exercising his power in excess of jurisdiction, the Commissioner may have trespassed the right of individuals of freedom of speech, of the press and of publication (Article 27 of the Basic Law), and freedom of opinion and express (Article 16 of the Hong Kong Bill of Rights CAP 383).

5. In considering any contravention of the Ordinance, **exemption under the Ordinance must be considered**. In a letter by the Commissioner date 19 March 2007 (**enclosed**) regarding the AAB appeal no. 46/2006, the Commissioner stated that "there is no duty on the Respondent (here it means the Commissioner) to fish for exemption provision" (para. 3 in letter dated 19 March 2007). Furthermore, the AAB decision also stated that "The Commissioner is not bound by the Ordinance to consider the issue of exemption at large" (para. 27(c) of AAB's decision).

6. In consideration of of granting criminal investigation and prosecution power to the Commissioner, and making contraventaion of a data protection principle an offence, it is suggested that **such considerations be cancelled at this stage** to avoid misuse of power by the Commissioner, and that the Commissioner has yet to demonstrate its proper exercise of power conferred under the Ordinance.

Please feel free to contact me should you need further information regarding the suggestions.

Thank you very much for your considerations.

Yours truly

(Signed)

(name)

(The sender requested anonymity.
Annexes not attached)

S0148



To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject [Revised]: Proposal on Cosultation Document on Review of the Personal Data (Privacy) Ordinance by iProA and ISACA

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

30/11/2009 19:07

To-Secretariat-for Constitutional and Mainland Affairs,

As we have some final amendment by our members later today, we would like to submit our revised version as attached for your review.

We are sorry for the inconvenient caused

Thanks

Gary

S0148



Response to Consultation Document on Review of the Personal Data (Privacy) Ordinance

By

Internet Professional Association & ISACA China Hong Kong Chapter

November 30, 2009

Contents

Introduction 3
Proposal No.1: Sensitive Personal Data 4
Proposal No. 2: Regulation of Data Processors and Sub-Contracting Activities 4
Proposal No.3: Personal Data Security Breach Notification 5
Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD 6
Proposal No.5: Legal Assistance to Data Subjects under Section 66 6
Proposal No.6: Award Compensation to Aggrieved Data Subjects 6
Proposal No.7: Making Contravention of a Data Protection Principle an Offence 7
Proposal No.8: Unauthorized Obtaining, Disclosure and Sale of Personal Data 7
Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts 7
Proposal No.10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles 7
Proposal No.11: Repeated Non-compliance with Enforcement Notice 8
Proposal No 12: Raising Penalty for Misuse of Personal Data in Direct Marketing 8
Proposal No 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data 8
Proposal No 14: Parent's Right to Access Personal Data of Minors 8
Proposal No 15: Access to Personal Data in Dispute 9
Proposal No 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation 9
Proposal No 17: Erasure of Personal Data 9
Conclusion 10
About iProA (Internet Professional Association) 10
About ISACA ® China HK Chapter: 11

Introduction

By and large, we are in favour of bringing the Ordinance up-to-date to ensure adequate protection to personal data, but we dissent on some facts of the Proposals, especially where IT and technology related issues are concerned.

It's beyond dispute that IT will continue to play a critical role in transforming our lives and society, and technology participants and developers must be given sufficient free hand and discretion to continue their innovation and development. We urge the Government to exercise extreme prudence when seeking to introduce any legislative amendments that would have the effect of potentially stifling any innovation, and thereby hurting the job market. The value created by innovation far outweighs the risks to privacy and security, and once the opportunity is gone, we would be forever trying to catch up with our neighbors, bidding farewell to our hard-earned competitive edge.

In particular, we'd like to point out that ***legislation is not the best tool to fix matters involving ever- evolving technology.*** We must acknowledge that technology development is very different from other disciplines, not the least of which is its ever evolving nature, which by itself stands at the opposite end of legislation which is meant to be robust, stand the test of time, and to last, at least for a good number of years. As such, neither legislation nor the Government is the best tool to fix it. The worst scenario is a dangerous combination of an uncertain legal framework with ongoing as well as emerging challenges to a free and open Internet.

In fact, with a totally new phenomenon brought by web 2.0, an individual's "privacy right is ZERO", as quoted by an IT practitioner and celebrity, Social networks such as Facebook have emerged as a new means of communication for all ages, business and social sectors, providing platforms for sharing and for free flow of information. Undue control over the participants may deprive all stakeholders, ourselves included, of a useful means of communication of untold potential. Public education is a preferred means to safeguard privacy in the long term rather than imposing regulations.

Having made our point, we are in favor of "**fair and reasonable**" amendments. In the following paragraphs, we'll provide our views on the various Proposals, focusing primarily on IT-related aspects:

Proposal No.1: Sensitive Personal Data

We are neutral to the proposal to introduce a new "sensitive data" category which would be subject to more stringent regulation. We should first start with a minimal set of sensitive personal data, which are really considered important, and may then add to the list only when necessary. Drawing reference from other countries, we think data such as "sexual life", "health or physical condition" are unlikely to be controversial. On the other hand, we're confounded by the Proposal which singled out biometrics as sensitive data. We strongly oppose making biometric information sensitive personal data, as by doing so, PCPD would deter, if not prohibit, the collection of such information for further development and usage of new technologies and applications. As technologies advance, our routine life-style has to change and adapt accordingly, else we run the risk of being left behind if not entirely left out. Many countries are developing applications using biometric data, and some of them are very advanced in the adoption of biometrics technology. If at this stage we take a broad brush approach to classify biometrics as sensitive personal data and subject them to more stringent regulations, this would amount to an undesirable act of interfering with and adding burden to local research and development. The singling out of "biometrics" in the Consultation as a potential candidate for sensitive data has already left the vendors and developers in biometrics very unsettled, resulting in major losses of business. Uncertainties abound, and it's difficult to reach a consensus on how biometrics should be defined and treated. **As such, we strongly advocate that Guidelines are more appropriate in dealing with biometrics than legislation.**

On the other hand, we strongly oppose the imposition of any criminal liability or a term of imprisonment in relation to non-compliance with DPPs with regard to the handling of sensitive personal data, as data users may be caught in an inadvertent act or omission. This will scare data users, increase their administrative cost, or force them to consider moving their business outside Hong Kong. Instead, we suggest PCPD to facilitate the collection of sensitive personal data by providing clear and comprehensive procedures and guidelines in collecting, handling, and protecting such data as well as any remedial actions that data users need to take in case of data leakage. We agree with the view to revise the existing level of fine and accept the proposal of increasing the monetary fine value. PCPD should provide clear definitions of the different levels of penalty and the conditions under which data users are considered to have violated the principles.

Proposal No. 2: Regulation of Data Processors and Sub-Contracting Activities

For better safeguard of personal data, we hold the view that data processors or third party subcontractors should exercise the same level of care and diligence as is required of data users. As such, we support the proposal that data users should be required to use contractual or other measures to secure compliance with

the relevant PCPD obligations when they outsource to third parties. On the other hand, we are not in favor of directly regulating data processors as this would make the regulatory framework unduly cumbersome, increase costs of operation and affect Hong Kong's competiveness. A lot of outsourcing businesses will be lost to other places which have less stringent regulatory regime, and this would hurt our job market and economic growth.

PCPD should leave no uncertainty in defining or identifying who are the parties classified as "data processors". The new class of social network websites presents a particular challenge as they can be perceived as both data users and data processors, with different obligations under each category. As an emerging and increasingly popular platform for free sharing and free flow of communication, we do not want to see too many constraints imposed on such social networking websites.

Proposal No.3: Personal Data Security Breach Notification

This is a good suggestion, at least in setting out procedures / steps for corporations to follow in case of data leakage. We support the view of PCPD that a requirement to notify all affected parties of each and every personal data leakage incident is costly to organizations and individuals. In addition, those same recipients who receive too many breach notices may have difficulty to assess which ones carry a real risk of harm and which ones are minor in nature and consequence. Or they may become desensitized to the notices and ignore some of the notices. Considering that a number of overseas jurisdictions adopt voluntary guidelines on privacy breach notifications, we agree with PCPD to start with a voluntary breach notification system so that we can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing undue burden on the community. We highly appreciate that the PCPD would issue clear guidelines on voluntary privacy breach notification.

On the issue of which circumstances that notification should be triggered, we think that the primary concern of the public is whether their sensitive information may allow criminals to take advantage and cause them to suffer financial loss. In this regard, we suggest if the leakage of personal data that involves any identity information, such as ID card number, passport number, and financial information such as credit card numbers, bank statements or transaction information, or insurance details etc., then the notification should be triggered; such notification should be sent to the PCPD and data subject; the time of notification should be right after the organization's risk assessment which has determined to trigger notification; the means of notifications could be mail, email, sms or phone calls, allowing different means of notification to mitigate the notification cost incurred by the organizations; the content of the notifications should include the leakage information, when and what to be alerted as well as the organizations' remedial actions.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

We are completely against granting more power to PCPD. We see no compelling reason to give it the power to investigate into and prosecute criminal offence cases because, as mentioned in the consultation, effective protection to personal data privacy hinges on the adequacy of penalty sanction, rather than on whom the party responsible for initiating prosecution is. Besides, the number of cases referred to for prosecution every year is manageable and do not see any trend of acute increase.

Proposal No.5: Legal Assistance to Data Subjects under Section 66

We do see a need to confer the PCPD with the power to provide legal assistance to aggrieved data subject because victims of the contravention of personal data protection cannot afford the huge cost for civil action, especially dealing with the government or large corporations. There are various legal action funds organized by government departments, for example Consumer Council which aims to assist and help people who cannot afford the cost of civil action on similar cases, and we suggest using this as a reference in reviewing whether we should provide legal assistance to victims of the contravention of personal data protection. Of course, we need to strike a good balance between providing legal aid for people with real needs and avoiding other people who just want to try their luck.

Proposal No.6: Award Compensation to Aggrieved Data Subjects

We should leave this in the hands of the judge. It is very strange to give PCPD that kind of right because firstly, we are concerned that awarding compensation would vest in a single authority an undesirable combination of enforcement and punitive functions as mentioned in the consultation paper. Secondly, we are concerned about the complexity and credibility in determining the judicious compensation amount, and any dispute on the amount will have to be settled in court eventually. Besides, if the PCPD have the power to determine the amount of compensation, it may lead to abuse since many people may just try their luck if there is no need to go through the court process, as a result of which the PCPD would have to handle many more cases that may not originally be eligible for compensation. Furthermore, the PCPD would have to expand its scale in investigation and enforcement activities; the expenditure budget of the PCPD would increase as a result.

Proposal No.7: Making Contravention of a Data Protection Principle an Offence

We would say "NO" loud and clear, as many IT practitioners would be caught in cases of inadvertent act or omission, and the uncertainty of the operating environment would be very damaging. We however support increasing the existing penalty levels to reinforce the deterrent effect.

Proposal No.8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

We do not agree to make unauthorized obtaining and disclosure of personal data an offence because it is very difficult to define if the person knowingly or mistakenly obtains or discloses personal data without consent. Instead, we would prefer data users to be contractually bound with their employees or sub-contractors, such that these parties clearly know their obligations towards others' personal data; and that disclosure and sale of personal data would become a commercial crime and should be handled by police.
The penalty of Unauthorized Obtaining, Disclosure and Sale of Personal Data could be increased to double or triple the current level as a deterrent.

Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts

Again, we're opposed to introducing crime or offences. As PCPD has not come across any case of circumvention of resuming the same contravening act or practice shortly after compliance with an enforcement notice issued against him, there is no compelling argument to make such act an offence. Instead, the penalty level could increase if there are repeated enforcement notices being issued.

Proposal No.10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

This should be left to the judge. Empowering the PCPD to determine monetary penalty on serious contravention of DPPs would involve the complexity of granting PCPD both the power of legislation and enforcement within a single department. This may not be welcomed. Apart from this complexity, we agree with the view of empowering PCPD to require data users to pay monetary penalty for serious contravention of DPPs, provided that a comprehensive guideline on the circumstances where PCPD considers appropriate

to issue a monetary penalty notice is well prepared and both data subject and users are well educated on this.

Proposal No.11: Repeated Non-compliance with Enforcement Notice

This needs clarification. On balance, we think that doubling the penalty level for repeated non-compliance with Enforcement notice would serve as effective deterrents, which would mean a new fine of up to $100,000, and in the case of a continuing offence, a new daily fine of $2,000. However, we do not agree to increase the sentence, which should stay at two years.

Proposal No 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

This requires clarification as it would impact on the marketing industry. We agree with the view of raising Penalty for Misuse of Personal Data in Direct Marketing subject to a comprehensive guidance on how such penalty is imposed on direct marketing companies. Every business requires promotion and follow-up services, and direct marketing plays an important part, which should not be unduly restrained. The penalty level can be raised to $50,000.

Proposal No 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data

We agree to adopt the definition of "relevant person" under the PDPO and include the guardians of data subjects with mental incapacity as the definition of third party to give consent to the change of use of personal data of vulnerable classes of data subjects.

Proposal No 14: Parent's Right to Access Personal Data of Minors

Parents have the natural duty to take care of their children, and that includes having access to their data if necessary. We do not agree to introduce new provisions to permit a data user to refuse a data access request made by a "relevant person". It is inappropriate for data user to make the decision on whether refusing the access really would protect the interest of the minors. In case of suspected child abuse, the data user should report to the authority and let the court make the decision. After all, Hong Kong has a sound law

enforcement and legal system in place, and there is no need for everybody to try and play judge.

Proposal No 15: Access to Personal Data in Dispute

We agree with the proposal to add the provision under the PDPO that, where the lawfulness of a refusal to comply with a data access request is in dispute before the AAB, a court or a magistrate, the relevant personal data should not be disclosed to the data requestor and other parties bound by the decision of the AAB, the court or magistrate, whether by discovery or otherwise, pending a determination in favor of the requestor. By doing so, it can effectively prevent the complainant from accessing the requested data should it ultimately rule that the data user's refusal to comply with the data access request was lawful. On the other hand, it is just a matter of time for data subject to have access to the requested data should the ultimate rule be in favor of the data subject.

Proposal No 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We agree with the proposal to add the provision of a new ground for a data user to refuse to comply with a data access request under Section 20(3) where the data user is obliged or entitled under any other ordinance not to disclose the personal data. In doing so, it clears the data user's dilemma of breaching the data access provision

Proposal No 17: Erasure of Personal Data

We agree with the view that PDPO requirements should not be such as to pose an excessive burden on businesses. We are neutral to the proposal on amending the PDPO so that the provisions concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use.

Conclusion

As we engage in the process of bringing in "fair and reasonable' amendments to the PCPD, we remain concerned that the unintended consequences of regulation could bring harm to consumers and affect the ability of the Internet and other technology sectors to innovate, to contribute to economic growth and productivity, to create new jobs, and to deliver social benefits to our community.

Issues in connection with IT and those arising from the advancement and application of IT are perhaps best dealt with by the IT professionals, rather than legislation. In this regard, we especially advocate that "biometrics" should be dealt with separately under a set of "Guidelines", to be supplemented by forums and seminars and publicity to educate the public and the community on its usage, and to build an open platform on which biometrics developers can come up with more innovative applications.

Submission by iProA & ISACA

About iProA (Internet Professional Association)

iProA is a non-profit making professional organization founded in December 1999. It represents over 2,300 professionals from Internet related industries, including CEOs and senior executives from leading information technology enterprises. Our members have made contributions in areas like innovative design, sales, marketing, infrastructure, e-commerce, consultancy, investment and other Internet related professional services, aiming to further develop the Internet industry in Hong Kong. We share the common goal of promoting the proper application of Internet technology and enhancing competitiveness of the IT industry. We work towards improving professionalism of information technology practitioners, encouraging IT professionals to share social responsibilities, as well as striving to bridge the digital divide in Hong Kong. Please visit website www.iproa.org for further information.

About ISACA ® China HK Chapter:

- Established in 1982
- Just celebrated 25th Anniversary in 2007
- Around 2,000 members
- One of the largest chapters worldwide

The objectives of ISACA ® China HK Chapter:

The primary purpose of the Chapter is to promote the education of individuals for the improvement and development of their capabilities relating to the auditing of and/or management consulting in the field of information systems audit and control. The objectives of the Chapter are:

- To promote the education of, and help expand the knowledge and skills of its members in the interrelated fields of auditing, quality assurance, security, and information systems audit and control;
- To encourage a free exchange of information systems audit and control, quality assurance, and security techniques, approaches and problem solving by its members;
- To promote adequate communication to keep members abreast of current events in information systems audit and control, quality assurance, and security fields that can be of benefit to them and their employers, and
- To communicate to management, auditors, universities and to information systems professionals the importance of establishing controls necessary to ensure the effective organisation and utilisation of information technology resources.

P 1/2

檢討《個人資料(私隱)條例》公眾諮詢

重點

二零零九年八月

引言

《個人資料(私隱)條例》("私隱條例")在1996年生效，政制及內地事務局在個人資料私隱專員("私隱專員")的協助下，就私隱條例進行了全面的檢討，研究隨着過去十年的發展，包括科技的進步，私隱條例的現有條文是否仍足以保障個人資料。

指導原則

在進行檢討時，我們以下述原則為依據：

- 個人的私隱權不是絕對的，必須與其他權利以及其他公眾及社會利益取得平衡；
- 需要在保障個人資料私隱與便利資訊及通訊科技持續發展之間取得平衡；
- 對私隱法例作出的任何修改，都不應削弱香港作為國際城市的競爭力和經濟效率；
- 需要避免商業活動和個別資料使用者承受沉重的負擔；
- 應充分考慮本地的情況；
- 私隱條例在科技轉變中應仍具彈性並且合時；
- 立法干預未必一定是最有效方法，在某些情況下，推行行政措施可達到保障個人資料私隱的效果。
- 社會對私隱課題有相當程度的共識至為重要。

我們就私隱條例提出了多項修訂建議，有關修訂或會對社會各界、公營部門、私營機構和市民有深遠影響。對於這些建議，我們持開放態度，歡迎市民就此提出意見。

主要建議

敏感個人資料

- 敏感個人資料(如指紋)應否受更嚴格的規管？ → 應該

資料保安

- 應否規管受託處理個人資料的資料處理者？ → 應該
- 應否規定資料使用者在發生個人資料外流事故時通知私隱專員及受影響的人士？ → 應該

私隱專員的權力

- 應否賦予私隱專員刑事調查和檢控的權力？ → 應該
- 若有資料當事人因資料使用者違反私隱條例的規定而蒙受損失並有意向資料使用者提出法律訴訟，應否授權私隱專員為受屈的資料當事人提供法律協助？ → 應該
- 應否授權私隱專員向受屈的資料當事人判給補償？ → 應該

進行及制裁

- 應否把違反保障資料原則訂為罪行？ → 不應該
- 應否把該罪未經資料使用者同意下取得的個人資料而從中取利或作惡意用途的行為訂為罪行？ → 不應該
- 應否把資料使用者已進行私隱專員發出的執行通知的規定，但不久又故意重犯的行為訂為罪行？ → 不應該
- 應否授權私隱專員就嚴重違反保障資料原則的行為宣布罰款？ → 不應該
- 應否將屢次違反執行通知的行為處以更重的懲罰？ → 應該
- 應否提高在直接促銷活動中不當使用個人資料的罰則？ → 應該

資料當事人的權利

- 應否授權第三者就更改未成年人或精神上無行為能力的人的個人資料用途給予同意？ → 應該
- 如資料使用者依從父母代其未成年子女提出的查閱資料要求並不符合子女的最佳利益，我們應否准許資料使用者拒絕該查閱要求？ → 不應該准許資料使用者拒絕該查閱要求

豁免適從私隱條例

- 應否向執法機關以及救護和支援機構給予豁免，以在緊急情況下處理個人資料？ → 應該
- 如未成年人的個人資料與家長或監護人履行照顧和監護責任有關，我們應否准許資料使用者把該等資料轉移給未成年人的父母或監護人？ → 應准許

你的意見

諮詢文件可從各區民政事務處索取或從本局的網頁下載(網址：www.cmab.gov.hk)，請在2009年11月30日或之前，以郵寄、傳真或電郵方式提交意見或建議：

地址　香港下亞里畢道
中區政府合署東座364室
政制及內地事務局(第4組)

傳真號碼　2523 0565

電郵地址：pdpo_consultation@cmab.gov.hk

S0149

補充

S0149

(低入標者的補充文件)

另外，有關閣下提出建議如下（大意：...）：

下見下的...（包括...）

和機構...

(i) ...

(ii) 關於...（例如...）。本公司...

...

(iii) ...

(iv) ...

(v) ...

(vi) ...

(vii) ...

(viii) ...

(ix) ...

(x) ...

(xi) ...

(xii) ...

(xiii) ...

(xiv) ...

(xv) ...

(xvi) ...

(xvii) ...

(xviii) ...

(xix) ...

(xx) ...

(xxi) ...

(xxii) ...

(xxiii) ...

(xxiv) ...

(xxv) ...

(xxvi) ...

(xxvii) ...

(xxviii) ...

(xxix) ...

(xxx) ...

(xxxi) ...

(xxxii) ...

(xxxiii) ...

(xxxiv) ...

(xxxv) ...

(xxxvi) ...

(xxxvii) ...

(xxxviii) ...

(xxxix) ...

(xl) ...

(xli) ...

(xlii) ...

(xliii) ...

(xliv) ...

(xlv) ...

(xlvi) ...

(xlvii) ...

(xlviii) ...

(xlix) ...

(l) ...

(li) ...

(lii) ...

(liii) ...

(liv) ...

(lv) ...

(lvi) ...

(lvii) ...

(lviii) ...

(lix) ...

(lx) ...

(lxi) ...

(lxii) ...

(lxiii) ...

(lxiv) ...

(lxv) ...

(lxvi) ...

(lxvii) ...

(lxviii) ...

(lxix) ...

(lxx) ...

(lxxi) ...

(lxxii) ...

(lxxiii) ...

(lxxiv) ...

(lxxv) ...

(lxxvi) ...

(lxxvii) ...

(lxxviii) ...

(lxxix) ...

(lxxx) ...

(lxxxi) ...

(lxxxii) ...

(lxxxiii) ...

(lxxxiv) ...

(lxxxv) ...

(lxxxvi) ...

(lxxxvii) ...

(lxxxviii) ...

(lxxxix) ...

(xc) ...

(xci) ...

(xcii) ...

(xciii) ...

(xciv) ...

(xcv) ...

(xcvi) ...

(xcvii) ...

(xcviii) ...

(xcix) ...

(c) ...

(ci) ...

(cii) ...

(ciii) ...

(civ) ...

(cv) ...

(cvi) ...

(cvii) ...

(cviii) ...

(cix) ...

(cx) ...

(cxi) ...

(cxii) ...

(cxiii) ...

(cxiv) ...

(cxv) ...

(cxvi) ...

(cxvii) ...

(cxviii) ...

(cxix) ...

(cxx) ...

(cxxi) ...

(cxxii) ...

(cxxiii) ...

(cxxiv) ...

(cxxv) ...

(cxxvi) ...

(cxxvii) ...

(cxxviii) ...

(cxxix) ...

(cxxx) ...

(cxxxi) ...

(cxxxii) ...

(cxxxiii) ...

(cxxxiv) ...

(cxxxv) ...

(cxxxvi) ...

(cxxxvii) ...

(cxxxviii) ...

(cxxxix) ...

(cxl) ...

(cxli) ...

(cxlii) ...

(cxliii) ...

(cxliv) ...

(cxlv) ...

(cxlvi) ...

(cxlvii) ...

(cxlviii) ...

(cxlix) ...

(cl) ...

(cli) ...

(clii) ...

(cliii) ...

(cliv) ...

(clv) ...

(clvi) ...

(clvii) ...

(clviii) ...

(clix) ...

(clx) ...

(clxi) ...

(clxii) ...

(clxiii) ...

(clxiv) ...

(clxv) ...

(clxvi) ...

(clxvii) ...

(clxviii) ...

(clxix) ...

(clxx) ...

(clxxi) ...

(clxxii) ...

(clxxiii) ...

(clxxiv) ...

(clxxv) ...

(clxxvi) ...

(clxxvii) ...

(clxxviii) ...

(clxxix) ...

(clxxx) ...

(clxxxi) ...

(clxxxii) ...

(clxxxiii) ...

(clxxxiv) ...

(clxxxv) ...

(clxxxvi) ...

(clxxxvii) ...

(clxxxviii) ...

(clxxxix) ...

(cxc) ...

(cxci) ...

(cxcii) ...

(cxciii) ...

(cxciv) ...

(cxcv) ...

(cxcvi) ...

(cxcvii) ...

(cxcviii) ...

(cxcix) ...

(cc) ...

(cci) ...

(ccii) ...

(ccciii) ...

(cciv) ...

(ccv) ...

(ccvi) ...

(ccvii) ...

(ccviii) ...

(ccix) ...

(ccx) ...

(ccxi) ...

(ccxii) ...

(ccxiii) ...

(ccxiv) ...

(ccxv) ...

(ccxvi) ...

(ccxvii) ...

(ccxviii) ...

(ccxix) ...

(ccxx) ...

(ccxxi) ...

(ccxxii) ...

(ccxxiii) ...

(ccxxiv) ...

(ccxxv) ...

(ccxxvi) ...

(ccxxvii) ...

(ccxxviii) ...

(ccxxix) ...

(ccxxx) ...

(ccxxxi) ...

(ccxxxii) ...

(ccxxxiii) ...

(ccxxxiv) ...

(ccxxxv) ...

(ccxxxvi) ...

(ccxxxvii) ...

(ccxxxviii) ...

(ccxxxix) ...

(ccxl) ...

(ccxli) ...

(ccxlii) ...

(ccxliii) ...

(ccxliv) ...

(ccxlv) ...

(ccxlvi) ...

(ccxlvii) ...

(ccxlviii) ...

(ccxlix) ...

(ccl) ...

(cclii) ...

(ccliii) ...

(ccliv) ...

(cclv) ...

(cclvi) ...

(cclvii) ...

(cclviii) ...

(cclix) ...

(cclx) ...

(cclxi) ...

(cclxii) ...

(cclxiii) ...

(cclxiv) ...

(cclxv) ...

(cclxvi) ...

(cclxvii) ...

(cclxviii) ...

(cclxix) ...

(cclxx) ...

(cclxxi) ...

(cclxxii) ...

(cclxxiii) ...

(cclxxiv) ...

(cclxxv) ...

(cclxxvi) ...

(cclxxvii) ...

(cclxxviii) ...

(cclxxix) ...

(cclxxx) ...

(cclxxxi) ...

(cclxxxii) ...

(cclxxxiii) ...

(cclxxxiv) ...

(cclxxxv) ...

(cclxxxvi) ...

(cclxxxvii) ...

(cclxxxviii) ...

(cclxxxix) ...

(ccxc) ...

(ccxci) ...

(ccxcii) ...

(ccxciii) ...

(ccxciv) ...

(ccxcv) ...

(ccxcvi) ...

(ccxcvii) ...

(ccxcviii) ...

(ccxcix) ...

(ccc) ...

(ccci) ...

(cccii) ...

(ccciii) ...

(ccciv) ...

(cccv) ...

(cccvi) ...

(cccvii) ...

(cccviii) ...

(cccix) ...

(cccx) ...

(cccxi) ...

(cccxii) ...

(cccxiii) ...

(cccxiv) ...

(cccxv) ...

(cccxvi) ...

(cccxvii) ...

(cccxviii) ...

(cccxix) ...

(cccxx) ...

(cccxxi) ...

(cccxxii) ...

(cccxxiii) ...

(cccxxiv) ...

(cccxxv) ...

(cccxxvi) ...

(cccxxvii) ...

(cccxxviii) ...

(cccxxix) ...

(cccxxx) ...

(cccxxxi) ...

(cccxxxii) ...

(cccxxxiii) ...

(cccxxxiv) ...

(cccxxxv) ...

(cccxxxvi) ...

(cccxxxvii) ...

(cccxxxviii) ...

(cccxxxix) ...

(cccxl) ...

(cccxli) ...

(cccxlii) ...

(cccxliii) ...

(cccxliv) ...

(cccxlv) ...

(cccxlvi) ...

(cccxlvii) ...

(cccxlviii) ...

(cccxlix) ...

(cccl) ...

(ccclii) ...

(cccliii) ...

(ccclv) ...

(ccclvi) ...

(ccclvii) ...

(ccclviii) ...

(ccclix) ...

(ccclx) ...

(ccclxi) ...

(ccclxii) ...

(ccclxiii) ...

(ccclxiv) ...

(ccclxv) ...

(ccclxvi) ...

(ccclxvii) ...

(ccclxviii) ...

(ccclxix) ...

(ccclxx) ...

(ccclxxi) ...

(ccclxxii) ...

(ccclxxiii) ...

(ccclxxiv) ...

(ccclxxv) ...

(ccclxxvi) ...

(ccclxxvii) ...

(ccclxxviii) ...

(ccclxxix) ...

(ccclxxx) ...

(ccclxxxi) ...

(ccclxxxii) ...

(ccclxxxiii) ...

(ccclxxxiv) ...

(ccclxxxv) ...

(ccclxxxvi) ...

(ccclxxxvii) ...

(ccclxxxviii) ...

(ccclxxxix) ...

(cccxc) ...

(cccxci) ...

(cccxcii) ...

(cccxciii) ...

(cccxciv) ...

(cccxcv) ...

(cccxcvi) ...

(cccxcvii) ...

(cccxcviii) ...

(cccxcix) ...

(cccc) ...

(ccccii) ...

(ccccciii) ...

(ccccciv) ...

(ccccv) ...

(ccccvi) ...

(ccccvii) ...

(ccccviii) ...

(ccccix) ...

(ccccx) ...

(ccccxi) ...

(ccccxii) ...

(ccccxiii) ...

(ccccxiv) ...

(ccccxv) ...

(ccccxvi) ...

(ccccxvii) ...

(ccccxviii) ...

(ccccxix) ...

(ccccxx) ...

(ccccxxi) ...

(ccccxxii) ...

(ccccxxiii) ...

(ccccxxiv) ...

(ccccxxv) ...

(ccccxxvi) ...

(ccccxxvii) ...

(ccccxxviii) ...

(ccccxxix) ...

(ccccxxx) ...

(ccccxxxi) ...

(ccccxxxii) ...

(ccccxxxiii) ...

(ccccxxxiv) ...

(ccccxxxv) ...

(ccccxxxvi) ...

(ccccxxxvii) ...

(ccccxxxviii) ...

(ccccxxxix) ...

(ccccxl) ...

(ccccxli) ...

(ccccxlii) ...

(ccccxliii) ...

(ccccxliv) ...

(ccccxlv) ...

(ccccxlvi) ...

(ccccxlvii) ...

(ccccxlviii) ...

(ccccxlix) ...

(ccccl) ...

(cccclii) ...

(ccccliii) ...

(cccclv) ...

(cccclvi) ...

(cccclvii) ...

(cccclviii) ...

(cccclix) ...

(cccclx) ...

(cccclxi) ...

(cccclxii) ...

(cccclxiii) ...

(cccclxiv) ...

(cccclxv) ...

(cccclxvi) ...

(cccclxvii) ...

(cccclxviii) ...

(cccclxix) ...

(cccclxx) ...

(cccclxxi) ...

(cccclxxii) ...

(cccclxxiii) ...

(cccclxxiv) ...

(cccclxxv) ...

(cccclxxvi) ...

(cccclxxvii) ...

(cccclxxviii) ...

(cccclxxix) ...

(cccclxxx) ...

(cccclxxxi) ...

(cccclxxxii) ...

(cccclxxxiii) ...

(cccclxxxiv) ...

(cccclxxxv) ...

(cccclxxxvi) ...

(cccclxxxvii) ...

(cccclxxxviii) ...

(cccclxxxix) ...

(ccccxc) ...

(ccccxci) ...

(ccccxcii) ...

(ccccxciii) ...

(ccccxciv) ...

(ccccxcv) ...

(ccccxcvi) ...

(ccccxcvii) ...

(ccccxcviii) ...

(ccccxcix) ...

(ccccc) ...

(cccccii) ...

(ccccciii) ...

(cccccciv) ...

(ccccv) ...

(ccccvi) ...

(ccccvii) ...

(ccccviii) ...

(ccccix) ...

(ccccx) ...

(ccccxi) ...

(ccccxii) ...

(ccccxiii) ...

(ccccxiv) ...

(ccccxv) ...

(ccccxvi) ...

(ccccxvii) ...

(ccccxviii) ...

(ccccxix) ...

(ccccxx) ...

(ccccxxi) ...

(ccccxxii) ...

(ccccxxiii) ...

(ccccxxiv) ...

(ccccxxv) ...

(ccccxxvi) ...

(ccccxxvii) ...

(ccccxxviii) ...

(ccccxxix) ...

(ccccxxx) ...

(ccccxxxi) ...

(ccccxxxii) ...

(ccccxxxiii) ...

(ccccxxxiv) ...

(ccccxxxv) ...

(ccccxxxvi) ...

(ccccxxxvii) ...

(ccccxxxviii) ...

(ccccxxxix) ...

(ccccxl) ...

(ccccxli) ...

(ccccxlii) ...

(ccccxliii) ...

(ccccxliv) ...

(ccccxlv) ...

(ccccxlvi) ...

(ccccxlvii) ...

(ccccxlviii) ...

(ccccxlix) ...

(ccccl) ...

(cccccli) ...

(ccccclii) ...

(cccccliii) ...

(ccccliv) ...

(cccclv) ...

(cccclvi) ...

(cccclvii) ...

(cccclviii) ...

(cccclix) ...

(cccclx) ...

(cccclxi) ...

(cccclxii) ...

(cccclxiii) ...

(cccclxiv) ...

(cccclxv) ...

(cccclxvi) ...

(cccclxvii) ...

(cccclxviii) ...

(cccclxix) ...

(cccclxx) ...

(cccclxxi) ...

(cccclxxii) ...

(cccclxxiii) ...

(cccclxxiv) ...

(cccclxxv) ...

(cccclxxvi) ...

(cccclxxvii) ...

(cccclxxviii) ...

(cccclxxix) ...

(cccclxxx) ...

(cccclxxxi) ...

(cccclxxxii) ...

(cccclxxxiii) ...

(cccclxxxiv) ...

(cccclxxxv) ...

(cccclxxxvi) ...

(cccclxxxvii) ...

(cccclxxxviii) ...

(cccclxxxix) ...

(ccccxc) ...

(ccccxci) ...

(ccccxcii) ...

(ccccxciii) ...

(ccccxciv) ...

(ccccxcv) ...

(ccccxcvi) ...

(ccccxcvii) ...

(ccccxcviii) ...

(ccccxcix) ...

(cccccc) ...

(ccccccii) ...

(cccccciii) ...

(ccccccciv) ...

(cccccv) ...

(cccccvi) ...

(cccccvii) ...

(cccccviii) ...

(cccccix) ...

(cccccx) ...

(cccccxi) ...

(cccccxii) ...

(cccccxiii) ...

(cccccxiv) ...

(cccccxv) ...

(cccccxvi) ...

(cccccxvii) ...

(cccccxviii) ...

(cccccxix) ...

(cccccxx) ...

(cccccxxi) ...

(cccccxxii) ...

(cccccxxiii) ...

(cccccxxiv) ...

(cccccxxv) ...

(cccccxxvi) ...

(cccccxxvii) ...

(cccccxxviii) ...

(cccccxxix) ...

(cccccxxx) ...

(cccccxxxi) ...

(cccccxxxii) ...

(cccccxxxiii) ...

(cccccxxxiv) ...

(cccccxxxv) ...

(cccccxxxvi) ...

(cccccxxxvii) ...

(cccccxxxviii) ...

(cccccxxxix) ...

(cccccxl) ...

(cccccxli) ...

(cccccxlii) ...

(cccccxliii) ...

(cccccxliv) ...

(cccccxlv) ...

(cccccxlvi) ...

(cccccxlvii) ...

(cccccxlviii) ...

(cccccxlix) ...

(cccccl) ...

(ccccccli) ...

(cccccclii) ...

(ccccccliii) ...

(cccccliv) ...

(ccccclv) ...

(ccccclvi) ...

(ccccclvii) ...

(ccccclviii) ...

(ccccclix) ...

(ccccclx) ...

(ccccclxi) ...

(ccccclxii) ...

(ccccclxiii) ...

(ccccclxiv) ...

(ccccclxv) ...

(ccccclxvi) ...

(ccccclxvii) ...

(ccccclxviii) ...

(ccccclxix) ...

(ccccclxx) ...

(ccccclxxi) ...

(ccccclxxii) ...

(ccccclxxiii) ...

(ccccclxxiv) ...

(ccccclxxv) ...

(ccccclxxvi) ...

(ccccclxxvii) ...

(ccccclxxviii) ...

(ccccclxxix) ...

(ccccclxxx) ...

(ccccclxxxi) ...

(ccccclxxxii) ...

(ccccclxxxiii) ...

(ccccclxxxiv) ...

(ccccclxxxv) ...

(ccccclxxxvi) ...

(ccccclxxxvii) ...

(ccccclxxxviii) ...

(ccccclxxxix) ...

(cccccxc) ...

(cccccxci) ...

(cccccxcii) ...

(cccccxciii) ...

(cccccxciv) ...

(cccccxcv) ...

(cccccxcvi) ...

(cccccxcvii) ...

(cccccxcviii) ...

(cccccxcix) ...

(ccccccc) ...

(cccccccii) ...

(ccccccciii) ...

(cccccccciv) ...

(ccccccv) ...

(ccccccvi) ...

(ccccccvii) ...

(ccccccviii) ...

(ccccccix) ...

(ccccccx) ...

(ccccccxi) ...

(ccccccxii) ...

(ccccccxiii) ...

(ccccccxiv) ...

(ccccccxv) ...

(ccccccxvi) ...

(ccccccxvii) ...

(ccccccxviii) ...

(ccccccxix) ...

(ccccccxx) ...

(ccccccxxi) ...

(ccccccxxii) ...

(ccccccxxiii) ...

(ccccccxxiv) ...

(ccccccxxv) ...

(ccccccxxvi) ...

(ccccccxxvii) ...

(ccccccxxviii) ...

(ccccccxxix) ...

(ccccccxxx) ...

(ccccccxxxi) ...

(ccccccxxxii) ...

(ccccccxxxiii) ...

(ccccccxxxiv) ...

(ccccccxxxv) ...

(ccccccxxxvi) ...

(ccccccxxxvii) ...

(ccccccxxxviii) ...

(ccccccxxxix) ...

(ccccccxl) ...

(ccccccxli) ...

(ccccccxlii) ...

(ccccccxliii) ...

(ccccccxliv) ...

(ccccccxlv) ...

(ccccccxlvi) ...

(ccccccxlvii) ...

(ccccccxlviii) ...

(ccccccxlix) ...

(ccccccl) ...

(cccccccli) ...

(ccccccclii) ...

(cccccccliii) ...

(ccccccliv) ...

(cccccclv) ...

(cccccclvi) ...

(cccccclvii) ...

(cccccclviii) ...

(cccccclix) ...

(cccccclx) ...

(cccccclxi) ...

(cccccclxii) ...

(cccccclxiii) ...

(cccccclxiv) ...

(cccccclxv) ...

(cccccclxvi) ...

(cccccclxvii) ...

(cccccclxviii) ...

(cccccclxix) ...

(cccccclxx) ...

(cccccclxxi) ...

(cccccclxxii) ...

(cccccclxxiii) ...

(cccccclxxiv) ...

(cccccclxxv) ...

(cccccclxxvi) ...

(cccccclxxvii) ...

(cccccclxxviii) ...

(cccccclxxix) ...

(cccccclxxx) ...

(cccccclxxxi) ...

(cccccclxxxii) ...

(cccccclxxxiii) ...

(cccccclxxxiv) ...

(cccccclxxxv) ...

(cccccclxxxvi) ...

(cccccclxxxvii) ...

(cccccclxxxviii) ...

(cccccclxxxix) ...

(ccccccxc) ...

(ccccccxci) ...

(ccccccxcii) ...

(ccccccxciii) ...

(ccccccxciv) ...

(ccccccxcv) ...

(ccccccxcvi) ...

(ccccccxcvii) ...

(ccccccxcviii) ...

(ccccccxcix) ...

(cccccccc) ...

(ccccccccii) ...

(cccccccciii) ...

(ccccccccciv) ...

(cccccccv) ...

(cccccccvi) ...

(cccccccvii) ...

(cccccccviii) ...

(cccccccix) ...

(cccccccx) ...

(cccccccxi) ...

(cccccccxii) ...

(cccccccxiii) ...

(cccccccxiv) ...

(cccccccxv) ...

(cccccccxvi) ...

(cccccccxvii) ...

(cccccccxviii) ...

(cccccccxix) ...

(cccccccxx) ...

(cccccccxxi) ...

(cccccccxxii) ...

(cccccccxxiii) ...

(cccccccxxiv) ...

(cccccccxxv) ...

(cccccccxxvi) ...

(cccccccxxvii) ...

(cccccccxxviii) ...

(cccccccxxix) ...

(cccccccxxx) ...

(cccccccxxxi) ...

(cccccccxxxii) ...

(cccccccxxxiii) ...

(cccccccxxxiv) ...

(cccccccxxxv) ...

(cccccccxxxvi) ...

(cccccccxxxvii) ...

(cccccccxxxviii) ...

(cccccccxxxix) ...

(cccccccxl) ...

(cccccccxli) ...

(cccccccxlii) ...

(cccccccxliii) ...

(cccccccxliv) ...

(cccccccxlv) ...

(cccccccxlvi) ...

(cccccccxlvii) ...

(cccccccxlviii) ...

(cccccccxlix) ...

(cccccccl) ...

(ccccccccli) ...

(cccccccclii) ...

(ccccccccliii) ...

(cccccccliv) ...

(ccccccclv) ...

(ccccccclvi) ...

(ccccccclvii) ...

(ccccccclviii) ...

(ccccccclix) ...

(ccccccclx) ...

(ccccccclxi) ...

(ccccccclxii) ...

(ccccccclxiii) ...

(ccccccclxiv) ...

(ccccccclxv) ...

(ccccccclxvi) ...

(ccccccclxvii) ...

(ccccccclxviii) ...

(ccccccclxix) ...

(ccccccclxx) ...

(ccccccclxxi) ...

(ccccccclxxii) ...

(ccccccclxxiii) ...

(ccccccclxxiv) ...

(ccccccclxxv) ...

(ccccccclxxvi) ...

(ccccccclxxvii) ...

(ccccccclxxviii) ...

(ccccccclxxix) ...

(ccccccclxxx) ...

(ccccccclxxxi) ...

(ccccccclxxxii) ...

(ccccccclxxxiii) ...

(ccccccclxxxiv) ...

(ccccccclxxxv) ...

(ccccccclxxxvi) ...

(ccccccclxxxvii) ...

(ccccccclxxxviii) ...

(ccccccclxxxix) ...

(cccccccxc) ...

(cccccccxci) ...

(cccccccxcii) ...

(cccccccxciii) ...

(cccccccxciv) ...

(cccccccxcv) ...

(cccccccxcvi) ...

(cccccccxcvii) ...

(cccccccxcviii) ...

(cccccccxcix) ...

(ccccccccc) ...

(cccccccccii) ...

(ccccccccciii) ...

(cccccccccciv) ...

(ccccccccv) ...

(ccccccccvi) ...

(ccccccccvii) ...

(ccccccccviii) ...

(ccccccccix) ...

(ccccccccx) ...

(ccccccccxi) ...

(ccccccccxii) ...

(ccccccccxiii) ...

(ccccccccxiv) ...

(ccccccccxv) ...

(ccccccccxvi) ...

(ccccccccxvii) ...

(ccccccccxviii) ...

(ccccccccxix) ...

(ccccccccxx) ...

(ccccccccxxi) ...

(ccccccccxxii) ...

(ccccccccxxiii) ...

(ccccccccxxiv) ...

(ccccccccxxv) ...

(ccccccccxxvi) ...

(ccccccccxxvii) ...

(ccccccccxxviii) ...

(ccccccccxxix) ...

(ccccccccxxx) ...

(ccccccccxxxi) ...

(ccccccccxxxii) ...

(ccccccccxxxiii) ...

(ccccccccxxxiv) ...

(ccccccccxxxv) ...

(ccccccccxxxvi) ...

(ccccccccxxxvii) ...

(ccccccccxxxviii) ...

(ccccccccxxxix) ...

(ccccccccxl) ...

(ccccccccxli) ...

(ccccccccxlii) ...

(ccccccccxliii) ...

(ccccccccxliv) ...

(ccccccccxlv) ...

(ccccccccxlvi) ...

(ccccccccxlvii) ...

(ccccccccxlviii) ...

(ccccccccxlix) ...

(ccccccccl) ...

(cccccccccli) ...

(ccccccccclii) ...

(cccccccccliii) ...

(ccccccccliv) ...

(cccccccclv) ...

(cccccccclvi) ...

(cccccccclvii) ...

(cccccccclviii) ...

(cccccccclix) ...

(cccccccclx) ...

(cccccccclxi) ...

(cccccccclxii) ...

(cccccccclxiii) ...

(cccccccclxiv) ...

(cccccccclxv) ...

(cccccccclxvi) ...

(cccccccclxvii) ...

(cccccccclxviii) ...

(cccccccclxix) ...

(cccccccclxx) ...

(cccccccclxxi) ...

(cccccccclxxii) ...

(cccccccclxxiii) ...

(cccccccclxxiv) ...

(cccccccclxxv) ...

(cccccccclxxvi) ...

(cccccccclxxvii) ...

(cccccccclxxviii) ...

(cccccccclxxix) ...

(cccccccclxxx) ...

(cccccccclxxxi) ...

(cccccccclxxxii) ...

(cccccccclxxxiii) ...

(cccccccclxxxiv) ...

(cccccccclxxxv) ...

(cccccccclxxxvi) ...

(cccccccclxxxvii) ...

(cccccccclxxxviii) ...

(cccccccclxxxix) ...

(ccccccccxc) ...

(ccccccccxci) ...

(ccccccccxcii) ...

(ccccccccxciii) ...

(ccccccccxciv) ...

(ccccccccxcv) ...

(ccccccccxcvi) ...

(ccccccccxcvii) ...

(ccccccccxcviii) ...

(ccccccccxcix) ...

(cccccccccc) ...

(ccccccccccii) ...

(cccccccccciii) ...

(ccccccccccciv) ...

(cccccccccv) ...

(cccccccccvi) ...

(cccccccccvii) ...

(cccccccccviii) ...

(cccccccccix) ...

(cccccccccx) ...

(cccccccccxi) ...

(cccccccccxii) ...

(cccccccccxiii) ...

(cccccccccxiv) ...

(cccccccccxv) ...

(cccccccccxvi) ...

(cccccccccxvii) ...

(cccccccccxviii) ...

(cccccccccxix) ...

(cccccccccxx) ...

(cccccccccxxi) ...

(cccccccccxxii) ...

(cccccccccxxiii) ...

(cccccccccxxiv) ...

(cccccccccxxv) ...

(cccccccccxxvi) ...

(cccccccccxxvii) ...

(cccccccccxxviii) ...

(cccccccccxxix) ...

(cccccccccxxx) ...

(cccccccccxxxi) ...

(cccccccccxxxii) ...

(cccccccccxxxiii) ...

(cccccccccxxxiv) ...

(cccccccccxxxv) ...

(cccccccccxxxvi) ...

(cccccccccxxxvii) ...

(cccccccccxxxviii) ...

(cccccccccxxxix) ...

(cccccccccxl) ...

(cccccccccxli) ...

(cccccccccxlii) ...

(cccccccccxliii) ...

(cccccccccxliv) ...

(cccccccccxlv) ...

(cccccccccxlvi) ...

(cccccccccxlvii) ...

(cccccccccxlviii) ...

(cccccccccxlix) ...

(cccccccccl) ...

(ccccccccccli) ...

(cccccccccclii) ...

(ccccccccccliii) ...

(cccccccccliv) ...

(ccccccccclv) ...

(ccccccccclvi) ...

(ccccccccclvii) ...

(ccccccccclviii) ...

(ccccccccclix) ...

(ccccccccclx) ...

(ccccccccclxi) ...

(ccccccccclxii) ...

(ccccccccclxiii) ...

(ccccccccclxiv) ...

(ccccccccclxv) ...

(ccccccccclxvi) ...

(ccccccccclxvii) ...

(ccccccccclxviii) ...

(ccccccccclxix) ...

(ccccccccclxx) ...

(ccccccccclxxi) ...

(ccccccccclxxii) ...

(ccccccccclxxiii) ...

(ccccccccclxxiv) ...

(ccccccccclxxv) ...

(ccccccccclxxvi) ...

(ccccccccclxxvii) ...

(ccccccccclxxviii) ...

(ccccccccclxxix) ...

(ccccccccclxxx) ...

(ccccccccclxxxi) ...

(ccccccccclxxxii) ...

(ccccccccclxxxiii) ...

(ccccccccclxxxiv) ...

(ccccccccclxxxv) ...

(ccccccccclxxxvi) ...

(ccccccccclxxxvii) ...

(ccccccccclxxxviii) ...

(ccccccccclxxxix) ...

(cccccccccxc) ...

(cccccccccxci) ...

(cccccccccxcii) ...

(cccccccccxciii) ...

(cccccccccxciv) ...

(cccccccccxcv) ...

(cccccccccxcvi) ...

(cccccccccxcvii) ...

(cccccccccxcviii) ...

(cccccccccxcix) ...

(ccccccccccc) ...

(cccccccccccii) ...

(ccccccccccciii) ...

(cccccccccccciv) ...

(ccccccccccv) ...

(ccccccccccvi) ...

(ccccccccccvii) ...

(ccccccccccviii) ...

(ccccccccccix) ...

(ccccccccccx) ...

(ccccccccccxi) ...

(ccccccccccxii) ...

(ccccccccccxiii) ...

(ccccccccccxiv) ...

(ccccccccccxv) ...

(ccccccccccxvi) ...

(ccccccccccxvii) ...

(ccccccccccxviii) ...

(ccccccccccxix) ...

(ccccccccccxx) ...

(ccccccccccxxi) ...

(ccccccccccxxii) ...

(ccccccccccxxiii) ...

(ccccccccccxxiv) ...

(ccccccccccxxv) ...

(ccccccccccxxvi) ...

(ccccccccccxxvii) ...

(ccccccccccxxviii) ...

(ccccccccccxxix) ...

(ccccccccccxxx) ...

(ccccccccccxxxi) ...

(ccccccccccxxxii) ...

(ccccccccccxxxiii) ...

(ccccccccccxxxiv) ...

(ccccccccccxxxv) ...

(ccccccccccxxxvi) ...

(ccccccccccxxxvii) ...

(ccccccccccxxxviii) ...

(ccccccccccxxxix) ...

(ccccccccccxl) ...

(ccccccccccxli) ...

(ccccccccccxlii) ...

(ccccccccccxliii) ...

(ccccccccccxliv) ...

(ccccccccccxlv) ...

(ccccccccccxlvi) ...

(ccccccccccxlvii) ...

(ccccccccccxlviii) ...

(ccccccccccxlix) ...

(ccccccccccl) ...

(cccccccccccli) ...

(ccccccccccclii) ...

(cccccccccccliii) ...

(ccccccccccliv) ...

(cccccccccclv) ...

(cccccccccclvi) ...

(cccccccccclvii) ...

(cccccccccclviii) ...

(cccccccccclix) ...

(cccccccccclx) ...

(cccccccccclxi) ...

(cccccccccclxii) ...

(cccccccccclxiii) ...

(cccccccccclxiv) ...

(cccccccccclxv) ...

(cccccccccclxvi) ...

(cccccccccclxvii) ...

(cccccccccclxviii) ...

(cccccccccclxix) ...

(cccccccccclxx) ...

(cccccccccclxxi) ...

(cccccccccclxxii) ...

(cccccccccclxxiii) ...

(cccccccccclxxiv) ...

(cccccccccclxxv) ...

(cccccccccclxxvi) ...

(cccccccccclxxvii) ...

(cccccccccclxxviii) ...

(cccccccccclxxix) ...

(cccccccccclxxx) ...

(cccccccccclxxxi) ...

(cccccccccclxxxii) ...

(cccccccccclxxxiii) ...

(cccccccccclxxxiv) ...

(cccccccccclxxxv) ...

(cccccccccclxxxvi) ...

(cccccccccclxxxvii) ...

(cccccccccclxxxviii) ...

(cccccccccclxxxix) ...

(ccccccccccxc) ...

(ccccccccccxci) ...

(ccccccccccxcii) ...

(ccccccccccxciii) ...

(ccccccccccxciv) ...

(ccccccccccxcv) ...

(ccccccccccxcvi) ...

(ccccccccccxcvii) ...

(ccccccccccxcviii) ...

(ccccccccccxcix) ...

(cccccccccccc) ...

(ccccccccccccii) ...

(cccccccccccciii) ...

(ccccccccccccciv) ...

(cccccccccccv) ...

(cccccccccccvi) ...

(cccccccccccvii) ...

(cccccccccccviii) ...

(cccccccccccix) ...

(cccccccccccx) ...

(cccccccccccxi) ...

(cccccccccccxii) ...

(cccccccccccxiii) ...

(cccccccccccxiv) ...

(cccccccccccxv) ...

(cccccccccccxvi) ...

(cccccccccccxvii) ...

(cccccccccccxviii) ...

(cccccccccccxix) ...

(cccccccccccxx) ...

(cccccccccccxxi) ...

(cccccccccccxxii) ...

(cccccccccccxxiii) ...

(cccccccccccxxiv) ...

(cccccccccccxxv) ...

(cccccccccccxxvi) ...

(cccccccccccxxvii) ...

(cccccccccccxxviii) ...

(cccccccccccxxix) ...

(cccccccccccxxx) ...

(cccccccccccxxxi) ...

(cccccccccccxxxii) ...

(cccccccccccxxxiii) ...

(cccccccccccxxxiv) ...

(cccccccccccxxxv) ...

(cccccccccccxxxvi) ...

(cccccccccccxxxvii) ...

(cccccccccccxxxviii) ...

(cccccccccccxxxix) ...

(cccccccccccxl) ...

(cccccccccccxli) ...

(cccccccccccxlii) ...

(cccccccccccxliii) ...

(cccccccccccxliv) ...

(cccccccccccxlv) ...

(cccccccccccxlvi) ...

(cccccccccccxlvii) ...

(cccccccccccxlviii) ...

(cccccccccccxlix) ...

(cccccccccccl) ...

(ccccccccccccli) ...

(cccccccccccclii) ...

(ccccccccccccliii) ...

(cccccccccccliv) ...

(ccccccccccclv) ...

(ccccccccccclvi) ...

(ccccccccccclvii) ...

(ccccccccccclviii) ...

(ccccccccccclix) ...

(ccccccccccclx) ...

(ccccccccccclxi) ...

(ccccccccccclxii) ...

(ccccccccccclxiii) ...

(ccccccccccclxiv) ...

(ccccccccccclxv) ...

(ccccccccccclxvi) ...

(ccccccccccclxvii) ...

(ccccccccccclxviii) ...

(ccccccccccclxix) ...

(ccccccccccclxx) ...

(ccccccccccclxxi) ...

(ccccccccccclxxii) ...

(ccccccccccclxxiii) ...

(ccccccccccclxxiv) ...

(ccccccccccclxxv) ...

(ccccccccccclxxvi) ...

(ccccccccccclxxvii) ...

(ccccccccccclxxviii) ...

(ccccccccccclxxix) ...

(ccccccccccclxxx) ...

(ccccccccccclxxxi) ...

(ccccccccccclxxxii) ...

(ccccccccccclxxxiii) ...

(ccccccccccclxxxiv) ...

(ccccccccccclxxxv) ...

(ccccccccccclxxxvi) ...

(ccccccccccclxxxvii) ...

(ccccccccccclxxxviii) ...

(ccccccccccclxxxix) ...

(cccccccccccxc) ...

(cccccccccccxci) ...

(cccccccccccxcii) ...

(cccccccccccxciii) ...

(cccccccccccxciv) ...

(cccccccccccxcv) ...

(cccccccccccxcvi) ...

(cccccccccccxcvii) ...

(cccccccccccxcviii) ...

(cccccccccccxcix) ...

(ccccccccccccc) ...

(cccccccccccccii) ...

(ccccccccccccciii) ...

(cccccccccccccciv) ...

(ccccccccccccv) ...

(ccccccccccccvi) ...

(ccccccccccccvii) ...

(ccccccccccccviii) ...

(ccccccccccccix) ...

(ccccccccccccx) ...

(ccccccccccccxi) ...

(ccccccccccccxii) ...

(ccccccccccccxiii) ...

(ccccccccccccxiv) ...

(ccccccccccccxv) ...

(ccccccccccccxvi) ...

(ccccccccccccxvii) ...

(ccccccccccccxviii) ...

(ccccccccccccxix) ...

(ccccccccccccxx) ...

(ccccccccccccxxi) ...

(ccccccccccccxxii) ...

(ccccccccccccxxiii) ...

(ccccccccccccxxiv) ...

(ccccccccccccxxv) ...

(ccccccccccccxxvi) ...

(ccccccccccccxxvii) ...

(ccccccccccccxxviii) ...

(ccccccccccccxxix) ...

(ccccccccccccxxx) ...

(ccccccccccccxxxi) ...

(ccccccccccccxxxii) ...

(ccccccccccccxxxiii) ...

(ccccccccccccxxxiv) ...

(ccccccccccccxxxv) ...

(ccccccccccccxxxvi) ...

(ccccccccccccxxxvii) ...

(ccccccccccccxxxviii) ...

(ccccccccccccxxxix) ...

(ccccccccccccxl) ...

(ccccccccccccxli) ...

(ccccccccccccxlii) ...

(ccccccccccccxliii) ...

(ccccccccccccxliv) ...

(ccccccccccccxlv) ...

(ccccccccccccxlvi) ...

(ccccccccccccxlvii) ...

(ccccccccccccxlviii) ...

(ccccccccccccxlix) ...

(ccccccccccccl) ...

(cccccccccccccli) ...

(ccccccccccccclii) ...

(cccccccccccccliii) ...

(ccccccccccccliv) ...

(cccccccccccclv) ...

(cccccccccccclvi) ...

(cccccccccccclvii) ...

(cccccccccccclviii) ...

(cccccccccccclix) ...

(cccccccccccclx) ...

(cccccccccccclxi) ...

(cccccccccccclxii) ...

(cccccccccccclxiii) ...

(cccccccccccclxiv) ...

(cccccccccccclxv) ...

(cccccccccccclxvi) ...

(cccccccccccclxvii) ...

(cccccccccccclxviii) ...

(ccccccccccccl

S0150

To "pdpo_consultation@cmab.gov.hk" <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject Updated document of the response from HKCS

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

30/11/2009 22:50

Dear Sir/Madam,
For your information I attach an updated response document from HK Computer Society. This is the final and official document (Version 2). Pl ignore the document (Version 1) which I sent you this afternoon.

Thanks for your attention.

rgds

Stephen Lau
Adviser,
HP Enterprise Services

Chairman
APICTA



HKCS response to PDPO revision -V2.doc

S0150

Hong Kong Computer Society (HKCS)
Response to the Consultation Document on
Review of the Personal Data (Privacy) Ordinance

November 2009

Guiding Principles

We take note of the guiding principles in conducting the review as articulated in the consultative document, viz:

(a) the right of individuals to privacy is not absolute. It must be balanced against other rights and public and social interests;
(b) balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology;
(c) any changes to the privacy law should not undermine Hong Kong's competitiveness and economic efficiency as an international city;
(d) the need to avoid putting onerous burden on business operations and individual data users;
(e) due account should be given to local situations;
(f) the PDPO should remain flexible and relevant in spite of technological change;
(g) legislative intervention may not always be the most effective way. In certain circumstances, personal data privacy protection may be achieved by administrative measures; and

(h) consensus in the community about the privacy issues is important.

We are in broad agreement to these guiding principles, in particular to the pursuit of balance between safeguarding personal data privacy and facilitating the continued development of information and communications technology, and the need to avoid putting onerous burden on business operations and individual data users. Furthermore, we wish to emphasise that our submission embraces the following supplemental guiding principles:

- A key focus of the PCPD (Privacy Commissioner for Personal Data) should be "evolving societal and cultural change through promotion and education", by devoting more resources to instilling broader and deepened awareness in both data subjects and data users of the importance of personal data protection, educating

the public in preventive measures to privacy intrusion and the provisions of the PDPO and the functions of the PCPD in providing protection to their personal data.

In light of the afore-mentioned, **granting of additional enforcement powers should be avoided, and if deemed necessary kept to a minimal level.**

We wish to respond selectively to your proposals, in particular those which we believe to be strategic and IT related:

---

1. **Sensitive personal data – should we subject sensitive personal data, such as fingerprints, to more stringent regulation?**

   Traditionally other data protection laws classify some societal data as sensitive, egg political opinion, religious belief, sexual orientation, criminal record. Only in recent years biometrics and genetic information are classified as sensitive data due to their unique and unchanging characteristics which uniquely identify a person.

   The PCPD proposes to classify biometric data as the first sensitive data under our law, such that their collection and use would be afforded with more stringent protective conditions. It is noted that the consultative document provides no pertinent argument on the relative merits or importance in the adoption of biometric data vis-à-vis the other societal data as fore-mentioned.

   There are two sides to the argument in the issue of biometric data. On one hand, the collection of biometrics is good for the collecting organization (data user) because it helps to uniquely identify the person/employee/customer, and good for the person (data subject) as well such that impersonation by others would be difficult (identity theft). On the other hand, the person as well the PCPD might find that it is too privacy invasive (using a hammer to crack a nut, eg using biometrics for , say, access to campus by a student or for recording attendance). It is also noted that the current data protection principles, in particular the security principle, stipulate that the extent of security measures should commensurate with the extent of potential harm caused by leakage/unauthorized access. The PCPD also brings up the issue of additional costs for organizations to comply with the additional requirements in collecting and use of sensitive data, which we concur.

   The major issue seen by the IT industry is that the PCPD has already voiced opposition to fingerprinting access system through complaints by individual

employee/student, and provided views on a case by case basis, "whether there is another option of achieving the same result/effect by using other less invasive method". Some of these complaints and opposition we understand have happened after system installation. Being aware of such possibilities, no wonder potential users shy away from considering installing such products (why bring on possible hassle from the authority!) , leading to a stagnant market for such products which would bring substantial benefits to the user organizations as well to the further development of the IT industry in Hong Kong.

Whether biometrics is classified as sensitive data or not, the industry view is for the PCPD to provide definitive views on "what is permissible" and "what is not permissible" from the PCPD's perspective with respect to IT systems and products which use biometric data for processing (eg is it permissible have the biometric data on the access card ,to match with the actual finger print presented at the point of entry , so there is no data collection by or stored in the computer system) such that the industry can design/install systems which will satisfy the PCPD. Specific guidelines or even better a "code of practice" would be preferred, rather than a "case by case" review scenario by the PCPD with uncertainties of the review outcome. One of the Review's guiding principles, "balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology", should be applicable in this context.

In summary, we are of the opinion that, with the current immature state of inadequate awareness by the community even with the general legal definition of personal data and the data protection principles as promulgated by the PDPO, and that the PDPO has already provided the general umbrella of data protection to ALL personal data, **that the classification of sensitive data should not be effected at this point in time.**

2. Data Security - should we regulate data processors entrusted with handling of personal data?

With outsourcing flourishing, at present the PDPO does not directly regulate the activities of a processing agent (data processor) which processes personal data for its principle (data user). The data processor is not required to comply with the law, and for the protection of data subjects, whose data are being processed by data processors, the data user is held liable, who usually should provide contractual agreement that the data processor should comply with the requirements of the PDPO.

In some other laws, including Canada and Australia, both data users and data processors are required to comply with the law.

The consultative document discusses whether a data processor should be directly regulated by the PDPO. We strongly disagree as

a. the definition of "data processor" is difficult to be comprehensively defined what with the continual and speedy IT technology advancement and its creative applications via innovative business models , particularly when the PDPO relies on the concepts such that the "purpose for which the data are to be used at the time of collection" to establish criteria of proper use, whereas many internet-related business will be unaware of the nature of the data, including the purpose for which it was originally collected. Many such businesses process the same data on behalf of several users, eg a social networking site processes data on behalf of the user who posts the data as well as those who search for the data.

b. many data processors are overseas entities, and are outside the jurisdiction of HK, which for PDPO is difficult if not impossible to enforce.

Therefore indirect regulation of data processors should be the case, by relying on the data user to ensure that its data processors provide security protection to data at a level comparable to itself, meaning that the data user is liable, thus would do its best to ensure using a reliable/credible data processor, in selection and thru contractual conditions, eg the data processor should have privacy policy which complies with the data protection principles of PDPO.

However, in noting the ever increasing cases of identity theft and fraud globally arisen from data breaches, we also encourage **the PCPD to further study the operational nature of "data processors",** in particular the different types of Internet intermediaries with regard to their collection, retention, processing, use and disclosure of personal data, to ascertain whether **, for specific data processors, some specific strengthening of relevant provisions should be considered** in view of the likely and serious potential impact on data privacy. There are a number of studies on the evolving nature of Internet intermediaries and the potential issues related to market, privacy and intellectual property etc. I attach below a relevant table from a recent document from the OECD.

EXAMPLES OF POTENTIAL ISSUES RELATED TO INTERNET INTERMEDIARIES' ROLE

Internet actors	Potential issues	Examples of market, regulatory and self-regulatory questions that may arise
Internet access and service Providers	Internet access, copyright, security threats, child protection, freedom of speech, due process and privacy	- identifying customers engaged in allegedly illegal or unauthorised activities. - notifying users regarding allegedly unauthorised material. - combating spam and other security threats. - informing customers of data breaches that might affect personal data. - investigating technical measures to block illegal content (*e.g.*, child abuse sites) or allegedly infringing content (*e.g.*, copyright material).
Data processing and Web hosting Providers Including domain name registrars	Access to information, copyright, security threats, defamation, child protection, illegal content. Security threats, especially phishing and spam[1], consumer protection, trademarks (cybersquatting)	- having "knowledge" of unauthorised or illegal character of content diffused on hosts' platforms. - determining legitimate vs. illegal character of content. - being able to legally qualify different types of hosts *e.g.* the cases in which hosts can also be considered to be "editors", "advertisers" etc. - withdrawing domain name services from users conducting illegal activities,[2] *e.g.*, phishing[3]. - prohibiting or minimising the use of fast-flux domains (domains for which the IP address rapidly fluctuates to avoid detection and takedown) to help fight malware.
Internet search engines and portals	Free flow of information, user choice, trademark, copyright, counterfeiting, security threats, click fraud, defamation, privacy	- developing industry standards and codes of conduct. - excluding some types of content from search results to comply with national legislations' treatment of illegal content. - hyperlinking to potentially illegal material and activities. - providing thumbnails of allegedly unauthorised material. - abiding by notice and take-down letters for copyright infringements and the effectiveness of counter-notification mechanisms. - advertising companies using third parties' trademarked terms as keywords. - being able to legally qualify participative search engines, *e.g.* as a host and/or as an advertiser or editor).
E-commerce platforms	User choice, consumer protection, counterfeiting, taxation	- developing community standards and associated rules. - determining whether sellers are businesses or individuals (*e.g.* to determine relevant consumer protection and taxation regimes). - identifying counterfeit goods being offered via auction platforms and respective roles of rights owners, notices and auction platforms. - informing customers of data breaches that might affect personal data. - being able to legally qualify auction platforms.
E-commerce payment systems	Illegal gambling, security threats, child protection, identity and privacy	- cutting off payment to merchants engaged in illicit activity; *e.g.* to e-casinos in jurisdictions where online gambling is illegal or to merchants storing allegedly improper content or engaging in fraud. - informing customers of data breaches that might affect personal data.
Participative Web platforms	Copyright, identity and privacy, defamation, child protection	- developing community standards and associated rules. - being able to legally qualify participative web platforms (*e.g.* as a host and/or as an editor).

3. Personal Data Security Breach Notification

With data breaches on the rise in Hong Kong and globally, it is noted that the PDPO does not require the data user to report to the PCPD of data breaches nor to notify the data subjects whose data have been stolen/lost/disclosed without authorization.

In discussing data breach notification, should it be mandatory or voluntary, the PCPD proposes a voluntary breach notification (one reason is mandatory breach notification could cause significant costs to the community, and also allow time to assess and fine tune the guidelines).

We prefer a general voluntary scheme (to PCPDand data subjects/organizations affected) but selectively mandatory for notification when a personal data security breach may result in a high risk of significant harm to individuals or organizations. By selectively we mean certain categories of data, eg to consider "financial data" and "medical data", which to many in the community are deemed personally sensitive and private. Not only would the affected individuals and organizations be informed by the notification and allow for constructive and consequential actions to be taken, the notification would further encourage the data user to be more focused on data protection to avoid the potential publicity and brand damage, as well as the costs of notification, which would be significant.

4. Enforcement Powers of the PCPD

The PDPO confers powers on the PCPD to conduct investigations and inspections, but not carry out criminal investigations (by the Police) or initiate prosecutions (by the Dept of Justice) on its own. To save time on referring cases to the Police and to help meet the statutory time limit to lay prosecution, and with PCPD being the most knowledgeable in personal data issues, PCPD proposes to be able to conduct criminal investigations and initiate prosecutions.

We are not in favor of this proposal, and the policy branch CMAB, Constitutional and Mainland Affairs Bureau, is also not in favor either, though it would, and we agree, to review the tight statutory time limit for initiating prosecution.

5. Legal Assistance to Data Subjects

PCPD would like to offer legal assistance to data subjects, similar to such capability provided by the EOC (Equal Opportunity Commission).

We are in favour of granting PCPD with such a capability, but it should only be exercised under strict guiding criteria as follows:

a. an important legal point or principle is at stake.

b. it is to tackle an important and systemic issue (which eg in the US would call for a class action).

6. Award Compensation to Aggrieved Data Subjects

Currently an aggrieved data subject is entitled to compensation from the data user for that damage through a court of law, though over the years this provision was seldom invoked sue to the high costs of court proceedings and the outcome of a civil claim unpredictable. PCO wants to have the power to award compensation.

We are not in favour of this proposal, as argued by the Law Reform Commission when it was discussed many years ago in the design of PCDO, award compensation vested in a single authority is an undesirable combination of enforcement and punitive functions, not to mention the heightening of expectation, may be even unrealistic, of the aggrieved party, and unease if not aggravation from the data user.

7. Making Contravention of a Data Protection Principle (DDP) an Offence

Currently contravention of a DPP is not an offence, with the PCPD issues an enforcement notice to take remedial action within a specified period, and only if the enforcement notice is contravened then it commits an offence.

We are not in favour of this proposal as the DDPs are couched in generic terms and can be subject to a wide range of interpretations., and making contravention of a DPP would have impact on civil liberties (an inadvertent act or omission could attract criminal offence!) We also believe that the PCPD should do more in promotion and education to induce a societal cultural change rather than to be more litigious.

However, if this proposal is accepted, then a selective approach in defining specific acts or practice, eg serious data breaches or sensitive data.

8. **Unauthorized Obtaining, Disclosure and Sale of Personal Data**

We agree with this proposal to make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained without consent, as the identity theft and fraud is now in the US and globally the most common commercial crime/misdemeanor.

9. **Transborder Data Flow**

Though this issue has not been raised in the consultative document, we wish to express our concern that Section 33 of the PDPO, which deals specifically with the "Prohibition against transfer of personal data to place outside except in specified circumstances", has not been brought into commencement despite the passage of more than 10 years since the Ordinance came into being on 1995. In reminding ourselves of the stated two-fold objectives of the PDPO, viz

- to protect the individual's right to privacy with respect to personal data; and
- to safeguard the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws.

We are mindful that Section 33 on transborder dataflow is a critical component in the satisfactory pursuit of the second objective of the PDPO, which has significant impact on our economic wellbeing in the globalized arena of international trade and commerce. Without the commencement of Section 33 Hong Kong will continue to be regarded as somewhat inadequate, particularly by the European Union (EU) whose data protection Directive is very specific in terms of transborder dataflow.

We hope to see an early date when Section 33 will be commenced.

S0151

HONG KONG DOCTORS UNION
香港西醫工會

30th November 2009

By fax and mail

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road, Hong Kong

Dear Sir/Madam,

Re: Review of the Personal Data (Privacy) Ordinance

Hong Kong Doctors Union (HKDU) refers to your invitation of 28th August 2009 to provide comments on the review of the Personal Data (Privacy) Ordinance. Following please find our Union's views on the proposals:

Proposal 1. Sensitive personal data

We agree in principle that doctors consider many biometric data such as height, weight, waist measurements, tattoos, scars and birthmarks to be unique to patients and have substantial bearing on medical management. (Ref: Consultation Document 3.08 to 3.12). These to us however are not sensitive data. Identifiable characteristics printed in passports still carry colour of iris, ethnic origin and even fingerprints to identify the person. We do not see these unique unchangeable characteristics that make us different from one another should suddenly be considered as sensitive data. History of Venereal Disease and mental illness likely to arouse discrimination may be sensitive and belong to a different category. Therefore should a list of sensitive personal data be established by the authority and legislated we prefer the medical profession be consulted first. Also, if that does happen we believe simply extending the present regulations governing contravention of DPPs to sensitive personal data is adequate and should not make such contraventions a more serious matter. We do not need to follow overseas experience blindly to produce unnecessary impact on civil liberty (3.12). We hope the mere mentioning of a person possessing acne or suffering from coryza will not be exaggerated to the point of offending the ordinance. Incidentally dates of birth, vital statistics, etc of film stars and celebrities are openly published daily in tabloids and gossip magazines. Should we really ban this practice when the public figures don't even mind? We do

Cont.../P. 2

HONG KONG DOCTORS UNION 香港西醫工會

S0151

agree with your suggestion of transitional or "grandfather" arrangement if new requirements on sensitive data are indeed imposed.

Proposal 2. Regulation of Data Processors and Sub-contracting Activities

We agree with improving security by directly regulating data processors and to ensure the limitation of their use only for the purposes for which such data are entrusted and that all practical steps are employed to ensure security and the erasure of data after fulfillment of the purpose of use. (4.14) We agree with the flexible requirement of expecting privacy policies adopted by many Internet-related businesses themselves and failure to keep to their own policies would render a data processor liable.(4.19)

Proposal 3. Personal Data Security Breach Notification

We agree with proposals to institute a voluntary notification system for breach of personal data as suggested in paragraphs 4.37 to 4.42 including the five days rule of discovery of breach.

Proposal 4. Granting Criminal Investigation and Prosecution Power to the PCPD

We do not agree with the proposed enhancement of the powers of the Privacy Commissioner for Personal Data. The existing arrangement of referring cases to the Police is working well (5.07) and under the Basic Law it is not advisable to confer direct prosecution power to the PCPD. So the status quo should be maintained.

Proposal 5. Legal Assistance to Data Subjects under Section 66

We disagree with conferring power to the PCPD to provide legal aid to aggrieved data subjects.

Proposal 6. Award Compensation to Aggrieved Data Subjects

We disagree with proposal to empower the PCPD to award compensation to aggrieved data subjects.

Cont.../P. 3

HONG KONG DOCTORS UNION
香港西醫工會

S0151

Proposal 7. Making Contravention of a Data Protection Principle an Offence

We do not support making contravention of a Data Protective Principle an offence as this would have a great impact on civil liberties.

Proposal 8. Unauthorized Obtaining Disclosure and Sale of Personal Data

We agree that unauthorized obtaining, disclosure and sale of Personal data can be made an offence if done through malice or for profits and the level of penalty should commensurate with the gravity of the misdeed. But reckless or unknowingly obtaining data and not sold for profit or disclosed with malicious intent should not be categorized as an offence.

Proposal 9. Repeated Contravention of a Data Protection Principle on Same Facts

We agree that intentional repeated contravention of a DPP on same facts after initially complying with enforcement notice satisfying the PCPD should be made an offence.

Proposal 10. Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

We have reservations about empowering the PCPD to impose monetary penalty on serious contravention of DPPs and as for going along with the suggestion in (6.20) that it may be more appropriate to single out particular acts of contravention as an offence. In the meantime we would like to ask the PCPD WHAT and how SERIOUS contravention is defined.

Proposal 11. Repeated Non-compliance with Enforcement Notice

We agree with raising the level of penalty for repeated non-compliance with enforcement notice.

Proposal 12. Raising Penalty for Misuse of Personal Data in Direct Marketing

We agree with raising the penalty for misuse of personal data in direct marketing.

Cont.../P. 4



S0151

(A) Rights of Data Subjects:

Proposal 13. Third Party to Give Prescribed Consent to Change of Use of Personal Data

We agree with the careful granting of prescribed consent by Relevant Person (as a better definition than third party) to the change of use of Personal Data provided that (a) the data subject cannot give prescribed consent for lack of full understanding and (b) that the intended use of data is beneficial to the data subject.

Proposal 14. Parents' Right to Access Personal Data of Minors

We agree that a data user may refuse to comply with a data access request by a related person on behalf of a minor if he has reasonable grounds to believe that compliance with the request would not be in the best interests of the data subject thus balancing parents' rights to access with the privacy rights of minors.

Proposal 15. Access to Personal Data in Dispute

We agree with the proposal to ban the release of data to the data requestor in any way where a dispute of access is being ruled by a court or the appeals board.

(B) Rights and Obligations of Data Users:

Proposal 16. Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

We agree with providing ground for refusal to comply with a data access request when there is a need to comply with secrecy in another ordinance.

Proposal 17. Erasure of Personal Data

We request the PCPD to clarify the criteria for doctors as data users to decide the time when data collected or used will cease to be required for medical purposes. Please advise if a patient's record could

Cont.../P. 5

HONG KONG DOCTORS UNION 香港西醫工會

S0151

be deleted after five or seven years if no consultation by that particular patient had occurred for that length of period. Should the medical profession be given a freer hand to keep rather than erase data since no one ever knows when will such data be required to save life or be referred in case litigation arises? In this respect we think it is better and more practical to avoid being too rigid and common sense may be a guide.

Proposal 18. Fee Charges for Handling Data Access Requests

We keep an open mind in seeing a fee schedule published under PCPD for Fee charging for Handling Data Access Requests, but hope that reference will be made to charges by the Hospital Authority and private hospitals and that the medical profession as a whole will be consulted before setting such a standard.

Proposal 19. Response to Data Access Requests in Writing and Within 40 days

We agree with the proposal to require a data user to inform (a) requestor in writing if he does not hold the requested personal data, save for a request related to criminal conviction record data which the Police dose not hold; and (b) a data user should be required to inform a requestor within 40 days if he does not hold the personal data for which a copy of the data is requested, irrespective in whether the response is in written or verbal form.

Proposal 20. Circumstances for Issue of an Enforcement Notice

We agree with the proposal to enhance the effectiveness of the PDPO in the protection of personal data privacy and allow discretion for the POPD to serve an enforcement notice when (a) irrespective of the act of contravention is continuing; (b) whether the contravention will continue or repeated; and (c) whether the contravention has caused or is likely to cause damage or distress to the data subject.

Proposal 21. Clarifying Power to Direct Remedial Steps in an Enforcement Notice

We agree with the proposal to specify in Section 50(1) that the PCPD has the power to direct the

Cont.../P. 6

HONG KONG
DOCTORS UNION
香港西醫工會

S0151

relevant data user in an enforcement notice to desist from doing an act or engaging in a practice.

Proposal 22. Removing the Time Limit to Discontinue an Investigation

We DO NOT agree with the proposal to remove the Time Limit to discontinue an investigation but instead we suggest that if the PCPD refuses to continue investigation initiated by a complainant, he has to notify the complainant of the refusal within 60 days (and not 45 days) after receiving the complaint.

Proposal 23. Additional Grounds for Refusing to Investigate

We agree with proposal 23 for additional grounds for refusing to investigate when as in 48(a) the primary cause of the complaint is not related to personal data privacy, but we Do NOT agree with 48(b) and 48(c) as additional grounds for refusing i.e. when the complaint relates to any action currently or soon to be under investigation by another regulatory body and when the act in the complaint relates to

personal data which are likely to be used at any stage in an legal proceedings or inquiry before any law/ enforcement or regulatory bodies.

Proposal 24. Transfer of Personal Data in Business Mergers or Acquisition

We agree with the proposal that DPP3 should be provided for the transfer or disclosure of personal data in intended merger acquisition or transfer of businesses subject to the condition that the resultant organization will offer substantially similar service to the original data user; and options set out in Consultation Document 52(a - f) are appropriate

Proposal 25. Provision of Identity and Location Data on Health Grounds

We agree to amend section 59 of the PDPO to broaden the scope of application of exemption to cover personal data relating to the identity and location of the data subject on health grounds, such as reputation.

Cont.../P. 7

HONG KONG DOCTORS UNION
香港西醫工會

S0151

Proposal 26. Handling Personal Data in Emergency Situations

We agree with the granting of specific exemption from DPP 1(3) of the PDPO in the handling of accidents and other life-threatening situations by Law enforcement agencies and rescue and relief agencies.

Proposal 27. Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

We agree exemption from DPP 3 should be provided to permit transfer of personal data of minors to their parents or guardians to enhance the protection of vulnerable minors and those at risk. However, such exemption should be provided on that specific conditions only involving health and even life of the minor.

We agree with proposals 28, 29 30, 32, 33, 34, 35, 36, 37, 38 and 39; but we Do NOT agree with proposal 31 to provide the PCPD with express power to impose at reasonable charges for undertaking educational or promotional activities or services.

We agree in principle in proposal 40 to extend the limit for laying information for prosecution BUT to specify that the time limit for laying information for prosecution of an offence under the PDPO should be ONE (and not two years) from the date of committing the offence.

We agree with the proposals 41, 42 and 43.

Thanking you for your attention.

Yours sincerely,

(Signed)

Dr. Ho O[illegible] Ling
Hon. Secretary
Hong Kong Doctors Union

Outgoing 15

S0152

30 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

By Fax (25230565)
and By Post

Dear Sirs,

Re: Consultation Document on Review of the Personal Data (Privacy) Ordinance

We would like to submit our views on the above consultation document as enclosed herewith. Should you require any further information from us, please do not hesitate to contact us. Thank you.

Yours faithfully,

(Signed)

(name)

Encl.

(The sender requested anonymity)

S0152

Position of *(the Organisation)* **in response to the government consultation document on Review of the Personal Data (Privacy) Ordinance**

INTRODUCTION

We are glad to have the opportunity to express our views on the government consultation document on Review of the Personal Data (Privacy) Ordinance (the "Document"). Many data users like us have already adopted the principles of privacy in practice by implementing necessary measures and policies that are compliant with privacy principles demonstrating the effectiveness of the Personal Data (Privacy) Ordinance ("PCPO") currently in force. Most of the proposals in the Document are therefore not so necessary and practical especially the one making contravention of a data protection principle ("DPP") an offence.

OUR RESPONSES

1. **Proposal No 2: Regulation of Data Processors and Sub-contracting Activities**

We do not see the need to impose further obligations or statutory requirements on data users or data processors since the practices presently adopted by them in connection with sub-contracting activities are satisfactory and work well under the law. We take the view that it should be left to the data users or data processors to keep and continue the prevailing practices avoiding excessive intervention or pointless restrictions from the Privacy Commissioner for Personal Data ("PCPD").

2. **Proposal No. 3: Personal Data Security Breach Notification**

We have no strong view on the proposed establishment of a voluntary breach notification system except that greater flexibility should be afforded to the data user in the adoption of notification mechanism since the business nature, operation scale and the types of personal data collected vary from one to the next. We believe our suggestion herein tallies with the PCPD's intention as reflected in the Document of "*not causing onerous burden on the community*".

3. **Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD**

We do not support the idea of this proposal as the current arrangements of criminal investigations being conducted by the Police and prosecutions by the Department

of Justice have worked well, making this suggestion redundant and a waste of resources when the role of criminal investigation and prosecution power overlapped among various authorities. Even if there is no such overlapping, it is not cost-effective to allocate extra resources for the PCPD to carry out the duties which are already working well and effectively by other authorities.

4. **Proposal No. 5: Legal Assistance to Data Subjects under Section 66**

Our view is that every penny of the public funds should be spent wisely and in a cost-effective manner. We, therefore, do not agree to confer power on PCPD to provide legal assistance to data subjects. This proposal would leave the door wide open to vexatious complaints and the PCPD would very likely be flooded with requests for legal actions over frivolous claims when they find it a lot easier to resort to legal action with the financial back-up from the PCPD.

5. **Proposal No. 6: Award Compensation to Aggrieved Data Subjects**

We share the view of the relevant Law Reform Commission ("LRC") Report issued in August 1994 (as mentioned in the Document) that "*conferring power on a data protection authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions. The LRC recommended that the PCPD's role should be limited to determining whether there has been a breach of the DPPs.*" We opine that determining the amount of compensation payable or awarding compensation should be the job of the court, not the PCPD.

6. **Proposal No. 7: Making Contravention of a Data Protection Principle an Offence**

We oppose the suggestion of making contravention of a DPP an offence since DPPs which are couched in generic terms owe their origins to concepts and principles that can be subject to different interpretations. It would therefore be an uphill battle, if not impossible, to implement this option without causing unfairness and generating disputes. Besides, making a breach of a DPP an offence will be disproportionate and unfair in terms of the level of punishment if the non-observance of a DPP is simply out of honest mistake or inadvertent omission. The spirit of the DPPs / PCPO is to rectify contraventions by data users, so it is different from the ordinances in respect of criminal offences. To make it an offence

when a DPP is violated is draconian and move away from the original intent of the DPPs.

7. **Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data**
We opine that maintaining the status quo is preferable as the situation is not out of control under the PCPO and so it does not signal any need to change as far as this proposal is concerned.

8. **Proposal No. 9: Repeated Contravention of a DPP on Same Facts**
As mentioned in the Document, "*(s)ince the enactment of the PCPO, PCPD has not come across any such case of circumvention..*" Hence, there is no strong or imperative reason to institute any revamp in this respect and maintaining the status quo is the best course of action that the PCPD should pursue now.

9. **Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs**
We are also of the view that "*whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment*" as stated in the Document and so it is not desirable or appropriate for the PCPD to take up this extra role which will only complicate the sound practice currently in force as disputes over the interpretation of the above issues are bound to proliferate rendering the PCPD inundated with appeal action.

10. **Proposal No.11: Repeated Non-Compliance with Enforcement Notice**
Again, given that "*(s)ince the enactment of the PDPO, there has not been a problem with repeated offenders*"(as expressed in the Document), the existing practice holds water, making any rectifications in this regard superfluous.

11. **Proposal No.12: Raising Penalty for Misuse of Personal Data in Direct Marketing**
By the same token, it is unnecessary to raise penalty as the current level of penalty suffices in terms of its deterrent effect. Every penalty should be made in a proportionate and reasonable manner. Unless the violations grow in magnitude and seriousness and causing proven great loss / damage of the data subject and the problem seems to exacerbate, the penalty should not be raised.

12. **Proposal No.16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation**

We welcome the proposal of providing a new ground for a data user to refuse to comply with a data access request under section 20(3) of the PCPO where the data user is unable to disclose the same because of the obligation of "secrecy" imposed by other ordinances.

13. **Proposal No. 17: Erasure of Personal Data**

The suggestion in the Document of "*amending the PDPO so that provisions concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use*" is supportable in principle. More should be explored and discussed to map out a more flexible, liberal and accommodating approach for the data user so as to ensure a healthy growth of the business.

14. **Proposal No. 18: Fee Charging for Handling Data Access Requests**

We do not concur with the proposal of setting the prescribed maximum in respect of fee charging for handling data access requests since the costs vary from one company to another, rendering the said suggestion practically inoperable.

15. **Proposal No. 22: Removing the Time Limit to Discontinue an Investigation**

We basically have no objection to the idea of removing the time limit to discontinue an investigation which will be more cost-effective for the PCPD and fair to the party being complained against especially when there are lots of vexatious and frivolous complaints these days.

16. **Proposal No. 23: Additional Grounds for Refusing to Investigate**

The additional specific grounds set out in the Document for the PCPD to refuse to carry out or continue an investigation are supportable in principle for the optimal use of the PCPD's resources.

17. **Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition**

We welcome the proposed exemption from DPP3 for the transfer or disclosure of

personal data in intended merger, acquisition or transfer of businesses which will be beneficial to the operation and growth of the business sector.

CONCLUSION

Introduction of undesirable and somewhat draconian measures (like making contravention of a DPP an offence) will not only exert unnecessary burden on the business sector resulting in its growth and development being stifled and Hong Kong's competitiveness being compromised, it may also undermine the harmony in our society with tensions between competing community interests mounting and different sectors of the community antagonized and alienated. Thus, while we appreciate there is room for improvements in certain areas as proposed in the Document like introducing new exemptions for transfer of personal data in business mergers or acquisition, no drastic and pointless reform is welcomed. We believe that more instead should be done on education to raise the awareness of and develop a culture in respecting privacy and the personal data of the individual.

(the Organisation)

30 November 2009

S0153

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

香港盲人輔導會
The Hong Kong Society for the Blind

S0154

Our ref:

Your ref:

Patron:
The Chief Executive
Hong Kong Special Administrative Region
The Honourable Donald Tsang, GBM

Vice Patrons:
Mrs. Marjorie Bray
Dr. Bessie Chiang
Mr. Patrick T.K. Nip, JP
Mrs. Helen Kwok
Professor Dennis S.C. Lam
Professor C.K. Poon, GBS, JP

Chairman:
Mrs. Rachel Cartland

Chief Executive:
Ms. Maureen C.Y. Tam

At Headquarters:
Central Administration
Jr Support & Development Centre
Centralised Braille Production Centre
Resource Centre for the Deafblind
General Eye & Low Vision Centre
Information Accessibility Centre
Kowloon Home for the Aged Blind
Morning Glory Day Activity Centre cum Hostel
Rehabilitation Centre
Vision 2020 Low Vision Resource Centre

At Other Locations:
Bernard Van Zuiden Health Massage & Treatment Centre (Tuen Mun Branch)
Bradbury Care & Attention Home for the Aged Blind
Factory for the Blind
General Eye & Low Vision Clinic (Yuen Long Branch)
Yuen Long Home for the Aged Blind
The Hong Kong Jockey Club Community Project Grant - Parents Resource Centre for Visually Impaired Children
Jockey Club Tuen Mun Home for the Aged Blind
Rehabilitation Centre (NT)
Yuen Long Home for the Aged Blind

致: 香港特區政府政制及內地事務局(第 4 組)

檢討「個人資料(私隱條例」公眾諮詢

香港盲人輔導會就最近政府檢討「個人資料(私隱)條例」所提出之有關建議，現作出以下回應：

1) 敏感個人資料 — 敏感個人資料(如指紋)，本會認為需要嚴格規管。香港盲人輔導會是本港服務視障人士之主要機構之一，從五十三年的服務經驗中，本會認為個人指紋對視障人士尤其重要。在很多公文簽署上，視障人士(特別是全失明人士)之指紋就等同個人簽名；資料使用者在保存及應用個人指紋時必須受到嚴格規管，以免資料當事人受到傷害。

2) 資料保安 — 為保障個人資料無故外洩或得不到妥善保存，政府應立法規管受託處理個人資料的資料處理者嚴格執行資料保安；如發生個人資料外洩事故，應通知受影響人士或呈報所屬機構主管；對於建議規定要向私隱專員呈報，效用不大。

3) 私隱專員的權力、罪行及制裁範疇所提建議 — 我們認為不必賦予私隱專員刑事調查及檢控權力；但同意把資料使用者在未得資料當事人同意下所作惡意用途之行為及故意重犯者定為罪行或施加罪款，這些措施具有阻嚇作用。

4) 資料當事人的權利 — 為協助資料當事人獲得最佳利益，同意授權第三者為未成年人或精神上無行為能力者更改或查閱當事人資料；但如資料使用者更改或提出查閱資料之要求並不符合當事人之最佳利益，則其監護人有權作出拒絕。

5) 豁免遵從私隱條例 — 在特殊情況下，執法機關和支援機構應可獲得豁免在緊急情況下處理個人資料，但如有不當使用，應予以規管；有關准許資料使用者把當事人資料轉移給未成年人的父母或監護人，如該等情況是以保障資料當事人獲得最佳利益的，應予以豁免。

香港盲人輔導會謹啟

二〇〇九年十一月三十日

Views on the Review of the Personal Data (Privacy) Ordinance

Personal Submission by Allan G. Dyer

1 Introduction

This submission addresses the review of the Personal Data (Privacy) Ordinance (PDPO), and the consultation document published by the Hong Kong Government on 28th August 2009. The areas include the limited scope of the review, comments on most of the Proposals in the Consultation Document and further discussion on biometrics.

2 Copyright, Privacy, Obscenity and Free Speech

In January 2009, I made a submission[1,2] to the Review of the Control of Obscene and Indecent Articles Ordinance, saying, in part:

> "It is clear that different people hold a wide range of views on what personal information (including images) they want to record and, optionally, make public, and the view might change according to the circumstances. Similarly, there are many views on public decency and obscenity, and the location can change the standards. In the current situation, laws intended for other purposes are sometimes used to try to address these emerging issues. In the early stages of the Edison Chen scandal, it was suggested that websites publishing the photos should be prosecuted under the COIAO, despite the fact that the images were of a similar nature to many erotic images on the internet. Should an obscenity law be used to

---

[1] Volume 39 of the written submissions received during first round consultation of the Review of the Control of Obscene and Indecent Articles Ordinance: http://www.coiao.gov.hk/pdf/consultation/volume_039_complete.pdf

[2] Views on the Control of Obscene and Indecent Articles Ordinance: http://articles.yuikee.com.hk/newsletter/2009/01/c.html

> protect privacy? Now, copyright law is being used against the perpetrators, but copyright was originally intended as a trade: creators get exclusive rights for a limited period and Society benefits from the creations when copyright expires and they pass into the public domain. Why should that be used for images that were intended solely for private enjoyment?"

The Edison scandal is over, but the issue remains, and reappears in other, less high-profile cases: cases that are essentially about Privacy are being forced into fitting other definitions (Copyright or Obscenity, in this case) because the PDPO is too weak on enforcement.

Copyright, Obscenity, Privacy and Free Speech are all related to the control of information and are interlinked in complex ways. The complexity cannot be addressed by a limited review of the PDPO, I quote again from my submission[ibid.] to the Review of the Control of Obscene and Indecent Articles Ordinance:

> "A new Review should be launched, with a scope that covers all the closely related areas: Telecommunications and the role of ISPs, Privacy, Copyright, and Obscene and Indecent articles."

3 Proposal No. 1: Sensitive Personal Data

Imposing more stringent regulation on personal data because it is "sensitive" implies that disclosure of some information is inherently more damaging than the disclosure of other information. This is untrue: a person attending a trade union meeting, or a Mass at a Catholic Cathedral, or drinking in a gay bar is displaying biometric information (their face) in a public place, and providing a strong indication of their membership of a trade union, or religious beliefs, or sexual life, yet the disclosure is (usually) harmless. It is how the information is (mis-)used that makes the difference. Conversely, home address is not listed in the examples of "sensitive personal data", but disclosure of it to a loan shark could be extremely damaging for the individual concerned.

It would also be wise to consider the implications of classifying biometric data as "sensitive" and probable future improvements in technology. Classifying racial origin, and health condition as "sensitive" necessarily makes genetic information "sensitive", because our genetic information records our racial origin, and our inherited diseases. In future, it might also be possible to predict a person's facial features or fingerprints from their genetic information. However, we all constantly shed genetic samples,

most commonly in the form of dead skin and hair. House dust is mostly comprised of dead skin cells. The bag of a vacuum cleaner contains a record of the people who have been where it has cleaned and it might soon become feasible to extract that information. Will we require cleaners to follow strict data disposal protocols, or will we focus on how information is processed and used?

Biometric data, and how it can be disclosed, is considered further in section 15 .

The protection of personal data should not depend on whether it is included on a list of "sensitive" data because the potential damage depends too much upon circumstances, and because the more stringent controls will, inevitably make normal activities, such as cleaning, impossible.

4 Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

There appear to be, broadly, three categories of Data Processor that are affected:

i) Commercial contractors and sub-contractors;
ii) Service providers that do not use the data themselves, including ISPs and search providers;
iii) Social networking sites and other internet-related businesses that process the same data for multiple users.

Of course, these are not rigidly-defined categories, and one organisation might fall into more than one category, depending on the circumstances.

For the first category, the Data Users and the Data Processors have (or should have) the technical expertise to understand the issues, and the power to negotiate the contract to comply with the law. In that case, the Data User should be required to use contractual or other measures to secure compliance; and the Data Processors should be directly regulated in their obligations.

For the second and third categories, the Data Users (individuals and SMEs) do not have the power or technical expertise to negotiate with the Data Processors – at best, there will be a "take-it-or-leave-it" End User Agreement. My submission on the Review of the COIAC[*ibid.*], section 3.1 included a discussion of an overly-restrictive ISP End User Agreement, if the same restrictions on Data Processors, intended for

Contractors were applied to ISPs, then, no doubt, ISPs would find it necessary to protect their interests with even more restrictive End User Agreements.

The law should regulate limitations on the agreement so that Data Users are not faced with either blindly accepting impossible conditions, or being excluded from the Information Society.

So, for the second category, ISPs and search providers, a balance can be achieved by exempting them from most PDPO provisions, but not from ensuring the same level of security that the data had (if a website publishes private information to the world, it is not reasonable to prosecute a search engine for indexing it), while restricting their End User Agreements.

For the third category, social networking sites, it is a lot more complicated because the Data Users include not just multiple individuals and the site provider, but also third-party application (often game) developers, that may request and require users to allow access to their profile before they can play the game. The biggest issue here is that there is a lack of transparency about who is getting access to which data. The Data Protection Principles, particularly DPP1, DPP3 and DPP5, address this issue already, but social networking sites are often based outside of Hong Kong, and there have been no legal cases covering this area in Hong Kong so there is no guidance on best practice for those involved. This could be improved by:

i) Giving the Privacy Commissioner the power and resources to start an investigation without having received a specific complaint.
ii) The Privacy Commissioner preparing Guidelines for Social Networking sites, and, in the future, whatever new types of internet-based businesses that appear.

5 Proposal No. 3: Personal Data Security Breach Notification

A voluntary privacy breach notification system is worthless – the worst offenders will not volunteer so the additional costs caused will be a burden only on responsible organisations. Responsible organisations will therefore be less competitive in the Free Market, and irresponsible organisations will succeed, the exact opposite of what is desired. Therefore, there should be a mandatory breach notification system.

6 Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

There appears to be insufficient reason to concentrate the additional power of prosecution in the Privacy Commissioner.

7 Proposal No. 5: Legal Assistance to Data Subjects under Section 66

The power to provide legal assistance would greatly enhance the effectiveness of the PDPO.

8 Proposal No. 6: Award Compensation to aggrieved Data Subjects

While deciding on and awarding compensation may be best left to the courts to decide, it should be noted that the process of noticing, researching, reporting and following up on a possible breach of the PDPO can be time-consuming for a Data Subject. For example, in Case No. 200214122[3] a Data Subject noticed a potential security flaw on a website, tested that it actually existed, and reported it to the Privacy Commissioner. After investigation, the Commissioner required the website owner to improve the security and asked the Data Subject whether the changes made were sufficient. The Data Subject identified new flaws and reported them but also expressed the view that it is not his intention to do unpaid security consultancy for the website owner.

Notwithstanding any claim for compensation, it would be appropriate, when an Enforcement Notice is issued, for the Privacy Commissioner to require the culprit to

---

[3] Privacy Commissioner tells Mobile Operator to Improve Website Security
http://articles.yuikee.com.hk/newsletter/2003/12/c.html

recompense the reporter a reasonable fee for the service of reporting the breach of the PDPO.

9 Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

The biggest weakness in the PDPO currently is the Enforcement Notice system whereby personal data can be negligently or maliciously disclosed, with potential of actual damage to the Data Subject(s), and the Privacy Commissioner is essentially limited to saying, "Naughty, naughty; don't do it again"!

Disclosure of information is non-reversible, once published, it cannot be "un-disclosed" and the damage caused cannot be undone. The Edison Chen case illustrates this dramatically: the culprit who copied the files without permission has been sentenced[4] yet the pictures are still locatable on the internet, and the subjects' careers are still in tatters. In addition, maybe Edison was negligent in storing such sensitive information with insufficient protection.

The Enforcement Notice system may work adequately in allowing the Privacy Commissioner to review the handling of personal data in responsible organisations, and recommend improvements in-line with the DPPs, for example, when the Privacy Commissioner ordered a school to stop fingerprinting children[5]. However, it ceases to be effective as soon as negligence or malicious intent are involved. In particular, when there has been an actual data leak, with potential or actual damage to the Data Subjects, there should be penalties to act as an effective deterrent.

Over the past couple of years, there have been a string of data leak incidents: from an IPCC contractor[6], from Hospitals[7], the Immigration Department, and HSBC[8], but no

---

[4] 8½ Months Jail for Sex Photo Techie http://articles.yuikee.com.hk/newsletter/2009/05/a.html

[5] HK Privacy Commissioner on Fingerprinting in Schools http://articles.yuikee.com.hk/newsletter/2006/11/b.html

[6] IPCC Data Leak http://articles.yuikee.com.hk/newsletter/2006/03/g.html

[7] Privacy Commissioner Recommends Improvements at the Hospital Authority http://articles.yuikee.com.hk/newsletter/2008/07/c.html

[8] Data Leak Disease http://articles.yuikee.com.hk/newsletter/2008/05/d.html

penalties for the negligent organisations and staff. This sends a clear message: don't bother about protecting personal data until you receive an enforcement notice.

10 Proposal No. 8: Unauthorised Obtaining, Disclosure and Sale of Personal Data

Breach of DPP3 is one of those areas where, as discussed above, in Section 9 , the Enforcement Notice system is inadequate, and it should therefore be an offence. The defence provisions used in the UK appear reasonable.

However, it should be noted that "identity theft" is, in general, an offence enabled by the negligence of Data Users that inappropriately use personal data for the purpose of authentication. It would not matter that a criminal could discover your mother's maiden name or the name of your first pet if you bank did not use that information for their "security questions". Disclosure of other biometric data is discussed in section 15 .

The Privacy Commissioner should make it clear that inappropriate use of personal information for authentication contravenes DPP1 ("Only personal data that are necessary for or *directly related to* the purpose should be collected") and DPP4 (security of personal data), and should issue Enforcement Notices to organisations, particularly banks and financial institutions (where the potential loss is greatest) that are negligent about this.

11 Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts

From a casual reading of the Privacy Commissioner's website, and other documents, it is not clear that this loophole exists. However, if it does, it is a serious flaw that should be fixed as soon as possible. The fact that no cases have occurred is irrelevant: a Data User that did this would be flouting the intent of the law with clear premeditation and there must be a strong motive for the action. The penalty level should be the same as simple non-compliance.

12 Proposal No. 10

No comment.

13 Proposal No. 11: Repeated Non-compliance with Enforcement Notice

A repeated offence should attract a heavier penalty.

14 Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

Before raising the maximum penalty, it should be considered whether making the penalty proportional to the number of Data Subjects that were victims would be effective. Thus, if a direct marketer misused an address list of 10,000 people, the magistrate could impose a fine of up to $10,000 for each person affected, which is 10,000 x 10,000 = $100,000,000 in total. If the base penalty is commensurate with the damage to the individual victim, then the total penalty will be commensurate with the damage to Society. Organisations that hold, and (mis-)use, data on individuals should realise that their responsibility grows with the number of individuals.

15 Biometric Data and Authentication

We all constantly disclose our biometric data in numerous ways – genetic information in dust has already been mentioned in section 3 , we disclose our face simply by walking down the street, and leave our fingerprints on each door handle and handrail we touch. More permanently, in the Hong Kong Polytechnic University there is a wall featuring the handprints of distinguished donors where the fingerprints are clearly discernable, and quite possibly recoverable. Should the wall be demolished, and we all be required, by law, to wear masks and gloves in public?

The problem is not in the disclosure of the information, but in the processing and use of it. Biometrics is frequently seen as the panacea for authentication problems when, in reality, it provides a (at best) unique identifier, not an authenticator. It is only under

carefully-controlled conditions, such as in the Immigration halls at our borders, that the connection between identity and authorisation can be reliably made.

16 Conclusion

The current PDPO restricts the Privacy Commissioner to being ineffective. No matter the severity of the case, he or she can only issue an enforcement notice in the first instance. The current situation means that there is little incentive for organisations to improve their handling of personal data, before an incident occurs. We have therefore seen a continued series of headline-grabbing incidents.

The implications of Social Networking and similar internet-based applications with numerous data users are a concern and should be considered in detail.

Review of the Personal Data (Privacy) Ordinance (PD(P)O)

The Electronic Health Record (eHR) Office of the Food and Health Bureau has sought comments from the members of the Working Group on Legal, Privacy and Security Issues of the Steering Committee on eHR Sharing. The comments of the eHR Office, the Department of Health (DH), Consumer Council (CC), Hospital Authority (HA), and the Office of the Government Chief Information Officer (OGCIO) are set out below.

Proposal No. 1: Sensitive Personal Data

Party	Comments
eHR Office	The eHR Office recognises that the leakage of some health information such as mental health and HIV status may cause serious harm to or discriminatory decision against the data subject. We do not object to categorising such health information as sensitive personal data (SPD) but the scope of sensitive health information should be carefully deliberated with input from the public and private healthcare sectors, various stakeholders, and the general public. On the other hand, we object to categorising all health information as SPD since the disclosure of general health information such as the height, weight, blood type or drug allergy of a person is unlikely to cause serious harm to a person and therefore does not warrant special protection over other non-sensitive personal data. Paragraph 3.09(f) allows the use of SPD if it is "necessary" for medical purpose. However, the necessity requirement is not defined. One may consider that only if the healthcare provider can establish that (a) the patient is in imminent danger; (b) there is no reasonable alternative to using the SPD; and; (c) the use of SPD is proportional to the danger avoided, he/she could use SPD for medical purpose. However, if SPD is only allowed to be used under such requirements, this is much too restrictive and would seriously undermine the ability of the provider to deliver care. During a medical consultation, healthcare providers have to view the record of a patient, which may or may not contain SPD, before they can assess whether the information within the record is

	necessary for (or even related to) the diagnosis of the patient. The provisions for using SPD in some overseas jurisdictions are less restrictive. For example, National Privacy Principle 2.1 (a)(i) of the Australia Privacy Act sets out that sensitive information may be used for a purpose "directly related to the primary purpose of collection". In view of the duty of confidentiality owed by healthcare providers which offers some protection to privacy of patients, the eHR Office suggests that the *reasonable* collection, use, disclosure, and handling of SPD by healthcare providers under duty of confidentiality for medical purposes should be permitted. We support the grandfathering arrangement as set out in paragraph 3.13. In addition, the grandfathering arrangement should be applied whenever new categories of data are added to the scope of SPD.
DH	It is noted that the intention to tighten control over "sensitive data" is restrictive in scope (limits to biometric data and does not cover health/medical data). DH is of the view that the implications of the proposals are not different for the non-eHR or eHR. As such, I have no comment on the consultation paper in the eHR context.
CC	In light of the potentially substantial damage to data subject caused by leakage of sensitive personal data, CC is of the view that additional requirements should be imposed for handling sensitive personal data and that contravention of the requirement should attract heavier penalty. However, CC cannot see the reason why biometric data is singled out for the subject to be addressed as a start of the proposed change. Biometric data, as the Consultation Document refers to, are used for identification and authentication. It is likely that they are mostly used by corporations for human resources management and security purposes. Therefore, the impact of the proposed amendment will be limited to giving better protection to corporations in this regard. On the other hand, sensitive personal data such as identity card number, medical data, bank account number, credit card number and sex orientation, may be much more vital to individuals because

	the leakage of which may put them at real risk of substantial loss in terms of finance, physical safety, employment opportunity, reputation or otherwise. CC thinks the Administration has recognized the significance of sensitive personal data privacy and attached particular importance on protecting them from being infringed. The Steering Committee on eHR Sharing may take the chance of the Review of the Ordinance to revisit the issue establishing a legal framework for eHR sharing system, If it is recognized that health record is sensitive personal data deserving a level of protection similar as that proposed in the Consultation Document, it seems that a practicable option of addressing the legal framework of the eHR sharing system will be to include health record or personal health data as one of the categories of regulated sensitive personal data in the principal legislation of the Personal Data (Privacy) Ordinance. Apart from that, a set of guidelines can be issued by the Commissioner for Personal Data specifically for the collection, holding, processing and use of ehealth record to help data users and data processor comply with the relevant statutory provisions.
HA	***HA does not support this Proposal to create a further category of sensitive personal data because the existing system is well in place and the requirements of the proposed model will impose onerous operational and financial burden on HA bearing in mind collection of biometric data in the course of diagnosis and treatment is very common and in substantial volume in HA.*** PDPO has an existing system well in place obliging data users to protect and safeguard all personal data of data subjects and to comply with the statutory requirements and the data protection principles (DPP) thereunder. It is questionable whether a further category of sensitive personal data with more stringent requirements over and above the existing system is necessary. We do not recommend a further category of sensitive personal data to be created.

	If such a separate mechanism were introduced, data users will be subject to additional operational and financial burden. The potential value and benefit from such a mechanism has to be weighed against the likely costs and resources to be expended in order to comply with such regime. Depending on what will be classified as sensitive personal data, it can potentially be onerous for HA to set up a new mechanism to handle this particular category. As a major health care provider in Hong Kong, HA handles substantial volumes of patients' personal data on a daily basis which are already subjected to the existing requirements of PDPO and under applicable law. If a special category of 'sensitive personal data' is introduced, it is important that the legislation precisely define the scope of such data and the scope be limited at the outset. Data users need to be clearly guided as to its coverage and a narrower scope will enable data users and the administration to assess the practicalities of the mechanism. If non-compliance with the new mechanism has potentially serious sanctions, it is all the more necessary that data users are facilitated by the legislative provisions and by administrative guidance on how to identify and handle such data. The possible regulatory model imposes a general prohibition on the handling of sensitive personal data unless in specified exceptions. The burden lies on the data user to justify on each and every occasion that it can collect, hold, process and use sensitive personal data. If this model is to be adopted, it is important that the legislation should state and define such exceptions with clarity and precision. This is particularly so if the administration intends to impose sanctions or make it an offence for non-compliance with the new mechanism. Under paragraph 3.09 in this proposal, the exceptions refer to situations where the data subject's prescribed consent has been (in subparagraph (a)) or cannot be obtained (in subparagraph (c)). The legislation should make clear how these exceptions apply particularly in the context of data subjects who are minors or who lack mental capacity.

	The exceptions use the word 'necessary' on different occasions under subparagraphs (b), (c) and (g). The future model (if introduced) should give good guidance as to by what criteria this word is to be applied and interpreted. Under paragraph 3.09(c), an exception is when the handling of the data is necessary for protecting the vital interests of the data subject or others where the data subject's prescribed consent cannot be obtained. Clear definition should be given as to what vital interests mean. Under the model in paragraph 3.09(d), good and detailed guidance as to what amounts to appropriate safeguards should be given. Indeed, safeguards already exist under the present regime in PDPO against transfer or disclosure of personal data.
OGCIO	Para 3.06 – This is rather misleading. There is no elaboration on how biometric data (e.g. iris, fingerprint, voice, etc.) can enable extensive monitoring of the activities of individuals, as well as identification of individuals without their knowledge or consent. It is also not apparent how biometric data in general (e.g. fingerprint, voice pattern or iris scan information, etc.) could reveal sensitive personal information such as health, genetic information or ethnic origin. This is confusing as whether the biometric data itself is personal data or whether this biometric data is used to authenticate for access to other personal data collected separately. Para 3.08 – A general sweeping statement of all biometric data to be classified as sensitive personal data needs to be explained and justified.

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

Party	Comments
eHR Office	The Indirect Regulation Model set out in paragraph 4.20 which relies on the data users to ensure that their data processors provide security protection to personal data at a level comparable to

	themselves may impose additional burden on the data users if they are obliged to take positive actions such as monitoring and auditing to ensure data processors meet their contractual arrangement to provide such protection. Furthermore, the proposal set out in paragraph 4.09 requiring data users to take steps to ensure the compliance of subcontractors may not be practicable as data users do not have a direct contractual relationship with subcontractors. Data users may not even be aware about the subcontracting activities. Even if the Indirect Regulation Model only requires data user to include a related clause in the contract with the data processor, redressing a contravention by a subcontractor will be a cumbersome process which requires the Privacy Commissioner for Personal Data (PCPD) to rely on the data user and the data processor to take appropriate action against the subcontractor under contractual law. In view of the extra burden imposed by the Indirect Regulation Model, the eHR Office prefers the Direct Regulation Model where the data processors and subcontractors are regulated directly by the PCPD.
HA	***HA does not support this Proposal because the existing PDPO already imposes obligations on data processors and sub-contractors to protect personal data against unauthorized use etc.*** The PDPO already imposes obligations on data users to take all reasonably practicable steps to ensure that personal data held by a data user are protected against unauthorized or accidental access, processing, erasure or other use. As the administration considers that the PDPO does not directly regulate the activities of an agent which processes personal data for its principal, the administration may wish to consider adjusting the definition of data user to include such data processors and subcontractors. This is particularly so in the context of eHR.
OGCIO	Para 4.08 and Para 4.21 – Under eHR Programme, it may be difficult to identify who or which party is the "data processor". The eHR sharing infrastructure holds the data, so should it be treated as the "data processor" only or "data user" as well? Moreover, the

	roles and legal liability of eHR Office who is responsible for the overall operation of eHR Sharing Infrastructure on behalf of all stakeholders should be clarified. On the other hand, there is need to explain the roles and responsibilities of "data user" and "data processor" to all eHR stakeholders from the public and private sectors who will participate and share the eHealth record.

Proposal No. 3: Personal Data Security Breach Notification

Party	Comments
eHR Office	The eHR Office supports the requirement for data users to notify the PCPD when a personal data security breach may result in a high risk of significant harm to individuals or organisations. On the other hand, a privacy breach notification system for affected individuals should set clear the circumstances which would trigger individual notification and the consequences of failing to give such notifications. The potential number of patients affected in a privacy breach incident in the eHR sharing infrastructure can be large. We concur with the view set out in paragraph 4.41 that individual notification will not be practical in some situations. The notification system should set out the acceptable substitute methods for individual notification and the circumstances when such methods may be applied.
HA	***HA supports this Proposal.*** The concept of a voluntary privacy breach notification system is supported but the specifics need to be worked on what needs to be notified and when. Clear guidance and adequate timing for such notification should be given. The voluntary mechanism should be limited to serious cases of personal data leakage or loss in the assessment of the data user. Being a voluntary mechanism, there should not be consequences for failing to give notification. Besides, to report the breach to PCPD within 5 business days is too tight for an organization to recollect the facts of the breach, analysis of the data lost and assessment of potential risks.
OGCIO	Para 4.43 – The voluntary notification mechanism seems work well for public bodies, e.g. for some losses of USB storage in public

	hospitals, the incident was reported and the data subjects were informed. The stakeholders from private sector and NGOs who will connect with eHR Sharing Infrastructure are advised to adopt the same notification mechanism as the eHR Office.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

Party	Comments
eHR Office	Given the existing arrangement of the PCPD to refer cases to the Police for prosecution has been working smoothly, the eHR Office concurs with the view set out in paragraph 5.09 that there is no strong need to give the PCPD the power to investigate into and prosecute criminal offence cases. Empowering the PCPD to conduct search for or seize evidence in the eHR sharing system for criminal investigation would raise public concern about the privacy of their health records, therefore we recommend the current power of the PCPD remain as is.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

Party	Comments
eHR Office	It is difficult to ascertain the potential liabilities and the extent of compensation to be awarded to the aggrieved data subjects. Hence this would create a lot of uncertainties on the responsibilities of data users/processors. Moreover, multiple data users and data processors can be held liable in a single act of contravention. The delineation of liabilities among different parties would be even more complicated, and may require judicial judgement. Should there be a mechanism for awarding compensation to aggrieve data subjects, the eHR Office considers that the proposal should specify the specific acts of contraventions which would lead to compensation being awarded to aggrieved data subjects. We also suggest that the amount of compensation awarded should be based on the actual damage suffered by the data subject. These clarifications will ensure the compensation scheme is fair to both data subjects and data users.

Proposal No. 7: Making Contravention of a DPP an offence, and
Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

Party	Comments
eHR Office	The proposals to criminalise or impose a monetary penalty on contravention of DPPs are difficult to enforce, as the DPPs are subject to a wide range of interpretations. These proposals will also undermine healthcare professional's interest in participating in eHR Sharing, fearing that they may accidentally commit a criminal offence. We support the suggestion in paragraph 6.20 that specific acts of contravention of DPP be singled out as offences, and suggest that monetary penalty or criminal liability be imposed according to the seriousness of each act.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

Party	Comments
eHR Office	The eHR Office supports in-principle the criminalisation of unauthorised obtaining, disclosure, and sale of personal data but suggest that the proposal should be strengthened. To also outlaw the use of personal data obtained without authorisation from data processors (such as hacking the eHR central database), the proposal should criminalise the *use and handling*, in addition to disclosure, of personal data for profits or malicious purposes obtained without consent from *data processors*, in addition to data users.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data, and
Proposal No. 37: Expand the Definition of "Relevant Person"

Party	Comments
eHR Office	The proposals of expanding the definition of "relevant person" to the legal representative or guardian of mentally incapacitated persons (MIP) and allowing relevant persons to give consent to the

	use and disclosure of personal data are essential to facilitate eHR sharing among minors, MIPs, and other persons unable to grant consent to participate in the eHR programme. The eHR Office supports these two provisions.
OGCIO	Annex 1, Para 2 – 6 – The option to allow third party (relevant person) to give consent to the change of use of personal data of vulnerable classes of data subjects is essential for the smooth operation of eHR.

Proposal No. 14: Parents' Right to Access Personal Data of Minors, and Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

Party	Comments
eHR Office	These two proposals, which set out the right of data users to deny a parent's access request to a minor's personal data and the right of data users to transfer a minor's personal data to his / her parents, requires data users to determine what constitutes the "best interest" of the minors. We also note that Section 21(1)(b) of the PD(P)O requires the data users to provide the reasons for refusing a data access request. Proposal No. 14, together with Section 21, would require healthcare practitioners denying the access request of a parent to explain why such decision is in the best interest of the minor. Relying on healthcare practitioners to make such judgements and explain their rationale on a case-by-case basis would place unnecessary burden to the practitioners and impact their ability to provide care. Instead, the amendment should set out clearly the circumstances when a parent's access request should be denied or the personal data of a minor should be transferred to the parents to avoid placing a healthcare practitioner in between a parent-child conflict. In addition, healthcare practitioners owe a duty of confidentiality to their patients. The transfer of medical information of minors to their parents may cause a breach of confidentiality, especially if the minor has expressly dissented to such a transfer. Therefore, Proposal No. 27 should be further clarified on whether acting on the best interest of the data subject constitutes a legal exemption to the

	duty of confidentiality. It should also lay out whether the transfer is still permitted if the minor expressly dissent to the transfer.
OGCIO	Annex 1, Para 7-12 – This proposal should follow the existing professional code of practice of medical practitioners.

Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data, and
Proposal No. 14: Parents' Right to Access Personal Data of Minors

Party	Comments
HA	***HA does not support these Proposals because it will be difficult for the HA to judge whether a request for a changed use or for disclosure of the personal data of the minor or a mentally incapacitated adult is or is not in his best interest or benefit.*** Proposal 13 contemplates amending the PDPO to allow certain third parties to consent on behalf of data subjects who do not have sufficient understanding or intelligence to a change of use by the data user of the data subject's personal data if it is in the data subject's best interests or clear benefit to do so. Proposal 14 is limited to a data access request situation in the context of a minor. It contemplates that a data user may refuse a data access request by a relevant person on behalf of a minor if the data user has reasonable grounds to believe that complying with the request would not be in the minor's best interests. Under Section 18 of the PDPO, a relevant person (whether as currently defined in the PDPO or as may be expanded under Proposal 37) on behalf of an individual may request a data user to supply the individual's personal data that it holds. The data user is obliged to comply with such request unless otherwise permitted under the PDPO. There is no need for the relevant person to show and there is no need for the data user to know for what purpose the data requested is to be applied and whether such use is in the data subject's interests or benefit. Following from this, the data user should not be laden with an

additional burden to judge and determine whether a request for a changed use or for disclosure of the personal data of a minor or a mentally incapacitated adult is or is not in his best interests or benefit. Often, the request for a changed use or disclosure is not initiated by the data user but by some third party, and the data user is only responding to the request made.

Paragraph 8(a) describes a circumstance where a parent may abuse the data access mechanism to obtain the personal data of the child for the parent's own purpose rather than making it "on behalf of" the child. However, it can be very difficult to judge if there is an abuse. It may or may not be possible for the HA to judge the circumstance described in paragraph 8(b), i.e., whether a parent is suspected to have committed child abuse.

Such a task to determine what is in a person's best interests or benefit can be difficult, especially for data users like HA which handles voluminous personal data of numerous data subjects. A data user may not have the information or ability to judge matters of clear benefit or best interests and it cannot be expected to embark on an investigation to check into or verify that. The data user may have little or no alternative but to place reliance on the assertions raised by the relevant person as to the benefit or best interests claimed. Indeed, what is 'clear' benefit can be hard to assess.

Furthermore, paragraph 6 under Proposal 13 raises a concept that other relatives or child care placement may be included as 'relevant person'. This calls into question how far the scope of relevant person should be extended. The practical logistics as to how this works need to be carefully canvassed especially when different persons claiming to be the 'relevant person' may object or consent to a changed use or disclosure and the data user is caught in the family dispute.

It would be helpful to take this opportunity to make clear what it means (in the context of a relevant person) to have parental responsibility and how it is applied in different situations such as divorced or separated parents, where a parent no longer has custody

	of the minor, where a parent has died or in a stepparent situation. Lastly, if a minor is assessed to be of sufficient understanding and intelligence, his wishes as to his personal data privacy will need to be respected. There may be conflict in views between such a minor and the relevant person. If such a minor agrees or disagrees to a disclosure, it will be difficult for the data user to override his wish. Making clear the priorities will be helpful.

Proposal No. 17: Erasure of Personal Data

Party	Comments
eHR Office	The eHR Office supports the proposal to relax the absolute duty on a data user to erase obsolete personal data. To leverage the health data within the eHR system for public health planning purposes, we also suggest Section 26(1)(b) of the PD(P)O be amended to explicitly include public healthcare purposes as an exemption from the duty to erase obsolete personal data.
OGCIO	Annex 1, Para 21-23 –The proposal should follow the existing regulation and practice on inventory and management of patient medical record.

Proposal No. 18: Fee Charging for Handling Data Access Requests

Party	Comments
eHR Office	The eHR Office considers that it is difficult to set a prescribed maximum fee for handling data access requests given the likely difference in administration costs of different data processors/users. Adjusting any prescribed maximum for inflation or other changes in costs will also be difficult.
HA	***HA supports this Proposal and our comments will be elaborated in the HA's response to the Constitutional and Mainland Affairs Bureau.*** Having a maximum fee is supported provided there is adequate consultation as to the setting of the fee level and the maximum fees for chargeable items are set at a reasonable level.

Proposal 22 – Removing the Time Limit to Discontinue an Investigation

Proposal 23 – Additional Grounds for Refusing to Investigate

Party	Comments
HA	*We support these Proposals.* Section 38 of the PDPO sets out circumstances whereby the PCPD shall carry out an investigation. Before embarking on such an investigation, the PCPD would carry out "preliminary enquiry" to obtain information in order to decide whether to exercise its investigation power under Section 38. In the course of such preliminary enquiry, the PCPD may ask for disclosure of personal data of the complainant or other data subjects without furnishing consent from these individuals. For the sake of certainty, it will be beneficial to clarify that a data user is permitted to and will not contravene the PDPO or the DPP if and when it discloses such personal data to the PCPD in response to questions raised by the PCPD under the preliminary enquiry.

Proposal No. 25: Provision of Identity and Location Data on Health Grounds

Party	Comments
eHR Office	The eHR Office supports the proposal to broaden the scope of application of exemption set out in Section 59 to cover data related to identity and location of the data subject. The proposal would allow the Administration and the Hospital Authority to take advantage of the information in the eHR system and execute operations in infection control by facilitating immediate access, rescue, and other preventive actions.
OGCIO	Annex 1, Para 54-58 –This exemption is necessary for using eHR Sharing Infrastructure for the purpose of disease control.

Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

Party	Comments
HA	*HA supports this Proposal but it can be difficult for HA to judge whether a disclosure is for discharging the parent or guardian's*

	responsibility on proper care and guardianship of the minor in the situation other than the provision of healthcare. Proposal 27 seeks to deal with the restriction under the PDPO disallowing data users to transfer, of their own accord, the minor's personal data to his parents or guardian even if such transfer is to the minor's benefit. Proposal 27 contemplates introducing an exemption from DPP3 to permit data users to transfer a minor's personal data to his parents or guardian so that parents and guardian can properly discharge their responsibility on proper care and guardianship. In the context of seeking consent for the provision of medical treatment to minors, the HA relies on the general law that consent can be obtained from those with parental responsibility of the minor. To obtain consent from those with parental responsibility, it is inherent that information will need to be provided to them in order to enable them to make the decision. This process will involve disclosure of the minor's personal data to them. Such disclosure is necessary as part of the rendering of healthcare to minors. In situations other than the provision of healthcare, it may be difficult for HA to judge whether a disclosure is for discharging the parent or guardian's responsibility on proper care and guardianship of the minor. Nevertheless, if a data user makes such transfer or disclosure in the belief that it is to enable the parent or guardian to discharge his or her responsibility, but the minor or the parent or guardian disagrees, the data user should not be penalized for taking such a step. Furthermore, data users will want to know whether it is necessary before applying such exemption to ascertain the views of the minor (especially if the minor is of sufficient intelligence and understanding). If such minor objects to the transfer or disclosure, then the priorities should be clearly set out.
OGCIO	This exemption is highly desirable for the smooth operation of eHR Sharing Infrastructure.

Proposal No. 33: Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings

Party	Comments
eHR Office	The eHR Office supports the proposal to exempt the use of personal data required or authorised by law from DPP 3. It will allow various public bodies, empowered by legislations such as the Prevention and Control of Disease Ordinance, to use the health information within the eHR system for public health surveillance and monitoring purposes.

Proposal 36 – Definition of Crime under Section 58 to mean a crime under Hong Kong law, or a crime or offence under the law of a place outside Hong Kong

Party	Comments
HA	***HA does not support this Proposal because data users may not have the ability or knowledge to assess whether a situation amounts to a crime and offence overseas.*** As the burden is on the data user to show it was justified to rely on a Section 58 exemption, data users may not have the ability or knowledge to assess whether a situation amounts to a crime and offence overseas. There can be practical difficulties to judge and determine the position under foreign law.

Proposal 37 – Expand the definition of "Relevant Person" to include the guardian of data subjects with mental incapacity appointed under Sections 44A, 59O and 59Q of the Mental Health Ordinance

Party	Comments
HA	***HA supports this Proposal.*** The administration may consider whether to expand the definition to cover, for example, an attorney appointed under an enduring power of attorney.

	Furthermore, applications for guardianship under Part IVB of the Mental Health Ordinance have to be supported by (amongst other matters) written reports of registered medical practitioners. In support of applications to the court under Part II of the Mental Health Ordinance, medical certificates are also required. As the data subject is mentally incapacitated, the party requesting for such reports or certificates from the HA is unable to furnish the data subject's consent to the HA for disclosure of the same. On the other hand, without these reports or certificates, the application will not be able to proceed. It would be beneficial to clarify that disclosure of personal data contained in such reports or certificates for the purpose of such applications under the Mental Health Ordinance will not be in breach of the PDPO or the DPP.

Proposal No. 38: Exclude Social Services from the Definition of "Direct Marketing"

Party	Comments
HA	***HA supports this Proposal.*** This proposal seeks to enable social workers in providing essential social welfare services for the benefit of target recipients to continue to use an individual's personal data without the need to inform the individual of an 'opt-out' right. In the HA, there may be circumstances where individuals may refer another person to the HA for psychiatric help and support and the person referred has not previously been treated in HA. The administration may consider extending the proposal to exclude from 'direct marketing' the provision of such needed services for the benefit of such persons being referred.

Other Comments

Party	Comments
HA	**HA believes that the status quo under PDPO should be adequate in respect of the following proposals:** (1) Proposal 4 – Granting Criminal Investigation and Prosecution

	Power to the Privacy Commissioner for Personal Data (PCPD) (2) Proposal 6 – Award Compensation to Aggrieved Data Subjects (3) Proposal 7 – Making Contravention of a Data Protection Principle (DPP) an Offence (4) Proposal 8 – Unauthorized Obtaining, Disclosure and Sale of Personal Data (5) Proposal 9 – Repeated Contravention of a DPP on Same Facts (6) Proposal 10 – Imposing Monetary Penalty on Serious Contravention of DPPs (7) Proposal 11 – Repeated Non-compliance with Enforcement Notice (8) Proposal 12 – Raising Penalty for Misuse of Personal Data in Direct Marketing (9) Proposal 20 – Circumstances for Issue of an Enforcement Notice (10) Proposal 21 – Clarifying Power to Direct Remedial Steps in an Enforcement Notice (11) Proposal 40 – Extend Time Limit for Laying Information for Prosecution **HA supports the following proposals:** (1) Proposal 16 – Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation (2) Proposal 17 – Erasure of Personal Data (3) Proposal 19 – Response to Data Access Requests in Writing

	and Within 40 Days (4) Proposal 24 – Transfer of Personal Data in Business Mergers or Acquisition (5) Proposal 25 – Provision of Identity and Location Data on Health Grounds (6) Proposal 26 – Handling Personal Data in Emergency Situations (7) Proposal 43 – Contact Information about the Individual Who Receives Data Access or Correction Requests **HA has no comment on the following proposals:** (1) Proposal 5 – Legal Assistance to Data Subjects under Section 66 (2) Proposal 15 – Access to Personal Data in Dispute (3) Proposal 28 – Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result (4) Proposal 29 – PCPD to Disclose Information in the Performance of Functions (5) Proposal 30 – Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit (6) Proposal 31 – Power to Impose Charges for Educational and Promotional Activities (7) Proposal 32 – Power to Obtain Information to Verify a Data User Return (8) Proposal 33 – Use of Personal Data Required or Authorized by

	Law or Related to Legal Proceedings (9) Proposal 34 – Transfer of Records for Archival Purpose (10) Proposal 35 – Refusal to Comply with a Data Access Request on Ground of Self-Incrimination (11) Proposal 39 – Exemption for Personal Data Held by the Court or Judicial Officer (12) Proposal 41 – Duty to Prevent Loss of Personal Data (13) Proposal 42 – PCPD to Serve an Enforcement Notice together with the Results of Investigation **HA supports the administration position on Annex 2 – Proposals not to be pursued.**

eHealth Record Office
Food and Health Bureau
November 2009

香 港 人 權 監 察
HONG KONG HUMAN RIGHTS MONITOR

人權監察就
港府〈檢討《個人資料(私隱)條例》的諮詢文件〉
的意見書
二零零九年十一月三十日

前言

1. 《個人資料(私隱)條例》(第486章)(「私隱條例」)在1996年生效,在個人資料方面保障個人的私隱。個人資料私隱專員公署(私隱公署)指出:「隨著電子年代的降臨,科技及電子交易及商貿的急速發展,引起全球對個人資料私隱的關注」[1]。個人資料私隱專員(私隱專員)經累積逾10年的監管經驗,認爲是適當時候從逐漸成形的國際宏觀私隱角度,對私隱條例作出全面檢討。私隱公署於2006年6月成立內部的條例檢討工作小組,並於2007年12月向政制及內地事務局呈交一套逾50項的修訂建議。

2. 政制及內地事務局於2009年8月推出「檢討《個人資料(私隱)條例》的諮詢文件」(諮詢文件),進行爲期3個月的諮詢。香港人權監察歡迎有關當局就檢討私隱條例諮詢公眾,認爲私隱條例必須檢討,以進加強對個人資料私隱的保障,並在此意見書的附件中詳列人權監察對逐項修例建議的意見。

指導原則與加強保障私隱對立

3. 私隱公署亦指出「海外政府及私隱規管機構均認爲有迫切需要檢討及改革私隱法例,以加強保障個人資料私隱權益」[2]。人權監察在歡迎政府進行諮詢的同時,亦注意到諮詢文件提出的多項指導原則並沒有包括爲個人資料私隱提供可行的最大保障,反而當中過分強調其他權利、某些公眾利益、社會利益、便利通訊及通訊科技持續發展等取得平衡、任何修改都不應削弱香港作爲國際城市的競爭力和經濟效率,及需要避免商業活動和個別資料使用者承受沉重負擔等,在在削弱對個人資料私隱的保障。人權監察認爲,私隱條例的修改應該以爲個人資料私隱提供應有的最大可行保障爲指導原則。

政府不予跟進的建議

4. 人權監察注意到,有9項私隱專員有關私隱條例規管範圍、豁免條文及私隱專員權力的建議,政府當局「經審議有關建議可能帶來的影響後」,並無意跟進。

5. 人權監察認爲,私隱專員有關的建議,對執行私隱條例或保障個人資料私隱都可能有

---

[1] 個人資料私隱專員公署就檢討《個人資料(私隱)條例》的資料文件(私隱公署就檢討私隱條例的文件)第1段,2009年9月9日。
[2] 同上,第2段。

相當重要的影響和意義，修例與否將會引起社會的關注和討論。人權監察特別注意到，私隱公署內部的條例檢討工作小組對該 9 項建議都是支持或支開放態度，亦特別指出「把互聯網規約地址 (IP 地址) 視爲個人資料」及「重整直接促銷的規管機制」兩項議題應該進行公眾諮詢[3]。即使在政府發出諮詢文件後，私隱公署亦再一次指出政府有需要就「把互聯網規約地址視爲個人資料」展開諮詢，及指出「有關公眾利益的裁決」的豁免條文的必要性[4]。人權監察強調，即使政府現階段不支持該 9 項建議，亦應該就此一併進行諮詢，了解社會大眾是否認同政府的意見。人權監察認爲政府應該接納那些加強對人權保障的建議。此外，訂明公眾利益爲豁免依據，亦甚爲重要，政府不應忽視這方面的建議。

充分考慮兒童的最大利益

6. 諮詢文件中有三項與兒童直接有關的建議 (建議 13、14 及 27)，人權監察均強調在考慮該三項建議時，「兒童的最大利益」是當中最重要的原則，而兒童私隱權及兒童表達權亦相當重要。人權監察認爲，不同持分者包括未成年人、家長、監護人及資料使用者可能對「兒童最大利益」有爭議，政府應設立機制，予未成年人上訴捍衛自己的權益，及當未成年人與家長出現爭議時，沒有機制協助未成年人。

[3] 公署 (個人資料私隱專員公署) 內部的檢討工作小組作出的修訂建議 (公署修訂建議)，第 139-142 頁。
[4] 私隱公署就檢討私隱條例的文件，第 13.1 至 14.10 段。

附件：香港人權監察對「檢討《個人資料 (私隱) 條例》的諮詢文件」逐項建議的回應

政府不予跟進的建議

(A) 私隱條例的規管範圍	
A.1：重整直接促銷的規管機制	人權監察支持有關建議，認爲政府應該加以跟進。 人權監察同意私隱公署指「太多不受控制的直接促銷活動會對個人造成滋擾和煩惱，並鼓勵大量出售個人資料，侵犯了資料當事人的個人資料私隱，尤其是「不被騷擾」的權利」[5]，並注意到《非應邀電子訊息條例》未有規管人對人促銷電話，故此贊成加強在私隱條例下對直接促銷的規管機制。 人權監察同意政府推行曾考慮的規管方案，包括 (a) 引入新規定，凡首次把個人資料應用於直接促銷，資料使用者須取得資料當事人明確同意，方可使用其個人資料(即資料當事人選擇同意對方使用其資料)；及 (b) 針對直接促銷活動，設立全港適用的拒收直接促銷電話中央登記冊。 政府亦應立法規定，在人對人電話的直接促銷中過程中，資料使用者有法定責任，向資料當事人或其代表，表明身分和說明如何取得有關的個人資料，否則應屬違法。而且在使用一定年期後 (例如十年後)，資料使用者如欲爲其個人牟利的目的而繼續使用有關的個人資料作直接促銷，則他必須在期滿前，再度取得資料同事人的明確同意。 人權監察認爲，即使政府拒絕在私隱條例上加強規管人對人直接促銷電話，亦應該考慮加強《非應邀電子訊息條例》對人對人直接促銷電話的監管。
A.2：把互聯網規約地址視爲個人資料	人權監察支持有關建議，認爲政府應該加以跟進。人權監察認同應該將 IP 地址視爲個人資料，或應該界定 IP 地址一旦與其他資料一同被披露，將會被視爲個人資料。 雅虎個案引起公眾對應否視互聯網規約地址 (IP 地址) 爲「個人資料」的關注。人權監察注意到，德國數據保護專家及歐盟資料保護小組負責人 Peter Scharr 於 2008 年初就曾於歐盟舉行的網路數據保護聽證會上指出，當可以通過 IP 地址確認用戶的身份時， IP 地址就應被視爲是個人資料。他進一步指出，大部分互聯網使用者都使

[5] 公署修訂建議第 141 頁。

S0157

	用固定的電腦及 IP 地址，而互聯網上出現了大量的 IP 地址查詢網站，互聯網使用者只需要輸入 IP 地址，就可以查出相關的個人或者公司[6]。 諮詢文件聲稱「把 IP 地址本身視爲個人資料，會對資訊科技界業內人士帶來不合理的負擔，兼有嚴重的遵從問題」[7]。人權監察重申，私隱條例的修改應該以爲個人資料私隱提供最大可行的保障爲指導原則，政府不應以技術困難爲理由而不作諮詢，而且私隱專員吳斌在最近的報章專訪中亦表示「若 IP 位址 (地址) 加上某些資料，這種新資料組合，足以證明個人身分，便應受法例管制」[8]。人權監察認爲，將 IP 地址視爲個人資料，及要求業界遵從並非完全不可行，促請政府就此項建議廣泛諮詢公眾，及與業界商討如何爲互聯網使用者提供最大的保障。 另一方面，諮詢文件指出把 IP 地址視爲個人資料，將會衍生出電郵地址、手提電話號碼、車牌號碼等資料爲何不同樣被視爲個人資料。人權監察同意此等資料亦應被視爲個人資料，促請政府加以跟進。
A.3：私隱條例的適用地區	人權監察同意政府指出，有關建議可能令管制個人資料的框架出現漏洞，使香港變成「無效規管個人資料的天堂」[9]，所以人權監察不支持私隱公署這項建議。 另一方面，人權監察注意到行政上訴委員會曾指出，私隱條例第 39(1)(d)的規定「沒有對條例是否在境外適用的問題提供答案」[10]，故此認爲私隱公署及政府當局有必要在這方面加以跟進。此外，人權監察亦希望政府解釋私隱條例第 33 條有關「禁止除在指明情況外將個人資料移轉至香港以外地方」的條文尚未實施的原因及其對條例執行的影響。
(B) 豁免條文	
B.1：有關公眾利益的裁決	人權監察支持有關建議，認爲政府應該加以跟進。 私隱公署指出，多個海外地方例如英國、澳洲及新西蘭等的私隱法例，都有有關「公眾利益」的豁免條文。人權監察支持訂立新條文，訂明公眾利益爲豁免依據，並授權私隱專員就相關資料使用者，包括 whistle-blowers (「揭密者」，即把某些犯法或不符合公眾利益的行爲告知機構或公眾的人) 及人權捍衛者提出的個別公眾利益

[6] Aoife White, "IP Address Are Personal Data, E.U. Regulator Says", The Washington Post, 22 January 2008.
[7] 檢討《個人資料 (私隱) 條例》的諮詢文件 (諮詢文件)，附件 2 第 10 段。
[8] 何素文：「IP 位址未列私隱 吳斌倡立法保障」，明報，2009 年 11 月 9 日。
[9] 諮詢文件附件 2 第 13 段。
[10] 公署修訂建議引述**行政上訴委員會第 16/2007 號**。私隱條例第 39(1)(d)條規定，如所投訴的作爲或行爲不符合任何指明的條件，則專員可拒絕進行或拒絕繼續進行由投訴引發的調查。

	豁免申請，作出裁定及視乎情況附加豁免條件。
B.2：公共領域豁免	人權監察認同諮詢文件指出，「資料存在於公共領域並不等於容許把有關資料用於任何用途」[11]，有關建議可能導致可以在公共領域取得的個人資料被濫用，故此不支持這項建議。
(C) 私隱專員的權力	
C.1：搜查及檢取證據的權力	人權監察支持有關建議，認爲政府應該加以跟進。 人權監察認爲，私隱專員需要的是廣泛的調查權，有否直接的檢控權並非關鍵所在。按照《巴黎原則》[12]，人權保障機構應有廣泛的權力，包括調查侵權的權力，故此應授予私隱專員搜查及檢取證據的調查權力，以有效執行職務（請參考建議 4 的回應）。但爲保障可能受影響人士的權益，私隱專員須先得到裁判官手令授權，才可搜查及檢取證據。 私隱公署特別指出，電訊管理局在《非應邀電子訊息條例》下，亦有類似權力[13]。人權監察認爲相比起發送非應邀電子訊息而言，不少侵犯私隱行爲對受害人的傷害更爲嚴重，私隱專員更應擁有搜查及檢取證據的權力。
C.2：召喚公職人員提供協助	人權監察支持有關建議，認爲政府應該加以跟進。 雖然諮詢文件聲稱「一直以來，私隱專員在執行規管職能時，都得到公職人員提供協助」[14]，但這只是一種善意或慣例的協助應該明文規定可召喚公職人員協助，在制度上，公職人員可以拒絕爲私隱專員提供任何協助而沒有任何後果。人權監察認爲有必要將這種做法制度化，明文規定私隱專員可召喚公職人員提供協助。 人權監察注意到，電訊管理局在《非應邀電子訊息條例》第 42 條下，有「妨礙電訊局長、獲授權人員等」的保障，將無合理辯解而沒有爲電訊局長或獲授權人員的合理要求提供協助，定爲罪行給予的其他協助但同時亦有無合理辯解而沒有給予電訊局長協助罪。而私隱公署亦特別指出，電訊管理局在《非應邀電子訊息條例》下亦獲授權召喚公職人員提供協助[15]。人權監察批評政府厚此薄彼，反對給予私隱專員類似的權力，明顯是雙重標準，歧視私隱專員的做法。
C.3：公開聆訊的權力	人權監察認爲政府應該加以跟進有關建議。

[11] 諮詢文件附件 2 第 19 段。
[12] 《巴黎原則》是 1993 年聯合國大會通過有關國家人權機構的國際標準，並請參考 Commonwealth Secretariat , "National Human Rights Institutions: Best Practice" (London, 2001).
[13] 公署修訂建議第 44 頁。
[14] 諮詢文件附件 2 第 24 段。
[15] 公署修訂建議第 39 頁。

S0157

	人權監察原則上同意聆訊應該公開進行，但亦明白諮詢文件中所指如果所有聆訊都要公開進行，有些市民未必會積極作出投訴[16]。人權監察建議應授權私隱專員在考慮有關個案的所有情況 (包括投訴人提出的要求和公眾利益) 後，決定是否不公開部分或全部聆訊。
C.4：回應專員調查 / 視察報告的時限	人權監察認同諮詢文件指出，要求資料使用者於 14 日內回應的期限「會不合理地過份緊迫」[17]，故此不支持這項建議。

主要修例建議：

敏感個人資料	
建議 1：敏感個人資料	人權監察原則上同意政府的修例建議，加強對處理敏感個人資料的規定。違反敏感個人資料的規定，可沿用現行的民事制裁，並輔以過渡性安排的措施。 人權監察同意將生物辨識資料列爲敏感個人資料，並強調資料當事人的訂明同意，即自願而明確的同意。但人權監察亦注意到資訊科技業界因爲生物辨識資料不會被還原而對此項建議有重大保留，人權監察促請政府多就這項建議諮詢資訊科技業界。 另一方面，人權監察注意到生物辨識資料只是私隱公署建議納入爲「敏感個人資料」的其中一項。諮詢文件強調的國際做法與標準，包括歐盟的《第 95/46/EC 號指令》、英國的《1998 年保障資料法令》及澳洲的《1988 年私隱法令》所規管的個人資料類別，都遠比生物辨識資料爲廣泛。綜合國際做法，私隱公署原本建議新增的「敏感個人資料」定義是包括[18]： - 資料當事人的原屬種族或族裔； - 政治聯繫； - 宗教信仰及聯繫； - 工會成員身分 (根據《職工會條例》(第 332 章) 中的定義； - 身體或精神健康或狀況； - 生物特徵資料；或

[16] 諮詢文件附件 2 第 26 段。
[17] 諮詢文件附件 2 第 29 段。
[18] 公署修訂建議第 4 頁。

	- 性生活。 人權監察認爲上述個人資料，及其他敏感資料如性傾向，亦應該被納入爲「敏感個人資料」以加強對個人資料的保障。政府應該全面考慮私隱公署這項建議，並廣泛地諮詢公眾。
資料保安	
建議 2：規管資料處理者及分判活動	鑑於把個人資料分判或委託給第三者處理的趨勢日益普遍，人權監察支持加強保安措施，以規管交託給代理處理的個人資料。 諮詢文件中提出以直接 (在私隱條例下直接規管資料處理者的活動) 或 / 及間接 (透過資料使用者以合約方式或其他方法間接規管資料處理者) 規管資料處理者。人權監察支持當局兼用兩種規管手法，在各層面保障個人資料。手法資料處理者兩種手法兼用 (應以法例直接監管) 諮詢文件第 4.14 段提出直接規管資料者的三項規定方向。人權監察同意對資料使用者的規管應以該三個方向作爲指導原則，但基於不同行業或機構在處理個人資料時有不同的情況，特別是互聯網及網上服務供應商有可能面對的困難，私隱公署應有權在充分諮詢相關持份者後，向不同類別的資料處理者施加不同責任，以確保有關規定是切實可行之餘，亦能有效保障個人資料。
建議 3：個人資料外洩通報機制	人權監察支持訂立通報機制，以減低當發生資料外洩事件時，受影響人士可能導致的損失。 諮詢文件指出政府已於 2008 年 11 月設立電子個人資料外洩事故通報機制。人權監察建議先爲公營機構訂立強制通報機制，同時向私營機構訂立自願通報機制，並定期就通報機制的運作作出檢討，再調校通報機制。鑑於當個人資料外洩事件發生時，未必容易評估對個別人士的影響，故此人權監察認爲若自願通報機制運作暢順並切實可行，可考慮訂立強制通報機制。 在通報機制的實際操作方面，人權監察認爲資料使用者須於發生事故後五個工作天內通知私隱專員是太長，而以郵遞形式向受影響個別人士通報可能比較慢，因爲一旦發生資料外洩，資料當事人可能會在短時間內受到影響，例如身分被假冒。
私隱專員的執法權力	
建議 4：授予私隱專員刑事調查及檢控權力	人權監察原則上同意授予私隱專員刑事調查及檢控權力，以便私隱專員更有效地執行私隱條例。 私隱專員專責保護私隱，是一人權保障機構，按《巴黎原則》應有廣泛的權力，故應授予刑事調查和檢控權。但私隱專員亦要小心行使此等權力，人權監察認爲現時已有有效制約，律政司司長有權中止或取代任何檢控。

S01157

	而事實上，香港的法律制度容許私人提出檢控，故此即使律政司司長否決私隱專員的檢控，亦可考慮讓私隱專員協助當事人提出私人檢控。至少，在檢控過程中，私隱專員可擔當案件主管的角色。
建議 5：在第 66 條下爲資料當事人提供法律協助	人權監察同意授權私隱專員爲受屈資料當時人提供法律協助，甚至取代當時人提起訴訟。正如諮詢文件指出，私隱專員爲受屈當時人提供法律協助，可以使受屈一方更能評估其民事索償的成功機會，亦不會因費用問題而卻步，亦可以對侵犯個人資料私隱的行爲或做法起更大的阻嚇作用。 人權監察強調，若最終落實是項建議，政府必須確保私隱專員有充足的財政資源，作有關的用途。
建議 6：向受屈的資料當事人判給補償	人權監察原則上同意法改會的意見，有關建議會將執法和處罰職能一併歸於單一機構，做法並不可取，故此對是項建議有所保留。
罪行及制裁	
建議 7：把違反保障資料原則訂爲罪行	人權監察擔心將違反資料原則本身定爲罪行，會令市民誤墮法網。私隱公署亦提出相似的擔憂，並指出落實這項建議需要考慮 (a) 是否需要強加刑事制裁以控制有關行爲或做法，及 (b) 是否有構成罪行的意圖的因素存在[19]。 諮詢文件指出「較爲恰當的做法是把某些嚴重的違規行爲或做法，訂爲刑事罪行」，人權監察同意這是一個較爲可行的方法，在避免市民誤墮法網之餘，亦可以加強對私隱的保障。但人權監察要指出，「嚴重的違規行爲或做法」的定義必須要明確，而且只能在一些合理而明確的情況，例如故意違反私隱條例或意圖圖利，才可予以考慮刑事規管。人權監察建議私隱專員可在研究過往案例的基礎上整理出應予刑事規管的情況，再徵詢公眾意見。
建議 8：在未經授權下取得、披露和出售個人資料	人權監察認爲可考慮政府的建議，把罪行的範圍收窄，透過選定某些嚴重違反保障資料原則的行爲或做法訂爲罪行，以遏止公然侵犯私隱的行爲。 但人權監察認爲，「嚴重」及「惡意用途」難下清晰的定義，其法律影響亦不明，故暫時只同意將諮詢文件第 6.06(a) 段所述意圖圖利的行爲，施以刑事化。 (私隱公署認爲有漏洞，指曾有案例，一名稅務主任記錄了 13400 名人士資料作日後個人用途，但因爲該稅務主任未有任何財務利益，故此無罪釋放) 就更大地擴大刑事化範圍，人權監察認爲需要謹慎研究考慮。故此對於會否支持引入《英國保障資料法令》第 55 條及其抗辯條文的類似刑法，人權監察認爲仍有待進一步了解有關法律的實施經驗和可能的影響，才能決

[19] 私隱公署就檢討私隱條例的文件，第 7.3 段。

S01157

	定。人權監察注意到私隱公署有基於英國的經驗，就政府的建議作初步回應，故此建議私隱公署廣泛地整理英國執行相關法例的經驗，再諮詢公眾。
建議 9：就同一事實重複違反保障資料原則	人權監察同意將故意重複執行通知所涉及的行爲或做法定爲罪行，以備不時之需。 在目前的私隱條例下，未經授權下取得、披露和出售個人資料，以及違反保障資料原則，均沒有廣泛地訂爲刑事罪行，把就同一事實重複違反保障資料原則訂爲罪行，更顯得重要。
建議 10：就嚴重違反保障資料原則處以罰款	人權監察認爲，有關建議能夠加強條例的阻嚇力。儘管有關建議會將將執法和處罰職能一併歸於單一機構，但諮詢文件第 6.19 段亦舉出司法機構以外的機構獲賦法定權力施加罰款的例子。 人權監察原則上同意是項建議，但強調要就「嚴重違反」附有清楚的定義，建議政府及私隱公署參考英國的做法，在條例的附表上表明罰款的上限、私隱專員需清楚述明行使判處罰款權力的情況，及設立上訴機制。
建議 11：重複違反執行通知	人權監察同意向重複違反私隱公署執行通知的資料使用者處以更重的懲罰 (現時違反執行通知的刑罰爲第 5 級罰款 (最高可達 50,000 元) 及監禁兩年；如持續犯罪，每日罰款 1,000 元)，以加強阻嚇作用。
建議 12：提高在直接促銷中不當使用個人資料的罰則	現時私隱條例對直接促銷中不當使用個人資料的最高刑罰爲 10,000 元，人權監察認同有關罰難起阻嚇作用，故此同意提高相關罪行的罰則。 人權監察認爲政府應立法規定，在直接促銷的過程中，資料使用者有法定責任，向資料當事人或其代表，表明身分和說明如何取得有關的個人資料，否則應屬違法，並促請政府及私隱公署加強宣傳，令市民知道他們有權要求資料使用者，停止把其個人資料用於直接促銷活動。

其他建議：徵詢意見

(A) 資料當事人的權利	
建議 13：由第三者給予訂同意更改個人資料用途	人權監察原則上同意由諮詢文件附件二第 5 段所列的人士，作爲「有關人士」代弱勢資料當事人，如未成年人或精神上無行爲能力的人等，提出披露資料以至修改、刪除資料等要求或指示。人權監察注意到，就這項建議政府的建議是「更改個人資料用途」，而私隱公署原本向政府建議的，是「使用個人資料於對資料當事人明顯有利的目的上」。人權監察希望政府釐清兩者的分別及優劣之處，讓公眾參考。 另一方面，有關法例必須清楚訂明「弱勢資料當事人的最大利益」的原則，以及註明在考慮他的最大利益時，

S01157

	資料使用者有責任在合理地衡量該當事人的年齡、心智及理解能力等因素的情況下，恰當地取得（除不切實可行者外）和考慮該資料當事人的意見[20]，才作出和執行適當的決定。該「有關人士」亦應該有權就資料使用者拒絕他如此提出的要求或指示，向私隱專員上訴。 人權監察擔心若將資料當事人的親戚或託兒人員納入爲「有關人士」，會令弱勢資料當事人私隱外泄的機會提高，或其他利益受損。若負有父母親或監護責任的人不知所蹤，或未有妥善照顧弱勢資料當事人，因而需要受託於其親戚或託兒所等，政府應設立新機制，讓私隱專員在考慮受託的親戚或託兒所甚或任何人的意見後，提出任何恰當的資料處理指示。
建議 14：父母親查閱未成年人士個人資料的權利	人權監察原則上同意基於兒童最大利益的原則， 爲尊重和保護兒童私隱權利，在諮詢文件附件二第 8 段所述的特殊情況下，資料使用者有權和有責任拒絕「有關人士」提出查閱資料的要求。 基於法律必須有確定性，有關法例必須清楚訂明兒童最大利益的原則，並將某些情況列爲特殊情況的原則及因素，協助資料使用者在衡量有否合理理由拒絕父母的查閱要求時，有所遵從。諮詢文件附件二第 8 段所述的三個特殊情況，都有合理理由拒絕父母親的查閱要求，人權監察特別強調聯合國兒童權利公約第 12 條 (1) 所提出，有主見能力的兒童所發表的意見應獲得適當尊重，故此附件二第 8 段所述的第三項情況，即「子女向資料使用者表明，不同意該使用者向其父母親透露其個人資料」，是拒絕父母親的查閱要求的合理拒絕理由。 法例亦可訂明私隱專員有權就父母親的查閱要求，向資料使用者提供意見，並設立上訴機制，讓被拒的「有關人士」向私隱專員上訴。
建議 15：查閱受爭議的個人資料	人權監察原則上同意在要求資料一方被行政上訴委員會或法庭裁定勝訴前，不得純粹因訴訟的理由，強制資料使用者及有關人士或機構，直接或間接向要求資料者等人，披露案件所涉的個人資料；但有關修例不應完全禁止其他披露，以保留應有的彈性，容許基於其他合理理由的披露。
(B) 資料使用者的權利及義務	
建議 16：爲遵從其他條例而拒絕依從查閱資料要求	人權監察原則上同意這項建議，訂明資料使用者若根據任何條例，有義務或有權不披露個人資料，以解決當資料使用者收到查閱資料要求，而同時受到保密法定責任束縛的困局。 另一方面，人權監察擔憂現行法例的保密條文可能未能保障包括個人資料的合理披露，例如《官方機密條例》未有以公眾利益作爲披露的抗辯理由，令修例建議一旦落實，可能會阻止一些個人資料的合理披露，故人權監

[20] 聯合國兒童權利公約第 12 條 (1) 指：「締約國應確保有主見能力的兒童有權對影響到其本人的一切事項自由發表自己的意見，對兒童的意見應按照其年齡和成熟程度給以適當看待。」聯合國殘疾人權利公約的原則，其中一項包括「尊重固有尊嚴和個人自主，包括自己作出的選擇，以及個人的自立」。

S01157

	察建議政府同時著手廣泛研究《官方機密條例》及其他法例的保密條文是否有修改的必要。
建議 17：刪除個人資料	人權監察原則上同意修例，訂明當資料使用者可以證明他已採取所有合理可行的步驟，刪除不再爲使用目的而有需要保留的個人資料時，使用者可視作已依從有關規定。 但有關條文亦必須明確阻止藉此而作的規避，例如特意改用微縮副本，以保存屬過時的個人資料。
建議 18：處理查閱資料要求所收取的費用	人權監察同意有關建議，規定資料使用者依從查閱資料要求所徵收的費用，不得高於私隱條例內收費附表列出的訂明最高收費；私隱公署有就依從查閱資料要求的費用列出詳細建議[21]，人權監察大致認同。
建議 19：在 40 日內以書面回覆查閱資料要求	人權監察同意修例建議，規定資料使用者如無持有要求查閱的個人資料，須以書面回覆要求者 (查閱的資料涉及個人刑事犯罪紀錄而警方並未持有該資料則屬例外) ，及規定資料使用者如無持有資料當事人的個人資料，因而無法應要求提供有關資料的複本，須在 40 日內回覆要求者，不論有關回覆是以書面或口頭方式作出。
(C) 私隱專員的執法權力	
建議 20：在何種情況下發出執行通知	人權監察同意這項建議，授予私隱專員酌情權，在以下任何情況：(a) 資料使用者正違反私隱條例下的規定；(b) 違反行爲將持續或會重複發生；或 (c) 違反行爲已對或相當可能對資料當事人造成損害或困擾，向資料使用者發出執行通知。 但人權監察注意到，私隱專員的原本建議中，除上述三項情況外，還有一項「專員認爲適合作出考慮的其他事宜」的情況，並詳細列出公署希望能夠作考慮的其他情況[22]。人權監察初步同意私隱公署的建議，促請政府就此項目再作公眾諮詢。
建議 21：澄清在執行通知中指示糾正違規行爲的權力	人權監察同意這項建議，訂明私隱專員有權在執行通知內，指令資料使用者停止作出某項作爲或行爲。
建議 22：取消中止調查的時限	人權監察同意這項建議，刪除有關中止調查決定須在指定時間 (45 日) 內作出的規定，亦同意政府的相關建議，保留私隱專員在決定不繼續調查時，須向投訴人發出書面通知，述明他所作決定的理由的規定，及投訴人就私隱專員不進行調查或中止調查的決定提出上訴的權利。
建議 23：拒絕調查的新增理據	人權監察只同意在條文內納入諮詢文件附件一第 48(a) 段，即「投訴的主因與個人資料私隱無關」的特定理據，作爲拒絕繼續進行調查的依據，並建議將當中的「主因」改爲「性質」。人權監察認爲，即使在諮詢文件附件一第 48(b) 及 (c) 段所指的情況下，私隱公署仍有其展開調查的價值，因爲另一規管機構的法定職能與私隱公署不同，其調查亦未必與私隱有直接關係，而即使所涉及的個人資料已在或相當可能在法律程序或研訊的某

[21] 公署修訂建議第 77 頁。

[22] 私隱公署就檢討私隱條例的文件，第 11.3 段。

	個階段使用，私隱公署亦可就使用前的不合理或不正當處理個人資料的行爲或作爲作出調查，所以不建議將附件一第 48(b) 及 (c) 段所指的情況納入爲拒絕理據。
(D) 新增豁免條文	
建議 24：商業併購過程中個人資料的轉移	人權監察原則上同意是項建議，但人權監察亦建議附件一第 52 段的 (a) 項條件須注明若所提供服務應不低於原資料使用者所提供的服務。另外若資料轉移後組成的機構或業務承讓方有需要保存該等資料，要先得私隱專員的批准。
建議 25：基於健康理由提供身分和所在地資料	人權監察同意是項建議，擴闊私隱條例第 59 條的適用範圍，涵蓋有關資料當事人所在地點的個人資料。
建議 26：在緊急情況下處理個人資料	人權監察同意這項原則，但認爲須明確及狹窄地界定「意外」，否則應只限於「危及生命的情況」。
建議 27：爲了履行監護責任和家長照顧責任而把未成年人的個人資料轉移	人權監察對此項建議有保留，認爲有關建議未有考慮兒童的私隱權益，亦未必符合「兒童最大利益」的要求。人權監察擔心，若此項建議獲得接納，可能會有家長濫用機制，向資料使用者（特別是社工）施壓，要求他們提供其子女的個人資料，這將會是對社工，或其他專業保密原則的重大挑戰。 若要採納此建議，人權監察認爲應加入特定條件加以限制，包括兒童最大利益原則，並可考慮引入機制，由申請披露資料的人向私隱專員申請，並先發通知予該未成年人，問其是否反對，再由私隱專員決定是否容許披露。 諮詢文件附件一第 65 段指出，目前警方在有真憑實據的情況下，已可引用私隱條例有關防止罪案的第 58 條，取得豁免，轉移資料。有真憑實據相信未成年人可能會干犯罪行，或會成爲屢犯者，而其父母或監護人若得悉此事，會有阻防止未成年人干犯罪行，則警方便可引用，把該等資料轉移給未成年人的父母或監護人。」人權監察指出，諮詢文件的建議放寬現行規定，不需要「真憑實據」及「未成年人的同意」亦可披露資料，單憑執法人員主觀判斷「是否合乎未成年人的最大利益」，有可能助長執法人員濫權的情況。若要採納此建議，必須要有一套機制，有效防止執法人員濫權。

私隱專員的雜項建議修訂

(A) 私隱專員的法定權力及職能	
建議 28：免卻私隱專員將調查結果通知已撤回投訴的人士的責任	人權監察並不完全同意這項建議。人權監察認爲，即使私隱專員可因此免卻相關的法律責任，如行政上訴程序等，但仍應盡量通知投訴人；另一方面，在投訴人撤回投訴而該投訴尚在調查或整理中時，其實並沒有調查結果可以通知該投訴人，若要在此情況下繼續調查或整理調查結果，卻可能不必要地浪費私隱公署的資源。

S0157

	人權監察建議，若投訴人撤回投訴而該投訴尚在調查或整理中，私隱專員可免卻將調查結果通知投訴人士的責任；但若該投訴已經完成調查並已整理好，人權監察認爲私隱公署應該告知投訴人該投訴的調查結果。
建議 29：私隱專員爲了履行職能而披露資訊	人權監察同意這項建議，讓私隱專員及其屬下人員可在恰當執行私隱專員的職能或行使其權力時，按合理需要披露資訊。
建議 30：私隱專員及他的訂明人員個人免受起訴的保障	人權監察同意這項建議，讓私隱專員及其屬下人員不會因行使私隱條例訂明的權力或執行訂明的職能，在免受起訴外，使他們亦無須負上個人責任。 但人權監察注意到，私隱公署建議的免責豁免是包括「根據條例執行或其意是執行職能及權力時以真誠作出的作爲或不作爲」[23]。私隱公署建議的豁免範圍似乎比此刻政府建議的爲闊，人權監察同意私隱公署的意見，並認爲政府應該加以跟進。
建議 31：授權私隱專員就教育或推廣活動 / 服務收取費用	私隱公署原本的建議除「進行教育、推廣或其他活動或服務」外，私隱專員還有權就「提供小冊子、書刊或其他印刷品」及「專員認爲在履行其職能方面有需要或有利的其他服務或活動」兩方面徵收合理費用[24]。人權監察認爲，私隱專員只應有權就同一時間大量提供印刷品予同一單位徵收費用，而「專員認爲在履行其職能方面有需要或有利的其他服務或活動」的定義亦廣泛。 人權監察認爲只授權私隱專員就教育或推廣活動／服務收取費用是合理做法，但亦認爲私隱專員應有減免該等收費的酌情權。
建議 32：授權私隱專員獲取資料以核實資料使用者申報表	人權監察同意授權私隱專員，獲取資料以核實資料使用者申報表的資料真確無誤。
(B) 新增豁免條文	
建議 33：因爲法例規定、准許，或與任何法律程序有關而使用個人資料	人權監察同意有關建議，豁免因爲法例規定、准許或法庭下令，或與任何在香港的法律程序有關或因確立、行使或維護法律權益而使用個人資料，免受保障資料第 **3** 原則規管。
建議 34：爲保留歷史檔案轉移資料	人權監察同意新增豁免條文，容許把有歷史、研究、教育或文化價值的個人資料的資訊轉交歷史檔案館作存檔保存之用，並毋需受保障資料第 3 原則規限；人權監察並建議在上述範疇加上「康樂」。
建議 35：以避免「導致自	人權監察原則上同意這項建議，新增豁免條文，讓資料使用者以依從查閱資料要求可導致本身入罪爲由，無需

[23] 公署修訂建議第 47 頁。
[24] 公署修訂建議第 27 頁。

S01157

己入罪」拒絕遵從查閱資料要求	依從有關要求。 但爲以有資料使用者濫用豁免，人權監察建議只有當私隱專員確認屬實下，有關的資料若依從查閱要求而披露，將可導致資料使用者入罪，才可以無需依從有關查閱要求。(但私隱專員能有足夠能力衡量有關資料是否會導致入罪？即資料使用者要先將可導致自己入罪的資料交予私隱公署？當中的保密條款如何？ → 英國無類似防止濫用機制)
(C) 澄清條例的適用情況	
建議 36：第 58 條中「罪行」的定義	人權監察不完全同意政府這項建議，只同意將「罪行」的定義訂爲香港法律訂明的罪行。 人權監察不同意政府建議將「罪行」的定義包括香港境外地方的法律訂明的罪行及犯罪行爲，而這些地方在司法或執法工作上與香港有合作安排。人權監察認爲這定義可能會導致一些良心犯或正被以言入罪的人，因而被定罪，故此建議採納私隱公署的建議，將「罪行」定爲包括《刑事事宜相互法律協助條例》(第 525 章)適用的罪行[25]。該條例第 5(1)(g) 條訂明：「如律政司司長認爲有以下情況，對於由香港以外某地方提出的要求根據本條例提供協助的請求，須予以拒絕：該項請求關乎某作爲或不作爲，而假使該作爲或不作爲在香港發生，將不會構成香港罪行。」
建議 37：擴展 「有關人士」的定義	人權監察同意將「有關人士」的定義，擴展至包括按《精神健康條例》(第 136 章)委任的合法監護人，以代表資料當事人向私隱專員作出投訴，以及提出查閱和更改資料的要求。
建議 38：從「直接促銷」定義中剔除社會服務	人權監察同意這項建議，從「直接促銷」的定義中，剔除社工向有需要人士提供的社會服務及設施。
建議 39：豁免法庭或司法人員持有的個人資料	人權監察同意這項建議，新增條文令條例不適用於法庭或司法人員因執行司法職能而持有的個人資料。
建議 40：延長提交資料以檢控罪行的時限	人權監察同意這項建議，訂明提交資料以檢控私隱條例下的罪行，需在犯罪行爲發生日起計兩年內提出。
建議 41：防止遺失個人資料的責任	人權監察同意這項建議，修訂附表 1 保障資料第 4 原則，清楚訂明資料使用者必須採取所有切實可行的步驟，以防遺失個人資料。
(D) 澄清其他運作事宜	
建議 42：私隱專員同時送達調查結果及執行通知	人權監察同意這項建議，容許私隱專員把調查結果送達相關各方的時候，同時送達執行通知。
建議 43：查閱或改正資料	人權監察同意這項建議，准許資料使用者提供查閱資料要求或改正資料要求的受理人員的職稱或姓名。

[25] 公署修訂建議第 10 頁。

S01157

要求的受理人員的資料	

參考文件：

檢討《個人資料 (私隱) 條例》的諮詢文件 (http://www.cmab.gov.hk/doc/issues/PDPO_Consultation_Document_tc.pdf)

個人資料私隱專員公署就檢討《個人資料(私隱)條例》的資料文件及其附件（公署內部的條例檢討工作小組作出的修訂建議）
(http://www.pcpd.org.hk/chinese/review_ordinance/files/Odnreview_Information_Paper_c.pdf)



30/11/2009 23:46

To "pdpo_consultation@cmab.gov.hk" <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject <<個人資料(私隱)條例>>檢討回應

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

致：私隱專員工處

本人就著<<個人資料(私隱)條例>>檢討有以下回應：

有關第三章: 敏感個人資料對指模數據的理解，認爲所有指模數據都是不能更改獨一無二的數據(如影像)已跟今天科技發展完全脫節，現今不少技術只是利用指模紋理排列加上各自的坐標定意而進行選擇性編碼，此等數據跟真正的不能更改指模影像數據经已是兩回事。本人認爲如私隱專員未能理解事實的全部，不應於此時加强規管，否則會對香港社會造成深遠的影響如下：

- 使用指紋認証系統不但能杜絕代人「代打卡」欺騙公司的情況，還能有效地減少成本，消費者亦能從中得益，合乎經濟利益。外國亦有研究顯示，使用指紋認証系統的公司能每年節省2.2%的薪金支付，而省回的營運成本可以直接令消費者得益。若不用指紋考勤機，令員工有機可乘找人代「代打卡」，令到公司的營運成本增加，最終只會將成本轉嫁消費者身上，令產品價格提高。

- 今天香港社會應用生物科技已遠遠落後於其他國家，加強規管只會令情況更差，削弱香港的競爭力。

- 因規管令本來已小的市場變得更小，握殺業介，國際性生物科技公司赤遠離香港，令香港長期處於落後階段。

Elvis Law
FingerTec Worldwide Ltd.
Founder GlobalTech Ltd.

S0159



To pdpo_consultation@cmab.gov.hk
cc
bcc
30/11/2009 20:44 Subject 提供意見

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

本人曾在一間公司入職前，公司要求驗身，在旨定的驗身公司要填寫一份個人資料表時，內容有一欄要求填寫家屬或直接親屬有的病歷，還要要求簽名同意將資料交給公司，我只申請初級文職，只報個人健康資料已足夠，無必要加其它人的資料，因對有家人有敏感性疾病者(例如：精神病者或癌症病者.....等)或長期性病患者的家庭很不公平和感到難受和受到歧視，應該阻止，就算事後入職了都難受。

另一件，另一公司，本人因年齡在40左右時，曾在一間公司工作時，被一位約20歲的上級知到的我年歲時，竟向其它同事靜靜透露我的年歲，經常拿來取笑，直接影響我的心理健康，她太無度得，應該阻止此行爲。

兩件事直接影響我離開公司後都難忘記，雖然我是成人，但都難控制忘記。

望有心人幫助改變風氣

(署名來函)

30-11-2009

(來信人要求不具名公開意見)

S0160

Professional Information Security Association

27 Nov 2009

Team 4, Constitutional and Mainland Affairs Bureau

Room 364, East Wing,

Central Government Offices,

Lower Albert Road

Dear Sir/Madam:

Ref: PISA position on Review of the Personal Data (Privacy) Ordinance Consultation

This document states the position of the Professional Information Security Association (PISA) of Hong Kong in relation to the "Consultation Document on Review of the Personal Data (Privacy) Ordinance", August 2009, Constitutional and Mainland Affairs Bureau.

PISA is an association of Information Security professionals in Hong Kong. Information Security and Personal Data Privacy are overlapping areas of concern. For example, what data to collect, when to destroy data, the rights of data subjects to know what data is held and to correct it, are Personal Data Privacy concerns but not directly Information Security concerns. Conversely, Information Security covers both corporate data and personal data, whereas Personal Data Privacy covers just personal data. The main area of overlap is the protection of personal data, which includes access controls to protect both confidentiality and integrity.

The formal positions of PISA are as follows.

1. PISA believes the current PDPO should be reviewed in light of the changing trends in uses of personal data. The environment continues to evolve, so

privacy law and operation of the Privacy Commissioner's office should be reviewed from time to time. For example, the recent increased prevalence of social networking and Cloud Computing has significant impacts on personal data privacy.

2. PISA has no formal position on many of the proposals in the Consultation Document, as many of the proposals are not related specifically to Information Security. However, PISA members are generally interested in the issues and many have strong personal views on the specific proposals.
3. PISA agrees that that there needs to be a balance between business interests and personal interests. However, the unbalanced power relationship between individuals and large corporations must be kept in mind. It is the role of Government to legislate and regulate to protect consumers and the public from exploitation by business.
4. PISA is concerned that the issue of trans-border data flows has not been addressed in this review, despite assurances from the Government that this issue is being actively considered. PISA would like to see an open public consultation on trans-border data flow privacy, including the pros and cons of enacting Section 33 of the Ordinance, and consideration of enabling "Safe Harbour" arrangements, similar to the USA Department of Commerce certification program, as an alternative.
5. Proposal 1 – Sensitive Personal Data

   PISA is of the view that sensitive personal data should be subject to more stringent regulation.

6. Proposal 2 – Regulation of data processors

   PISA is of the view that Data Processors should be specifically regulated rather than leaving this to contractual arrangements. This will help ensure consistency and help ensure that remedies are sufficient. This is particularly important where the data processor is a larger more powerful organisation than the data-owner client, where the client would have difficulty negotiating strong enough contractual arrangements.

7. Proposal 3 – Notification of data leakage

   PISA is of the view that notification of data leakage should be mandatory. Breach notification is important to help enable evidence-based information security approaches, which focus scarce money and effort in proportion to the real risks. Moreover, The affected party has no cost-effective means to

S0161

法 定 代 表 律 師 辦 事 處
OFFICIAL SOLICITOR'S OFFICE

本函檔號 Our Ref.

By Fax

來函檔號 Your Ref. CMAB/CR/7/22/40 Pt. 7

電 話 Telephone

30 November 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Team 4
Government Secretariat
Lower Albert Road
Hong Kong

Attn: Miss Joanna C. H. Choi

Dear Sir,

Re: **Public Consultation on the**
Review of the Personal Data (Privacy) Ordinance ("PDPO")

We thank you for your letter of 28 August 2009 enclosing the English and Chinese versions of the above Consultation Document.

We have considered the Consultation Document. So far as the Official Solicitor is concerned, Proposal nos.13, 14, 27, 33, 37 are relevant. We set out below our views on these proposals for your consideration.

Proposal 13

At present, there is no provision in the PDPO to permit a person to give consent on behalf of a data subject to the change of the use of the latter's personal data. Since mentally incapacitated persons ("MIP") and minors may not possess the capacity to give the prescribed consent, to safeguard their interest, we welcome the proposal to devise a system which empowers a "specified third party" to give consent to the change of use of personal data of such data subjects when it is in their best interest to do so.

We support the proposal that the "specified third party" will be allowed to give consent on condition that:
(a) the data subject is incapable of giving prescribed consent; and
(b) the proposed use of the personal data involves a clear benefit to the data subject.

As for the definition of "specified third party", the option to allow a "relevant person" of the data subject as defined in Section 2(1) of the PDPO to give prescribed consent on behalf of a data subject is supported. However, we note the concern that allowing only the "relevant person" to give prescribed consent to the change of use may

pose difficulties or prolong the process for the data subject concerned to access essential services. We suggest that, in cases where no "relevant person" is available to give the prescribed consent (e.g. no person has been appointed by a court to manage the affairs of a MIP, and no guardian has been appointed (assuming that Proposal No.37 is adopted), or where the person having parental responsibility for the minor is untraceable), consideration may be given to allowing a third party, such as those having primary care of the MIPs or minors to give the prescribed consent.

Proposal 14

To strike a balance between respecting parents' role in taking care of their children and respecting children's privacy right, we support that new provisions should be introduced to permit a data user to refuse a data access request made by a "relevant person" on behalf of a minor if the data user has reasonable grounds to believe that compliance with the request would not be in the best interests of the minor.

Proposal 27

The proposal to provide an exemption to allow data users to transfer personal data of a minor that are relevant to parental care and guardianship to the parents or guardian of the minor is supported, on condition that the transfer is absolutely necessary for the best interests of the minor. However, it should be stressed that a balance has to be struck on the need to protect the well-being of minors at risk as against protection of their personal data privacy and any exemption to be granted has to be narrowly defined.

Proposal 33

We support the proposal to create an exemption from DPP3 for use of personal data required or authorized by or under law, by court orders, or related to any legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights.

Proposal 37

The proposal to expand the definition of "relevant person" under section 2 to include the guardians of data subjects with mental incapacity, who are appointed under Sections 44A, 59O, 59Q of the MHO is supported.

Yours faithfully,

(Signed)

(Ms. Sherman Cheung)
for Official Solicitor

SC/gh

香港醫學會
The Hong Kong Medical Association

S0162

Via Fax & Mail

30 November 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong

Dear Sir,

Response on the Consultation Document on Review of the Personal Data (Privacy) Ordinance

Thank you for your letter of 28 August 2009 inviting us to express our views on Review of the Personal Data (Privacy) Ordinance. Our views are as follows:

1. ***Proposal No. 1: Sensitive Personal Data***

Sensitive personal data include racial or ethnic origin, political opinion, religious or philosophical beliefs, membership of trade union, health condition, sexual life as well as biometric data such as iris characteristics, hand contour reading and fingerprints which are unique personal identifiers should be subjected to more stringent regulation, given the gravity of harm that may be inflicted upon the data subject in the event of data leakage.

The suggested regulatory regime and sanctions as proposed in 3.09 to 3.12 of the document are appropriate.

However, the suggestion to apply the new requirements only to sensitive personal data collected after the relevant legislative provision comes into force ("grandfathering") is undesirable. We would favour a transitional period following the enactment of the new provision.

2. ***Proposal No 2: Regulation of Data Processors and Sub-contracting Activities***

We support that a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties.

The activities of a data processor should be directly regulated under the PDPO instead of indirectly regulated through the data user by contractual or other means. Otherwise

香港醫學會
The Hong Kong Medical Association

S0162

the data user may be held fully liable under Section 65(2) of the PDPO for the wrongdoings of data processors and also sub-contractors with whom the data user has no direct contractual relations.

As to whether different categories of data processors should be subjected to different obligations, we believe that they all should be subjected to the same principles of regulations as provided in Section 4.14 of the Consultation Document. Neverthe less, we agree that in this fast-evolving world of Internet-related business, it is appropriate for them to adopt a privacy policy that is appropriate to their business and which is acceptable to their customers.

3. ***Proposal No. 3: Personal Data Security Breach Notification***

We do not support a voluntary privacy breach notification system in Hong Kong. It should be made mandatory just like in the US and the EC. The data user has the duty to notify individuals of certain defined security breaches of personal information, especially the sensitive personal data.

In notifying the individuals concerned, the notice shall include the information as listed in Section 4.39 of the Consultation Document.

4. ***Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD***

We agree that there is no strong case to give the PCPD the power to investigate into and prosecute criminal offence cases. The existing arrangement of referring cases to the Police for investigation and prosecution has been working smoothly.

5. ***Proposal No. 5: Legal Assistance to Data Subjects under Section 66***

We support to empower the PCPD to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under Section 66 of the PDPO, along the lines of the EOC model.

6. ***Proposal No. 6: Award Compensation to Aggrieved Data Subjects***

We concur with the opinion of the LRC that conferring power on a data protecting authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions. The PCPD's role should be limited to determining whether there has been a breach of the principles. It would be for a court to determine the appropriate amount of compensation payable.

7. ***Proposal No. 7: Making Contravention of a Data Protection Principle an Offence***

We concur with the view that DPPs are couched in generic terms and can be subject to a wide range of interpretations. To make contravention of a DPP an offence would

會 學 醫 港 香
The Hong Kong Medical Association

S0162

have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability.

8. ***Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data***

We support that a person who discloses for profit or malicious purposes personal data which he obtained from a data user without the latter's consent should be subject to sanction.

We also agree that there should be some defense provisions such as that listed out in Section 6.08 of the Consultation Document.

The appropriate penalty should not be less than contravening the enforcement notice, i.e. a fine at Level 5 (up to $50,000) and imprisonment for 2 years.

9. ***Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts***

Despite the fact that since the enactment of the PDPO, the PCPD has not come across any such case, it doesn't mean that it will not happen in the future. We still support to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice.

We agreed that the penalty level for the offence should be more than non-compliance with an enforcement notice.

10. ***Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles***

We do not think it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs because it is not common for non-judicial bodies to have the statutory power to impose monetary penalties. Moreover, we think the argument on Proposal No. 7 above also applies here.

11. ***Proposal No.11: Repeated Non-compliance with Enforcement Notice***

We agree that heavier penalty should be imposed for a second or subsequent conviction of Section 64(7).

We think imprisonment terms should be considered.

12. ***Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing***

We support that the penalty for misuse of personal data in direct marketing should be

會 學 醫 港 香
The Hong Kong Medical Association

S0162

raised.

We think imprisonment terms should be considered.

13. ***Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data***

We agree that the definition of the "third party" in this case should be built on the existing framework of the PDPO to mean:

(a) where the individual is a minor, a person who has parental responsibility for the minor;

(b) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs.

14. ***Proposal No. 14: Parent's Right to Access Personal Data of Minors***

We support that new provisions should be introduced to permit a data user to refuse a data access request made by a "relevant person" on behalf of a minor in order to protect the interests of minors taking into account the need for parents to exercise their rights and responsibilities over their children for the proper care of them

One possible option is to allow a data user to refuse to comply with a data access request made by a "relevant person" on behalf of a minor if the data user has reasonable ground to believe that compliance with the request would not be in the best interest of the minor.

15. ***Proposal No. 15: Access to Personal Data in Dispute***

We agree that, where the lawfulness of a refusal to comply with a data access request is in dispute before the Administrative Appeals Board ("AAB"), a court or a magistrate, the relevant personal data should not be disclosed to the data requestor and other parties bound by the decision of the AAB, the court or magistrate, whether by discovery or otherwise, pending a determination in favour of the requestor.

16. ***Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation***

We support the provision of a new ground for a data user to refuse to comply with a data access request under Section 20(3) of the PDPO, where the data user is obliged or entitled under any other ordinances not to disclose the personal data.

17. ***Proposal No. 17: Erasure of Personal Data***

According to Section 26 of the PDPO, a data user shall erase personal data held by it

香港醫學會
The Hong Kong Medical Association

S0162

where the data are no longer required for the purpose. We support to amend the PDPO so that the provisions concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use.

18. ***Proposal No. 18: Fee Charging for Handling Data Access Requests***

We support that the data user should be required not to charge fees for complying with a data access request in excess of the prescribed maximum as set out in a fee schedule in the PDPO.

In setting the prescribed maximum, the parameters to consider should include labour costs and actual out-of pocket expenses involved in locating, retrieving and reproducing the requested personal data.

19. ***Proposal No. 19: Response to Data Access Requests in Writing and With 40 days***

We agree that a data user should be required to inform a requestor in writing if he does not hold the requested personal data.

This should be done within 40 days of the request.

20. ***Proposal No. 20: Circumstances for Issue of an Enforcement Notice***

We support to allow discretion for the PCPD to serve an enforcement notice when the contravention has caused or is likely to cause damage or distress to the data subject.

21. ***Proposal No. 21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice***

We support to specify in Section 50(1) of the PDPO that the PCPD has the power to direct the relevant data user in an enforcement notice to desist from doing an act or engaging in a practice.

22. ***Proposal No. 22: Removing the Time Limit to Discontinue an Investigation***

We support to remove the time limit impose under Section 39(3) of the PDPO with regard to a decision to discontinue an investigation but to retain the existing requirement that the PCPD should notify a complainant in writing his decision not to continue investigation and the reasons for the decision.

23. ***Proposal No. 23: Additional Grounds for Refusing to Investigate***

We support to include the grounds as listed out in paragraph 48 of Annex I of the Consultation Document for the PCPD to refuse to carry out or continue investigation under Section 39(2) of the PDPO.

香港醫學會
The Hong Kong Medical Association

S0162

24. ***Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition***

We supported that an exemption from DPP3 should be provided for the transfer or disclosure of personal data in intended merger, acquisition or transfer of business subject to the condition that the resultant organization will offer substantially similar service as the original data user. We also consider the option set out in paragraph 52 of Annex I in the Consultation Document is appropriate

25. ***Proposal No. 25: Provision of Identity and Location Data on Health Grounds***

We support to amend Section 59 of the PDPO to broaden the scope of application of exemption to cover personal data relating to the identity and location of the data subject on health grounds as in rescue missions.

26. ***Proposal No. 26: Handling Personal Data in Emergency Situations***

We agree that specific exemption from DPP1(3) and DPP 3 of the PDPO should be granted in the handling of accidents or other life-threatening situations by law enforcement agencies ("LEAs") and rescue and relief agencies.

27. ***Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship***

We agree that an exemption from DPP3 should be provided to permit transfer of personal data of minors to their parents or guardians to enhance the protection of vulnerable minors and those at risk so that parents and guardians can properly discharge their responsibility on proper care and guardianship.

However, this exemption has to be narrowly defined, such as restricting the disclosure to minor "at risk" cases, and on condition that the transfer is in the best interest of the minor.

Yours sincerely,

(Signed)

Dr. TSE Hung Hing
President

THH/yl
g:\govt\C&MAB\20091130_PDPOreview.doc

S0163

The DTC Association

(The Hong Kong Association of Restricted Licence Banks and Deposit-taking Companies)

存款公司公會（香港有限制牌照銀行及接受存款公司公會）

Your Ref.: CMAB/CR/7/22/40 Pt.7

30th November, 2009 (Mon)

Miss Joanna C. H.. Choi,
for Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong
(Fax: 2523 0565; Page Faxed: 1)

Dear Miss Choi,

Public Consultation on
the Review of the Personal Data (Privacy) Ordinance

Dear Miss Choi,

Thank you for your letter of Friday the 28th of August, 2009 consulting our Association members over the captioned subject.

We would like to let you know that our members have not raised any issues arising from that paper.

Looking forward to more substantive discussion with you on future occasions,

Yours Sincerely

(Signed)

Pui-Chong LUND
Association Secretary

S0164

By Email and by Fax
Total 4 pages

1 December 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong
(Fax: 2523 0565)
(Email: pdpo_consultation@cmab.gov.hk)

Views and Comments on the Public Consultation on Review of the Personal Data (Privacy) Ordinance

Attn: Ms Vinci Chan

Reference to my email dated 1 December 2009 below:

QUOTE

Dear Ms Chan

Kindly allow me to add another piece of important enclosure on my submission dated 30 November 2009. It is a copy of the web page concerned in the use of personal data as mentioned in the Enforcement Notice dated 16 August 2006 issued by the Personal Data (Privacy) Commissioner. Attached copy of the web page. It is an Exhibit P8(1) submitted by the police in the court case

Thank you for your consideration.

Best regards
(name)

UNQUOTE

(The sender requested anonymity.
Annexes not attached)

香港工程師學會
THE HONG KONG INSTITUTION OF ENGINEERS

S0165

Your reference: CMAB/CR/7/22/40 Pt. 7

By post and by fax at 2523 0565

30 November 2009

Secretary for Constitutional and Mainland Affairs
Constitutional and Mainland Affairs Bureau
Government Secretariat
Lower Albert Road
Hong Kong

(Attention: Miss Joanna CHOI)

Dear Miss Choi,

Review of the Personal Data (Privacy) Ordinance

Subsequent to our letter of 11 November 2009, we are pleased to provide herewith our views on the Review of the Personal Data (Privacy) Ordinance as set out in the enclosure for your consideration.

Yours sincerely,

(Signed)

Monica YUEN (Mrs)
Secretary

Enc

MY/KL

香港工程師學會
THE HONG KONG INSTITUTION OF ENGINEERS

S0165

Enclosure

Constitutional and Mainland Affairs Bureau

Views from the Hong Kong Institution of Engineers on the Review of the Personal Data (Privacy) Ordinance (PDPO)

General

In the past few years, there have been many large volume data leakage incidents, which usually involved either digital devices or IT systems. In August 2009, the Constitutional and Mainland Affairs Bureau (CMAB), with the support of the Privacy Commissioner of Personal Data (PCPD) issued a consultation document on "Review of the Personal Data (Privacy) Ordinance" and would like to receive public and professional comments. In view of those data leakage incidents related directly or indirectly to engineering and IT professional, the IT Division (ITD) therefore organized a forum for members of HKIE and IT professional bodies to share their opinions with regard to the consultation document. As a follow up to the forum, the ITD then consolidates opinions from member engineers and put forward this written submission.

2. It is important to note that the consultation document include many proposals that will affect engineers and the public directly or indirectly. In particular, professional engineers and IT professionals have been involved in various activities related to personal data, such as collection, processing and management. Moreover, engineering and IT professionals often participate in the design and development of IT systems that handle personal data. Some may participate in management and/or operation of IT systems that collect, store and process such data. The potential liabilities of such tasks and the responsibility of individual professional in the consultation document are not clear.

Views on Proposals

3. In view of the "Review of the Personal Data (Privacy) Ordinance" consultation document by the CMAB, the Hong Kong Institution of Engineers would like to express his view in respect to the key proposals discussed in the document as follow:

Proposal No. 1: Sensitive Personal Data

(a) We agreed in principle that biometric data should be considered as personal data and therefore should be covered by the Personal Data (Privacy) Ordinance.

(b) We have diverse views on whether there should be different levels of sensitivity associated with personal data:

(i) Some members don't see the need of special handling of such set of data with a special classification "sensitive personal data" and believe all personal data should be treated in a homogenous manner.

(ii) Some members believe it is beneficial to differentiate personal data that are "sensitive" from those that are not to allow more focus on protecting the sensitive data. Sensitive data should not be limited to

biometric data. Further consideration should be given to personal data such as certain medical data (e.g. HIV/AIDS), certain personal preference (e.g. sexual preference).

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

(a) We also highlighted that subcontracting activities in IT field can be quite complicated, e.g. data user, data processor and the data center may be different parties. We therefore hope that future legislation should well define the roles and responsibilities of different parties involved. Moreover, those different parties involved may exist in different jurisdictions. We therefore suggest the future legislation should make it clear how such scenarios should be handled, or to enforce the data storage for personal data should be kept locally in Hong Kong unless prior consent has been obtained from the data subject.

(b) With many different parties involved and participated in handling and processing the personal data, it is likely that professionals from different disciplines may participate. We therefore suggest that future legislation should well define the roles and responsibilities of different professionals involved.

(c) With respect to the control of data processors and sub-contractors, our members have different views:

(i) Some members believe it is necessary to regulate the data processors and sub-contracting activities in the similar way as to the data users

(ii) Some members believe that any direct regulation should also consider what a data processor should do in order to comply with the regulatory requirements. For example, security compliance of a data processor is enforced by certification of security compliance by qualified security professional. This is essential to remove uncertainties and enable data processor to meet regulatory requirements. Otherwise, data processors are force to consider establishing their operations outside Hong Kong to avoid the burden imposed by the regulation.

Proposal No. 3: Personal Data Security Breach Notification

(a) We agreed it is necessary to put in some kinds of personal data security breach notification system, which should include the PCPD and the affected individuals. We don't think a voluntary breach notification system is effective. On the other hand, public announcement may not be necessary.

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to PCPD

(a) We support to grant criminal investigation power to PCPD so that complaints can be handled more effectively and efficiently.

(b) We do not support to grant prosecution power to PCPD. We believe such power should be remained with Department of Justice and do not see the need of another prosecution arm in Hong Kong.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66 S0165

(a) We support the proposal that legal assistance should be provided to data subjects that suffer damage by reason of a contravention of a requirement under PDPO by the data user in relation to his personal data.

(b) Providing assistance to aggrieved data subjects in respect of legal proceedings is expected to have a positive effect on achieving greater deterrence on intrusion of personal data privacy.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

(a) We are neutral for this proposal.

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

(a) We do not support the proposal that making contravention of a data protection principle (DPP) an offense.

(b) The conditions for any criminal liabilities should be well defined and their interpretations should be simple and limited. DPPs are defined in generic terms and therefore inappropriate to be used here.

(c) We do support making misuse or mishandling of personal data under specific conditions an offence. We believe large volume of personal data will be stored in IT systems and therefore necessary to enforce registered IT professionals to review and audit IT systems that handle large volume of personal data.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

(a) We support the proposal to make it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes. To avoid ambiguity, it is necessary to clearly define what personal data are included.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

(a) Similar to Proposal No. 8, we do not agree any offence related to violation of DPPs.

(b) We do support the idea that repeated violations of the PDPO on the same facts by the same data user should be an offence.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

(a) We support the proposal to impose monetary penalty on "serious" contravention of DPPs. On the other hand, we would like to see the précised definition of "serious".

Proposal No. 11: Repeated Non-compliance with Enforcement Notice S0165

(a) A repeated offender should be subjected to heavier penalty as a measure to encourage greater deterrent effect. We therefore support the proposal that heavier sanction for data users who repeated contravene an enforcement notice

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

(a) There has been increasing misuse of personal data in direct marketing. We therefore support raising the penalty level for misuse of personal data in direct marketing in order to curb misuse of personal data in direct marketing activities.

Proposal No. 21: Clarifying Power to Direct Remedial Steps in an Enforcement Notice

(a) We support the proposal that PCPD should be given the power to direct the relevant data user in an enforcement notice to desist from doing an act or engaging in a practice.

Proposal No. 24: Transfer of Personal Data in Business Mergers or Acquisition

(a) We support the proposal that an exemption from DPP 3 should be provided for the transfer or disclosure of personal data in intended merger, acquisition or transfer of businesses subject to the condition that the resultant organization will offer substantially similar service as the original data user.

(b) We agree the option set out in Para. 52 in the consultation document are appropriate. To safeguard the exemption from being abused, the handling of the personal data during the process should be properly documented and be subjected to review and audit by professional people.

4. We in principle support the following proposals:

- Proposal No. 13: Third Party to Give Prescribed Consent to Change of Use of Personal Data
- Proposal No. 14: Parent's Right to Access Personal Data of Minors
- Proposal No. 15: Access to Personal Data in Dispute
- Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation
- Proposal No. 17: Erasure of Personal Data
- Proposal No. 18: Fee Charging for Handling Data Access Requests
- Proposal No. 19: Response to Data Access Requests in Writing and Within

40 days

S0165

- Proposal No. 20: Circumstances for Issue of an Enforcement Notice
- Proposal No. 22: Removing the Time Limit to Discontinue an Investigation
- Proposal No. 23: Additional Grounds for Refusing to Investigate
- Proposal No. 25: Provision of Identity and Location Data on Health Grounds
- Proposal No. 26 Handling Personal Data in Emergency Situations
- Proposal No. 27: Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

01/12/2009 11:08

To pdpo_consultation@cmab.gov.hk
itvoice <itvoice@itvoice.hk>
cc
bcc
Subject IT Voice response to PDPO review

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear officer,

Please see the submission attached.

We are open to discuss this with you face to face should you found it necessary. If you need to contact us, please email to (deleted) or phone Mr. S.C. Leung at (deleted)

Regard,

IT Voice 2009-11 IT Voice Response to PCPO review.pdf

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

30 November 2009

Dear Sir / Madam,

Response to Public Consultation on
Review of the Personal Data (Privacy) Ordinance

IT Voice is a group of liberal IT professionals committed to contribute to the prosperity of Hong Kong and the industry. We comment on IT development strategies and public policies from time to time.

In this letter, we would like to respond to the public consultation on review of the Personal Data (Privacy) Ordinance.

TAKING PERSONAL DATA BREACH SERIOUSLY

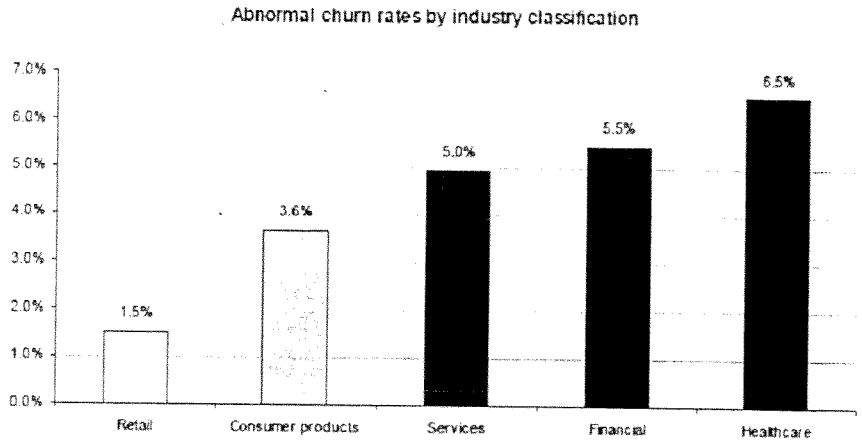
In the light of the following pillars, it is our opinion that public and private organizations should take personal data breach more seriously.

- *Rights. Privacy is a fundamental human right.* It underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age.[1]
- *Financial Impact to Organizations.* A benchmark study of companies by Ponemon Institute found that data breaches have serious financial consequences on an organization.[2] The cost of breach includes not only the cost of detection, escalation, notification and incident response, but also the opportunity costs like

[1] Marc Rotenberg, "Protecting Human Dignity in the Digital Age" (UNESCO 2000)

abnormal churn (negative turnover) rate of existing customer and diminished new customers.

- *Adverse effect on consumer victims.* This was echoed by a Gartner research which found that there was an adverse effect on consumer victims. Some suffered long term damaged credit rating. Victims are significantly changing their financial transaction behaviours.[3]
- *Impact to Hong Kong economy.* The Ponemon Institute study also revealed that healthcare and financial industries have highest abnormal churn rate after data breach. As an international financial centre, Hong Kong enterprises should be alerted that data breach can bring about very far reaching impact to our economy.



- *Confidence on public institutions.* On the confidence of public institutions, previous case of data breaches in IPCC (2006), Hospital Authority (2008-2009) and Hong Kong Police (2009) had brought about very negative image to the governance.
- *Internal Negligence as major source of data breaches.* The Ponemon Institute research also found that 88% of the breach was caused by negligence and 12% by malicious act. In this aspect, organizations should be better regulated to prevent personal data breach.
- *Future of Hong Kong.* The move of Hong Kong to a networked society implies a

---

[2] Dr. Larry, "Fourth Annual US Cost of Data Breach Study", Ponemon Institute January 2009

[3] Avivah Litan, "Data Breaches and Financial Crimes Scare Consumers Away" (Gartner Research February 2009)

continuous expanding of information flow, which may have potentially escalated exposure to data breaches if we do not take proactive measures.

RESPONSES TO THE REVIEW

The enactment of the PDPO was a monument of Hong Kong to stand as a world leader in the protection of personal data privacy. It has contributed to making Hong Kong a free and safe confluence of information and business. As a continuous improvement and a response to recent data breach incidents, we welcome very much the review of the PDPO.

IT Voice recognizes the importance of balancing business interests and individuals' rights. When dealing with the context of personal data privacy in Hong Kong, we also take into account the weaker consumer community as compared to the businesses and the lack of class action in litigation. When we make our comments on the review, we keep in mind the proper balance of power and we take the common good of the citizens as the highest priority.

In the response below, we include the proposal number set out in the consultation paper in the beginning of each session.

Sensitive Personal Data

Proposal No. 1 Sensitive Personal Data

- We hold that sensitive personal data be defined as that, once breached, may left data subject vulnerable to attack or unfair treatment because of the data breached. This definition is in agreement with many overseas jurisdictions.
- Accordingly, sensitive personal data should include racial or ethnic origin, political affiliation, membership of trade union, religious belief, health condition, sexual orientation and practices, gender history, etc. In addition to these types of data, the UK and Australia also classify criminal record as sensitive personal data, while Australia also regards genetic information as sensitive personal data. Genetic information is sensitive NOT because it is biometric information as in "it cannot be

changed" or that "it can be used to uniquely identify a person", but rather it is because genetic information may be used as a discrimination against a person (e.g. due to genetic tendencies to illness etc.)

- As such, sensitive data is not equal to information that can uniquely identify a person, nor is it equal to information that a person cannot change (e.g. biometric information).
- In principle, we support that there is a category of "sensitive" personal data where more stringent regulation is enforced. Sensitive data should require a higher barrier of collection (or on voluntary basis), retention, access and protection. However, we also alert the clear guidelines and education must be accompanied to educate the community how to classify sensitive data and how to provide different protective measures to different class of personal data.

Data Security

Proposal No. 2 Regulation of Data Processors and Sub-contracting Activities

- Taking information security and privacy management as a holistic approach, we agree that data processors and sub-contractors of data processing should be accountable as data users when they are processing personal data.
- We agree that specific obligations should be imposed on the data users by requiring them to take specific security measures when contracting out the processing of personal data to third parties.
- At the same time, the scope of inclusion should be clearly defined and restricted to penalize only negligent parties but not ignorant parties. There are cases where service providers have no knowledge of whether they are holding personal data. For example, data processors of test data who are not informed that test data given by careless data users are real personal data; Internet service providers and online service provides who are only providing conduits or platforms for data communication and storage do not know the nature of data passing through the conduits or stored in the platform.

Proposal No. 3 Personal Data Security Breach Notification

- We hold that the right to be informed of personal data breach is a human right [4] and the notification is also essential for the victims to mitigate the damage.
- We propose the mandatory notification of personal data security breach.
- We hold that the notification be effective only if it is mandatory. Without legislation mandating breach disclosure by all organizations managing private data, it is extremely unlikely that organizations will voluntarily disclose security breaches. Organizations that choose to disclose breaches will be disadvantaged in the market when competitors choose not to disclose similar breaches.[5] Voluntary disclosure practices will not create a fair playing field for organizations and will not provide customers with reliable or consistent information concerning the quality of security assurance available from all vendors in the market.
- The U.S. can provide good reference on successful implementation of notification laws. The California Security Breach Information Act was introduced in 2003. Subsequently over 40 states in the U.S. enacted similar law. In November 2009, the U.S. Senate Judiciary Committee approved both the Personal Data Privacy and Security Act and the Data Breach Notification Act by large majority. The Data Breach Notification Act requires any federal agency or business entity engaged in interstate commerce that uses, accesses, or collects sensitive personally identifiable information, following the discovery of a security breach, to notify the resident whose information may have been accessed or acquired, the owner or licensee of any such information that the agency or business does not own or license. The bill also requires agencies and businesses to report large data breach to the U.S. Secret Service.
- We propose that large data breach be reported to PCPD who should keep a database of data breach of previous 7 years for public enquiry.
- We propose the notification of breach be implemented in phase according to risk level and nature of business so that the community (especially small businesses)

---

[4] "[E]veryone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representations (implicit or explicit) that those individuals make concerning their moral qualities." Posner, "The Right of Privacy", 1978

[5] Australian Voluntary Breach Disclosure Will Not Produce Transparency in Security Failures, Andrew Walls, Gartner

can adapt. Government, public institutions, critical infrastructure, financial and other regulated industries should be mandatorily required to implement the notification mechanism in the first phase to act as a model. All other sectors, including small and medium enterprise not falling into first phase should implement in second phase (three years after the start of the first phase).

Enforcement Powers of the Privacy Commissioner for Personal Data ("PCPD")

Proposal No. 4 Granting Criminal Investigation and Prosecution Power to the PCPD

- We are of the opinion that the criminal investigation and prosecution power should be vested with law enforcement agencies.

Proposal No. 5 Legal Assistance to Data Subjects under Section 66

- We support to provide legal assistance to aggrieved data subject when they are in need.

Proposal No. 6 Award Compensation to Aggrieved Data Subjects Court

- We are of the opinion that it is the power of court to decide compensations for damages. PCPO should remain to be the institution to decide if there is data breach.

Offences and Sanctions

Proposal No. 7 Making Contravention of a Data Protection Principle an Offence

Proposal No. 9 Repeated Contravention of a Data Protection Principle on Same Facts

Proposal No. 10 Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

- We are of the opinion that making the contravention of the broad Data Protection Principles an offense would create turmoil and confusion. Any offense should be clearly defined. We notice that contravention of the enforcement notice issued by PCPD is currently an offence.

Proposal No. 8 Unauthorized Obtaining, Disclosure and Sale of Personal Data

- We support to make it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes.

Proposal No. 11 Repeated Non-compliance with Enforcement Notice

- We support a heavier sanction for data users who repeatedly contravene an enforcement notice.

Proposal No. 12 Raising Penalty for Misuse of Personal Data in Direct Marketing

- We support raising the penalty level for misuse of personal data in direct marketing.

Rights of Data Subjects

Proposal No. 13 Third Party to Give Prescribed Consent to Change of Use of Personal Data

- We think that the scope must be clearly defined, for example, a person who has parental responsibility for the minor

Enforcement Powers of the PCPD

Proposal No. 20 Circumstances for issue of an Enforcement Notice

- We support the discretion power for the PCPD to serve an enforcement notice under any of the following circumstances stated in the proposal:
  (a) whether the act of contravention is continuing;
  (b) whether the contravention will continue or be repeated;
  (c) whether the contravention has caused or is likely to cause damage or distress to the data subject.

Proposal No. 21 Clarifying Power to Direct Remedial Steps in an Enforcement Notice

- We support to empower PCPD to direct the relevant data user in an enforcement notice to desist from doing an act or engaging in a practice.



New Exemptions

Proposal No. 25 Provision of Identity and Location Data on Health Grounds

- We agree to permit disclosure of any personal data where disclosure is necessary to prevent or lessen a serious threat to the life or health of an individual.

Proposal No. 26 Handling Personal Data in Emergency Situations

- We agree to grant exemption to law enforcement agencies and rescue and relief agencies for handling personal data in emergency situations

Miscellaneous Proposed Amendments to the PDPO

Proposal No. 31 Power to Impose Charges for Educational and Promotional Activities"

- We agree that PDPO be empowered to impose reasonable charges for educational or research projects similar to Equal Opportunity Committee.

Proposal Not to be Pursued

We have **strong opinions** on the following areas that the proposal does not try to pursue. We like to have your attention and your action to put them into action items.

"A.2 Internet Protocol Address as Personal Data"

- IP address alone is not personal data. However, when correlated other information, like ISP's customer database, time stamp, it becomes data of an identifiable person. In that case, we are of the opinion that such information should be regarded as personal data and entitled to the protection of the ordinance.

"A.3 Territorial Scope of the PDPO"

- Currently PDPO has not enacted Section 33 to order data user to take all reasonable precautions and to exercise all due diligence to ensure that the personal data will not be collected, held, processed or used in a place outside Hong Kong in any manner which, if that place were Hong Kong, would be a

contravention of a requirement under the Ordinance.

- The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[6] and the Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data[7] set out specific rules covering the handling of electronic data across the border.
- The PDPC had informal discussions with the EU over the question of the adequacy of data protection under the EU Data Protection Directive, but has not received a formal reply. Hong Kong will likely not be deemed adequate before the enactment of Section 33 of the Ordinance.[8]
- Many countries, especially in Asia, have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognize that consumers are uneasy with the increased availability of their personal data, particularly with new means of identification and forms of transactions. These countries recognize consumers are uneasy with their personal information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules. Rise of off-shore data repository, e.g. cloud computing, software-as-a-service makes regulation of trans-border data flow of personal data more essential than before.
- Many countries are adopting new laws or updating older laws based on the Council of Europe Convention No. 108 and the EU Data Protection Directive in order to ensure that trade will not be affected by the requirements of the European Union Directive.
- The Madrid Privacy Declaration[9] urges countries that have not ratified Council of Europe Convention 108 together with the Protocol of 2001 to do so as expeditiously as possible;
- We are of the view that our PDPO should be compared against international standard. PDPO should enact Section 33, to comply with the EU requirement and

---

[6] ETS No. 108, Strasbourg, 1981

[7] OECD, Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data" (1981)

[8] http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559532

OECD guideline. The compliance is vital for Hong Kong to stay competitive and allow outsourcing business to capture the international market.

Other Opinions

Training and Awareness Education is most effective preventive measures

- We regarded preventive measures like training and awareness education a critical success factor for PDPO. Taking good experience of EOC and ICAC, Government should provide sufficient funding to PDPO to expand their reach the corporations, schools and the community.

We are open to discuss this with you face to face should you found it necessary. If you need to contact us, please email to (deleted) or phone Mr. S.C. Leung at (deleted)

Regards,

The IT Voice Team

Robin Bradbeer
Edmon Chung
Francis Fong
Charles Mok
Joseph Ng
S.C. Leung
Chester Soong
Joe Yau
Lento Yip
Sang Young

---

[9] Article 2, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-565563

S0167

(發件人要求以保密方式處理意見書)

(The sender requested confidentiality)

S0168

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Submission to PDPO review from ISOC-HK

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

01/12/2009 14:27

Pls find attached the submission from the Internet Society Hong Kong for the PDPO review.-
Thank you for your attention.

Charles Mok
Chairman
Internet Society Hong Kong

PDPO response.doc

Response to the Review of the Personal Data (Privacy) Ordinance S0168

1. **Internet Society Hong Kong** (ISOC-HK) welcomes the review of the Personal Data (Privacy) Ordinance (PDPO). The ordinance was enacted before Internet usage became so widespread. As the awareness among citizens for personal data protection and privacy increases, the expectation of our citizens have overtaken the reach of the existing ordinance.

2. We generally agree with the guiding principles of the review as stated, in particular that "balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology," and the PDPO "should remain flexible and relevant in spite of technological changes."

Sensitive Personal Data

Proposal No. 1: Sensitive Personal Data

3. We do not support Proposal No. 1 to differentiate "sensitive" personal data at this stage, because we do not believe any such "more stringent regulation of sensitive personal data" would result in a higher level of protection, and we find the Government's proposed classification of, or indeed the singling out of, biometric data is problematic and unreasonable.

4. Although, as the consultation paper indicates, biometric data are "unchangeable," and "the harm caused to an individual is substantial in any biometric system security failure," we believe that these factors should not be the sole or primary considerations in determining what may constitute "sensitive data." Instead, as other jurisdictions normally include "racial or ethnic origin, political opinion, religious or philosophical beliefs, membership of trade unions, health condition, and sexual life.... (and) criminal records" as sensitive personal data, we believe the "effect" of such data being made known without consent of the data subject is vastly more important than whether these data are unchangeable or not.

5. We believe at the current stage our legislative priorities should be to strengthen enforcement for *all* personal data protection, instead of singling out one type of data for "more stringent regulation," especially given the very dubious reasoning for such classification.

6. It is also noted by the information technology industry that such singling out of biometric data – which is hardly an international norm by any measure – has already sent a chilling effect over the use of such technology, which runs against one of the guiding principles of the consultation, that of seeking a balance of privacy protection with the development of ICT.

Data Security

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

7. The definition of data processing and the classification of data processors can be cover a wide range of activities and players such as software developers and testers, Internet service

providers (ISPs), online service providers (OSPs), web hosting service providers, software-as-a-service providers, or even social media. Direct regulation on such a wide range of data processor companies, some of them possibly being overseas, may prove to be difficult to define and execute.

8. We are concerned about the effects of direct regulation on Internet-related businesses, as "such data processors typically have no knowledge of whether the data they are holding are personal data." As the consultation paper points out, "compliance...may frustrate free flow of information on the Internet."

9. We believe that the option of indirect regulation would be sufficient, "as a first step," to provide the means for redress for the data subject against the data user when necessary, but striking a balance with the nature of Internet-related business and the free flow of information.

Proposal No. 3: Personal Data Security Breach Notification

10. Over the past few years, it is evident that "privacy breach notification" has become part of the expectation held by the public, at least on some of our major institutions, such as those holding our "sensitive" (generally speaking) personal data, such as our financial or health data. Indeed, some would consider the right to be informed of personal data breach to be a "human right," and notification is also essential for the data subject victim to mitigate the damage.

11. While we acknowledge the "burden" on business operation, or indeed the operation of the Privacy Commissioner for Personal Data (PCPD), under a mandatory notification requirement, we are concerned that a purely voluntary system may not provide significant incentives for businesses or institutions to give notifications voluntarily. We are uncertain about the effectiveness of the supposed but yet (at present) unknown "guidelines on voluntary privacy breach notifications."

12. We believe that there are significant overseas experience to make references of for establishing a mandatory privacy breach notification regime for certain kinds of breaches and certain types of institutions, such as Government and public institutions, critical infrastructure or regulated utilities, financial and educational institutions.

13. We also propose that a database of privacy data breaches to be maintained by the PCPD for a period of at least seven (7) years, for the public to search and be informed about the privacy performance of various organizations.

Enforcement Powers of the PCPD

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

14. We do not support the granting of criminal investigation and prosecution power to the PCPD, as we are concerned about the PCPD holding the dual roles and powers of being the regulator, investigator and prosecutor all at the same time.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66 S0168

15. In principle, we agree with the proposal to allow the PCPD to be given the power to provide legal assistance to the aggrieved data subject, as it is common that an average aggrieved citizen would find it difficult to pursue costly legal proceedings. However, we also believe that conditions should be imposed on the granting of such assistance, such as, similar to the case of the Equal Opportunities Commission (EOC), if the case raises a question of principle, and if the case is a representative case with public interest.

16. However, we are also concerned about the possible effects of such actions taken against ISPs and OSPs, which merely provide the conduits (as a common carrier) or the open platform for Internet users' expressions. Any frivolous action may deter the free flow of information and cause detrimental effects on the freedom of expression. Hence, we propose that a clear set of guidelines be established to "regulate" the scope of enforcement of the PCPD, especially over cases that may involve the freedom of expression in an open forum.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

17. We concur with the Legal Reform Commission's view that the combination of enforcement and punitive functions vested in a single authority is undesirable. We agree that it should be left for a court to determine the amount of compensation to the data subjects.

Offences and Sanctions

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence
Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts
Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

18. We believe making such contravention of the broad data protection principles an offence would cause turmoil and confusion, as "DPPs are couched in general terms and can be subject to a wide range of interpretations," and as the consultation paper suggests, may "have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability."

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

19. We agree in principle to make it an offence if a person "knowingly or recklessly obtained the personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes." However, we believe clear guidelines must be issued to the public, as the behaviors of many Internet users are currently accustomed to may come very close to entering an offence.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

20. We support imposing a heavier sanction for data users who repeatedly contravene an

S0168

enforcement notice.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

21. We support raising the penalty level for misusing personal data in direct marketing.

Proposals not to be Pursued

A.2: Internet Protocol Address as Personal Data

22. We agree that an IP address alone is not personal data, but when correlated with other information, such as a time stamp and an ISP's customer database, the IP address clearly becomes the data that initiate the trace-route of identifying a person. As clearly shown in a previous case, the fact that an IP address is not classified as a personal data means it is not subject to the data protection principles, and for example be transferred to a third party legally, leading to the identification and prosecution of the person. There is clearly a loophole.

23. We believe that IP address should be classified as personal data and subject to protection under the ordinance under certain circumstances and conditions, and it is unreasonable for the Government not to consult this proposal.

About Us

30. Internet Society Hong Kong (ISOC-HK) is the local chapter of the Internet Society (ISOC), the global organization of Internet users and professionals, providing leadership in issues confronting the future of the Internet, including global coordination, development and cooperation of the Internet, technology standards, Internet governance and online civil society.

Internet Society Hong Kong

2009.11.30



01/12/2009 15:00

To <pdpo_consultation@cmab.gov.hk>
cc
bcc
Subject HKCSS's View on PDPO Review

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear sir/madam,

Enclosed please find the HKCSS's submission on PDPO review consultation .

Any enquiry please feel free to contact me directly .

Thanks!
MOSES

MUI Wai-keung, Moses
Chief Officer
Service Development (Family & Community)
The Hong Kong Council of Social Service



HKCSS Paper on PDPO Review.pdf

S0169

香港社會服務聯會
The Hong Kong Council of Social Service

贊助人
行政長官 曾蔭權先生
PATRON
The Chief Executive the Hon. Donald TSANG Yam-kuen

行政總裁
方敏生女士
CHIEF EXECUTIVE
Ms. Christine M. S. FANG

香港下亞厘畢道

中區政府合署東座364室

政制及內地事務局（第4組）

就檢討《個人資料（私隱）條例》的諮詢文件的意見

政府就《個人資料（私隱）條例》（下稱"私隱條例"）進行全面檢討，就着過去十年各方面的發展，研究私隱條例的現有條文是否仍足以保障個人資料，並提出了一系列修訂建議。就眾多修訂建議中，社會福利界對其中兩項尤為關注，包括建議14及27，有關意見可參考隨函附件。

如對有關意見有何查詢，請直接與本會服務發展總主任(家庭及社區)梅偉強先生（（刪除））聯絡。

多謝垂注。

業務總監(服務發展)

（已簽署）

陳榮亮博士

2009年11月30日

附件：香港社會服務聯會就檢討《個人資料（私隱）條例》的諮詢文件的意見

香港社會服務聯會
就檢討《個人資料（私隱）條例》的諮詢文件的意見

背景

政府就《個人資料（私隱）條例》（下稱“私隱條例”）進行了全面檢討，就着過去十年各方面的發展，研究私隱條例的現有條文是否仍足以保障個人資料，並提出了一系列修訂建議。就眾多修訂建議中，社會福利界對其中兩項尤為關注，包括建議14及27，有關意見闡述如下。

建議14：父母親查閱未成年人士個人資料的權利

就著在尊重父母照顧子女的角色以及兒童的私隱權兩方面取得平衡，原則上本會同意在現有私隱條例中加入新的條文，准許資料使用者拒絕一位代表一名未成年人的“有關人士”提出的查閱資料要求，以保障未成年人的利益。

另一方面，本會亦同意當一位代表一名未成年人的“有關人士”提出查閱資料的要求，而資料使用者有合理理由相信如果依從該項要求，並不符合該名未成年人的最佳利益，則可以拒絕該項要求。惟當中必須確立專業評估機制，以衡量有關合理理由拒絕父母的查閱要求，當中考慮因素應包括：

- 父母是否以子女最佳利益為本作查閱資料
- 父母會否懷疑涉及虐待子女
- 子女的個人意願（除涉及子女之人身安全外）

建議27：為了履行監護責任和家長照顧責任而把未成年人的個人資料轉移

本會原則上同意在現有私隱條例中訂定豁免條文，准許把未成年人的個人資料轉移給其父母或監護人，以加強對易受誘惑的未成年人和邊緣少年的保護，以及使父母及監護人可妥善地履行適當照顧和監護兒童的責任，但必須清楚界定何謂「未成年人」及「邊緣少年」。

另外，本會亦同意附加特定條件，以限制轉移個人資料的做法只適用於絕對有需要的個案，有關「特定條件」應視乎是否有足夠證據顯示當事人正身處危機當中。

2009年11月

Construction Industry Council
建造業議會

S0170

本會檔號 Our ref.:

本會檔號 Your ref.: CMAB/11/73

電話 Tel. No.: (deleted)

傳真 Fax No.: (deleted)

電郵 E-Mail: (deleted)

1 December 2009
By Fax and by Post

Ms Christina Chong
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Ms Chong,

Re: Review of the Personal Data (Privacy) Ordinance

Thank you for your letter dated 1 December 2009 on the above subject.

As discussed with your colleague this afternoon, we enclose herewith a letter regarding our comments on "Consultation Document on Review of the Personal Data (Privacy) Ordinance" Issued in August 2009 for your consolidation.

Yours faithfully,

(Signed)

(Christopher To)
Executive Director

Encl.

CT/AL/kc

Construction Industry Council
建造業議會

S0170

本會檔號 Our ref.:
本會檔號 Your ref.:
電話 Tel. No.: (deleted)
傳真 Fax No.: (deleted)
電郵 E-Mail: (deleted)

27 November 2009

Assistant Secretary (Constitutional and Mainland Affairs)4B
3/F, East Wing,
Central Government Offices
Lower Albert Road
Central, Hong Kong

Dear Sir,

Comments on "Consultation Document on Review of the Personal Data (Privacy) Ordinance" Issued in August 2009

We are writing to provide our comments on two particular proposals (Proposal Nos. 1 and 5) which concern the construction industry as per "Consultation Document on Review of the Personal Data (Privacy) Ordinance" issued in August 2009.

Proposal No. 1: Sensitive Personal Data

1. *Whether biometric data is "personal data"*

1.1 The CIC does not dispute that biometric data is personal data in that it is data derived from an individual and used to verify or identify the data subject. This is the case both for biometric images (i.e. raw biometric data) and the more commonly used biometric templates (i.e. the conversion of the biometric image into a numeric template consisting of a string of numbers).

2. *Whether biometric data is "sensitive data"*

2.1 The CIC does not disagree that, as a matter of principle, certain categories of personal data may, owing to their inherently sensitive nature, warrant enhanced protection and more stringent regulation under the PDPO. The question is whether biometric data is sufficiently "sensitive" so as to warrant such enhanced protection and more stringent regulation.

2.2 As noted in paragraph 3.03 of the Consultation Paper, personal data commonly regarded by overseas jurisdictions as being "sensitive" includes racial or ethnic origin, political opinion, religious or philosophical beliefs, membership of trade union, health condition, criminal record and sexual life. For example, under both the United Kingdom Personal Data Act (1988) and Australia's Privacy Act

(1988), "sensitive personal data" is defined as the following types of data concerning an individual:

(a) racial or ethnic origin;

(b) political opinions;

(c) membership of a political association;

(d) religious beliefs or affiliations;

(e) philosophical beliefs;

(f) membership of a professional or trade association;

(g) membership of a trade union;

(h) sexual preferences or practices;

(i) criminal record.

(Under the Australian Privacy Act, health information about an individual and genetic information about an individual that is not otherwise health information also fall within the definition of "sensitive personal data".)

2.3 Neither the United Kingdom's Personal Data Act (1988) nor Australia's Privacy Act (1988) currently incorporates biometric data in the definition of "sensitive" personal data or otherwise distinguishes the way in which biometric personal data can be collected, used and/or processed from other types of "non-sensitive" personal data. (The CIC notes, however, that in Australia the Australian Law Reform Commission has, during a recent review of the Australian privacy legislation, recommended that biometric information be expressly incorporated in the Privacy Act. There is no similar proposal for the differentiation of biometric data in the United Kingdom.)

2.4 The justification for differentiating the above categories of "sensitive" personal data ("Traditional Sensitive Data") is based on the potential harm that could result if such data were to be mishandled. As noted in paragraph 3.03 of the Consultation Paper, the criteria generally adopted in deciding whether certain kinds of personal data is sensitive are:

(a) intimate data about an individual; and

(b) data likely to be utilised in discriminatory decisions.

2.5 Applying these criteria, the CIC does not consider biometric data to be inherently sensitive in the same way that Traditional Sensitive Data is. This would seem to be supported by the statement in paragraph 3.06 of the Consultation Paper that *"Biometric information could reveal sensitive personal information such as*

health, genetic information or ethnic origin... Any security failure in biometric systems could result in sensitive personal information of individuals being compromised". i.e. the cause for concern with biometric data does not stem from any inherent sensitivity of the data itself, but rather from the purposes for which biometric data could be used, and from the security of biometric systems.

2.6 As such, the CIC does not consider it appropriate that any new definition of "sensitive data" introduced into the PDPO should include biometric data. If biometric data is to be distinguished in the PDPO, then it should be categorised separately from, and treated differently to, Traditional Sensitive Data.

3. *Potential concerns to be addressed by proposed amendments to the PDPO*

3.1 The main privacy related objections raised in respect of biometrics are:

(a) That biometric data are unique identifiers (i.e. in that fingerprints, facial geometry, irides, etc, and to a lesser extent behavioural characteristics such as key stokes and voice, are unique to each person) which are incapable of being lost, changed or forgotten;

(b) That biometric data, which are collected and stored via biometric systems, give rise to heightened security risks.

3.2 While some biometric systems capture and retain identifiable biometric images or samples, for the most part nowadays they do not. With fingerprint scanning, which is the particular focus of these submissions, most technologies do not capture the fingerprint, but rather they convert the image of fingerprints into a numeric template that consists only of a string of numbers useful only to the particular device. Further, biometric templates vary with each biometric recording - e.g. the same finger, placed over and over again on the same device, will generate a different template each time. In this sense they are not unique identifiers in that each data subject can generate multiple different fingerprint templates not only by using different biometric systems, but by using the same biometric system. Further, if properly encrypted with one-way decoding, fingerprint templates cannot be reverse engineered so as to recreate the actual fingerprint.

3.3 Security concerns are not inherently founded in the nature of biometric data but rather are systemic in nature. Biometric data cannot be separated from the biometric system, and the broad range of biometric technologies, infrastructures and deployment environments render any all-encompassing statements on biometrics meaningless. Biometrics, like any technology, are defined by their usage and can be deployed in a privacy-invasive manner or in a privacy-neutral or even privacy protective manner. As noted in paragraph 3.06, *"any security failure in biometric systems could result in sensitive personal information of individuals being compromised".* This is especially the case for biometrics

systems which store biometric data on a scanning/matching device or centralised server.

3.4 As with almost all types of personal data, there is of course also the potential for biometric data to be misused and/or deployed for inappropriate purposes. But this risk is to an extent mitigated by the systemic and operational controls which are incorporated into most biometric systems. As noted above, biometric data cannot be separated from the biometric system, and for the most part the particular biometric system itself will limit the usage of the biometric data (including the purposes for which they can be used) to specific functions, for example verification of identification. To address privacy concerns, many biometric systems have now been developed accordingly and are self contained in the sense that they do not have interoperable functionality and do not facilitate the storage of biometric data with other types of personal data (such as name, Hong Kong ID card number, etc).

3.5 Additional concerns relate to:

(a) unnecessary or unauthorised collection - gathering biometric information with the subject's permission or knowledge, or gathering biometric data without explicitly defined purposes;

(b) unauthorised use - using biometric information for purposes other than those for which they was originally acquired;

(c) Unauthorised disclosure - sharing or transmitting biometric information without the user's explicit permission

(d) function creep - gradually using biometric data for a variety of purposes beyond its original intention and scope.

However again, these concerns apply across the board to all personal data and can be eliminated through the deployment of appropriate systemic security and operational measures.

3.6 Further, many biometric systems now operate by storing biometric data on individual devices owned by and under the control of the data subject (e.g. smartcards, USB keys), which means that a subject's biometric data is not at any point in the cycle of recording, reading and identifying a fingerprint match, collected or accessible by the data user. In fact there are some types of biometric systems which can be deployed without any actual collection by the data user of biometric data for the purposes of the PDPO. This was recognised by the PDPC in the Investigation Report issued on 13 July 2009 relating to the Collection of Employees' Fingerprints for Attendance Monitoring Purposes". In that report, the PCPD noted that identification verification through a certain type of biometric system which converted certain features of the fingerprint into a unique value and stored it in a smart card held by a data subject did not involve

the collection of the data subject's fingerprint data or the value, and accordingly that such system did not fall within the scope of the PDPO.

4. *Benefits of biometric systems*

4.1 The benefits of the deployment of biometric systems and the use of biometric data with appropriate security and operational controls are obvious.

4.2 Biometric systems are becoming increasingly deployed, both in public and private sectors, as a method of access management and access control. Biometrics systems offer an efficient, secure method to make highly accurate verifications of individuals, eliminating the need to carry badges and other identification, and preventing the use of forged identifications.

4.3 In the private sector, biometric systems facilitate:

(a) Enhanced security of access to workplaces which (for some industries in particular, including the construction industry), can in turn result in a significant improvement of workplace safety for workers.

(b) Prevention of access fraud, including reduction of losses resulting from practices such as 'buddy punching', to which certain industries (including the construction industry) are particularly susceptible.

(c) More efficient human resource management including, in particular, the more timely and accurate calculation and payment of wages to workers.

4.4 These benefits are particularly relevant to the construction industry, which is characterised by:

(a) an extremely large base of multi-skilled, transient workers (including other employees, contractors and subcontractors);

(b) allocated to multiple concurrent projects at different sites; and

(c) working in a highly dangerous workplace environment.

4.5 There are currently around 50,000 manual construction workers in Hong Kong. Manual Workers are either directly employed by the main contractor, or indirectly employed as subcontractors or gangers, and include skilled, semi-skilled and general workers. At any given time there are approximately 1,000 construction sites operational in Hong Kong. For larger construction sites it is not uncommon for more than 200 workers to be working at a particular construction site at any given time.

4.6 While there has been a significant decrease in construction site accidents in recent years, the number of accidents, calculated annually, still reaches the thousands, with fatalities averaging at least 20 per year over the past 5 years. Construction sites are the most dangerous land based work places in the world

and Hong Kong is no exception. Safety hazards are numerous and varied and include, most commonly, falls from height, motor vehicle crashes, electrocution, machinery malfunction, and being struck by falling objects. The failure to wear the right protection, not operating machinery properly or merely turning the wrong way can result in a serious and potentially life threatening accident. Workers not properly trained in site safety pose a significant threat not only to themselves but to their workmates.

4.7 It is therefore critical that only persons with appropriate experience and training, in particular with respect to site safety, are able to access construction sites or, depending on their role, restricted areas of construction sites identified as being particularly hazardous.

4.8 Photographic identification cards or even magnetic access cards do not prevent fraudulent access, which is particularly prevalent in a project based industry where, for any given project, the workers are not necessarily employed or even subcontracted by a centralised company, and are allocated to different projects and sites on an as needs basis.

4.9 Additionally, the nature of the construction industry is such that the management of human resources, in particular the administration of payroll, is extremely complicated and often results in the miscalculation of wages and/or delays in payment. The deployment of a centralised biometrics system would serve to provide a corollary benefit to workers in that the ability of the industry as a whole to centrally and manage and monitor site access could also serve to significantly improve the efficiency of human resource management and payroll administration.

4.10 The United Kingdom provides an excellent example of a jurisdiction where biometric systems have been successfully deployed in the construction industry in order to enhance site access security and the management of human resources. By way of example, the following high profile construction projects, which are all ongoing as of the date of these submissions, all rely on biometric data site all utilise biometric data in the management access management, time and attendance:

(a) the 2012 Olympic Park;

(b) Crossrail, a new east-west railway running under the centre of London; and

(c) a large hospital extension project in the north-east of England.

4.11 To date, there have been no recorded objections by workers, including complaints filed with the relevant data protection authorities, to the deployment of such deployment biometric systems.

5. *The PDPO as it currently applies to the deployment of biometric systems*

5.1 Under the PDPO in is unclear whether the deployment of similar biometric systems in the management of construction projects in Hong Kong would be permitted.

5.2 The collection of biometric data is regulated by DPP1 (which only permits the collection, by fair means, of personal data which is strictly necessary for and commensurate to the lawful purposes of the data user) and DPP 2 (which, among other things, requires personal data to be collected by means which are lawful and fair in the circumstances of the case).

5.3 There have been a number of recent cases in Hong Kong involving complaints relating to the collection of fingerprint data. For example:

(a) Case 2008004 involved the use by a primary school of a fingerprint recognition system for recording its pupils' attendance, provision of library services and purchase of lunch.

(b) Case 2005012 involved the use by a furniture company of a similar fingerprint recognition system for security and attendance monitoring

6. *Whether the proposed regulatory regime as set out in paragraphs 3.08 to 3.14 of the Consultation Paper is appropriate*

6.1 The introduction of any new regulatory regime which applies to the deployment of biometric systems must be founded on the principle of proportionality (on which the PDPO is founded).

6.2 It is the CIC's submission that the diversity of biometric systems already in existence, and the highly industry specific variability of the respective advantages and disadvantages for data users vis-à-vis data subjects of the deployment of such systems, necessitates at the very least that the regulatory regime is flexible in the way that it applies to the collection, use and processing of biometric data. Flexibility will also be crucial so that the regime can adapt to accommodate inevitable developments in biometrics technology.

6.3 Specifically, it would be inappropriate to introduce amendments to the PDPO which prohibited (albeit on a restrictive basis) the collection of biometric data and the utilisation of biometric systems across the board, especially in circumstances where they have been proven not only to be effective, but to be advantageous to both data users and data subjects alike in certain industries. To do so would be to ignore and undermine the proportionality principle which underpins the DPDP. That principle requires a consideration of:

(a) The degree of sensitivity of the biometric information.

(b) How well the data user will protect the information.

(c) Whether the business objectives of the employer are legitimate and bona fide, and whether the biometric information is effective in meeting those objectives.

(d) Whether there are alternative methods of achieving the same level of security at comparable cost and with comparable operational benefits.

6.4 As set out above, in the context of industries such as the construction industry privacy intrusion (i.e. security risks) is offset if not at the very least outweighed by the benefits of the deployment of biometric systems which address not only the shortfalls in construction site access, but also the inefficiencies of human resource management and payroll administration.

6.5 The proposed amendments as set out in paragraph 3.09 proposes to introduce a blanket prohibition on the collection, holding, use and processing of biometric data in circumstances that are, relevantly (to the construction industry), in circumstances where

(d) handling of the data in the course of the data user's usual lawful function and activities with appropriate safeguard against transfer or disclosure to third parties without prescribed consent of the data subject.

6.6 The CIC is also concerned that this exception is ambiguous. i.e. What is meant by "lawful functions and activities"? Would this include the protection of workplace safety and the facilitation of the efficient management of human resources including the accurate and timely payment of wages? Does "handling of the data" include collection?

6.7 The PDPO in its current form already restricts the ability of data users to deploy biometrics systems but allows for flexibility in the application of the proportionality principle to be applied on a case by case basis to determine whether any loss of privacy to data subjects is not disproportionate to the costs and operational and security benefits of the data user.

6.8 The CIC submits that the introduction of a new regulatory regime applicable to biometrics is unnecessary.

6.9 If any such new regime is to be introduced, then the CIC submits that data users such as companies in the construction industry having a bona fide need to deploy biometrics should have a positive right to do so subject to complying with safeguards such as (currently):

(a) ensuring that biometric data is encrypted immediately after collection;

(b) restricting some secondary uses of biometric information without express free and informed consent; and

(c) introducing an obligation of accountability through an extra notice obligation, audit of biometric systems and use of privacy impact statements.

6.10 Further developments in biometrics technology will inevitably impact upon such safeguards and their application to certain industries. As such, the CIC submits that any regime that may be introduced regulate biometrics above and beyond what is already provided for in the PDPO should be implemented as a code of practice which could evolve with further technological developments.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

1. *Assistance for legal proceedings instituted on public policy grounds*

1.1 The CIC has no objection in principle to aggrieved data subjects having access to legal assistance, including public funds, in instituting legal proceedings pursuant to Section 66 of the PDPO, where the decision to assist a data subject is based solely on the belief by the PDPC that the data subject has suffered harm which cannot be compensated other than by an award of damages.

1.2 The CIC objects to the provision of legal assistance to an aggrieved data subject where the decision to assist the data subject is based primarily on public policy grounds, for example:

(a) To provide a deterrent effect (as noted in paragraph 5.13 of the Consultation Paper); or:

(b) To facilitate legal proceedings for cases which "raise a question of principle" (as noted in paragraph 5.12(a) of the Consultation Paper).

1.3 It would be grossly unfair for any particular data user to in effect be required to bear the burden of funding legal proceedings brought for the public benefit in order to deter contraventions of the PDPO (particularly in cases where the alleged contravention in question is commonplace among data users or among data users in a particular industry) or to settle a legal principle.

2. *Liability for costs*

2.1 The Consultation Paper does not address the issue of the data user's legal costs in circumstances where the data user is found by the relevant court not to have contravened the PDPO (and therefore not to have any liability to compensate the data subject under Section 66).

The CIC has no objection in principle to aggrieved data subjects having access to legal assistance, including public funds, in instituting legal proceedings pursuant to Section 66 of the PDPO, provided that liability for the payment of costs is based on the model provided by the Legal Aid Ordinance, specifically Section 16C. i.e. that where a court or the Court of Final Appeal makes an order for costs against a legally assisted data subject, or an agreement is entered into for the payment of costs by a legally assisted data subject in favour the data user, then the Hong Kong Government will be liable for payment in each case.

The above summaries our views and suggestions, and should you require any further input from us on the same, please feel free to let us know.

Yours faithfully,

(Signed)

Keith Kerr
Chairman
Construction Industry Council

S0171

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Personal Data (Privacy) Ordinance Review

01/12/2009 20:24

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Asst. Sec. (Constitutional and Mainland Affairs) 4B

Dear Sir/Madam,

Please find attached my submission. My apologies for it being a day late.

Yours sincerely,

Graham Greenleaf
--
--
Graham Greenleaf
Professor of Law

%Greenleaf_submission.pdf

Making Hong Kong's data protection law effective

A submission to the Hong Kong Constitutional and Mainland Affairs Bureau

Professor Graham Greenleaf
Co-Director, Cyberspace Law & Policy Centre
Faculty of Law, University of New South Wales
Formerly Distinguished Visiting Professor (2001-2)
Faculty of Law, University of Hong Kong

30 November 2009

The Hong Kong Constitutional and Mainland Affairs Bureau has released a *Consultation Document on Review of the Personal Data (Privacy) Ordinance* (August 2009), calling for submissions. The following submissions address only the proposals raised in the Consultation Document, not other issues under the Ordinance that need reform, such as the question of data exports and the need to bring s33 into force.

Proposal No 1 – Biometric information

The Consultation Document says 'Given the challenges posed by the development of biometric technology on an individual's privacy, as a start we may consider classifying biometric data (such as iris characteristics, hand contour reading and fingerprints) as sensitive personal data'. It is not clear whether they propose to consider other categories, but since they do not mention any, it seems unlikely.

The approach suggested is only to limit the collection of what is deemed 'sensitive', not to impose more stringent requirements on use and disclosure once collected, so it is a very limited proposal.

Submission 1(a): Other categories of information should be included under 'sensitive information', not only biometric data, as is common in the data protection legislation of other jurisdictions. This should at least include medical data, and information about sexual practices, sexual orientation, race and ethnicity.

Submission 1(b): More stringent requirements on use and disclosure should be imposed on sensitive information once it is collected.

Proposal No. 2: Data Processors

The Discussion Paper says that 'at present, the [Ordinance] does not regulate processors which process personal data for data users', and therefore proposes that

> ... a data user who transfers personal data to a data processor for holding, processing or use, would be required to use contractual or other means to ensure that his data processor and any sub-contractors will take all practicable steps to ensure the security and safekeeping of the personal data, and to ensure that the data are not misused and are deleted when no longer required for processing.

This would be valuable, but only of limited use in Hong Kong because it retains the doctrine of privity of contract, and the data subject will not be able to sue to enforce the contract or obtain remedies for its breach, particularly if the processor is outside Hong Kong.

A more robust option under consideration is

> ... we can consider directly regulating data processors by imposing obligations on them. They would be required to exercise the same level of due diligence as the data user with regard to security, retention and use of the personal data thus entrusted.

Imposing obligations directly on the processor is a much more direct solution, and much more valuable to data subjects if they can simply enforce the data protection Principles against the processor, but that is subject to the processor being within the territorial or extra-territorial scope of the Ordinance. A further strengthening would be to make the principal vicariously liable for the actions of the processor.

Submission 2(a): Data subjects should be able to enforce the data protection Principles directly against the processor.

Submission 2(b): In order to deal with the problem of processors located outside the jurisdiction of the Ordinance, it should make the principal (data user) vicariously liable for the actions of the processor.

Proposal No. 3: Personal Data Security Breach Notification

The Consultation Paper merely says 'we consider it more prudent to start with a voluntary breach notification system', a conclusion which seems at odds with the very high levels of large scale data breaches in both the public and private sectors that have taken place in Hong Kong over the last three years.

Submission 3: Data breach notification should be made compulsory.

Proposal No. 4: A role in criminal offences for the Commissioner

The Consultation Document does 'not see a strong case to give the PCPD the power to investigate into and prosecute criminal offence cases' and this seems correct.

Submission 4: The PCPD should not be given the power to investigate into and prosecute criminal offence cases.

Proposal No. 5: Legal Assistance to Data Subjects under s66

The Consultation Document invites views 'on whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject'. The New Zealand Commissioner can recommend that legal aid be provided to complainants. However, the main issue in Hong Kong is the provision of some alternative forum in which compensation can be obtained without complainants having to go to a Court.

Submission 5: The PCPD should be conferred the power to provide legal assistance to an aggrieved data subject.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

The Consultation Document invites views on 'whether it is appropriate to introduce an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects' while being clearly of the opinion that this is not appropriate.

Although allowing the PCPD to award compensation would be better than the current non-functioning system via the Courts, there are good reasons not to combine the mediating function and the adjudicative function. The real problem, which the

Constitutional and Mainland Affairs Bureau does not seem to appreciate, is that the Hong Kong Commissioner does not mediate in complaints, particularly not to obtain compensation, in contrast to Commissioners in most other jurisdictions. The Ordinance needs to be changed to give the Commissioner a specific function of mediating in this way.

An alternative to allowing the Commissioner to award compensation, one which works best in New Zealand with its Human Rights Review Tribunal (HRRT), is to have a low-cost quasi-judicial tribunal that can make compensation payments, with the Commissioner referring matters to it that cannot be mediated, and preferably with some agreed statement of facts etc so that the matter does not have to be heard *ab initio*. A similar approach operates in New South Wales and Victoria with their administrative tribunals (NSWADT and VCAT). One quasi-judicial tribunal in Hong Kong that could be empowered to award damages may be the Administrative Appeals Board. This would involve giving a body which normally deals with appeals a 'first instance' function of deciding damages, but there is no obvious alternative in Hong Kong if the Commissioner is not considered appropriate, and the existing provision before a Court under s66 has failed.

Submission 6(a): Consideration should be given to whether the Administrative Appeals Board or another low-cost tribunal in Hong Kong could be given the function of deciding compensation claims for breaches of Principles in the Ordinance.

Submission 6(b): If the proposal in Submission 5(a) cannot be met, the Commissioner should be empowered to award compensation.

Proposal No. 8: Unauthorized dealings in Personal Data

The Consultation Document says that 'to curb irresponsible dissemination of leaked personal data, we may consider making it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes'. A reform such as this should not be very contentious. The PRC and Vietnam have already passed such laws during 2009.

Submission 8(a): It should be an offence if a person obtains personal data without the consent of the data user and (i) discloses the personal data so obtained for profits or malicious purposes; or (ii) holds the data with such intent.

Submission 8(b): It should be presumed that a person who obtains personal data without the consent of the data user did so with the requisite intent, so the onus is on the defendant to rebut such a presumption.

Submission 8(c): It should also be an offence for anyone to sell such personal data for profit whether or not they obtained it from the data user (if this is not already implied in the proposal).

Proposal No. 9: Repeated Contravention of DPPs

The Consultation Document proposes the hypothetical problem of a data user who breaches a DPP but then complies with subsequent enforcement notice, but then subsequently breaches the DPP again in the same way. It would seem reasonable that such a subsequent breach of a DPP could be an offence.

Submission 9: Subsequent breach of a DPP could be an offence, as proposed.

Proposal No. 10: Monetary Penalty for Serious Contravention

Although it is not common for non-judicial bodies to have the statutory power to impose monetary penalties, the Consultation Document proposes consideration being given to empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. Again, this type of 'administrative penalty' is not uncommon in other jurisdictions, and is found in Macao and in the current proposals by the Australian government.

Submission 10: The PCPD should be empowered to require data users to pay monetary penalty for serious contravention of DPPs.

S0172

高永昊

電話：（刪除）

香港下亞厘畢道
中區政府合署東座 364 室
政制及內地事務局（第 4 組）

敬啓者：

檢討《個人資料（私隱）條例》的諮詢

本人希望貴局檢討現時電訊服務商及互聯網服務供應商把使用簽約流動電話的使用者視爲已年滿 18 歲成人及使用該流動電話號碼是持有該流動電話號碼持有人本人出現以下問題：

使用簽約流動電話並非全是成年人

- 使用簽約流動電話並非全是與流動電話公司(電訊商)簽約上台的成年人，有部份使用者是未滿 18 歲青少年及兒童，他們自己不能簽約上台，需要父母簽約上台給他們使用流動電話，部份兒女雖然已年滿 18 歲，但如有精神問題，行爲不能自控，亦需要父母親友簽約上台，限制他們使用流動電話費用不超出預算。現時提供色情訊息的電訊服務商及互聯網服務供應商是不會要求客戶提供其它個人資料核實使用戶，單憑客戶提供簽約流動電話號碼就可登記成爲會員，提供如廣告(附件一)所述性愛錄音，成人色情短片及圖片，使未滿 18 歲青少年及兒童可得到成人色情資訊，違反淫褻及不雅物品管制條例。

使用簽約流動電話並非與電訊商簽約上台客戶本人

- 使用簽約流動電話並非全與電訊商簽約上台客戶本人，電訊服務商及互聯網服務供應商不要求客戶提供其它個人資料核實使用者身份，單憑客戶提供簽約流動電話號碼就可登記成爲會員，提供資訊，收取昂貴資訊費，超出使用人負擔能力，由於可收取昂貴資訊費，亦出現提供資訊以虛假交友訊息，向流動電話持有人騙取資訊費，本人附上向消費者委員會投訴信(附件二)以供參考。客戶到電訊商簽署的合約上，電訊商是會提供信貸予客

戶使用流動電話，但電訊商並沒有寫出一個客戶可負擔及合理的信貸額，電訊服務商及互聯網服務供應商是以電訊商的信貸額提供是增值服務予客戶，如果電訊商不提供信貸予客戶，如已沒有預付值的電話卡，電訊服務商及互聯網服務供應商是不會提供增值服務的，電訊商爲電訊服務商及互聯網服務供應商向客戶收取增值費用，是在香港發展另一交付系統，可能並不完全符合附合電訊條例內所訂電訊商可提供信貸要求，需要檢討(一)電訊服務商及互聯網服務供應商向客戶收取費用，應該每次提供服務收取，如巴士費、地鐵車費；(二) 在客戶仍有簽約剩餘分鐘、接收及發出訊息的情況下，電訊商爲了代電訊服務商及互聯網服務供應商向客戶追收取費用而把客戶流動電話停台，是抵觸[基本法]所訂立自由通訊，電訊商是應該提供二個賬戶給客戶，一個賬戶計算簽約使用分鐘、接收及發出訊息，另一個賬戶用作計算爲代電訊服務商及互聯網服務供應商向客戶收取費用，以符合[基本法]所訂定自由通訊不受阻礙。

(已簽署)

高永昊 謹上
2009 年 11 月 30 日

附件

附件一　色情訊息廣告
附件二　給消費者委員會投訴信

(不連附件)

香港房屋經理學會
The Hong Kong Institute of Housing

S0173

30 November 2009

Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road,
Hong Kong Institute of Housing By Mail and Fax:

Dear Sir,

I refer to the consultation paper "Public Consultation on Review of the Personal Data (Privacy) Ordinance" issued in August 2009. The Hong Kong Institute of Housing would like to respond as follows:

Sensitive personal data

Should the Government subject sensitive personal data, such as fingerprints, to more stringent regulation?

First of all, we wish to know how stringent the regulation is. For better management of a building/estate, the property manager must keep a register of owners which contains some sensitive information such as the names appearing on the ID card/passport, ID number/passport number, contact telephone number and the contact person in case of emergency. The names and ID number of owners are used for ensuring the validity of the owners/proxies in the owners' meeting. The telephone number of owner/occupant/contact person is used for contact in emergency.

In view of the development of intelligent buildings, the finger prints of owners/occupants will be collected for identification for the right of access.

In an owners' meeting, the attendance record showing the names of the owners/occupants may be requested for disclosure. To ensure the owners' meeting is conducted in a proper way in accordance with the Building Management Ordinance Cap344, a property manager may video-tape the whole meeting for record purpose. We wish to know if these records could be regarded as sensitive data and the property manager may refuse the request of the third party for inspection of these records.

If the regulation is too stringent, the quality of the management of a building/estate will, to a certain degree, be affected.

Data Security

Should the Government regulate data processors entrusted with handling of personal data?

S0173

It depends on how the government regulates the data processors. If the government intends to exercise a stringent regulation, the details must be made known to the public. A property manager must be sure about what can be done or cannot be done and explain to the owners/occupants clearly. In most of the circumstances, a guideline is sufficient.

Should the Government require data users to notify the PCPD and affected individuals of personal data leakage incidents?

A professional property manager always keeps alert on the protection of personal data. However, there may be personal data leakage by accident. We are of the view that the PCPD must be notified of any personal data leakage by accident but we have reservation on notifying the affected individuals of personal data leakage incidents as it may arouse unnecessary panic.

Powers of the PCPD

Should the Government give the PCPD criminal investigation and prosecution power?

We guess that most of the personal data leakage incidents are caused by carelessness. If the leakage is a deliberate and malicious act, the crime could be investigated and prosecuted by the police. There is no obvious reason for PCPD to take over the power from the police.

Should the Government empower the PCPD to provide legal assistance to an aggrieved data subject who suffers damage by reason of a data user's contravention of a requirement under the Ordinance and intends to institute legal proceedings against the data user?

We are of the view that the self help principle should prevail in this situation. If the aggrieved subject who suffers damage by reason of a data user's contravention of a requirement under the Ordinance, he has to show sufficient evidence that the damage is substantial and the damage does cause by the contravention. If legal assistance from PCPD is available, it only encourages "aggrieved data subject" who claims to suffer damage, though insignificant in nature, initiating legal action. For property management's point of view, the legal actions may mean additional burden to the management and the owners of the whole building/estate. Such legal actions damage the working relationship of the manager and the owners.

Should the PCPD be empowered to award compensation to an aggrieved data subject?

We consider the proposal is not advisable. It only prompts the data subject to make unfounded or unreasonable complaints.

Offences and Sanctions

Should the Government make contravention of a Data Protection Principle an offence?
Should the Government make it an offence when a person discloses for profits or malicious purposes personal data obtained from a data use without the latter's consent?
Should we make it an offence when a data user intentionally resumes the same contravening act shortly after complying with an enforcement notice issued by the PCPD against him?

S0173

We support making abusing the use of or malicious acts on personal data an offence.

Should the Government empower the PCPD to impose monetary penalty on serious contravention of Data Protection Principle?

There is no obvious reason to empower PCPD to impose monetary penalty on serious contravention of Data Protection Principle. We do not see the rationale of taking the power from the court to PCPD.

Should the Government impose heavier penalty or repeated non-compliance with an enforcement notice?
Should the Government raise the penalty for misuse of personal data in direct marketing?

We support the proposals.

Rights of Data Subject

Should the Government empower a third party to give consent to the change of use of personal data of a minor or a mentally incapacitated person?

We support the proposal. It helps to mollify the worry of an estate manager in collecting personal data from a minor or a mentally incapacitated person. For minor, it is still easy to spot by checking the ID card but for mentally incapacitated person, it is not easy. A property manager, if not handle with utmost care, may fall into another trap of Discrimination of Handicapped.

Should the Government permit a data user to refuse a data access request made by parents on behalf of a minor when compliance with the request is not in the minor's best interest?

For property management industry, there are seldom such cases.

Exemption from the PDPO

Should the Government grant exemption to law enforcement agencies and rescue and relief agencies for handling personal data in emergency situations?

We support such proposal. It is for the best benefit of the data subject, especially in emergency situation such as fire, gas leakage or domestic accidents.

Should the Government allow data users to transfer personal data of minors that re relevant to parental care and guardianship to parents or guardians?

For property management, we seldom come across this situation.

Yours faithfully,

(Signed)

Henry Chan
President
Hong Kong Institute of Housing

就個人隱私條例修訂作出建議。 (P1)

① 現行沒有法例規管私人竊聽電話，但部有法例監管公職人員竊聽。這樣造成不平衡現象，有錢人可以邀請私家偵探長期偷聽，甚致對目標人物進行控制、軟禁、以求達到目的。

我建議政府必須將偷聽電話刑事化，以便私隱專員進行刑事調查。同時，對偷聽人士必須進行重罰(e.g. 監禁5年或以上)。

② 不當地使用個人資料(如：偷聽電話、偷錄他人生活影像、偷拍照片)必須刑事化，警方犯事者，必須嚴罰，監禁。特別是對主事人(用錢收買目標人物資料)予以重罰。

③ 偷盜個人財物是刑事行為，偷盜個人資料及不當地使用，都必須視為刑事犯法行為，予以監禁。

④ 管有偷聽工具即屬違法。我曾經在地鐵站使用手提電話被人"白線"(偷聽)。這私人電話一直24小時跟進，竟不間斷我家中電話，我母親家中電話長期被人偷聽。

建議藏有或管有偷聽工具必須領有牌照；沒領牌照即屬違法及監禁。

⑤ 盜取及使用(未得當事人同意)個人資料罪行，必須為刑事罪行，同時經刑事調查，才能取得逮捕及起訴令狀，將一干人等純為事之前後左右拿走問話，及搜查其電腦，及找拿走電腦，及

S0174 (P2)

本秘書台（請將電話號碼，聯絡人姓名，若可以，請詳細請出資料給秘書台，也或可以從手机中顯示出有關資料.）

（署名來函）

30 Nov 2007

（未能確定來信人是否願意公開姓名）



To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Re: PDPO consultation

07/12/2009 12:47

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

History: This message has been replied to.

I am sorry for my late response, but I hope it can be included

Thanks

Submission on the Review of the Personal Data (Privacy) Ordinance

Professor John Bacon-Shone
Former chairman, LRC subcommittee on privacy
Director, Social Sciences Research Centre
The University of Hong Kong
Pokfulam Road
Hong Kong

General Point

I am disappointed that the government has failed to honor the commitment it gave to the Legco Home Affairs panel on February 9th, 2007 to respond to all the reports of the Law Reform Commission (LRC) on privacy. In particular, other than the commitment to address stalking in the 2009-10 policy address, the recommendations of the LRC on interception of communications (other than Law Enforcement Agencies (LEA)), covert surveillance (other than LEAs), media intrusion and civil torts of privacy have not yet been addressed. In particular, the civil torts arguably provide a better solution for some of the problems raised in the consultation document, but they are ignored.

Proposal #1 Sensitive Personal Data

As made clear in the LRC report, sensitive personal data is a difficult concept because of the cultural dependence. However, it is feasible to look at the problem in a different and more useful way. The major concern for personal data is the possible consequences of errors or leakage of the personal data. Consequences can be divided into different types including the following:

a) Identification/authentication: these consequences are important as identity theft can lead to serious financial and social consequences, especially if the personal data cannot be easily changed, such as biometrics.
b) Reputation: these consequences are primarily social, but can be devastating, especially if they cannot be easily changed, such as HIV status.
c) Location: the right to be left alone is a core element of privacy and personal data that enables the location can lead to security problems and even serious risk to life and limb in the case of abused persons, such as wives at risk from husbands.
d) Group identification: this is not usually considered to be serious, but for certain groups, such as Jews, they have historical

justification for being concerned about this personal data being leaked.

As the consequences may be very different for different individuals, it is problematic to provide weaker protections for any class of personal data, but there may be a case for providing restrictions on the collection and storage of particular types of personal data because of the consequences, but sensitivity alone is not a useful basis for those distinctions.

Proposal #2 Data processors and sub-contracting

While there appears no good reason for excluding data processors from regulation under the PDPO, it is important to recognize that the failure of the government to implement any cross boundary data flow restrictions means that regulating data processors will not help if the data processing has been outsourced outside Hong Kong. Hence, it is critical for the protection of the personal data of Hong Kong residents that the government requires data users to take all necessary measures including contractual measures to protect any personal data that they transfer to data processors.

Proposal #3 Breach notification

It is important to distinguish between different levels of breach, namely: breach of security, known loss of personal data and known use of leaked personal data. Unfortunately, the first level of breach has become so common that notification may not be helpful, whereas the third level of breach clearly needs immediate notification to all affected data subjects. The consultation document is not a balanced presentation of the situation. It is essential that the regulator be notified of all significant breaches, subject to a clear statement by the regulator of what is the necessary level of breach to be reported. It is also essential that the regulator can determine for which breaches the data user needs to inform the data subjects.

Proposals #4-12

These proposals, other than #5 (PCPD to provide legal assistance to data subjects) are contrary to the original vision of the PCPD as a body independent of government that is focused on education and support. I believe that proposal #5 deserves strong support, so that data subjects, who likely cannot afford to fight expensive legal battles against wealthy data users will be able to take action against data users that have caused

or allowed damage to data subjects. What is missing from the discussion in the consultation document is mention of the privacy torts, which would provide much broader mechanisms to protect privacy that go beyond the narrow confines of the PDPO. One problem with legal action is that it may lead to further privacy damage to the data subjects, so mediation leading to compensation would be an excellent addition to these processes. The combination of legal assistance, mediation and the privacy torts would provide the much-needed tools to balance the positions of data subjects and data users.

Proposal #13 Third party consent

While I support the general thrust of this proposal, it does not fully take into account the autonomy of adolescents to make their own decisions. It is clear from the research literature that adolescents are capable of making many decisions themselves, when they are given adequate time and information to make that decision.

Proposal #14 Parents right of access

My concerns over the autonomy of adolescents also apply to this proposal. For example, what if the adolescent is already married? Surely we would not expect the parent's right of access to override that of a married 17-year-old child?

Proposal #25/26/27 Provision of data on health/emergency grounds

I strongly support an amendment to make it clear that transfer can take place where the benefits to the well being of the individual clearly outweigh the privacy intrusion and the disclosure is proportionate and the process is clearly specified and approved by the PCPD. However, in the case of minors, it is again important to take into account the autonomy of adolescents as opposed to small children who may not be able to understand the issues.

A2 IP addresses

I am concerned that the discussion of this item is incomplete. The discussion does not consider the case that for some individuals, IP addresses and email addresses may well be personal identifiers, while for other individuals, they may not. Unlike say a mobile phone number, there is a mechanism for converting an IP address back to a specific computer attached to that address, so the analogy is poor. Also, email addresses

may contain a full name and hence be a personal identifier. It is essential to take into account how the data is being used. If it is not being used in a way that facilitates identification of other personal data, there is little concern, but if it is being used to trace an individual, the PDPO should be relevant.

B2 Public Domain

It is clear to me that there are already problems in Hong Kong with reuse of personal data in public registries and it would be unwise to weaken the protection of personal data in those registries.

C3 Public Hearing

I believe that the logic of the LRC still holds today. It is unclear the public has any right to know the full details of any hearing. However, I strongly support the PCPD issuing reports on investigations that properly protect the personal data of the individuals concerned.

41 Duty to prevent loss

I believe this highlights an important clarification, which is much needed, given the frequent losses of personal data that have taken place in recent years.

Mandatory Provident Fund Schemes Authority

S0176

強制性公積金計劃管理局
MANDATORY PROVIDENT FUND SCHEMES AUTHORITY

FAX

Date: 9 December 2009

IMPORTANT: This transmission is intended for the addressee only. If you have received this transmission in error, please notify us immediately and destroy the transmission without using, copying or disclosing it or its contents to anyone. Any comments or information contained in this transmission that do not relate to our official business shall not be construed to be expressed or endorsed by the Mandatory Provident Fund Schemes Authority.

To:	From:
Secretary for Constitutional and Mainland Affairs	M(CA)1
Attn: (Attn: Miss Joanna C H Choi)	Phone: (deleted)
Phone: (deleted)	Fax: (deleted)
Fax: (deleted)	Our Ref: (deleted)

Total no. of pages (including this page): 7

Please contact (deleted) at (deleted) if message received is incomplete.

☐ Urgent ☐ For information ☐ For advice ☐ For consideration ☐ Please follow up ☐ Please reply

Message:

同心機構
caringorganisation 2008-09
Awarded by The Hong Kong Council of Social Service
香港社會服務聯會嘉許

強制性公積金計劃管理局
MANDATORY PROVIDENT FUND SCHEMES AUTHORITY

S0176

電話號碼 Tel. No. : (deleted)
傳真號碼 Fax. No. : (deleted)
本局檔號 Our Ref. : (deleted)
來函檔號 Your Ref. : CMAB/CR/7/22/40 Pt.7

BY FAX

9 December 2009

Secretary for Constitutional and Mainland Affairs
(Attn: Miss Joanna C H Choi)
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Dear Miss Choi,

Consultation Document on
Review of the Personal Data (Privacy) Ordinance

Thank you for inviting the comments of the Mandatory Provident Fund Schemes Authority on the captioned Consultation Document. I enclose our comments for your consideration.

Please accept our apologies for being late in our response.

Yours Sincerely,

(Signed)

(Alice Tang)
Manager
Corporate Affairs Department

Encl
3/6

同心展關懷
caringorganisation 2005-09
Awarded by The Hong Kong Council of Social Service
香港社會服務聯會頒授

S0176

Mandatory Provident Fund Schemes Authority ("MPFA")

Comments on the Consultation Document on Review of the Personal Data (Privacy) Ordinance issued by CMAB in August 2009

After reviewing the Consultation Document ("CD") in the light of operational experience and considering the implications of the proposed amendments to the Personal Data (Privacy) Ordinance ("PDPO") on the operations of the MPFA, we set out our views and comments below.

General Comments

- As indicated in the Executive Summary of the CD, one of the guiding principles for the review is that the right of individuals to privacy must be balanced against other rights and public and social interest. We support this principle.
- In our past experience, we find that in pursuing some initiatives for the benefit of members of the public, the collection of certain personal data is necessary. For example, in order to offer better services to members of the public by allowing them to access their account details via an Interactive Voice Response System or the Internet, it is desirable to collect a number of personal identifiers for added security in verifying their identity before the information is released. In interpreting whether the data collected are excessive, the benefit made available to the public should be taken into consideration. The collection of more than one personal identifier in the above example is in fact in the interest of the public as it will give added assurance that the persons enquiring account information are actually the account holders themselves. Flexibility should be exercised when the wider public interest overrides the protection of an individual's personal data.

Comments on Specific Proposals

Proposal No. 1: Sensitive Personal Data (page 10 of CD)

- Under the proposal, "sensitive personal data" should be subject to more stringent data protection requirements. Without a clear definition of "sensitive personal data", we cannot assess the implications of the proposal on the MPFA.
- If the proposal is to be pursued, the term "sensitive personal data" must be clearly defined. It would also be useful to define the term "vital interests" in paragraph 3.09(c) of the CD.
- Under the proposal, the collection, holding, processing and use of sensitive personal data would be prohibited unless with the prescribed consent of the data subject. We suggest considering whether the inability to obtain sensitive personal

data due to lack of prescribed consent can be a defence to liability under the discrimination ordinances.

Proposal No. 2: Regulation of Data Processors and Sub-contracting (page 16 of CD)

- We support the suggestion that the activities of a data processor (e.g. a sub-contractor, who processes personal data for a data user) should be directly regulated under the PDPO (paragraph 4.21(b) of the CD).
- Currently, the PDPO governs data users only. Data processors are at best bound by contractual arrangements with their principals (i.e. the data users) to handle personal data with care. By making it a legal obligation for them to observe data protection requirements, data processors would be given an added impetus to protect the security of the personal data transferred to them for handling.

Proposal No. 3: Personal Data Security Breach Notification (page 25 of CD)

- We are generally in support of the voluntary privacy breach notification proposal to require data users to notify the Privacy Commissioner for Personal Data ("PCPD") and affected individuals when a breach of data security leads to the leakage or loss of personal data.
- It is necessary to set out clear guidelines on the notification mechanism, such as the type/nature of events that warrants a notification, the content to be covered, the timing and the means of sending the notification, etc.
- While the notification mechanism clearly applies to breaches by a data collector, it should be clarified whether the mechanism also covers breaches by a third party to whom personal data are transferred.
- We support the mechanism in paragraph 4.41 that allows notification by alternative means, such as posting notices in newspapers instead of regular mail, when the number of individuals to be notified is large or the cost for individual notification is extraordinary. Such means can also cater for scenarios when the data subjects' addresses are not updated. We suggest clarification on whether individuals can be partially identified in such notices (e.g. by showing part of their HKID number).

Proposal No. 7: Making Contravention of a Data Protection Principle ("DPP") an Offence (page 38 of CD)

- Currently, little action can be taken against a breach of a DPP. This can lead to abuse and tougher sanctions are supported.
- However, as mentioned in the CD, DPPs are couched in generic terms and can be

subject to a wide range of interpretations. If contravention of a DPP is made an offence, the PCPD must give specific, clear and detailed guidance to the public on what will constitute a contravention of a DPP.

- The following example can illustrate the problems associated with the interpretation of the generically drafted DPPs:
  - Under section 8(1)(d) of the PDPO, the Commissioner is empowered to examine any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal data and report the results of the examination to the person proposing the legislation.
  - When a regulator proposes changes to a piece of legislation, it normally has a thorough understanding of the operational environment and public sentiments.
  - The Commissioner and the regulator in performing their respective roles may have conflicting views on the proposed legislation in relation to personal data. For example, after gauging the views of stakeholders and reaching consensus with them, as well as paying attention to the DPPs in the PCPO, the regulator (i.e. the data user) may consider it necessary to proceed with legislative proposals empowering it to collect sufficient amount of personal data to facilitate future authorized disclosure of the data to the data subjects. The Commissioner may however consider that the proposed collection and disclosure of such amount of personal data excessive, thus contravening DPP1(1)(c). In that predicament, it could be difficult for the regulator and the Commissioner to come to an agreement due to the following:
    (1) DPPs are couched in generic terms and can be subject to a wide range of interpretations, so any issues concerning collection and use of personal data could be qualitative in nature subject to individual judgment (e.g. sufficient vs excessive)
    (2) while the Commissioner is the expert in the area of protection of privacy of individuals, the regulator concerned, after having gauged the views of stakeholders through consultation, should know best what the needs of the community as a whole are in the particular setting
  - When the PCPD is considering making contravention of DPPs an offence, as a side issue, it would be most useful if the PCPD would take the opportunity to devise means to resolve the possible conflicts set out above, for example by issuing guidance notes on their examination of proposed legislation for the guidance of regulators.

- The above example also shows that it might be desirable for the PDPO to be relaxed in situations where the wider public interest overrides the protection of an individual's personal data.

Proposal No. 16: Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation (page 55 of CD)

- As stated in the CD, sections 20 and 28(5) of the PDPO stipulate various grounds under which a data user can refuse to comply with a data access request under section 19 of the PDPO. However, the grounds for refusal do not cover the situation where a data user is obliged or entitled under any other ordinances not to disclose the personal data.
- Section 41(1) of the Mandatory Provident Fund Schemes Ordinance ("MPFSO") stipulates that a person who obtains information in the exercise or performance of the MPFA's statutory functions:
  (a) must not disclose the information to any other person, unless the disclosure is necessary in order to exercise or perform those functions; and
  (b) must not enable another person to have access to the information, except in so far as that access is necessary to allow that other person to exercise or perform functions under or for the purpose of MPFSO.

  The application of section 41 of the MPFSO is subject to the exemptions in sections 41 and 42 of the MPFSO.
- If a data access request is received which requests the MPFA to disclose personal data obtained in the exercise or performance of its statutory functions, the MPFA may breach the data access provision of the PDPO when complying with the "secrecy requirement" of MPFSO.
- In view of the competing legislative requirements under the PDPO and the MPFSO, we agree with the proposal of providing a new ground for a data user to refuse to comply with a data access request under section 20(3) of the PDPO where the data user is obliged or entitled under any other ordinances not to disclose the personal data.

Proposal No. 17: Erasure of Personal Data (page 56 of CD)

- According to Section 26 of the PDPO, a data user shall erase personal data held by it where the data are no longer required for the purpose for which the data were used unless such erasure is prohibited under any law or it is in the public interest that the data are not to be erased. DPP 2(2) also requires that personal data shall not be kept longer than is necessary for the fulfillment of the purpose for which the data are to be used.

- We agree with the example quoted in the CD that, in certain situations, it may not be practicable for the data user to erase only obsolete personal data (e.g. when the data form only a part of a document). We therefore support the proposal to amend the PDPO so that the provisions concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use.

Proposal No. 33: Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings (page 81 of CD)

- According to DPP3 of PDPO, personal data shall not be used for any purpose other than the original purpose of collection or its directly related purpose unless prescribed consent of the data subject is obtained. The use of personal data required or authorized by or under law, by court orders, or related to legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights is not exempted from DPP3. As it is reasonable and legitimate for data users to change the use of personal data in such circumstances, the CMAB/PCPD propose to create an exemption from DPP3 for such use of personal data so that a data user would not run the risk of contravening DPP3 in such circumstances.
- We support the proposed exemption. Section 41(2) of the MPFSO does not prevent the disclosure of, or the provision of access to, information in accordance with an order of a court or in accordance with a law or a requirement made under a law. The MPFA also uses personal data in bringing legal actions against parties that breach the MPF legislation. Without the proposed exemption, the legitimate use of personal data in these circumstances may constitute a breach of DDP3. This anomaly can be resolved with the introduction of the proposed exemption.

Mandatory Provident Fund Schemes Authority
9 December 2009

S0177

Wharf T&T Limited
九倉環球有限公司



Direct Fax No: (deleted)
Direct Tel No: (deleted)

10 December 2009

Team 4, Room 364,
East Wing Central Government Offices
Lowe Albert Road, Hong Kong

By Facsimile

Dear Sirs,

Public Consultation on Review of the Personal Data (Privacy) Ordinance

We enclose our views on the consultation on the review of the Personal Data (Privacy) Ordinance. Please do not hesitate to contact us if you have any queries in relation to our submission.

Yours faithfully,

(Signed)

Agnes Tan
Vice President
Legal, Regulatory and Carrier Affairs

Encl.

Submission to CMAH on PDPO_DIAec09(2)



& IT services subsidiary



S0177

Wharf T&T Limited's Response to Key Proposals of the Public Consultation on Review of the Personal Data (Privacy) Ordinance

1. **Proposal No. 2 – Regulation of Data Processors and Sub-contracting Activities**

We believe the initiative of this proposal meant well, however given the increasing trend of outsourcing data-processing work by Hong Kong organizations to offshore contractors/sub-contractors, the proposal would not extend to cover these offshore processors, thereby rendering the proposal futile. Further we are concerned that the proposed direct regulation on the data processors might in some circumstances create confusion as to who should have the responsibilities to ensure compliance with the Ordinance and who should be held liable for any contravention. In the normal circumstances where data users contract third parties data processors, they would impose obligations under the contract requiring the data processors to take all steps to ensure the proper use and security of the data. Direct regulation on the data processors would not mean the data users would relax the contractual obligations, rather with this proposal, the data processors could find themselves liable under the Ordinance as well as in breach of their contract with the data users. This does not seem fair to us, we therefore do not support this proposal.

2. **Proposal No. 3 – Personal Data Security breach Notification**

We are fairly neutral about this point.

3. **Proposal No. 4 – Granting Criminal Investigation and Prosecution Power to the PCPD**

Since there is already a mechanism to conduct criminal investigation by the police, this would appear to be a waste of public funds to duplicate functions which are already in place.

4. **Proposal No. 5 – Legal Assistance to Data Subjects under Section 66**

We do not support this proposal as there is already an existing mechanism in providing recourse for the aggrieved parties and they can also apply for legal aid if they are eligible for it. Further, we believe the proposal would bring about more claimants. We should not have to spend resources on dealing with vexatious or frivolous claims. We are very concerned that, if the proposal were made into law, it would open a floodgate for claims. As the existing mechanism provides sufficient recourse for the aggrieved and this proposal would not be necessary.

5. **Proposal No. 6 – Award Compensation to Aggrieved Data Subjects**

S0177

Since we do not support that PCPD be conferred the investigative power, by the same token, we take the same stance in relation to awarding compensation to aggrieved data subjects which should be the job of the court, not the PCPD. It is our view that it is more desirable to separate the enforcement and punitive functions.

6. **Proposal No. 7 – Making Contravention of a Data Protection Principle an Offence**

Since an offence is criminal, a breach of which may attract imprisonment. The last thing we wish to see is, for example, an offence is committed as a result of a genuinely inadvertent breach of a DPP. Hence we do not support this proposal.

7. **Proposal No. 8 – Unauthorized Obtaining, Disclosure and Sale of Personal Data**

We welcome the proposal which focuses on curbing "blatant privacy intrusive acts" which can be something like a person *knowingly or recklessly* obtained the personal data without the consent of the data user and discloses the personal data so obtained *for profits or malicious purposes.*. We agree that liabilities should not be imposed on data users in case of accidental leakage, which does not result in substantial harm to the data subjects. We further agree that suitable defense should be provided to strike a proper balance.

8. **Proposal No. 9 – Repeated Contravention of a DPP on Same Facts**

This proposal should only be if the contravention brings about consequences of serious gravity.

9. **Proposal No. 10 – Imposing Monetary Penalty on Serious Contravention of DPPs**

We do not support this proposal on the same ground as per paragraph 5 herein.

10. **Proposal No. 11 – Repeated Non-compliance with Enforcement Notice**

This proposal should only be if the respondent cannot furnish a legitimate defence for repeated non-compliance.

11. **Proposal No. 12 – Raising Penalty for Misuse of Personal Data in Direct Marketing**

Whilst "direct marketing" was quoted by the consultation paper as *"a cause of complaint (under Section 34(1)(ii) of the Ordinance) and nuisance to the data*

S0177

subjects", we should not ignore or underestimate its contribution to the GDP of Hong Kong and its value as an inexpensive means for consumers to access the latest information of products and services.

The review on whether to raise the penalty under Section 34(1)(ii) for the purpose of discouraging uncontrolled direct marketing cannot be treated as an isolated issue or a standalone question. The review should not lose sight of the Guiding Principles of the consultation paper. Guiding Principle A states that, *"the right of individuals to privacy is not absolute... (and) must be balanced against other rights and public and social interests"*. We query if there is any evidence supporting that the balance of privacy right and public interests has been upset by direct marketing and therefore justifies raising the penalty under Section 34(1)(ii) of the Ordinance.

The recent complaint statistics concerning Section 34 or breach of DPP, namely, 59 in 2006, 87 in 2007 and 67 in 2008 alone does not justify adopting Proposal No. 12, especially given that the Unsolicited Electronic Message Ordinance has been in place to regulate direct marketing by means of facsimile transmission and electronic mails and that OFTA is in the process of releasing a code of practice to provide guidance on person-to-person marketing calls.

As such, we do not support this proposal. With direct marketing be annoying as it may, it does have its economic values with regard to provision of job opportunities and information on products and services available to the consumers who are interested in those products and services otherwise.

12. **Proposal No. 24 – Transfer of Personal Data in Business Mergers or Acquisition**

We welcome the proposed exemption from DPP3 for the transfer or disclosure of personal data in intended merger, acquisition or transfer of business, which would be beneficial to the operation and growth of the business sector since mergers and acquisitions constitute very important business activities in Hong Kong. The exemption would streamline the procedures in mergers and acquisitions.

Conclusion

Prior to any amendments being made to the Personal Data (Privacy) Ordinance, considerations of the interests of all relevant parties should be balanced against. While we appreciate the importance of protection of personal data, we hope the legislators would consider carefully the practicality and cost implications for business entities on the implementation of any amendments to the law.

S0178

民主黨立法會議員秘書處
Secretariat of Legislative Councillors of The Democratic Party

政制及內地事務局局長林瑞麟先生：

對檢討《個人資料（私隱）條例》的諮詢文件的意見

回應當局於八月公佈的檢討《個人資料（私隱）條例》的諮詢文件，民主黨就文件內的多項建議提出意見，希望 閣下認真考慮。

若有垂詢，請聯絡研究主任陳惠嬋

民主黨政制政策發言人 何俊仁 劉慧卿
（陳惠嬋代行）
二零零九年十二月十五日

S0178

民主黨對檢討《個人資料（私隱）條例》的諮詢文件的意見

A. 指導原則

1. 諮詢文件列出八項指導原則[1]，指個人資料私隱的保障須因應經濟、科技發展等因素而作出妥協，因此建議亦傾向保守。

2. 《公民權利和政治權利國際公約》第十七條規定，任何人之私生活不得無理或非法侵擾，因此，保障私隱是基本人權，政府應該以保障私隱作爲首要原則，而不輕易作出妥協。

B. 私隱條例的規管範圍

將互聯網規約地址視爲個人資料

3. 雅虎香港於 2003 年向內地政府提交大陸記者師濤發電郵給海外的資料，包括 IP 及電郵地址和發放資料的時間。內地當局基於這些資料起訴師濤，並將他判刑十年，根據《個人資料（私隱）條例》，雅虎披露的 IP 地址並不屬法例所界定的個人資料。可是，若將 IP 地址連同其他可供識別的個人資料，如電郵地址，便可間接確定或追蹤發電郵的人士。

4. 雅虎事件引發的問題是，IP 及電郵地址應否被視爲個人資料。另外，當其他地方的執法機構要求香港機構提交一些個人資料，而該地方沒有和香港相若的法律保障，有關機構是否應該可以引用條例第 58 條，提供個人資料給另一個司法管轄區，作爲偵測或拘捕罪犯之用？

5. 個人資料私隱專員公署（公署）建議將 IP 地址視爲個人資料（建議 A2），但政制及內地事務局（當局）卻不接納。不將 IP 地址視爲個人資料，容許互聯網服務供應商向其他地區政府提供情報，市民私隱得不到保障。

---

[1]八項指導原則包括：

- 必須平衡個人的私隱權與其他權利及公眾及社會利益；
- 必須平衡個人資料私隱與便利資訊及通訊科技持續發展；
- 任何法例的修改都不應削弱香港的競爭力和經濟效率；
- 需避免商業活動和個別資料使用者承受沉重的負擔；
- 應充分考慮本地情況；
- 私隱條例在科技轉變中應具彈性且合時；
- 立法干預未必一定是最有效方法；
- 社會對私隱課題有共識至爲重要。

6. 當局謂若把 IP 地址視爲個人資料，會對資訊科技界帶來不合理的負擔，並會出現嚴重的遵從問題。但有資訊科技界人士表示，業界對將 IP 地址視爲個人資料並不強烈反對。若政府能界定 IP 地址的使用準則，會令業界有規可循，對業界亦是一個保障。

7. 基於以上考慮，當局應跟進公署的建議，諮詢資訊科技界，若將 IP 地址視爲個人資料，應該如何界定詳細的使用準則。

跨境處理個人資料

8. 現時有很多機構在服務的運作過程中，將部份程序轉到其他地方進行，個人資料因而亦被轉移到香港以外地方。這些個人資料在香港以外地方會否受到保障，是一個令人關注的問題。諮詢文件並未就這個問題提出解決方案。

9. 民主黨建議，香港可參考歐洲共同體委員會 108 公約以及 2001 年協議（Council of Europe Convention 108 together with the Protocol of 2001），只有當另一地區的司法制度在個人資料方面能提供足夠水平的保障，香港的資料使用者才可將個人資料轉移到該地區。

C. 敏感個人資料

10. 當局建議把生物辨識資料（如瞳孔特徵、掌紋及指模）列爲敏感個人資料，提供較高程度的保障，把處理敏感個人資料限於指定的情況（建議 1）。

11. 條例沒有區別「敏感」與「非敏感」的個人資料。檢討文件建議修改法例，對敏感個人資料提供較嚴格的保障，例如必須在當事人自願而明確的同意下，才可收集及持有敏感個人資料，民主黨原則上支持這建議。

12. 由於生物辨識資料不能取消或改變，我們認爲應將這些資料列爲敏感個人資料。保障個人敏感資料的私隱，應該是首要考慮因素。對於資訊科技界的顧慮，指加強規管會窒礙生物辨識系統的發展。當局應與資訊科技界商討，在保障敏感個人資料的前題下，提供清晰的界定和指引，減少業界面對的不明朗因素，創造空間，繼續發展生物辨識系統。

D. 資料保安

規管資料處理者及分判活動

13. 諮詢文件提出，在分判個人資料給第三者處理時，資料使用者應透過合約方式，確保分判承辦商採取步驟，確保個人資料不會被不當使用，以及在無需再作處理時刪除。諮詢文件亦提出的另一方案，是直接規管資料處理者（建議 2）。

14. 資料使用者在分判資料給第三者處理時，以合約方式確保對方履行私隱條例所訂的責任，有助加強資料使用者和資料處理者對保障個人資料私隱的責任，但這種間接規管制度未必足夠。我們建議政府提出的兩個方案同時執行。除了規定資料使用者必須和資料處理者就保障私隱訂立分判合約，法例亦直接規管資料處理者有責任遵守保障資料原則。最重要的是，新的規定不應成爲資料使用者將責任推卸給資料處理者的藉口，資料使用者應承擔最後責任。

個人資料外洩通報機制

15. 有建議訂立個人資料外洩通報機制，資料使用者若遺失或外洩個人資料，應通知私隱專員及受影響人士。諮詢文件建議先推行自願性通報機制，專員可就自願通報機制發出指引（建議 3）。

16. 資料當事人在資料外洩後，若能盡快獲得通知，有助其採取措施，減少所受影響。因此，我們認爲應該推行強制性的通報機制。考慮到強制性通報機制對各行業的影響，民主黨認爲，香港可參考美國經驗，按高、中、低風險分類，針對涉及高風險個人資料的行業，如銀行和金融業，先落實推行強制性的通報機制，再分階段在較低風險的行業推行。

E. 私隱專員的執法權力

授予私隱專員刑事調查及檢控權力

17. 諮詢文件提及應否賦予私隱專員刑事調查及檢控的權力（建議 4），民主黨認爲，公署較其他執法機構更了解私隱事務和相關法例，負責刑事調查是合適的安排。此外，對於一些需要緊急處理的個案，即使由專員提出檢控，亦無法及時處理。我們認爲，法例應該容許專員向法庭申請禁制令，令他能在短時間內停止侵犯個人資料私隱的行爲。

爲資料當事人提供法律協助及向受屈的資料當事人給予補償

18. 根據條例第 66 條，若資料使用者違反條例，當事人可索償，但條例沒有

授權專員爲當事人提供法律協助。諮詢文件建議授權專員提供法律協助（建議 5）。文件亦提及應否授權私隱專員，就當事人蒙受損失釐定補償額（建議 6）。

19. 民主黨支持當局的建議，由專員爲當事人提供法律協助，透過法律程序索償。此外，在採用法庭程序前，應考慮由專員公署進行調解，香港可以仿效澳洲的做法，投訴人可要求被投訴人道歉、解釋或作出金錢補償，私隱專員則擔當投訴人和被投訴人的調解人，這樣做可以有效地處理投訴和索償的申請，亦節省法庭的工作。

F. 罪行及制裁

未經授權下取得、披露和出售個人資料，以及重複違反保障資料原則

20. 現時私隱專員可發出執行通知，要求資料使用者採取措施，糾正違反保障資料原則的問題。若資料使用者不遵守執行通知，才會受處罰。諮詢文件提出是否應將違反保障資料原則的行爲列爲罪行（建議 7）。民主黨認爲保障資料原則的字眼涵義廣泛，如果直接將違反保障資料原則訂爲罪行，市民容易誤墮法網，因此並不可取。

21. 諮詢文件建議，任何人在未經當事人同意而取得個人資料，並加以披露，從中獲利或作惡意用途，將被訂爲罪行（建議 8），若資料使用者重複違反保障資料原則，有關行爲亦被訂爲罪行（建議 9）。民主黨認爲，將故意、重複、圖利的行爲訂爲罪行，較爲可取。由於「惡意用途」的定義不清晰，當局需仔細研究外國相關法例的實施情況，才決定是否採用「惡意用途」的概念。

直接促銷中不當使用個人資料

22. 現時法例規定資料使用者如將個人資料用作直接促銷，須通知當事人讓他有權拒絕。如當事人要求停止，但資料使用者卻繼續使用，可被罰款 10,000 元。

23. 個人資料被用作直接促銷的情況非常普遍，不少市民對於被直銷電話滋擾感到不勝其煩。現行條例雖然規定，資料使用者有責任通知當事人他有權拒絕，但是不足以遏止個人資料被用作直銷電話用途。民主黨認爲增加罰款的建議（建議 12）並不足夠，政府應該接納公署的建議，引入新規定，在首次將個人資料用作直接促銷時，必須取得當事人明確同意。

同時，設立全港適用的拒收直接促銷電話中央登記冊。

24. 此外，民主黨建議規定資料使用者在直接促銷時，有責任告知當事人他是如何取得其個人資料，讓當事人有渠道通知資料來源，拒絕繼續接受直接促銷。

G. 資料使用者的權利及義務

25. 諮詢文件建議，資料使用者若根據其他條例的保密條文，有義務或有權不披露個人資料，應豁免依從私隱條例關於查閱資料的條文，拒絕查閱資料的要求（建議 16）。民主黨原則上同意這項建議，但關注有哪些條例容許哪些機構有權不披露個人資料。當局應該提供具體資料，讓社會詳細討論。

H. 新增豁免條文

基於健康理由提供身分和所在地資料、緊急情況下處理個人資料

26. 根據現行法例，爲了防止或減輕對當事人的身體或精神健康造成嚴重損害，條例容許披露當事人的身體或精神健康有關的個人資料，諮詢文件建議擴大豁免範圍，容許披露當事人身分和所在地的個人資料（建議 25）。此外，文件提及，是否應明文規定，執法機關、救援及支援組織在處理意外或其他危及生命的情況時，可獲豁免條例對個人資料搜集和使用的規定（建議 26）。

27. 民主黨原則上同意這些建議，但是我們認爲，必須仔細界定「意外」和「危及生命」，同時應界定哪些執法機關、救援及支援組織可獲豁免。

I. 未成年人的個人資料

父母親查閱未成年人士個人資料的權利

28. 諮詢文件提出，當代表未成年人士的「有關人士」（對未成年負有作爲父母親的責任的人）要求查閱該名未成年人的資料，而資料使用者有合理理由相信依從該項要求並不符合該名未成年人士的最佳利益，資料使用者可拒絕該項要求。相關的例子包括離婚家長向學校查閱子女的所在，加以追踪；父親或母親懷疑虐待子女；子女表明不同意透露個人資料（建議 14）。

29. 民主黨原則上同意這項建議，但認爲應清楚說明哪些情況不符合「最佳利益」。

由第三者訂明同意更改個人資料用途

30. 現時條例沒有條文准許有人代替當事人同意更改其個人資料的用途。政府建議修改法例，若當事人因爲不能充份理解、沒有足夠能力完全理解更改資人資料用途的建議，同時有關的用途對當事人有明確的好處，第三者（包括對未成年負有作爲父母親的責任的人）應被賦權更改資料用途（建議 13）。

31. 民主黨原則上同意建議，容許未成年人的父母或負有父母責任的人，代當事人更改其個人資料。但是，文件沒有提供外國經驗，此外，這項建議是否適用於 18 歲以下人士，政府應該就此提供進一步資料，供社會討論。

爲了履行監護責任和家長照顧責任而轉移未成年人的個人資料

32. 諮詢文件建議設豁免條文，准許資料使用者主動將未成年人的個人資料轉移給父母或監護人，以加強對未成年人的保護，及使父母及監護人可履行照顧和監護兒童的責任。若設豁免條文，應設特定條件，例如，規定必須符合未成年人的最佳利益（建議 27）。

33. 民主黨對這項建議有所保留。首先，文件沒有提供外國經驗或理據，若這項建議是適用於 18 歲以下的人士，政府應該就此提供進一步資料，供社會討論。其次，資料使用者若認爲有需要將未成年人的個人資料轉移給其父母或監護人，應該先行取得該名未成年人的同意。

S0179



04/01/2010 15:34

To pdpo_consultation@cmab.gov.hk
cc
bcc
Subject Privacy protection - consultation document

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

Dear Sir/Madam,

Re the Consultation Document on citizens' Privacy protection, I comment as follows:

Re para. 4.21 (b): I support a regulatory model in which the activities of a data processor should be directly regulated under the PDPO.

Re para. 4.22: I support a personal data security breach notification be instituted to require organisations to notify the PCPD and affected individuals when a breach of data security leads to the leakage or loss of personal data.

Re para. 6.12 (a): I support we make it an offence for a person who discloses for profits or malicious personal data which he obtained from a data user without the latter's consent.

Re para. 6.16 (a): I consider it appropriate to make it an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice.

Regards

(name)



To vchan@cmab.gov.hk
cmabenq@cmab.gov.hk
cc
bcc
12/02/2010 17:08 Subject HKPASEA: Comments on PDPO

☐ Urgent ☐ Return receipt ☐ Sign ☐ Encrypt

敬啓者

-

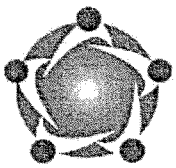
謹附上本會就檢討個人資料(私隱)條例之意見書，以茲參閱。

-



HKPASEA_22_Comments_On_PDPO.pdf

S0180



HONG KONG PROFESSIONALS AND SENIOR EXECUTIVES ASSOCIATION

香港專業及資深行政人員協會

檢討《個人資料（私隱）條例》諮詢文件

意見書

2010年2月

香港專業及資深行政人員協會 S0180

2009/2010 年度理事會成員

會長：	容永祺先生, MH, JP	
常務副會長：	胡曉明先生, JP	
副會長：	陳建強醫生	陳世強律師
	陳紹雄工程師	何順文教授
	詹志勇教授, BH, JP	林大輝博士, BBS, JP
	羅范椒芬女士, GBS, JP	李鏡波先生
	梁美芬博士	林雲峯教授, JP
	盧偉國博士工程師, BBS, MH, JP	吳長勝先生
	伍翠瑤博士	史泰祖醫生, JP
	孫德基博士, BBS, JP	
秘書長：	謝偉銓先生	
財務長：	林義揚先生	
副秘書長：	黃偉雄先生	
理事：	陳茂波先生, MH, JP	陳鎮仁先生, BBS, JP
	鄭國漢教授, JP	邱達根先生
	周伯展醫生	鍾志平博士, JP
	范耀鈞教授, BBS, JP	馮柏棟資深大律師
	何君堯律師	許漢忠先生, JP
	洪克協先生	劉勵超先生, SBS
	劉秀成教授, SBS, JP	李樂詩博士, MH
	李惠光先生	梁家棟博士
	梁建楓先生	梁定宇先生
	莫華倫先生	伍山河牧師
	彭詢元先生, SBS, CSDSM	彭　華先生
	譚偉豪博士, JP	鄧淑明博士, JP
	曾其鞏先生, MH	黃天祥先生, JP
	黃友嘉博士	鄔滿海先生, SBS
	吳德龍先生	楊位醒先生, MH

註：排名依英文姓氏字母排列

HONG KONG PROFESSIONALS AND SENIOR EXECUTIVES ASSOCIATION

香港專業及資深行政人員協會

社會發展委員會

聯席主席：陳建強醫生、陳紹雄工程師

委員：陳記煊先生、何順文教授、劉勵超先生, SBS, 李大拔教授、梁燕城教授、梁永安先生、伍翠瑤博士、伍山河牧師、柯廣輝律師、沈培華博士、譚志偉博士、鄧鳳賢女士、蔡少浩先生、黃偉雄先生、葉惠民教授、郝德芬博士, BH, JP、張沁女士

醫療融資研究小組

聯席主席：陳建強醫生、何順文教授、周伯展醫生

委員：陳記煊先生、陳大信教授、陳偉光醫生、陳一華牧師、卓嘉雯醫生、趙偉仁醫生、朱君璞醫生、秦鈺池先生、何兆煒醫生, JP、管胡金愛女士、林正財醫生, JP、羅裕群先生、李大拔教授、伍翠瑤博士、伍山河牧師、吳國聲先生、沈培華博士、譚志偉博士、曹聖玉女士、吳德龍先生、葉國興醫生

教育政策研究小組

聯席主席：林大輝議員, BBS, JP、羅范椒芬女士, GBS, JP、曾其鞏先生, MH

委員：歐陽敬考博士、張翠先生、朱露茜女士、朱泰和先生、何兆煒醫生, JP、許正宇先生、洪詠慈女士、孔美琪博士、郭文坤校長、李大拔教授、李志剛先生、李允琪教授、梁美智女士、廖子芳女士、雷智欣律師、呂新榮博士、呂宇俊先生、吳宏偉教授、龐劉湘文女士、潘國城博士, SBS, OBE、謝安如博士、蘇俊文大律師、蘇偉文博士、沈培華博士、曾昭學先生、謝伯開先生, MH、楊偉國博士、郝德芬博士, BH, JP、張沁女士

文體政策研究小組

聯席主席：胡曉明先生, JP、曾其鞏先生, MH、楊位醒先生, MH

委員：歐陽敬考博士、曹眾女士、李永康先生、廖子芳女士、駱文輝先生、游錦榮先生、楊志偉先生、葉惠民教授

環境政策研究小組

聯席主席：詹志勇教授, BH, JP、林雲峯教授, JP、梁定宇先生、鄧淑明博士, JP

委員：陳國輝先生、陳博智先生、朱露茜女士、范約翰先生、郭棟強先生、劉勵超先生, SBS、羅范椒芬女士, GBS, JP、羅躍添先生、盧恩澤律師、駱文輝先生、馬振峰先生、潘國城博士, SBS, OBE、葛珮帆博士、張連蕙馨女士、黃天祥先生, JP、黃元山先生、楊凱山先生、楊耀明先生、張敏女士

HONG KONG PROFESSIONALS AND SENIOR EXECUTIVES ASSOCIATION
香港專業及資深行政人員協會

福利政策研究小組

聯席主席：何順文教授、伍翠瑤博士、曾其鞏先生, MH

委員：周驪莉女士、何兆煒醫生, JP、許正宇先生、林正財醫生, JP、潘承進律師、謝安如博士、鄧鳳賢女士、黃綺年女士、黃元山先生、楊耀明先生、余秀珠女士, MH, JP、郝德芬博士, BH, JP

社會企業研究小組

聯席主席：胡曉明先生, JP、郝德芬博士, BH, JP

委員：張洪秀美女士、周伯展醫生、程式藩先生、鍾惠玲博士、紀治興先生、林慧怡女士、李志剛先生、梁美智女士、魏文富先生、潘國城博士, SBS, OBE、譚志偉博士、黃瑞華律師、汪敦敬先生、吳德龍先生、任德煇先生、嚴俊民先生、余秀珠女士, MH, JP

註：排名依英文姓氏字母排列

S0180

香港專業及資深行政人員協會

就檢討《個人資料（私隱）條例》諮詢文件

意見書

前言

個人資料（私隱）條例於 1996 年生效至今已十多年，其間科技的迅速發展為個人資料私隱的保障帶來新的挑戰。隨著以電子方式儲存和處理個人資料越趨普及，市民的日常生活少不免會接觸其他人的個人資料，故本會同意在此時對條例作出檢討是有需要的。香港專業及資深行政人員協會轄下的社會發展委員會，經過對「檢討『個人資料』(私隱）條例」諮詢文件的深入研究後，現提出如下意見，供政府參考。

一．個人資料宜有一致的保障

隨著社會以電子方式處理個人資料的情況越來越普及，諮詢文件建議，把生物辨識資料，例如瞳孔特徵、掌紋及指模，列為敏感個人資料，以便與國際做法一致，並為此制訂另一套的禁止收集、持有、處理和使用的規管標準。然而，值得關注的是，國際並沒有一套公認的「敏感個人資料」定義，有些國家把刑事記錄列為敏感個人資料，有些則把宗教、健康狀況列為敏感個人資料，而現時有關香港的諮詢文件則建

議把生物辨識列為敏感個人資料。我們認為，凡屬個人資料不論是身份證和電話號碼、住址、或生物辨識資料等，均應受到同一程度的保障，因為任何一類的個人資料被不適當使用，簡單如手提電話號碼，也可以導致資料所屬的當事人出現嚴重的損失或傷害。事實上，生物辨識技術往往只記錄個人部份特徵，並非一個完整的個人資料，因此單憑生物辨識資料，並不容易辨識該資料上的個人身份。加上國際社會並沒有統一的做法，因此，在現階段本會認為不宜把生物辨識資料列為敏感個人資料，以及為此制定新規定。

鑑於生物辨識技術在社會上漸漸為人所採用，在考慮保障個人資料私隱與便利資訊及通訊科技持續發展之間取得平衡之下，若政府欲要作出相關的規管，建議就私人機構使用生物辨識技術，發出實務守則，讓私人機構遵守。本會認為，若全面把生物辨識資料列為敏感個人資料，並加以規管，恐怕只會妨礙有關技術在香港的應用。（3.01-3.15 段）

此外，針對過往曾出現遺失存有病人病歷紀錄的 USB，或不適當外洩病人資料等，當局宜加強監管，強化相關的實務守則，以確保病人資料得到適當的保存和使用。

二．規管處理個人資料的分判商

把個人資料分判或委託給第三者處理日趨普遍，甚至會出現

「判上判」的情況，但鑑於現行「私隱條例」，主要規管資料使用者的行為，一旦外判商遺失個人資料，而資料使用者在沒有與外判商存有合約的關係下，可能要承擔全部責任。因此，本會同意當資料使用者把個人資料委託第三者處理時，應有一定的規管。例如可規定，把個人資料轉移給資料處理者持有、處理或使用的資料使用者須以合約形式，確保其資料處理者及任何分包承辦商，採取切實可行的步驟，以保障資料安全及妥為保管。但由於資料處理者還包括從事互聯網業務的公司，為免窒礙互聯網業務的發展，在作出相關的規管時，必須要取得平衡。而當局先行要求互聯網業界透過自我監管形式，以保障個人資料的處理和保存，毋須一定修訂私隱條例，這種安排可以是一個取得平衡的選擇。（4.02-4.21 段）

三．設立通報機制

目前，私隱條例沒有規定資料使用者於發生個人資料外洩事故時，須通知私隱專員或受事件影響的人士。根據近年個人資料外洩事件，公營機構在外洩事件發生後，一般會向私隱專員公署作出通報，但卻未見有私人機構向私隱專員公署作出通報。然而，本會考慮到設立強制性的通報機制，並要求各行業遵守，將對社會構成沉重的負擔，故同意應採用自願性通報機制；但若外洩個人資料事件，涉及個人敏感資料，並可對個人或機構造成重大的損失，例如財務及病歷資料，

則應要求公營和私營機構作出強制性通報，以便讓當事人及時採取措施，保障自身的利益。(4.22-4.43 段)

四・維持公署現行職權

文件提出，私隱專員公署要求賦予刑事調查及檢控權力，以便更有效地執行私隱條例。然而，從私隱專員公署過去三年的承辦個案數字顯示，由約一千多宗的投訴，至最終轉介往當局作出檢控的，其實每年不多於十宗，因此我們相信公署有足夠的能力處理案件，加上現行安排運作暢順，所以本會認為應維持公署現狀，毋須賦予公署更多權力。(5.02-5.09 段)

五・個人資料私隱專員公署繼續提供專業意見

文件又提出，根據私隱條例第 66 條，受屈當事人可提出訴訟，但沒有授權私隱專員提供協助。本會認為，由於訴訟可以涉及大量公帑，加上目前已有法律援助向財政情況一般的市民提供協助，故此建議仍由私隱專員公署向受屈當時人提供專業意見，以及安排律師或大律師提供意見及協助，但不宜參照平機會的模式，向受屈當事人提供法律協助。(5.10-5.14 段)

六・由法庭釐定補償

現時若當時人因資料使用者違反私隱條例而蒙受損害，可根據法例向資料使用者提出申索補償。文件指出，可考慮授權私隱專員釐定補償額的方案，但本會認為，既然相關的條文多年以來甚少被引用，加上類似的機構如平機會，也沒有獲授予裁定補償的權力，故宜維持現行做法，即交由法庭釐定補償。(5.15-5.22 段)

七・把蓄意違反保障資料訂為罪行

近年發生多宗個人資料外洩事件，反映現行私隱條例並未能收阻嚇之效，然而本會同意，若把違反保障資料原則訂為罪行，或會影響公民自由，因此，在平衡條例缺乏阻嚇性和保障公民自由的原則之下，本會同意在保障個人資料的大前提下，應把蓄意違反保障資料原則的行為訂為罪行，也同意在未得資料使用者同意下，知情或罔顧後果地取得個人資料，再把所資料披露而從中獲利的行為，訂為罪行。(6.03-6.12 段)

八・把重複違反保障資料原則訂為罪行

鑑於違反保障資料原則的使用者，在收到執行通知後，可能在短期內重複違反保障資料原則的行為，為打擊這種做法，

本會同意把同一事實重複違反保障資料原則，訂為罪行。(6.13-16 段)

九．提高直銷活動中不當使用個人資料的罰則

鑑於直銷電話滋擾情況日趨嚴重，而不斷的直銷來電，除了直接影響工作之外，更涉嫌侵犯個人私隱，因此，就私隱專員建議提高直銷活動中不當使用個人資料行為的罰則，以遏止直銷電話，本會同意有關做法。(6.26-6.31 段)

十．加強公眾教育

隨著資訊科技迅速發展、互聯網廣泛普及等，我們很輕易便可儲存、處理、檢索及傳輸大量個人資料；而近年發生多宗個人資料外洩事件，反映市民在保障個人資料方面的意識仍有待提高。就此，本會認為當局應加強公眾教育，讓公眾認識在享有資訊自由的同時，也要注重保障個人資料。由於個人的不當儲存和處理個人資料行為，可以直接構成罪行，建議當局參考版權條例的執行做法，在作出相關的法例修訂時，必須讓公眾有廣泛的討論，以便獲得公眾的支持。