

Article 17: Protection of privacy, family, home, correspondence, honour and reputation

Interception of Communications and Surveillance Ordinance

17.1 In paragraph 12 of its previous Concluding Observations, the Committee raised concern on the lack of a clear statutory regime to regulate interception and covert surveillance conducted by law enforcement agencies (LEAs). To this end, the Interception of Communications and Surveillance Ordinance, which was enacted in August 2006, specifies by law detailed provisions on the purposes for which, and the circumstances and authority under which, LEAs may lawfully intercept communications and conduct covert surveillance involving the use of devices. The Ordinance provides stringent safeguards at all stages of the regime – from the application for the authorisation, execution of the authorisation, to the subsequent oversight. The Ordinance is in conformity with Article 30 of the Basic Law, and seeks to protect the right to privacy under Article 17 of the Covenant.

17.2 According to the Interception of Communications and Surveillance Ordinance, LEAs would conduct interception of communications or covert surveillance only if it is necessary for the purpose of prevention or detection of serious crime or protection of public security. LEAs must obtain authorisation before carrying out such covert operations. For interception of communications and the more intrusive type of covert surveillance, the authorising authority is one of the panel judges, who must be judges of the Court of First Instance. Less intrusive covert surveillance would be authorised by designated senior officers of LEAs. The authorising authority must be satisfied that the tests of proportionality and necessity are met before issuing the authorisation. All intercept and surveillance products are required to be destroyed as soon as their retention is not necessary for the relevant purpose of the prescribed authorisations.

17.3 An independent commissioner, the Commissioner on Interception of Communications and Surveillance, is appointed by the Chief Executive to oversee LEAs' compliance with the relevant requirements of the Ordinance. According to the Interception of

Communications and Surveillance Ordinance, the Commissioner should, in his annual report to the Chief Executive, include an assessment on the overall compliance with the relevant requirements. In addition, if any person suspects that covert operations were conducted by LEAs on him, he may apply to the Commissioner for an examination under the Ordinance.

17.4 The Commissioner indicated in his annual reports to the Chief Executive that he was generally satisfied with the compliance of the LEAs with the requirements under the Ordinance. The operation of the regime under the Ordinance has been smooth since it came into effect in August 2006.

17.5 The Commissioner has made some recommendations to enhance the operation of the Interception of Communications and Surveillance Ordinance regime in discharging his oversight function. For those recommendations which do not require legislative amendments, the Government has implemented them as far as practicable and amended the Code of Practice issued under section 63 of the Ordinance where appropriate. Regarding the remaining recommendations, the Government will study them in detail in the comprehensive review of the Ordinance.

Protection of privacy

Personal data privacy

17.6 The position is essentially as explained in paragraphs 305 to 307 of Part II of the initial report. As at 30 June 2010, the Privacy Commissioner for Personal Data is supported by a staff of 58. Between April 2004 to March 2010, the PCPD received 5 672 complaints and 89 352 inquiries relating to operational matters and compliance with the provisions of the PDPO. In the same period, the PCPD issued 493 warnings and 145 enforcement notices and referred 32 suspected offences to the Police for investigation and consideration of prosecution.

17.7 Since the PDPO came into force in December 1996, the PCPD has issued three codes of practice⁶, one guideline and seven guidance notes that provide practical guidance for compliance with the PDPO. It has continued to promote public awareness of and compliance with the Ordinance.

17.8 The Government, with the support of the PCPD, conducted a comprehensive review of the PDPO in 2009 to see whether its existing provisions still afford adequate protection for personal data in the wake of the developments over the last decade or so. The Government conducted a public consultation from August to November 2009 to gauge public views on the proposals to amend the PDPO. The Government published on 18 October 2010 the Report on Public Consultation on Review of the PDPO and launched further public discussion on the legislative proposals to strengthen personal data privacy protection under the PDPO.

17.9 Some commentators raised concern on the composition of the selection board for the recruitment of the new Privacy Commissioner in 2009. The Government attaches great importance to the work of the Privacy Commissioner. The selection board comprised members with extensive experience and knowledge respectively in community services, public administration, corporate governance and management and other fields, and was chaired by an non-official member. The selection board considered all candidates carefully in accordance with objective criteria and made a recommendation to the Chief Executive on the suitable candidate.

17.10 Some commentators expressed concern on instances concerning the leakage of personal data following the development of information technology, and asked for more resources be made available to the PDPO for it to better discharge its duties. The Government attaches great importance in providing sufficient resources to the PCPD to meet its operational needs. It had increased the allocation to the PCPD from \$36.2 million in 2007-08 to \$48.6 million in 2010-11, which

⁶ The codes of practice are, namely, Code of Practice on Human Resource Management, Code of Practice on the Identity Card Number and other Personal Identifiers, and the revised Code of Practice on Consumer Credit Data.

is more than a one-third increase. In 2010-11, an additional provision of \$4.57 million was provided to the PCPD to create five posts to step up its enforcement and promotion work.

17.11 Some commentators enquired about actions taken by the Government to follow up the collection of data (video or photographs) by Google Maps Street View. After thorough investigations, the Privacy Commissioner decided on 30 July 2010 not to carry out a formal investigation on the incident. The main basis of the decision was that the Privacy Commissioner was reasonably satisfied that: (a) the data do not contain any meaningful details that can directly identify any one individual; (b) Google had no intention to compile personal information through the Street View car operation in Hong Kong; and (c) Google had not accessed or used any of the Wi-Fi payload data captured in Hong Kong through the operation. Google has also given a written undertaking to the Privacy Commissioner on appropriate remedial measures, including to completely delete the payload data at the direction of the Privacy Commissioner and provide the Privacy Commissioner with an independent third party's verification of the deletion. It has also undertaken that future Street View car operations carried out in Hong Kong shall comply with the requirements of the PDPO.

CCTV and video recording

17.12 Various Government departments have installed CCTV cameras in public places, such as strategic locations in the transport infrastructure, public rental housing estates, entrances to public facilities and lift cabins, for traffic monitoring, facility management and other lawful purposes. District Councils of Wan Chai and Yau Tsim Mong have also installed CCTV camera to deter the acts of throwing objects from height. The Police does not install any CCTV system in public places on a permanent basis for the purpose of maintaining law and order. To ensure the propriety of the operation of CCTV and the use of information collected therefrom, the PCPD issued a Guidance Note on CCTV Surveillances Practices in July 2010 for Government departments and the public to follow. Individual departments have issued internal guidelines to ensure that relevant recording strictly complies with the PDPO.

Privacy at schools

17.13 Some commentators expressed concerns about the impact of CCTV monitoring system in schools on the privacy of students and teachers. There were also concerns about the school drug-testing scheme on the privacy of students. We understand from the schools that CCTV monitoring systems are installed mainly for security purposes. They are often installed at public areas like entrances and exits of the schools. In many cases, staff and students are informed of the installation of the systems. The Trial Scheme on School Drug Testing in Tai Po District was launched in December 2009. The Scheme was guided by four principles, one of which is “keeping personal information strictly confidential”. To protect the privacy of students participating in the Scheme, designated officers have been assigned to observe the operation of the Student Drug Testing Team and provide advice to participating schools on the data privacy requirements relating to drug testing as set out in a protocol. The Scheme implemented in the 2009-10 school year has been completed smoothly in June 2010. The procedures set out in the protocol have been strictly adhered to and personal information of the students has been safeguarded according to the data privacy requirements as set out in the Protocol. Participating students and parents are positive and cooperative towards the Scheme.

Law Reform Commission reports on privacy

17.14 Some commentators enquired about the Government’s position on whether there should be a statutory tort of invasion of privacy. At present, 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 for that damage under section 66 of the PDPO.

17.15 The LRC published a series of reports on various aspects of privacy. One of the reports was on civil liability for invasion of privacy, which recommended the creation of specific torts of invasion of privacy by statute to enable an individual to seek civil remedies for unwarranted invasion of privacy. Many recommendations in the LRC reports are controversial. We need to strike a good balance between the protection

of privacy and upholding press freedom. We shall handle the LRC report on stalking first as there are relatively fewer controversies on regulating stalking behaviours. The report proposed the introduction of anti-stalking legislation to render the pursuit of a course of conduct causing another person alarm or distress a criminal offence and a civil wrong. We are studying this report in depth for formulating the way forward, and making preparations for undertaking public consultation on the subject.