立法會

Legislative Council

LC Paper No. LS21/05-06

Paper for the Panel on Information Technology and Broadcasting

Scope of "personal data" under the Personal Data (Privacy) Ordinance (Cap. 486) and related issues

Purpose

At its meeting held on 1 November 2005, the Panel on Information Technology and Broadcasting discussed issues related to the protection of personal information of e-mail account subscribers arising from a recently reported incident on alleged disclosure by an e-mail service provider in Hong Kong of its account subscriber's personal information. To assist members of the Panel in their further consideration of the matter, this paper provides information on the scope of "personal data" as defined under the Personal Data (Privacy) Ordinance (Cap. 486) ("PD(P)O") and other related issues.

Definition of "personal data" under PD(P)O

2. Section 2(1) of PD(P)O defines "personal data" as meaning any data relating directly or indirectly to a living individual and from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and such data is in a form in which access to or processing of the data is practicable. In other words, to constitute "personal data", the data must satisfy the requirements of identifiability and retrievability. "Data" is defined to mean any representation of information (including an expression of opinion) in any document, and includes a personal identifier. Under PD(P)O, a personal identifier means an identifier that is assigned to an individual by a data user for the purpose of the operations of the user and that uniquely identifies that individual in relation to the data user, but does not include an individual's name used to identify that individual.

3. The above definition of "personal data" under PD(P)O is similar to the definition of the term under the data protection laws of other jurisdictions. In Australia and New Zealand, the concept of "personal information" instead of "personal data" is adopted. Under Australia's Privacy Act 1988, "personal information is defined to mean "information or an opinion…about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion". In New Zealand, the definition is in similar terms where "personal information" is defined as "information about an identifiable individual".[1] The definition of "personal data" under the European Union's Directive on the Protection of Personal Data and on the Free Movement of Such Data ("the EU Directive") is also comparable. Under the EU Directive, "personal data means "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified directly or indirectly".[2] The Preamble to the EU Directive states additionally that in order "to determine whether a person is identifiable, account should be taken of all means likely reasonably to be used either by the controller or by any other person to identify the said person".[3] Member states of the European Union such as the United Kingdom and Germany have enacted data protection laws with a view to implementing the EU Directive.

Interpretation of "personal data" by courts and quasi-judicial bodies

4. Although there are data protection laws in a number of jurisdictions, there have been few judicial decisions which turn on the interpretation of data protection statutes. Commentators considered that this may be due to the existence and regulatory strategies of data protection authorities and the fact that decisions of most data protection authorities or complaints which authorities fail to resolve do not go directly to courts for adjudication but to quasi-judicial bodies first.[4] Examples of such bodies are the Complaints Review Tribunal in New Zealand and the Data Protection Tribunal in the United Kingdom. Under PD(P)O, a complainant may lodge an appeal against the refusal of the Privacy Commissioner for Personal Data to carry out an investigation of a complaint to the Administrative Appeals Board. A summary of the relevant cases decided by the courts and quasi-judicial bodies is set out in the Annex for members' reference.

---

[1] Privacy Act 1993, New Zealand, section 2.
[2] Directive 95/46/EC, art 2(a).
[3] Recital 26.
[4] Lee A Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law – Part 1, *Privacy Law and Policy Reporter* [2000] PLPR 19.

5. An analysis of the relevant cases indicates that the courts and other relevant authorities appear to have adopted a rather restrictive approach in interpreting data protection legislation. The decisions in these cases have led to diverse comments from commentators and legal academics. For example, the decision of the Court of Appeal in *Eastweek Publisher Ltd. v Privacy Commissioner for Personal Data*[5] has been criticised by commentators for restricting the reach of privacy protection by imposing a judicial requirement for an intention to identify by the data collector which is not prima facie present in the legislation.[6] There has also been criticism that the court in *Eastweek* has failed to examine the identifiability test which covers both direct and indirect ascertainment of an individual's identity, nor has it considered the reasonable practicability of identifying the complainant from the photograph.[7]

6. On the other hand, commentators have expressed the view that the narrow interpretation of the term "personal data' adopted by the English Court of Appeal in *Durant v Financial Services Authority*[8] misconceives the role of the definition of "personal data" or "personal information" in determining the scope of the information privacy law since the basic assumption of all information privacy laws is that the privacy of the data subject is threatened by the processing of any information which identifies the data subject, or is capable of identifying the data subject, regardless of the nature of the information.[9]

7. When commenting on the two cases decided by the New Zealand's Complaints Review Tribunal, namely, *C v ASB Bank Ltd.*[10] and *Proceedings Commissioner v Commissioner of Police*[11], another commentator was of the view that the Tribunal adopted different approaches to the issue of "identifiability".[12] In the former case, the Tribunal rejected the identifiability of an individual by way of combination with other information known about the particular individual. This approach is different from the approach adopted in *Proceedings Commissioner v Commissioner of Police* where the Tribunal held that so long as information had the capacity to identify the individual to some members of the public, it was personal information for the purposes of New Zealand' Privacy Act. The latter approach has

---

[5] [2000] 1 HKC 692

[6] Sharon Nye, 'Internet privacy – regulatory cookies and web bugs', *Privacy Law and Policy Reporter* [2002] PLPR 26

[7] Mark Berthold and Professor Raymond Wacks, *Hong Kong Data Privacy Law* (Sweet and Maxwell Asia, 2003).

[8] [2003] EWCA Civ 1746.

[9] David Lindsay, 'Misunderstanding 'personal information' : Durant v Financial Services Authority', *Privacy Law and Policy Reporter* [2004] PLPR 13.

[10] (1997) 4 HRNZ 306.

[11] [2000] NZAR 277.

[12] Paul Roth, "Information" about individuals', *Privacy Law and Policy Reporter* [2002] PLPR 31.

been considered to be consistent with the international standards set out in Article 2(a) of the EU Directive, which defines "personal data" as information concerning "an identified or identifiable" individual. The reference to "identifiable" could be interpreted to involve the use of linked data leading to the individual's identification whereas "identified" entails identification through the information itself.[13]

8. Based on the decided cases on the interpretation of data protection legislation set out in the Annex, it seems that the following principles are relevant in determining what amounts to "personal data" under PD(P)O:

(a) In general, information about companies is not personal information because it is not information about a natural person, and this is so even though the information relates to a one-person company;

(b) To qualify as "personal data" or "personal information", the data or information concerned must relate to an individual in the sense that it has an idiosyncratic connection with the individual;

(c) A primary piece of information may be regarded as personal if the identity of an individual can be reasonably ascertained by the use of other collateral information; and

(d) There is an intention on the part of the data collector to identify the individual.

Application of data privacy laws to the Internet

9. Information gathered on the Internet from Internet users may be provided by the users voluntarily or involuntarily. Information may be provided voluntarily through registration pages, contest sign-ups, applications or order forms. Users will often give crucial information such as name and address believing that the information is being collected for a specific purpose.

[13] Paul Roth, *I.b.i.d.*

10. On the other hand, some information is collected by the covert operation of technology. Such information include a user's Internet Protocol address ("IP address"), the type of computer and browser used and limited information about the browsing activity (notably the time and date of access and the referring website's Internet address). An IP address is basically a specific machine address assigned by the Web Surfer's Internet Service Provider ("ISP") to a user's computer and is therefore unique to a specific computer.[14] Whenever a transaction requesting or sending data occurs on the Internet, this unique address accompanies the data. Moreover, the deployment of cookies by a website would allow the website to recognize a computer's IP address and to recall details of the user's browsing activity.

11. In the matter under consideration by the Panel, the Panel has taken note of the Changsha Intermediate People's Court of Hunan Province Criminal Verdict (2005) in relation to the trial of "Shi Tao" in which it was reported that Yahoo Holdings (Hong Kong) Limited ("Yahoo Holdings") had confirmed the user information corresponding to an IP address. Since the user information is apparently derived from the relevant IP address, it may be useful to consider whether an IP address is "personal data" under PD(P)O in considering whether the alleged disclosure amounts to a contravention of PD(P)O.

12. According to Yahoo! Hong Kong's privacy policy (Exhibit B to LC Paper No. CB(1)186/05-06(03)), Yahoo! Hong Kong will automatically receive and record information such as IP address and the information recorded in Yahoo! cookie and the web pages visited. It is not known whether the IP address allegedly disclosed in the trial of Shi Tao was disclosed by Yahoo Holdings. It is possible that cookies may be used by third parties uninvolved in the transaction between the user and Yahoo Holdings and whose existence is unknown to the user.

13. According to our research, there has not been any judicial authority on whether an IP address is personal data or personal information within the scope of data protection laws. Some commentators suggest that it is quite possible that IP addresses can constitute "personal data" as defined in Article 2(a) of the EU Directive as an IP address which discloses the location of a computer used to access a website can be traced to an identifiable individual.[15] Some have argued that it is a question of fact whether an individual's identity can be ascertained from transactional details

---

[14] Brian Keith Groemminger, 'Personal Privacy on the Internet: Should it be a Cyberspace Entitlement?' *The Trustee of Indiana University Law Review* 2003, 36 Ind. L. Rev. 827

[15] Lee A. Bygrave, 'Data Protection Law – Approaching its Rationale, Logic and Limits, 316 *Kluwer Law Journal*, 2002.

where only an IP address was collected, and it is a further question of fact whether it can "reasonably" be so ascertained.[16] However, in the light of the restrictive approach adopted by courts, it appears unlikely that the courts in Hong Kong are prepared to rule that IP addresses constitute "personal data" as defined under PD(P)O. Indeed, applying the principles set out in paragraph 8 above, it could be said that an IP address lacks an idiosyncratic relationship with the user because the information is about an inanimate computer, not the individual.

14. In respect of the alleged disclosure by Yahoo Holdings, there is the additional difficulty that the user information corresponding to the relevant IP address relates not to a natural person but to an entity instead. Given the narrow approach adopted in *Durant*, *Smith* and *C v ASB Bank*, it appears unlikely that the courts in Hong Kong would regard the user information allegedly disclosed by Yahoo Holdings as relating to a living individual under PD(P)O. However, if the courts are prepared to take a broader approach in construing the legislation, it could be argued that whether the corresponding user information relates to a natural person or an entity is not relevant; what is relevant is that the IP address discloses the physical location of the computer concerned. The question then is whether it is reasonably practicable to identify an individual from the location of the computer in the circumstances of the case. If the approach in *Proceedings Commissioner v Commissioner of Police* decided by the New Zealand' Complaints Review Tribunal is followed, it would be a question of fact for the courts to decide whether some members of the public, with prior knowledge about the individual, are able to identify the individual from the location of the computer.

Approaches adopted by some overseas jurisdictions to address privacy and data protection issues on the Internet

15. Unlike in the traditional processing of personal data where there is usually a single authority or entity responsible for protecting the privacy of data subjects, there is no such overall responsibility on the Internet assigned to a specific entity. Moreover, it seems that the use of Internet services does not allow adequate anonymity as the covert operation of the technology would facilitate surveillance of communications by methods such as cookies and the monitoring of IP addresses.

---

[16] Graham Greenleaf, 'Privacy principles – irrelevant to cyberspace?' *Privacy Law and Policy Reporter* [1996] PLPR 58

16. Some jurisdictions have taken action to address the issues of privacy and data protection on the Internet. For example, Germany has included in its Teleservices Data Protection Act 1997 provisions dealing with issues associated specifically with the use of Internet, namely, transactional anonymity, cookies, processing of clickstream data.[17] The Council of Europe has published guidelines for the protection of privacy on the Internet.[18] In the Directive on Privacy and Electronic Communications adopted by the European Union in 2002, there are provisions dealing with the confidentiality of communications made over a public electronic communications network, the use of cookies and the inclusion of personal data in public directories.

Protection of information of ISP customers under the Telecommunications Ordinance

17. According to the paper provided by the Administration (LC Paper No. CB(1)173/05-06(01)), ISPs are licensed through the Public Non-exclusive Telecommunications Service ("PNETS") licence granted by the Telecommunications Authority ("TA") under the Telecommunications Ordinance (Cap. 106) ("TO"). In addition to the prescribed general conditions, TA has, in exercise of the power conferred by section 7A of TO, attached a special condition to PNETS licences to protect the information of customers of ISPs licensed in Hong Kong.[19] The relevant special condition, as drafted, is not confined to protecting personal information of customers but to protecting information of an ISP customer and information provided by the customers of an ISP or obtained in the course of provision of service to its customers. Under TO, a breach of licence conditions can result in financial penalties and even revocation of the licence in exceptional cases.

---

[17] Clickstream data is the generic name given to the information a website can know about a user simply because the user has browsed the site.

[18] The guidelines were adopted by the Committee of Ministers on 23 February 1999.

[19] Special Condition 7 of the PNETS licence provides that (a) the licensee shall not disclose information of a customer except with the consent of the customer, which form of consent shall be approved by TA, except for the prevention or detection of crime or the apprehension or prosecution of offenders or except as may be authorized by or under any law; (b) the licensee shall not use information provided by its customers or obtained in the course of provision of service to its customers other than for and in relation to the provision by the licensee of the service under the licence.

Conclusion

18. It can be seen from the decided cases that a restrictive approach is generally adopted in the interpretation of data protection laws as applied to the traditional processing of data. It remains to be seen as to whether the courts are prepared to adopt a broader approach when applying the data protection laws to data collected on the Internet, especially in respect of the identifiability of an individual from information which apparently relates to a computer.

19. From the policy point of view, Members may wish to consider the following matters in deciding how the issues arising from the alleged disclosure by Yahoo Holdings should be dealt with:

(a) whether it is necessary to ask the Administration to review whether PD(P)O offers adequate protection to personal data collected on the Internet having regard to the development of technology; and

(b) whether specific legislation or additional privacy principles are necessary to address the issues of privacy and data protection on the Internet with reference to the approaches adopted by some overseas jurisdictions.

20. Apart from considering the matter from the perspective of personal data protection under PD(P)O, members may, in the light of paragraph 17 above, ask the Administration to consider whether any action could be taken under the licensing framework provided in TO.

Encl.

Prepared by

Legal Service Division
Legislative Council Secretariat
January 2006

Annex

Summary of cases on the interpretation of "personal data/information" by courts and quasi-judicial bodies in Hong Kong and overseas jurisdictions

Jurisdiction	Case	Case Summary
Hong Kong	*Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* [2000] 1 HKC 692	● The case concerned a complaint made by a woman whose photograph appeared in a magazine published by Eastweek. The photograph was taken without the complainant's knowledge or consent. The main issue before the Court of Appeal was whether the publisher had collected personal data using unfair means and whether the published photograph constituted "personal data". ● In deciding that the publisher had not collected personal data, the Court took into account the complainant's anonymity and the irrelevance of her identity so far as the photographer, the reporter and the publisher were concerned and the fact that the publisher had no intention to identify the complainant.
United Kingdom	*Durant v Financial Services Authority* [2003] EWCA Civ 1746	● A narrow interpretation of the term "persona data" under the Data Protection Act 1998 of the United Kingdom was adopted by the English Court of Appeal. The Court concluded that "personal data" was information affecting the privacy of the data subject, whether in his or her personal, business or professional capacity. ● The Court laid down two tests for distinguishing protected from unprotected information, namely that the information must be "biographical in a significant sense", and that the data subject must be the focus of the information.
United Kingdom	*Smith v Lloyds TSB Bank Plc*. [2005] EWHC 246, Ch.	● The narrow interpretation of "personal data" adopted by the English Court of Appeal in *Durant* has recently been followed in *Smith v Lloyds TSB Plc*. ● The court held that documents held by Lloyds concerning certain loans between Lloyds and a company of which Smith was the managing director and controlling shareholder were not personal data for the purposes of the Data Protection Act 1998. Although Smith was mentioned in those documents, the courts considered that this was only because he was acting on behalf of the company and hence were not biographical about Smith to a significant extent and did not significantly affect his privacy.

New Zealand	*Harder v The Proceedings Commissioner* [2000] 3 NZLR 80	In interpreting "information about an identifiable individual" under New Zealand's Privacy Act, the Court of Appeal came to the view that in order for information to be about an individual, some idiosyncratic connection with the individual was required.
New Zealand	*C v ASB Bank Ltd.* (1997) 4 HRNZ 306	● The issue before the New Zealand Complaints Review Tribunal in this case was whether information about a company could constitute personal information for the purposes of privacy legislation. The case concerned a one-person company where the plaintiff was the sole director and owner of all but one of the shares of the company. The Tribunal was asked to decide whether the defendant bank's unauthorized disclosure of the bank statements of the plaintiff's company to the plaintiff's former wife was a disclosure of the plaintiff's personal information in terms of New Zealand's Privacy Act 1993. ● It was held that the bank statements were not personal information about the plaintiff since the bank statements concerned were information about a company rather than an identifiable individual. ● Although the information from the company statements, when combined with other information which the former wife held about the plaintiff might become personal information about the plaintiff, the Tribunal considered that the bank statements contained information about the financial transactions of the company and as such they stood alone. The Tribunal did not accept the use of other information to establish the link leading to the identification of the individual.
New Zealand	*Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277	The Complaints Review Tribunal held that under the Privacy Act 1993, personal information was not limited to information that identified the complainant. It included information about her recorded in statements made by and about her. Thus the information contained in the statements she made about the type of injuries she sustained is information about her. It also had the capacity to identify her to some members of the public. An identifiable individual's privacy could be breached if an identification could be made as a result of prior knowledge by some members of the public of an individual, not just by strangers.
Germany	*'The Census Decision'* (1984) 5 HRLJ 94	The German Constitutional Court held that a proposal for national census was unlawful on data protection grounds. The Court expressed concern that although data gathered from the census would be published only in aggregated format, modern data processing techniques might permit the de-anonymisation of census data.