An evaluation of personal data protection in Hong Kong Special Administrative Region (1995–2012)

Anne S. Y. Cheung*

Abstract

- In 1995, the Hong Kong Special Administrative Region (Hong Kong) was the first jurisdiction in East Asia to enact a comprehensive piece of legislation for the protection of personal data privacy.
- As a result, Hong Kong has now long moved on from the pioneering phase to the present juncture of reform, and in June 2012, the *Personal Data (Privacy) (Amendment) Ordinance (the Amendment Ordinance)* was passed by the Legislative Council.
- Through a study of complaint statistics before the Privacy Commissioner and the Administrative Appeals Board, together with an analysis of cases brought before courts between 1996 and 2011, this article identifies additional valid concerns among the Hong Kong public with regard to direct marketing.
- Furthermore, the article examines just how much, over a number of years, the regulatory and judicial bodies have been responding to and shaping the expectation of Hong Kong citizens on personal data protection.

Introduction

In 1995, the Hong Kong Special Administrative Region (Hong Kong) was the first jurisdiction in East Asia to enact a comprehensive piece of legislation for the protection of personal data privacy under the *Personal Data (Privacy) Ordinance (PDPO)*.[1] Since 1996, the Ordinance has come into force over the subsequent 15 years. As a result, Hong Kong has now long moved on from the pioneering phase to the present juncture of reform.

In June 2012, the *Personal Data (Privacy) (Amendment) Ordinance (the Amendment Ordinance)* was passed by the Legislative Council.[2] This reform was largely a response to the Octopus card scandal in 2010, when it was discovered that the subway company had been selling the personal data of nearly 2 million customers without their express consent for the company's own profit. Hong Kong society was immediately alarmed. Fortunately, this scandal turned out to be a blessing in disguise as it had acted as a direct impetus for the present reform.[3] As expected, under *the Amendment Ordinance*, new rules governing direct marketing and the sale of personal data have been added. While these are certainly welcome moves, direct marketing regulation should not be one's sole concern as this will only reinforce Hong Kong's image as a 'privacy pragmatist',[4] and the belief that Hong Kong's legal regime

* Anne S.Y. Cheung, Professor, Faculty of Law, The University of Hong Kong. E-mail: anne.cheung@hku.hk. The author is particularly grateful for helpful comments from Mr Allan Chiang, the Privacy Commissioner of Hong Kong, and Professor Rolf H Weber at the University of Zurich to earlier drafts of this article. She would also like to thank her research assistants, Carol Wong and Michael Cheung. The research project was funded by Privacy International (UK), International Development and Research Council (Canada), and General Research Grant Fund (Hong Kong).

1 Cap. 486, Laws of Hong Kong.

2 Personal Data (Privacy) (Amendment) Ordinance 2012, Ord. No. 18 <http://www.legco.gov.hk/yr11-12/english/ord/ord018-12-e.pdf> assessed 20 July 2012.

3 Allan Chiang (Hong Kong Privacy Commissioner for Personal Data), 'Data Protection: Recent trends and developments in Hong Kong' (speech delivered at Privacy Laws & Business 24th Annual International Conference, Cambridge, UK, 13 July 2011) <http://www.pcpd.org.hk/english/files/infocentre/speech_20110713.pdf> accessed 20 July 2012.

4 Raymond Tang, 'Partners in Privacy—Working Towards a Privacy Aware Society in Hong Kong' (Privacy Laws & Business 16th Annual International Conference, Cambridge, UK, 7 July 2003) para. 7.7 <http://www.pcpd.org.hk/english/files/infocentre/speech_20030707.pdf> accessed 23 July 2012.

and reform on personal data are driven largely by business considerations.[5] In other words, within the horizon of personal data protection there remains a diversity of concerns by different parties.

Consequently, through a study of complaint statistics before the Privacy Commissioner and the Administrative Appeals Board, together with an analysis of cases brought before the courts between 1996 and 2011, this article identifies additional valid concerns among the Hong Kong public with regard to direct marketing. Furthermore, the article examines just how much, over a number of years, the regulatory and judicial bodies have been responding and shaping the expectation of Hong Kong citizens on personal data protection. Clearly, among citizens and other various sectors, the protection of personal data is a dynamic process in which citizens set out to test their right while those who flagrantly disregard privacy will have to reconsider their behaviour. Therefore, in presenting the trends and major judicial cases that are pertinent to personal data protection over this period, this study raises certain questions: what are the major challenges and concerns of the local community? And has the law provided an adequate solution? Bearing in mind that the Hong Kong PDPO is modelled after the Organization for Economic Co-operation and Development (OECD) Data Privacy Principles and the European Union Personal Data Directive,[6] it is hoped that the Hong Kong experience can provide a better understanding for the legal design, and all the challenges it entails, for an effective model for personal data protection.

The personal data landscape

The basic legal framework: The Personal Data (Privacy) Ordinance

In Hong Kong, privacy is a constitutional right, protected under Article 28 (personal privacy), Article 29 (territorial privacy), and Article 30 (communication privacy) of the Basic Law. In addition, Article 14 of the Hong Kong Bill of Rights protects the private and family life of Hong Kong residents. Yet, it is only the PDPO that directly governs the protection of personal data.

Under Section 2 of the PDPO, personal data are defined as any data (i) that relate directly or indirectly to a living individual; (ii) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (iii) that are in a form in which access to or processing of the data is also practicable. In this model, the three essential features of personal data, neatly summarized by Berthold and Wacks, are attribution, identification, and retrievability of personal data.[7] This piece of legislation aims to protect living individuals, known as data subjects, in relation to the data users. The latter are defined, under Section 2, to be persons who, 'either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.' Under section 4 of the PDPO, data users have to comply with six Data Protection Principles (DPP) governing the collection, accuracy, retention, use, notices and practices, security, and accessibility of personal data under Schedule 1 of the PDPO. Data subjects are provided with the right to access, and to correct personal information. The PDPO has also established complaint procedures and allowed compensation for damages suffered. Enforcement of the Ordinance is entrusted to the Privacy Commissioner's Office. If data users or complainants are not satisfied with the Commissioner's decision and interpretation of the PDPO, they can appeal to the Administrative Appeals Board.[8] Yet, for any claims of compensation, the aggrieved parties have to go to court.

It is important to note that while the contravention of the provisions of the main body of the PDPO is an offence, contravention of the data principles does not violate the criminal law. It is only when the Privacy Commissioner has found that a data user has contravened a data protection principle under the Ordinance, and has, therefore, served an enforcement notice on the data user directing him to take steps to remedy that contravention, but when the data user has failed to comply with the enforcement notice, that an offence has been committed under Section 64(7) of the PDPO. On the other hand, if the Commissioner is satisfied that remedial measures will be taken and the incident is unlikely to happen again, an enforcement notice may not even be issued. In sum, although the serving of an

5 Warren B. Chik, 'The Lion, The Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore—Two Differing Asian Approaches' (2006) 14 International Journal of Law and Information Technology 47.

6 Stephen Lau (Hong Kong Privacy Commissioner for Personal Data), 'The Asian Status with respect to the observance of the OECD Guidelines and the EU Directive' (19th International Conference of Privacy Data Protection Commissioners, Brussels, Belgium, 17–19 July 1997) <http://www.pcpd.org.hk/english/infocentre/speech_19970917.html> accessed 23 July 2012.

7 Mark Berthold and Raymond Wacks, *Hong Kong Data Privacy Law* (2nd edn, Sweet & Maxwell 2003) 209.

8 Item 29, Schedule, Administrative Appeal Board Ordinance, Cap. 422, Laws of Hong Kong.

enforcement notice is the 'most significant legal power' of the Commissioner,[9] this type of notice could only be served if the Commissioner considered that a data user was likely to repeat or continue a contravention of the PDPO.[10] Such contravention of an enforcement notice carries a maximum penalty of two years imprisonment and a maximum fine of HK$50,000.

The call for reform: The Octopus card scandal

Given the stringent requirements on the issuing of an enforcement notice, the Commissioner's power was rightly criticized as limited and inadequate.[11] Indeed, the Octopus card scandal fully exposed the problem. In July 2010, Octopus Rewards Limited (ORL), a company wholly owned by Octopus Holdings Limited (OHL) and the subway company in Hong Kong, was discovered to have sold, to six different companies, the personal data of 1.97 million registered individuals participating in the Octopus Rewards Program. They made a massive profit of US$5.7 million out of the sale.[12] It was easy for the company to get hold of the personal data of so many individuals because Octopus cards are a daily necessity for most Hong Kong residents. The cards are used for transportation of all kinds together with other types of purchases such as in coffee shops, supermarkets, and convenience stores. Not only do many Hong Kong residents use the cards all the time, but they also join a related rewards programme so that information about a person's ride or purchase are recorded which give the holder's name, identity card number, and even credit card number.

Shortly after the outbreak of the scandal, the Privacy Commissioner duly carried out an investigation and then published a report.[13] He criticized strongly the practices of OHL and condemned the company for violating Data Protection Principle One (DPP1) for excessive collection of personal data and for their failure to take all reasonable practicable measures to protect individual personal data.[14] In addition, the Commissioner also concluded that Data Protection Principle Three (DPP3) had been contravened by OHL who had failed to obtain prescribed consent from the data subjects.[15] Despite a strong wording, no penalty was imposed on the subway company, nor was an enforcement notice issued as the Commissioner considered that repeated or continuous contravention of the Ordinance was unlikely. The OHL simply accepted all the findings and recommendations in the reports, and confirmed that they would not apply for any judicial review to overturn the findings of the Commissioner. To appease the public, OHL pledged to donate the profit from these sales to charity.

In the face of such blatant violations of the data protection principles and the massive scale involved, it was hard to imagine that a data user could get away so easily without any legal liabilities. But this was apparently the case in Hong Kong, even though the Octopus card scandal only represented the tip of the iceberg. In their study, Greenleaf and McLeish point out around the same period of the scandal, there were 14 similar cases under investigation by the Privacy Commissioner's office involving the unauthorized sale and use of personal data.[16] Of these, eight involved telecommunications companies, five involved banks, and one involved an insurance company. Nevertheless, other than naming and shaming some of the data users, no real penalty was ever imposed on any of those investigated by the Privacy Commissioner. While facing the problem of unauthorized sales of personal data, Hong Kong has also been plagued by massive data leakage involving the Police Force and the Hospital Authority.[17] Again, no solution was in sight, at least not from the legal side. Rather, it was only when the Octopus card scandal was exposed that the Government had decided to implement legal reform.

The reform and the new law

Paving the road for reform

Although the PDPO was amended in 2012, the call for reform had taken place much earlier in 2005 which the Privacy Commissioner had already advocated,[18] and

9 Graham Greenleaf and Robin McLeish, 'Hong Kong's Privacy Enforcement: Issues Exposed, Powers Lacking' 116 Privacy Laws & Business International Report (2012) 25, 25–8.

10 S. 50(1)(b) of the PDPO.

11 Greenleaf and McLeish (n 9).

12 Hong Kong Privacy Commissioner, 'The Collection and Use of Personal Data of Members under the Octopus Rewards Programme run by Octopus Rewards Limited' (R10-9866, 18 October 2010) <http://www.pcpd.org.hk/english/publications/files/R10_9866_e.pdf> accessed 25 July 2012.

13 Ibid.

14 Ibid. Chapter 4.

15 Ibid.

16 Greenleaf and McLeish (n 9).

17 Office of the Privacy Commissioner for Personal Data, 'Legislative Council Panel on Home Affairs, Protection of Personal Data Privacy' (LC Paper No. CB(2)2454/07–08(01), June 2008) <http://www.legco.gov.hk/yr07-08/english/panels/ha/papers/ha0704cb2-2454-1-e.pdf> accessed 24 July 2012. See also Robin McLeish and Graham Greenleaf, 'Hong Kong' in James B Rule and Graham Greenleaf (eds) *Global Privacy Protection: The First Generation* (Edward Elgar 2010).

18 'Consultation on Review of the Personal Data (Privacy) Ordinance' (Newsletter of the Office of the Privacy Commissioner for Personal Data, Hong Kong, Issue No. 2, October 2009) <http://www.pcpd.org.hk/english/publications/newsletter_issue22.html> accessed 24 July 2012.

in 2006 an internal Ordinance Review Working Group was formed to assess and study the PDPO.[19] By 2007, the Privacy Commissioner's Office had submitted a comprehensive package of over 50 amendment proposals to the Constitutional and Mainland Affairs Bureau of the Government.[20] Major areas that were listed for amendment included the leakage of personal data on the Internet and disclosure of personal data by Internet or email service providers. Other issues included obtaining the prescribed consent of individuals, regulation of direct marketing activities, investigation and prosecution procedures, and enforcement and penalty.[21] But it was not until 2009 and 2010 that public consultations were conducted by the government.[22]

Eventually in the summer of 2012 *the Personal Data (Privacy) Amendment Ordinance* was passed. Shortly after, on 1 October 2012, most of these provisions came into operation, except those on the use, transfer, and sale of personal data for direct marking purposes and that of the legal assistance scheme provided by the Privacy Commissioner.[23] The estimated date for full implementation of the amended law is early 2013 so that the Privacy Commissioner, corporations, data users, and the public are better informed and prepared for the new scheme.[24]

Features of the new legislation

There are three major areas of reform. The first concerns the setting up of a new regime governing the use of personal data in direct marketing. The second introduces a new offence on disclosure of personal data obtained without consent for malicious purposes. The third empowers the Privacy Commissioner to improve enforcement of the law. As the major focus of this article is not on the new legal model, we will concentrate on only some of the features in this discussion.[25]

The first major amendment on direct marketing has been dedicated to a whole new section, Part VIA, on this subject. Under *the Amendment Ordinance*, direct marketing is defined as 'the offering, or advertising of the availability, of goods, facilities or services; or the solicitation of donations or contributions of charitable, cultural, philanthropic, recreational, political or other purposes through direct marketing means.'[26] While this definition is in line with the one in the PDPO, significant amendments have been made on the provisions governing the required form of consent in direct marketing.

Under the existing regime of PDPO, Section 34 only requires a data user to inform the concerned data subject on the first occasion that his personal data is used for direct marketing. If the data subject objects, the data user has to cease using the personal data concerned. This is generally referred to as the 'opt-out' arrangement. Furthermore, the sale of personal data per se is not at present prohibited by the PDPO. A victim could only argue, as in the Octopus card scandal, that such a sale without the prescribed consent of the data subject is inconsistent with the initial collection purpose and use of personal data, and constitutes a violation of DPP3.

In contrast, under the new regime, data subjects have to be informed and given notice of any use of personal data in direct marketing regarding (i) the kind of personal data will be used; (ii) the classes of marketing persons or companies that the data may be providing; and (ii) the classes of goods or services to be offered or advertised.[27] This information must be provided in an easily readable and understandable manner.[28] Such data, therefore, cannot be used unless consent from the data subject is given, and the data user must provide a channel to allow the subject communicate his consent without charge.[29] Under the new Section 35A of the

19 Ibid.

20 Ibid.

21 Ibid.

22 Constitutional and Mainland Affairs Bureau, the Government of the Hong Kong Special Administrative Region, 'Public Consultation on Review of the Personal Data (Privacy) Ordinance' (August 2009) <http://www.cmab.gov.hk/doc/issues/PDPO_Consultation_Document_en.pdf> accessed 25 July 2012; Constitutional and Mainland Affairs Bureau, 'Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance' (October 2010) <http://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf> accessed 25 July 2012.

23 Section 1 of the Personal Data (Privacy) (Amendment) Ordinance (the Amendment Ordinance).

24 Office of the Privacy Commissioner for Personal Data, Hong Kong, 'Passage of the Personal Data (Privacy)(Amendment) Bill 2011 by the Legislative Council' (Media Statement, 28 June 2012) <http://www.pcpd.org.hk/english/infocentre/press_20120628.html> accessed 25 July 2012.

25 For discussion on the reform of the PDPO, see Robin McLeish and Graham Greenleaf, 'Reform of Hong Kong's Privacy Ordinance after 15 years' (2011) 113: 1 Privacy Laws & Business International Report 15–17. Although the article discusses the proposed reform before the adoption of the new law, the analysis is still applicable. See also Gabriela Kennedy, Heidi Gleeson and Fiona Chan 'Reports and Analysis Hong Kong—The Personal Data (Privacy) Ordinance has been Amended: Are Your Data Protection Practices and Policies Adequate?' 1 (Hogan Lovells, 3 July 2012) <http://www.hoganlovells.com/files/Publication/e94596fb-07e1-415e-ad78-cfa0d97e92c2/Presentation/PublicationAttachment/270c09e5-87e6-4307-8e13-d947bf719411/HKGLIB01-%23989129-v1-IPMT_newsflash__The_Hong_Kong_Personal_Data_(Privacy)_Ordinanc.pdf> accessed 25 July 2012.

26 Section 35A of the Amendment Ordinance.

27 Section 21 of the Amendment Ordinance adds s. 35C to the PDPO.

28 Section 21 of the Amendment Ordinance adds s. 35C(4) to the PDPO.

29 Section 21 of the Amendment Ordinance adds s. 35C(2)(c) to the PDPO.

amended PDPO, consent in the context of direct marketing includes 'an indication of no objection to the use or provision'. Contravention of the new direct marketing provisions on unauthorized use may carry a fine of up to HK$500,000 and three years imprisonment. However, in the light of these new requirements and all their implications, the provisions governing the use of personal data in direct marketing will not apply to personal data that has been collected and used in direct marketing before the commencement of the Amendment Ordinance.[30] This allowance is known as a 'grandfathering arrangement' of the new law.[31]

Seemingly, these new arrangements on the use of personal data for direct marketing are more stringent, whereby express consent (in the form of an indication of no objection) must be given by data subjects. It is, therefore, closer to an opt-in regime. However the actual effect of the implementation of the Amendment Ordinance is uncertain, given how 'an indication of no objection' is likely to be interpreted. For instance, some have argued that when a data subject has not exercised his or her right to opt-out by failing to tick an 'opt-out' box on a specific form, this should be seen as an indication of consent.[32]

As for the sale or provision of personal data to a third party, this is specifically governed under the new law. Similar rules apply on notification to the ones outlined above in respect of direct marketing activities.[33] What is different is that notification and response from data users must be in writing, as well as consent from the data subjects.[34] Other than informing the data subjects of the kinds of personal data to be provided and the classes of marketing subjects, the data users must inform them that the data are provided for gain, together with the classes of persons to which the data are provided or sold.[35] In contrast to the use of personal data, there is no grandfathering arrangement for the provision or sale of personal data to a third party in direct marketing. In essence, the new law has tightened the requirement for data users on notification and consent, and on the use, sale, and provision of personal data in direct marketing.

Turning to the second major amendment, a new offence is included governing the disclosure of personal data obtained without consent from data users.[36] It will be an offence for a person to disclose any personal data of a data subject obtained from a data user without the user's consent if there is intent to obtain gain or to cause loss to the data subject. It will also be an offence if such disclosure causes psychological harm to the data subject. The maximum penalty for committing such an offence is a maximum fine of HK$1 million and 5 years imprisonment.

Regarding, the third major amendment on the powers of the Privacy Commissioner, and unlike the PDPO, the Privacy Commissioner is no longer required to satisfy either the requirement that the behaviour of the data user will continue or whether there are likely to be repeated breaches of the Ordinance before the issuing of an enforcement notice.[37] Thus, the Commissioner can issue an enforcement notice to the data user at the same time that he delivers his investigation result. Non-compliance (including repeated non-compliance) of an enforcement notice carries a maximum fine of HK$50,000 (HK$1000 per day for continuing breaches) and two years imprisonment.[38] The Commissioner is also given the power to give legal assistance to aggrieved parties to claim compensation under the PDPO.[39]

While the task of reforming the PDPO has been successfully accomplished after a long haul of 17 years, the three areas mentioned are not the only battle fronts which have been fought over on the issue of personal data protection.

An examination of the PDPO in action

It is a formidable task to interpret both the trends and results of the PDPO over the last 15 years. As only decisions from the courts are binding, the focus of this part will be on judicial decisions including a statistical overview of decisions taken before the Privacy Commissioner and the Administrative Appeals Board (AAB).

Before the Office of the Privacy Commissioner

Since the enactment of the PDPO in Hong Kong, the Office of the Privacy Commissioner (the Office) has played an indispensable role in the handling of enquiries

30 Section 21 of the Amendment Ordinance adds s. 35D to the PDPO.

31 The Privacy Commissioner has proposed specifying a cut-off data for this new scheme. Office of the Privacy Commissioner (n 24).

32 Kennedy, Gleeson and Chan (n 25).

33 Section 21 of the Amendment Ordinance adds s. 35J and s. 35K to the PDPO.

34 Section 21 of the Amendment Ordinance adds s. 35J(2)(a) to the PDPO.

35 Section 21 of the Amendment Ordinance adds s. 35J(2)(b) to the PDPO.

36 Section 36 of the Amendment Ordinance has replaced the old s. 64 of the PDPO with the new one.

37 Section 28 of the Amendment Ordinance amends s. 50 to the PDPO.

38 Section 29 of the Amendment Ordinance adds s. 50A to the PDPO.

39 Section 39 of the Amendment Ordinance adds new s. 66B to the PDPO.

and complaints on personal data protection. In 1996, there were 2,423 enquiries brought before the Office and 52 formal complaints.[40] By 2011, the number of enquiries and complaints had increased dramatically to 18,103 and 1,225 respectively.[41] This represent a staggering increase of more than seven-fold in enquiries and more than 25 times in complaints. In terms of the total number of enquiries and complaints between 1996 and 2011, the Office received 232,942 enquiries, and 11,690 complaints,[42] which meaans that only 5 per cent of enquiries ended up as formal complaints. Likewise, not all the received complaints were formally investigated by the Office for a number of reasons ranging from the nature of the complaint being outside the provisions of the Ordinance to a lack of prima facie evidence. Also many complaints were not formally investigated because the involved parties had already reached a settlement through mediation. In fact, out of these complaints, the majority was resolved through mediation (1470 cases representing 24 per cent), while only about 6 per cent (369 cases) proceeded to formal investigation.[43] Of those which were formally investigated, 56 per cent (207 cases) were found to have violated the data principles.[44] Between 1998 and 30 September 2009, 42 cases involving suspected breaches of the Ordinance had been referred by the Office to the police for follow-up action, of which there were only nine cases where the parties concerned had been charged and convicted in a magistrate's court. This was clearly inadequate.[45]

Of the available complaint data between 1996 and 2011, the majority were concerned with possible violations of DPP3 (45 per cent; 5,695 cases), that is unauthorized use of personal data without proper consent. The next two categories of major complaints were about unfair means of collection (24 per cent; 3,035 cases) and inadequate security (12 per cent; 1,519 cases). Complaints concerning direct marketing practice only constituted 6 per cent (804 cases). Between 2003 and 2011, of the complaints about the private sector, 22 per cent (1,229) were in the finance sector, followed by 19 per cent (1,064) in the telecommunications sector, with 12 per cent (691) in property management sector. In parallel, of the complaints about the public sector in the same period, 14 per cent (157) were against the Hospital Authority, with 12 per cent (127) against the police force, and 7 per cent (81) against the Housing Authority.

We can tell from the figures that the Privacy Commissioner's Office has played a significant mediatory and conciliatory role in the protection of personal data privacy in Hong Kong. Residents in Hong Kong are likely, therefore, to approach the Office as a point of contact because they have confidence in it. It is also laudable that under the new regime, the Commissioner will be given new power to assist parties to claim legal compensation before the courts. In the meantime, for parties who are not satisfied with the Commissioner's decisions, they can appeal to the Administrative Appeals Board or go to court.

Before the Administrative Appeals Board

Behind the statistics

Under Section 39(4) of the PDPO, an appeal may be lodged by the complainant to the Administrative Appeals Board (AAB) against the decision of the Privacy Commissioner in refusing to exercise his power to investigate or to continue to investigate a complaint. Under Section 47(4) of the PDPO, a complainant can appeal against the Commissioner's decision in refusing to issue an enforcement note against the data user complained of after completion of an investigation. On the other hand, a data user investigated also has the right to appeal to the AAB under Section 50(7) of the PDPO against the decision made by the Commissioner in issuing an enforcement notice against him. Decisions of the AAB are not binding but have been regarded as an important guideline for the subsequent handling of enquiries and complaints by the Privacy Commissioner.[46]

Out of more than ten thousand complaints, there were only 191 cases heard before the AAB between

40 Privacy Commissioner's of Personal Data, 'PCPD 1996–1997 Annual Report' 6–7.

41 For the number of enquiries, see Privacy Commissioner's of Personal Data, 'PCPD 2010–11 Annual Report' Compliance Actions 93 <http://www.pcpd.org.hk/english/publications/files/anreport11_06.pdf> accessed 28 July 2012. For the number of complaints, see Privacy Commissioner's of Personal Data, 'PCPD 2010–11 Annual Report' 57 <http://www.pcpd.org.hk/english/publications/files/anreport11_05.pdf> accessed 28 July 2012.

42 The data were an accumulation of available information from the PCPD Annual Reports from 1996 to 2011, available at <http://www.pcpd.org.hk/english/publications/annualreport.html> accessed 28 July 2012.

43 The data were an accumulation of available information from the PCPD Annual Reports from 2002–2011, available at <http://www.pcpd.org.hk/english/publications/files/anreport11_05.pdf> accessed 28 July 2012.

44 Ibid.

45 Roderick B Woo, 'The Work Report of the Privacy Commissioner' (December 2009) 50 <http://www.pcpd.org.hk/english/publications/files/work_report_e.pdf> accessed 3 August 2012.

46 Office of the Privacy Commissioner for Personal Data, Hong Kong, *Data Protection principles in the Personal Data (Privacy) Ordinance—from the Privacy Commissioner's Perspective* (2nd edn, Office of the Privacy Commissioner for Personal Data, Hong Kong 2010), p. 1.

1998 and 2011.[47] And of these 191 cases, 166 (86.9 per cent) were dismissed, 24 (12.6 per cent) were allowed (of which five cases were sent back to the Commissioner for further factual enquiry), and one case was settled without ruling. Similar to the nature of complaints before the Privacy Commissioner, the majority of disputes were about unauthorized use of personal data (DPP3), which constituted 30.4 per cent (58) of all cases.[48] In considering the complainants in initial disputes, the majority of cases involved complaints about employers (23 per cent; 44 cases), followed by cases against property management companies (16.2 per cent; 31 cases), and thirdly against government and statutory bodies (13 per cent; 25 cases). Judging from those cases concerning workplace personal data protection, it is clear that there is a strong attitude among employees on the extent to which employers seem to have the right to collect, use, or not use their personal data. In particular, these complainants suspect that employers have been collecting data unlawfully to establish a case of possible dereliction of duty.[49] In addition, there are concerns about the obtaining of medical or financial data without their consent.[50] As will be discussed in the following section, one such case that eventually ended up in court involved the world-renowned airline company, Cathay Pacific.[51]

Another important feature that is worth noting from the AAB statistics is the number of complaints relating to data access requests under Section18 of the PDPO and DPP6, which constituted 12.6 per cent (24) of cases before the AAB. As Hong Kong does not have a freedom of information law, the PDPO has effectively become an alternative powerful tool in requests to access one's own information. For instance, in this category of cases, university students were involved who wanted to have access to their files,[52] and exam scripts,[53] or there are former employees who wish to discover documents relating to themselves,[54] and patients who wanted to have access to their own medical records.[55] This last category of requests from patients calls for more special attention. In fact, our study reveals that 6.3 per cent (12) of cases were concerned about alleged wrongful collection, unauthorized use, or denial of access to medical data. The Hong Kong Hospital Authority has a notorious reputation for losing patients' data,[56] and this is particularly worrying given that Hong Kong is currently considering the implementation of electronic medical health record sharing among health service providers.[57] Obviously, before introducing such a scheme, it is essential for the Hospital Authority and others to ensure the security of the personal data of the patients, and to carry out a privacy impact assessment to identify the risks involved. Hong Kong needs a scheme that must protect the security of the personal data of patients notwithstanding the need for easy access of data for both health providers and patients.

These issues concern access requests by data subjects, who are understandably eager to find out about their own personal data held by others, although these requests can put data users in a dilemma especially when the requested data involves that of third parties. In some situations, however, data subjects may also make data access requests in order to bypass the discovery procedures in court. For these two scenarios, positions have been elaborated by judges, which raise discussion on judicial decisions.

47 Decisions from the Administrative Appeals Board from 1998 to 2011 are available from the database of The Office of the Privacy Commissioner for Personal Data, Hong Kong at <http://www.pcpd.org.hk/english/casenotes/decisions.html> and the Hong Kong Legal Information Institute at <http://www.hklii.hk/eng/hk/other/pcpd/AAB/> (English database) and <http://www.hklii.hk/chi/hk/other/pcpd/AAB/> (Chinese database) accessed 9 October 2012. Cases counted were based on the date of decision delivered.

48 One case might have involved alleged contravention of more than one data principles. This study classified the cases according to the major issue discussed by the AAB.

49 *Lin Pengying Mandam Wong Suk WA v the Privacy Commissioner for Personal Data* [2008] HKPCPDAAB 23 (in Chinese).

50 *Luo Weijie v Privacy Commissioner for Personal Data* [2004] HKPCPDAAB 26 (in Chinese).

51 *Cathay Pacific Airways Ltd. v Privacy Commissioner for Personal Data* [2007] HKPCPDAAB 3. *Cathay Pacific Airways Ltd. v Administrative Appeals Board & Anor* [2008] 5 HKC 229.

52 *Hung Kwok Ching v Privacy Commissioner for Personal Data* [2005] HKPCPDAAB 3; *Hung Kwok Ching v Privacy Commissioner for Personal Data* [2005] HKPCPDAAB 5.

53 *Young Yim-yi, Bonnie v Privacy Commissioner for Personal Data* [2007] HKPCPDAAB 7.

54 *Yuen Oi Yee, Lisa v Privacy Commissioner for Personal Data* [2005] HKPCPDAAB 59. Another case eventually ended up in court: *Tsui Koon Wah v Privacy Commissioner for Personal Data* [2004] HKCFI 1464; [2004]2 HKLRD 840 (in Chinese).

55 These included *Wu Kit Ping and Privacy Commissioner for Personal Data* [2004] HKPCPDAAB 17;*Gu Jiebing and Privacy Commissioner for Personal Data* [2006] HKPCPDAAB 36; *Madam Wu Kit Ping and the Privacy Commissioner for Personal Data* [2006] HKPCPDAAB 27.

56 Office of the Privacy Commissioner for Personal Data, Hong Kong, 'Report Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap. 486)' (R08-1935, 24, December 2008) <http://www.pcpd.org.hk/english/publications/files/UCH_investigation_report_e.pdf> accessed 31 July 2012

57 Government of the Hong Kong Special Administrative Region, 'Public Consultation on the Legal, Privacy and Security Framework for Electronic Health Record Sharing' (2011) <http://www.ehealth.gov.hk/en/public_consultation/> accessed 30 July 2012.

Beyond statistics

Although the decisions of the AAB do not have binding effect and most of them involve disputes on factual details, the decision in *Shi Tao v Privacy Commissioner for Personal Data* is worth highlighting and discussing.[58] The case is particularly sensitive as it involved Yahoo! Hong Kong handing in information to the Beijing Chinese authorities about the appellant, a Chinese journalist, who was prosecuted for sending state secrets to an overseas organization through his email account. Eventually, he was sentenced to ten years imprisonment by the People's Republic of China's (Chinese) authorities.[59] The judgment from the Chinese court revealed that the details of the email transactions from the appellant's account, including the IP address from which a person had logged in to send the relevant emails, were disclosed to the Chinese authorities by the Beijing office of Yahoo!China, a business owned by Yahoo!Hong Kong (YHHK). It was YHHK who disclosed the email account holder information and the email content to the authorities. On behalf of the journalist, a complaint was brought before the Hong Kong Privacy Commissioner for wrongful disclosure of personal details under the PDPO.[60] The Commissioner concluded that (i) the YHHK was not a data user; (ii) the Ordinance did not have extra-territorial application; and (iii) an IP address of an internet account holder was not personal data within the meaning of Section 2 of the PDPO.[61] Unsatisfied and undeterred, the appellant brought the complaint before the AAB.

On the more straightforward point on whether YHHK was a data user, the AAB disagreed with the Privacy Commissioner and considered that YHHK was a data user because it had retained control of the personal data of its users.[62] But on the two remaining points, the AAB sided with the Commissioner. On the issue of the extraterritorial application of the PDPO, the AAB considered that the issue had been mischaracterized.[63] It pointed out that under Section 39(1)(d) of the PDPO, the Commissioner was entitled to refuse to carry out or continue an investigation when the case had no connection with Hong Kong.[64] Furthermore, since the appellant had given prescribed consent for Yahoo!China to disclose the disputed information 'in accordance with legal procedure' when he first signed up for using the email service, Yahoo!China was authorized to disclose the information.[65]

On the last and most controversial point concerning whether personal data were involved, the AAB held that an IP address was not a form of personal data as it was not reasonably practicable to ascertain and identify the actual user from such information.[66] What was revealed, in the opinion of the AAB, was only the IP login information showing an email had been sent from a computer located at the address of a particular business entity, and the date and time of the transaction.[67] Hence, there was no conclusive evidence and no certainty that that information necessarily was in relation to the personal data of the appellant. Along this line of reasoning, the AAB concluded that it was not such as would enable the identity of the appellant to be ascertained directly or indirectly with reasonable practicability.

Seemingly, the AAB is correct as an IP address per se only leads one to a computer and not an individual and thus will not satisfy the definition of personal data under the PDPO in relation to an individual. However, in the hands of an internet service provider, an IP address will become personal data when combined with other information that is held, which will include a user's name, address, and his online activity. It is also through this way that the appellant was identified by the Chinese authorities. It is only logical to consider an IP address as part and parcel of a package of personal data. In fact, this view has been confirmed by the European Court of Justice, which has ruled that an IP address is a protected form of personal data as this would lead to the identification of an individual.[68]

What the AAB had managed to achieve was to evade the issue of extraterritorial effect and to adopt a very restrictive interpretation of 'personal data' so as to steer away from any potential political repercussions on a politically delicate and sensitive case. It is yet to be seen how the Hong Kong court will rule on like issues should such an opportunity arise in the future.

58 [2008] 3 HKLRD 332.

59 *Changsha People's Procuratorate of Hunan Province v Shi Tao (Changsha Intermediate People's Court of Hunan Province*, 27 April 2005), Case no. 19-10 at <http://www.globalvoicesonline.org/wp-content/ShiTao_verdict.pdf> (Chinese and with translated English version) accessed 10 October 2012.

60 [2008] 3 HKLRD 332, 336, para. 7.

61 Ibid, 343–44.

62 Ibid,8, para. 83.

63 Ibid, 349, para. 86.

64 Ibid, 349, para. 86.

65 Ibid, 350, para. 94.

66 Ibid, 346, para. 67.

67 Ibid.

68 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Case C-70/10, 24 November 2011, European Court of Justice.

Before Hong Kong courts

Between 1997 and 2011, there were 21 cases with major issues concerning the hearings of the PDPO before the Hong Kong courts.[69] As mentioned earlier in this article, a complainant who is not satisfied with the decision of the Privacy Commissioner or with the AAB can seek judicial review from the court. However, if a party would like to claim compensation against a third person, he or she has to bring a civil action to court directly. Of the 21 cases before the courts, six (28.5 per cent) were challenges on the decisions of the Privacy Commissioner and the Administrative Appeal Board, in which the court upheld the decisions of the Privacy Commissioner and the regulatory body in all but two disputes.

The rest of the 15 cases (71 per cent) were legal challenges brought against individual parties, and seven of them were concerned with access to personal data and disclosure of such under Section 58 of the PDPO. As the majority of court decisions are on this issue, this will be further discussed in the section entitled 'Data Access Request, Discovery and Exemption' of this article. We will find that on the issue of data access and the reliance on the exemption clause, the court has given an expansive interpretation of Section 58 and sided with the plaintiffs in six out of the seven actions. For the rest of the eight cases concerning claims against individual third parties, the court had dismissed all actions except in one appeal case where the court ruled in favour of the appellant due to the fact that the plaintiff had brought an action against the wrong party.[70]

In total, of the 21 judgments delivered by the court, ten decisions (47.6 per cent) were allowed and 11 (52.3 per cent) were dismissed. Of the ten decisions allowed, six were on data access and exemption to disclosure under Section 58 of the PDPO; two were on the unlawful collection of personal data under DPP1, in which the court overruled decisions of the Privacy Commissioner and the AAB; and the other two were on DPP3 and Section 64(1) of the DPDP.[71]

Of the two cases where the court overruled the decision of the Privacy Commissioner, one of them was *Eastweek Publisher Ltd. & Anor v Privacy Commissioner for Personal Data*,[72] where the court took a decision about what would not count as personal data. The Court of Appeal ruled that a photo of an anonymous individual taken by a magazine was not a form of personal data collection as the magazine never intended or sought to identify the individual concerned.[73] Although the case is hailed as a victory for photo-journalism and news gathering in general, many may not agree with the analysis especially when a person can be easily identified by others through a photo image. Since much discussion has already taken place about *Eastweek*, there is no need for further detailed elaboration here.[74] Instead, we will discuss the second case where the court overruled the decision of the Privacy Commissioner and the AAB, *Cathay Pacific Airways Ltd v Administrative Appeals Board & Anor*,[75] in detail in the next section.

In addition, in the next section, we will cover three principal areas of concern that have underlined the development and significance of personal data litigation in (i) the collection and use of personal data by employers; (ii) the use of medical records by doctors; and (iii) making data access requests and discovery. These three areas are chosen for different but equally significant reasons. First, 11 (52.3 per cent) of the 21 cases before the courts involved disputes in the work place. Second, Hong Kong is currently considering establishing a system of e-health records. Third, seven (33.3 per cent) out of the 21 cases were about data access requests and discovery and the court had ruled in favour of the plaintiffs in six out of the seven cases.

Collection and use of personal data by employers

Statistics mentioned earlier in this article have shown that the majority of complaints (29 per cent) before the Administrative Appeals Board were brought by complainants in their capacity as employees. Although the majority of cases brought before the courts were not brought by employees, 52.3 per cent of them were work-related. Thus, the ratio on personal data protection being developed in this area cannot be ignored.

We referred briefly to an earlier case involving Cathay Pacific which was fought all the way to the Court of First Instance in Hong Kong. The case was *Cathay Pacific Airways Ltd v Administrative Appeals Board & Anor*.[76] Cathay Pacific Airways (Cathay) is the largest airline in Hong Kong employing several thousand employees as cabin crew. In 2005, Cathay

69 Out of the 21 cases, six cases were brought by three different parties on appeal from the Court of First Instance.

70 *Jiang Enzhu v Lau Wai Hing Emily* [2000] 1 HKLRD 121.

71 DPP3 is on unauthorized use of data while s. 64 of the PDPO is on specific offences, for example in providing misleading or false information to the Privacy Commissioner.

72 [2000] 2 HKLRD 83.

73 Ibid.

74 For comments on the *Eastweek* case, see Raymond Wacks, 'Privacy and Anonymity' 30 Hong Kong Law Journal (2000) 177, and Office of the Privacy Commissioner for Personal Data, Hong Kong, Chapter 3 (n. 47).

75 [2008] 5 HKC 229.

76 Ibid.

introduced a revised programme for its cabin crew members, effectively requiring those staff who took long or frequent sick leave to give consent to Cathay to have access to their relevant medical records for the past 12 months. Any member who refused to participate or cooperate in the new programme might be subject to disciplinary action. It was in 2007 that the Privacy Commissioner received anonymous complaints that Cathay had been collecting personal data on its staff unlawfully and unfairly in violation of DPP1(2). Upon investigation, the Commissioner recognized that medical records were of a highly sensitive personal nature. While the means of collecting was lawful, the Commissioner was of the opinion that the method was unfair because the staff were under threat and fearful of a disciplinary process for failure to cooperate. Thus the consent given by them was not free consent.[77] The Commissioner's decision was supported by the Administrative Appeals Board.[78] However, Justice Hartmann and Justice Lunn of the Court of First Instance did not support their decisions.

In their judgment, Justices Hartmann and Lunn asserted that the PDPO had never required that consent given by a data subject must be based on 'complete freedom' of choice 'unburdened by any possible adverse consequences'.[79] Rather, DPP1(3) only required that a person be fully informed on the date of or before the collection of data and made fully aware of the consequences of failure to supply the data.[80] Therefore, since the disclosure of medical records was properly and fairly made mandatory in the circumstances, it was only necessary to advise the employee of the consequences of failure to make a disclosure.[81]

The litigation aptly illustrates, on the one hand, the perennial conflict between employees' entitlement to benefits and privacy (personal data) protection and, on the other, the employers' interests in preventing abuse of the leave system. While the result of the judgment was fair and justified in the given context, the focus of the Commissioner's decision and the subsequent judicial review seemed to have be been on the 'blunt and brusque manner', 'the threatening or oppressive tone' of the employer.[82] What may be a more useful reference and guideline for future disputes between employees and employers on similar disputes would be on the scope and nature of the personal data collected, or, in fact, whether such collection is necessary and excessive, and whether an employer should have access to an employee's medical data covering a 12-month period.

Use of medical records by doctors

Thus far, this study is premised on the basis that the PDPO is being relied on as the principal ordinance in complaints and litigation. An exception is the case of *Chan Tak Ming v Hong Kong Special Administrative Region* before the Court of Final Appeal.[83] Chan was a doctor, appealing his conviction for misconduct in public office. Obviously, this was a criminal case and the PDPO was not the major piece of legislation at issue. Yet, discussion of data principles and protection of personal data was intended to better inform what would constitute an act of misconduct in public office.

In 2007, Chan was a senior oncologist in a public hospital, who had tendered his resignation and was about to set up his own private practice. Before leaving the hospital, he wished to inform his patients of his departure and new practice. Initially, Chan only wanted to inform 500 patients who had a close long-term relationship with him. However, after Chan had sought help from a clerk to obtain the contact information of his patients for the above-mentioned purpose, the clerk and her supervisor inadvertently offered a quicker solution—downloading the contact information and electronic records of 2,000 patients from the hospital's computer system for Chan.[84] After this was discovered, Chan was prosecuted and convicted before the magistrate's court for misconduct in public office under common law, and for obtaining access to a computer with a view to dishonest gain for himself under Section 161(1)(c) of the Crimes Ordinance.[85] He was also found by the magistrate to have violated the Professional Code and Conduct of the Medical Council of Hong Kong, and Data Protection Principle 3 (unauthorized use of personal data) of the PDPO.[86]

By the time the case had reached the Court of Final Appeal, the single issue had become whether Chan was rightly convicted for misconduct in public office. This common law offence is committed when 'a public official in the course of or in relation to his public office willfully misconducts himself by act or omission...

77 Ibid, paras 34–37.
78 Ibid, paras 39–40.
79 Ibid, para. 41.
80 Ibid, para. 42.
81 Ibid, para. 45.
82 Ibid, para. 51.
83 (2010) 13 HKCFAR 745 <http://legalref.judiciary.gov.hk/lrs/common/ju/ju_frame.jsp?DIS=74140&currpage=T>accessed 1 August 2012; appeal dismissed, from *HKSAR v Chan Tak Ming, Paddy* [2010]3 HKC 382.
84 *HKSAR v Chan Tak Ming, Paddy* [2010]3 HKC 382, 386, para. 7.
85 Cap 200, Laws of Hong Kong.
86 *HKSAR v Chan Tak Ming, Paddy* [2010]3 HKC 382, 388–390, paras 13–21.

without reasonable excuse of justification; and where such conduct is serious . . . having regard to the responsibilities of the office and the office-holder, the importance of the public objects which they serve and the nature and extent of the departure from those responsibilities.'[87] Although the Court of Final Appeal did not refer to the PDPO, its relevance and significance for the interpretation of the meaning and standard of 'serious' misconduct should not be ignored.

The appellant challenged the court on the grounds that he was wrongly convicted for misconduct in public office on the basis that although official data had been abstracted for private use, the prosecutor had never specified in the pleadings to what private use that data was put. To this, the court replied that the facts were indisputable because the appellant had obtained official data in order to advertise his private practice which formed a 'plainly sufficient basis on which to find the necessary seriousness' of misconduct. Clearly, the patients in a public hospital were entitled to have their privacy respected.[88] Furthermore, the court reiterated that the test to be applied was whether the misconduct was 'sufficiently serious'. The court quoted the lower court's judgment, indirectly endorsing that the use of patient data for such purpose was 'extreme'.[89] It was a 'breach of trust'[90] and an exploitation of patients' lack of knowledge for Chan's intention to secure business.[91] Finally, the court agreed that the legal test for the required state of mind for such an offence is any deliberate intention, including wilful disregard of the risk of one's conduct.[92] Although the court explained that it was inappropriate for the appeal judge to use the term 'recklessness', it was right for him to point out that Chan had committed the act wilfully and intentionally for failing to take steps to take advice or counsel before taking and using the personal data.[93]

Without referring to the PDPO, the need for personal data protection of patients has informed the court both indirectly and effectively in setting the normative standard of professional conduct for medical practitioners, and the criminal standard for misconduct in public office. Chan's proposed use of patients' personal data in 2007, and the unquestionable support from the clerical staff were telling signs of the lack of awareness for such protection in hospital culture at that time. This 2010 judgment delivered by the highest court in Hong Kong is an important reminder of such need, especially at this critical time when Hong Kong is considering the implementation of a system of electronic medical health records.

Data access request, discovery, and exemption

As mentioned in our previous discussion under AAB decisions, another noticeable trend in personal data litigation is the exercising of the rights of data subjects to request data access. Specifically, under Section 18 and DPP6 of the PDPO, an individual may make a request to ascertain whether the data user holds personal data about him or her, or if there is a right of access to have a copy of such data. It sounds only reasonable for the data subject to request this. Yet, the situation can become complicated when the data requested also covers a third party, or when the data requested are not about the applicant but are about a third party. In this case, what is involved is often an application for non-party disclosure in court proceedings.

The first situation when personal data involves both the applicant and third parties is being discussed in the case of *Wu Kit Ping v Administrative Appeals Board*.[94] The facts concerned an earlier complaint brought by Wu against a clinic for alleged incorrect diagnosis of her medical condition, which was considered to be unfounded by the Department of Health. Later, Wu made a formal data access request to receive her medical report and the report of the complaint investigation, but she only received a redacted copy with the names of certain persons being blacked out. She complained to the Privacy Commissioner and the AAB but to no avail. Undeterred, she went to court and sought judicial review.

The issue before the court was whether the AAB had decided correctly that the provision of a redacted statement was lawful and constituted proper compliance with the data access request. To this, the court affirmed the decision of the Commissioner and the AAB, and held that a data subject is entitled to a copy of any representation of information relating directly or indirectly to herself but not to every document which referred to her. Justice Saunders stated very clearly that '[i]t 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 that individual.'[95] Specifically, he ruled that the name of the writer of the report was not, in fact, part of the personal data of the applicant.[96] In

87 (2010) 13 HKCFAR 745, para.3.
88 (2010) 13 HKCFAR 745, para. 25.
89 Ibid, para. 19.
90 Ibid, para. 19.
91 Ibid, para. 20.
92 Ibid, para. 29.
93 Ibid, para. 28 and 29.
94 [2007] 5 HKC 450.
95 Ibid, 457, para. 32.
96 Ibid, 459, para. 38.

addition, he also stated that opinion expressed in the report should be accessible to the applicant only if the opinion was about her.[97] Otherwise, 'an opinion expressed in the same document, by the maker of the document, about the maker of the document himself, unless relating indirectly to the data subject, will not constitute the personal data of the data subject.'[98] The general understanding is that unless the consent of the third party has been obtained, request for such disclosure should be rejected.[99]

The above ratio has indeed provided a sensible guideline to data access requests involving the personal data of third party. But what about if one wishes to have access to documents not directly related to oneself, but likely to have critical information related to one's interest? Examples of such requests include an estranged wife seeking an order from the court directing the Director of Housing to disclose the new address of her husband who had moved into a new unit and failed to pay a maintenance fee;[100] a case of another bitter husband who applied to the court to ask for the specific discovery of invoices of payment issued by a private detective company hired by his wife to observe his activities;[101] a third example is a company that applied for discovery against an estate management company for a CCTV tape recording of an intended civil claim against a suspected case of employee theft.[102] Here, the courts are being asked to deal with the second scenario of non-party disclosure application.

It is not unusual for data users to turn down requests from applicants for fear of infringing the rights of any third party involved, as evidenced in the response from the Director of Housing and the estate management company mentioned in the previous paragraph. Eventually, in those two cases, the court had to order disclosure of personal data based on Section 58(1)(d) of the PDPO. The said provision is an exemption clause which allows a data user to disclose information without the consent of the data subject, and allows others to have access to personal data if one of the statutory purposes stated in Section 58(1) could be satisfied, which includes the 'remedying of unlawful or seriously improper conduct, dishonesty or malpractice, by persons'. Although Section 58 of the PDPO allows exemption from the legal requirements governing the use of personal data (DPP3) and data access requests (s. 18 and DPP6), its interpretation and application is not without difficulty as illustrated in the case of *Lily Tse Lai Yin & Others v The Incorporated Owners of Albert House & Others*.[103]

This case concerned a tragic accident involving the collapse of a canopy onto a pavement, seriously injuring and causing the death of pedestrians. At the time when the criminal investigation was going on, the victim plaintiffs wanted to have access to a witness statement taken by the police after the accident in order to bring a civil claim for personal injuries. The police objected to the request based on DPP3 of the PDPO, which required consent from the data subjects (witnesses) and, regarding the use of data collection (witness statement), they must be consistent with the purpose of data collection (criminal investigation and prosecution).

However, Justice Suffiad considered that Section 58 should apply as the application for non-party discovery in the given case was concerned with a claim for damages in a personal injuries action, which was a civil wrong, falling within the scope of Section 58(1), allowing 'remedying... unlawful or seriously improper conduct'. Furthermore, he pointed out that DPP3 itself also allowed the secondary use of personal data for a purpose directly related to the initial purpose. Since both criminal investigation and the civil claims were concerned with understanding the same event, it was unnecessary to ask for additional witness' consent for the civil action. However, critics have expressed their reservation with Justice Suffiad's approach and have cautioned for a more constrained interpretation. Wacks and McLeish argue that while the application of the law may well be justified in the given context of the case, the judge seems to have forgotten the additional legal requirement under Section 58.[104] They point out that Section 58 has two limbs. For an exemption to apply, one has to be satisfied that one of the said purposes under Section 58(1) can be fulfilled. Then one has to show that complying with the data protection principles (DPP3, DPP6, and Section 18) would be likely to prejudice the said purposes. Among these various purposes mentioned under Section 58(1) are the

97 Ibid, 460, para. 51.

98 Ibid.

99 Ibid, 458, para. 37.

100 *M v M* [1997] HKFamC 2.

101 *Jorst Joachim Franz Geicke v 1-Onasia Ltd. and others* (17/10/2011, HCA 2379/2009) <http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=78646&QS=%2B&TP=JU> accessed 3 August 2012.

102 [2010] 2 HKLRD 1155.

103 10/12/1998, HCPI 828/97 <http://legalref.judiciary.gov.hk/lrs/common/ju/ju_frame.jsp?DIS=20437> accessed 3 August 2012.

104 Raymond Wacks, 'Privacy and Process' 29 Hong Kong Law Journal (1999) 176. Robin McLeish, 'Discovery and Data Protection' 31 Hong Kong Law Journal (2001) 49.

remedying of seriously improper conduct, prevention or detection of crime, and the prevention or preclusion of significant financial loss.

A more cautious approach has indeed been adopted in the later case of *Cinepoly Records Co. Ltd, and Others v Hong Kong Broadband Network Ltd. and Others*.[105] In addition to following the judgment of *Lily Tse*, the court also applied the second requirement of prejudicing the stated purpose of the law. In addition, In *Wu Kit Ping*, the court reminds us that the purpose of PDPO is not to 'supplement rights of discovery in legal proceedings, nor to add any wider action for discovery for the purpose of discovering the identity of the wrongdoer'.[106]

Having said that, application for non-party disclosure may be less complicated under the new personal data regime. Under Section 60B of the new PDPO, one may be exempted from the requirement of disclosure and consent under DPP3 if the use of the data is required or authorized by the court, or in connection with any legal proceedings in Hong Kong; or for establishing, exercising, or defending one's legal rights.[107]

Conclusion

This study is intended to underline the major legal development and the identification of the major issues on personal data protection in Hong Kong. Although the latest legislative reform may have given the impression that the high point of the personal data debate is on direct marketing, our survey of actual complaints and litigation reveals the contrary. However, this does not mean that personal data protection in direct marketing is not a concern for the public. A plausible explanation is that consumers may not even be aware that their data have been sold or passed onto a third party. In fact, as we have shown in our study, the latest legal reform rightly reflects the concerns of the public on unauthorized use of personal data which is confirmed by the bulk of cases and complaints on this alleged violation (DPP3). Alongside this, there is the equally pressing concern of data access requests and the related issue of non-party discovery for court proceedings. Our survey of the number and nature of cases reveal that much of the personal data agenda has been concerned with disputes between employees and employers, and between patients and hospitals on personal data protection.

Over the years, what has emerged is definitely an awareness of personal data protection in thought and practice as reflected in the different complaints and cases before the Privacy Commissioner, the Administrative Appeals Board, and the court, especially on issues related to unauthorized use of personal data, and data access requests. From the decisions of the AAB and the court, we have noticed a restrictive interpretation of the concept of personal data but an expansive reading on data access requests and related provision. The latter proves to be particularly important as Hong Kong does not have a freedom of information law. Another important feature to note is there is evidently a growing reliance on and trust of the Privacy Commissioner, and his decisions have been confirmed by the AAB in most cases (87 per cent). Likewise, decisions from the Privacy Commissioner and the AAB have also been upheld by the court in the majority of cases (60 per cent). It is through these challenges that new approaches and an understanding of personal data protection has been opened up in the Hong Kong community.

Yet, many questions and challenges have yet to be addressed. Other than the unknown impact and effectiveness of the new *Amendment Ordinance*, unresolved problems existing include data leakage and data security. The statutory provision on cross-border data flow has yet to come into force.[108] Challenges brought by ever-advancing technologies in cloud computing, geolocation data, online naming and shaming,[109] and other areas have yet to attain a legal solution.

Thus, personal data protection still has a long way to go in Hong Kong. For now, perhaps, it is encouraging to see how personal data protection had grown from only about 50 complaints before the Privacy Commissioner more than a decade ago to a field that could garner support from the mass population to bring the eventual long-awaited legal reform at its present time. Amidst others, the 1995 legislation has delivered an important task: 'to produce, out of the society we have to live in, a vision of the society we want to live in'.[110]

doi:10.1093/idpl/ips033
Advance Access Publication 28 November 2012

105 (28/08/2006, HCMP943/2006) <http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=54082&QS=%24%28cinepoly%7Crecords%7Ccompany%29&TP=JU> accessed 7 August 2012.

106 [2007] 5 HKC 457, para. 32.

107 Section 34 of the Amendment Ordinance adds s. 60B to the PDPO.

108 Section 33 of the PDPO.

109 This is popularly known as 'human flesh search' or 'qidi' in Chinese society, in which the personal data of an individual are exposed by numerous unknown online contributors. For further discussion on the phenomenon and its legal implications, Anne SY Cheung, 'Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd' [2009] 2 Journal of Media Law 191.

110 Alec Scott, 'Frye's Anatomy' (quoting a saying from Northrop Fye), University of Toronto Magazine (Spring 2012) 39.