University of New South Wales
University of New South Wales Faculty of Law Research Series
2012

Year 2012 *Paper* 15

Hong Kong's privacy enforcement: Issues exposed, powers lacking

Graham Greenleaf* Robin McLeish†

*University of New South Wales, g.greenleaf@unsw.edu.au

†Gray's Inn, London, and Hong Kong SAR, mcleish@templechambers.com

Hong Kong's privacy enforcement: Issues exposed, powers lacking

Graham Greenleaf and Robin McLeish

Abstract

This article concerning the Hong Kong SAR is the second in a series surveying significant recent examples of data privacy enforcement actions in the Asia-Pacific. Hong Kong's Privacy Commissioner for Personal Data (the PC) does not have any power under the Personal Data (Privacy) Ordinance (the Ordinance) to award compensation or order other remedies. His most significant legal power is the power to serve an enforcement notice when he concludes that a data user is likely to repeat or continue a contravention of the Ordinance. Where a suspected breach of the Ordinance may constitute a criminal offence he may refer the matter to the Police and the Department of Justice for investigation and prosecution. Where the PC completes investigations of more serious cases of breaches of the Ordinance, it is now common for him to issue detailed reports on the outcomes under s48(2), and in 2010 and 2011 he issued thirteen such reports.

One of the s48(2) reports issued in 2010 was on the 'Octopus' case, which involved the transfer of personal data of users of the widely-used Octopus contactless-card payment system to third-parties for direct marketing purposes. The PC issued s48(2) reports in June 2011 in respect of four of the bank cases in which he named the banks, and announced that such naming 'will henceforth be adopted for all investigation reports published under section 48(2) of the Ordinance', subject to certain exceptions. He is is the first personal data authority in the Asia-Pacific to explicitly adopt 'naming and shaming' of data users found to have been in breach as a means of promoting compliance with personal data legislation.

This article examines a wide variety of s48(2) reports on the following issues: the CITIC Bank case, where there was mass infringement, but no real penalty, on data retention, on fees for data access which were excessive, on disclosure of

details of a debtor's relatives, on unfair collection practices and improper use of public register information, and where covert monitoring was unfair collection. Other than in the debt collection case, the PC did not serve an enforcement notice in any of the cases summarised above because he was not of the opinion that the breaches found by him had occurred in circumstances that made it likely they would continue or be repeated.

The most recent s48(2) reports relate to "paparazzi" style photo journalism using systematic surveillance and telescopic lens photography to take clandestine photographs of TV personalities within their private residences. In both cases, the PC found that the taking of the photographs amounted to collection of their personal data by unfair means contrary to DPP1(2). He served enforcement notices directing the magazines to remedy their contraventions and the matters occasioning them. The details of the enforcement notices are, however, omitted from the published versions of the PC's reports.The two magazines have appealed to the Administrative Appeals Board. The article also examines a number of criminal prosecutions resulting from breaches of the Ordinance which have resulted in small fines. The PC commented that 'the current level of fine is too low to be of deterrent effect, especially for organizational data users'. The overall conclusion is that the PC is tackling a wide variety of compliance issues in spite of the limitations on his formal powers of enforcement, and the absence of powers to order compensation or other remedies, as well as the inadeuqate penalties imposed by Courts.

Hong Kong's privacy enforcement: Issues exposed, powers lacking

Graham Greenleaf and Robin McLeish[*]

Privacy Laws & Business International Report, Issue 116: 25-28, April 2012

8 April 2012

Contents

This article is the second in a series[1] surveying significant recent examples of privacy enforcement actions,[2] in the Hong Kong SAR, most occurring in 2011. The next article in the series will cover the other Chinese-speaking Asian jurisdictions, Taiwan, Macau and the Peoples Republic of China.

'Name and shame' strengthens inadequate powers

Hong Kong's Privacy Commissioner for Personal Data (the PC) does not have any power under the *Personal Data (Privacy) Ordinance* (the Ordinance) to award compensation or order other remedies. His most significant legal power is the power to serve an enforcement notice when he concludes that a data user is likely to repeat or continue a contravention of the Ordinance.[3] The PC also has powers to issue reports on recommendations arising from inspections of personal data system and the results of investigations into breaches of the Ordinance. In addition, where the PC comes across a suspected breach of the Ordinance that may constitute a criminal offence he may refer the matter to the Police and the Department of Justice for investigation and prosecution.[4] In the two calendar years 2010 and 2011 the PC issued thirteen such reports (five in 2010 and eight in 2011).

One of the s48(2) reports issued in 2010 was on the 'Octopus' case, which involved the transfer of personal data of users of the widely-used Octopus contactless-card payment system to third-parties

[*] Graham Greenleaf is Professor of Law & Information Technology, University of New South Wales; Robin McLeish is a Barrister in Hong Kong.

[1] See Greenleaf G and Evans K 'Privacy enforcement strengthens in Australia & New Zealand' (2012) 115 PLBIR 8-13

[2] By 'significant examples of privacy enforcement actions' we mean as follows. First, the action results from complaints to an authority/Court, or 'own motion' actions by an authority responding to a specific situation. (General investigations or reform proposals by authorities are not included.) Secondly, the authorities concerned could be Data Protection Authorities/Privacy Commissioners but they could also be telecommunications regulators, financial regulators, government agencies and so on. Independent industry self-regulatory bodies could also be included. Court or Tribunal decisions of any type are also included. Third, the result is a significant remedy for an individual; or a remedy for a group of people; or a significant change in the interpretation of the law; or a significant change in business/government practices.

[3] See Greenleaf, G 'Country Studies: B.3 - Hong Kong (Information privacy in Hong Kong', Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments, D. Korff, ed., May 2010, at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2025550>

[4] Section 48(2) reports may be found at <http://www.pcpd.org.hk/english/publications/invest_report.html>

for direct marketing purposes.[5] Around the time the Octopus case blew up in 2009, the PC commenced investigation into fourteen similar cases, eight of which involved telecommunications companies, five involved banks and the one involved an insurance company. The PC issued s48(2) reports in June 2011 in respect of four of the bank cases in which the PC named the banks concerned (Citibank (Hong Kong) Limited, Fubon Bank (Hong Kong) Limited, Industrial and Commercial Bank of China (Asia) Limited and Wing Hang Bank Limited) and announced that:

> 'This practice of naming the organizational data user which has contravened the requirements under the Ordinance will henceforth be adopted for all investigation reports published under section 48(2) of the Ordinance, subject to the following exceptions: (i) it is against Hong Kong's public interests such as security, defence or international relations; (ii) it will prejudice the investigation or detection of crime; or (iii) there are other legislative requirements prohibiting publication and identification of the relevant data users in particular cases.'[6]

Explaining the rationale for this new practice, the PC commented, 'We hope that the practice of naming data users will invoke the sanction of public scrutiny. In turn it will serve to encourage compliant behaviour by data users concerned and related parties.'

The PC is the first personal data authority in the Asia-Pacific to explicitly adopt 'naming and shaming' of data users found to have been in breach as a means of promoting compliance with personal data legislation. However, in order for a data user to be 'named and shamed' it must have committed a breach of the Ordinance that the PC considered serious enough for the issuing of a s48(2) report, rather than a brief case note or summary, and the case must not fall within any of the exceptions he has laid down.

The CITIC case: mass infringement, no real penalty

In December 2011 the PC issued a fifth s48(2) report on the transfer of customer data by a bank to third parties for direct marketing. This disclosed that CITIC Bank International Limited (CITIC) had transferred personal data of around 90,000 of its account or credit card customers to insurance companies in the previous five years. The personal data that had been transferred included name, gender, phone number, address, date of birth, partial HK ID number, marital status, partial account number, account type, partial credit card number, card type, number of months lapsed since becoming a customer of CITIC, and whether the customer was a holder of any existing policy of the insurance companies concerned.

The PC concluded CITIC had not taken all practicable steps to ensure that on or before the collection of the personal data from its customers, the customers had been explicitly informed of the classes of persons to whom the data might be transferred as required by the notification data protection principle of the Ordinance (DPP1(3)). He further concluded that such arrangements constituted in substance the sale of personal data by CITIC for monetary gain. Since this purpose of use of the customers' personal data was not stated in the notice given by CITIC at the time of collection the PC considered it fell outside the purpose for which CITIC had collected the data concerned (the Collection Purpose), and was not for a purpose directly related to the Collection Purpose (having regard to the reasonable expectations of the customers) or done with the customers' express consent (as required by the Ordinance if

[5] See Greenleaf, G 'Octopus scandal exposes Hong Kong privacy deficiencies' *Privacy Laws & Business International Newsletter* Issue 108, December 2010

[6] http://www.pcpd.org.hk/english/infocentre/press_20110620.html

personal data are to be used for a purpose other than, or not directly related to, the Collection Purpose). Accordingly, the PC concluded that CITIC had contravened the use limitation principle (DPP3) as well as the notification principle (DPP1(3)).

In spite of the PC's finding of breaches of two data protection principles in relation to 90,000 customers, since CITIC had ceased all programmes and activities involving the transfer of customer data to unconnected third parties for marketing purposes, such data as had been so transferred had all been destroyed and CITIC had given undertakings as to future compliance with the Ordinance, the PC considered repeat contraventions by CITIC were unlikely and no enforcement notice was served on CITIC. There is also no suggestion in the report that CITIC disgorged the revenue obtained from these programmes and activities by making a payment to a charitable organisation, as occurred in the Octopus case, or otherwise.

Wide variety of cases investigated by the PC

Other s48(2) reports issued by the PC since the beginning of 2010 illustrate the wide variety of cases investigated by the PC.[7]

- *Data retention* An investigation prompted by a complaint revealed that Hang Seng Bank had been engaged in the practice of retaining its customers' bankruptcy data for 99 years. The PC found this contravened the Ordinance's personal data retention restrictions (DPP2(2) and s26(1)). At the conclusion of the PC's investigation, the bank gave an undertaking. which the PC considered adequately addressed his findings of contravention of the Ordinance, not to retain customers' bankruptcy data for more than 8 years from the dates of the declaration of bankruptcy and erase and destroy such data already held of a greater vintage than 8 years.

- *Fees for data access excessive* A bank set up a new fee structure intending to charge all customers a flat-rate fixed fee of HK$200 (US$25) for complying with a data access request to obtain copies of his/her personal data in the custody of the bank. The Ordinance (s28) prohibits data users from imposing an 'excessive' fee for complying with a data access request, but does not define what is 'excessive'.[8] The PC was of the opinion that a data user may recover only the labour costs and actual out-of-pocket expenses incurred in locating, retrieving, reproducing and sending the requested data to the requestor based on the work involved being done by a clerical or administrative staff. The bank failed to establish it had taken this approach, and was found to have imposed a fee structure that was liable to be excessive. The Bank abandoned the proposed fee structure before implementing it.

- *Disclosure of details of debtor's relatives* A finance company passed a loan application form containing personal data of the relatives of a debtor to a debt collection agency, which then posted up personal particulars of the relatives in public places as part of its debt recovery activity.[9] The PC found that this practice of the debt collection agency contravened the use limitation principle (DPP3). He also found that, although the finance company had not expressly instructed the debt collection agency to engage in the practice concerned, it had impliedly authorised it as the agency's principal, meaning that it too had contravened the use limitation principle (DPP3).[10] In the absence of any information that the finance company

[7] The PC's s48(2) reports are at < http://www.pcpd.org.hk/english/publications/invest_report.html>

[8] The bank is not named this s48(2) report, which predated the public announcement of the PC's 'naming and shaming' practice,

[9] Neither the finance company nor the debt collection agency is named in this s48(2) report, which predated the public announcement of the PC's 'naming and shaming' practice,.

[10] By virtue of s65(2) of the Ordinance.

would take measures to prevent a repetition of what had occurred, the PC considered it was likely that the contravention would continue or be repeated. Accordingly, he served an enforcement notice on the finance company requiring it to instruct its authorised debt collection agents in writing not to publicly display the personal data of family members of debtors..

- *Unfair collection practices and improper use of public register information* A complainant was dissatisfied that a company involved in the management of parking facilities, Imperial Parking (HK) Limited (Imperial), had collected his personal data from the Register of Vehicles (the Register) maintained by the Transport Department for direct marketing purposes in order to promote their parking services. The PC found that Imperial was in breach of two Principles in the Ordinance. It breached the requirement of DPP 1(2) to collect personal data by means which are lawful and fair because its employee had stated to the Transport Department in the Application Form for a Certificate of Particulars of Motor Vehicle (the Application Form) that the purpose for the application was for "legal proceedings", but the real purpose was to promote preferential parking rate at Imperial's Car Park. In addition, although the relevant legislation did not state an express purpose for which the Register was established, the PC found a breach of the use limitation principle (DPP 3) because Imperial's act of using the personal data of car owners for business promotion was unrelated to the purposes of the Road Traffic Ordinance. Therefore, it fell outside the reasonable expectation of the Complainant. The Transport Department stated in the Application Form that the personal data in the Register would be used for the purposes of traffic and transport matters. Imperial's use was neither a legitimate primary or secondary use of the personal information. In response to the PC's investigation, Imperial destroyed the data it had obtained from the Register and gave an undertaking not to collect vehicle owners' data from the Register for purpose of marketing its services. The PC also noted the Transport Department was taking steps to amend the legislation under which the Register was established in order to clarify the purposes for which it was maintained and limit the circumstances in which the personal data of vehicle owners would be released. 'If data users indiscriminately use personal data retrieved from public registers for direct marketing, they do so at their own peril' said the PC.

- *Covert monitoring was unfair collection* Covert video recording by a property management company, Hong Yip Service Company Limited, of its employees in a changing room on a housing estate by means of a 'pin-hole camera' was found by the PC to be unfair collection of personal data in breach of DPP1(2). The PC considered, 'Covert monitoring is generally regarded as highly privacy intrusive.' He also noted that under the 'Privacy Guidelines: Monitoring and Personal Data Privacy at Work' issued by him there must be reasonable suspicion of the commission of unlawful activity and the need to resort to covert monitoring to detect or collect evidence of that unlawful activity must be absolutely necessary under the circumstances. . In the course of the PC's investigation, Hong Yip removed the recording device and confirmed it had destroyed all the images of the complainants recorded by it.

Other than in the debt collection case, the PC did not serve an enforcement notice in any of the cases summarised above because he was not of the opinion that the breaches found by him had occurred in circumstances that made it likely they would continue or be repeated.[11]

Taking on the media

So far in 2012 the PC has issued four s48(2) reports, the most recent of which are two s48(2) reports (both issued on 28 March 2012) that relate to "paparazzi" style photo journalism using systematic surveillance and telescopic lens photography to take clandestine photographs of TV

[11] As required by s50(1)(b) of the Ordinance before an enforcement notice may be served on a data user found to have breached a requirement of the Ordinance.

personalities within their private residences. The first of these cases involved the publication by Sudden Weekly of photographs of a male TV personality within his flat in a state of undress. His flat was on the high floor of a building that was not exposed to public view with unassisted vision. In the second case, Face Magazine published pictures of an unmarried male and female TV personality engaged in acts of daily life and intimacy within a flat that faced a hillside some distance away.

In both cases, the PC found the individuals concerned would not reasonably expect that they would be photographed within their homes and that the taking of the photographs amounted to collection of their personal data by unfair means contrary to DPP1(2) of the Ordinance. The PC commented, 'An individual should be protected from unwarranted intrusion to his/her personal life, irrespective of his/her social status and occupation. The complainants in question should not be deprived of this privacy right just because they are TV artistes.'

The PC dismissed public interest justifications for the publication of the photographs based on the magazines' claims the photographs demonstrated that denials of cohabitation by the TV personalities concerned were untrue, saying 'the state of cohabitation or otherwise is an individual's sensitive personal data which he or she is under no obligation to divulge to others.' Further, the 'disproportionate use of lurid and sensational photos by the two magazines casts grave doubt on their contention that they have acted in the public interest rather than to satisfy readers' curiosity of the private lives of the artistes concerned.'

Whereas in the cases summarised above no enforcement notices were served due to the absence of a threaten continued or repeated breaches of the Ordinance (other than in the debt collection case), in these cases the PC served enforcement notices directing the magazines to remedy their contraventions and the matters occasioning them. The details of the enforcement notices are, however, omitted from the published versions of the PC's reports.

The matter may not rest there since the two magazines have appealed against the issuing of enforcement notices against them to the Administrative Appeals Board.

Broad scope but small fines

Investigations and prosecutions of criminal offences under the Ordinance are carried out by the Police and the Department of Justice. Such investigations are usually undertaken as a result of referrals by the PC but he has to act quickly because of the default 6 month limitation period applicable to summary offences. In recent years, the PC has successfully fostered improved understanding with the Police and the Department of Justice in order to increase the number of successful prosecutions.

Two examples of recent successful prosecutions are as follows.

- Ricacorp Properties Limited, a large property agent, and its estate agent were convicted of breaching s34(1)(ii) of the Ordinance, which requires a data user to stop using an individual's personal data for direct marketing purposes upon receipt of an opt-out request, such contravention being an offence under s64(10). Both pleaded guilty and were fined HK$2,500 (US$322) and HK$2,000 respectively, although the maximum fine is HK$10,000. The Complainant purchased a flat in 2007 via the Company, which collected the Complainant's personal data. Since then, the Complainant received numerous calls from the Company soliciting sale or purchase of properties, and requested the Company more than once not to call her for this purpose, but it continued to do so. The PC referred the complaint to the Police.

- In a similar case, CITIC Bank International was convicted after pleading guilty and was fined $2,500 (US$322), for continuing to send direct mail to a customer since 2008 despite her requests to stop. Since the commencement of the Ordinance in 1996, this is the second conviction for contravention of the Ordinance due to sending of direct mail despite the complainant's opt-out requests.

The PC commented about each of these cases that 'it is believed that it represented only the tip of an iceberg. … This also reflects that the current level of fine is too low to be of deterrent effect, especially for organizational data users. The PC expects that through legislative amendment the Administration's proposal of increasing the penalty to $500,000 and imprisonment for 3 years will cause more deterrent effect'. Hong Kong's Legislative Council has not yet enacted this legislation.[12]

The overall conclusion to be drawn from the enforcement actions that have been surveyed in this article is that the PC is tackling a wide variety of compliance issues in spite of the limitations on his formal powers of enforcement and absence of powers to order compensation or other remedies.

[12] See McLeish R and Greenleaf, G 'Reform of Hong Kong's Privacy Ordinance After 15 Years', Privacy Laws & Business International Report, Issue 113, pp. 15-17, October 201, available at <http://papers.ssrn.com/abstract_id=1972669>