COMMENT

WHO LET THE CAT OUT OF THE BAG? INTERNET DATA LEAKAGE AND ITS IMPLICATIONS FOR PRIVACY LAW AND POLICY IN HONG KONG

The cat is out of the bag and there is no putting it back. On Friday, 10 March the South Morning China Post reported that 20,000 complaint files against the Hong Kong police were freely accessible on the Internet on the website www.china2easy.com. Included in the complaint files were the names, addresses, and identification numbers of complainants, the dates of the complaints, and in a few instances, details of previous criminal convictions. Some of the more serious cases involved corruption, fraud, and sexual abuse. Of the cases disclosed, seven are still being investigated. While the information on the website was quickly removed, the information could still be accessed several days later via the Google Archives and Cache.[1] It soon became apparent that this information had been leaked and made available on the Internet some three years earlier, although it was only recently that it was tripped upon and the situation exposed by shareholder activist David Webb.[2] The full extent of the damage sustained by the complainants and the greater Hong Kong community has yet to be assessed.

A series of incidents occurring in Hong Kong at about the same time served to compound the issue. These included the discovery that personal customer records of the telecommunications company CSL, and insurance records of ING customers who had purchased insurance from 1984 and 2004, were available on the Internet;[3] a shooting of two police officers in Tsim Sha Tsui which appeared to be related to police corruption;[4] a complaint lodged with the Privacy Commissioner regarding the unlawful disclosure of personal information from Yahoo!hk leading to the arrest and jailing of mainland journalist Shi Tao;[5] and finally, the release of customers' personal data by employees of banks and financial companies to outside third parties.[6]

These incidents combined to set alarm bells ringing in the Hong Kong community, with calls for reform of personal data law, including Internet

1 The list was additionally uploaded as a bitTorrent file to the Internet by a user know by the pseudonym "Big Crook", with several hundred people having downloaded the list.

2 *See* report in the *South China Morning Post*, 10 Mar 2006.

3 *See* Robin Kwong, "Details of 600 insurance holders found on Google," *South China Morning Post*, 14 Mar 2006.

4 *See* CNN report, "'Devil Cop' shooting shakes HK," available at http://edition.cnn.com/2006/WORLD/asiapcf/03/26/hk.devilcop.ap/index.html (last accessed 4 Apr 2006).

5 *See* Cynthia Wan and Gary Cheung, "Privacy complaint over Yahoo's mail leak," *South China Morning Post*, 1 Apr 2006.

6 Chandra Wong, "Court hears of 'unwritten law' to release personal data," *South China Morning Post*, 29 Mar 2006.

Service Provider (ISP) liability and responsibilities, a review of data security technology and policies, and a re-evaluation of the Independent Police Complaints Council (IPCC) and the Complaints Against Police Office (CAPO). While the public may have been shocked by these bombshells, many privacy and technology experts were not. They knew that the privacy bomb had been dropped a long time ago, at the beginning of the digital era. It had merely taken time for the public to feel the bomb's reverberations.

These incidents are a timely reminder of the need for an adequate level of technological, administrative, and legislative safeguards to effectively protect personal data in the digital age. This Comment examines the potential legal remedies available for those individuals on the IPCC database whose personal information was disclosed on the Internet.

Using Privacy Law for Legal Redress

The concept of privacy may be divided into two general aspects. The first is protection from invasion of or interference with one's privacy in the more general sense of the term. This is often referred to as interception of communications or surveillance, and is protected by constitutional instruments (Articles 28 and 29 of the Basic Law[7]), international instruments (Article 39 of the Basic Law, which gives effect to Articles 17 and 8 of the International Covenant on Civil and Political Rights (ICCPR)), specific legislative instruments (pending enactment of the Interception of Communications and Surveillance Bill[8]), and general common law principles such as the tort of invasion of privacy. The second aspect relates to the protection of personal data or information privacy which is often protected by personal data instruments, such as the Personal Data (Privacy) Ordinance[9] (PDPO) and by common law principles such as the tort of breach of confidence, and negligence.[10] This Comment is concerned with personal data and information privacy.

Why the PDPO is not Likely to Provide an Appropriate Legal Remedy

Several individuals from the complaint files have lodged complaints with the Privacy Commissioner. It is doubtful, however, that the PDPO will be able to provide an appropriate legal remedy. To understand why this is so, reference must be had to certain terms in the PDPO:

7 The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (Cap 2101).

8 Interception of Communications and Surveillance Bill (Bills Committee first reading, 8/3/2006).

9 Cap 486.

10 For a comprehensive overview of applicable privacy law *see* generally Mark Berthold and Professor Raymond Wacks, *Hong Kong Data Privacy Law: Territorial Regulation in a Borderless World* (Hong Kong: Sweet & Maxwell Asia, 2003).

"data subject" (資料當事人), in relation to personal data, means the individual who is the subject of the data;

"data user" (資料使用者), in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data;

"personal data" (個人資料) means any data–

(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable.

Under section 4 of the PDPO, data users must follow the six Data Protection Principles espoused in Schedule 1. The principles can be summarised using the following headings:

Principle 1: Purpose and manner of collection of personal data
Principle 2: Accuracy and duration of retention of personal data
Principle 3: Use of personal data
Principle 4: Security of personal data
Principle 5: Information to be generally available
Principle 6: Access to personal data

The PDPO binds both the Government (each government agency or department is a separate data user), non-government entities (eg corporations), and individuals. Often, personal data disclosure on the Internet is not subject to the PDPO. The nature of the information disclosed would not constitute personal data for the purposes of the PDPO. For example, one's internet protocol address, home phone number, web browsing habits and even a photograph – anything short of an *intent* to reveal information on the scale of the name of an individual[11] – would likely not fall within the purview of the PDPO. In the case of the IPCC disclosure, all definitions are clearly satisfied and, on the face of it, there was a violation (even perhaps aptly described as a

[11] *See* Alana Maurushat, "Multi-lateral Recognition of PKI Certification Authorities in the Asian Region: Transborder Data Flow and Information Privacy Issues," (2005) 35 *HKLJ* 569. The author writes, "The 1999 Court of Appeal case of *Eastweek Publisher v Privacy Commissioner*, casts serious doubt as to the broad scope of PDPO. Eastweek Publisher published a photograph of a young woman taken from the populated and busy area of Hong Kong known as Causeway Bay. Although the photographer was unable to obtain consent from the young woman, the photograph was published. The photograph was labeled, 'Japanese Mushroom Head' followed with a scathing article describing this young woman's utter lack of fashion sense. On the issue of whether the PDPO had been violated, the court ruled, in a 2 to 1 ruling, that there was a lack of intent to identify the young woman or to compile personal data about her" (p 582).

gross violation) of Data Principle 4: security of personal data. That said, it is unlikely that the PDPO would provide a suitable legal remedy in the form of compensation.

Data Principle 4 mandates that the data user take all *reasonably practicable* steps to protect personal data. Berthold and Wacks identify five important security data factors:

1) the kind of data and the harm that could result if any of those things should occur,
2) the physical location where the data is stored,
3) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored,
4) any measures taken to ensure the integrity, prudence and competence of persons having access to the data, and
5) any measures taken to ensure the secure transmission of data.[12]

In the current context, the facts are not conclusive but seem to indicate that human oversight was the culprit. The government has comprehensive security policies in place.[13] However, the exact type of technology and security measures taken have not been officially disclosed to the public. Bits of information have been revealed in the newspapers and, not surprisingly, some of the best commentary on the situation may be found on web blogs.[14] It is difficult at this point to paint a full picture of the technological blunder. The IPCC had commissioned EDPS Systems to reformat the files from the old IPCC computer system to a new system which would match CAPO's system. EDPS then sub-contracted the task to an independent data engineer, Kirren Heung (all this was standard outsourcing practice). Initially, the IPCC claimed that the information had never been put on an Internet system. A few days later the IPCC indicated that the contractor made the false assumption that the information was password-protected for both the uploading and downloading of files. Subsequently, during the transfer, the information was made available on the Internet in raw data form. Data leaks are often caused by misconfiguration of software allowing for malware (malicious software, eg computer virus, spyware, bug) to retrieve the data.[15] This theory would not, however, explain how the information became available on www.china2easy.com under the sub-file of "Kirren". It is possible that the

[12] Note 10 above, pp 274–277.

[13] *See* the Hong Kong Government Security Standards issued by the Office of the Government Chief Information Officer: *Baseline IT Security Policy* and *Baseline Security Guidelines*.

[14] For example, *see* the reporting from the web blog, "Data Blunder" on the website "flagrant harbour" available at http://flagrantharbour.com/?p=178 (last accessed 3 Apr 2006).

[15] G. Serazzi and S. Zanero, "Computer virus propagation models," (2004) Performance Tools and Applications to Networked Systems, Lecture Notes in Computer Science, Vol 2965, pp 26–50.

contractor did not use the FTP protocol to shield it from the directories of search engine spiders used by Google (HTTP would allow for this). Still, this does not explain how it became available in the sub-file of a Hong Kong company specialising in mobile phone accessories and kitchenware.[16] Shortly afterwards, EDPS painted a different picture of the situation, claiming that the sub-contractor requested a dummy file to conduct a test run. The disc provided by the IPCC, however, contained the real and live data. EDPS claims that the IPCC did not inform it that the disc did not contain phoney information, but the actual real and sensitive information from the files. And so we still do not have the full picture.

If we assume that all of the alleged facts are correct, it is clear that using such sensitive data for a test run without, at the very least, password protection for both the upload and download would constitute a security breach. In fact, it is standard practice that data of this level of sensitivity be encrypted. There is no evidence to date that such an elementary security measure was taken. It would be difficult to conclude that all reasonably practicable steps had been taken. It seems that all parties involved (IPCC, EDPS, and the independent contractor) share a degree of negligence such that Data Principle 4 has been violated. But the reality is that it probably doesn't matter. As Professor Graham Greenleaf comments:

> "The new Privacy Commissioner Roderick Woo freely admits the law's deficiencies, noting that data users who breach a privacy principle (such as the security principle) cannot be prosecuted if they take steps to stop further breaches occurring. In effect, 'everyone is allowed one mistake,' he says."[17]

The focus of the PDPO is on education and mediation between data subjects and data users. Normally the Privacy Commissioner will investigate the complaints, then make a report with a series of recommendations for the data user, to prevent further violations. If the Privacy Commissioner takes exception to this case, it is within his authority to order that fines be paid of up to HK$50,0000 – hardly an appropriate solution given the severity of negligent conduct and the harm which may result from the disclosure of such sensitive data. Prosecution may occur but there is a paucity of cases that have been referred for prosecution. In the event of a recommendation to prosecute, the prosecution itself would be conducted by the police as the Privacy Commissioner does not possess the power to prosecute. The inappropriateness of this

[16] The www.china2easy.com page is no longer accessible on the Internet, though it was on 14 Mar 2006, in spite of the file having been removed from the site on 10 Mar 2006.

[17] Graham Greenleaf, "Personal data spills stun Hong Kong," for publication in Privacy Laws and Business International Newsletter (19 Mar 2006).

arrangement, given the circumstances of the leak and the nature of the data, concerning as it did, police conduct, is obvious and need not be elaborated further.

Section 66 may appear to offer an appropriate remedy as it allows the affected individuals to sue in the courts, as well as to instigate a class action suit. Section 66 confers discretion on the court to award damages for "injury to feelings." There is no cap on monetary compensation under this provision. On the surface the use of section 66 would appear to be straightforward. There are a number of hurdles however which make this remedy less attractive. First, no one has ever succeeded in court. Second, Hong Kong courts generally do not invite class actions. Third, the onus is on the plaintiff to show that there was a failure on the part of the data user to take all reasonably practicable steps to secure the data. The foregoing requirement may indeed prove onerous given the unclear picture as to how the data was actually leaked. Last, the Privacy Commissioner does not have the power to assist citizens in litigation, in which case affected individuals have to hire their own legal counsel.

Why the Common Law may not Provide a Better Remedy than the PDPO

Two pertinent tort actions may appear to be more useful as a means of legal redress: breach of confidence and negligence. The tort action for breach of confidence provides an equitable remedy where confidential information is unlawfully disclosed. The exact legal test for breach of confidence is unsettled in Hong Kong law. It is generally thought that three elements have to be proved for a case in breach of confidence to succeed, though it remains unclear as to whether the third element is a requirement, or merely a consideration to be taken into account:

- the information itself must have the necessary quality of confidence about it,
- that information must have been imparted in circumstances importing an obligation of confidence, and
- there must be an unauthorised use of that information to the detriment of the party communicating it.[18]

The recent House of Lords decision in *Campbell v MGN Ltd*[19] has altered the requirements for a breach of confidence action. The House of Lords' decision eliminated the need for there to be a relationship of confidence, and replaced

[18] Kenny Wong and Alice Lee, *A Practical Approach to Intellectual Property in Hong Kong* (Hong Kong: Sweet & Maxwell Asia, 2002) p 227. The authors refer to the test put forth in the case of *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41, p 47.

[19] [2004] UKHL 22 [hereinafter *Campbell*].

the former requirement of "unauthorised use" with one of misuse of private information. The emphasis in *Campbell* was placed on the question of whether the information was private in nature. The House of Lords stated that the tort of breach of confidence was better suited to the name "wrongful disclosure of private information". We do not know whether Hong Kong will follow the *Campbell* decision or whether the original three elements for breach of confidence will stand.

If Hong Kong adopts the test in *Campbell*, then the IPCC and EDPS should have their chequebooks on hand. If, however, the Hong Kong courts reject the approach in *Campbell*, the third element of "unauthorised disclosure" may be difficult to prove. Past case law has focused on whether the plaintiff had expressly or impliedly consented to imparting with personal information.[20] In the Hong Kong circumstance, the information was given to the IPCC with express consent, although this consent would not apply to the misuse of the information. Another interesting point is whether consent is required when the data user outsources computer security tasks that involve sensitive information. Damages in this case would likely be for emotional distress but, due to the safety implications of this sensitive information, it is of no small matter that we may see additional types of damages sought in the future.

Although the conduct of the IPCC and EDPS would imply negligent conduct in the ordinary sense of the term, the tort of negligence is not applicable in this circumstance. Negligence does not protect privacy interests in the absence of physical damage or, in the context of a *Hedley Byrne* style relationship,[21] economic loss.

Concluding Remarks

In a series of press releases the Privacy Commissioner has urged affected citizens to seek compensation. Unfortunately, as noted above, the Privacy Commissioner does not have any power to award compensation, nor does he have the right to assist citizens in any type of litigation. There are obstacles in the way of those individuals who select the litigation route. They may not be able to find sufficient evidence as to what actually transpired in the process leading up to the data leakage. The potential high cost of legal fees may also act as a further deterrence.

Is there a flower among the weeds? The driving force of this incident may provide the motivation for change. There is incentive to expand the powers

[20] Berthold and Wacks, "Chapter 4: Data Privacy and the Common Law," p 19. The authors cite the case of *Saltman Engineering Co. Ltd v Campbell Engineering Co. Ltd* (1948) 65 RPC 203 at 213 *per* Lord Greene MR.

[21] *Hedley Byrne & Co. Ltd v Heller & Partners Ltd* [1964] AC 465. The requirements are onerous. *See* generally Rick Glofcheski, *Tort Law in Hong Kong* (Hong Kong: Sweet and Maxwell Asia, 2002) pp 160–173.

of the Privacy Commissioner, to amend information data law to reflect privacy needs in the digital era, to review the policies and information systems used in data transfer (eg outsourcing, smart ID cards), and to revisit the issue of an independent monitoring authority for the IPCC at the first opportunity.

*Alana Maurushat**

* Visiting lecturer, Faculty of Law, University of Hong Kong; formerly Deputy Director of the LLM Programme in Information Technology and Intellectual Property Law, Faculty of Law, University of Hong Kong.