Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 3 >>> MARCH 2015

Data Privacy Protection in Hong Kong: Highlights of the Past Year, Preview of the Coming Year

By Gabriela Kennedy and Karen H.F. Lee, of Mayer Brown JSM, Hong Kong.

2014 saw the Hong Kong Privacy Commissioner take a proactive approach in the protection of personal data, as well as an increase in public awareness of data privacy, as evidenced by the number of complaints received by the Office of the Privacy Commissioner.

This Focus article reviews Hong Kong's data privacy landscape in 2014 and surveys the outlook for 2015.

Complaints and Enquiries

On January 28, 2015, the Privacy Commissioner issued his Annual Report for 2013-2014 (April 2013 through March 2014) ("Annual Report"), summarising developments concerning the Personal Data (Privacy) Ordinance ("PDPO") throughout the year as well as activities undertaken by the Office of the Privacy Commissioner. A total of 1,888 complaints were received by the Privacy Commissioner in 2013-2014. This represented a 53 percent increase compared with the previous year. Out of these 1,888 complaints, 78 percent were made against private organisations, the vast majority of which are in the banking and finance industry. Most of the complaints concerned the use of personal data without the requisite consent.

This increase in the number of complaints not only demonstrates a heightened awareness of privacy rights by the public, but also underscores the need for companies to heed the call from the Privacy Commissioner to move from mere "compliance" to "accountability" of the personal data that they hold. The growth in public awareness, coupled with the Privacy Commissioner's enforcement actions (discussed below), is likely to result in companies taking a proactive approach to implement more sophisticated methods to ensure compliance and a move towards accountability for their data.

Increased Enforcement Actions

Not only have the number of complaints risen when compared with previous years, but the number of enforcement notices issued by the Privacy Commissioner have also continued to rise. In 2014, the Privacy Commissioner issued 90 enforcement notices to stop or prevent further contraventions, whilst only 25 had been issued in the previous year.

In addition, 2014 marked the very first time a prison sentence was issued for a breach of the PDPO since it came into force in 1996. An insurance agent was found guilty in December 2014 of knowingly making a false statement to the Privacy Commissioner and was sentenced to four weeks' imprisonment (*see report by the authors at WDPR, January 2015, page 33*).

The Privacy Commissioner is likely to refer more cases to prosecution in the year ahead, and, given the constant barrage of headlines concerning breaches of privacy these days, it is likely that the Hong Kong courts will take a firmer approach in the future against offenders.

The Privacy Commissioner is likely to refer more cases to prosecution in the year ahead, and, given the constant barrage of headlines concerning breaches of privacy these days, it is likely that the Hong Kong courts will take a firmer approach in the future against offenders.

We anticipate that breaches of Section 35E (*i.e.,* using an individual's personal data for direct marketing without his or her consent), Section 50A (*i.e.,* breaching an enforcement notice issued by the Privacy Commissioner) and possibly Section 64 (*i.e.,* disclosing any personal data obtained from a data user without that data user's consent, such as a rogue employee stealing personal data from his or her employer in order to sell it to a competitor) may come before the courts and may result in prison sentences in the future.

The Privacy Commissioner has also continued to initiate his own investigations. In fact, the number of self-initiated investigations rose from 19 in the previous year to 102 in 2014, and 217 compliance checks were conducted, up from the 208 checks in the previous year. The emphasis has clearly been on creating a privacy safe environment in Hong Kong.

The Privacy Commissioner has also had on his radar offering legal assistance to complainants under new provisions that were introduced in 2012 and came into force in 2013. Legal assistance can now be provided by the Privacy Commissioner in the form of legal advice, mediation or legal representation for an aggrieved person. Of the 17 requests made in 2013-2014, only one was granted legal assistance, and seven were refused (either because of lack of *prima facie* evidence that the PDPO had been breached or because of failure to substantiate any alleged damages suffered). The rest were either withdrawn or are still being considered.

Cross-Border Transfers

The speed with which data can move across borders enabled by technology and the increasing uptake in cloud-based services, at both the consumer level and the enterprise level, focused attention on cross-border transfers in 2014.

Section 33 of the PDPO prohibits the transfer of personal data outside Hong Kong except in specific circumstances, including the transfer of data to a country that is in the "white list" of jurisdictions which the Privacy Commissioner considers to have laws that protect personal data to a level commensurate with the PDPO. However, Section 33 is still the only provision of the data privacy law in Hong Kong that has not come into force, 19 years since its enactment.

In 2013, the Privacy Commissioner completed a survey of 50 jurisdictions and provided to the Government a recommended "white list" of countries that have data protection laws substantially similar to the PDPO.

As an interim step, on December 29, 2014, the Privacy Commissioner issued a Guidance Note on the transfer of personal data outside Hong Kong, "Guidance on Personal Data Protection in Cross-border Data Transfer", to help data users prepare for the eventual implementation of Section 33 (*see analysis at WDPR, January 2015, page 15*).

The Annual Report makes it clear that the Privacy Commissioner will continue to focus his attention in 2015 on the protection of personal data in respect of mobile apps.

The Annual Report makes it clear that the Privacy Commissioner will continue to focus his attention in 2015 on the protection of personal data in respect of mobile apps.

Even though the Guidance Note is not mandatory, any failure to comply will most likely be taken into account by the Privacy Commissioner when assessing whether or not the PDPO has been breached (either in respect of Section 33, when it eventually comes into operation, or any other relevant provision of the PDPO, *e.g.,* breach of Data Protection Principle 1).

As an interim measure, the Guidance Note offers some indication as to where the law on Section 33 will eventually stand.

Apps and Technology

In a connected city like Hong Kong, where the mobile penetration rate is very high, it comes as no surprise that, in 2014, the Privacy Commissioner received 1,702 complaints, 12 percent of which were in relation to the use of information and communications technology. This marked an increase of 122 percent in the number of complaints relating to information and communications technology when compared with the previous year.

The Privacy Commissioner's focus on mobile apps and technology is nothing new, but is definitely an area that warrants continued oversight.

In November 2012, the Privacy Commissioner issued an Information Leaflet "Personal data privacy protection: what mobile app developers and their clients should know" (*see analysis by the authors at WDPR, September 2013, page 37*), which was followed by its "Best Practice Guide for Mobile App Development" issued in November 2014. The Privacy Commissioner has also carried out investigations into mobile apps, most famously an investigation of the mobile app "Do No Evil", which was found to infringe the PDPO (*see WDPR, September 2013, page 29*).

The Annual Report makes it clear that the Privacy Com-

   ISSN 1473-3579

missioner will continue to focus his attention in 2015 on the protection of personal data in respect of mobile apps.

The increased scrutiny of financial institutions by the data privacy regulator and the financial regulators is likely to continue throughout 2015.

Since a Guidance Note and an Information Leaflet have already been issued, the Privacy Commissioner's activities in this area will likely focus on educating app developers and conducting self-initiated investigations and compliance checks to ensure that mobile app developers are complying with the PDPO and the Privacy Commissioner's recommendations.

A new privacy awareness campaign targeted at mobile app developers was launched in January 2015.

Privacy Management Programme

In February 2014, the Privacy Commissioner launched the Privacy Management Programme, an initiative through which the Privacy Commissioner has encouraged organisations to proactively embrace personal data protection as part of their corporate governance responsibilities, rather than merely treating it as a legal compliance issue. The Government and 25 companies pledged to implement and comply with the Privacy Management Programme, which involves the adoption of an all encompassing privacy management programme that applies to all business and operational areas within an organisation, to ensure that privacy policies and procedures are properly implemented (*see analysis by Gabriela Kennedy and Eugene Low, of Mayer Brown JSM, Hong Kong, at WDPR, April 2014, page 19*).

The Privacy Management Programme was considered by the Privacy Commissioner to be an interim substitute for the Data User Returns Scheme ("DURS"). The DURS provisions under the PDPO have been in force since the enactment of the PDPO in 1996. These provisions enable the Privacy Commissioner to specify certain categories of data users that must periodically provide returns to the Privacy Commissioner setting out prescribed information, *e.g.,* the type of personal data held, the purposes of collection, *etc.* The DURS has never been activated, as no such categories of data users have ever been specified by the Privacy Commissioner.

In July 2011, the Privacy Commissioner issued a consultation document setting out the proposed implementation of the DURS (*see WDPR, September 2011, page 26*). Due to lack of support, notably from the financial sector, the introduction of the DURS was put on hold, and the Privacy Management Programme was introduced instead.

It is unlikely that the DURS will be reconsidered in 2015. Instead, the Privacy Commissioner has indicated that he will continue to focus on encouraging data users to adopt the Privacy Management Programme.

Focus on the Financial Sector

It comes as no surprise that a sector very much in the spotlight these days should also be a sector of focus for privacy regulators. The majority of private-sector complaints in 2014 were made against organisations in the banking and finance industry.

The sensitive nature of the information handled by banks and the heightened risk of cyber attacks merited a Guidance Note from the Privacy Commissioner, "Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry", published in the last quarter of 2014 (*see analysis at WDPR, November 2014, page 4*).

The Securities and Futures Commission ("SFC") issued a "Circular to All Licensed Corporations on Internet Trading, Reducing Internet Hacking Risks" in January 2014, which was followed by a "Circular to All Licensed Corporations on Internet Trading, Information Security Management and System Adequacy" in November 2014 ("SFC Circulars"). The SFC Circulars reconfirm that licensed corporations must comply with Chapter 18 and Schedule 7 of the SFC Code of Conduct (which relate to obligations for ensuring the integrity and security of the company's electronic trading system), and also make specific suggestions on security control techniques and procedures (*e.g.,* secure coding, login controls, firewalls, *etc.*). The SFC Circulars also highlighted the major design and control deficiencies discovered by the SFC following its review of selected licensed organisations, which posed security and integrity risks. Some of the major deficiencies identified include the absence of any formal IT management polices or procedures for disaster recovery, monitoring of suspicious websites, the absence of independent or qualified IT and security risk management functions, *etc.*

On October 14, 2014, the Hong Kong Monetary Authority ("HKMA") issued a Circular "Customer Data Protection" ("HKMA Circular") (*see WDPR, October 2014, page 32*). The HKMA Circular focused on the methods of control needed to help banks prevent and detect loss or leakage of customer data and the procedures needed to address and report such incidents. In addition to the obligations under the PDPO, financial institutions need to account to the HKMA on the adequacy and effectiveness of their existing controls and procedures by completing a critical review by the first quarter of 2015.

The increased scrutiny of financial institutions by the data privacy regulator and the financial regulators is likely to continue throughout 2015.

The emergence of mobile payments in Hong Kong will most likely trigger further attention from the Privacy Commissioner on the security of data and data handling practices.

The emergence of mobile payments in Hong Kong will most likely trigger further attention from the Privacy Commissioner on the security of data and data handling practices.

The Year Ahead

The Privacy Commissioner has stated that, in 2015, the areas he will specifically focus on shall include:

- the use of mobile apps and their implications for personal data privacy protection (discussed above);
- continuing to assist organisations in administering the Privacy Management Programme (discussed above);
- the protection of personal data contained in public registers maintained by the Government;
- a survey on the public's perception of the Privacy Commissioner and various topical privacy issues; and
- assisting the Bills Committee in its deliberations on the Electronic Health Record Sharing System Bill.

The statements made by the Privacy Commissioner so far indicate that his action points will be to:

- educate app developers and conduct self-initiated investigations and compliance checks on mobile apps;
- continue to encourage and assist data users to adopt and implement the Privacy Management Programme; and
- conduct self-initiated investigations and compliance checks, as well as hosting further seminars and workshops to help educate organisations on the use of personal data contained in public registers.

Despite the issuance of the Guidance Note on personal data protection in cross-border data transfer at the end of 2014, the Privacy Commissioner has not identified the introduction of Section 33 in his list of areas that he will specifically focus on in 2015. This is unlikely to mean that the Privacy Commissioner will be abandoning his attempts to bring Section 33 into force or that he will not pay attention to cross-border data flows, especially given the increasing adoption of cloud services in Hong Kong. The Guidance Note on personal data protection in cross-border data transfer indicates the exact opposite. The timing of the Guidance Note suggests that Section 33 may take a while to come into force and that, in the interim, a foreshadowing of its re-phrasing should be accepted/tested through the model clauses (core and additional) proposed in the Guidance Note.

Another notable omission is any reference to the possible introduction of a binding corporate rules ("BCR") regime. The European Union's BCR regime, whereby organisations that implement a legally binding group policy on the transfer of personal data, which has been approved by the relevant data protection authority, can transfer personal data outside the European Economic Area to affiliates globally, may be a lobbying item on the agenda in 2015, especially by multinational corporations for which the model clauses in the Guidance Note will present a challenge. This is largely because the model clauses cannot accommodate additions of new entities to a group of companies, or changes in group functions, all of which would require new suites of documents each time a change occurs.

A Crystal Ball for Data Privacy Enforcement in 2015?

2015 will continue to be a busy year for the Privacy Commissioner, with continued active enforcement and oversight, particularly in areas such as apps, new mobile payment technology, cloud services and security of data.

Data users should not sit back and wait for the Privacy Commissioner to come knocking, and should instead take a page from the Privacy Commissioner's book and be proactive in ensuring that their systems are in place and they are accountable for the data they hold.

The Privacy Commissioner's Annual Report for 2013-2014 is available at http://www.pcpd.org.hk/english/resources_centre/publications/annual_report/annualreport2014.html.

The Privacy Commissioner's Guidance Note "Guidance on Personal Data Protection in Cross-border Data Transfer" is available at http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf.

The Privacy Commissioner's Information Leaflet "Personal data privacy protection: what mobile app developers and their clients should know" is available at http://www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/apps_developers_e.pdf.

The Privacy Commissioner's "Best Practice Guide for Mobile App Development" is available at http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/Mobileapp_guide_e.pdf.

The Privacy Commissioner's January 8, 2015, statement announcing the launch of a new privacy awareness campaign targeted at mobile app developers is available at http://www.pcpd.org.hk/english/news_events/media_statements/press_20150108.html.

The Privacy Commissioner's "Privacy Management Programme: A Best Practice Guide" is available at http://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf.

The Privacy Commissioner's "Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry" is available at http://www.pcpd.org.hk/english/news_events/media_statements/files/GN_banking_e.pdf.

The Securities and Futures Commission's "Circular to All Licensed Corporations on Internet Trading, Reducing Internet Hacking Risks" is available at http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=14EC3.

The Securities and Futures Commission's "Circular to All Licensed Corporations on Internet Trading, Information Security Management and System Adequacy" is available at

   ISSN 1473-3579

http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=14EC48.

The Hong Kong Monetary Authority's Circular "Customer Data Protection" is available at http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf.

Gabriela Kennedy is a Partner at Mayer Brown JSM, Hong Kong, and Head of the Asia IP and TMT Group. She may be contacted at gabriela.kennedy@mayerbrownjsm.com. Karen H.F. Lee is an Associate at Mayer Brown JSM, Hong Kong, and a member of the IP and TMT Group. She may be contacted at karen.hf.lee@mayerbrownjsm.com.