The 'Big Data' era calls for greater accountability of data users

Margaret Chiu, Former Deputy Privacy Commissioner for Personal Data and
Lexis® Practical Guidance - Data Protection Consultant Editorial Board member

What is 'Big Data'?

'Big data'[1] is characterised by its huge volume, velocity of growth and variety in data contents. Big data was born out of the performance of lawful functions by public bodies, or through the carrying out of commercial activities by commercial organisations. For example, the Hong Kong Immigration Department holds the demographic data of millions of Hong Kong citizens in the course of managing the Births and Deaths Registers and the documents which identify us. On the other hand, mega search engines and social networking sites, such as Google and Facebook collect and process countless netizens' data as commercial enterprises.

Technological advancement: a catalyst for building up big data

Every day we use smart devices such as smart phones, tablets, octopus cards and IP cams which are connected to various networks. Some popular online platforms such as WhatsApp, Gmail, Facebook and Twitter seem to many as indispensable to modern living. The application of these online platforms includes e-banking, online shopping, paying bills, online games, sharing photos and information with friends. Whether we agree or not, our personal data has become part of this 'big data'.

> *"Whether we agree or not, our personal data has become part of this 'big data'."*

[1] The term 'big data' is not found in the Personal Data (Privacy) Ordinance (Cap 486). According to EU's Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to their processing in the EU adopted on 16 September 2014, 'big data' is said to be a broad term that covers a great number of data processing operations, some of which are already well identified, while others are still unclear and many more are expected to be developed in the near future.

LexisNexis®

Why should we care about big data?

Big data includes information such as names, gender, age, identification documents, credit data, health data, biometric data, educational backgrounds and shopping records. This data can be used to analyse the behaviour patterns of individuals, whether individually or as members of a group. Controllers of big data can also use such information for multiple purposes. Thus, if such data is misused, the potential harm to the affected data subjects is incalculable. Data subjects should stay alert to the privacy risks commonly associated with big data.

Excessive collection of massive and sensitive personal data

The Personal Data (Privacy) Ordinance (Cap 486) (PDPO) only allows a data user to collect necessary, adequate but not excessive personal data for its lawful functions and activities (Data Protection Principle 1). However, in 2010, the Octopus Cards Company was found to have been collecting the HKID card numbers of hundreds of thousands of the subscribers to its Octopus Rewards Programme[2]. Then, in 2013, a body fitness centre California Fitness was discovered to have been unlawfully collecting over 200,000 copies of the HKID cards of its members. These incidents show that one single breach can have a great adverse impact on many data subjects.

The International Global Privacy Enforcement Network privacy sweep exercise conducted in 2014[3] showed that 75% of the mobile apps requested one or more permissions to access the subscribers' information. The sweepers were concerned that about 31% of the mobile apps collected personal data beyond these apps' functionality. 43% of the apps were also found not to have effectively communicated their privacy policies and practices to the subscribers.

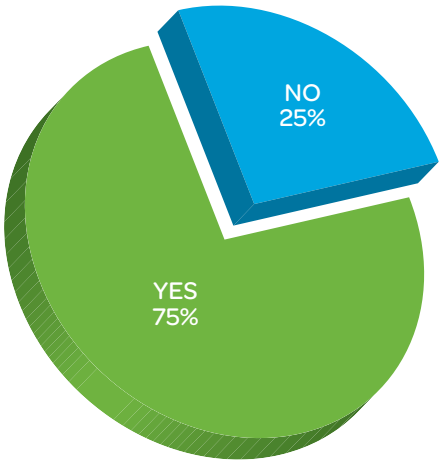
Smartphones and tablets contain personal or even sensitive data such as phonebook contacts, GPS locations, photos and communications records. By agreeing to share such data with third parties, the data subjects are making themselves vulnerable to possible data breaches.

Wrongful uses of personal data harvested in the public domain

Cyberbullying is an abuse of personal data and can cause threat or even psychological harm to the affected individuals. For instance, in August 2016 some internet users banded together to retrieve online the profile of a returning officer responsible for handling electoral matters in the 2016 LegCo Election. Verbal attacks were posted on the Facebook displaying her name, photo, office address and telephone numbers[4].

Social networking sites contain a big data set of personal information, photos and opinions retrievable online. They facilitate cyberbullying. Once personal data is posted online and open to the public, there is practically no 'right-to-be-for-gotten' that enables a data subject to completely stop their personal data from further online dissemination. Unfortunately, cyberbullying is not outlawed, and cyberbullies can even be considered as being 'protected' under the PDPO, notably, s 52.

Mobile apps requesting one or more permissions to access subscriber information *



*Global Results of the Second International GPEN Privacy Sweep published on 12 September 2014

[2] Investigation Report R10-9866 by the Privacy Commissioner for Personal Data
[3] Global Results of the Second International GPEN Privacy Sweep published on 12 September 2014

LexisNexis®

> *Once personal data is posted online and open to the public, there is practically no 'right-to-be-forgotten' that enables a data subject to completely stop their personal data from further online dissemination*

More examples can be found in the 'Do-No-Evil' mobile app which provided bankruptcy and litigation data and directorship of any targeted individuals by way of a name search. The Privacy Commissioner for Personal Data (PCPD) found such use of personal data a serious infringement of the personal data privacy rights of individuals, whose personal data was culled from various public registers whose purposes did not extend to cover such secondary uses. In a UK art exhibition in August 2016[5], an artist made available for sale a 'backdoored.io' art piece which captured images of homeowners and their activities at home, which were retrieved online by the artist from clips recorded by unencrypted IP cams installed by these homeowners in Hong Kong! Fortunately the artist has agreed to block the images of the affected individuals upon the intervention by the PCPD.

Data breaches and identity theft

Data users' computer systems are susceptible to malicious cyberattacks. Recent examples can be found in VTech Learning Lodge's data breach in December 2015, which led to the leakage of more than 5 million customers' accounts and 200,000 children's profiles including names, email addresses, passwords, and residential addresses worldwide[6]. In December 2015, Sanrio Town website announced that due to a security default, some 3.3 million of its members' personal data including name, email address, date of birth and encrypted password had become publicly accessible[7].

Unencrypted USB flash drives containing personal data have often been reported to have been lost by officers of public bodies. Recently, a number of controversial video clips were exposed online which showed the activities of Hong Kong prisoners. This was the direct result of the loss of a USB flash drive by an officer of the Correctional Services Department. Such lost or stolen data might consist of an individual's name, contact details, credit card information and identification document. They are perfect ingredients of identity theft.

The Hong Kong Police Force reported that in the first half of 2016, Hong Kong citizens lost $106.99 million through telephone deceptions[8]. The fraudulent cases of fake property owners of properties had caused loss of more than $12.5 million.

These only represent the tip of the iceberg as very often data subjects are unaware of the fact that their personal data security has been compromised. They may be kept in the dark forever because data users are not required by law to give data breach notification.

> *When there is a disparity of bargaining power between the parties or when withholding consent means a discontinuance of services which the data user considers essential, can the data subject really afford to withhold his consent?*

Recently, WhatsApp sought agreement from its subscribers to share their account information with Facebook. If subscribers refused to agree within a prescribed period, WhatsApp would stop the service. A subscriber could tick the big blue sign of 'AGREE' to signify their consent to the change of the original Terms and Privacy Policy. There was a small blue print of the word 'read' if the subscriber was minded to read the revised Terms and Privacy Policy. There, a default button set as 'opt-in' to the sharing of their account information with Facebook was provided. A subscriber could choose to switch off this default button if they did not agree to the proposed sharing of information.

---

[4] See Press Release by HKSAR Government dated 1 August 2016 titled 'Government condemns personal attacks against officers responsible for electoral matters'.
[5] Media Statement by PCPD dated 16 August 2016
[6] Media statement released by PCPD on 1 December 2015
[7] Media statement released by PCPD on 23 December 2015
[8] Hong Kong Police Force's Press Conference on Hong Kong Crime Situation of Mid-Year 2016

What WhatsApp did not indicate was that by pressing the small print 'read', a subscriber can not only read the revised Terms and Privacy Policy but also be given the choice to opt out. It was certainly not privacy friendly to set the default button as 'opt-in' if the subscriber accepts without reading the revised Terms and Privacy Policy.

The privacy attitude of data subjects was examined in the Baseline Survey of Public Attitudes on Privacy and Data Protection conducted by the PCPD in 2014[9]. The Survey showed that more participants in the focus group aged 41 and above would provide their personal data (except ID number) in exchange for benefits than those participants aged 18 to 40. It is intriguing to note that more participants with a higher educational level would provide their personal data in exchange for benefits than those with a lower educational level; and that they would also generally provide their personal information in exchange for online efficiency and convenience.

If the Survey was anything to go by, it seems that more educated data users, in welcoming technological convenience, are becoming more ready and willing to make privacy tradeoffs.

Greater accountability of big data users

It is evident that big data affects countless data subjects because of the huge quantity and variety of personal data. The mishandling of big data can lead to dire consequences for both the data subjects and the data users. In light of the prevalence of malpractice and the sensitive nature of some personal data, the Government has seen fit to tighten control by amending the PDPO over the use of personal data in direct marketing[10]. Legislation has also been enacted in 2015[11] to regulate the sharing of patients' health data in the electronic health sharing system to prevent abuse. These measures were made in order to hold data users accountable for improper handling of personal data.

> *"The mishandling of big data can lead to dire consequences for both the data subjects and the data users."*

Legislative measures aside, big data users can positively respond to the call for greater accountability by building up a sound privacy management regime appropriate to its business or functions. This should lead to better compliance with the statutory requirements and minimise the risks of data breaches.

A data user's commitment to discharge its corporate social responsibility in the proper handling of personal data is manifested in:

(i) a transparent policy for handling different kinds of personal data collected by it
(ii) the implementation of appropriate privacy enhancing measures to protect the personal data in the whole cycle of data processing
(iii) maintaining a response mechanism to handle data breaches, and
(iv) the building up of an efficient monitor and audit mechanism to ensure that the practices align with its privacy policies, which must be regularly updated to meet the changing privacy risks and are strictly followed by its employees and agents

It is good practice for the data user to undertake a privacy impact assessment before launching a new product or service which involves the collection of massive personal data. The assessment should alert the data user to possible risks the new product or service may bring. These risks can be reduced by minimising the amount of personal data to be collected and using appropriate privacy enhancing technologies. Once the product or service is in operation, data users should carry out vigilant oversight and audits.

With well-developed privacy governance in place, data users will not only gain the trust of the data subjects but will also demonstrate that reasonable precautions and diligent steps have been taken to prevent data breaches. This may also be a defence for data users in case of an accidental breach which leads to a suspicion that an offence may have been committed under the PDPO.

---

[9] Press statement released by PCPD on 28 July 2015
[10] Part VIA of the PDPO regulates the use of personal data for direct marketing and took effect on 1 April 2013
[11] Electronic Health Record Sharing System Ordinance, Cap625 effective since 2 December 2015

Margaret Chiu has been a Hong Kong qualified solicitor since 1986. She engaged in private legal practice for many years before turning to work for various NGOs, including the Privacy Commissioner for Personal Data, HKSAR. She is a former Deputy Privacy Commissioner for Personal Data and was instrumental to the production of various educational publications by the PCPD, such as the first and the second editions of the Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's Perspective. She is now a Privacy Management Programme Consultant giving training and workshops to data users to promote privacy governance. She also presents CPD courses for the Hong Kong Academy of Law.

Margaret is Consultant Editorial Board member for Lexis® Practical Guidance – Data Protection, a one stop solution for all your data privacy needs.

Lexis® Practical Guidance – Data Protection provides comprehensive and up-to-date guidance on data privacy. Easy to follow checklists and step-by-step practice notes make it easy to comply with legislation and best practice. Exclusive drafting notes accompany all the key precedents you need, making your work quicker and more efficient.

The Data Protection service is written by Hong Kong experts, skilled in the interpretation of the law and able to offer genuinely commercial guidance. Topics covered include employee data collection and monitoring, surveillance, cybersecurity and data collection and usage. This essential resource covers the Personal Data (Privacy) Ordinance (Cap. 486) and other related ordinances, as well as multi-jurisdictional guides.

For more information visit www.lexisnexis.com/ap/pg/hkdataprotection/home
or call Customer Support on +852 2179 7888.

LexisNexis®