CHALLENGES POSED BY BIOMETRIC TECHNOLOGY ON DATA PRIVACY PROTECTION AND THE WAY FORWARD

By Roderick B. Woo, the Privacy Commissioner for Personal Data, Hong Kong

BIOMETRICS AND PRIVACY

1. It is a constant challenge trying to balance technology and privacy. Undoubtedly, technological advancements have brought efficiency and convenience to our daily lives and the conduct of businesses. Increasingly biometric data, which include fingerprints, DNA samples, iris scans, hand contour are collected for identification and verification purposes by using biometric technology devices such as fingerprint scanner and facial recognition devices.

2. Biometric data are very personal because they are information about an individual’s physical self. They are generally considered sensitive since they are fixed and, unlike a password or a PIN, cannot be reset once they have been inappropriately released. Biometric data can reveal other sensitive personal information such as information about one’s health, racial or ethnic origin. They are capable of providing a basis for unjustified discrimination of the individual data subjects.

3. Biometric technologies can help identifying individuals without their knowledge or consent. A biometric sample is taken from an individual and the data from the sample are then analyzed and converted into a biometric template which is stored in a database or an object in the individual’s possession, such as a smart card. A biometric sample taken from the individual can then be compared with the stored biometric template to identify the individual. In most instances, the use of biometric technology involves the compilation of personal data from which an individual is identifiable and hence the use of the data falls within the purview of the Personal Data (Privacy) Ordinance, Cap.486 laws of Hong Kong.

4. The proliferation of biometric technologies results in significant impacts on data privacy protection. Improper collection and handling of biometric data

can lead to negative consequences such data mining, data profiling, excessive retention, and risk of identity theft, etc. There is a valid concern that the data collected might be re-engineered or collated with other database leading to uses which are beyond the reasonable expectation of the data subjects. It can also incite fears of constant surveillance, profiling and control which create adverse effects on data privacy protection. The seriousness of harm is aggravated in the event of unauthorized or accidental access or handling. Furthermore, the safety and integrity of these personal data being stored in large digital database is another significant privacy concern that calls for special care and attention.

REGULATORY EXPERIENCE IN HONG KONG

5. In Hong Kong, the use of biometric technologies for identification and security purposes has become increasingly popular. Biometric technologies infiltrate many aspects of our lives. Many organizations have adopted new biometric devices to record access to their facilitates and supervise employee's attendance. Biometric devices are also used on minors. My Office had investigated into a primary school's fingerprint recognition device which was used to record students' activities including attendances, the purchase of lunch and the borrowing of books.

6. In recent years, there is a sharp rise in complaints lodged with my Office concerning the collection of biometric data. Most of them concern employers' collection of employees' fingerprints for attendance purpose. The phenomenon sends out a clear message: people feel uncomfortable to hand out lightly their biometric data. It is easy to understand that the use of biometric devices in the management of human resources are convenient and costs-effective, these activities should not be conducted without consideration for personal data privacy of the persons involved.

7. In July 2009, my Office published a report[1] concerning the collection and recording of employees' fingerprint data for attendance purpose by a furniture company. In that case, I found that the collection of employees' fingerprint data by the company for monitoring attendance purpose was excessive and the means of collection was not fair in the circumstances of the case and for those reasons the company's practice was in contravention of Data Protection Principle ("DPP") 1(1) and DPP 1(2) in Schedule 1 of the Ordinance.

[1] Available at http://www.pcpd.org.hk/english/publications/files/report_Fingerprint_e.pdf

In gist, DPP 1(1) requires that personal data to be collected should be necessary, adequate but not excessive. DPP 1(2) requires the means of collection should be lawful and fair in the circumstances of the case.

8. My regulatory experience on this subject has led me to form certain views.

(a) First and foremost, if the act or practice does not involve the collection of "personal data", it is outside the jurisdiction of the Ordinance. For example, if a fingerprint recognition system which converts certain features of the fingerprint into a unique value and store it in the smart card held by the employee, the employer who does not hold a copy of the data has not “collected” the fingerprint data. In practice, the employee puts his finger and the smart card on the recognition device to complete the verification process. The system simply compares and matches the value in the smart card with the fingerprint features presented each time. Since the employer has no access to the personal data concerned, he has not collected any "personal data" and the Ordinance as it stands is not concerned with such a practice.

(b) If the fingerprint recognition system involves the collection of personal data, employers should be mindful not to collect fingerprint data purely for day to day attendance purpose. In many instances, less privacy intrusive alternatives which can achieve the same purpose are available. Whether or not features of the fingerprints are converted into value, such an act amounts to collection of excessive personal data and the employers risk contravening the requirements of DPP1(1), unless the genuine consent of the data subject has been obtained.

(c) If a data subject provides his fingerprint data voluntarily for a particular purpose, the application of the DPPs should not override the data subject's right to informational self-determination. I shall respect his consent if given voluntarily and explicitly.

(d) Fingerprint data should not be collected from children of tender age, regardless of any consent given by them, for the reason that they may not fully appreciate the data privacy risks involved.

(e) Before collecting employees' fingerprint data for attendance purpose, employers must offer employees a free choice in providing their fingerprint data, and they must be informed of the purpose of collection and given other less privacy intrusive options (e.g. using smart cards or passwords).

(f) The means of collecting employees' fingerprint data must be fair. Employees should be able to give their consent voluntarily without undue pressure from the employers and should have the choice of other options; otherwise there may be contravention of the requirements of DPP1(1) and DPP1(2).

NO COMPILATION OF PERSONAL DATA?

9. I have come across arguments that the data stored in a fingerprint recognition system are not personal data because:-

(a) the stored biometric data are just meaningless numbers, and therefore are not personally identifiable information; and

(b) a biometric image cannot be reconstructed from the stored template.

10. Let’s look at the first argument. I think no one can agree that these numbers when linked to other personal identification particulars are capable of identifying an individual. After all, the purpose of collecting the data and convective them into numbers is to identify and verify a person. This is similarly true in the second scenario. The templates will ultimately be linked to identify a person. Hence, no matter how the templates are generated (in the form of numerical codes or otherwise), they will be considered “personal data” when combined with other identifying particulars of a data subject.

11. As to the claim that a fingerprint image cannot be reconstructed from the stored biometric template, I would like to make reference to the paper entitled

"Fingerprint Biometrics: Address Privacy Before Deployment"[2] published by the Information and Privacy Commissioner of Ontario in November 2008. The paper explains that reconstruction of a fingerprint image from the minutiae template with striking resemblance is not uncommon and there is positive match in more than 90% of cases for most minutiae matchers. We don't need reminders that technology is advancing in an alarming speed. What is regarded impossible to-day should not be regarded impossible next month or next year.

GOOD ATTITUDE AND PRACTICE

12. I believe a healthy society should embrace different and sometimes conflicting interests. Technology development and privacy can and should exist in harmony. It is important that end users and various stakeholders recognize and give more thought on the impacts brought by biometric technologies on data privacy protection.

13. From the end users' perspective, less privacy intrusive alternatives should be offered and measures to lessen the adverse privacy impact should be taken before a practice is adopted which involves the collection and processing of biometric data. Data users should always ask themselves whether the degree of intrusion into personal data privacy is proportional to attaining the purpose behind before they start collecting other people's biometric data. In this evaluative process, the following questions should be addressed.

(1) What is the scope of the practice?
(2) How many people will be affected?
(3) The vulnerability of the people who may be affected.
(4) Will the biometric data be transferred transferred to third parties?
(5) What security measures will be taken?
(6) What are the risks of identity theft?
(7) How long will the data be retained?

14. To promote good practice, my Office has issued a Guidance Note on Collection of Fingerprint Data in August 2007 which can be downloaded from my Office website. I wish to highlight a few of the measures that should be taken.

[2] Available at http://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf

(1) Confine the act or practice only to those data subjects the collection of their fingerprint data are necessary for attaining the lawful purpose of collection. Avoid universal, wide scale or indiscriminate collection.

(2) Avoid collection of fingerprints from data subjects who lack the mental capacity to understand the privacy impact (e.g. children of tender age).

(3) Inform the data subjects explicitly of all the uses, including the intended purposes of use on the fingerprint data collected and the class(es) of persons to whom the fingerprint data may be transferred.

(4) Steps have to be taken to prevent misuses of the fingerprint data, for example, through unnecessary linkage with other IT systems or databases.

(5) Ensure that there are sufficient security measures in place to protect the fingerprint data from unauthorized or accidental access. Privacy enhancement technologies, such as proper encryption should be adopted to guard against decryption, or reverse engineering of the full image of the fingerprints. Personnel entrusted with handling the fingerprint data should possess the requisite training and awareness on protection of personal data privacy.

(7) The collected fingerprint data should be regularly and frequently erased upon fulfillment of the purpose of collection; excessive retention and hoarding of the data increases the privacy risk.

(8) Where adverse action, for instance, disciplinary action or termination of employment, may be taken against the data subject in reliance of the fingerprint data, the data subject should as far as practicable, be given a chance to respond and challenge the accuracy of the data so used.

15. Currently, my Office is working on an update of the Guidance Note so please stay tuned.

WAY FORWARD – LAW AMENDMENT

16. Let's now look ahead forward. The Ordinance was designed in the mid 90s of the 20th century. Is it still capable of giving sufficient protection to data privacy protection? My Office carried out a full review of the Ordinance, and proposed to the Government in December 2007 some 50 amendment proposals. The Government agreed with most of these proposals and has just concluded a Public Consultation inviting comments.

17. One of the proposals my Office made was to classify biometric data as sensitive personal data. My proposal echoed the recent recommendation of the Australian Law Reform Commission to extend the definition of "sensitive personal data" to cover biometric information. I also suggested that broadly in line with the EU Directive 95/46/EC[3] other special categories of personal data should include racial or ethnic origin of the data subject, his political affiliation, his religious beliefs and affiliations, membership of any trade union, his physical or mental health or condition, his biometric data and his sexual life. The Government favoured biometric data as a start to be classified as sensitive personal data. In my recent response to the Consultation Document, I urged the Government to review its decision to include other categories.

18. In the proposal, I suggest that the collection, holding, processing and use ("handling") of sensitive personal data ought to be prohibited except in certain prescribed circumstances:-

(a) with the prescribed consent of the data subject;
(b) it is necessary for the data user to handle the data to exercise his lawful right or perform his obligations as imposed by law;
(c) it is necessary for protecting the vital interests of the data subjects or others where prescribed consent cannot be obtained;
(d) handling of the data is in the course of the data user's lawful function and activities with appropriate safeguard against transfer or disclosure of personal data without the prescribed consent of the data subjects;
(e) the data has been manifestly made public by the data subjects;
(f) handling the data is necessary for medical purposes and is

[3] EU Directive 95/46/EC *Guidelines on Protection of Privacy and Transborder Flows on Personal Data*.

undertaken by a health professional or person who in the circumstances owes a duty of confidentiality; and

(g) handling of the data is necessary in connection with any legal proceedings.

19. Many stakeholders have expressed concerns on the possible adverse effect and confusion the proposal may bring. They fear a reduction in business opportunities. However, the proposal does envisage a transitional period. Perhaps in the long run, the public will support the view that personal data privacy right should be properly balanced with but not be sacrificed too readily for the sake of economical gains.

ROLE OF PRIVACY REGULATOR

20. As a privacy regulator, I am concerned whether the requirements of the Ordinance are complied with. The question of how particular personal data should be regulated is always on my mind. However, I need to stress that the Ordinance is technology neutral. I have no intention whatsoever to hinder businesses from using advanced technologies or to discourage development in biometric technologies. My role is to identify privacy risks, consider the views from different sectors, promote and monitor the compliance of the Ordinance and make recommendations to enhance data privacy protection in light of changing social needs and interests.

21. Stakeholders often ask me what they should do. My reply is always : recognize the need to cope with the privacy risks involved; Understand and comply with the requirements of the Ordinance; Give due consideration and show positive response. I am sure that with the cooperation of data users and data subjects, we can look forward to a world where personal data privacy is respected and protected and that personal information can flow freely in accordance with the law.

- End –

Abstract :

Biometric technologies advancement has created a significant impact on data privacy protection in Hong Kong. Its Privacy Commissioner for Personal Data shares his experience and explains his role in regulating activities involving the use of biometric devices in collecting personal data. He will discuss the good practice that should be adopted by the end users. The recent public consultation on the review of the Personal Data (Privacy) Ordinance also included the proposal to classify biometric data as sensitive personal data.

Keywords:

Regulating the collection of biometric data in Hong Kong – Good practice to be adopted – Greater protection should be given to biometric data currently under review in Hong Kong