Report Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap. 486)

Report Number: R09-7884

Date issued: 13 July 2009

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Employer Collecting Employees' Fingerprint Data for Attendance Purpose

This report in respect of an investigation carried out by me pursuant to section 38(a) of the Personal Data (Privacy) Ordinance, Cap 486 ("the Ordinance") against a furniture company ("the Company") is published in the exercise of the power conferred on me by Part VII of the Ordinance. Section 48(2) of the Ordinance provides that *"the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report –*

(a) setting out -

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit."

Roderick B. WOO
Privacy Commissioner for Personal Data

(Note: This is an English translation of the Report compiled in Chinese.)

The Complaint

The Complainant was employed by the Company as a furniture installer. On the first day he reported duty at the Hong Kong headquarters of the Company, the Company collected and recorded his fingerprint data. The Complainant said that the Company had not informed him that they would need to collect and record his fingerprint data when he accepted the employment offer. The Complainant was of the view that fingerprint data were sensitive personal data and he was astonished by such collection. Therefore, the Complainant lodged a complaint with the Commissioner, who then carried out an investigation under section 38(a) of the Ordinance.

Relevant Provisions of the Ordinance

2. Data Protection Principle ("DPP") 1(1) and DPP1(2) of Schedule 1 to the Ordinance are relevant to the complaint.

3. DPP1 governs the collection of personal data. It stipulates that:

> *" (1) Personal data shall not be collected unless—*
> *(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;*
> *(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and*
> *(c) the data are adequate but not excessive in relation to that purpose.*
>
> *(2) Personal data shall be collected by means which are—*
> *(a) lawful; and*
> *(b) fair in the circumstances of the case.*
> *..."*

4. Moreover, under section 2(1) of the Ordinance, "personal data" 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."

Reasons for the Collection of Staff's Fingerprint Data and the Operation of the Fingerprint Recognition System

5. In the course of investigation, the Company stated that a Fingerprint Recognition System ("the System") had been adopted since 2005 for the purpose of recording staff attendance. The Company further explained that as the use of time clock could not eliminate the practice of punching time cards for one another among its staff, after balancing different factors, it decided to use the System.

6. The Company confirmed that it had collected the Complainant's fingerprint data, but the data were deleted after he left the Company. So far, the Company had collected fingerprint data of about 400 staff and no staff member had ever refused to have his fingerprint data recorded. Apart from the System, no alternative for recording attendance was provided to its staff. The Company also confirmed that the System was not used for security purpose.

7. The System collected certain features of a fingerprint, such features were then converted into numerical codes and recorded in that format. The Company was not equipped with the facility that could convert the numerical codes into fingerprints, and so was not able to reverse the process. Besides, the System was connected to the Company's computer server by a fingerprint scanner through the Ethernet. When a new staff member put his finger on the fingerprint sensor of the scanner, it would only convert certain features of the fingerprint into numerical codes, which would then be encrypted and recorded. Whenever a staff member subsequently put his finger on the sensor, the scanner would search for the most proximate data from the records so as to identify the staff member concerned and record the time (or open electrically operated door lock). Only the time records could be downloaded whenever the System was connected to the server. Furthermore, the System did not have any output port, the Company could not directly access or transfer the fingerprint records from

the System.

8. After going through the operation manual of the System, this Office found that apart from fingerprint recognition, the System also offered the options of using passwords or passwords plus fingerprints for recognition of identity purpose. The System had the function of "System Manager". If the Company did not define and set up the "System Manager", the System could be accessed by any user. The System also had the access right and password functions to restrict the access rights of certain types of data to certain classes of user. Moreover, the Company could choose to link up the System with other databases.

9. In addition to the System, the Company had set up a surveillance camera beside each fingerprint scanner to monitor the use of the scanner by its staff and to review staff attendance records.

Information Provided to Staff by the Company in Relation to the Collection of Fingerprint Data

10. The Company replied to this Office that when a staff member reported duty on the first day, the Human Resources and Administration Department would give him a briefing on the codes of practice for employee, register his fingerprint data, and explain that the fingerprint data registered would be used for recording his daily attendance time during the employment period for calculation of monthly salary.

11. The Company has put in place four sets of employee code of practice for "New Frontline Staff", "Frontline Non-sales Staff/Cashiers/Warehouse Staff", "Office Staff" and "Frontline Staff". The following provisions were set out in the four codes of practice:

(i) *"On the first day of employment, staff should have their fingerprints registered. The data will only be used for recording the time of reporting for duty, getting off duty, having meals and outdoor work, as well as for security system. In case of an accident, the staff can be located. All fingerprint records will be handled according to the Privacy Ordinance and will not be*

leaked. Once a staff member leaves the employment, his fingerprint record will be permanently deleted";

(ii) *"Staff going out for lunch or work must have their fingerprint scanned/their time cards punched when they go out and return. Three hours of salary will be deducted for each failure to have fingerprint scanned/the time card punched,..."; and*

(iii) *Staff who purposely violate the above regulations repeatedly will be immediately dismissed without any compensation or prior warning."*

The Commissioner's Findings

Collection of Features of Fingerprint was Collection of "Personal Data"

12. In this case, though the System adopted by the Company only collected certain features of a fingerprint and not the whole image, the System could ascertain the identity of the staff. Therefore, the data collected satisfied the definition of "personal data" under the Ordinance.

13. Given its uniqueness and unchangeable nature, fingerprint data are sensitive personal data. Extra care is needed when handling fingerprint data.

Collection of Staff's Fingerprint Data for Attendance Recording Purpose was Excessive and Contravened DPP1(1)

14. When considering whether the collection of fingerprint data is excessive, data users should balance the benefits brought by such collection against the adverse impact on personal data privacy. If there are other less privacy intrusive options, data users should consider using them so as to eliminate or mitigate the adverse impact on personal data privacy.

15. The System was privacy intrusive and had adverse impact on personal data privacy in this case. Relevant factors that should be considered included:

(a) The sole purpose of installing the System was to record staff attendance. The installation locations were the Company's offices entrances/shops main entrances. The Company's offices/shops were not high-security or sensitive places which required fingerprint recognition systems to identify visitors. The Company also clearly stated that the System was not used for security purpose;

(b) The number of data subjects involved in this case was considerable. The number of affected staff was about 400. Their personal data were constantly reviewed by the System and would be accumulated over time. The huge database so formed would inevitably bring higher privacy risk;

(c) When asked what measures were taken to prevent its staff's data from accidental or unauthorized access, the Company only replied that it had confirmed with the supplier that the System could not download fingerprints. The Company did not provide any information as to whether access right and passwords process were set in the System, and whether it was ensured that the System was only linked to the database essential for attendance review purpose in the server. As there was no confirmation from the Company that it had taken appropriate security measures, I considered that there was a likelihood of accidental access and abuse of staff's data;

(d) Moreover, the Company did not tell its staff whether the whole or partial images of their fingerprints were collected by the System, and did not inform them of the classes of persons to whom the data may be transferred. Regarding the measures or steps in managing privacy risk, the Company only mentioned in its employees' code of practice that: "*All fingerprint records will be handled according to the Privacy Ordinance and will not be leaked*." This is obviously not enough. For enabling staff to make an informed decision, apart from giving the above

information, the Company should also inform its staff of the measures taken to safeguard fingerprints data against abuse or improper handling; whether any mechanism is set up for the staff to query the accuracy of the relevant data; the retention period of such data; persons who could access such data; how the System operates, etc.

16. Although I agree that it is the common goal of commercial organizations to collect staff's attendance record effectively and accurately, achievement of such goal alone is not a sufficient ground for the collection of fingerprint data. Especially in this case, the Company has installed surveillance cameras to monitor staff attendance so as to avoid fraudulence. In addition, the System offered the option of using passwords for identification. By allowing its staff to choose the use of passwords or time clock system, the Company could still prevent the practice of punching time cards for one another among its staff (because the surveillance cameras should effectively prevent the occurrence of such practice). Therefore, I consider that the collection of staff's fingerprint data was excessive in this case.

17. After considering the above factors and all the relevant circumstances of this case, I am of the view that the adverse impact on personal data privacy exceeds the benefits which were allegedly brought by the System. For the purpose of recording attendance, the collection of staff's fingerprint data by the Company was unnecessary and excessive, and the Company had contravened DPP1(1).

Unfair Means of Collecting Staff's Fingerprint Data and Contravention of DPP1(2)

18. DPP1(2) of the Ordinance requires data users to collect personal data by means which is lawful and fair in the circumstances of the case. It is obvious that collection of staff's fingerprint data is a lawful act, but whether it is fair, I have to consider it from different perspectives.

19. Generally speaking, if a data subject agrees to the collection of his personal data, the means of collection appears to be fair on the face of it.

However, it is important that we have to know whether the data subject is free and voluntary to give such consent. If the data subject gives his consent under undue pressure, undue influence or threat, e.g. if a data user compulsorily collects the personal data of data subjects without any legal basis or reasonable grounds and takes adverse action against those who are not willing to provide their data, such means of collection should not be regarded as fair. Furthermore, I have to consider if the data user has provided any information to let the data subjects to clearly understand the possible impact of collection of their fingerprint data on them, including any adverse impact, and whether the data subjects are provided with other less privacy intrusive options in order to make an informed decision.

20. There was disparity in bargaining powers between the employer and the employees. Moreover, the Company requested every new staff member to undergo the fingerprint registration procedure when he/she signs the employment agreement on the first day of employment. Therefore, unless the Company had offered other options of recording attendance in addition to the System, the consent might not be given voluntarily and freely. Furthermore, the code of practice of the Company clearly specified that: "*Staff who purposely violate the above regulations repeatedly will be dismissed immediately without any compensation or prior warning*." It is obvious that if staff did not cooperate in using the System for recording attendance, they might be dismissed immediately. Apart from its own administrative convenience, I do not find the Company has any legal or reasonable ground to collect staff's fingerprint data compulsorily. I have to point out that mere administrative convenience cannot justify the Company's use of compulsory means to collect staff's fingerprint data. In this connection, I have good reasons to believe that staff members were under undue pressure and threat and dare not object to the use of the System. Moreover, the Company had not provided the information mentioned in paragraph 15(d) to let its staff make an informed decision, but simply claimed that: "*All fingerprint records will be handled according to the Privacy Ordinance and will not be leaked*", therefore I opine that the means of collection of staff's fingerprint data by the Company under all circumstances of the case was unfair and the Company had contravened the requirements under DPP1(2).

Enforcement Notice

21. Pursuant to section 50 of the Ordinance, I may serve an enforcement notice on the Company if I am of the opinion that the Company has contravened the requirements under DPP1(1) and DPP1(2) in circumstances that make it likely that the contravention will continue or be repeated.

22. As there was no information showing that the Company would stop collecting its staff's fingerprint data, I am of the opinion that the Company's contravention of the requirements of DPP1(1) and DPP1(2) will likely continue or be repeated.

23. Accordingly, pursuant to section 50 of the Ordinance and in consequence of the investigation, I served an enforcement notice on the Company directing it to cease collecting its staff's fingerprint data (unless prior express consent was given voluntarily by individual staff) and immediately destroy all fingerprint data collected.

Compliance with the Enforcement Notice by the Company

24. Upon receipt of the enforcement notice, the Company confirmed to me that in compliance with the enforcement notice, it had stopped collecting its staff's fingerprint data and substituted passwords for fingerprints for recording attendance. Moreover, the Company confirmed to me that the fingerprint data in the System had been destroyed.

Recommendations and Other Comments

25. Technological advancement is beneficial to our daily life. For example, personal data can be collected easily and quickly by electronic devices (such as the fingerprint recognition system in this case) to achieve efficient and effective human resources management. However, as large volume of personal data can be collected and stored in a cost-effective way, improper handling may lead to personal data privacy problems, especially when collection of sensitive personal data (e.g. fingerprints) is involved. Being a unique and unchangeable personal identifier, fingerprint data are different from other personal data in the way that

they are irrevocable and unchangeable. Damages caused by theft or unauthorized or accidental access, processing or use could be very serious and prominent.

26. Before deciding to collect staff's fingerprint data, employers are advised to carry out serious and cautious assessment to determine whether the collection of such personal data is in compliance with the requirements of the Ordinance, especially DPP1(1), i.e. the data are collected for a lawful purpose directly related to a function or activity of the employer, and in relation to that purpose, the fingerprint data are necessary, adequate but not excessive. Employers should carefully assess whether the advantages of collecting staff's fingerprint data exceed the disadvantages with regard to the purpose of collection. The following are some (but not exhaustive) relevant factors for consideration:

(i) the number of staff affected;
(ii) the period of retention of staff's fingerprint data;
(iii) the scope and extensiveness of the collection of fingerprint data (e.g. whether only applicable to high-security areas);
(iv) the intended use of the data collected;
(v) the impact of the collection of fingerprint data on employer-employee relationship;
(vi) whether current security measures are adequate to prevent staff's fingerprint data from leakage or theft;
(vii) the adverse actions (e.g. disciplinary action or termination of employment, etc.) that may be taken in using staff's fingerprint data by employer; and
(viii) the extent of harm caused to staff in the event of a data leakage or improper handling.

27. Privacy risk (as mentioned above) must be proportionate to the purpose of collection. When fingerprint data are collected merely for attendance recording purpose, the privacy risk caused will likely exceed the benefits brought under the purpose of collection. To act prudently, employers should consider if there are any other less privacy intrusive options for fulfilling the same purpose of collection.

28. To strike a balance, data users should deal with the question of how to mitigate the adverse impact of the factors mentioned in paragraph 26 on personal data privacy. The scope and extensiveness of the collection of staff's fingerprint data should be restricted as far as practicable, and adequate security measures should be put in place to protect the data collected against improper use, unlawful or unauthorized access, processing or erasure, etc. It is better to keep records of the relevant assessment process and to consult staff about their reasonable expectation towards privacy.

29. If staff genuinely consent to the use of their fingerprint data by their employers for stated purpose(s), I will respect their right of self-determination. However, I would like to stress that the relevant consent must be given freely and voluntarily. In this connection, employers have to consider carefully the disparity in bargaining powers between employers and employees, and avoid exerting undue pressure or influence on employees. The most important thing is that employer must provide the employees with other less privacy intrusive options in addition to the collection of their fingerprints for employees to choose freely.

30. Regarding the collection of fingerprint data, I have issued a guidance note, "Personal Data Privacy: Guidance on Collection of Fingerprint Data", to highlight the salient points for data users who need to collect fingerprints data. The guidance note, which specifies relevant requirements of the Ordinance, provides a useful reference for data users in considering whether to collect fingerprints data. The guidance note is available for download from the website of my Office (www.pcpd.org.hk).

31. I believe that data users and data subjects can only enjoy the benefits of technological advancement with good privacy protective measures being adopted.

Compensation Liability of Contravention of the Ordinance

32. At last, I call for carefulness and prudence be exercised by organisations in the collection of personal data (especially sensitive personal data) and their compliance with the requirements of the Ordinance; otherwise under section 66

of the Ordinance, a data subject who suffers damage (including injury to feelings) by reason of a contravention of a requirement under the Ordinance by a data user shall be entitled to compensation from that data user for that damage.