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

Investigation Report:

Collection of Fingerprint Data by Queenix (Asia) Limited

Report Number: R15 – 2308

Date issued: 21 July 2015

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

Investigation Report:
Collection of Fingerprint Data by Queenix (Asia) Limited

This report in respect of an investigation carried out by the Privacy Commissioner for Personal Data (the "**Commissioner**") pursuant to section 38 of the Personal Data (Privacy) Ordinance, Cap. 486 is published in the exercise of the power conferred on the Commissioner by Part VII of the Personal Data (Privacy) Ordinance. Section 48(2) of the Personal Data (Privacy) 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."

ALLAN CHIANG
Privacy Commissioner for Personal Data

Investigation Report:
Collection of Fingerprint Data by Queenix (Asia) Limited

An ex-employee of a high-end fashion trading company, Queenix (Asia) Limited ("Queenix"), complained to the Office of the Privacy Commissioner for Personal Data (the "PCPD") against Queenix for collecting her fingerprint data at the entrance of its office. At the conclusion of an investigation into the complaint, the Commissioner found that the collection of the data was unnecessary and excessive in the circumstances, and the manner of collection was unfair, thereby contravening the requirements under Data Protection Principle 1(1) and (2) in Schedule 1 to the Personal Data (Privacy) Ordinance, Cap. 486 (the "Ordinance"). An Enforcement Notice was served on Queenix directing it to take remedial actions and to prevent recurrence of contravention.

I. The Complaint

The Complainant was employed by Queenix as a fashion buyer in early June 2014, and she left the employment on 23 June 2014. Queenix collected the Complainant's fingerprint data through a fingerprint recognition device at the entrance of Queenix's office on her first day of work.

2. According to the Complainant, there were two fingerprint recognition devices, one installed at the entrance of Queenix's office and the other one at the entrance of its showroom. Both devices were installed for security and staff attendance purposes. To access Queenix's office or showroom, employees were required to place their fingers on the fingerprint recognition devices.

3. The Complainant considered fingerprint data as sensitive personal data, and she was therefore reluctant to have her fingerprint data collected by Queenix. She requested Queenix to provide other alternatives in lieu of collecting her fingerprint data, but her request was ignored. Left with no alternative, the Complainant allowed Queenix to collect her fingerprint data. On the second

day of reporting for duty, the Complainant presented Queenix with a sample consent form and suggested Queenix to obtain written consent from staff members before collecting their fingerprint data. Her suggestion was not taken up by Queenix.

4. The Complainant felt that Queenix was not justified to collect her fingerprint data, and she lodged a complaint with the PCPD. An investigation was conducted by the PCPD under section 38 of the Ordinance to ascertain if Queenix had contravened the relevant requirements under the Ordinance by collecting the fingerprint data of the Complainant and its other staff members.

II. Relevant Provisions of the Ordinance

5. Of relevance to this complaint is Data Protection Principle ("**DPP**") 1(1) and (2) in Schedule 1 to the Ordinance, that stipulates:-

> "*(1) Personal data shall not be collected unless-*
> *(a) the data is 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 is 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.*"

6. According to 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.*"

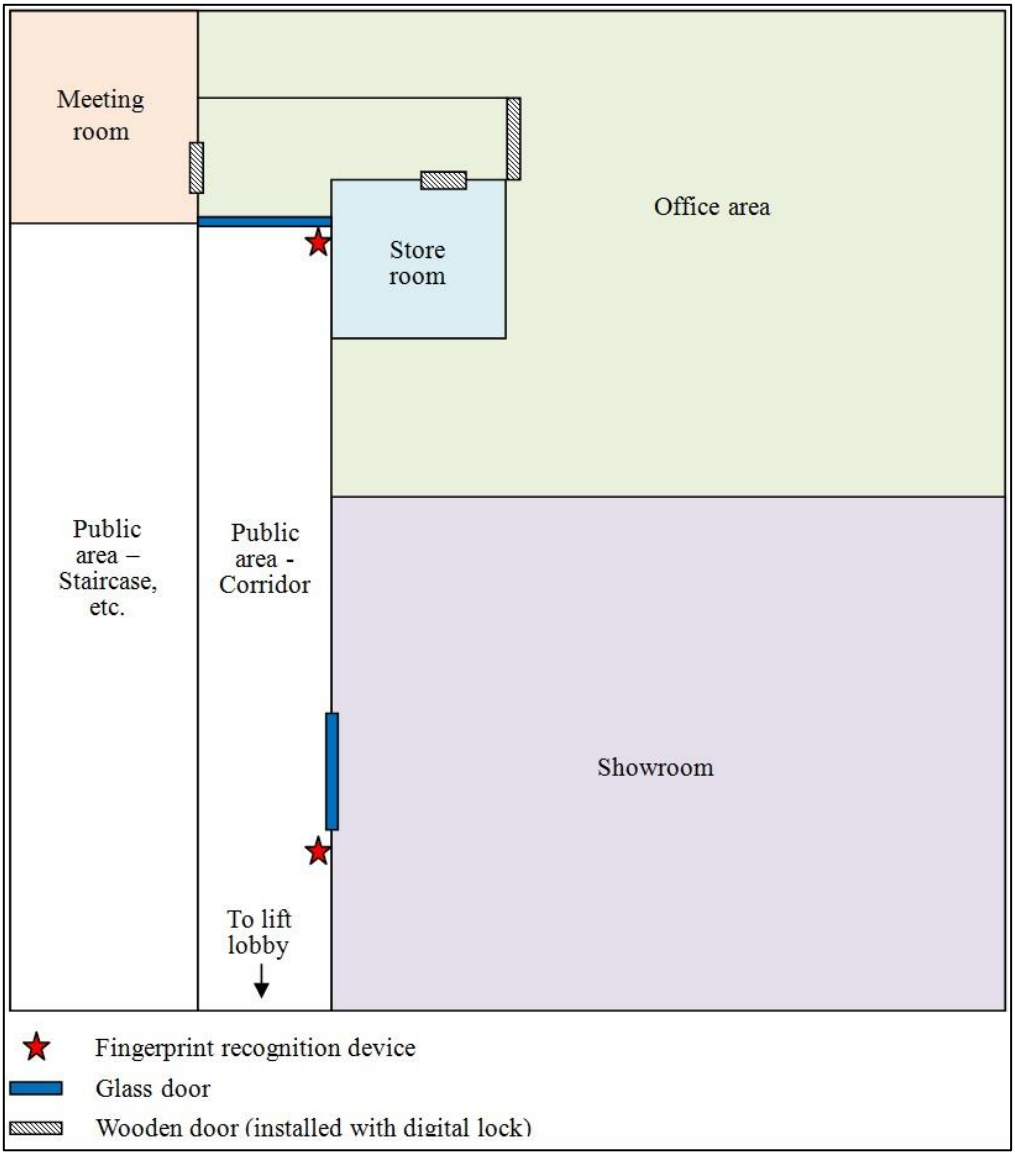
III. Information Collected during the Investigation

7. Below is a summary of the information collected by the PCPD during the investigation.

(a) Site inspection

8. A site inspection was conducted at Queenix's office and showroom which are located adjacent to each other with separate entrances in a commercial building. A floor plan of Queenix is reproduced below (not drawn to scale).

Diagram 1: Floor plan of Queenix



9. On arrival by the PCPD's officers at Queenix's office at around 10:30 am on a working day, the doors to Queenix's office and showroom were half opened (see Diagram 2 below). Employees were seen entering and leaving the office and showroom freely without using the fingerprint recognition devices. A postman and a courier also went freely into the office area. The doors of the office and showroom remained half opened during the PCPD's entire visit which lasted for about one hour.

Diagram 2: Entrances of the Queenix's office (upper) and showroom (lower)

(i) The showroom

10. During the inspection, Queenix informed the PCPD that the fingerprint recognition device[1] installed at the showroom was solely for security purposes. This was contradictory to what the Complainant stated in her complaint. The use of the device for recording staff attendance, as pointed out by the Complainant in her complaint, was not mentioned by Queenix.

11. The showroom has a size of around 1,500 square feet. The PCPD's officers saw the showroom packed with an extensive range of high-end branded fashion items, including clothes, accessories, and shoes. Queenix claimed that the value of its fashion items kept in the showroom ranged from several thousands to tens of thousands of dollars per item. Only Queenix's sales staff and customers accompanied by its sales staff would be allowed access to the showroom.

12. Four CCTV cameras were seen at the four corners of the showroom on the ceiling. Queenix explained that outside of their opening hours, the entrance would also be secured by a door lock and a chain lock.

13. During the PCPD's inspection, Queenix also stated that there had been several incidents of theft in its showroom and office, which were committed by its customers during visits to the showroom and by its staff. The culprits were identified through CCTV footage, and the stolen goods, comprising accessories valued at around HKD 3,000 to HKD 4,000 per item and company souvenirs (such as water bottles and watches) with value ranging from HKD 100 to HKD 1,000 per item, were recovered. The PCPD was told that Queenix had not reported these incidents to the police.

[1] Model "Fingertec R2" was installed at the showroom.

(ii) The office

14. The PCPD's officers saw a fingerprint recognition device at the entrance of the office[2] and a CCTV camera installed inside the office pointing at the glass door of its entrance. It served to record the activities at the office entrance. After entering the office, the PCPD's officers proceeded to a hallway leading to a storeroom, a meeting room, and an office area. The doors to these three rooms were installed with digital locks that required a password to open. Again, the doors to the meeting room and to the office area were left open at the time of the PCPD's inspection.

15. During the PCPD's inspection, Queenix explained that the fingerprint recognition device installed outside the office were both for the purposes of security and recording of staff attendance. Queenix stated that although most of its fashion items were stored in the showroom, products rejected by customers were sometimes placed in the office area, pending return to the manufacturer. Queenix showed the PCPD's officers a rack for hanging rejected fashion items, and the PCPD estimated that around 20 - 30 clothing items could be hanged on that rack.

(b) Written and verbal replies from Queenix

16. Queenix started using the fingerprint recognition devices when it moved into the current premises more than ten years ago. It stated that:-

- the fingerprint recognition device at the office entrance was for attendance and security purposes; and
- the fingerprint recognition device at the showroom entrance was solely for security purpose.

17. Queenix stated that the fingerprint recognition device outside the showroom was not connected to computer, while the one at the entrance of the office was connected to a desktop computer, i.e. the host computer, which was located inside the office area and assigned to the accountant. The host computer

[2] Model "Star Finger 007" was installed at the office.

was protected by a password. The accountant would generate an attendance report from the host computer monthly, containing the full names of its employees, date and time of their "sign in and out".

18. Queenix was asked to explain the operation of its fingerprint recognition devices in the following regards:-

(i) whether the devices collected a full image or partial image of a fingerprint;
(ii) whether the image of the fingerprint was converted into numerical code (also known as a "template") for the purposes of subsequent retention and verification;
(iii) whether the devices encrypted the fingerprint data during data transmission and retention; and
(iv) whether the fingerprint data was exported to other devices, such as a computer server or a host computer.

19. Queenix expressed that it had no idea with regard to all of the above. Furthermore, Queenix was unable to state how many employees' fingerprint data (past and present) it had collected and stored in the system. Queenix had lost the user manuals of its fingerprint recognition devices and the contact information of the vendor who installed the devices for it. Queenix stated that it would simply replace any device that was out of order.

(c) The user manuals download from the Internet

20. The PCPD downloaded from the Internet[3] a copy of the user manuals for the fingerprint recognition devices[4] used by Queenix. According to the user manuals, staff attendance reports can be generated through a host computer, based on the attendance information recorded by the fingerprint recognition devices. The user manuals do not state whether the devices collect a complete or partial fingerprint; whether the fingerprint data is stored in the form of an image or numerical code in the finger recognition devices; or whether the fingerprint data is encrypted during transmission or retention. Both devices

[3] Websites:-
http://www.idteck.com/en/customer/customer/download/view/1135?p=1&d1=01&d2=01&m=06&t=3
http://www.fingertec.com/customer/download/postsales/HUM-AC900R2-E.pdf
[4] Models "Star Finger 007" and "Fingertec R2"

may be operated by the use of a smartcard carrying an identification number, a password, or presenting a fingerprint, or a combination of any two of these means.

21. There is an additional function in the fingerprint recognition device installed outside the showroom[5] that allows the device to operate by using a smartcard with the fingerprint template embedded therein.

(d) Operations of Queenix's fingerprint recognition devices through the use of fingerprint, smartcard, password

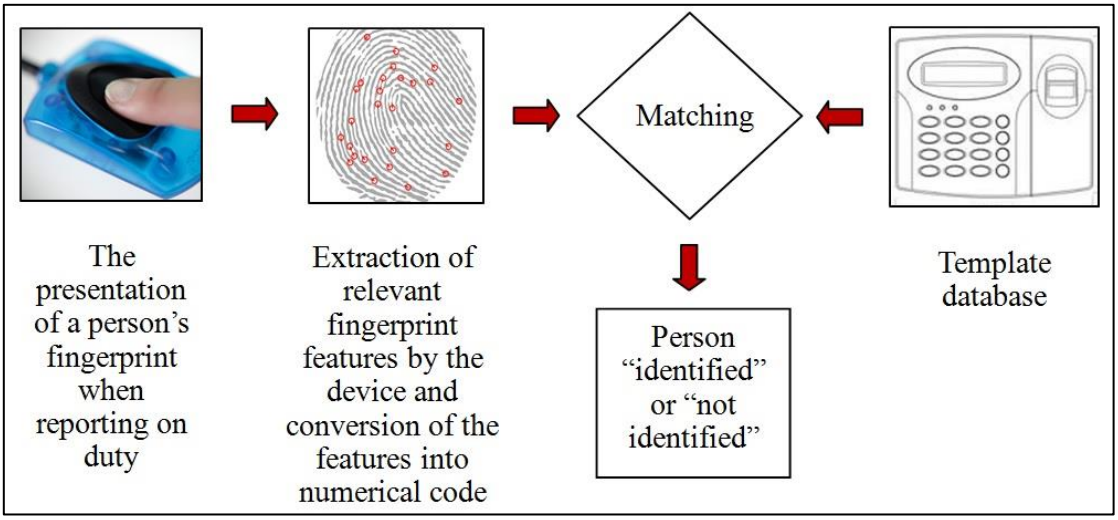
22. Although Queenix was unable to explain how its fingerprint recognition devices were operated through the use of fingerprint, password, or smartcard, the PCPD has reasons to believe that they are operated in the following ways:-

(i) Fingerprint

23. To operate the fingerprint recognition devices through the use of fingerprint, a user has to first pre-register the fingerprint of any one of his fingers with the device by recording relevant features of that fingerprint (such as ridge ending, diversion, merger, etc.) and converting them into a fingerprint template. This fingerprint template is stored to constitute a database in the fingerprint recognition device. After the registration, whenever a person presents his finger of which his fingerprint has been registered to the device, relevant features of his fingerprint will be extracted and converted into a fingerprint template. The device will then try to match this fingerprint template with the fingerprint templates already stored in its database. If the fingerprint template of the finger presented by the person matches with any of the stored fingerprint templates, the device will record the time of matching, and if the device is connected to an electric door lock, as in this case, will trigger off unlocking of the door. For illustration, please see Diagram 3.

[5] Model "Fingertec R2"

Diagram 3: Operation of Queenix's fingerprint recognition devices by use of fingerprint



(ii) Password

24. For the alternative of using a password instead of fingerprint, a user pre-registers by inputting a five-digit password of his choice into the fingerprint recognition device. The device will then record the password in its database. After this, the door will be unlocked if any person inputs the same password to the device thus achieving a match with the pre-registered password. This alternative does not involve collection of personal data.

(iii) Smartcard that carries an identification number

25. Each smartcard contains a unique identification number pre-recorded in the fingerprint recognition device. When a person presents the smartcard, the device will match the identification number in the smartcard with the identification number already stored in the database of the device. This alternative also does not involve collection of personal data.

(iv) Smartcard that carries a fingerprint template

26. To use a smartcard that carries a fingerprint template, certain features of the user's fingerprint is converted into a fingerprint template and stored in a smartcard held by the user himself. Whenever a person presents the smartcard carrying his fingerprint template, and presses his corresponding finger against the fingerprint recognition device, the device will compare the fingerprint template in the smartcard with the actual fingerprint presented by the person. The fingerprint recognition device does not retain the user's fingerprint data.

(e) Queenix's argument of not providing other alternative

27. Queenix stated that any employee who was habitually late for work would be subjected to disciplinary action (such as a written warning). In order to monitor staff attendance, Queenix depended on the fingerprint recognition device at the office entrance to record staff attendance. Queenix did not allow its employee to use smartcard that carries an identification number or password to operate this fingerprint recognition device, due to concerns that the employees might "sign in" for work for each other. Queenix was, however, unable to confirm whether any "buddy-punching" incidents had occurred before it started using this finger recognition device. Queenix emphasised that no employee had objected to having his fingerprint collected.

(f) Queenix's policy on collection, retention, use, and security of fingerprint data

28. Queenix admitted that it had no written policy regarding the collection, retention, use or security of the fingerprint data. Each employee was verbally informed of the following on their first day of joining the company:

(i) employees' fingerprint data was collected for security and recording attendance purposes;
(ii) employees were required to "sign in and out" by placing the registered finger on the fingerprint recognition device at the entrance of the office when arriving at office in the morning and leaving office at day end; and

(iii) the fingerprint data would be deleted from the fingerprint recognition devices the day immediately after an employee left employment.

29. Queenix also admitted that it had no policy on the security and retention of the employees' attendance records in the host computer.

IV. The Findings of the Commissioner

(a) The fingerprint data collected by a fingerprint recognition device amounts to "personal data" (section 2(1) of the Ordinance)

30. A full fingerprint image is a unique physiological trait that identifies the individual. It is hence personal data. However, some may argue that if the collected fingerprint data is converted and stored in numerical code, the resultant numbers are meaningless and therefore not personal data. The Commissioner does not agree with this argument as these numbers are still capable of identifying an individual, when linked to other personal identification particulars such as the individual's name. After all, the purpose of collecting fingerprint data through these fingerprint recognition devices is to identify a person or verify his identity.

31. There is also the argument that if only some features of a fingerprint are collected, they may not amount to personal data, as a full fingerprint image cannot be reconstructed from the features. Hence, the use and collection of these features would not breach any DPPs relating to personal data. On this point, the Commissioner would like to draw reference to the paper entitled "Fingerprint Biometrics: Address Privacy Before Deployment" published by the Information and Privacy Commissioner of Ontario (Canada) in November 2008. The paper explains that reconstruction of a fingerprint image from just features of a fingerprint with striking resemblance of the real image is not uncommon[6].

[6] "*Until recently, the view of non-reconstruction was dominant in the biometrics community. However, over the last few years, several scientific works were published that showed that a fingerprint can, in fact, be reconstructed from a minutiae template (features of fingerprint). The most advanced work was published in 2007 by Cappelli et al. The authors analyzed templates compatible with the ISO/IEC 19794-2 minutiae standard. In one test, they used basic minutiae information only (i.e. positions x, positions y, and directions). In another test, they also used optional information: minutiae types, Core and Delta data, and proprietary data (the ridge orientation field in this case). In all the tests, the authors were*

The paper goes on to demonstrate that it is not difficult for someone to create an artificial fingerprint using the information in the fingerprint template to fool a fingerprint recognition system for malicious purposes[7].

32. In sum, the collection of fingerprint data of its employees by Queenix, regardless of whether the data takes the form of a full image or a numerical code based on only some features of the fingerprint, amounted to the collection of "personal data" as defined under section 2(1) of the Ordinance.

(b) Fingerprint data is sensitive personal data

33. Fingerprint is a unique physiological trait which an individual is born with. It is a unique identifier of an individual which remains unchanged throughout his lifetime. As such, it is used commonly in criminal investigation. Unlike a password or a personal identification number, an individual cannot change his fingerprint if his fingerprint data is stolen or lost. Hence, any improper collection or use of fingerprint data can lead to grave consequences, such as identity theft. In short, fingerprint data is highly sensitive personal data, and its collection, use and retention should be managed with extreme caution. These processes can be justified only if less privacy-intrusive means to achieve the same goal in the circumstances are not available.

(c) The collection of fingerprint data by Queenix was excessive (DPP1(1))

34. The following questions were addressed in determining whether Queenix's collection of fingerprint data was excessive:

---

able to reconstruct a fingerprint image from the minutiae template. Very often, the reconstructed image had a striking resemblance with the original image. Even though this reconstruction was only approximate, the reconstructed image was sufficient to obtain a positive match in more than 90% of cases for most minutiae matchers."
(Source: https://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf)

[7] "*The potential repercussions of this work for the security and privacy of fingerprint minutiae systems are as follows: The fingerprint image reconstructed from the minutiae template, known as a 'masquerade' image since it is not an exact copy of the original image, will likely fool the system if it is submitted. A masquerade image can be submitted to the system by injecting it in a digital form after the fingerprint sensor. A malicious agent could also create a fake fingerprint and physically submit it to the sensor. The techniques of creating a fake fingerprint are inexpensive and well-known from the literature. The ability to create a masquerade image will increase the level of interoperability for the minutiae template. The masquerade image can be submitted to any other fingerprint system that requires an image (rather than a minutiae template) as an input. No format conversion of the minutiae template would be required.*"
(Source: https://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf)

(i) Was the collection of fingerprint data necessary to meet the purposes of safeguarding office security and monitoring staff attendance?
(ii) Was the collection of fingerprint data an effective means to serve the aforesaid purposes?
(iii) Was the adverse impact on personal data privacy proportionate to the benefits brought by the collection of fingerprint data?
(iv) Was there any less privacy-intrusive way to achieve the same purposes? If yes, data user should consider using the alternative way so as to eliminate, minimise or lessen the adverse impact on personal data privacy.

35. In this regard, the Commissioner has the following observations:-

Security

(i) Queenix experienced several day-time theft incidents in its office and showroom. The thefts concerned, however, were all committed by its staff and customers, who were authorised to access the office and showroom, and as such, the installation of the fingerprint recognition devices to prevent unauthorised entry would not help prevent these thefts. Indeed, these thefts happened after the installation of the fingerprint recognition devices. Installation of CCTV cameras appears to be a more effective means. As mentioned above, the thefts were detected and the culprits identified through the CCTV footage.

(ii) Furthermore, always keeping the entrance doors to both the office and the showroom locked would help maintain security during Queenix's opening hours. The observation of this basic security rule is more important than choosing a door lock operated by fingerprint in preference to a door lock operated by other means.

(iii) The installation of fingerprint recognition device outside the showroom may help deter burglars from breaking into the showroom outside Queenix's opening hours. However, a strong door lock or a chain lock, both of which do not involve collection and retention of personal data, will serve the same purpose. Indeed, Queenix had already installed several security devices to

safeguard its property outside opening hours, including CCTV cameras, digital locks, ordinary door locks and a chain lock. These all render the fingerprint recognition devices redundant.

Attendance

(iv) It is basic office administration for organisations to maintain accurate attendance records of their employees. Nonetheless, solely to serve this relatively simple task is not a sufficient ground for the collection of fingerprint data of employees, taking into account the privacy intrusiveness of collection of fingerprint data and the possible adverse impact it could result in the event that the fingerprint data is leaked or misused, as explained in paragraph 33 above.

(v) As Queenix had only 20 employees, it would be relatively easy to monitor their attendance without the use of a fingerprint recognition device. Queenix could have used other alternatives that do not involve the collection or retention of additional personal data, e.g. a password or a smartcard that carries an identification number, as explained in paragraphs 24 and 25 above. Furthermore, it may consider using a smartcard that carries the fingerprint template of its employee as explained in paragraph 26 above. However, the smartcard should be an anonymised smartcard and only kept by the corresponding employee to which the fingerprint belongs to. Moreover, the CCTV cameras monitoring the activities at the entrance of the office should help discourage the "buddy-punching" activities, if any.

36. Having carefully considered all the above factors, the Commissioner is of the view that it is not absolutely necessary for Queenix to collect employee fingerprint data for the purposes of security and monitoring staff attendance. There are readily available alternatives which do not involve collection of personal data, e.g. smartcard and password. The collection of fingerprint data by the fingerprint recognition devices generated a benefit to Queenix in terms of safeguarding office security and monitoring staff attendance. This, however, was disproportionate to the potential harm that could be caused to the staff.

37. Accordingly, the Commissioner finds the collection of employees'

fingerprint data by Queenix was excessive in the circumstances of the case, thereby constituting a contravention of DPP1(1) of the Ordinance.

(d) The collection of fingerprint data by Queenix was unfair (DPP1(2))

38. While the Commissioner respects the free will of a data subject to voluntarily consent to providing fingerprint data for different legitimate purposes, the Commissioner is also concerned with the question of whether or not the consent is genuine and an informed one.

39. A genuine consent is one given freely, unhampered by improper pressure, undue influence, or threat. In a situation where a disparity of bargaining power exists, such as an employer-employee relationship in this case, the consent could not be considered to be freely given by the employees if they are not given the choice to opt for other alternatives. As Queenix made the provision of fingerprint data compulsory without providing any alternatives, the Commissioner has reasons to believe that employees did not give their consent freely, as in the case of the Complainant.

40. An informed consent could be made only if Queenix's employees were the choice to opt for other alternatives. Queenix did not inform its employees of relevant matters such as whether the whole or partial images of fingerprints were collected; how the fingerprint recognition devices operated; the class of persons to whom fingerprint data might be transferred; the privacy risk associated with the collection and use of fingerprint data and the measures to prevent abuse or improper handling of the data; the channel for employees to inquire about the accuracy of their attendance data collected; the retention period of their fingerprint data and the persons who could access the fingerprint data, etc. Given Queenix had no knowledge of most of these matters, it could not have taken measures to prevent leakage or improper handling of its employees' fingerprint data.

41. In sum, the purported consent to providing data by Queenix's employees was neither genuine nor an informed one, and the Commissioner is of the view that the collection of the employee fingerprint data by Queenix was not fair in the

circumstances, and was thus a contravention of DPP1(2) of the Ordinance.

(e) Conclusion

42. Based on the above, the Commissioner finds that the collection of the employee fingerprint data by Queenix for the purposes of security and monitoring staff attendance constituted contraventions of DPP1(1) and (2) of the Ordinance.

V. Other Recommendations

43. Decades ago, fingerprint recognition technology was used almost exclusively in government programmes and law enforcements activities such as issue of identification documents, border control and criminal investigation. With advancement in technology leading to improved effectiveness and lowered cost in the use of fingerprints for identification purposes, business applications directed at consumers have become a growing trend. Fingerprint recognition devices are now readily available, affordable, and commonly used. If one walks through a computer shopping mall or browses eBay, one can easily find a range of models of these devices priced at as low as HK$200. Not coincidentally therefore, fingerprint door locks are being used by individual residential and commercial units. Fingerprint recognition devices are increasingly used by employers for the purposes of enhancing office security and monitoring staff attendance, as manufacturers of these devices promote their products as handy tools and a quick fix to the issue of "buddy-punching". A further common example of the use of fingerprint recognition technology is to unlock one's smartphone with a fingerprint instead of a password.

44. As the use of fingerprint recognition and other biometric technologies becomes increasingly common, it is imperative that privacy and data protection are not compromised. The use of fingerprint recognition devices by Queenix is a vivid example of preferring the convenience and affordability of such devices to the neglect of the underlying privacy concerns. The case illustrates how privacy rights could be sacrificed on the altar of technology if people fail to understand and assess the privacy risks which technology can generate.

Technology is certainly to be embraced because it works wonders but irresponsible use of technology must be discouraged.

45. As discussed in paragraph 33 above, fingerprint data (and indeed many biometric data) is highly sensitive personal data because it is a unique physiological trait which an individual is born with. It can irrefutably identify an individual and it remains unchanged throughout his lifetime. Given its uniqueness and immutability, fingerprint data must be protected against identity theft or misappropriation. It should be collected only when justified, and used with appropriate procedural and technological safeguards to prevent unauthorised access to and use of the data.

46. Before collecting fingerprint data, an organisation must satisfy itself that this is necessary to meet a specific need and there is no other less privacy-intrusive means which could be equally effective to serve the same need. A fingerprint recognition device should not be used simply because it is readily available, convenient and cost-effective. It may be an appropriate tool to control entry to high security areas but to apply it merely for checking staff attendance would be questionable.

47. Where the use of fingerprints is justified, the organisation would need to further consider the number of fingers that needs to be engaged and the amount of fingerprint data (in terms of minutiae and non-minutiae information) that needs to be collected to achieve a desired level of accuracy in identification or authentication of individuals. In this regard, it should be borne in mind that identification and authentication are related but different processes.

48. In an identification system which involves a "one-to-many" match of a person's fingerprint with a pool of fingerprint templates stored in a central database, the number of templates in the database will determine how much fingerprint data needs to be collected. In other words, the number of employees that have to be checked for security access determines the amount of fingerprint data that needs to be collected from each employee and stored in the central database.

49. On the other hand, authentication does not require identification each and every time an eligible individual uses a service or an authorised person gains access to a restricted area. Once a person's eligibility for a service or authority to gain access to a restricted area has been verified, he could store his fingerprint template on a smart card given to him as proof of his eligibility or authority (see paragraph 26 above). Subsequent authentication would then involve a "one-to-one" match of his live fingerprint with the stored template in his possession. In the circumstances, the organisation is not required to collect the fingerprint data and store it in a central database, and the individuals will be in a position to keep a tight rein on their own fingerprint data.

50. Further, employers should not exert undue influence or threaten employees when seeking to gain the latter's consent to collect their fingerprint data, as such conduct would amount to unfair collection of personal data. In this regard, one needs to bear in mind the disparity in bargaining power between an employer and his employee as the latter may hesitate to decline to provide his fingerprint when asked to do so. Hence, unless the employer offers to the employees options other than the collection of fingerprint data, the consent of the employees obtained might not be regarded as genuine. In addition, the consent must be unambiguous and informed. In other words, the employees have to be told of the privacy risks associated with the collection and use of fingerprint. Finally, the employees' consent should be recorded in writing to avoid misunderstanding and subsequent dispute.

51. Further details on the procedural and technological safeguards for the collection and use of fingerprint data are found in the "Guidance on Collection and Use of Biometric Data" published by the PCPD. The guidance provided also applies to other biometric data used for recognition purposes including DNA, retinal scans, facial image, palm vein image, and handwriting pattern.