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

Investigation Report: The Hong Kong Police Force

Leaked Internal Documents Containing Personal Data via Foxy

(English translation)

(This is an English translation of the Report compiled in Chinese. In the event of any conflict between this English version and the Chinese version, the Chinese version shall prevail.)

Report Number: R13 - 15218

Date issued: 24 October 2013

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

Investigation Report: The Hong Kong Police Force leaked internal documents containing personal data via Foxy

This is the report of the investigation carried out by the Privacy Commissioner for Personal Data (the "**Commissioner**") pursuant to section 38(b) of the Personal Data (Privacy) Ordinance, Cap. 486 (the "**Ordinance**") against the Hong Kong Police Force (the "**HKPF**") in relation to two incidents of data leakage of police documents containing personal data via Foxy, a peer-to-peer file sharing software ("**Foxy**") in August 2011 and September 2012 respectively. This report is published in the exercise of the power conferred on the Commissioner 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."

ALLAN CHIANG
Privacy Commissioner for Personal Data

Investigation Report: The Hong Kong Police Force leaked internal documents containing personal data via Foxy

Media reported that members of the public found the Hong Kong Police Force ("HKPF") accidentally leaking internal documents which contain personal data via the sharing software Foxy. An investigation into two incidents concluded that the HKPF did not adhere to the Data Protection Principle 4 ("DPP4") with regard to data security in a case that involves 210 copies of witness statements, internal documents and correspondences. But the HKPF has since 2009 implemented adequate data protection measures to prevent recurrence of similar incidents. However, human errors cannot be totally eliminated. In this regard, the Commissioner advocates the building of a privacy culture in the HKPF.

Background

2. This Office received a complaint[1] in August 2008 which alleged that the HKPF leaked its police documents containing personal data through Foxy[2]("**the Case**"). After investigation by this Office, it was found that although the HKPF had instructed its off-duty officers not to take away documents containing personal data without approval, some officers would nevertheless store these documents in their personal floppy discs/portable storage devices and their personal computers for catching up with work. This was the cause for the data leakage incident.

3. The Commissioner therefore decided in the Case that the HKPF had contravened DPP4 of Schedule 1 to the Ordinance[3] for failing to take practicable measures to protect the complainant's personal data against unauthorised or accidental access, and served on the HKPF an Enforcement Notice pursuant to section 50 of the Ordinance on 23 December 2009. In January 2010, the HKPF confirmed to the Commissioner that it had taken a series of measures to comply with the requirements of the Enforcement Notice, which included (among others), stating clearly that the HKPF officers were forbidden to use their own computers installed

[1] Case No. 200808126

[2] Foxy is a peer-to-peer file sharing software developed by a Taiwanese IT company. Users generally may not be aware that Foxy would run automatically each time a computer is switched on, causing files in the computer to be sharable for download by anyone else running Foxy. Users may not have an effective means to stop the sharing and have no way to know who has downloaded their files. More information is available from: www.cuhk.edu.hk/itsc/security/gpis/tipsfoxy.html

[3] The Personal Data (Privacy) Ordinance was substantially amended on 1 October 2012, but the applicable law during the material time of this case was the version before 1 October 2012.

with Foxy for work, that they were forbidden to use any personal information and communication devices/ data storage devices of any kind for work purposes, and making "*protecting personal and confidential data*" as part of the code of conduct that should be observed by the HKPF officers, etc.

4. In August 2011 and September 2012, the media reported that numerous police documents containing personal data were searchable via Foxy. (see the table below).

Table: Two data breach incidents under investigation

	Documents containing personal data leaked via Foxy
Incident 1 (reported in the press in August 2011)	A "Reply Slip of Preliminary Selection of Police Constable Application" of the HKPF's Recruitment Division ("**the Reply Slip**"), which contained the personal data of an applicant, including his name and HKID card number. (Other documents included an operation record of HKPF officers ("**the Record**") containing operation details and a witness statement ("**the Statement**") containing the personal data including the name and address of a witness. These items were not included in this investigation as they had been covered in the Case)
Incident 2 (reported in the press in September 2012)	210 copies of witness statements, HKPF's internal memoranda, forms and correspondence ("**the Documents**") were leaked on the Internet via Foxy. The personal data involved were names, HKID card numbers, addresses and details of the prosecution of some witnesses and arrested persons.

Follow-up by this Office

5. This Office made written enquiries to the HKPF on 23 August 2011 and 10 September 2012[4]. According to the information obtained by this Office, the Record and the Statement in Incident 1 had been leaked as early as in 2008 and were within the scope of the investigation and the Enforcement Notice issued in relation to the Case. However, the Reply Slip and the Documents were not within the scope of the Case. The Commissioner therefore decided in October 2012 to commence formal investigation against the HKPF to ascertain whether its handling of documents containing personal data in the two incidents had contravened the relevant requirements of the Ordinance.

Relevant Provisions of the Ordinance

6. The provisions of direct relevance under the Ordinance to this case are as follow:

DPP4 of Schedule 1 to the Ordinance:

"*All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to –*

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data are stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data."

7. Moreover, according to section 2(1) of the Ordinance, "practicable" means "reasonably practicable".

[4] Case Nos. 201112130 and 201213584

Information obtained in relation to Incident 1

Replies of the HKPF

8. In response to our enquiry, the HKPF provided the following information:

8.1 As the HKPF had not installed any file-sharing software including Foxy in its computer system, the Reply Slip was not leaked from the HKPF's computer system;

8.2 According to the HKPF's record, it had sent a template file of "Reply Slip of Preliminary Selection of Police Constable Application" to the person whose personal data was leaked via the HKPF's email system in the incident ("the Data Subject"). He was the one who had applied for the post. Later on, the Data Subject returned the completed Reply Slip to the HKPF in person and not by email; and

8.3 According to the HKPF, its investigation officers had contacted the Data Subject and inspected his computer. It was found that Foxy was installed and the Reply Slip was stored as a file in the Data Subject's computer. There was no information showing that the leakage was caused by the HKPF's officers or the HKPF's information system problems. Hence, the HKPF believed that the incident was caused by the Foxy file-sharing software installed in the Data Subject's computer.

Replies of the Data Subject

9. This Office wrote to the Data Subject to seek his response to the HKPF's reply above. The Data Subject confirmed in writing that Foxy was installed in his computer at the material time. The HKPF subsequently checked and found a file-sharing option in the Foxy which could not be deactivated. The information stored in his computer was therefore downloadable in its entirety by others. It was very likely that this was the cause of the data leakage.

Information obtained in relation to Incident 2

Replies of the HKPF

10. In response to our enquiries, the HKPF provided the following information:

10.1 According to the HKPF, subsequent to the issue of the Enforcement Notice on the HKPF in 2009 by this Office, the HKPF has taken improvement measures, including configuring the USB ports of HKPF's computers since August 2009 to accept approved USB thumb drives only; formulation of information security instructions and guidelines; strengthening of security measures and support; and enhancement of the HKPF officers' knowledge of information security. In this connection, the HKPF provided to this Office for reference the relevant parts of Police General Orders ("**PGO**") and the Force Information Security Manual ("**FISM**") revised since 2009;

10.2 The PGO and the FISM were uploaded to the HKPF's intranet for the information of all the HKPF officers. They would also be informed of any amendment by announcements on noticeboards. Every officer is duty-bound to read the provisions;

10.3 Regarding the leakage of the Documents in Incident 2, the HKPF's initial enquiry revealed that a police officer ("**the Police Officer**") had since 2007 occasionally used his private USB thumb drive to download documents to his own computer ("**the Computer**") and occasionally used the Computer for work purpose, all without the approval of the HKPF;

10.4 The Police Officer had attended training organised by the HKPF on four days between February 2009 and May 2010. The training included personal data protection and information security requirements in the PGO and the FISM;

10.5 The HKPF reminded all officers of the importance of information security and their duty to observe the same by email on 23 November 2010. The email also stated that officers shall not use their own computers for work purpose unless prior approval from the Formation Information Technology Security Officer ("**FITSO**") has been obtained in accordance with the FISM. According to the HKPF's record, the Police Officer read the email on 13 December 2010;

10.6 The Police Officer sold the Computer in mid-2011 without first handing the equipment to the FITSO for inspection in accordance with the requirement of the FISM;

10.7 Though the Police Officer had tried to delete all the information in the hard disk by the erasure software that came with the Computer before selling the Computer, he did not remove the hard disk or use the software approved by the Chief Systems Manager (Information Technology Branch) to securely erase all the official information in accordance with the requirements of the FISM;

10.8 Therefore, the HKPF considered that the Documents could have been recovered from the hard disk after sale of the Computer, and the data was leaked subsequently. The HKPF pointed out that the incident was just an isolated case and was not related to the security of its information system; and

10.9 Police officers who repeatedly or blatantly violated the requirements of the FISM will be subject to disciplinary action. The HKPF is conducting a disciplinary investigation against the Police Officer under section 3(2)(e) of the Police (Discipline) Regulations (Cap. 232A), for the punishable disciplinary offence of "contravention of police regulations, or any police orders, whether written or verbal".

Statement of the Police Officer

11. The Police Officer made a statement to this Office in respect of Incident 2 which contains the following information:

11.1 The Police Officer admitted that since his unit in which he worked in 2007 had only one office computer, he had used his own USB thumb drive to download certain documents containing personal data from the HKPF's computer to the Computer for work convenience. But the Police Officer clarified that he had only downloaded such documents once;

11.2 The Computer was used for handling office work until August 2008 when he was transferred to a post with an office computer provided. Following another job transfer in February 2009, he resumed using the Computer for office work;

11.3 However, the Police Officer claimed that he had not used the Computer to connect to the Internet or allowed others to use the Computer, so leakage of documents stored in the Computer by Foxy was impossible;

11.4 In mid-2011, the Police Officer sold the Computer. Before the sale, he had formatted the hard disk repeatedly by using the software that came with the Computer, but the software was not the one approved by the Chief Systems Manager (Information Technology Branch) in accordance with the FISM. Moreover, the Police Officer had not surrendered the Computer to FITSO for inspection before sale, thus contravening the requirements in the FISM; and

11.5 The Police Officer stated that he knew that HKPF officers had to obtain prior approval before using their own computers for work purposes. He also knew that before selling the Computer which had been used for work purposes, the HKPF required that the hard disks had to be removed, that an approved software had to be used for data erasure, and that the computers had to be handed to FITSO for inspection. But since he had not applied for permission before using the Computer for work purposes in the first place and he did not envisage that his act would lead to serious consequences, he had not followed the above-mentioned requirements.

The Findings of the Commissioner

12. Under DPP4, the HKPF is obliged to take all practicable steps to ensure that personal data held by it are protected against unauthorised or accidental access, processing, erasure or other use.

13. In this case, the Commissioner has to consider whether the HKPF has taken all reasonably practicable measures to safeguard the personal data in the Reply Slip in Incident 1 and the Documents in Incident 2.

Whether the HKPF Had Contravened DPP4 in Incident 1?

14. According to the HKPF, Foxy was not installed in its computer system, but it was installed in the Data Subject's computer which stored the file of the Reply Slip. Hence, the HKPF believed that the leakage of the Reply Slip was caused by the Foxy installed in the Data Subject's computer.

15. The Data Subject agreed with the HKPF's view. He added that there was a file-sharing option in the Foxy that could not be deactivated, but at that time he was not aware that the data in his computer could be downloaded by others due to this setting.

16. The information provided by the HKPF and the Data Subject in this incident was consistent, and there was no information showing that Incident 1 was caused by other reasons. Hence, the Commissioner does not find in Incident 1 a DPP4 contravention on the part of the HKPF.

Whether the HKPF Had Contravened DPP4 in Incident 2?

17. In examining whether the HKPF had contravened DPP4 in Incident 2, the Commissioner has to consider two aspects. Firstly, the Commissioner has to understand the cause of the incident and ascertain whether the HKPF had any policy in place to prevent the incident from happening. Secondly, the Commissioner has to examine whether the HKPF had taken adequate measures to ensure that the relevant HKPF officers knew, understood and complied with the policy. If there was policy alone but no mechanism or measures to implement it, the HKPF could still contravene DPP4.

18. The Commissioner has examined the revisions or improvements in information security measures laid down in the PGO and the FISM. He noted that the following new requirements[5] have been in place since August 2009 ("**the 2009 requirements**"):

(a) PGO Chapter 19-21: "*Security measures such as encryption using Force provided tools, and password protection of electronic files/data shall be taken to protect sensitive or classified information*";

(b) PGO Chapter 19-21: "*Force members are not permitted to use their private ICT* [information and communications technology] *equipment (e.g. memory cards, USB thumb drives or non-government provided storage facilities) to process or store electronic information or data unless written approval has been obtained from their Formation Commander who may seek advice from the FITSO or CIP SCU IS*";

(c) PGO 19-21: "*Force members shall not carry any information or electronic data (stored in any media) of or above 'Confidential' classification off police premises unless prior approval from direct supervisor at SP rank or above has been obtained*";

(d) FISM paragraph 2.2.14.3: "*Classified information must not be processed or stored in privately owned computers and privately owned portable electronic storage devices, such as USB storage devices, Flash memory cards, except with the written approval from the Formation Commander of SP rank or above*";

(e) FISM paragraph 4.15.1.1: "*user who wishes to withdraw privately owned computers for official use at work shall notify the FITSO seven days before removing it from the formation. The FITSO shall conduct a physical inspection of the hard disk drive and all data storage media containing official information to ensure that all data connected with official purposes are securely erased, by using software approved by CSM IT* [Chief System Manager (Information Technology Branch)], *before removal*";

[5] Requirements in paragraphs 18(a) to (c) are quoted from the current version of the PGO. Requirements in paragraphs 18(d) to (f) are translation of the provisions in the August 2009 version of the FISM.

(f) FISM paragraph 4.15.2.1: "*Before the removal for repair or the transfer of ownership of any privately owned computer which has been approved for duty purposes, the hard disk shall be physically removed or securely erased, by using software approved by CSM IT, of all data relating to the officer's official duties. The officer shall not allow unauthorized persons' access to the information on the hard disk*".

19. There is an apparent discrepancy between the information provided by the HKPF (paragraph 10.3 above) and the Police Officer (paragraph 11.1 above) as to how often the Police Officer had used his own USB thumb drive to download police documents containing personal data from police computers. Nevertheless, since the USB ports of the HKPF's computers accepted in practice only approved USB thumb drives from August 2009, it can be deduced that any such unauthorised downloading by the Police Officer would have ceased at the latest by August 2009. However, during the period between 2007 and August 2009, the improved security requirements noted in paragraphs 18(b) to (d) above, and the specific measure that only authorised USB thumb drives may be accepted by HKPF's USB connectors noted in paragraph 10.1 above were not in place. At that time, there were only general guidelines on using HKPF officers' own computers for official purpose in the FISM (i.e. police officers were required to seek prior approval). With regard to the handling and storage of electronic data or use of private USB thumb drives, there was no specific instruction and guideline in the then FISM and PGO.

20. Therefore, in keeping with our conclusion in the Case of 2009, the Commissioner is of the view that when the Police Officer downloaded police documents containing personal data to his private USB thumb drive, the HKPF had not taken all practicable measures to prevent this misconduct from occurring. Hence, it had contravened DPP4.

21. Notwithstanding this finding, the HKPF had in 2007 required the HKPF officers to seek prior approval for the use of their own computers for work purposes. Also, the 2009 requirements were formulated to prevent police officers from using USB thumb drives to store police documents, and to ensure that police documents stored in HKPF officers' own computers would be safely deleted. Besides, the HKPF had used various means as set out in paragraph 10 to inform police officers of those instructions and guidelines, including the uploading of the PGO and the FISM to the HKPF's intranet, the sending of email reminder to all officers, and, in particular, the provision of four relevant training sessions to the Police Officer between 2009 and

2010. In the circumstances, the continued unauthorised use of the Computer for work after August 2009 with the previously downloaded and stored police documents, and the improper means in deleting the official information before sale of the Computer in mid-2011, represented the acts and omissions attributable to the Police Officer, in contravention of the HKPF's standing instructions (which were revised in 2009).

22. In fact, according to the information provided by the HKPF, the Officer had attended four training sessions. The training materials gave an overview of the personal data protection and the requirements of the Ordinance. The 2009 requirements had been covered in the two training sessions held in 2010. (see paragraph 10.4 above). The Police Officer admitted that he knew the requirements. If the Police Officer, after learning the 2009 requirements, had sought the HKPF's approval for the continued use of the Computer for work purposes, and had complied with the requirements of the FISM by handing the Computer to FITSO for inspection, removing the hard disk and using approved software to delete the data before selling the Computer in 2011, Incident 2 should have been avoided.

23. The duty imposed on data users by DPP4 is that "*all practicable steps shall be taken*" to safeguard personal data. Data users' obligations are not absolute. They are not expected to prevent data leakages at all costs. Whether a data user has contravened DPP4 depends on whether it has taken all practicable steps in formulating appropriate policies, devising a robust system to safeguard data and implementing adequate measures under this system. In view of the 2009 requirements drawn up by the HKPF, and the measures adopted in paragraph 10 (in particular the four training sessions provided by the HKPF to the Police Officer), the Commissioner opines that the measures taken by the HKPF at present are adequate. The Police Officer's post-2009 unauthorised and continuous use of the Computer for work purposes without approval, and his failure to use approved software to erase all official materials before the sale of the Computer, was an isolated incident of human error which does not constitute another DPP4 contravention on the part of the HKPF. The Commissioner therefore sees no justification to serve another Enforcement Notice on the HKPF directing it to step up its efforts to safeguard personal data.

Advice to the HKPF

24. It should be pointed out that although the HKPF currently has "*taken all practicable steps*", given the importance and sensitivity of the personal data contained in the HKPF documents, the Commissioner urges the HKPF to go beyond fulfilling the minimum requirements under the Ordinance and strive for further means to safeguard data with a view to preventing recurrence of similar incidents.

25. Incident 2 revealed that despite the implementation of the HKPF's 2009 requirements, the past use of USB thumb drives to store official data/documents and the continued unauthorised and improper use of the HKPF officers' own computers for work purposes by individual police officers could still lead to leakage of police data (which might contain personal data) years later. As police officers who used their own computers and USB thumb drives could be subject to disciplinary action due to breach of the 2009 requirements, they may be tempted not to follow the requirements of the FISM, but to use other means to fix the problem themselves.

26. In this regard, even though human errors cannot be totally eliminated, the Commissioner is of the view that the HKPF should proactively face the problem and adopt effective improvement measures to minimise data leakages caused by human error, including the above non-compliance of standing instructions by police officers who were caught in a dilemma. The HKPF can adopt different formal or informal means to address the above dilemma. To be effective, these means must be designed to suit the operation nature and corporate culture of the HKPF. Therefore, the Commissioner can only provide general advice to the HKPF but cannot prescribe measures in concrete terms.

27. For example, the Commissioner learned from the information obtained in the Case that the HKPF's IT Division had provided a "Personal Computer Cleaning" programme for police officers' use in December 2009 to help them check and delete the personal data/confidential data on their own computers. Though this is an effective measure, the Police Officer was apparently unaware of the programme since he still adopted an improper method to erase the information contained in the Computer. The HKPF is advised to consider strengthening the internal promotion of this programme. The HKPF may also set up enquiry hotlines to offer assistance to police officers who wish to seek help on an anonymous basis.

28. In addition, the Commissioner recommends that the HKPF promotes case sharing and exchange of experience among police officers to enhance the awareness of personal data protection and the serious consequences that may ensue as a result of data leakages on the Internet. This will help promote the building of a privacy-respectful and data-secure culture, and compliance with the HKPF's security instructions and guidelines.

Concluding Remarks

29. Data users are obliged to protect personal data by reasonable security safeguards against such risks as loss, unauthorised access, destruction, use, modification or disclosure of data. They should note that many security breaches are simply the result of human error. Recklessness or simple carelessness of a single employee can undermine sound privacy policies and robust security practices. This underlies the importance for organisations to institute comprehensive internal training and awareness programmes for their staff. To ensure an organisation-wide commitment, the building of a culture of privacy is imperative.

30. Organisations collecting and managing personal data are always faced with data security risks, regardless of the form in which the data is retained. However, rapid advances in computing power, coupled with easy access to desk-top and mobile devices globally connected through the Internet, have increased the scale and volume of personal data flows, the ability to store data indefinitely and the associated risks of data breaches.

31. Both data users and data subjects should be aware of the privacy pitfalls in the use of ICT. The Foxy software in this case is a good learning point. Once a data file is leaked through the Foxy network, there is practically no effective recovery means. Although the company which developed Foxy has ceased business, at least 400,000 users are still running this software on their computers. They are advised to make sure that they (and anyone using their computers) understand how their version of Foxy works and configure it appropriately to protect their data files. For persons who for some reasons still wish to download this software for use, they will have to resort to unofficial channels and thus run the risk of obtaining a copy which contains malware or one which may have been tampered with, rendering the extent of data sharing uncontrollable.