根據《個人資料（私隱）條例》（第 **486** 章）第 **48**（**2**）條

發表

# 調查報告：警務處經Foxy共享軟件外洩載有個人資料的警隊文件

**報告編號：R13 - 15218**

發表日期：**2013** 年 **10** 月 **24** 日

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

# 調查報告：警務處經Foxy共享軟件外洩載有個人資料的警隊文件

個人資料私隱專員（下稱「**專員**」）根據《個人資料（私隱）條例》（第 486 章）（下稱「**條例**」）第 38(b)條對香港警務處（下稱「**警務處**」）先後於 2011 年 8 月及 2012 年 9 月發生兩宗涉及載有個人資料的警隊文件經 Foxy「點對點」共享軟件（下稱「**Foxy**」）外洩的事故，主動進行調查，並根據條例第 VII 部行使賦權發表本報告。條例第 48(2)條列明，「*專員在完成一項調查後，如認為如此行事是符合公眾利益的，可－*

*(a) 發表列明以下事項的報告－*

*(i) 該項調查的結果；*

*(ii) 由該項調查引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及*

*(iii) 由該項調查引致的、專員認為適合作出的任何其他評論；及*

*(b) 以他認為合適的方式發表該報告。」*

**個人資料私隱專員　蔣任宏**

# 調查報告：警務處經Foxy共享軟件外洩載有個人資料的警隊文件

**有傳媒報導指香港警務處人員經 Foxy 共享軟件意外洩漏警隊文件，內含個人資料。私隱專員經調查報導涉及的兩宗事故後認為，在一宗涉及 210 份證人口供、警務處內部文件及書信文件外洩的事故中，警務處未有依從資料保安方面的保障資料原則（第 4 原則）。惟該處已於 2009 年起實施充分的資料保障措施，以避免事件重演。然而，人為錯失是未可完全避免的。因此，專員建議警務處應建立保障私隱的文化。**

## 背景

2. 公署於 2008 年 8 月接獲市民投訴[1]，指警務處涉嫌將載有其個人資料的警務處文件經 Foxy[2]外洩（下稱「**該個案**」）。公署經調查後，認為警務處雖然已訂明警務人員不得擅自攜帶載有個人資料的文件下班，但他們往往為追趕工作進度，而在未經上司批准的情況下，便妄自把載有個人資料的文件儲存於私人的電腦磁碟或便攜式儲存裝置上，以及其私人擁有的電腦內，以致發生資料外洩事故。

3. 專員在上述該 2008 年個案中裁定警務處未有採取切實可行的預防措施，保障有關投訴人的個人資料免受未獲准許或意外的查閱，因而違反了條例[3]附表 1 的保障資料第 4 原則的規定，專員並根據條例第 50 條，於 2009 年 12 月 23 日向警務處發出執行通知。於 2010 年 1 月，警務處向專員確認已採納該執行通知的指示而採取一系列措施，包括明文禁止警務處人員使用安裝有 Foxy 分享軟件的私人電腦處理公務及禁止使用私人資訊及通訊科技設備或任何形式的數據儲存裝置作公事用途及將「保護個人及機密資料」定為警務處人員須遵從的警隊行為指引之一等。

---

[1] 個案編號：200808126

[2] Foxy 是一個點對點分享軟件，由台灣一間資訊科技公司開發。由於 Foxy 一經安裝後會在用家不了解的情況下自動啟動，強制將用家電腦上資料分享夾的檔案分享，供其他 Foxy 的用戶搜尋和下載。用戶無法完全停止分享，也不會知悉誰人下載了檔案。
了解更多：www.cuhk.edu.hk/itsc/chinese/security/gpis/tipsfoxy.html

[3] 《個人資料（私隱）條例》已於 2012 年 10 月 1 日大幅修訂。但本個案關鍵時間適用的法律是條例於 2012 年 10 月 1 日前的版本。

4. 其後，在 2011 年 8 月及 2012 年 9 月，傳媒報導經 Foxy 搜尋到多份載有個人資料的警務處文件的事故(見下表)。

表: 本調查報告涵蓋的兩宗個人資料外洩事故

| | 經 Foxy 於互聯網上<br>外洩含有個人資料的文件 |
|---|---|
| 事故一<br>(傳媒於 2011 年 8 月報導) | 警務處招募組的「警員職位申請初步遴選」回條（下稱**「該回條」**），當中載有一名投考警隊人士的姓名及身份證號碼等個人資料。<br><br>(公署已在先前該個案中調查報導所指的其他外洩文件，包括一份警務人員的行動紀錄，及一份證人口供紙，內有警務人員的相關行動經過，以及該證人的姓名及住址等個人資料) |
| 事故二<br>(傳媒於 2012 年 9 月報導) | 210 份證人口供、警務處內部備忘錄、表格及書信文件（下稱「**該些文件**」），涉及證人及被逮捕人士的姓名、香港身份證號碼、地址及檢控的內容等個人資料。 |

*公署的跟進*

5. 公署先後在 2011 年 8 月 23 日及 2012 年 9 月 10 日向警務處作書面查詢[4]。根據警務處回覆的資料，事故一涉及的警務人員行動紀錄及證人口供紙均早在 2008 年已被外洩，公署已於該個案的調查中處理及納入執行通知的範圍內。至於事故一中的該回條及事故二的該些文件，則不包括在該個案中。因此，專員於 2012 年 10 月決定就上述兩宗事故對警務處展開正式調查，以確定警務處在處理載有個人資料的文件時有否違反條例的相關規定。

[4] 個案編號：201112130 及 201213584

## 條例的相關規定

6. 條例下與本個案有關的條文如下:

> 條例附表 1 的保障資料第 4 原則（下稱「第 4 原則」）訂定：
>
> *「須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料(包括採用不能切實可行地予以查閱或處理的形式的資料)受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響，尤其須考慮—*
>
> *(a) 該等資料的種類及如該等事情發生便能做成的損害；*
> *(b) 儲存該等資料的地點；*
> *(c) 儲存該等資料的設備所包含(不論是藉自動化方法或其他方法)的保安措施；*
> *(d) 為確保能查閱該等資料的人的良好操守、審慎態度及辦事能力而採取的措施；及*
> *(e) 為確保在保安良好的情況下傳送該等資料而採取的措施。」*

7. 另外，按條例第 2(1)條的釋義，「*切實可行*」是指「*合理地切實可行*」。

## 事故一調查所得的資料

### *警務處回應*

8. 警務處回應公署的查詢時提供了以下資料：

> 8.1 警務處表示該處的電腦系統並沒有安裝 Foxy 或其他分享軟件，因此該回條並非經警務處的電腦系統外洩；

8.2 根據警務處的紀錄，警務處曾將「警員職位申請初步遴選回條」的空白範本檔案，經警隊的電郵系統傳送予案中的資料當事人（即有關應徵人士），以便他填交警員職位申請。其後，資料當事人將填妥的回條親身交回警務處，而沒有經電郵系統傳送；

8.3 警務處調查人員曾聯絡該資料當事人，及檢查他的電腦，發現該資料當事人的電腦安裝了 Foxy 軟件，電腦上存有該回條的檔案。因此，警務處認為事故是由該資料當事人電腦的 Foxy 軟件所引致，及並沒有資料顯示洩漏事件關乎警務處的人員或該處資訊系統的問題。

*資料當事人回應*

9. 公署發信給事故一的資料當事人，以徵求他就警務處上述回覆的回應。該資料當事人在書面回覆中確認在案發時間，他的電腦確實安裝了 Foxy。經警務處檢查後，警務處發現 Foxy 內的共享電腦資料選項無法關閉，所以他的電腦內的資料可經 Foxy 網絡任人下載，而極有可能因此而導致資料外洩。

<u>事故二調查所得的資料</u>

*警務處回應*

10. 警務處回應公署的查詢時提供了以下資料：

10.1 警務處表示，在公署於 2009 年向警務處發出執行通知後，警務處已採取相應改善措施，包括自 2009 年 8 月起警隊電腦的 USB 接頭只容許使用經認可的 USB 記憶體；制定資訊保安的規定及指引；加強安全設施及支援；提高警隊成員對資訊保安的認識等工作。就此，警務處提供了警務處在 2009 年起修訂的《警察通例》及《警隊資訊保安手冊》的相關部分予公署參考；

10.2 《警察通例》及《警隊資訊保安手冊》均上載到警察內聯網供所有人員參閱，每次修訂均會透過警察內聯網警隊告示欄通知所有人員，而每一位人員均有責任閱讀各項條文；

10.3 就事故二中該些文件的外洩，警務處進行的初步調查發現文件來自一名警務人員（下稱「**該警員**」）的私人電腦。該警員未得警務處批准，從 2007 年起偶爾使用其私人 USB 記憶體從警隊電腦中下載文件至其私人電腦（下稱「**該電腦**」），並用該電腦處理公務；

10.4 該警員在 2009 年 2 月至 2010 年 5 月期間，出席了四次由警務處舉辦的訓練，訓練內容包括保護個人資料以及《警察通例》和《警隊資訊保安手冊》內有關資訊保安的規定；

10.5 警務處曾於 2010 年 11 月 23 日向所有警務人員發出電子郵件，提醒各人員資訊保安的責任及重要性，並述明警務人員如有需要使用私人電腦用作公務用途，必須根據《警隊資訊保安手冊》，事先獲得單位資訊科技保安主任的批准。根據警務處紀錄，該警員已於 2010 年 12 月 13 日閱讀該電子郵件；

10.6 該警員在 2011 年中出售該電腦，但在出售前未有按照《警隊資訊保安手冊》的要求，將該電腦交予單位資訊科技保安主任檢查；

10.7 該警員在出售該電腦前，已用隨該電腦附送的移除程式清除硬碟內所有資料，但他未有按照《警隊資訊保安手冊》的規定，移除硬磁碟機或使用經警務處總系統經理（資訊應用科）許可的軟件安全地清除所有與公務有關的資料；

10.8 因此，警務處認為有可能有人從該出售的電腦，把將硬磁碟機內已清除的文件復原，並將其外洩。警務處指事件只屬個別事件，並不涉及警務處的資訊系統的保安問題；及

10.9 警務人員屢次或公然違反《警隊資訊保安手冊》的規定會遭受紀律處分。警務處根據香港法例第 232A 章《警察(紀律)規例》第 3(2)(e)條可予以懲罰的違紀行為，即「違反警察規例或任何書面或口頭的警察命令」，正對該警員進行紀律調查。

## *警員作證*

11. 該警員就相關事宜向公署作證時提供了以下資料：

11.1 該警員承認，由於 2007 年時他所隸屬的單位只擁有一部公務電腦，為工作方便他曾使用一枝私人 USB 記憶體從警務處的公務電腦下載一些載有個人資料的警務處文件至該電腦。但該警員表示這樣的行為只此一次；

11.2 他一直使用該電腦處理公務，直至 2008 年 8 月調職至一個有提供公務電腦的崗位為止。該警員於 2009 年 2 月調職至另一單位後，他再次使用該電腦處理公務；

11.3 不過，該警員報稱不曾使用該電腦上網，亦沒有讓其他人使用，因此該電腦儲存的文件沒可能因 Foxy 而外洩文件；

11.4 2011 年中，該警員將該電腦出售。在出售前，他曾用電腦隨附的軟件多次將電腦的硬碟格式化以清除硬碟機內的資料，但並沒有按《警隊資訊保安手冊》的規定使用警務處總系統經理（資訊應用科）許可的軟件清除資料。此外，該警員亦沒有按《警隊資訊保安手冊》的規定將該電腦於出售前交予單位資訊科技保安主任檢查；及

11.5 該警員表示知悉警務人員使用私人電腦作公務用途前須事先獲得批准，同時知悉警務處規定出售曾用於公務的電腦前須移除硬磁碟機／使用許可軟件清除資料，並須交予單位資訊科技保安主任檢查。但鑑於他從一開始使用該電腦時亦無作出申請，及他沒有考慮到事情會引致嚴重後果，因此他沒有依從上述的規定。

## 專員的調查結果

12. 根據第 4 原則，警務處必須採取所有切實可行的步驟，以確保由其持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響。

13. 專員經調查後要確立警務處是否已就事故一的該回條及事故二的該些文件所載的個人資料的安全，採取所有合理而切實可行的保障資料措施。

*警務處在事故一有否違反第 4 原則？*

14. 警務處表示其電腦系統內並沒有安裝 Foxy 軟件，以及發現該資料當事人的電腦內裝有 Foxy 軟件及該回條的檔案。因此，警務處認為該回條外洩的事故，是由該資料當事人的電腦所安裝的 Foxy 所致。

15. 該資料當事人同意警務處的說法，並補充謂，Foxy 內有一個無法關閉的共享電腦資料選項，但他當時並不知道其電腦內的資料因而可讓他人下載。

16. 事故中警務處及資料當事人提供的資料一致，而本個案中亦無資料顯示有其他原因導致事故一。故專員認為警務處在事故一中沒有違反第 4 原則的規定。

*警務處在事故二有否違反第 4 原則？*

17. 專員在審視警務處在事故二中有否違反第 4 原則的規定時，需考慮兩方面。首先是事故的成因，警務處是否有既定政策防止事故發生。其次，即使警務處有相關的政策，警務處是否已採取足夠的措施使相關的警務人員知悉、瞭解並遵從政策。假如警務處空有政策，但並無機制或措施加以落實，仍然會違反第 4 原則的規定。

18. 專員參閱了警務處自公署對該個案展開調查後，對《警察通例》及《警隊資訊保安手冊》有關資訊保安方面作出修定或改善的部分，注意到警務處對警務人員自 2009 年 8 月起有以下新增的規定[5]（下稱「**2009 年規定**」）：

(a) 「*須採取保安措施保護敏感或機密資料，例如使用警隊提供的工具進行加密，以及利用密碼保護電子檔案／數據*」（《警察通例》第 19 章 21 節）；

(b) 「*除非在單位指揮官徵詢單位資訊科技保安主任或總督察（保安）（資訊系統）後，取得書面批准，警隊人員不准使用私人的資訊及通訊科技設備（例如記憶卡、USB 手指驅動器或非政府提供的儲存設施）處理或儲存電子資料或數據*」（《警察通例》第 19 章 21 節）；

(c) 「*除非事先獲得警司或以上職級的直屬上司批准，警隊人員不得把列為「機密」或以上級別的資料或電子數據（儲存在任何媒體內）帶離警察處所*」（《警察通例》第 19 章 21 節）；

(d) 「*所有機密的資料均禁止在私人擁有的電腦及私人擁有的便攜式電子儲存裝置，如 USB 儲存裝置及快閃記憶卡上處理及儲存，除非得到其警司級或以上的單位指揮官的書面批准*」（《警隊資訊保安手冊》第 2.2.14.3 段）；

(e) 「*使用者如不欲再使用私人擁有的電腦辦理公事，必須在電腦搬離單位前 7 日通知單位資訊科技保安主任。單位資訊科技保安主任須於電腦搬走前，使用經總系統經理（資訊應用科）許可的軟件檢查該部電腦的硬磁碟機及載有官方資料的資料儲存媒體，以確保所有與公職有關的資料已遭安全地清除*」（《警隊資訊保安手冊》第 4.15.1.1 段）；及

[5] 第 18(a)-(c)段的規定載於目前版本的《警察通例》。第 18(d)-(f)段的規定載於 2009 年 8 月版本的《警隊資訊保安手冊》。

(f) 「*在需要搬走進行維修的獲批准作公務用的私人擁有電腦或轉移其擁有權之前，必須移除硬磁碟機或使用經總系統經理（資訊應用科）許可的軟件安全地清除所有與公務有關的資料。有關人員不得容許未經授權人士取用硬磁碟的資料*」（《警隊資訊保安手冊》第 4.15.2.1 段）。

19. 就該警員使用私人 USB 記憶體下載含有個人資料的警務處文件的次數，警務處的初步調查結果（上文第 11(c)段）及該警員的證供（上文第 12(a)段）有相異之處。不過，基於警務處自 2009 年 8 月起規定警隊電腦的 USB 接頭只容許使用經認可的 USB 記憶體，該警員使用私人 USB 記憶體下載警務處文件的行為，理應最遲在 2009 年 8 月後停止。但在 2007 年至 2009 年 8 月這段期間，上文第 19(b)至(d)段提及的改良保安規定，以及上文第 11(a)段有關警隊電腦 USB 接頭只容許經認可的 USB 記憶體及針對使用 USB 裝置下載文件等措施尚未實施。當時的《警隊資訊保安手冊》就使用私人電腦作公事用途，只有一般性的指引（即要求警務人員須先取得批准）。但就電子資料的處理／儲存或使用私人 USB 記憶體裝置的情況，當時的《警隊資訊保安手冊》及《警察通例》均未有具體規定及指引。

20. 故此，正如公署在 2009 年對該個案所作的結論一樣，專員認為事故二中的該警員使用私人 USB 記憶體下載載有個人資料的警務處文件之時，警務處並未採取所有切實可行的措施以防止這不當行為的發生，因而違反了第 4 原則的規定。

21. 雖然如此，公署得悉警務處早於 2007 年時已有規定，警務人員擬使用私人電腦作公務用途，事前須獲批准；另外 2009 年規定則旨在防止警務人員使用私人 USB 記憶體儲存警務處文件，以及確保儲存於私人電腦的警務處文件會被安全地清除。此外，警務處使用上文第 10 段所述的措施，告知警務人員有關規定及指引，包括上載《警察通例》及《警隊資訊保安手冊》到警察內聯網；發出電子郵件以提醒警務人員，及在 2009 至 2010 年間提供四次相關的訓練。事故二中的該警員在下載及儲存警隊文件後，於 2009 年 8 月後，未經預先批准而持續地使用該電腦處理公務，以及在 2011 年中出售該電腦前未有正規地清除電腦內的資料，乃屬該警員沒有跟從警務處 2009 年已修訂的恆常規定所引致。

22. 事實上，根據警務處提供的資料，該警員出席的四次訓練的講義中已具體指明保障個人資料方面的規定，當中 2010 年兩次訓練已包含 2009 年規定（見上文第 10.4 段），而該警員亦承認他知悉該些規定。假如該警員在得悉該些規定後，按規定向警務處申請用該電腦處理公務；於 2011 年出售該電腦前之時依照《警隊資訊保安手冊》的規定將其交予單位資訊科技保安主任檢查，以及在出售前移除硬磁碟機／使用許可軟件清除資料，事故二應可避免。

23. 在第 4 原則之下，資料使用者有責任「*須採取所有切實可行的步驟*」以確保個人資料的安全。該原則並無對資料使用者施以「零事故」的絕對要求。資料使用者會否違反第 4 原則的規定，須視乎其在政策、制度及運作方面是否已採取所有切實可行的措施。鑑於警務處已作出 2009 年規定，以及採取上文第 10 段的措施（特別是警務處為該警員提供的四次訓練），專員認為警務處在保障個人資料方面所採取的措施是足夠的。至於該警員在 2009 年後未經批准和授權而持續使用該電腦作公務用途，及於出售該電腦前沒有使用許可的軟件穩妥地清除所有與公務有關的資料，則屬於個別警務人員的人為錯失，並不構成警務處就第 4 原則的另一次違反。因此，專員認為沒有理據再次向警務處發出執行通知，以指令該部門加強資料保安措施。

## 進一步建議

24. 公署須在此指出，雖然警務處目前已「*採取所有切實可行的步驟*」，但鑑於該些文件所載的個人資料的重要性及敏感性，專員敦促警務處在符合條例最低要求之餘作出改善，以避免同類事件再次發生。

25. 事故二揭示了個別警務人員在 2009 年規定生效前使用私人的 USB 記憶體儲存公務資料／文件的做法，及未獲批准而持續使用私人電腦處理公務，在多年之後仍然可能導致警務處資料（其中可能包含個人資料）外洩。有關警務人員可能考慮到早前已違規私下使用私人電腦及 USB 記憶體，可能會遭受紀律處分，選擇不按照《警隊資訊保安手冊》的規定行事，反而選擇私下採取其他辦法去處理問題。

26. 儘管人為錯誤是不可能完全避免的，專員認為警務處應正視問題並積極實施有效的改善方法，以減少人為失誤而導致的資料外洩，包括上述警務人員因進退維谷而沒有遵循規定的情況。警務處可用正式或非正式的方法去處理上述兩難情況，惟任何方法都必須基於警務處的運作性質及機構文化而釐訂。因此，專員只能為警務處提出方向性的建議，而不能指定具體的措施。

27. 舉例說，專員從該調查所獲得的資料中，了解警務處的資訊系統部在 2009 年 12 月曾提供一個「個人電腦清洗」程式供警務處人員用作檢查及清除其個人電腦所載有的個人資料／機密資料。雖然這不失為一項有效的措施，然而事故二中的該警員顯然不清楚警務處備有該程式可供使用，以致自行採用不穩妥的方式清除該電腦的資料。警務處可考慮加強在內部宣傳該程式。警務處亦可考慮設立諮詢熱線向有需要的人員以不記名方式提供支援。

28. 此外，專員建議警務處促進警務人員之間的個案分享及經驗交流，藉以加深警務人員對個人資料保護及資料外洩，特別是在網上資訊外洩可能造成的嚴重後果的認知等。這些措舉有助在部門內締造保護個人資料的文化，在潛移默化下使警務人員緊遵有關保護個人資料方面的規定及指引。

## 總結

29. 資料使用者有責任採取合理的保安措施，保護個人資料免遭遺失、未經授權的查閱、毀壞、使用、修改或披露。值得留意的是，很多資料保安的事故，都是由人為錯失釀成的。即使是完備的私隱政策和嚴格的保安措施，都有可能因為個別員工的鹵莽或粗心大意而拖跨。機構應為員工提供全面的內部培訓和提高保障私隱的意識，這是至為重要。建立尊重私隱的機構文化，是推動整個機構致力實踐的重要前提。

30. 機構在收集和管理個人資料方面，無論資料以何種形式保存，都經常面對資料保安的風險。隨著電腦運算速度提升， 桌面和流動裝置均可提供便捷的上網服務聯繫世界，大大增加了個人資料流動的範圍和流量及保存數據的能力，進而增加了資料洩漏的風險。

31. 資料使用者和資料當事人都必須留意應用資訊科技的私隱陷阱。本案中的 Foxy 軟件正是值得引以為鑑的例子。一旦資料檔案經過 Foxy 網絡外洩，基本上無有效的方法可以將資料挽回。雖然 Foxy 的開發商經已結業，但迄今全球至少有 40 萬人的電腦仍啟動著 Foxy 軟件。這些用家(以及會使用他們的電腦的人士)必須了解其 Foxy 版本如何運作，並加以適當的設定，以保護資料檔案。市民現時若需要下載這軟件，只能到非官方渠道下載，這是非常冒險的，因所得的版本有可能是惡意程式，或遭加工而招致無法控制的資料外洩事故。