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

2016 年智能健身腕帶的私隱政策透明度抽查報告

2017 年 1 月

目錄

引言

香港個人資料私隱專員公署（「**公署**」）是「全球私隱執法機關網絡」（Global Privacy Enforcement Network）[1]的成員之一，並已連續第四年參與該網絡統籌的抽查行動。

2. 今年，25 個來自世界各地的私隱執法機關，包括公署，參與抽查行動以檢測「物聯網」裝置的生產商和供應商向用戶傳達有關私隱事宜的情況。

3. 2016 年抽查行動的主題是「物聯網的問責性」。物聯網是實物網絡，當中的實物內置技術可實現其與內部狀況或外部環境溝通、感應或互動[2]。物聯網裝置的典型例子包括智能電視[3]、智能讀數錶[4] 及穿戴裝置[5]。物聯網裝置大大改善了人們的生活質素，亦創造了商業機會。然而，物聯網裝置同時亦帶來私隱關注，因為它們可在用戶不知情下收集、分析及產生有關用戶的資料，並與第三者分享有關資料。

4. 參與抽查行動的私隱執法機關可因應其管轄區的情況及他們關注的事項等，自行決定檢測的物聯網裝置的類型。鑑於智能健身腕帶方便購買及日益流行，公署決定揀選本地製造的智能健身腕帶作為抽查對象。公署檢測了五款本地製造的智能健身腕帶及其支援的流動應用程式（「**程式**」）。此外，公署亦檢測了由一間知名的美國公司 Fitbit 製造、較受消費者歡迎的智能健身腕帶及其流動程式，以作比較。

5. 公署發現智能健身腕帶及其流動程式可能收集敏感的個人資料及對用戶構成私隱風險。不過，智能健身腕帶生產商並沒有向用戶提供足夠的私隱資訊，讓用戶評估私隱影響及採取措施保障其個人資料。

---

1 全球私隱執法機關網絡於2010年成立，旨在促進國際間的私隱執法合作。截至2016年7月31日，該網絡的成員包括來自47個管轄區的63個私隱執法機關。

2 來源：Gartner 的資訊科技詞彙，見 www.gartner.com/it-glossary/internet-of-things/

3 智能電視是可連接互聯網及具瀏覽功能的電視。智能電視除了像電腦般讓觀眾瀏覽互聯網外，還可播放網上的電視節目／電影、安裝及操作特別編寫的應用程式（資訊、社交媒體等）。

4 智能讀數錶可透過有線或無線技術遙距讀取資料，提供食水、電力及煤氣用量的詳細讀數（例如每分鐘的數據）及記錄用量。

5 穿戴式裝置是個人可穿戴以監察其身體活動或生理狀況的裝置（例如智能健身腕帶、血壓／心跳追蹤器）或作為其智能電話的延伸（例如智能手錶、類似 Google 眼鏡的裝置）。

6. 作為抽查行動的跟進行動，公署會向智能健身腕帶生產商提供相關建議，包括如何提高私隱資訊的透明度及更適當地處理個人資料，亦會提醒智能健身腕帶用戶在使用此類產品時如何保障其個人資料。

智能健身腕帶的操作

7. 智能健身腕帶是用戶配戴在手腕的電子感應器，用來追蹤日常活動（例如步行距離、消耗的卡路里、睡眠持續時間及質素），而有些更能夠讀取生理狀況指標，例如心跳率，甚至透過全球定位系統收集用戶的實際位置。一般而言，智能健身腕帶不能自行操作，而是需要連同支援的流動程式一起使用，智能健身腕帶可透過下述三個方式收集用戶的個人資料：

7.1. 用戶在登記帳戶時遞交（例如姓名、年齡、體重、身高）；
7.2. 在使用時由智能健身腕帶收集（例如步行距離、睡眠持續時間）；及
7.3. 支援的流動程式透過直接讀取用戶智能電話內的資料而收集（例如用戶的實際位置）。

抽查行動的目的

8. 公署留意到智能健身腕帶及類似的物聯網裝置在香港越來越普及。很多公司，包括初創企業，日後或會加入這個市場[6]。而透過參與抽查行動，公署旨在：

8.1. 探究智能健身腕帶及物聯網裝置普遍對私隱帶來的挑戰及影響；
8.2. 提高智能健身腕帶及物聯網裝置生產商的私隱意識，及鼓勵他們遵守《個人資料（私隱）條例》（「**條例**」）；

[6] 美國研究公司 Gartner, Inc 預測在 2016 年，全球發售的智能健身腕帶（Gartner, Inc.的報告中使用 “wristbands” 字眼）達 3,497 萬條，較 2015 年增加 16%。Gartner 亦預測，智能健身腕帶的銷售於 2017 年會快速增長，預期全球銷售量為 4,410 萬條，較 2016 年增加 26%。有關詳情請見 www.gartner.com/newsroom/id/3198018。

8.3. 教育智能健身腕帶及物聯網裝置的用戶如何保障其個人資料；

8.4. 識別日後進行私隱教育、推廣及執法的重點範疇；及

8.5. 與其他私隱執法機關分享公署的抽查結果，以促進跨境私隱執法及知識分享。

智能健身腕帶的甄選

9. 每個參與抽查行動的私隱執法機關可自行按其策略重點及管轄區的情況，而決定研究物聯網裝置的類型和數目。全球抽查行動的目的是評估物聯網裝置生產商如何向用戶傳達有關私隱的事宜。公署透過向智能健身腕帶生產商作出查詢，進一步探究他們在保障用戶個人資料方面所採取的保安措施。

10. 公署考慮到智能健身腕帶在香港越來越普及，於是決定以它作為檢測目標。另外，公署進一步把檢測範圍限於本地製造的智能健身腕帶，以便因抽查行動而衍生的任何跟進行動或建議亦可適用於本地生產商。

11. 智能健身腕帶一般能配合以 Android 及iOS 操作系統的智能電話一同運作。因此，它們相應的流動程式通常可在 Google Play 及 AppStore 程式商店中找到。

12. 公署使用下述策略找出及甄選本地製造的智能健身腕帶：

12.1. 由於智能健身腕帶需要配合其流動程式來操作，於是公署首先在 Google Play 程式商店下的「健康與健身」類別開始進行搜尋。公署檢測了這類別下超過 1,000 個流動程式，查看它們是否與智能健身腕帶有關；如是，有關腕帶是否由香港公司製造及在香港市場銷售；

12.2. 此外，公署亦通過下述網站搜尋智能健身腕帶，或與智能健身腕帶有關的生產商或其流動程式：

12.2.1. 香港一個有關消費性電子產品的格價網站；

12.2.2. 香港貿易發展局主辦的 2016 年香港春季電子產品展的網站及參展商名單；

12.2.3. 由政府資訊科技總監辦公室策動、香港無線科技商會主辦的香港資訊及通訊科技獎之流動程式獎；及

12.2.4. 網上搜尋潛在的生產商和智能健身腕帶。

13. 最後，公署找到並購買了五款本地製造的智能健身腕帶進行檢測。

14. 公署亦揀選了由一間知名的美國智能健身腕帶公司製造的智能健身腕帶進行檢測以作比較。

15. 被甄選的智能健身腕帶及其流動程式詳列於**附錄A**。

被甄選的智能健身腕帶及其流動程式的檢測方式

16. 公署於 2016 年 4 月 11 日至 6 月 16 日期間進行抽查行動。抽查行動以下述方式進行：

16.1. 購買被甄選的智能健身腕帶（五款本地及一款美國生產商的產品），並以Android 及 iOS 操作系統的智能電話試用並了解其功能及特點；

16.2. 閱讀智能健身腕帶在其產品包裝、其流動程式及／或生產商網站的私隱聲明及用戶指引，以回答一套預設的問題（詳情見第17段）；及

16.3. 按一套預設的問題向有關的生產商作查詢（詳情見第20段）。

17. 抽查行動的目的是評估生產商向用戶披露私隱訊息方面的表現。所有參與的私隱執法機關均利用以下由全球私隱執法機關網絡制定的預設問題來進行評估：

17.1. 智能健身腕帶有沒有私隱政策？如有，私隱政策是針對智能健身腕帶而設，抑或是一般性的私隱政策？

17.2. 私隱政策（如有）有沒有說明智能健身腕帶及其流動程式會收集哪些個人資料，以及收集目的？

17.3. 私隱政策（如有）有沒有說明用戶的個人資料可能會被轉移予甚麼人？

17.4. 用戶有沒有獲告知所收集的個人資料的儲存地點、儲存及傳輸資料的方法，以及保障資料所採取的保安措施？

17.5. 用戶有沒有被要求或提醒更改智能健身腕帶及其流動程式的預設私隱設定？

17.6. 用戶有沒有獲告知如何從智能健身腕帶及其流動程式刪除其個人資料？

17.7. 用戶有沒有獲提供智能健身腕帶生產商的聯絡資料，以便作出有關私隱事宜的查詢？

17.8. 智能健身腕帶生產商有沒有就公署的查詢提供適時及詳細的回應？

18. 全球私隱執法機關網絡為今次抽查行動而制定的問卷載列於**附錄B**。

19. 由於部分問題需要測試人員作主觀判斷，為確保評估的公平性，每款智能健身腕帶均會由兩名公署職員進行檢測。如兩名職員提交的結果有差異，雙方會進行討論及協調。而這項安排亦有助反映一般用戶的典型體驗。

20. 除了檢測智能健身腕帶、其流動程式及網站外，公署亦向裝置生產商作出書面及口頭查詢。公署提出的問題包括：

20.1. 智能健身腕帶及其流動程式收集了用戶甚麼個人資料？

20.2. 用戶的個人資料是否儲存於智能健身腕帶、連接的流動電話、生產商的伺服器或其他地方？

20.3. 用戶的個人資料在儲存時及在裝置之間傳輸時是否有加密處理？

20.4. 生產商會否與其他人士分享或轉移用戶的個人資料？

20.5. 用戶如何能從智能健身腕帶、其流動程式及生產商的伺服器刪除、提取及輸出其個人資料？

20.6. 生產商有沒有進行風險評估，以識別智能健身腕帶的潛在私隱風險？

21. 公署向全部六個生產商進行查詢，當中有四個本地生產商向公署提供部分回應。

22. 公署將五個本地的智能健身腕帶的檢測結果與美國的智能健身腕帶的檢測結果互相比較。並非所有檢測結果都有重要的發現，但如有，公署會在下文闡述。

全球抽查行動

23. 全球 25 個私隱執法機關檢測了 314 個物聯網裝置。裝置類型的分佈如下：

裝置類型	**檢測裝置的私隱執法機關數目** **（每個私隱執法機關可檢測多於一種裝置）**
醫療／健康物聯網裝置（例如血壓監控器、睡眠監控器）	11
健身穿戴裝置	10
家用輔助裝置	6
智能電視	2
智能讀數錶	2
行為計費保險裝置	1
聯網玩具	1
聯網汽車	1

24. 根據全球私隱執法機關網絡制定的預設問題，參與的私隱執法機關匯報了下述五個指標的結果：

24.1. 沒有向用戶解釋如何收集、使用及披露其個人資料的裝置數目；
24.2. 沒有向用戶解釋如何儲存由裝置收集的資料，以及如何保障資料免於外洩的裝置數目；
24.3. 沒有向用戶提供易於識別的聯絡資料以查詢有關私隱事宜的生產商數目；
24.4. 沒有解釋用戶可如何從裝置刪除其個人資料的裝置數目；及
24.5. 沒有就查詢提供適時、充分及清晰的回應的生產商數目。

抽查結果

25. 智能健身腕帶的固件、其流動程式和生產商的網站可能會不斷更新或改變。因此，本報告的抽查結果只能反映被甄選的智能健身腕帶、其流動程式及網站在 2016 年 4 月至 6 月抽查行動期間的狀況。

26. 此外，抽查行動只屬研究性質，而非循規審查或正式調查。因此，公署不適宜透露個別智能健身腕帶的具體抽查結果。下述的抽查結果因而是整體性的。

27. 就下述每個檢測項目，報告會先列出本地智能健身腕帶的檢測結果，隨後是美國智能健身腕帶的結果。此外，在適當情況下，本地智能健身腕帶的結果亦會與其餘 24 個私隱執法機關匯報的五個環球指標結果作比較。不過，讀者須留意，不是所有私隱執法機關都有檢測智能健身腕帶，因此公署是將本地智能健身腕帶與被檢測的全球各種物聯網裝置進行比較。

主要結果

私隱政策

28. 五個本地智能健身腕帶生產商中，只有兩個 (40%) 在其網站或支援的流動程式向用戶提供私隱政策。該兩份私隱政策中，只有一份 (20%) 是針對智能健身腕帶而設，而另一份只是關於生產商透過其網站收集資料的情況。

29. 只有為智能健身腕帶制定具體私隱政策的本地生產商有向用戶說明會收集甚麼類別的個人資料（例如電郵地址、出生日期、身高、體重）及收集目的。其餘四個本地生產商並沒有提供任何有關這方面的資料。

30. 相比之下，美國生產商有在其流動程式中向用戶提供針對智能健身腕帶而設的私隱政策。該美國生產商在其私隱政策中向用戶解釋它會收集甚麼類別的個人資料及收集目的。

31. 在全球檢測結果方面，大部分被檢測的物聯網裝置沒有向用戶提供特別編寫的私隱政策。它們傾向在私隱政策中提供可能收集的資料的例子，但沒有列明每項會確實收集的資料。

32. 有關私隱政策的檢測結果概要：

	五款本地 智能健身腕帶	**美國 智能健身腕帶**	**全球物聯網裝置 (314 個裝置／公司)**
提供私隱政策的裝置	2 (40%)	有	41% (有向用戶充分解釋如何收集、使用及披露其個人資料)
在私隱政策中提供有關收集甚麼類別資料的資訊	1 (20%)	有	

33. 欠缺透明度可能令用戶不能掌握資料收集的全貌。當用戶發現某項他不預期被收集的資料被收集了，他可能會感到託異。此外，用戶可能未能作出知情的選擇，從而購買可保障其私隱的智能健身腕帶。

在登記及使用流動程式期間收集個人資料

34. 在登記流動程式時，所有本地智能健身腕帶都會收集用戶某些個人資料，例如用戶的姓名、電話號碼、電郵地址、出生日期／年齡、體重及身高，當中有些是強制收集，有些是自願提供。不過，每款智能健身腕帶所收集的個人資料的類別及數量各有不同。例如，有些智能健身腕帶收集用戶的電話號碼及電郵地址，而有些則不收集此類資料。由此反映電話號碼及電郵地址對於智能健身腕帶的正常運作可能並非必需，因而不應被收集，或應讓用戶自行決定是否提供有關資料。

35. 在使用時，所有六款智能健身腕帶（包括美國智能健身腕帶）都會收集用戶的健康資料。所收集的資料可能包括卡路里攝取量、卡路里消耗量、心跳率、睡眠時間、睡眠期間的活動及步行距離等。由於智能健身腕帶的功能是監察用戶的活動及健康狀況，而這些資料與其功能直接相關，所以可能屬必需。

36. 支援的流動程式亦可以讀取用戶智能電話的資料及使用其功能，例如讀取位置資料、相片、文字訊息及社交媒體帳戶，控制智能電話的鏡頭等。同一款流動程式的 Android 及 iOS 版本在讀取資料的範圍方面亦可能會有差異。

37. 在iOS 操作系統的設計下，流動程式在讀取用戶於智能電話內的資料前，須取得用戶的同意。另一方面，使用 Android 操作系統的智能電話，流動程式只需在安裝前通知用戶，便可讀取電話內的資料。不過，如智能電話是使用 Android 6.0 或以上版本，用戶可在安裝後剔除程式的某些讀取權限。

38. 公署注意到，部分以 Android 系統操作的智能健身腕帶的程式以預設方式取得用戶智能電話的某些權限，但同樣的程式在 iOS 操作系統下卻沒有

要求取得有關權限。例如，以 Android 系統操作的一款本地智能健身腕帶的流動程式以預設方式取得讀取位置資料及控制智能電話鏡頭的權限。不過，當公署職員在 iOS 操作系統使用同一款流動程式及智能健身腕帶時，該程式並沒有要求這些讀取權限。這顯示部分智能健身腕帶生產商可能以預設方式取得過多權限，而這些權限對智能健身腕帶及其流動程式的正常運作並非必需的。

39. 在全球檢測結果方面，被檢測的物聯網裝置同樣向用戶收集不同類別的個人資料，包括姓名、電郵地址、出生日期／年齡、地址、電話號碼、體重、身高、醫療資料、位置資料、相片及裝置獨特識別碼，不論是強制收集或自願提供。與本地智能健身腕帶的檢測結果類似，其他地區的檢測人員都關注某些類別的資料是否必需，例如出生日期及位置資料。

40. 有關收集個人資料的檢測結果概要：

<table>
<tr><th></th><th>五款本地
智能健身腕帶</th><th>美國
智能健身腕帶</th><th>全球物聯網裝置
(314 個裝置／公司)</th></tr>
<tr><td>要求用戶在登記時提供個人資料</td><td>5
(100%)</td><td>有</td><td rowspan="2">有被收集的資料：
• 姓名 – 84%
• 電郵地址 – 83%
• 出生日期／年齡 – 64%
• 位置 – 68%
• 電話號碼 – 55%
• 相片／影像／音頻檔案 – 41%
• 裝置獨特識別碼 – 61%</td></tr>
<tr><td>在用戶使用智能電話時讀取資料及／或功能</td><td>5
(100%)</td><td>有</td></tr>
</table>

41. 值得注意的是，若生產商將在用戶登記時所收集的資料與在使用時所收集的資料結合，很多時不單能識別用戶的身份，亦可能取得用戶的私密資料，例如健康狀況、習慣及生活模式。生產商應減低收集資料的數量及儘量

收集私隱侵犯程度最低的資料（例如收集「用戶匿稱」以代替真實全名；收集年齡／出生年份以代替完整出生日期）。

42. 公署留意到一款智能健身腕帶只要求用戶自願提供一些為使智能健身腕能正常運作而必需的個人資料，例如姓名、性別、年齡、體重、身高及步幅。它的程式並無其他欄位要求用戶提交其他資料，例如電郵地址及電話號碼，從而避免收集了不必要的資料。這是「從設計保障私隱」[7]的良好例子，因為智能健身腕帶的用戶一般可能傾向儘量填滿在資料收集表格中的欄位。故此，要減少收集的資料，較為可取的做法是從表格中刪除不必要的資料收集欄位，而不是讓用戶自願決定是否在欄位中提供資料。

<u>轉移個人資料予第三者</u>

43. 只有兩款本地智能健身腕帶 (40%) 在其私隱政策中表明它們會向第三者（例如聯營公司、代理及夥伴）轉移用戶的個人資料，並解釋如此轉移資料的目的（例如向用戶提供服務），但沒有提及會轉移甚麼類別的資料。至於餘下三個本地智能健身腕帶 (60%)，則沒有提供這方面的資料。

44. 相比之下，美國生產商在其私隱政策中向用戶解釋它會向第三者（例如策略夥伴及服務供應商）轉移個人資料。它亦指明可能會在甚麼情況下轉移個人資料（例如履行訂單、遵循法規等）。不過，該美國生產商亦沒有提及會向第三者轉移甚麼類別的個人資料。

45. 全球的抽查結果未有提供有關這方面的數據。

[7] 「從設計保障私隱」(Privacy by Design) 的做法確保任何設計在一開始時便加入私隱的考慮。這做法可確保把保障私隱融入科技的設計、商業慣例及實體基礎設施。在系統落實前預測及評估私隱憂慮，並在私隱風險顯現前作出防範。

46. 有關轉移個人資料的透明度的檢測結果概要：

	五款本地 智能健身腕帶	**美國 智能健身腕帶**
披露資料承轉人：		
– 在私隱政策中	0 (0%)	有
– 回應公署的查詢時	2 (40%)	沒有回應
披露轉移予第三者的資料類別：		
– 在私隱政策中	0 (0%)	沒有
– 回應公署的查詢時	1 (20%)	沒有回應

47. 如用戶不獲告知所轉移資料的類別及潛在承轉人的類別，便不能就應該／可以把甚麼個人資料披露予智能健身腕帶生產商作出知情的決定。

<u>儲存個人資料</u>

48. 五款本地智能健身腕帶中，沒有任何智能健身腕帶 (0%) 在其私隱通訊中向用戶提供足夠的資訊，說明用戶的資料會儲存於甚麼地點，或會否聘用第三者儲存資料。

49. 公署透過向生產商作查詢，取得有關儲存用戶個人資料的進一步資訊。兩個 (40%) 本地生產商表示他們聘用第三者把資料分別儲存於中國內地及新加坡。其餘三個 (60%) 本地生產商沒有回覆或沒有充分回應公署的問題。

50. 相比之下，美國智能健身腕帶在其私隱政策中說明個人資料會儲存於美國，但沒有提及是否聘用第三者儲存資料。

51. 在全球檢測結果方面，大部分被檢測的物聯網裝置沒有在私隱政策中向用戶解釋如何儲存個人資料。即使有提及儲存資料，這些私隱政策很少向

用戶解釋儲存資料的地點、資料的保留時期及儲存資料的方式（例如在雲端儲存）。

52. 有關儲存個人資料的檢測結果概要：

	五款本地智能健身腕帶	**美國智能健身腕帶**	**全球物聯網裝置(314個裝置／公司)**
披露儲存資料的地點：			
– 在私隱政策中	0 (0%)	有 – 在美國	32%
– 回應公署的查詢時	2 (40%)	沒有回應	沒有相關數據
	五款本地智能健身腕帶	**美國智能健身腕帶**	**全球物聯網裝置(314個裝置／公司)**
披露由第三者儲存：			
– 在私隱政策中	0 (0%)	沒有 – 沒有披露相關資訊	32%
– 回應公署的查詢時	2 (40%)	沒有回應	沒有相關數據

<u>保障個人資料</u>

53. 五款本地智能健身腕帶中，沒有任何智能健身腕帶 (0%) 在其私隱通訊中向用戶提供足夠資訊，以說明資料會否在儲存及傳輸的過程中受到保障（例如透過加密方式）。只有 1 個本地智能健身腕帶 (20%) 在其私隱政策中承諾會使用保安措施保障用戶的個人資料，但沒有提供保安措施的詳情。

54. 公署透過向生產商作出查詢，取得有關保障用戶個人資料的進一步資訊。兩個 (40%) 本地生產商回應指他們沒有對被儲存及傳輸中的資料進行加密，但其中一個（即在私隱政策中承諾會使用保安措施的生產商）表示有用

其他方法保障個人資料（例如須以密碼登入流動程式）。另外，一個本地生產商 (20%) 表示會加密被儲存的資料，以及在智能電話與生產商的伺服器之間傳輸的資料。其餘兩個 (40%) 沒有回覆或沒有充分回應公署的問題。

55. 相比之下，美國生產商在其私隱政策中表示它使用「*防火牆*、*加密技術及認證程序的組合*」來保障用戶的個人資料。

56. 在全球檢測結果方面，51%被檢測的物聯網裝置有向用戶說明會如何保障他們的個人資料，及以甚麼措施來防止未獲授權的用戶查閱有關資料（例如密碼防護或認證問題）。與全球的標準相比，本地智能健身腕帶在這方面的透明度看來較低。

57. 有關保障個人資料的檢測結果概要：

	五款本地智能健身腕帶	**美國智能健身腕帶**	**全球物聯網裝置 (314個裝置／公司)**
承諾會保障收集的資料：			
– 在私隱政策中	1[8] (20%)	有	51%
– 回應公署的查詢時	1[9] (20%)	沒有回應	沒有相關數據
使用加密方式保障資料：			
– 在私隱政策中	0 (0%)	有	沒有相關數據
– 回應公署的查詢時	1 (20%)	沒有回應	沒有相關數據

58. 基於智能健身腕帶收集的個人資料的敏感性，用戶通常預期生產商提供較大的保障。此外，各管轄區對個人資料的法律保障亦有不同。因此，資

[8] 此生產商在回應公署查詢時重申有採取措施保障個人資料。

[9] 此生產商並無在其私隱政策中表明會保障資料。

料的儲存及保安欠缺透明度可能會削弱用戶選購裝置的信心。在香港這個私隱保障意識較高的地方，情況會更為顯著。

私隱影響評估

59. 公署以書面向智能健身腕帶生產商查詢他們有否進行任何私隱影響評估，以識別與智能健身腕帶有關的潛在私隱風險。只有一個 (20%) 本地生產商表示有進行評估，而另一個 (20%) 則表示日後會進行評估。其餘三個 (60%) 沒有回覆或沒有充分回應公署的問題。

60. 至於美國生產商，它沒有在其私隱政策提及私隱影響評估，亦沒有回應公署的查詢。

61. 全球的抽查結果未有提供有關這方面的數據。

62. 有關私隱影響評估的檢測結果概要：

	五款本地 智能健身腕帶	**美國 智能健身腕帶**
進行私隱影響評估	1 (20%)	沒有回應

63. 如欠缺私隱影響評估，生產商未必能有系統地識別其智能健身腕帶的私隱風險。因此，他們未必能實施足夠的保障私隱措施。

刪除個人資料

64. 在五個本地生產商中，沒有生產商 (0%) 告知用戶如何刪除智能健身腕帶及其流動程式所收集的個人資料。只有一個 (20%) 本地生產商在其私隱政策中向用戶提供電郵地址，讓用戶發送刪除資料的要求。另一個本地生產商在回應公署的查詢時，表示用戶可聯絡他們刪除儲存於腕帶、其流動程式及／或他們儲存的資料。餘下的本地生產商沒有向用戶提供刪除個人資料的方法，或沒有回應公署的問題。一般而言，用戶沒有獲提供方便的途徑以刪除個人資料。

65. 相比之下，美國智能健身腕帶在其網上用戶手冊表示，如智能健身腕帶被連接至另一帳戶，所有在腕帶內儲存的原有用戶個人資料便會被刪除。它亦在私隱政策中提供電郵地址，讓智能健身腕帶用戶提出刪除資料要求。

66. 在全球檢測結果方面，只有 28% 被檢測的物聯網裝置在其私隱政策中向用戶解釋如何從裝置／流動程式中刪除他們的個人資料。在某些情況下，刪除資料的過程是複雜的。全球檢測結果與本地的智能健身腕帶的檢測結果類似，用戶未獲提供足夠的有關資訊以刪除個人資料。

67. 有關刪除個人資料的檢測結果概要：

	五款本地 智能健身腕帶	**美國 智能健身腕帶**	**全球物聯網裝置 (314個裝置／公司)**
如何刪除所收集的資料的資訊：			
– 在私隱政策中	1 (20%)	有	28%
– 回應公署的查詢時	1[10] (20%)	沒有回應	沒有相關數據

68. 智能健身腕帶收集個人資料的主要目的是讓用戶了解自己的健康狀況，而不是供生產商使用。因此，用戶應有權控制其個人資料的保留及刪除。欠缺刪除資料的資訊會削弱用戶的權利。

<u>更改預設設定</u>

69. 在五個本地生產商中，沒有生產商 (0%) 提醒用戶檢查及更改智能健身腕帶及其流動程式的預設私隱設定。至於美國生產商在其私隱政策中有解釋，哪些類別的帳戶資料會預設為與公眾分享及與用戶的「朋友」分享。它亦告知用戶可隨時在其網站更改私隱設定。

[10] 回覆公署書面查詢並表示用戶可聯絡它們以刪除個人資料的智能健身腕帶，與在其私隱政策中提供電郵地址以供提交刪除資料要求的智能健身腕帶不同。

70. 全球的抽查結果未有提供有關這方面的數據。

71. 有關更改預設設定的檢測結果概要：

	五款本地 智能健身腕帶	**美國 智能健身腕帶**
在私隱政策中提示用戶更改有關私隱的預設設定	0 (0%)	有

72. 公署注意到在 Android 系統操作的流動程式可能以預設方式取得過多讀取智能電話資料的權限（見上文第38段）。有關程式亦可能會超乎用戶的預期地，向他的「朋友」或其他用戶披露他的個人資料。因此，用戶應檢查私隱設定，及取消不必要／不想要的讀取權限和資訊分享功能。

查詢私隱事宜的聯絡資料

73. 只有兩個 (40%) 本地生產商向用戶提供了聯絡資料（即電郵地址），以供他們查詢有關私隱的事宜。

74. 同樣地，美國生產商有向用戶提供電郵地址以查詢有關私隱的事宜。

75. 在全球檢測結果方面，62% 被檢測的物聯網裝置有向用戶提供聯絡資料，讓用戶可提出有關私隱的問題。與全球的標準相比，本地智能健身腕帶在這方面的透明度看來較低。

76. 有關聯絡資料的檢測結果概要：

	五款本地 智能健身腕帶	**美國 智能健身腕帶**	**全球物聯網裝置 (314 個裝置／公司)**
在私隱政策中向用戶提供聯絡資料以查詢有關私隱事宜	2 (40%)	有	62%

77. 若用戶未獲提供聯絡資料，便不能釐清有關私隱事宜及行使其查閱及改正資料的權利，這或會引致有關私隱方面的投訴及對公司的不滿，最後影響公司聲譽。

主要結果的概要

78. 整體而言，美國智能健身腕帶在向用戶提供私隱資訊方面的表現較本地智能健身腕帶為佳，原因如下：

78.1. 有提供度身訂造的私隱政策，解釋會收集甚麼類別的個人資料及收集目的；
78.2. 有解釋在甚麼情況下會把個人資料轉移予第三者；
78.3. 有解釋（雖然非常概括）保障個人資料的保安措施；
78.4. 有提供方法讓用戶刪除其個人資料；及
78.5. 有列明聯絡資料，讓用戶聯絡他們作出有關私隱的查詢。

79. 與全球的檢測結果相比，本地智能健身腕帶在某些方面的私隱資訊溝通表現似乎較遜色，例如就保障個人資料的措施的溝通，以及提供用作查詢私隱事宜的聯絡資料方面。不過，須注意的是，香港與全球抽查行動的比較結果未可必反映真實情況，因為香港的結果只代表智能健身腕帶的表現，而全球結果則代表不同種類的物聯網裝置的表現。

結論及建議

80. 智能健身腕帶可能收集用戶大量的敏感個人資料。若資料被濫用或外洩，會對用戶構成私隱風險。因此生產商應向用戶提供足夠資訊，提醒他們留意私隱風險。生產商亦應採取足夠的措施保障個人資料。然而，抽查行動揭示本地生產商提供的私隱及保安資訊並不足夠。

81. 為增加處理個人資料的透明度及保安，公署建議智能健身腕帶生產商應：

81.1. 以簡單語言向用戶提供私隱政策，及協助用戶輕易地在私隱政策中找出重要資料（例如把私隱政策分為不同部分及在每個部分加上標題）；

81.2. 清楚列明收集的個人資料的類別、收集目的、個人資料的潛在承轉人，以及為保障資料而採取的保安措施；

81.3. 採取「從設計保障私隱」的做法：減少資料的收集；在傳輸及儲存個人資料時採取足夠的保安措施；及為智能健身腕帶及其流動程式採取私隱侵犯程度最低的預設設定；

81.4. 若支援的流動程式會讀取智能手機內的資料，而這些資料與智能健身腕帶的主要目的並非直接有關（例如位置及聯絡人清單等），則應容許用戶拒絕提供；

81.5. 提供清晰的指示，讓用戶刪除他們在智能健身腕帶、智能電話及遠端儲存媒體（例如生產商的後端伺服器，及（如合適）與運動有關的社交網絡）內的個人資料；

81.6. 提供聯絡資料（例如聯絡人、電話號碼、電郵地址及辦公地址）讓用戶查詢有關私隱事宜，及向用戶提供適時回應以解決他們的私隱關注。

82. 智能健身腕帶的用戶亦有責任保障其個人資料私隱。公署建議用戶：

82.1. 在購買智能健身腕帶前了解它對個人資料私隱的影響，以及生產商與其支援的流動程式收集的個人資料的類別及程度、所收集的個人資料擬用於的用途及現有的保安措施；

82.2. 儘量使用假名進行帳戶登記；

82.3. 為智能健身腕帶設立專屬帳戶（例如專屬電郵帳戶），儘量避免把智能健身腕帶帳戶連結社交媒體帳戶；

82.4. 檢測智能健身腕帶及其流動程式的預設設定，儘量關閉不必要的功能（例如全球定位系統）；

82.5. 修補智能健身腕帶的固件及適時更新其流動程式，以提升保安程度；

82.6. 在棄置／轉售智能健身腕帶前，刪除內裏的資料。

83. 根據抽查行動的結果，公署發出了題為「保障、尊重個人資料 — 明智使用物聯網」[11]的圖鑑，提醒用戶在使用物聯網裝置時如何保障其個人資料私隱。

[11] 請參閱
https://www.pcpd.org.hk/tc_chi/resources_centre/publications/surveys/files/sweep2016_c.pdf

附錄 A – 被甄選的智能健身腕帶及其流動程式

智能健身腕帶	流動程式	生產商	流動程式的下載日期及版本	
			Android	**iOS**
本地智能健身腕帶				
innoBand-D	innoBand	3 N Half Limited	2016 年 4月12日 v.1.1.6	2016 年 4月13日 v.1.4.1
iHeHa Dao	HeHa	爽樂健康科技有限公司	2016年 4月11日 v.2.5.0	2016年 4月13日 v.2.5.0
Archon Touch Fitness Wristband	Archon	Millennium Pacific Concept Limited	2016年 4月27日 v.3.4.60	2016年 4月13日 v.3.1.62
Digicare ERI Fitness Activity Tracker	DigiCare	凱瑞信息技術有限公司	2016年 4月14日 v.1.7.4	2016年 4月13日 v.3.1.2
ELAH BT-009	MyWay Fit	立業電子有限公司	2016年 5月17日 v.3.3.60	2016年 5月17日 v.1.3.4
美國智能健身腕帶				
Fitbit Alta	Fitbit	Fitbit, Inc.	2016年 5月12日 v.2.24	2016年 5月12日 v.2.21.1(488)

附錄 B – 抽查行動的問卷

<table>
<tr><td>Basic info
Device type</td><td colspan="15">Wearable ☐ Health-related device ☐ Smart TV ☐ Appliance ☐ Smart meter ☐ Connected car ☐ Other ☐ Please state</td></tr>
<tr><td>Device/ company details</td><td colspan="3">Device name:</td><td colspan="3">Name of organisation:</td><td colspan="3">Sector:</td><td colspan="3">Relationship of org to device:</td><td colspan="3">Country of relevant company:</td></tr>
<tr><td>Collection, use & disclosure of data</td><td colspan="15">Does the website/app have a privacy policy? ☐Y ☐N
Do privacy communications indicate what personal information is collected by the device? ☐Y ☐N
Are privacy communications specific to the device? ☐Y ☐N
Do privacy communications state that personal information is disclosed to other companies and for what purpose?
☐Y ☐N ☐ Don’t know
If the company does share information with other companies, is the user told which companies? ☐Y ☐N ☐N/A
Are users told to change the default settings for the device? ☐Y ☐N
How do users consent to the collection of their personal data? ☐ Through literature ☐ On the device itself
☐ During registration ☐ Other ……. ☐ Don’t know</td></tr>
<tr><td rowspan="3">Information collected

Mandatory
Optional
Not Collected</td><td colspan="9">During registration</td><td colspan="6">During use</td></tr>
<tr><td>Name</td><td>User name</td><td>Address</td><td>Phone number</td><td>Email address</td><td>DOB/ age</td><td>Weight/ height</td><td>Medical details (e.g. diabetic)</td><td>Other (please state)</td><td>Location</td><td>Health/ Fitness info (e.g. heartrate)</td><td>Photo/ Video/ Audio file</td><td>Unique device ID</td><td>Other (please state)</td></tr>
<tr><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td><td>☐M
☐O
☐NC</td></tr>
<tr><td>Explanation for how info is used</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td><td>☐Y
☐N</td></tr>
<tr><td>Storage of information and safeguards</td><td colspan="15">Do privacy communications make reference to the storage of personal information collected by the device? ☐Y ☐N
Is personal information stored and/or transferred in an encrypted form? ☐Y ☐N ☐Don’t know
Do privacy communications mention the use of security safeguards to keep unauthorised users from accessing the device or data? (e.g. password protections or authentication questions?) ☐Y ☐N</td></tr>
</table>

Storage of information and safeguards	Is the data stored in the same country as the manufacturer/relevant data controller? ☐Y ☐N ☐Don't know Does the company use third parties to store data? ☐Y ☐N ☐Don't know (***If company is contacted directly***) Did the company conduct any risk assessment procedures to identify potential privacy risks associated with the device? ☐Y ☐N ☐Don't know				
Contact information	Do privacy communications include contact details to allow a user to contact the company about privacy related matters? ☐Y ☐N				
Deleting personal information	How many steps are required to delete personal information from the device? ..... Are deletion instructions clear and easy to follow? ☐Y ☐N ☐N/A If a user sells their device, does the company provide tools to help clear the device of personal data? ☐Y ☐N ☐Don't know If a user loses their device, are tools available to delete/remove personal data from the device (i.e. remote wiping)? ☐Y ☐N ☐Don't know				
OPTIONAL **DC response**	Did the data controller respond within the deadline? ☐Y ☐N Did the response address all questions? ☐Y ☐N Was the response clear and easy to understand? ☐Y ☐N				
INDICATOR Based on the above responses	1) Do privacy communications adequately explain how PI is **collected, used** and **disclosed**?	2) Are users fully informed about how personal information collected by the device is **stored** and are there **safeguards** to prevent loss of data?	3) Do privacy communications include **contact details** for individuals wanting to contact the company about a privacy-related matter?	4) Do privacy communications explain how a user can **delete** their information?	5) Did the data controller provide a **timely**, **adequate** and **clear** response?
RESPONSE Answer: Y or N (see advice below)					
Comments: Any positive observations identified during the Sweep (in relation to the communication of privacy information to customers) – whether related to the questions or not.			Any additional concerns identified during the Sweep – whether related to the questions or not.		