「物聯網」時代所帶來的「個人資訊」風險
—以台灣及中國的情況為例

將群法律事務所 袁鴻毅律師

一、物聯網的概念及具體運用情形

「物聯網(Internet of Things, IoT)」係由多個裝置相連而形成的網路，網路上的每一裝置上均裝設有微型感測晶片，微型晶片中包含無線射頻辨識(RFID)、感測器、無線通訊等電路，以使各裝置成為智慧裝置，並將散處各地的各式裝置和設施，透過各種無線和有線通訊網連結，實現溝通和對話(包括物與物的交流、物與人對話、以及人與人的對話)，以提供管理和服務功能。美國交通部預測，全球連網裝置數量將從 2014 年的 70 億台，到 2018 年擴張至 180 億台。根據網際網路資料中心 IDC 預估資料，2020 年亞太地區(不含日本)連網物品與設備的市場規模，將由 2500 億美元（約 7.83 兆台幣），成長到 5830 億美元（約 18.25 兆台幣）。因此，物聯網帶來龐大商機，台灣、中國廠商亦盡力投入此一領域的產品研發。

國際電信聯盟(international telecommunication union, ITU)於 2005 年的一份報告曾描繪「物聯網」時代的圖景：當司機出現操作失誤時汽車會自動報警；公文包會提醒主人忘帶了什麼東西；衣服會「告訴」洗衣機對顏色和水溫的要求等等。物聯網把新一代 IT 技術充分運用在各行各業之中，具體地說，就是把感應器嵌入和裝備到電網、鐵路、橋梁、隧道、公路、建築、供水系統、大壩、油氣管道等各種物體中，然後將「物聯網」與現有的互聯網整合起來，實現人類社會與物理系統的整合，在這個整合的網路當中，存在能力超級強大的中心電腦群，能夠對整合網路內的人員、機器、設備和基礎設施實施實時的管理和控制，在此基礎上，人類可以以更加精細和動態的方式管理生產

和生活，達到「智慧」狀態，提高資源利用率和生產力水平，改善人與自然間的關係。

凡是物聯網內的裝置，都包含感測器以偵測週遭環境中的資訊，再透過無線通訊電路將資訊傳遞出去。例如，穿戴式裝置可以偵測使用者的呼吸、心跳等生理資訊，並將此一資訊經由網路傳遞至中央伺服器。由於物聯網裝置能夠產生有用的資訊，以供裝置的管理及控制，因此物聯網裝置成為了「智慧」裝置，能夠依據外界的變動產生回應或修正本身的運行規則。

二、物聯網於「台灣」運作可能帶來的「個人資訊」風險

物聯網裝置蒐集資訊的性質，有可能違反台灣「個人資料保護法」的相關規定。「個人資料處理法」(下稱「個資法」)對於個人資料之「**蒐集、處理**或**利用**」，均有明確的限制規定，違反者需負損害賠償責任。因此，當物聯網裝置所蒐集之資訊係屬於「個人資料」之範疇，相關廠商必須小心謹慎，避免所開發的產品違反「個資法」的限制規定。以下對於物聯網產品有可能違反的個資法規定作一說明。

(一) 何種「個人資訊」物聯網裝置不得蒐集

有關蒐集資料的類別，個資法第 6 條規定「有關**醫療、基因、性生活、健康檢查及犯罪前科**之個人資料，**不得**蒐集、處理或利用」。因此，物聯網裝置必須避免蒐集或利用此類資訊。

(二) 物聯網裝置蒐集個資，應取得「書面同意」

個資法第 19 條規定，限於符合「法律明文規定、與當事人有**契約**或**類似契約**之關係、當事人**自行公開**或其他已合法公開之個人資料、經當事人**書面同意**、個人資料取自於一般可得之來源」等情況，非公務機關方可對蒐集個人資料，因此物聯網裝置若進行個資之蒐集，必須符合前述事由方為合法。舉例來說，若穿戴型裝置蒐集使用者的血壓或心跳等個人相關資訊，必須在說明書中載明使消費者知悉，並載明蒐集該等資訊之用途，最好能於販售時一併取得消費者所

出具的同意書。

(三) 物聯網裝置所蒐集之個資，應於「特定目的」範圍使用

個資法第 20 條規定，「非公務機關對個人資料之利用，應於**蒐集之特定目的必要範圍**內為之」。若物聯網裝置將所蒐集之資訊使用於非經當事人同意之用途，則有違反個資法第 20 條之虞。

(四) 物聯網裝置侵害個資，應負「損害賠償」之責

最後，若物聯網裝置侵害個資，則需依個資法第 29 條負損害賠償責任。因此，開發物聯網產品的廠商，若產品涉及蒐集或處理個人資訊，產品的營銷團隊必須於銷售過程中配合個資法取得消費者之同意，以避免違反個資法相關規定的疑慮。

三、物聯網於「中國」運作可能帶來的「個人資訊」風險

中國全國人民代表大會常務委員會於 2012 年 12 月 28 日通過「關於加強網路信息保護的決定」，內容係規範「網路服務提供者」關於「個人資料」之保護義務。物聯網裝置涉及網路服務之運作，且具有蒐集資訊的性質，物聯網服務的提供者有可能違反中國「關於加強網路信息保護的決定」的相關規定。「關於加強網路信息保護的決定」對於個人資料之「**收集**或**使用**」，均有明確的限制規定，違反者除需負民事損害賠償責任外，還會受吊銷許可證或者關閉網站等行政處分，構成犯罪者尚須受刑事處罰。因此，當物聯網裝置所蒐集之資訊係屬於「個人資料」之範疇，相關廠商必須小心謹慎，避免所開發的產品違反「關於加強網路信息保護的決定」的限制規定。以下對於物聯網產品有可能違反的相關規定作一說明。

(一) 收集、使用個人資訊之「目的、方式、範圍」應經被收集者同意

有關蒐集資料的類別，關於加強網路信息保護的決定第 2 條規定「網路服務提供者和其他企業事業單位在業務活動中收集、使用公民個人電子信息，應當遵循合法、正當、必要的原則，明示**收集、使用**

資訊的目的、方式和範圍，並經被收集者同意，不得違反法律、法規的規定和雙方的約定收集、使用資訊。」。因此，物聯網裝置若進行個資之蒐集，必須在說明書中載明收集資料的內容及用途，使消費者知悉，最好能於販售時一併取得消費者所出具的同意書。

(二) 不得「出售、洩露、非法向他人提供」個人資訊

關於加強網路信息保護的決定第 3 條、第 4 條分別規定，「網路服務提供者和其他企業事業單位及其工作人員對在業務活動中收集的公民個人電子信息必須嚴格保密，不得洩露、篡改、毀損，**不得出售或者非法向他人提供**」;「網路服務提供者和其他企業事業單位應當採取技術措施和其他必要措施，確保資訊安全，防止在業務活動中收集的公民個人電子信息洩露、毀損、丟失」。因此物聯網服務提供者對所蒐集之個人資料負有「保密義務」。

(三) 物聯網裝置侵害個資，需受「行政處罰」，並負「民事賠償責任」及「刑事責任」

最後，若物聯網裝置侵害個資，依加強網路信息保護的決定第 11 條，「對有違反本決定行為的，依法給予警告、罰款、沒收違法所得、吊銷許可證或者取消備案、關閉網站、禁止有關責任人員從事網路服務業務等處罰，記入社會信用檔案並予以公佈；構成違反治安管理行為的，依法給予治安管理處罰。構成犯罪的，依法追究刑事責任。侵害他人民事權益的，依法承擔民事責任」。因此，開發物聯網產品或提供物聯網服務的廠商，若產品涉及蒐集或處理個人資訊，產品的設計必須謹慎小心，以避免違反中國「加強網路信息保護的決定」的相關規定。