

保密到家：以智慧型手機 App 為例

／ 劉俊偉

只要有資訊設備，就會有資安風險。根據國家通訊傳播委員會行動通訊市場數據顯示，截至 2018 年底行動電話用戶數已達 2921 萬戶，智慧型手機已成為現代科技資訊之主流，人人甚至機不離手。然而，除了常見的手機病毒與木馬惡意程式外，使用者更易忽略手機內潛藏之危機——App 行動應用程式，對於此程式之資安管理尚在萌芽階段，並未能掌握風險。您可知當我們在享受便利時，惡質企業也同時在分享你的隱私？



行動應用程式潛存風險

一、App 行動應用程式資安檢測回顧

2017 年由行政院及所屬部會、機關設置的行動 App，共有 144 個潛藏高度資安風險。從清查結果顯示，其中被檢測出有 6 項資安弱點的政府 App 更高達 6 件。國發會當即通知相關機關於期限內完成改善，否則立即下架，以提升資安防護。另 2018 年行政院消保處抽測市面 15 款熱門應用 App 資安檢測，包括線上購物、線上支付、線上訂票及保險業類等，初測結果全數未通過，揭露出不論是政府或私人企業開發之 App 都存有不少的資安風險，顯示手機資安風暴正在成形。

二、手機品牌製造來源分析

中國大陸手機品牌在全球市占率持續提升，根據 IDC（國際數據資訊有限公司）發布 2018 年第 4 季調查報告顯示，全球智慧型手機出貨量統計為 3.7 億支。依全球手機出貨量來看，目前排名前 5 大的手機品牌，三星仍穩居第 1，市占率達 18.7%，居於榜首。蘋果排名第 2，市占率達 18.2%。原排名第 2 的中國大陸手機品牌華為，受美國打壓影響，市占率降為 16.1%。第 4、5 名，分別為 OPPO、小米，市占率為 7.8% 及 7.6%。綜觀整體數據，陸牌手機已透過低廉價格與豐富功能之特

使用者在下載 App 時，因注意以下事項：

1. 避免安裝來路不明或不需要的 App，只信任安裝來自可靠來源的行動應用程式。
2. 密切注意程式所請求的存取權，不隨意提供非必要隱私權限。
3. 將行動裝置的作業系統更新到最新版，因為更新版本通常也會對漏洞進行修正。
4. 注意 App 實際發揮的功能與請求授予權限項目是否相符。
5. 參考其他使用者的評論，判斷此應用程式的安全性及可用性。

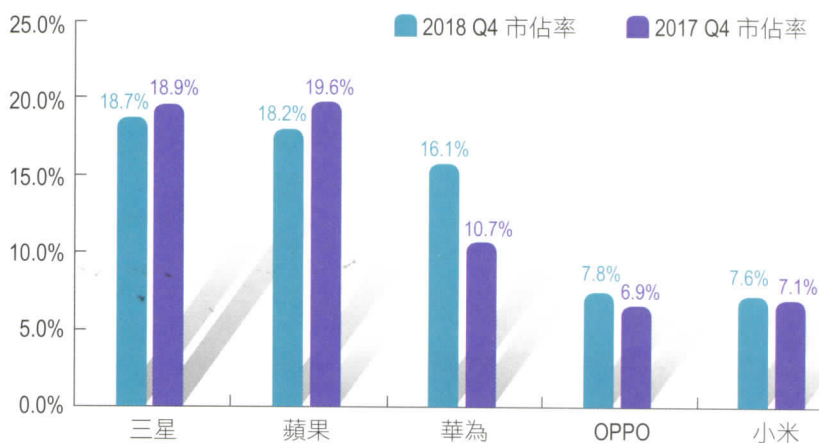
資料來源：行政院消保處

性，漸次拓展全球消費市場，且諸多款式均能支援「北斗衛星導航系統」。該系統於去（107）年5月上線，除可提供移動、即時定位和導航，進一步發展智慧城市、物流、自動駕駛等商用外，更透過系統功能性，進行各項情報之蒐集。因此，手機製造來源亦是造成國家資安威脅之一。

行動資訊服務應有認知與作為

一、周延法律規範與檢測

根據 106 年 7 月 28 日修正之《行政院及所屬各機關行動化服務發展作業原則》，為規範各機關提供之行動化服務應通過經



2018 第 4 季全球智慧型手機市占率統計，排名前 5 大的手機品牌為：三星、蘋果、華為、OPPO、小米。（資料來源：IDC 國際數據資訊有限公司）

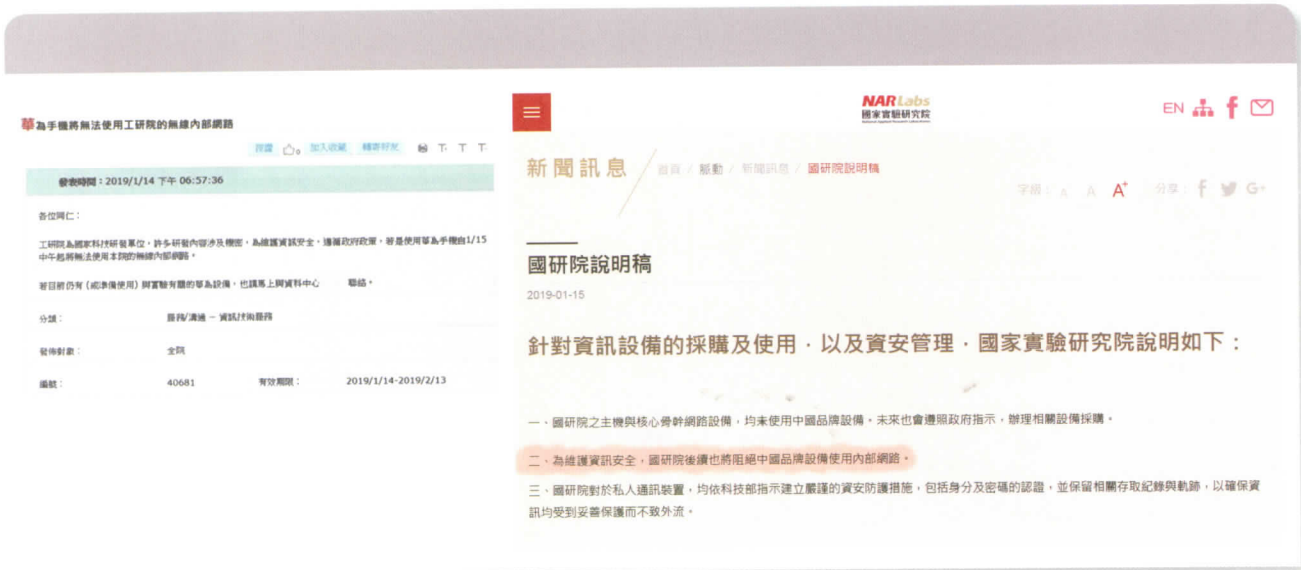
濟部工業局訂定之相關資安檢測規定：「各機關開發之行動化服務應符合個人資料保護法及行政院訂定之政府資通安全管理等相關規定，並通過經濟部工業局訂定行動化應用軟體之檢測項目，始得提供民眾下



華為手機是 2018 第 4 季全球手機出貨市占率第 3 名，而其餘如 OPPO、小米也分別名列第 4、5 名，顯示陸牌手機已透過低廉價格與豐富功能，逐漸拓展至全球消費市場。（Photo Credit: Kārlis Dambrāns, <https://www.flickr.com/photos/janitors/16103979223/in/album-72157650786478488>）



北斗衛星導航系統可提供移動、即時定位和導航，有利於各項情報之蒐集，去年 12 月中國衛星導航系統管理辦公室宣布開始提供「全球服務」。（圖片來源：中新社／達志影像）



工研院透過內部公告系統通知，1月15日起全體員工禁止使用華為手機、電腦等，國家實驗研究院後跟進公布訊息。（圖片來源：工研院，國家實驗研究院，<https://www.narlabs.org.tw/xmdoc/cont?sid=0J016316862277167493&xsmsid=01148622737263495777>）

載使用」。其次，為建立績效及資安檢測管考機制：「各機關發展行動化服務應建立績效管理機制，定期檢討服務成效。行政院所屬二級機關應於每年12月31日前彙整其所屬機關（構）之績效及資通安全檢測報告，送國家發展委員會進行管考」。基此，上揭所增列之官方 App 資安檢測規定，均必須經資安檢測通過後方能上架，同時，亦透過經濟部工業局將檢測服務納入共同供應採購契約，進而讓各個政府機關依需求採購 App 資安檢測服務，確保政府 App 資安防護健全。

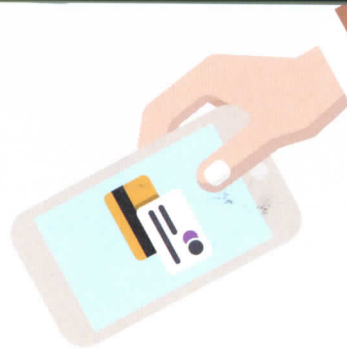
二、縝密手機來源管控

根據美國眾議院情報委員會（House Intelligence Committee）早在2012年便曾發表報告指出，建議美國企業不要採



國軍對大陸廠牌手機嚴格禁止帶入營區，並於採購契約中明定禁用；另對於其他廠牌智慧型手機，亦需加裝限制功能的軟體，維護資安。（圖片來源：截自東森新聞，<https://youtu.be/qfMkoSde1QA>；TVBS 新聞，<https://youtu.be/6csqXToZ6sw>）





用中國大陸業者華為（Huawei）和中興（ZTE）的設備與服務，也要求政府機構直接將華為與中興踢出採購名單。2014年時華為品牌即被禁止參與美國政府的競標案。對此，美國眾議院軍事委員會在去年5月公布2019年「國防授權法」（NDAA）法案細節，明確禁止任何美國政府機關使用華為或中興等大陸公司所生產的「高風險」科技產品。

鑑此，美國國防部亦在國家資安風險考量下，認定大陸政府可能會追蹤使用華為或中興通訊設備的美軍行蹤，例如獲悉軍事基地行動，或掌握軍隊何時在基地外集結，故要求軍中販賣部停止販售（或下架）華為、中興通訊兩家陸企製造的智慧型手機。我國軍方在採購方案中亦有明文規定，嚴禁使用中國廠牌的智慧型手機。

結語

智慧型手機的普及，雖大幅提升日常生活的便利性，但行動裝置卻因防護措施的不健全，已成為全世界政府頭痛的問題。丹麥 TV2 電視臺在 2015 年製作的紀錄片《手機不設防》（Addicted to My Phone），如實闡述了 App 所潛藏之危機與風險，數位世界正以前所未見的速度快速擴張，這意味著網路威脅與攻擊目標也正在各地迅速蔓延。美國總統川普於 2018

年底簽署《網路安全與基礎安全署》法案，將網路安全事務的管理拉高到聯邦層級。歐盟更於今（2019）年 2 月研擬禁用大陸 5G 設備，將修改網路安全法以因應即將鋪天蓋地的網路威脅。因此，智慧型手機的防護與檢測，對我國安而言，更是不容忽視之課題。



紀錄片《手機不設防》，揭露手機與 APP 所潛藏的資安風險及危機。（圖片來源：截自世界公視大展 youtube，<https://youtu.be/HnRsvhUuRgw>）