

保密到家：以智慧型手機 App 為例

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。

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。

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 MyPhone)，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。

(轉自清流雙月刊 108 年 3 月號)