



公務機密維護

運動手環APP洩漏你的行蹤

苗栗縣政府政風處
1月份公務機密維護宣導

資料來源：法務部調查局雙月刊2018年5月號
作者：陳姿陵

前言

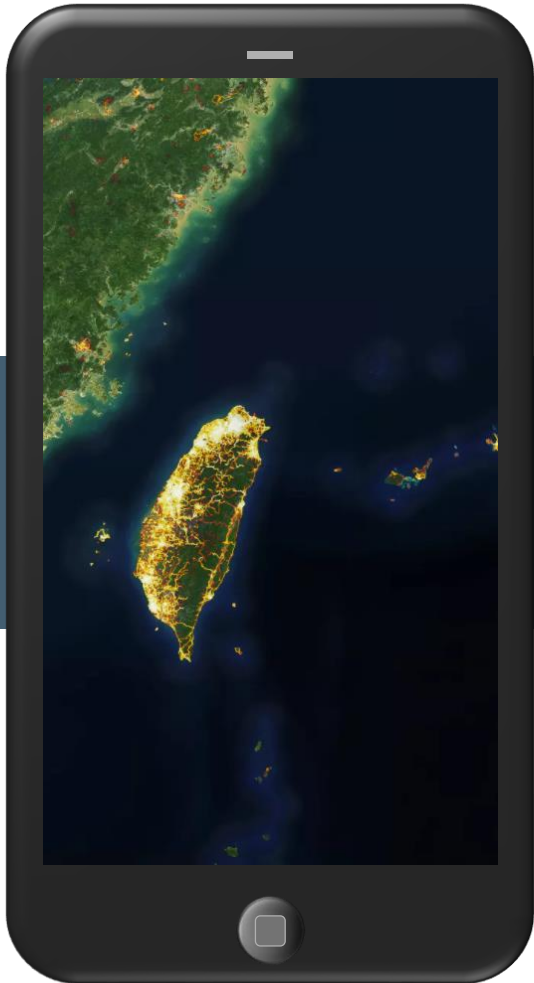


在運動風氣盛行下，美國GPS 定位公司Starva Labs 推出可使用於運動手環之智慧型APP 後，大受歡迎；該公司將過去2 年從全球用戶蒐集來的大數據，繪製成一份健身追蹤地圖（又名「全球熱圖（Global Heat Map）」）並於2017 年11 月間上網公布，其上顯示出全球超過十億條跑步和騎車健身路線，卻引爆各國秘密軍事基地被曝光的危機。





現今科技日新月異，「雲端」、「WIFI」與「APP」等技術或軟體相繼問世，現代人生活已離不開科技；隨處可見的個人電腦以及智慧型手機，在無線網路的進步下，其資訊傳播速度更有大幅度的躍進，例如：智慧型手機加上網路便是個人的GPS 定位系統；當透過Google Map 或其他地圖系統，便可使用衛星導航之功能；加上手機內建的相機鏡頭，便可隨時隨地上傳相片或影片，透過社群網站可與全世界朋友們分享生活點滴。然而在如此的便利的環境下，卻也暗藏了許多個人隱私遭侵入及國家機密遭窺視之危機。



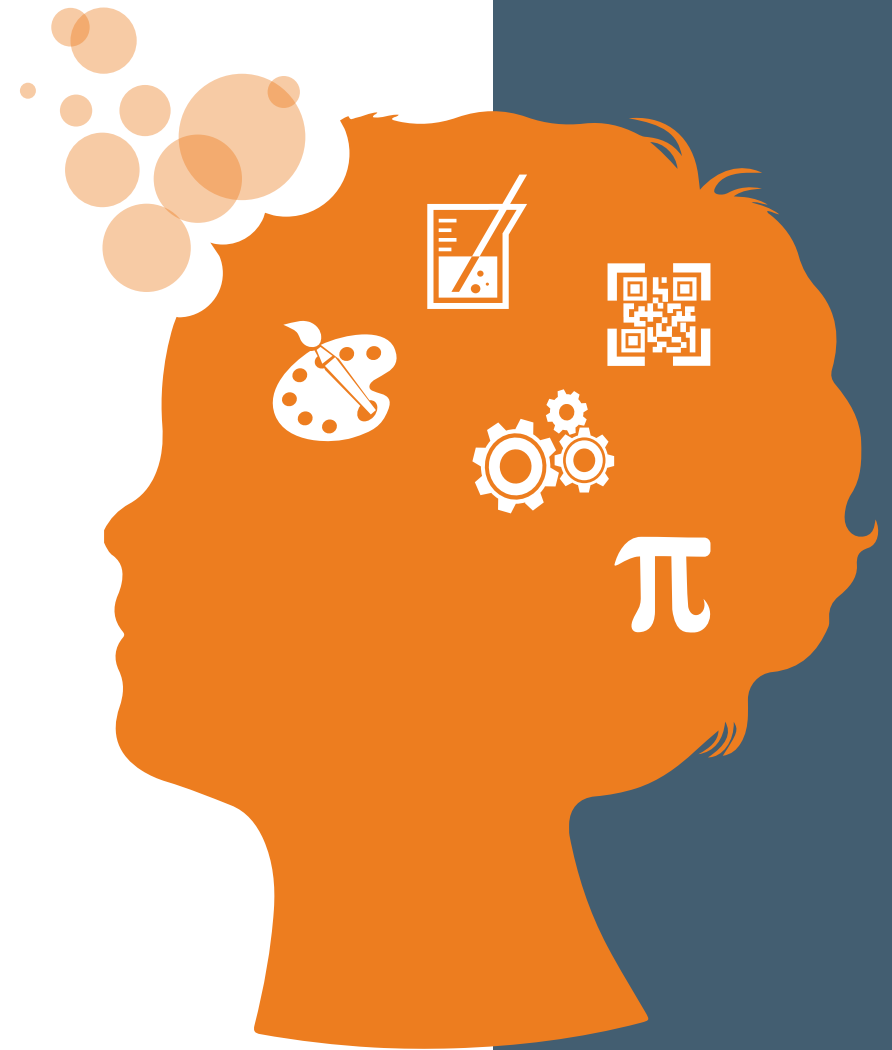
近期網友熱烈關注一款智慧型手機應用程式（APP），是由美國GPS 衛星定位追蹤公司Strava Labs 所推出，號稱「運動員的社群網路應用程式」，可呈現穿戴此電子產品的全球用戶騎單車、跑步、游泳、滑雪時行經的所有路線的地圖熱點。



光線越強的地方，代表在此地記錄跑步或騎單車的用戶越多，臺灣亦不乏熱中使用此款APP 的用戶。有位澳洲大學生魯瑟（Nathan Ruser），在研究「熱圖」公布的路徑後，意外發現在中東戰亂地區有部分光線很強，由於中東當地人會使用這種高科技運動手環的人應該很少，故推測「熱圖」已暴露了美國海外秘密的軍事基地；而依據「熱圖」所暴露全球各地敏感的軍事基地中，赫然發現臺灣某軍事基地在其中。

另依據媒體報導，美國國防部長馬提斯（Jim Mattis）在獲悉健身APP 洩漏軍隊機密消息後，開始考慮禁止士兵使用帶有GPS 定位手機入部隊的可能性。新加坡國防部更於Starva 軟體洩密曝光後，即刻於2018 年2 月2 日在國防部網站發布新聞，禁止軍人使用健身手環。新加坡此等效率頗值得我政府借鏡。

保密工作對個人及國家安全有著相當大的影響，無論平時或戰時均應落實執行管控措施，尤其負責國防安全之國軍弟兄更應留意。由於手機APP 或智慧手環有定位功能，國軍官兵進入營區需先關閉。在營外，用戶APP 內有可關閉上傳數據的功能，應瞭解相關隱私設定，以確保個人行蹤不會被洩漏。





除了前述APP 外，**來路不明的WIFI 連結**，極有可能隨時遭駭客入侵盜取資料及操控，而不明連結網址引誘點擊，易讓使用之行動電話遭歹徒入侵利用，致使個人資料遭竊取及偷拍。此外，在公共場所隨意使用商店提供**免費或未經加密認證的無線網路（WIFI）**進行金融交易、購買商品等動作，易使手機內的資料遭有心人士盜用，潛存被詐騙風險。



據統計，資安漏洞大都來自於人為的破壞與疏忽，故最有效的資安防護政策，就是個人養成良好的資安保密習慣。例如：落實實體隔離、機密資訊儲存使用加密軟體、不因吸引人的主旨標題而開啟來路不明的電子郵件、公務不家辦，唯有如此才能將資安風險降到最低。

在近年間駭客入侵國內外關鍵基礎設施事件增多、企業遭網路勒索病毒攻擊事件愈來愈頻繁，而且智慧型手機用戶不斷創新高的情況下，不論是政府為提高施政品質、企業追求營業額或個人享受科技便利之同時，對於資通安全更要提高警覺，以慎防秘密於無意間流出。



“



廉政專線：037-356639

苗栗縣政府政風處

關心您~

