線上社交網路之隱私

（作者：劉敏慧，行政院國家資通安全會報技術服務中心研究員）

當用戶使用線上社群網路（Online Social Networks, OSN）與同儕分享個人訊息時，每個用戶都可以啟用一些隱私的設定來管理存取權限。不過，即使用戶能夠設定自己主頁的隱私，駭客仍可經由用戶本身或朋友公開的管道進行入侵。2013 年 Securecomm 研討會中，來自美國的學者團隊發表一篇研究報告，探討用戶在 OSN 的隱私保護設定，以及非故意的隱私洩漏。他們蒐集超過三十萬個 Facebook 用戶的公開資訊，並評估其隱私設定；觀察的結果為：雖然大多數用戶都將自己的基本資料或好友列為隱私，但這些資料仍可經由公開資料而被揭露。

選擇 Facebook 作為研究目標，除了它是用戶最多的 OSN 之一，提供許多靈活的特性和資源；更重要的是，其隱私設定跟大多數現有的 OSN 採用的設定策略類似，但更為細密。在 Facebook 上，用戶可以設定每則訊息是否為公開，以及是給所有人、特定人或所有「朋友」。

當在蒐集資料時，研究團隊把自己當成一般用戶，既不屬於任何特定的團體，也沒有與任何樣本用戶有連接的設定；檢索到的資訊都設置為「公開」，亦即每一個正常的用戶都可以存取，因此，推斷實驗，可以由任何的其他用戶再複製。此外，由於研究團隊只蒐集公開資料，未打破 Facebook 的安全政策；基於對隱私的考量，用戶名和 ID 是使用匿名方式，將 30 萬個 Facebook 用戶的資料設定方式，有組織地變成資料庫，由 50 位研究生在同一機構以廣度為優先的方式進行資料蒐集。研究與統計結果為：有多達 37.8%的用戶會對陌生人隱藏自己的朋友列表，顯示用戶已意識到這部分與隱私是相關的；大約有 83.8%的用戶只會公開部分的、不完整的個人基本資料；只有 9.9%的用戶會公布完整的個人資料。這些統計數據顯示，有相當數量的用戶會注意自己的個人隱私，反映出隱私設定的有效性。研究團隊調查 OSN 的用戶，即使執行了隱私保護的設定，仍會在無意間洩漏隱私。研究團隊檢查用戶在 Facebook 不同 Section 所設定的隱私保護，然後對每個可能的隱私設定進行一些對應措施，嘗試可否從用戶的主頁與其他公開的資料或連結，發現隱私的洩漏；最後，將每個個別案例予以統計並量化。統計的結果可以推斷出，即使用戶有做隱私的設定，但若有一些小小疏漏，隱私資料仍會被揭露。攻擊者不需要太多的資源也能做跟研究團隊一樣的事情，因此，這些用戶的隱私可能很輕易就會被破壞。

Facebook 上的隱私問題早已引起廣大爭議，真正的問題是：我們應該放多少資料在網路上？有多少資料能提供給免費社群使用？最有爭議的也許是歐盟監管機構所建議的「被遺忘的權利」，讓用戶可以要求將他們的資料從網站資料庫中刪除。「被遺忘的權利」只能應用在用戶原本提供資訊的對象，很難對其他只是抓取公開資訊或製作索引的網站提出要求。而任何資訊一旦被公開發表之後，

就會被認為是公開的，是屬於網路的。這些爭議在短時間內不會有答案，用戶能做的就是減少放在社群媒體的資料，如果他們在意隱私的話。

要民眾注意這些資安或隱私問題並了解如何因應，大概也只能透過推廣或訓練，反覆不斷地灌輸正確觀念。已經盛行多年的電話詐騙，經由各界不斷的努力，製作宣傳短片於各大媒體強力播放，甚至在提款機上印製警示標語，轉帳按鍵在確認之前也會跳出提醒語句；即便如此，現在詐騙案件成功的比例雖有降低，但依然有人得逞。民眾在資安與隱私保護方面知識的不足，雖然政府注意到了，但仍缺乏政策性的規劃與落實，期盼未來能有更務實的推動方式以提升民眾的資安意識。

臺灣屏東地方法院檢察署關心您