專題企劃

社群網站與個人資料保護初探

臺灣臺北地方院檢察署檢察官 林冠佑

目　次

壹、緒論

電腦（Computer）及網際網路（Internet）的應用，發展至今，普及和應用的層面越來越廣，其中就電腦而言，因為電腦硬體設備的進步，使得電腦的元件在相同的面積下，可以放置或裝上更多的電晶體[1]，因此足可開發出更小、效能更強的電腦系統。甚或目前的所謂智慧型行動裝置，可以將大部分的電腦元件設置在體積微小的手持裝置之內；另一部份，網際網路的頻寬及連線速度飛快拓寬，費用也相對更加低廉之外[2]，以往僅負責語音通訊的電信服務業者，經由開發並使用俗稱2.5G的GPRS、3G的WCDMA、3.5G的HSDPA到3.75G的HSUPA，甚至現在演進到4G的WiMax和LTE等行動網路技術，可以提供使用者利用行動電話基地台連接網際網路。再搭配上ADSL實體線路配合短距離Wi-Fi技術，電腦和網際網路的發展，使人們已徹底擺脫PC（Personal Computer，桌上型電腦）及NB（NoteBook）不便移動的束縛，使用者可以隨時利用平版電腦、智慧型行動電話等行動裝置，隨時存取網路資源。如果再搭配上應用軟體及裝置內的定位、校準產品，應用性實然大大增加。

發展至今，智慧型行動裝置已然成為現今社會中重要的社會活動輔助產品，根據調查，至2011年6月為止，國內使用網際網路之人數已然達到2,577萬戶[3]，其中將近75%是利用行動網路上網，畢竟對消費者而言，住家縱然沒有申請或連接寬頻上網設備，但仍可能利用行動網路的方式取得網路資源，但是如果申辦了智慧型行動裝置，就必定要搭配行動網路技術，否則該行動裝置的功能就無法發揮。目前而言，智慧型行動裝置的OS[4]系統，以APPLE的iOS系

1　摩爾定律（Moore's Law），是由英特爾（Intel）創始人之一，戈登．摩爾（Gordon Moore）所提出之預測理論。內容為在相同尺寸的晶片上可容納的電晶體數目，約每隔12個月（此段時間或有更動或變異）便會增加一倍。該定律中的時間會隨著產業發展小幅更動，但主要是預見科技製程的進步快速。

2　至2011年12月止，臺灣地區一般個人用戶可申請的頻寬，以規模最大的ISP（Internet Service Provider，網路服務提供商）業者中華電信股份有限公司為例，提供的網路服務從較低廉的ADSL技術到以光纖為數據通信傳導載體的「光世代」服務，傳輸速度最慢的服務為下行512K、上行64K，而光世代的最高速率則可達下行100M、上行5M的速度。

3　資策會FIND網站，網址：http://www.find.org.tw/find/home.aspx?page=many&id=301，此部分含行動網路及家戶固定式設備，如XDSL、光纖、Cable等。

4　OS（Operating System），指電腦主機中負責管理軟硬體資源的基礎程式，如Windows、Linux。

統、NOKIA的Symbian系統和Google的Android系統囊括將近八成以上的市占率，而為了發揮行動裝置更多樣、更有效的功能，各個平台無不傾力發展各項應用程式，以不同程式搭配行動裝置定位或上網的功能，滿足各使用者的需求。

但不可諱言，越來越充實、存取越來越快速的網路資源，就需要使用者投注更多的「資源」，而在網際網路上大量流竄的資源中，很大多部分都是使用者的個人資料，網路上普遍的購物網站、電子金融商務等活動，已經將大量的個人資料送到網際網路的每次連線，在網路資訊的時代，資訊的內容就等同現金，2010年的網路攻擊目標多數皆為針對特定公司進行攻擊，以竊取資料，包括企業財務資訊、個人社交網站或網路銀行帳號，因為此些個人資料，都是駭客眼中相當有價值的資訊[5]。尤其在本文所談到的社群網站興起後，各式各樣不同的個人資料，更如江河入海般注入網路世界，在此狀況下，如果使用者還有著對於個人資料及隱私權的一絲想望，那個人如何兼顧，或應該如何督促相關政府部門重視、處理這日益嚴重的問題，在我國刑事訴訟中身為偵查主體的檢察機關，面對因此衍生的刑事案件，又應如何應對，實有探究之必要。

貳、社群網站的興起

人際關係的交流，原本就是人類生活中不可或缺的一環。紅白帖、明信片、聖誕或新年賀卡，甚至越洋電話的問候，在在就是牽起一條又一條，一張又一張人際關係的網。而網路的發展，甚至行動裝置上網的便利性，讓人們利用網際網路互相「即時」溝通，變得輕而易舉，也因此社群網站隨即應運而生。

從1996年以色列特拉維夫的Mirabilis公司開發出第一款即時通訊軟體ICQ開始，利用網路及軟體進行聯繫社交的機能，就已經展開。嗣後因應著網際網路頻寬和電腦硬體的成熟，除文字通訊外，語音或視訊通信都可以直接在電腦上完成，MSN、Skype或行動智慧裝置使用的Viber、LINE、WhatsApp等程式應運而生，但無論如何，此類利用軟體和「好友」或「聯絡人清單」進行通訊的方式，大多僅限於1對1的交流，如果要進行二人以上的通訊，通常必須增加數個步驟，並確認談話的對象，因此還是普遍歸屬於單點式的社交工具。但另一部份，因為網站撰寫及支援程式的進步，利用各種不同的設計軟體，可以將表單、視訊、音樂、動態圖片、互動式影片甚至是其他網站的服務嵌入到自己設計的網頁中，而因為現在的網路使用者已經大多可以利用行動裝置連接網際網路，頻寬和網路速度也已達到足可隨時存取網路資源而無遲延的地步，因此近年來，大量社群網站的發展以及使用人數的遽增，是網際網路的顯著現象。

所謂社群網站（Social Networking Sites），並無一定的定義和範圍。不久之前的部落格，可以讓使用者在網路上記事、分享心情和照片、影片等，已為社群網站之濫觴，但與前揭的即時通訊軟體相同，畢竟仍不脫於單點式的接觸，而以目前的網路現狀及科技發展而言，網際網路的功能足以承擔更為繁重的聯繫任務，因此現在的社群網站，除了專注於個人動態記事、聯絡人資料整理、影音視訊分享之外，還能以「社群」之方式，將使用者即時發佈的訊息或活動，「推播」[6]至所有社群或預設社群可得接收的位置，以達到社交的功能。但就廣義的社群網站而言，只要能達到社交、分享的目的，就可以大略含括

5 Symantec Internet Security Threat Report，2011年4月。

6 推播（PUSH），指網站將最新的訊息或資源自動傳送至使用者的裝置內，無庸手動更新。

其中。在2011年12月的統計資料中顯示，美國地區的上網人口中，有9.31%的使用者會拜訪（Visited）[7]Facebook[8]，而在各大網站流量的統計數據中，也可大略顯示目前全世界的網站流量中，Facebook的網站拜訪率均名列前茅，而在前十大的社群網站中，Facebook更是以超過半數的63.6%的拜訪次數領先群雄[9]。

社群網站的存在目的，就使用者而言，是利用網站和好友、朋友進行分享、聯繫，但就網站經營者而言，唯一的目的就是營利，但有趣的是，到本文寫作時的2011年12月間，全世界較為普及，為大多數人所利用的社群網站，例如Facebook、Google+、Youtube、Twitter、MySpace等，都是免費的。為什麼這些網站要如此麼佛心，花費眾多人力、物力，不停的撰寫、改進程式；建設電腦機房（或租用雲端設備），保持頻寬連線和系統穩定，以供全世界的人進行分享和聯繫呢？又一個不收費的網站如何營利呢？此部分雖然屬於社群網站的商業經營模式，但是因為和個人資料息息相關，因此仍有說明之必要。

其實目前網際網路上大部分的免費網站所賴以維生的收入，除了捐款之外，就是廣告。社群網站也不例外，以Facebook為例，在Facebook的營收中，主要比例來自於廣告和虛擬貨幣[10]。據市調公司eMarketer估計，Facebook今年的營收可能突破42.7億美元，較去年的營收18.6億美元相較，成長驚人[11]。在這42.7億的營收中，估計廣告佔大約90%，其餘的營收，則來自於虛擬貨幣。在Facebook網站中，實際上可以使用的虛擬貨幣不少，除了Facebook官方所設計的F幣外，還有各個第三方公司所設計，使用在各自開發的應用程式之中，例如Playfish公司的魚幣，Zynga公司也有所謂的Cash幣可以購買，但除了F幣之外，均只能使用在各自開發的遊戲之中。但無論此些社群網站如何經營，為了達到擴大廣告營收，並完成使用者的交流目的，社群網站必須持續蒐集個人資料，但相對而來的個人資料保護問題，一直是一個使用上的隱憂，而在我國法制上如何因應，政府與使用者是否已經做好準備，亦有討論之必要。

最末，本文在討論社群網站的個人資料問題時，因為以目前現狀而言，Facebook的使用者人數最多，網站功能也較為多元，因此在討論個人資料內容和隱私權保護制度時，將大部分以Facebook網站作為討論之對象，以凸顯問題之所在。

參、我國個人資料保護規範

我國對於個人資料保護的出發點，應屬民國84年（1995年）訂定的「電腦處理個人資料保護法」，當時是感念於個人資料如經由電腦大量處理，如未加以控管，遭濫用後恐生危害情事，因此立法加以規範。但是在隔年公佈的「電腦處理個人資料保護法施行細則」，卻僅明訂「徵信業、電信業、醫院、學校、金融業、證券業、保險業、大眾傳播業」等八大行業必須適用個人資料保護法，而且以條文名稱

7 意指使用者瀏覽該網站之意，該數字是受調查使用者瀏覽網站次數之百分比，亦即100次的瀏覽活動中，有9.31次是拜訪Facebook。

8 原指美國學校發給新生的手冊，裡面會載有新加入成員的通訊資料，原意協助新生融入環境。但經Facebook創辦人Mark Zuckerberg引為社群網站之名稱。

9 參閱Hitwise United States，Top Ten Websites，網址：http://www.hitwise.com/us/datacenter/main/dashboard-10133.html，最後檢索日：2011年12月26日。

10 與流通貨幣不同，虛擬貨幣係在網際網路環境中使用之電磁記錄「點數」，通常可以流通貨幣購得，依設計之不同，亦得在會員帳號間轉讓。

11 聯合新聞網，網址http://mag.udn.com/mag/digital/storypage.jsp?f_ART_ID=343825，最後檢索日：2011年12月25日。

亦可知，此份法案保護的客體僅限於以電腦處理之個人資料，因此適用的範圍非常狹隘。匆匆數年過後，網際網路的發展，促成網路活動的多樣性和便利性，大量的個人資料俯拾皆是，再以單純限於八大行業方得以適用的個人資料保護法規，顯然不足以應付社會需求，因此新修訂的「個人資料保護法」，已於99年（2010年）4月27日通過立法院三讀程序，並於同年5月26日經總統公布[12]。

新修訂的個人資料保護法，適用主體和客體均有重大的改變。其中主體部分包括公務機關與非公務機關。依個人資料保護法第2條第1項第7款：「公務機關：係指依法行使公權力之中央或地方機關或行政法人」；第8款：「非公務機關：係指前述以外之自然人、法人或其他團體」之規範，已經斷然刪除非公務機關行業別之限制。而另一個重點在於，新修訂的個人資料保護法更是將規範的客體規範，改為單純的個人資料即受保護，而不再限於以電腦處理者，適用程度因此擴大，以因應日漸擴大的社交生活。

一、個人資料定義與內容

個人資料保護法第2條第1項第1款規定，個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。實際上實在是因為因社會態樣複雜，有些資料雖不是直接以姓名、國民身分證統一編號等直接辨識個人，但是如果一旦揭露，如仍得以識別為某一特定人，對個人隱私仍會造成侵害，爰參考一九九五年歐盟資料保護指令（95/46/EC），將「其他足資識別該個人之資料」修正為「其他得以直接或間接方式識別該個人之資料」[13]。

另外，我國新修正之個人資料保護法更將個人資料的部分內容，定義為所謂「敏感性資料」，依個人資料保護法第6條規定，敏感性資料係指「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料」。新法之所以做如此之修正，是因為此類資料的內容，大多攸關個人的重要隱私，如果遭受侵害，通常會帶來比較嚴重的侵害結果，而且遭受侵害後也通常難以回復，因此除有法律明文規定外，科以公務機關或非公務機關等蒐集機關較重的法定義務，除當事人自行公開等情形外，原則上此類資料不得任意蒐集、處理及利用[14]。此外，為了符合社會一般生活之常情，個人資料保護法第51條規定，如係一般人單純為個人或家庭活動目的及在公開場合或活動所得之未與其他個人資料結合的影音資料外，並不適用個人資料保護法。因此，個人行動電話中的聯絡人清單、通訊錄等，或是因旅遊或紀念等目的而在公開場所的攝影或錄影，即非個人資料保護法所規範的個人資料[15]。

二、個人資料的法律規範

新修訂之個人資料保護法除了擴大個人資料之範疇外，另外對於個人資料之蒐集、利用或處理，也做了詳盡的規範，茲簡要說明如下：

㈠當事人之權利：

個人資料保護法第3條規定，當事人得就其資料為1.查詢或請求閱覽；2.請求製給複製本；

12 依個人資料保護法第55條、第56項第1條，施行細則及施行日期分別由法務部及行政院定之，但迄至100年12月，仍尚未公佈施行日期，亦未公佈施行細則。

13 參見個人資料保護法第3條修法說明第三點。

14 參見個人資料保護法第6條修法說明第二點。

15 此處可探討的是，某些非公務機關，如微信社、媒體等為了執行業務，而針對追蹤對象所拍攝的影片或照片，因為明顯不是屬於個人或家庭活動目的，而如果配合上車牌號碼、姓名等與個人連結之資訊，是否也屬於個人資料之範疇，殊堪玩味。

3.請求補充或更正；4.請求停止蒐集、處理或利用；5.請求刪除。

㈡蒐集機關之義務：

1.特定目的：

對於個人資料之蒐集或處理，除敏感性資料應依第6條之規定，原則上不得蒐集外，應有其特定目的，並符合下列法定情形之一：⑴執行法定職務必要範圍內；⑵經當事人書面同意：⑶對當事人權益無侵害。

另外，於蒐集處理後之利用，原則上須與蒐集之特定目的相符，並在法定的必要範圍內為之，僅於法定之例外情形，始得為特定目的外之利用。其情形包含：⑴法律明文規定；⑵為維護國家安全或增進公共利益；⑶為免除當事人之生命、身體、自由、財產之危險；⑷防止他人權益之重大危害；⑸公務機關或學術研究機構基於公共利益，為統計或學術研究之目的而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從辨識特定之當事人；⑹有利於當事人權益；⑺經當事人書面同意。

2.告知義務：

公務機關或非公務機關在蒐集資料時，應踐行告知義務。依同法第8、9條之規定，其內容應明確告知當事人蒐集機關名稱、蒐集目的、個人資料類別、利用期間、地區、對象、方法等相關事項，如係間接取得者，尚需告知當事人其資料來源及前揭事項。如係以書面同意為蒐集個人資料之依據者，還必須先行完成告知義務。

3.正確義務：

依本法第11條規定，蒐集資料之機關負有維護個人資料正確性之義務，應主動或依當事人之請求更正或補充，並於法定期限內通知資料當事人。當個資正確性有爭議時，除取得當事人同意或執行職務所必須外，原則上須立即停止處理或利用。

4.保管義務：

同法第18條、第27條第1項規定，機關保有個人資料者，應指定專人維護資料安全，以防止個人資料被竊取、竄改、滅失、毀損或洩漏。

5.利用限制：

非公務機關利用蒐集之個人資料行銷時，須於首次利用時，提供當事人表示拒絕接受行銷的方式，如當事人表示拒絕接受行銷時，應立即停止利用其個人資料。如不停止利用者，依本法第48條之規定，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣2萬元以上20萬元以下之罰鍰。

在跨境傳輸部分，非公務機關進行國際傳輸時，如⑴涉及國家重大利益；⑵國際條約或協定有特別規定；⑶接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞；⑷以迂迴方法向第三國（地區）傳輸個人資料規避本法者，新法第21條規定中央目的事業主管機關得限制之。

6.行政檢查：

鑑於非公務機關對個人資料之管理，不一定如公務機關般有上級機關定期監督、管理，故新法訂有行政檢查制度，賦予事業主管機關有命令、檢查及處分權，得派員攜帶執行職務證明文件，進入檢查，得命相關人員為必要之說明、配合措施或提供相關證明資料，檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。非公務機關及其相關人員不得規避、妨礙或拒絕。

㈢損害賠償及團體訴訟：

新的個人資料保護法加重了蒐集機關的注意義務，新法第28、29條規定，機關如違反本法之規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。而在民事的注意義務部分，公務機關採「無過失責任」，只要公務機關有違反本法之規定致生損害於當事人者，即須負賠償責任；非公務機關則採「舉證責任倒置」之過失責

任，必須由非公務機關舉證證明其無故意或過失者，才不需負損害賠償責任。

至於賠償責任內容，如係非財產上之損害，得請求慰撫金；名譽受損時，亦得請求為回復名譽之處分。當事人如能證明其損害自得請求賠償，惟為避免損害賠償範圍難以舉證證明之，故新法對於不易舉證之情形，有固定之賠償範圍，以每人每一事件新臺幣500元以上2萬元以下計算之。對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣2億元為限。但因該原因事實所涉利益超過新臺幣2億元者，以該所涉利益為限。同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受每人每一事件最低賠償金額新臺幣500元之限制。

另新法第33至40條亦增訂團體訴訟之規定，對於同一原因事實而生之多起個資法侵害事件，當事人得授予財團法人或公益社團法人訴訟實施權，由該法人向侵權者提起訴訟。

㈣刑事責任：

新法第41、42條規定違反第6條第1項（不得蒐集、處理敏感性資料）、第15條（公務機關對於個人資料之蒐集、處理應有特定目的並有法定情形）、第16條（公務機關對於個人資料之處理應與蒐集之目的相符）、第19條（非公務機關對於個人資料之蒐集、處理應有特定目的並有法定情形）、第20條第1項規定（非公務機關對於個人資料之處理應與蒐集之目的相符），或中央目的事業主管機關依第21條限制國際傳輸之命令或處分，足生損害於他人者，處2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金。如有意圖營利之特殊主觀要素，而非法變更、刪除個人資料檔案，致妨害個人資料檔案之正確而足生損害於他人者，處5年以下有期徒刑、拘役或科或併科新臺幣100萬元以下罰金。

整體而言，新修訂的個人資料保護法將保護客體擴大到所有個人資料；加重了蒐集機關的蒐集、處理、利用、傳輸義務；並賦予當事人更多控制個人資料，要求更正或停止利用、刪除之權利；以行政檢查和民、刑事處罰之手段，督使蒐集機關重視並注意個人資料之保全，但是否能夠落實執行，還需要後續的觀察。

三、社群網站的個人資料

社群網站的概念雖然發展已久，但是趨於完備（或造成個人資料危害）則是近幾年的事。社群網站的存在目的，既然是為了幫助使用者進行社交聯誼，那麼想當然的，就必須讓使用者在網站上建立自己的人際關係網絡，而為了更加精準的達到前述目的，通常社群網站會要求使用者提供相當數量的個人資料，以供進行比對和查找。以目前最多人使用的Facebook為例，Facebook可以說是在這兩至三年內崛起最為快速，也是對個人資料保護危害最烈的社群網站。Facebook竄起的原因，主要在於Facebook的切入點和經營策略在一開始就獲得使用者和廣告商的青睞，Facebook開始營運時，搜尋引擎的戰爭了無新意，Google也沒有推出其他殺手級的服務，而如Twitter、Plurk、MSN、Youtube等社群網站，不是停留在單點式的聯繫，就是專注於微網誌的發展，對於社交活動總是少了那麼一點交流的動力，網路使用者對於上網只能搜尋和購物，業已感到無趣，此時Facebook提供了一個全面性的網站內容，讓使用者得以更加善用網路通信功能進行交流。而Facebook的吸引會員方式，首要在使用者在登入後，必須先提供姓名、年籍、居住城市、電子郵件、電話號碼、婚姻狀態、興趣、工作經歷等個人資料，經過Facebook與資料庫內現存的會員資料比對後，會先協助使用者建立基本的「好友」列表。嗣後Facebook會不停蒐集使用者的網頁活動，並依據好友清單和會員的增加，找出共同認識之友人，再持續推薦使用者點選加入清單，以隨時擴大使用者的交友圈。另一方面，Facebook也利用由第

三方軟體公司[16]在網站上提供的網頁遊戲，經由使用者授權該第三方軟體公司存取相關聯絡人資料後，可以利用該遊戲與好友列表上的朋友進行遊戲內的互動，無形之間增加了使用者對於Facebook的「黏性」[17]，也大大促進了社交的功能，因此會員人數激增，網站拜訪率也居高不下。此外，Facebook除了要求使用者提交個人資料外，還非常注重個人資料的準確性，要求註冊會員須以本名註冊[18]，並大量封鎖對知名人物冒名申請的帳號，因此在Facebook上所找到或推薦的「好友」通常就會是你正在尋找，或久未聯繫的那一位。因此，Facebook從2004年2月開站開始，到2011年12月本文寫作時使用者人數已達到7億9千多萬人[19]，這套作法，讓急於累積會員人數的Google+也不得不按表操課，從眾多系統程式推薦的聯絡人圖像中，逐一拖曳到友誼圈內加入，已然成為Google+操作上的特色。

但是社群網站的個人資料問題，並不光在於個人資料的提交。使用者持續的利用社群網站的功能與好友聯繫，並一方面留下所有的個人生活足跡，諸如去過的景點、定位的位置、感興趣的議題、分享的新聞、參與的應用程式、上傳的照片、影像、不斷增加的聯絡人清單和通訊資料等等，均不斷充實社群網站的資料。這些資料雖然有時候以單項來說，並不足以辨識個人，但只要數量較多，經過比對後仍有識別特定人之可能[20]，仍不宜輕易排除在個人資料之範疇之外。此外，社群網站於取得該些資料，並將該些資料和個人資料進行分析後，可以取得，洞悉使用者的消費習性，生活習慣、需求等，並針對使用者的消費習慣，將適當的廣告傳送至該名使用者的螢幕，顯然亦具有一定之經濟價值。因此，此種持續監控、記錄之作法雖然對於社群網站的營收有莫大助益，但是是否符合我國個人資料保護法之規範，實有疑問。

肆、個人資料的安危

網際網路普及後，因為網路的介質和協定設計，讓所有的電腦彼此之間可以傳輸資料，從而，在電腦內包含各式各樣內容的電磁紀錄，在一定的條件下，都可以從遠端進行存取。本文所討論的個人資料，如果經過分析和歸類，可以作為商業經營或廣告行銷的有利武器，更遑論利用個人資料之內容如涉及購物歷程、信用卡資料等經濟活動，更可作為遂行詐騙犯罪之資料，在在彰顯個人資料的價值。因此，擁有眾多個人資料的社群網站，當然也必須面對資訊安全危害的威脅。

現在的資訊安全問題，不是擁有超高運算效能電腦的，或懂得利用軟硬體破解電腦網路程式或設備的「駭客」[21]，也不是那些國、高中就自學而擁有電腦軟體程式設計能力，能獨立撰寫出病毒（Virus）[22]的「天才」，所造成

16 在Facebook與使用者簽訂合約後，契約存在於雙方之間。但Facebook容由第三人在Facebook網站上提供服務，如經使用者授權，亦得存取使用者相關個人資料，稱為第三方軟體公司。

17 所謂黏性，係指使用者對於該網站的依賴程度。

18 臉書實名制，如經官方認為並非實際名稱或非本人，註冊帳號將強制關閉，要回復必須向官方申訴。相關實際案例請參考「臉書推實名運動，藝人伍佰也遭殃」，今日新聞網，網址http://www.nownews.com/2011/01/16/327-2682441.htm，最後檢索日：2011年12月25日。

19 參閱Facebook Marketing Statistics, Demographics, Reports, and News – CheckFacebook，網址http://www.checkfacebook.com/，最後檢索日：2011年12月25日。

20 否則，Facebook就無法推薦你可能認識的朋友清單給你了。

21 駭客（Hacker）係指對某領域程式語言有足夠了解，可以快速編寫出有用軟體，並樂在其中的人。駭客的電腦編譯技巧高明，對電腦組成的軟硬體架構亦瞭如指掌，但不一定會從事破壞性的動作。而所謂怪客（Cracker），則指擁有駭客技巧，但是卻熱衷於破壞他人電腦權限、電磁記錄以毀損系統或檔案，危害資訊安全的人。

22 參閱下文。

的損害也不全是讓發電廠停止運作或是取得某份國家尖端武器的設計圖。任何一位行為人，只要經由些許的步驟或心理戰術，利用簡單的電腦程式，就足以破壞資安狀態。而對於社群網站而言，大量的個人資料充斥其中，實令人不得不深究其中帶來的資訊安全危害。

一、內部威脅——網站經營者

社群網站的使用者將個人資料提交後，首要面對的是網站經營者對於個人資料的威脅。在社群網站興起前，網際網路使用者的使用習慣，通常是經由入口網站或搜尋引擎以存取、連接網路資源。但如Facebook等社群網站平台出現後，因為該些平台可以供使用者連結親朋好友的近況、訊息，甚至也可以分享網路資源，因此吸引了大量的網路使用者趨近並加以利用。但Facebook最遭人詬病之處，在於隱私權條款的設計晦暗不清，使用者對於Facebook如何利用個人資料，也常常無法窺得全貌。甚至以Facebook而言，在2011年12月推出了「時間軸」的新版本，可以將使用者的網站活動，從申請成為Facebook會員那一天開始，鉅細靡遺的排序到現實生活的這一刻。換句話說，表示使用者在Facebook活動的歷程記錄，全然留存在Facebook的資料庫內，無一遺漏。而如果Facebook沒有提供這功能，使用者可能根本不知道Facebook到底保存了什麼資料，又對這些資料為如何之處理，簡言之，社群網站最重要的隱私權問題在於，你根本不知道網站經營者做了什麼！

另一方面可得確定的是，如前述社群網站如Facebook，會和廣告商或是第三方軟體公司合作，容由廣告商或第三方軟體公司在社群網站上置放連結，如果使用者點選或是使用了第三方軟體公司發布的程式，則會授權該第三方公司取得在社群網站內留置的個人資料。但是通常此類授權說明或是授權內容都很簡短，因此使用者實在無法光從簡單的點選動作知悉其後的法律效力和結果，當然，此類作法也無形之間「強制」加重了使用者在管理個人資料上的負擔，並無形中「強制」減輕了社群網站的法律責任，是否合宜，亦容有疑問。

二、外部威脅——網路資訊安全

隨著電腦科技及軟硬體的發展，寬頻上網、無線網路、行動裝置連結基地台通訊等日漸普及，傳統病毒或惡意程式傳染的途徑，也隨著此些新的應用方式，更加深入。傳統的防火牆、防毒軟體、URL過濾等資安技術，已經無法有效阻擋網路犯罪者的混合式攻擊。惡意網站數量從2009到2010年的增加幅度為111.4%，在所有內合惡意程式碼的網站中，有79.9%屬於已遭侵入的合法網站，52%資料竊取攻擊在網路上進行，大約34%的惡意Web/http攻擊，內含用來竊取資料的惡意程式碼，89.9%的電子郵件內含垃圾攻擊網站和（或）惡意網站的連結，美國和中國仍舊是前二大容納最多惡意程式碼以及接收最多遭竊資料的國家，而在Facebook最新動態訊息中，有40%包含網址連結，而這些連結中又有10%屬於垃圾攻擊或惡意網站[23]。

因此社群網站的使用者除了面對社群網站經營者對個人資料未知的傳輸、散布、處理、利用外，使用者還需面對利用社群網站所生的網路資訊安全問題。其實此類問題並不限於使用社群網站，但是大量利用社群網站的功能，如未有完善的資訊安全概念，遭受資訊安全危害而外洩個人資料，並非少見。因此在討論社群網站的資訊安全問題之時，不能不對於資訊安全危害的相關議題，有所認識。以下就針對社群網站較為常見的資訊安全危害手段、程式或新興的資訊安全威脅為之簡介：

23 參閱資安人網站，網址：https://www.informationsecurity.com.tw/seminar/news_detail.aspx?tv=41&aid=5971，最後檢索日：2011年12月26日。

㈠社交工程

社交工程（Social Engineering ）係目前網路盛行的攻擊方式之一，所謂社交工程，係指行為人刻意揣摩、操縱使用者的心理，利用一些詭計，讓使用者因此「猝不及防」、「措手不及」而採取特定行動，並因此洩漏資訊。例如寄送標題為目前備受矚目的重大事件與新聞之電子郵件或惡意連結；或利用人類愛聽八卦、偏好腥、羶、色的心理，鋪陳惡意連結程式作為誘餌；也可能利用使用人日常活動或工作相關的情報，例如線上理財、投資、帳單管理、購物及偽冒身份等等，讓使用人因為期待取得前揭資料而點選並瀏覽含有惡意程式的網站、傳送個人資訊、變更電腦設定等等。2011年3月11日日本發生規模9.0的地震後，就有人利用"日本"、"地震"、"海嘯"（"Japan", "Earthquake", "Quake", "Tsunami"）等關鍵字登記網域名稱，繼而發出含有惡意連結的詐騙電子郵件，誘使使用者鏈結至釣魚網站或含有惡意軟件網站[24]進行操作。此外，也有行為人偽冒公司經營者或決策機關致電或聯繫公司資訊部門，要求資訊部門提供相關秘密登入資料，如資訊人員一時不查，又擔心得罪假的企業負責人而屈服並提供資料，均可列入社交工程之討論範疇。

而以社群網站而言，因為社群網站中的網站內容並非全由網站經營者單方面提供，而可容由使用者自行撰寫、發布或分享的，甚至還有所謂第三方軟體公司的參與，因此吸引了大量社交工程行為。行為人可能向網友推薦新聞鏈結或張貼一些短網址，並進而分享在「塗鴉牆」[25]上，這些短網址經過分享或散布後，根本無法追查來源，但是此些訊息或短鏈結會一併夾查一些「生活常識」、「心理測驗」、「心情分享」、「警世箴言」、「幽默笑話」等社交工程標題，讓使用者失去戒心而點選，如經點選後恐會造成惡意程式的執行，或是直接載入惡意程式，使用者實不可不慎。

另一個在Facebook網站上引發的資訊安全問題，在於按「讚（Like）」，這個設計。基本上如果是屬於使用者的訊息散布或照片、影片分享，按「讚」僅表達在頁面上，顯示觀覽者的感想。但是如果是在Facebook內的社團、粉絲團或應用程式頁面上按「讚」，就表示同意加入該團體，或容許該團體存取使用者的個人資料。因此行為人就會將前揭頁面上訊息散布或照片、影片分享及短網址上的「讚」連結到特定的應用程式或社團，當使用者以為只是單純的說「讚」而加以點擊之時，實際上卻是點選了另一個功能，以至於無意間就加入了某社團、粉絲團或是同意應用程式存取資料，在無形之間，個人資料就已外洩[26]。

㈡惡意程式

電腦運作的內容，由程式來完成，因此如果某一組程式經執行或運作後，對電腦主機的合法控制權人造成具有惡意的結果，該段程式就統稱為惡意軟體（Malicious Software）。而所謂惡意的結果，係指該程式誤導或未經合法使用者同意即行安裝、啟動，並使行為人取得電腦之資訊或存取權限。

在討論惡意軟體之前，我們先認識一下早先對電腦病毒（Computer Virus）、特洛伊木馬程式（Trojan horses）與間諜軟體（Spyware）等電腦程式之定義。其實因為電腦程式的多元

24 香港電腦保安事故協調中心，<日本地震災難，騙徒虎視眈眈>，2011.3.15，網址：https://www.hkcert.org/mobile_url/zh/blog/11031501。最後檢索日：2011年12月25日。

25 Facebook供使用者互相交換、分享訊息的頁面。通常個別使用者觀覽的頁面，依好友數量和人別的不同，會顯示不同的內容。

26 此稱為clickjacking，Sophos, <Security Threat Report 2011>，2011.5，頁17，網址：http://www.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/sophos-security-threat-report-2011-wpna.aspx?leadId=832085279&response=b5eb188a68fe22c4b09ee8de19c6b0f9。最後檢索日：2011年12月25日。

和變化並無界限，因此對前揭的惡意程式，並無一致的定義，但根據科技界的共識，病毒是一種會自我複製的可執行程式，當病毒執行時（發病）時，它很可能會破壞硬碟中的重要資料，有些病毒則會重新格式化（Format）硬碟。而有些病毒就算未直接破壞系統內的電磁紀錄，但也可能會佔據一些系統的記憶空間，並尋找機會自行繁殖複製，因此電腦效能將會變得比一般正常的電腦慢[27]。

而所謂特洛伊木馬程式，源出自西元前九、八世紀之古希臘荷馬史詩，描述西元前12世紀希臘國王攻打特洛伊城，因久攻10年不下，遂造一大型木馬於馬腹內暗藏軍士後退去；嗣特洛伊人將木馬引入城內，隱身馬腹內之軍士即乘機離開馬腹，自城內與仍在城外之古希臘軍隊應合破城，又稱為木馬屠城。此處借該史詩暗喻，其概念似遠端管理程式，係指電腦在無預警之情形下遭植入安裝「木馬程式」或稱「後門程式」，通常有隱蔽、自動啟動、欺騙、自我恢復、破壞、傳輸資料等特徵，通常透過偽裝、電子郵件或直接嵌在網頁之超文件標示語言MTML、XML中，吸引用戶下載執行或安裝，製作木馬程式之人，得利用已遭植入木馬程式之電腦伺機予以直接連線，或在已遭植入木馬程式之電腦內透過背景連線，並在已遭植入木馬程式之電腦內執行程式指令、刪除、變更、取得已遭植入木馬程式之電腦的文件或操作畫面，甚至透過網路連線以遠端遙控方式，控制已遭植入木馬程式之電腦，其目的多以蒐集已遭植入木馬程式電腦之使用人不欲洩漏於外或應隱藏、非以明碼方式呈現之資訊，例如連線密碼、信用卡號碼等，或將前揭應秘密之資訊集中儲存在電腦硬碟特定資料夾中，再伺機至本機存取，或將已遭植入木馬程式之電腦充作連線中繼電腦（即為跳板電腦、僵屍電腦）進行下一台連線電腦之連線工具等；木馬程式之功能可包含隱匿控制端之IP位址、遠端遙控、截錄封包、記錄鍵盤輸入資料、傳遞資訊、提供封包轉送達到跳板功能……等。

至於間諜軟體，觀其名就可以知悉，此類軟體的主要功能，在於監控使用者的電腦使用活動，並在使用者不知情的狀況下，將使用者的活動內容如帳號密碼等，傳送到特定人可得接收的端點。其他諸如強制開啟廣告的程式、未告知使用者即修改Hosts[28]檔案的程式，因為並非合法控制權人所同意或授權之電腦運作，均可以統稱為惡意程式。

惡意程式的運行，是目前電腦資訊安全中一般使用者最容易遇到，也最為氾濫的問題。因為惡意程式的內容不一而足，以目前的資訊安全風險而言，沒有單純是電腦病毒的程式、也沒有僅有遠端控制功能，而無法傳送資訊的程式。因為以惡意程式而言，該組程式在網路上流通，我們很難期待這些程式有版權聲明或著作權的保護，而對於此些程式進行改良或添加功能，對於網路上大多數的惡意行為人並非難事，因此現在的惡意程式通常改版快、內容或功能繁雜，很多時候連開發者都不一定認識自己撰寫的程式，因為已經被改版多次了。所以惡意程式的內容，絕非僅含前述三種，畢竟前述三種惡意軟體的定義，也只是科技或資訊安全業者的各自表述。而幾乎所有的資訊安全問題，背景必定有惡意程式的執行，方才能達到取得存取權限或電磁紀錄的目的。社群網站也是一樣，行為人可能利用社群網站發佈或上傳檔案、傳送連結等功能，配合社交工程手法，讓使用者無意間執行惡意程式，以達到獲

27 趨勢科技網路安全百科，<防毒入門——基本概念——認識電腦病毒>，網址：http://www.trend.com.tw/corporate/security/virusprimer_1.htm，最後檢索日：2011年12月25日。

28 Microsoft Windows電腦系統中，做為網路名稱和IP位址解析的系統檔案，供電腦辨識網址和IP位址的對應關係，優先權大於DNS伺服器。

取個人資料或電腦主機控管權限之目的，不可不防。

㈢網路釣魚

網路釣魚（Phishing）係指在網際網路活動中，以偽冒的合法廠商網頁，誘使不知情之使用者誤信為真實合法廠商所提供之服務，或以不實但吸引人的網路服務[29]，讓使用者在含有惡意傳送功能的網頁上自動填載並提供相關個人資料。最常見的莫過於偽冒知名銀行、廠商或網路服務業者如Citibank、Amazon、MSN或著名的社群網站Facebook、Google+等。

網路釣魚最大的難處，是要如何誘使使用者連結到虛假不實的網站或服務以鍵入個人資訊。此部分行為人可能以社交工程之方式寄發一封不實連結的電子信件，向使用者說明要更新資料、取得贈品或線上客服等，當使用者連結至偽冒的網頁後，就可能因此輸入資料；抑或冒用聯絡人名義，直接以即時通訊軟體傳輸錯誤連結；甚而向搜尋引擎服務廠商購買關鍵字廣告，當使用者查詢時，建議鏈結到偽冒之網站而進行釣魚。至於社群網站，因為有大量的個人資料存在，因此行為人更有利用此方式取得社群網站帳號密碼之價值，蓋因如此項帳號密碼外洩，表示整個詳盡的個人資料紀錄和好友資料，均同時為行為人獲得，損害要為重大。

㈣短網址

所謂短網址，乃因目前網際網路上所使用的網址，縱然已經容許使用人類可得辨識的文字，而非電腦主機可以認識、連接的IP位址，以幫助使用者記憶，但因各項網路服務的拓展迅速，服務多元，慢慢的網址也就越來越長，因此有的網路服務商即推出短網址服務，利用異常簡短但通常無意義的簡短網址，方便使用者進行鏈結或傳遞訊息。目前常見的短網址服務有「http：//tinyurl.com/」、「http：//Orz.tw/」、「http：//ppt.cc/」、「http：//goo.gl/」、「http：//bit.ly/」等。

短網址雖然有效縮短了網址的長度，讓網際網路使用者可以方便記憶，或在多種平台上直接鍵入網址瀏覽網站。但是就原本長度的網址，其中可能含有由公司註冊的網域或商標，可以因此代表該網站的正確性，也是辨識該網站是否屬於網路釣魚網頁的一種方式，如今全部的網址均變成一截簡短而無意義的文字，因此駭客多利用來作為社交工程或網頁掛馬的連結工具，使網路使用者防不勝防。開放Web軟體安全計畫（Open Web Application Security Project）於2010年選定的第10名網路安全威脅：不明的轉址或轉向（Unvalidated Redirects and Forwards）[30]，就包含短網址所帶來的威脅，這個問題在社群網站中同樣存在，社群網站中大量分享的短網址，通往的網頁到底是天堂還是地獄，使用者可能在點選後連結到任何一個惡意程式網頁，豈可不謹慎。

㈤網頁掛馬（Drive-by Downloads）

自從網際網路盛行以來,網頁製作上為了增加網站服務的功能，也避免使用者必須繁複、重複的設定、同意網頁活動，因此Java Script[31]和ActiveX[32]的網頁技術逐漸被廣泛使用，此些技術的特性在於不用使用者同意就可以自動執行，因此如果遭到惡意使用，就有可能修改電腦主機的設定或傳送某些敏感資訊。

29 之前MSN曾盛極一時的網路釣魚行動：誰在封鎖你（Who Block You）？行為人寄送廣告信或即時通訊，告知使用人只要連結網頁，並依說明只要鍵入MSN的帳號密碼，就可以知道誰封鎖了你，一時之間使得使用者瘋狂將帳號、密碼送給駭客。

30 OWASP，https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project，最後檢索日：2011年5月20日。

31 昇陽電腦（Sun Micro Systems）開發的跨平台應用軟體的物件導向的程式語言，也就是說使用Java語言編寫的程式可以在編譯後不用經過任何更改，就能在任何硬體裝置條件下執行。

32 ActiveX係由微軟公司所開發，安裝在IE瀏覽器上增加網際網路瀏覽功能的程式。

大部分的網頁掛馬，都不是專門設置網頁掛馬的網頁，讓使用者讀取，因為那樣網頁的流量實在太低。因此慣常的作法，行為人會先行取得某些網站的存取權限，並伺機在較大觀覽流量的網頁上，另行加入使用含有惡意動作的前揭程式碼，當使用者瀏覽該網站時，電腦即會自動執行該段程式，而進行惡意動作。一般來說，網頁掛馬通常會修改瀏覽器設定、用戶作業系統、傳送機密資訊，也可以要求電腦至特定網址下載惡意程式，當然，重點是使用者都不知道。

伍、社群網站的挑戰

社群網站的運用在現代人的生活中不可或缺，利用電腦蒐集、處理及利用個人資料之情形日益普遍，但社群網站上充斥著關於個人隱私等足以辨識個人之資料，相對的保護更形重要。經濟暨合作發展組織（Organization for Economic Cooperation and Development，OECD）、亞太經濟合作會議（Asian-Pacific Economic Cooperation，APEC）及歐盟這類的國際性組織，皆對個人資料之保護訂有國際性規範；此外，許多先進國家如美國、德國、日本等均訂有個人資料保護相關法制配套，而我國雖然已修正個人資料保護法，希望能夠處理個人資料遭受威脅的困境，但是在面對社群網站的衝擊與挑戰時，相關政府機關是否確實已做好配套或執行的準備？而在這場個人資料與資訊流通的戰爭中，到底使用者又應該認識什麼？誰又是最後的贏家？

一、沒有敵人的戰爭

正視一個基本的問題，目前全世界較為著名的社群網站，不管是Google+、Facebook、MSN、Twitter或Tagged等，「沒有一家網站經營公司將相關設備和電腦主機放置在我國境內」[33]，甚至還有很多家公司，在我國境內根本沒有設立辦公處所[34]，也就是說，除了透過網際網路提供服務之外，該公司與我中華民國完全沒有任何聯繫因素，因此對於社群網站的個人資料議題，除了網站官方所提供的電子郵件外，我國使用者完全沒有任何聯繫或是申訴的管道，連要提出民、刑事訴訟都不可得。就連政府機關要介入輔導或協商，也會因為網站的經營階層或公司根本在我國沒有任何聯繫窗口，政府機關想要介入協助，也根本無從著手。

更嚴肅的結果是，這會變成我國空有個人資料保護法之制度，但是對於此些擁有眾多個人資料的社群網站，卻完全沒有執行或實現法律規範內容的可能。例如我國個人資料保護法中的行政檢查，因為係與資訊安全或科技技術相關的事項，諸如：資料是否正確，有無補充更正、是否發生資安危害、是否建立適當的安全措施等，因為這些事項不一定公示，而可能由社群網站所經管，甚至所謂「個人資料檔案安全維護計畫」或「業務終止後個人資料處理方法」，更無任何標準以資遵循。而如果只是單純要求有計畫或方法，卻無從監督計畫是否落實、是否依照處理方法確實銷毀（刪除），均無從得知。更甚者，以現今的網路經營態樣，跨境傳輸和遠端操作已為常態，當存放個人資料的電腦主機根本不在我國境內之時，如Facebook的主機在美國境內，Plurk的主機在加拿大，相同的是對我國國民提供服務、蒐集資料，也同樣的在我國境內沒有任何營業據點，則根本沒有行政檢查之餘地。更甚者，社群網站之經營公司如果在我國境內沒有公司登記、稅務稽核等聯繫，又如何踐行前述眾多行政裁罰、民事求償或刑事處罰規範，此為我國政府

33 參前註9。

34 例如Facebook、Plurk、Twitter 等，在我國境內均沒有設立據點。

或使用者在面臨網際網路世界時不可避免之課題，亦為現實遇到的具體難處，但至今仍未見有對應之方法。

二、不是對手的戰爭

另一部份，因為社群網站的使用者眾多，「黏性」漸次增強，其後帶來的結果就是，社群網站的經營者會片面決定網站的內容和契約（包含隱私權設定）的條件。雖然網站通常在修改隱私權條款時，會公告周知，或以彈跳視窗、訊息之方式通知使用者，但是使用者如果打算繼續使用該網站，除了點選同意之外，根本沒有討價還價或個別洽談約定內容之可能，則此種同意，是否真的是使用者的真意，殊有疑問。

除了必須片面接受約定內容之外，另一部份，社群網站挾著充沛的軟硬體資源和龐大的使用者資料，對於個別用戶的意見，通常不可能，也不願意重視。這雖然是因為此類免費網站使用者眾多，無法逐一或個別提供服務之必然慣例，但目前的社群網站不僅僅是對於個人用戶的意見不予理會，連國家或政府的要求，亦已得抗衡或「不服從」，可見力量之龐大。例如2011年6月間，臺北市政府法規會要求Google所管控、經營的Android Market內所販售的應用程式，必須遵守我國消費者保護法之規定，給予消費者7天之鑑賞期，但是Google則認為我國的消費者保護法7天鑑賞期的規定不應適用於網路軟體銷售，因此雙方對於此部分容有歧見。至同年6月27日，因協商不成，臺北市政府裁罰Google新臺幣100萬元，但因為雙方歧見尚未消失，Google也認為自己的主張沒錯，為避免遭連續裁罰，從當天起Android Market內的所有付費軟體全部下架[35]，直到本文寫作的同年12月底，仍未有恢復之跡象，因此我國使用者至今仍無法購買Android系統下任何付費之應用軟體。從而，可以想見臺北市政府法規會為了使用者權益所為之行政作為，與國際性的網路服務供應商直接衝突的結果，是所有使用者無法使用付費的應用軟體，而變成網路的第三世界成員。此雖為我政府機關所不樂見，但已可實際窺見在面對此些國際性的網路服務供應商時，如政府未有完善的配套，實際上受害最大的，終究還是使用者。

三、置於規劃的戰爭

承上，可以發現對於社群網站蒐集、處理、利用個人資料，或對個人資料之刪除、國際傳輸等，我國使用者或是政府機關根本無力，也無能著手管理或制衡。而臺北市政府之前「牛刀小試」的結果，除了傷害我國使用者的利益之外，似乎並沒有帶來其他確實的助益，畢竟除了修法之外，臺北市政府和Google各持己見，臺北市政府也不可能突破此種法律意見上之僵局。因此目前我國使用者和政府能做的，就是依賴其他政治團體進行管制和遊說。2011年12月21日，愛爾蘭資料保護委員會（DPC）經過3個月的審核後，公布一份審核報告，認為Facebook的隱私保護政策過於複雜及缺乏透明性，且用戶恐在不知情下公開個人資料，因此Facebook必須提供用戶更清楚的隱私政策，並給用戶更多控制權。例如賦予用戶永久刪除歷史訊息、朋友邀請、戳一下（poke），用來引起其他用戶注意的功能、標籤、發文的能力。而且，Facebook無限期保留用戶廣告點選紀錄的行為「令人無法接受」，也提到Facebook的臉部辨識功能，可讓用戶辨識或「標籤」照片裡的人，此功能應以「更恰當的方式」實施[36]。而關於DPC的報告內容和要求，Facebook的回應是，會「立刻將保留期限

35 自由時報電子報，「拒絕7天退費被罰100萬／Google槓北市府付費APP不賣了」，網址：http://www.libertytimes.com.tw/2011/new/jun/28/today-life1.htm。最後檢索日：2011年12月25日。

36 全文請參閱網址：http://www.dataprotection.ie/docs/Home/4.htm。最後檢索日：2011年12月25日。

改為2年」，並「應審核結果要求，臉書愛爾蘭總部已同意在接下來6個月實施多項改善的『最佳作為』」[37]。為文至此，為何Facebook對於DPC的要求照單全收的原因昭然若揭，只有一個，Facebook的總公司設立在愛爾蘭。

因此，我們可以發現，唯有相關網站經營者的公司登記、稅務、金流收支、員工、設備、電腦主機與某個國家或地區間有更深的聯繫關係，則所謂的個人資料或隱私權保護，該國政府或執法機關才有「執行」或「要求」的能力，這也是國際社會和跨國貿易的不爭事實。然而，在與社群網站經營者的戰爭中，我國相關政府機關對於此類國際性社群網站的存在或個人資料的蒐集，除了無力管制、監督或裁罰外，亦完全沒有任何的規劃和政策。因此就我國現狀而言，這是一場沒有敵人，無力著手，無法預見，也無力對抗的戰爭。在面對社群網站、國際性企業的充沛能量，我國政府至今仍無法拿出相對應的具體政策，更沒有吸引投資或加強合作的目標，更遑論吸引此些網路服務供應商在我國設立據點，則空有完善的法規卻無法執行，至為遺憾。

陸、結論

目前較常為國人使用之網路服務，大多為外國之跨國企業所提供，這些網路服務，社群交友的內容多元，變化豐富，目前國人使用的人數和使用時間亦逐漸上升，各項社會行為也與該些服務發生關係。但經由使用者提交，或由網站留存的個人資料，如消費習慣，瀏覽網站等隱私資料等等，斷難視為該些網路服務供應商之私人資產，而應仍由使用者擁有控制之權限，此可由我國個人資料保護法中第8條第1項明定非公務機關向當事人蒐集個人資料時，應明確告知當事人蒐集之目的、個人資料之類別、個人資料利用之期間、地區、對象及方式。第11條第3項本文更明文個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料可知，但在面對這些社群網站時，如何落實使用者控管個人資料的能力，則是政府應該設法面對的問題。

其實，前揭難處均係肇因於該些網站經營者在本國一無據點、二無設備，因此可渾然不受我國法令之管控，形成網際網路上的治外法權。我國政府唯有積極協助，甚至要求預計在我國境內，或針對我國國民提供服務之網路服務供應商，不論該些服務是有價或是無償，均應在本國設立分公司或建立電腦網路通訊、傳輸或轉接設備。此項作為之具體作法可以是獎勵，也可以是投資限制[38]。則不僅可增進我國在國際社會、網路事業即全球通信之重要性外，並可督促事業機構間負起社會責任，以配合我國法令規範、繳納稅捐，達到有效的政府監督機制，以實際遂行我國個人資料保護之立法目的。

37 雅虎奇摩電子報，「隱私政策不透明臉書將修改」，網址：http://tw.news.yahoo.com/%E9%9A%B1%E7%A7%81%E6%94%BF%E7%AD%96%E4%B8%8D%E9%80%8F%E6%98%8E-%E8%87%89%E6%9B%B8%E5%B0%87%E4%BF%AE%E6%94%B9-063757583.html，最後檢索日：2011年12月26日。

38 更甚者，是否進行「輕度」的網路管制，亦為目前討論的方向。目前預計對網路進行輕度管制的國家越來越多，參閱iThome Online，「全球對網路管制的國家越來越多」，網址：http://www.ithome.com.tw/itadm/article.php?c=43491，最後檢索日：2011年12月26日。