



Research Center for information Technology Innovation

TWISC

TAIWAN INFORMATION SECURITY CENTER

中央研究院-資安前瞻關鍵技術基礎研究計畫

前瞻議題研究小組 林伯樺

《FACEBOOK個資洩漏事件法律責任分析》

FACEBOOK個資洩漏事件法律責任分析

一、前言

二、案件說明

三、法律分析

(一) Facebook洩漏公開之使用者個人資料

(二) Facebook洩漏非公開之使用者個人資料

(三) 關於GSR及劍橋分析取得Facebook上使用者個人資料

(四) 於歐盟一般資料保護規則下法律適用之可能狀態

四、結論

摘要

知名社群網站Facebook於2月底3月初，發生大規模個資遭盜用之資料外洩事件，遭盜用之個資據傳遭使用於英國脫歐公民投票及2016年美國總統大選中，用以投放針對性之政治廣告、訊息，引發各界對於Facebook個資安全之高度重視；復又正值歐盟一般資料保護規則（GDPR）生效前夕，Facebook個資事件亦再次激起對各大網站就於個資收集、使用之爭論。本文試以Facebook案為例，檢討Facebook公司與案件中關連企業劍橋分析、全球資訊分析（GSR）等公司之法律責任，企以初步釐清各國對於個資保護之態度。

一、前言

全球知名社群網站Facebook於3月爆發個資外洩事件，據估計有至少近5000萬人之個人資料，被不當使用於2016年美國總統大選中，致使Facebook股價一度嚴重受挫；而於4月初更有消息指出外洩個資可能涉及8300萬名用戶，甚至是絕大多數的用戶均有個資外洩之可能。本文以下就此案例，試分析其個資外洩事件之本質與法律上可能之關係。

二、案件說明

本案之中，Facebook並未受到駭客攻擊或內部員工盜賣個資等常見的個資外洩事件之影響，嚴格來說此次事件甚至不是個資的「外洩」，而應為個資被未經授權的使用事件，茲簡要說明如下。一般使用者於使用Facebook時，即會將許多個人資料交給Facebook，諸如居住的城市、畢業的學校、婚姻感情狀態等，而在Facebook上的活動過程中，亦會產生許多相關的個人資料，例如閱覽的文章、按讚的文章，甚至是被按讚的文章等。Facebook在一般使用狀態下，即透過蒐集此類個資並經由大數據（巨量資料(Big Data)）分析判斷使用者的喜好，並予以投放廣告或透過演算法呈現出使用者會關心的貼文、動態等。¹

其次是Facebook上第三方程式，Facebook原本開放第三方程式的存在，亦即除了Facebook本身程式外，可由第三人藉由Facebook所提供的平台開發並運行程式，例如在Facebook上常見的心理測驗、猜謎等諸多小程序，皆屬於此種第三方程式。而此類程式在執行的過程中會要求使用者對程式開放隱私權權限，亦即容許其讀取、取得使用者原先已經放在Facebook上的相關個人資料；進一步，第三方程式的開發者取得使用者的個人資料後，再用於開發者自身之特定目的用途，包括學術研究、作為將來開發商品或相關服務之基礎，但此類使用必須符合第三方程式開發者與Facebook簽訂的契約，在使用目的上受到限制。²

¹ Facebook 資料政策 (2016.6.29)，available at: https://www.facebook.com/full_data_use_policy，last visit:2018.03.31。

² 前揭註 1。

而本次爆發的劍橋分析一案，即是此類第三方程式所引發的個資問題。首先係由任職於英國劍橋大學心理學家Aleksandr Kogan，在2014年開發了名為“thisisyourdigitallife”的性格心理測驗程式，這個程式會讀取使用者於Facebook上的相關個人資料並加以分析，並宣稱將把所得到之個資用於心理方面的學術研究；約有27萬人使用了此程式，並將其個人資料，包括好友的名單交給了Aleksandr Kogan和其所創辦的「全球科學研究公司」(Global Science Research, GSR，位於英國)。

其後GSR進一步透過該應用程式所得到的好友名單資料連結到次名使用者，同時因Facebook限制寬鬆，2015年之前，除非用戶設定為不公開，否則這些第三方程式(application, App)可取得用戶的朋友清單，因此讓GSR公司進一步擴張到用戶的朋友網路，從下載App的27萬人到取得5千萬人的個資。GSR在未經次名使用者同意的情形下，讀取了其於Facebook上存放的個人資料，可能包括其原先並未設定為公開之個人資料(但依照Facebook的說法其系統並未遭駭³)，最終獲得了5000萬(另說或為8300萬)名使用者的個人資料。⁴

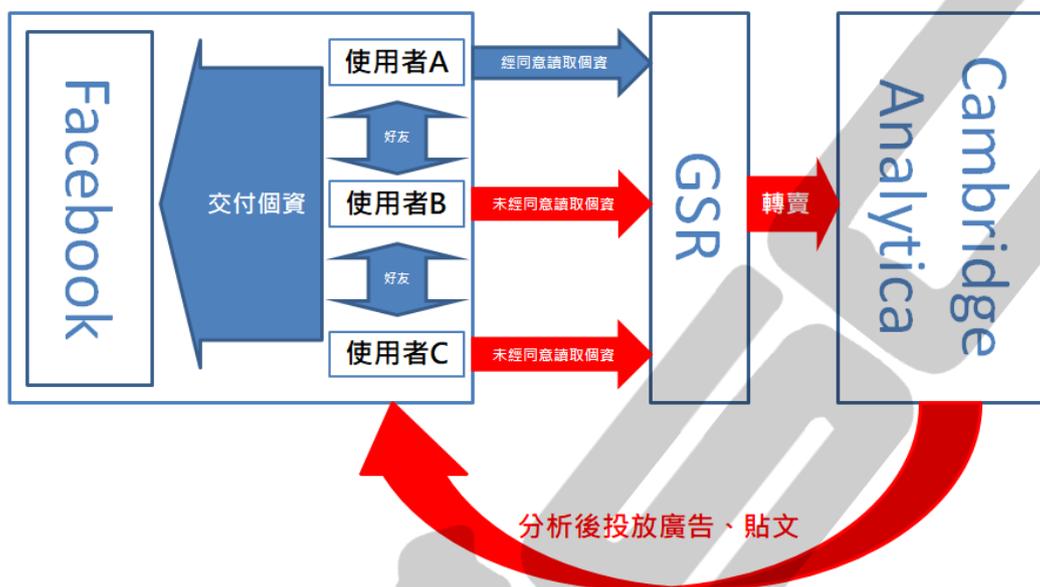
第三步，GSR將其獲得的使用者資料轉手販賣給一家名為「劍橋分析」(Cambridge Analytica，位於英國)的資料分析公司，此公司曾由白宮前首席策略師與美國總統顧問史蒂芬巴農(Steve Bannon)擔任行政主席，並曾獲得共和黨金主億萬富豪默瑟(Robert Mercer)1,500萬美元投資。而據劍橋分析之離職員工懷利(Christopher Wylie)所稱，劍橋分析則將其獲得的數據用於2016年美國

³ 蘋果日報，《fb 爆 5 千萬用戶個資外洩》，available at: <https://tw.news.appledaily.com/international/daily/20180319/37961885/>，last visit:2018.03.31。

⁴ 中央社，《8700 萬用戶個資外洩 臉書將一一通知》，available at: <https://tw.news.yahoo.com/8700%E8%90%AC%E7%94%A8%E6%88%B6%E5%80%8B%E8%B3%87%E5%A4%96%E6%B4%A9-%E8%87%89%E6%9B%B8%E5%B0%87-%E9%80%9A%E7%9F%A5-143604946.html>，last visit:2018.03.31。

科技新報，《一款心理測驗 App，引爆 Facebook 史上最大個資外洩危機》，available at: <https://technews.tw/2018/03/20/facebook-and-the-endless-string-of-worst-case-scenarios/>，last visit:2018.03.31。

總統大選中，判斷使用者之政治傾向並投放相關的廣告或訊息⁵，相關關係參見下圖。



若以上圖為例觀察，使用者A是自己使用了GSR所開發的第三方程式，經過同意後GSR讀取了A的個人資料，但B、C的部分則是因與A、B為好友關係，在未得B、C同意的情形下，GSR也蒐集、取得其個人資料；最終GSR將所有個資販售給劍橋分析，而劍橋分析再利用取得的數據分析後投放對於2016年美國總統大選有影響之廣告及貼文，用於影響該次大選結果。依據此等關係，GSR透過使用者A同意使用該心理測驗程式而取得A之個人資料，倘若於進行測驗前履行告知義務並取得使用者同意，依據Facebook隱私政策而言，並不生使用者隱私權之侵害。因而可能具有隱私侵害、資料外洩性質者，即為透過A之個人資料在未經其他使用者同意的情形下取得B、C等人的個人資料，其後將個資轉賣予劍橋分析公司，以及劍橋分析公司將該等個資用於分析利用等部分。倘若進一步區分，須將GSR未經同意所取得使用者B、C之個人資料，區分為使用者於Facebook上設定為公開之個人資料，與使用者設定為不公開部分之個人資料，兩者分別討論之。

⁵ 中央廣播電臺，《FB 個資外洩 四大要點看「劍橋分析」》，available at: <https://news.rti.org.tw/news/view/id/401341>，last visit:2018.03.31。

三、法律分析

於討論Facebook本次個人資料外洩事件時，首先須先行思考者在於準據法之疑義。依據Facebook服務條款，當消費者與其發生爭議時，若係因服務條款或Facebook提供服務所生，消費者得於所在國家法院適用該國法律為訴訟請求；其餘情形下，均係以美國加州北區地方法院或位於聖馬刁郡（San Mateo County）的州法院為屬人之有管轄權法院，且請求應以加州法律為準據法⁶；加以本次個人資料外洩案件中，絕大多數使用者均位於美國境內⁷，因此關於Facebook個資外洩部分之討論應以美國關於個人資料之相關規範作為準據法。然關於GSR取得個人資料、將個人資料轉讓與劍橋分析，及劍橋分析利用處理本案中個人資料之部分，則可能有不同之準據法。由於GSR及劍橋分析兩公司皆設立於英國境內，因此其相關部分之準據法，除因所蒐集個人資料主要皆為位於美國境內之美國國民而有美國法之適用外，尚須考慮英國對於個人資料之管制規範。至於歐盟之一般資料保護規則，由於其生效日期為2018年5月，於本案發生時尚未生效，依據法律不溯及既往原則僅得做為參考。

其次必要說明者在於，由於案發後Aleksandr Kogan所開發之程式“thisisyourdigitallife”已遭Facebook下架，且GSR公司亦以解散，因此目前難以確知案發時該程式要求使用者同意之隱私、個人資料使用範圍為何，對於當初使用該程式並同意GSR取得個人資料之27萬使用者，其個人資料被轉讓予劍橋分析公司並被其分析利用一事，其適法性難以完整確定探討，因而本文以下討論皆以未使用“thisisyourdigitallife”程式而被獲取個人資料之使用者部分為主，此特說明之。再加以考量前揭使用者資料區分為公開與非公開兩種不同形式，則下文以Facebook洩漏公開之使用者資料、Facebook洩漏非公開使用者資料、GSR與劍橋

⁶ Facebook 服務條款，available at: https://www.facebook.com/legal/terms/plain_text_terms，last visit:2018.03.31。

⁷ ETtoday 新聞雲，《一鍵秒查！Facebook 讓你自我檢查「是不是劍橋分析受害者」》，available at: <https://www.ettoday.net/news/20180413/1149960.htm>，last visit:2018.03.31。

分析取得處理使用者資料三階段討論之。

(一) Facebook洩漏公開之使用者個人資料

第一種情形，GSR公司透過使用其心理測驗程式並同意其取得個資之使用者的好友名單，連結至未使用該程式亦未同意其取得個資之Facebook使用者，取得該未同意使用者於Facebook中設定為公開部分之個人資料，造成Facebook資料外洩部分，其法律上效果究竟如何？Facebook就此部分是否應該負責？

美國對於個人資料係以隱私權之概念加以處理，換言之，個人擁有不被探知的權利，不受他人或國家打擾之權利；而其判斷標準，係以Katz v. United States一案中對憲法第四修正案所提出的「合理隱私期待」原則作為判斷標準，意即當事人有無主觀上隱私期待，再考慮此期待是否受到社會一般性認可為準⁸。詳言之，當事人對該事項是否具有將之保留為私人領域事項之主觀想法，倘具有此想法、期待時，尚須考慮社會一般共通觀念，是否認為此等想法、期待係屬合理。倘社會通念認為此等隱私期待係屬合理，則認為該等事項屬於隱私權保護範圍；反之，倘社會通念認為該期待並不合理（亦即一般不認為屬私領域或得保留隱私狀態之事項），或當事人根本沒有主觀的隱私期待時，該等事項即屬公開領域範圍而不受隱私權保護。一般而言，而網路係屬於公共大眾得接近之領域，性質上屬於公共場所，依據上揭合理隱私期待之判斷標準而論，實難受憲法第四修正案之保障⁹。

縱或認為網路不能一概而論全屬公共領域空間，依據其使用方式之不同，亦有屬於私領域空間之餘地；然本案中，使用者於Facebook網站上所登載之個人資料，本即有設定公開與否之權限，倘使用者自行設定為公開，亦即其理解此等個人資料將可被任意、不特定第三人所接近讀取，因而就此等使用者自行設定為公開之個人資料，難以認為當事人具有合理的隱私期待，因此也非屬私領域空間而

⁸ Katz, 389 U.S. 347, 361 (Harlan, J., concurring).

⁹ 蔡蕙芳，從美國隱私權法論刑法第三一五條之一與相關各構成要件（上），興大法學第6期，2010.05，頁93。

受憲法第四修正案之保障。換言之，倘若使用者自行設定為公開之個人資料，即屬公領域空間範圍而不受隱私權之保障，Facebook於此部分亦不存在有「洩漏」之問題。

（二）Facebook洩漏非公開之使用者個人資料

關於第二部分，即為使用者設定為非公開之個資遭Facebook外洩部分。依據前揭報導中Facebook副總裁兼副法律顧問葛瑞沃(Paul Grewal)所稱其系統並未被入侵，加以報導中提及2015年前Facebook之系統設定寬鬆，致使第三方程式得以讀取相關個資，因此在進一步調查出現前，可認為本次事件係Facebook系統給予GSR讀取、接觸使用者非公開個資的權限，亦即等同Facebook將使用者非公開個資交付給GSR，而須思考Facebook法律責任究竟如何。

就個資當事人之主觀而言，由於此類個人資料已由使用者設定為非公開狀態，可見當事人具有將此類個資保留於私人領域之主觀意圖；而客觀上由於設定為非公開狀態，不特定之普通使用者無法輕易接觸此類個人資料，亦因而會認知到此為個資當事人之隱私領域，是以社會通念亦應得認可當事人主觀隱私期待係屬合理可接受之範圍，致使此類個資係具有合理隱私期待，屬隱私權所保障之範疇。則以美國法作為準據法時，對於網路空間之隱私權保障規範，係由聯邦或州立法配合產業之自治模式、市場機制來決定¹⁰，相對於歐洲採取由政府管理為主之機制，美國政府並不積極介入個人資料的蒐集、處理、利用，而僅於特定產業形成隱私權濫用危機時方立法介入¹¹。換言之，美國處理線上隱私權議題時，係由個別企業與使用者、消費者所簽訂之契約作為主要依據，僅有在特定企業或議題上才適用政府所訂立的法案作為依據。

¹⁰ Corey A. Ciocchetti, E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors, American Business Law Journal Vol.44 No.1, Spring 2007 ,P.72, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1090398。

¹¹ 翁清坤，網路上隱私權政策之效力：以美國法為中心，台大法學論叢第 45 卷第 1 期，2016.03，頁 157。

而本案中所涉及之法規範，在聯邦層級應為兒童線上隱私保護法¹²，於州層級則為加州青少年數位隱私權法¹³及加州線上隱私權保護法¹⁴。若以本案中劍橋分析公司蒐集當事人個資主要係用於影響美國2016年大選之目的加以考量，則似乎可以暫且忽略關於兒童及青少年之隱私權問題，蓋因蒐集不具有投票權之兒童及青少年個資，對劍橋分析欲投放針對性、政治性廣告之目的而言似無幫助可言；若此，本案例中涉及的法規可能僅有加州的線上隱私權保護法。加州線上隱私權保護法被認為係全美國線上隱私權保護之先驅¹⁵，甚至有謂加州線上隱私權保護法形同美國線上隱私權政策之國家標準規範者¹⁶。但事實上綜觀該法規定，其僅要求網站業者必須公布其隱私權政策並遵守之，其必要項目包括所蒐集個人資料類型、將分享個人資料之第三人類型、重大變更之通知程序等，並未對於業者所應該採取之隱私權政策具體內容有更多的要求規範，亦未對業者違反自身所制定之隱私權規範時所應承擔的法律責任進行規範，這意味著倘一旦業者違反自身所制定的隱私權政策，僅成為與當事人間的民事契約不履行而必須承擔民事責任，同時亦表示當事人必須透過冗長的民事訴訟程序及複雜的舉證行動來捍衛自身隱私權。

因而於本案例中，若僅以加州線上隱私權法為前提討論Facebook所將面臨的法律責任，則須取決於Facebook自身之隱私權政策約定內容，對其將個人資料傳輸予第三方之相關規範如何。依據Facebook資料政策之內容，其對於如何分享資訊中「我們服務提供的或使用我們服務的應用程式、網站及第三方整合」此項目所做出的說明為下¹⁷：

如果您使用的第三方應用程式、網站或其他服務使用了我們的服務，或與我

¹² 15 U.S. Code Chapter 91 (§6501 - 6506).

¹³ California Business and Professions Code §22580 - 22582.

¹⁴ California Business and Professions Code §22575 - 22579.

¹⁵ 前揭註 11，頁 163。

¹⁶ Cyrus Wadia, California-Style Privacy Goes National, Orange County Lawyer Magazine Vol.54-Jun, 2012.06, P28-29.

¹⁷ 前揭註 1。

們的服務整合，則他們可能會收到與您的貼文或分享內容相關的資訊。例如，當您和Facebook朋友一起玩遊戲，或是在其他網站上使用Facebook「留言」或「分享」按鈕，遊戲開發商或網站可能會取得您在遊戲中的相關活動資料，或是收到您從他們網站分享至Facebook的留言或連結資訊。此外，當您下載或使用這類第三方服務，他們就可以取得您的公開個人檔案，其中包含您的用戶名稱或用戶編號、年齡範圍、國家／地區、使用語言、朋友名單，以及您與他們分享的任何資訊。這些應用程式、網站和整合式服務所收集的資料，均受各自的條款及政策所規範。

而在可傳輸資訊的第三方類型中，關於「廠商、服務供應商及其他合作夥伴」項目則做出了如下的規範¹⁸：

我們將資訊轉移給在全球為我們提供支援的廠商、服務供應商及其他合作夥伴，例如提供技術基礎架構服務、分析我們服務的使用方式、衡量廣告和服務的成效、提供顧客服務、讓付款流程更順暢或進行學術研究和調查。這些合作夥伴必須嚴格遵守符合此資料政策的保密義務，以及我們與其所簽訂的協議。

依據Facebook於2016年訂定之此版本資料政策規範可發現，其所能與第三方分享之資料範圍顯然相當廣泛。由此可見在對於廠商、服務供應商與合作夥伴之部分，資訊轉移並沒有其他的限制在內；當2016年版本的資料政策都充斥如此寬鬆的規定時，雖目前網路上無法取得先前之版本，但可以想見其應遠較現行版本資料政策更為寬鬆。而本案中GSR之所以可獲得大量的個人資料，即是利用Facebook相當寬鬆的資料政策，並假借了學術研究作為目的。據此，倘若依據加州線上隱私權法規範，Facebook似乎在本次個人資料洩漏事件中，得以逃脫美國法律所賦予之責任，使用者將陷入嚴峻的訴訟程序與舉證責任中；換言之，本文認為本案中就非公開個人資料部分，縱或Facebook涉有保護個人隱私不力之虞，但倘就其所制定之隱私權政策而論，使用者就Facebook違約並造成隱私侵犯之法

¹⁸ 前揭註 1。

律主張得成立之空間並不大，縱或有得以主張之空間，但使用者勢必會陷入相當嚴苛、困難之訴訟舉證責任中。

另一方面，Facebook並非第一次出現此等重大的隱私權爭議，而是向來在隱私權上就一直為人所詬病，美國聯邦貿易委員會（Federal Trade Commission, FTC）亦發現Facebook在隱私權方面所造成之疑慮係現有的法令不足以規範者，因此於2011年即對Facebook進行調查，並於同年11月與Facebook簽署了一份協議¹⁹，對Facebook之隱私權相關事宜進行規範。其中協議之第一部分要求Facebook必須清楚說明既有之准許第三方取得之個資、由第三方提供之隱私權與資訊保護之檢驗等；協議第二部分中，Facebook則被要求必須於事前清楚的向使用者說明，向第三方揭露之使用者非公開個資種類、作為揭露對象之第三方的資訊或特定類別，及此種向第三方揭露與使用者隱私設定之關係，並應取得使用者之同意等規定。協議之第四部分則要求Facebook必須制定並維護合理的隱私計畫，針對現有及發展中的產品、服務，以確保個人資料的隱私及保密。

據此，Facebook所提供的隱私權政策，是否符合其與交易委員會所簽訂的協議，可能是有疑慮的。由Facebook所提供的隱私政策說明觀察，使用者僅能得知Facebook會大量的、全面的傳輸各種個人資料，給予不同、多種的合作對象，但不能真正得知個人資料揭露對象的種類，更遑論揭露對象的實際身分，亦不可能確定哪些揭露對象會獲得哪些個人資料。因此很難認定Facebook之隱私權政策完全符合與FTC協議之要求，亦造成FTC對於Facebook產生訴訟之空間；事實上，FTC已經著手調查Facebook本次個資事件，評論者也大多認為FTC是Facebook平安度過國會聽證之後最大的挑戰²⁰。

但FTC是否真的會對於Facebook造成嚴重的損失或打擊，本文採取保守的看

¹⁹ FTC, Agreement Containing Consent Order, 2011.11.29, available at:

<https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>, last visit: 2018.03.31.

²⁰ Katy Steinmetz, Mark Zuckerberg Survived Congress. Now Facebook Has to Survive the FTC, TIME, available at: <http://time.com/5237900/facebook-ftc-privacy-data-cambridge-analytica/>, last visit: 2018.04.15.

法。FTC目前處理消費者隱私議題，係依據聯邦貿易委員會法禁止「商業中或影響商業的不公平欺罔行為」方式加以處理，將未經通知而蒐集個人資料、未清楚而顯著方式提供隱私政策、違反個人資料蒐集利用揭露政策，及溯及既往變更隱私政策等案例加以起訴²¹。但FTC提起訴訟的相關案件中，幾乎所有案件均撤回或與當事企業達成和解，僅有極少數案件獲得法院裁判²²；因此在此種狀態下，加以Facebook對於一般消費者採取免費政策，以及本案中並非Facebook主動將個人資料傳輸與GSR，而係被動的由GSR進行個人資料之蒐集，因此最終FTC調查結果使否致使Facebook產生大規模賠償或罰鍰義務，本文採較為保守的看法；亦即，本案爆發後Facebook勢必被迫調整其關於個人隱私的設定、政策無疑，但應不致被迫產生大規模賠償或罰鍰，縱有賠償或罰鍰亦應為小規模為是。

（三）關於GSR及劍橋分析取得Facebook上使用者個人資料

但於GSR與劍橋分析取得Facebook上使用者個資一事，則可能有完全不同的法律效果。GSR與劍橋分析公司均係設立於英國之企業，因此除美國法對於隱私權之規範外，尚應該考慮英國法對於個人資料之規範，已如前述，則首先即就美國法針對此案可能發生之作用加以檢討。就美國法而言，由於其對於個人資料之態度係以隱私權概念規範已如前述，因此GSR與劍橋分析公司取得未使用應用程式“thisisyourdigitallife”之使用者的公開資料，並不會造成隱私權之侵害，此部分與前揭說明相同；問題在於取得未使用其程式使用者之非公開資料，可能構成對使用者之隱私權侵害。亦即基於隱私權之概念，使用者非公開個人資料係屬於使用者有意保留於私領域且受一般認可，具有合理隱私期待之隱私權保護範疇，GSR與劍橋分析取得利用此等資料係屬於對隱私權之侵犯。

對於GSR與劍橋分析最為有利之說法，應當係依Facebook使用者隱私權政策之規範，Facebook有權將該等非公開資料交付與第三方，因而，GSR與劍橋分析

²¹ 前揭註 11，頁 212-215。

²² 前揭註 11，頁 216。

公司，得據以主張獲得使用者非公開個人資料，係經過使用者概括性同意而未造成隱私權侵害。但此種說法是有爭議的！首先在於Facebook的隱私權政策，如前揭說明，並未能清楚的看出其要交付的資料範圍與交付的對象為何，很難認定GSR與劍橋分析於此是屬於使用者概括同意的交付對象，同時本案中是將個人資料用於政治用途的分析，屬於一般個人資料法制下敏感資料之部分，更使得使用者是否真正具有授權使用之意圖產生疑慮。第二，本文中Facebook主張係由GSR違規使用個人資料所致，更可以認定Facebook方面認為GSR與劍橋分析係違背了其與Facebook間之協議而使用該等個人資料，因此該主張獲得授權使用難有法律上正當性。

但問題在於美國法體系下，對於GSR及劍橋分析兩公司是否具有有效之制裁方式？首先GSR已經解散，因此縱然認定其取得使用者非公開個人資料違反隱私權，使用者亦發生求償無門的狀態。而劍橋分析公司部分，雖因被認定違反隱私權保護而得作為求償之對象，但美國法下隱私權之侵害，除非如同Facebook一般與FTC訂有協定，否則係由被侵害者自行訴訟向侵害者求償。因此本文中使用者需自行承擔對劍橋分析的跨國訴訟，並舉證個資受劍橋分析使用後所產生之損害及因果關係。對此本文認為，縱然採取集體訴訟方式處理本案，本文中受侵害之使用者要證明損害之存在可能是一件非常困難的任務，理論上雖然可以認定劍橋分析違法侵權，但訴訟實務上可能最終無法獲得制裁之效果。

但於英國法的規範下，即可能有大不相同之結果。依據英國之資料保護法案（Data Protection Act 1998, DPA）第1部分第5條1項(a)規定，凡設立於英國境內的資料管理者均受英國DPA之規範，而劍橋分析與GSR均設立於英國境內，因此應受該法之管轄。其次依據該法第1部分第7條1項(a)之規定，資料當事人有權於資料被個資管理者進行處理時獲得通知；再者，本次GSR蒐集並交付劍橋分析使用之個人資料，均屬於第1部分第1條第1項中所稱之資料（Data）與個人資料（Personal Data），關於政治取向這部分甚至是第2條(b)所規定之敏感性個人資料；

而違反DPA之結果，依據第1部分第60條(2)之規定係可被處以罰款。亦即無論GSR與劍橋分析所取得者究竟係公開或非公開個人資料，於英國DPA之規定下，其均有向個資當事人為告知之義務，然於本案中此二公司並未向個人資料當事人為告知即處理利用個資，明顯係違背英國資料保護法案之規定而得已被英國政府所追訴處罰。

據上述，如果GSR與劍橋分析確實使用了Facebook上的個人資料，違反英國DPA規範之可能性相當的高。而Facebook也已經開始對劍橋分析是否使用了Facebook所持有之個資進行調查²³，但問題在於英國政府會否就劍橋分析違法使用Facebook個資一案加以裁罰？英國政府於3月底起，已經對於劍橋分析違法使用Facebook個資一案進行調查²⁴，但其著重的案件在於英國脫離歐盟公投一案；而劍橋分析雖違法使用5000多萬，甚至8300萬之使用者個人資料，但絕大部分使用者均為美國公民，屬於英國公民比率並不高；此等前提下，英國政府對於劍橋分析會採取多大的打擊力度，可能並非單純是法律問題而是政治議題。

(四) 於歐盟一般資料保護規則下法律適用之可能狀態

歐盟將於2018年5月25日起實施之一般資料保護規則（General Data Protection Regulation, GDPR），依據此一規定，則Facebook案可能有不同之結論。依據GDPR之規定，對個人資料並非以隱私權概念加以理解，GDPR並不區分公開或非公開之個人資料，而係以不同程度之規範均加以保障；依據GDPR第14條2項²⁵之規定，蒐集、處理非經由當事人而取得之個人資料時仍應該向當事人履行告知義務，且其中必須告知當事人個資取得來源及是否由公開來源取得，足見歐盟GDPR並不因個人資料已經被公開而免除資料處理者對個人資料當事人之責任；

²³ 中央通訊社，Facebook 個資外洩爭議 劍橋分析成風暴核心，2018.03.20， available at: <http://www.cna.com.tw/news/aopl/201803200401-1.aspx>，last visit:2018.03.31。

²⁴ 中時電子報，劍橋分析 曾介入英脫歐公投，2018.03.25， available at: <http://www.chinatimes.com/newspapers/20180325001105-260108>，last visit:2018.03.31。

²⁵ GDPR Article 14(2), available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L .2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC>，last visit:2018.03.31。

換言之，縱或係於公開來源取得個人資料而非向個資當事人直接收集，於GDPR之規範下亦應向個資當事人為告知，並說明係由何種公開來源取得其個資。詳言之，GDPR並非將個人資料視為隱私權之一環予以保護，而係將個人資料本身視為一種當事人之基本權²⁶，或者說其係將個人資料視為當事人人格形成之人格權一環加以保護。

按上述，本案中GSR於Facebook上蒐集未使用心理測驗“thisisyourdigitallife”之其他使用者之公開個人資料，雖該資料係由作為個資當事人之Facebook使用者自行設定為公開狀態，但GSR蒐集個資後未向個資當事人告知，仍屬未盡對當事人之告知義務，違反GDPR第14條規定；其未獲個人資料當事人同意而進行個資處理，亦違反GDPR第6條關於個資處理要件之規定；再者本案中劍橋分析向GSR購買個資後進行處理一事，亦為未盡告知義務而違反第14條規定，且未取得當事人同意的處理個資，仍屬違反GDPR第6條規定之情形。

進一步，倘涉及非公開個人資料時，GSR與劍橋分析違反GDPR之情形可能更加嚴重。由於GDPR並不區分公開與非公開個人資料，所以GSR與劍橋分析對於非公開個人資料之蒐集與處理，亦如同前述的違背GDPR之規定無疑，但對於非公開個人資料之處理，可能另行違背GDPR關於敏感個人資料處理之程序規範。按照GDPR第9條第1項之規定，種族或民族出身、政治觀點、宗教信仰、哲學思想、工會會員身分、基因資料、生物識別特徵、關於健康之資料、關於性生活或性傾向之資料等均係屬於敏感個人資料²⁷，雖然尚未有證據明確得知GSR與劍橋分析所蒐集之個人資料範圍，但既然劍橋分析處理個資之目的係欲用於投放影響政治選擇之廣告，則有相當高度之可能性會涉及上揭敏感個資之範疇。依據該項規

²⁶ GDPR Article 1(2), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC , last visit:2018.03.31。

²⁷ GDPR Article 9, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC , last visit:2018.03.31。

定，此等敏感個人資料原則上禁止被處理利用，除非合乎同條2項所規定之特定目的或要件。而該條2項(a)款至(j)款所規定之特定目的，基本係以公共利益、公共衛生、維護當事人重大基本權利、司法權行使等較具公益性目的為主，而非屬此等公益性質之合法處理要件，僅有「經當事人特別同意」及「當事人自行公開」二者。於此，對於公開之敏感個資，GSR與劍橋分析尚可主張係由當事人自行公開而合乎敏感個資之處理要件；但非公開之敏感個資部分，即有高度可能屬於違反GDPR關於敏感個資之規範的違法個資處理。

關於Facebook方面而言，倘若Facebook將此個人資料視為係GSR與劍橋分析不當的取得，縱或Facebook免於GDPR規範內身為個人資料管理者將個人資料向第三人揭露之告知義務；然根據GDPR第33條、34條之規定，Facebook此時會發生向個人資料保護主管機關通報，及向個人資料當事人告知之義務。²⁸而其中向主管機關之通報義務最遲需於事件發生後72小時內為之，對當事人之通知雖然並未明確規定期限，但條文要求係「無遲延（without undue delay）」的向當事人為通知。於此觀之，Facebook於事件發生後並未向任何主管機關通報，也並未向任何使用者為通知，直至本次事件因Christopher Wylie向媒體爆料而爆發之後，始有向個資洩漏疑慮之使用者為通知，明顯與GDPR之規範有悖。但必須再次強調的，GDPR於2018年5月25日方才正式生效施行，而本案之發生係於2014至2015年間，基於法律不溯及既往原則，因此GDPR之規定並無法適用於本案，僅得做為參考而不能據以要求Facebook、GSR或劍橋分析承擔GDPR所規定之法律責任。

四、結論

就最終結論而言，本文認為在美國法寬鬆地將個人資料視為隱私權一環加以保護的狀態下，Facebook本身透過其隱私權政策，有相當高度可能於本案中免於使用者、FTC的求償，或者以相對低廉的價格與使用者或FTC達成和解。至於GSR

²⁸ GDPR Article 33, 34, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L .2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC> , last visit:2018.03.31。

與劍橋分析兩公司部分，其利用使用者公開之個人資料部分，雖不違背美國以隱私權概念對個人資料之保護，但就此二公司因設立於英國而必須遵守英國法之部分，係違背英國資料保護法案之規定；就非公開資料之部分，兩公司使用Facebook上使用者非公開資料，雖有侵害使用者隱私權之可能，但因美國法對於隱私權寬鬆的規範，導致使用者在向此二公司求償上會產生制度性的困難，至於英國法的部分雖可透過DPA之規範對此二公司為追訴，但由於主要受害使用者為美國國民，英國政府是否會強力追訴尚屬政治性議題而不可知。行文至此，復又有劍橋分析進行清算解散之消息傳出²⁹，於此狀態下，將致使英國政府對於劍橋分析的調查嚴重受挫（雖英國政府表示仍會持續調查並追訴，資訊委員辦公室（Information Commissioner's Office, ICO）亦有相關調查動作³⁰），但最終是否能於劍橋分析解散的狀態下找到最後負責的自然人，可能仍屬未定之數。

無論如何，在GSR與劍橋分析均解散的狀態下，加以Facebook又主張係此二者違反與Facebook間的使用條款違法的使用個人資料，要追究Facebook於法律上的責任可能是相當困難的，換句話說，Facebook在法律層面可能已平安度過本次個人資料洩漏的風暴，縱或Facebook受美國或英國政府處罰，該處罰之嚴重程度亦應極為有限；剩餘的問題應是即將實施之歐盟一般資料保護規則（GDPR）會否因此次個資洩漏事件，將更多的注意力放在Facebook上，以確保Facebook將來之個人資料政策不會再次導致類似的大規模資料盜用或外洩事件；另一方面在於全球使用者對於自身個人資料的重視程度所造成之壓力，是否足以促使Facebook這個全球最大的社群網站企業重視其個人資料政策，修正其利用個人資料的方式以及政策；以及最終此次事件，能夠令其他握有大規模個人資料的企業，如Google、Apple何種的啟示，使其尊重個人資料之權利以及避免類似事件的再次發生。

²⁹ 中央社，《劍橋分析生意毀滅：立即停止所有營運》，2018.05.03，available at: <http://news.ltn.com.tw/news/world/breakingnews/2413894>，last visit: 2018.05.06。

³⁰ 麥浩禮，《不是聲請破產就沒事了 英國下令劍橋分析 30 日內交出美國選民數據》，上報，2018.05.06，available at: https://www.upmedia.mg/news_info.php?SerialNo=40253，last visit: 2018.05.06。