國立交通大學

科技法律研究所

碩士論文

行動應用程式的個人資料保護——公開透明原則的強化與本國實證研究

Personal Data Protection and Mobile Applications Practices on Smart Devices: Empirical Study and Transparency Principle Reinforced

研究生：鄭忻忻

指導教授：王立達　副教授

中 華 民 國 一○三 年 一 月

行動應用程式的個人資料保護—

公開透明原則的強化與本國實證研究

研 究 生：鄭忻忻　　Student：Hsin-Hsin Cheng

指導教授：王立達　　Advisor：Dr. Li-Dar Wang

國 立 交 通 大 學

科技法律研究所

碩 士 論 文

A Thesis

Submitted to Institute of Technology Law

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Law

January 2014

Hsinchu, Taiwan, Republic of China

中 華 民 國 一○三 年 一 月

行動應用程式的個人資料保護—公開透明原則的強化與本國實證研究

學生：鄭忻忻　　指導教授：王立達

國立交通大學科技法律研究所碩士班

摘　　要

智慧型裝置的普及，讓行動應用程式逐漸成為日常生活中不可或缺的重要工具，這也使行動應用程式不當蒐集、使用和揭露使用者個人資料的情形，更加引起社會關注。而行動應用程式的功能日趨多元，以及上下游供應鏈多重的個資蒐集處理業者，使得可能存在的個人隱私侵犯愈發複雜與嚴重。本文以行動應用程式的產業運作實況切入，從個人資料保護的目的與種類出發，分析行動應用程式對個資影響的深度和廣度。由於我國對行動應用程式招致的隱私議題，尚無明確的法律政策，本文藉由比較法分析途徑，針對歐盟與美國主管機關、以及國際組織在 2013 年先後發表的行動應用程式隱私保護意見書與規範建議，進行政策的比較研究。此外，透過問卷調查我國民眾對行動應用程式的隱私意識，以及目前行動應用程式產業提供的隱私通知之效度，作為本文提出政策建議的基礎。最後，針對現今各國通用的「通知和同意（notice and consent）機制」在實際運作上所面臨的難題，以及我國個人資料保護法在行動應用程式議題上所面臨的困境，本文亦逐一加以剖析，並且研擬可能的因應對策與解決方案。

關鍵字：行動應用程式、智慧型裝置、個人資料保護法、行動隱私、通知和同意

Personal Data Protection and Mobile Applications Practices on Smart Devices: Empirical Study and Transparency Principle Reinforced

Student：Hsin-Hsin Cheng　　Advisors：Dr. Li-Dar Wang

Institute of Technology Law
National Chiao Tung University

ABSTRACT

Smart devices and mobile applications (apps) are increasingly indispensable to modern people. When users operate their smart devices and apps, however, they share a variety of personal information with a multitude of known or unknown players, which significantly raises the public's concerns on possible privacy invasion. How to protect user's mobile privacy thus becomes a timely issue. This thesis explores how apps collect personal data, which type of data is collected, and why those practices impose risks on user's personal privacy. The thesis further analyze the opinions and staff reports of the European Union, United States and International Governmental Organizations newly published in 2013, and find that the notice-and-consent mechanism remains a primary regulatory measure in securing mobile privacy. As identifying the key rule of transparency, the thesis makes an empirical study survey Taiwanese mobile apps user how their attitude and awareness toward current notice-and-consent mechanism and mobile privacy. Basing on the result of the survey, the thesis concludes the deficiencies of notice-and-consent mechanism and present an alternative approach to enhance the efficacy of privacy notice. On those bases, this thesis critically reviews Taiwan's Personal Information Protection Act and other regulation pertinent to mobile privacy protection, and propose feasible resolutions to contemporary mobile privacy issues in Taiwan.

Keywords: Mobile applications, Smart devices, Personal Information Protection Act, Mobile privacy, Notice and consent.

誌　　謝

寫論文就像經歷一趟奇幻旅程，裡面有說不完的故事和道不盡的感謝。能夠來到寫謝辭的這一刻，都要謝謝師長、親友、和家人的支持與打氣。

對於指導教授王立達老師的教誨，難以言喻我心中的感謝。在我心目中，老師就像帥氣版的哆啦A夢，隨時能夠掏出各式厲害的法寶，協助我跳脫卡關，繼續前進。在寫論文的過程中，最喜歡閱讀老師寄給我的信。信中除了逐字逐句批閱後的論文檔案和論點的討論與導正外，更常出現的是暖暖的字句和滿滿的打氣，讓我保持對論文的興趣和信心。

謝謝口試委員王明禮老師和劉定基老師，兩個小時的口試就像是上了一堂課。老師們以宏觀的角度，提示我思考的盲點，更啟發我對行動隱私和個資法的許多想法。謝謝王明禮老師在口試過程中，引領我觸及通知和同意機制困境的癥結，與了解隱私保護的多重面向與矛盾。謝謝劉定基老師，惠准我旁聽資訊隱私法課程，指點我可以閱讀或參考的資料，更在口試中，協助我能精緻化、深化論點的論述與討論。口試後老師們細細批閱的口試本，對我而言是最好、最重要的禮物。

謝謝交通大學科技法律研究所老師們、所有授課的老師與法院實習指導法官：賴英照老師、許玉秀老師、劉尚志老師、倪貴榮老師、王敏銓老師、林志潔老師、陳銘雄老師、林建中老師、陳在方老師、林欣柔老師、林三元老師、吳巡龍老師、邱忠義法官、楊雅清法官。謝謝您們以身教、言教，教導我學術研究的態度與對社會正義的關懷。

謝謝科法所所辦每一位助理：以欣助教、珮瑜助教、玉珮助教、嫚君助教、莉雯助教、和嘉陽助教，謝謝您們在研討會、課程或者各種行政事項，總是伸出援手，幫助我安然度過研究所的每一天。

在科法所的五個學期中，謝謝所有照顧我的學長姐、同學與學弟妹們。謝謝王俊雯學姊、呂書瑋學長、郭政雄學長、簡儀婷學姊、陳師敏和達門的大家，傳承、交流論文的經驗與心得，協助我釐清論文的論點與疏忽的細節，十分珍惜互相打氣、切磋的革命情感。科法所所有一起共同修課的專班／碩班學長姐們，謝謝您們不吝分享人生經驗，給予最中肯的開導。科法所100級的同窗們，能和優秀的你們一同學習是我的榮幸，因為有你們，科法所研究生活如此多彩繽紛、充滿歡笑。謝謝所狗多芬，總是願意離開溫暖的轉角小窩，陪我走過黑黑的走廊和傾聽秘密。

謝謝好朋友們，無論是失意得意，我們總是給彼此建議與關懷。最喜歡和你們一起思辯、一起成長；最喜歡和你們一起聽音樂、一起看展覽；也最喜歡和你們一起享食、一起玩樂，用我們的哈哈大笑，共譜青春樂章。

特別銘謝協助問卷作答的受訪者們，因為您們耐心、詳實地填答，幫助我能更具體地描述現階段行動隱私面臨的挑戰與難題。

最後謹以這本論文，向家人獻上最深摯的愛與感謝。感謝爸爸鄭定維先生、媽媽濮文雅女士這26年來的呵護、養育和栽培，陪我走過人生的每一步，永遠以我為榮。謝謝弟弟鄭光佐，你的窩心與陪伴是我最大的安慰。

目錄

表格目錄

圖表目錄

一、 緒論

1.1. 研究動機和研究目的

在公共場所中無處不見到人們低頭注視著手中的螢幕，手指不斷上下左右滑動，藉由不同功能的行動應用程式滿足不同的需求，諸如傳送訊息、玩遊戲、看影片或導航、甚至是購物等。尤其在筆者購買智慧型手機後，更深刻感受到智慧型手機和行動應用程式的魅力與影響力，和同儕間互相交流要下載哪些有用的應用程式，無論是好玩的遊戲類應用程式、具有社群交流功能的應用程式、甚至是督促自己完成進度的 To Do List 應用程式等。每一次安裝行動應用程式時，螢幕上會顯示該行動應用程式的隱私權政策（假如有的話）、須要授權的項目，其中在授權項目中，往往會列出該程式會蒐集使用者哪些個人資料。雖然每一個授權項目下，都會有簡要的說明和名詞解釋，然而大部分的術語均非筆者得以理解。此外，有時下載某一工具型態的應用程式，該程式卻要求蒐集多種個人資料，筆者亦無法看出該程式的功能和所欲蒐集的個人資料間存在的連結與關係，而造成困惑與疑問。同時，當行動應用程式安裝的數量漸增，筆者亦開始思考智慧型裝置[1]在扮演使用者完美助理和玩伴的同時，是否也同時扮演最佳臥底，將我們的個人資料穿過雲端傳給行動應用程式業者和其他相關業者，進而對我們的隱私造成侵擾？

美國與歐盟在 2013 年初，均公布行動應用程式隱私保護的建議報告，並且無獨有偶，兩者均以通知和同意（notice and consent）[2]機制作為制度建議核心，並以隱私通知（privacy notice）或隱私權政策（privacy policy）的揭示，作為加強隱私操作揭露的主要解決手段[3]。一般而言，隱私通知是較簡短的隱私聲明，而

---

1 智慧型裝置（smart device），又稱行動裝置（mobile device），包含智慧型手機、平板電腦等，以筆記型電腦、個人數位助理器 PDA、及功能型行動電話整合，可獨立運行獲悉互搭配已完成服務的設備。林建廷、李元生，行動商務概論實務與應用，頁 2-2（2012）。

2 有部分文章將 Notice and Consent 譯為「通知後同意」，可將通知和同意的關聯強化，固然有其道理。然本文考量「通知後同意」的譯法，似乎意味著同意才是主要義務，通知只是協助其發揮效用的附帶前提；惟就個人資料保護而言，通知和同意乃是業者必須同時履行的義務，且如何有效地對行動應用程式使用者進行通知，才能兼顧消費者充分理解及不過度繁冗，已經成為本議題當今討論焦點之一，其與同意之重要性，應該等量齊觀。是故，本文將 Notice and Consent 直譯為「通知和同意」，特此說明。

3 國際隱私專家協會（International Association of Privacy Professionals）對隱私通知和隱私權政策有定義有所區別，認為隱私通知是對外告知資料當事人的聲明，用以描述機關如何蒐集、使用、保存和揭露個人資料。隱私通知有時會以隱私聲明、公正處理聲明（fair procedure statement）或隱私權政策的方式呈現。隱私權政策則是機關內部的聲明，用以指示員工如何蒐集、使用個人資料，以及資料當事人的法定權利。換言之，國際隱私專家協會隱私權政策具有兩種意涵，對外的隱私通知，以及業者內部的隱私操作指引。然而本文以為大部分的隱私權政策皆為機關對外的聲明，希冀透過隱私權政策告知資料當事人業者隱私操作的內容，因此於本論文中，隱私權政策和隱私通知均為對外的聲明，作為揭露機關隱私政策的方法。*About the IAPP*, IAPP, https://www.privacyassociation.org/about_iapp/ (last visited Aug. 18, 2013); *Glossary*, IAPP, https://www.privacyassociation.org/resource_center/privacy_glossary/#P (last visited Aug. 18, 2013).

隱私權政策則是以類似法律文件的方式呈現。以下為方便討論，將以「隱私聲明（privacy statement）」作為隱私通知和隱私權政策的統稱，僅於隱私通知和隱私權政策因為呈現方式有別，而須特別說明時，才分別以隱私通知或隱私權政策表示，合先敘明。然而隱私聲明應該具有何種內容？通知和同意與隱私聲明等解決措施，對於終端使用者和行動應用程式相關業者分別有何影響？是否足以發揮保護使用者隱私權的效果？我國在個人資料保護法大幅修正之後，又應該採取何種措施，以保護使用者的行動隱私？由於以上議題不僅關係到個別人民的基本人權保護，更攸關行動科技與行動商務的未來發展，筆者試圖透過本篇論文解析此等問題。

1.2. 研究範圍與研究方法

本文的研究範圍著重於，一般行動應用程式產業進行蒐集、利用、處理和傳輸使用者個人資料的行為時，應如何保護使用者的隱私與個人資料。由於絕大部份的應用程式產業業者為非公務機關，因此本文的研究範圍僅處理非公務機關透過行動應用程式蒐集、利用、處理和傳輸使用者個人資料的情況。此外，行動應用程式除了一般生活日常用途外，更為醫學界做為遠距醫療的工具和管道，惟此類型應用程式涉及患者的病情與健康隱私，隱私保護的密度遠高於一般類型的個人資料，為能聚焦於一般應用程式適用個人資料保護法的情況，本文並不會討論行動應用程式在遠距醫療應用下，所涉及的隱私議題。再者，由於兒童的隱私保護目的不同於一般使用者，隱私保護的密度也不同，因此本文著重於一般使用者使用行動應用程式的情形。

本文主要的研究方法為文獻分析法、比較法分析途徑、以及實證量化研究。首先，藉由回顧專書、論文、期刊文章、我國與外國相關函令、報告與意見書以及報章新聞等現有文獻，強化問題意識與建構論文脈絡。由於我國對行動應用程式招致的隱私議題，尚無明確的立場和態度，因此藉由分析歐盟、美國聯邦交易委員會、美國加州司法部、其他國家、乃至於國際組織在行動隱私所發表的報告與意見書，以了解各國對於行動隱私的立場與採取的政策。最後，由於國家對隱私採取的政策與管制途徑，須與人民的隱私意識與態度相符，因此本文透過問卷調查民眾對行動應用程式的隱私意識，並調查目前行動應用程式產業提供的隱私通知之效度，作為本文提出政策建議的基礎，以期與我國國民對行動隱私的態度相一致。

1.3. 論文架論

本論文共計七章，第一章為緒論，說明本文研究動機、問題意識、研究範圍與研究方法。第二章為行動應用程式與個人資料保護，從一般商業應用與消費型行動應用程式切入，說明並探討行動應用程式對於個人資料處理現況下，個人資料保護的目的與種類。第三章，筆者透過比較法分析，主要研究歐盟和美國現今個人資料保護政策，以及對行動應用程式侵犯個人隱私的因應對策。此外，由於

行動網路無國界，各國的個人資料保護法規事實上均帶有域外效力，本部分亦將簡要論及國際合作保護面向。第四章透過量化研究，探討我國民眾使用行動應用程式的隱私意識調查，作為提出政策建議的背景與基礎。第五章則是針對現行各國通用的通知和同意（notice and consent）機制，探討其所面臨的現實挑戰以及可能的解決途徑。第六章，本文總結以上討論，回歸我國相關法律規範，以行動應用程式與行動隱私保護作為關注焦點，詳細檢視我國個人資料保護法目前所遭遇的困境，並且提出可資因應的修法或立法建議。第七章為結論，綜合前述研究成果，提出本文結論。

二、 行動應用程式與個人資料保護

行動應用程式（applications, 簡稱 apps.）係指為完成某項或多項特定工作的電腦程式，以智慧型裝置作為其載體，內容五花八門，包含通訊、娛樂、購物與即時資訊等各種功能，乃為行動商務的具體體現。業者藉由行動應用程式與服務的供應，可從中蒐集使用者高度私密個人資訊（highly personal information），包含位置、通訊錄、照片、訊息、電子郵件、社群關係、行事曆、乃至購物習慣等，招致侵犯使用者隱私的疑慮[4]。行動應用程式下載至使用者的智慧型裝置之後，不僅可能蒐集使用者的個人資料，還可能連帶蒐集與使用者有聯繫的其他人個人資料，影響層面相當廣泛[5]。

行動應用程式在當前行動商務運作過程中居於相當核心之地位。行動商務係利用行動通信裝置，透過行動通信網路結合網際網路，以從事具有「即時性」及「移動性」的各種電子商務[6]。為滿足使用者各式需求，現今行動商務的內容變得愈發多元。如何透過網際網路與行動通信裝置，進行多樣性的行動商務活動，貼近消費者的使用情境，提供所需要的各種即時服務，便有賴行動應用程式作為使用者之工具與橋樑，使其能夠透過前述通訊平台迅速有效地滿足其需求。因此行動應用程式之效能與可親性，即成為行動商務是否成功的關鍵之一。而行動應用程式之人機介面和功能設計能否吸引消費者，以及操作上是否流暢好用，可否充分發揮智慧型裝置的特性，也成為行動商務業者彼此競爭的重要戰場[7]。惟在業者提供行動服務的同時，往往亦廣泛蒐集使用者的個人資訊，而有侵害使用者者個人資料之疑慮[8]。本部分將探討行動應用程式業者蒐集使用個人資料帶來的隱私侵害，綜合分析目前常見的個人資料蒐集種類與隱私聲明的內容，並且從使用者與業者雙方觀點，討論其可能的隱私侵害與利益衝突。

---

4 *June 2012 FPF Mobile Apps Study*, FUTURE OF PRIVACY FORUM, 1 (2012), http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf (last visited Nov. 29, 2013).

5 Larry Magid, *App Privacy Issues Deeply Troubling*, THE HUFFINGTON POST, Feb. 21, 2012, http://www.huffingtonpost.com/larry-magid/iphone-app-privacy_b_1290529.html; *What They Know – Mobile*, THE WALL STREET JOURNAL, http://blogs.wsj.com/wtk-mobile/ (last visited March 30, 2013).

6 董顯康，「行動商務廣告中資訊隱私之研究」，國立臺灣大學國家發展研究所碩士論文，頁 15（2011）。

7 參考鄭逸寧，成功的企業 App 必須貼近使用情境，達到使用者、裝置、周遭環境、網路之間的互動效果，並有效解決使用者面臨的問題，iThome，http://www.ithome.com.tw/itadm/article.php?c=73463&s=1（最後瀏覽時間：2013 年 8 月 11 日）。*See* Jeremy Olson, *How To Succeed With Your Mobile App*, SMASHING MAGAZINE, Nov. 7, 2012, http://mobile.smashingmagazine.com/2012/11/07/succeed-with-your-app/ (last visited Nov. 29, 2013).

8 *See* Hayley Tsukayama, *California attorney general warns app makers over user privacy*, THE WASHINGTON POST, (Oct. 30, 2012), http://www.washingtonpost.com/blogs/post-tech/post/california-attorney-general-warns-app-makers-over-user-privacy/2012/10/30/33ac9afc-22cd-11e2-8448-81b1ce7d6978_blog.html?wpisrc=nl_tech (last visited Nov. 29, 2013).

2.1. 行動應用程式產業簡介

2.1.1. 行動裝置簡介：特性和限制

行動裝置（mobile device），又稱智慧型裝置（smart device），包含智慧型手機、平板電腦等，以筆記型電腦、個人數位助理器 PDA、及功能型行動電話整合，可獨立運行或互搭配以完成服務的設備[9]。行動裝置有以下的特性[10]：

(1) 個人專用：

高度個人化的行動裝置設定，例如電話簿的名單、下載所需要的應用程式、以及建立自己使用行動裝置的習慣。

(2) 便於攜帶：

行動裝置是比個人電腦或筆記型電腦更貼身、私人的裝置，使用者可以帶著行動裝置到處走，並可以儲存許多私人的資料在裝置中。尤其是行動裝置通常都是可塞入口袋的大小，幾乎是使用者走到哪，手機就跟到哪。

(3) 多元功能：

行動裝置除了可以利用應用程式，提供傳統手機的通話功能或傳文字簡訊的功能外、打字與他人溝通外，亦可利用視訊等方式與他人對談。此外，除了通訊的功能外，行動裝置還有照相、錄影音、導航、閱讀電子書和瀏覽網頁等功能。

縱使行動裝置的運算能力，猶如一台小型、輕便的個人電腦，可隨著搭載不同的應用程式，而加強行動裝置的功能性與實用性。然而行動裝置具有以下二種主要的限制[11]：

(1) 小型螢幕（Small Screen Size）：

螢幕僅能呈現少量的內容，若字體過小或內容過多，會造成使用者沒有興趣閱讀（unreadable）。因此行動應用程式或者行動網頁，必須盡可能將大量、豐富且複雜的資訊，簡化成使用者可在行動裝置上閱讀的形式，並以使用者眼睛可接受的呈現方式[12]。

---

9 林建廷、李元生，前揭註 1，頁 2-2（2012）。

10 整理自恰克．馬丁，許瑞宋譯，決戰第三螢幕——隨時、定位、互動、行動時代緊貼顧客的行銷與消費新模式，頁 21-24，33-79，68（2011）。

11 *See* P. CANDACE DEANS, E-COMMERCE AND M-COMMERCE TECHNOLOGIES 32-55 (2005); *see also* ANDROMEDA YELTON, BRIDGING THE DIGITAL DIVIDE WITH MOBILE SERVICE 15-16 (2012).

12 *See* B. Karstens et al., *Presenting Large an Complex Information Sets on Mobile Handhelds*, in E-COMMERCE AND M-COMMERCE TECHNOLOGIES 32, 32-55 (Mehdi Khosrow-Pour ed., 2005); *see also* Steven Sanderson, *Build a Better Mobile Browsing Experience*, MSDN MAGAZINE, July 2011, at 74.

(2) 只能手滑，沒有滑鼠和鍵盤（No Mouse or Keyboard）：

使用者須透過手指點擊（click）或滑動頁面，來閱讀網頁或行動應用程式的內容，這與使用者以滑鼠點擊電腦的瀏覽模式稍微不同。因為手指相較於滑鼠，無法精確地將手指指尖停留在某個連結按鈕(button link)上，進而加以點擊(hover model) [13]。

綜前所述可知，由於行動裝置的限制，行動網頁或行動應用程式業者，在呈現提供的服務和內容時，需要進行調整，讓使用者得以閱讀或方便操作。除此之外，從前述的特性可得知，使用者會透過行動裝置、行動裝置配備的程式以及使用者下載的應用程式，得以便利地處理生活上或商務上的事務。

2.1.2. 行動應用程式供應鏈：上、中、下游產業關係

在智慧型裝置上參與提供行動應用程式給消費者使用、蒐集利用消費者個人資訊的行動商務業者，並不單單只有行動應用程式開發商(application developer)，除此之外還包含行動設備製造商（device manufactures）、作業系統商（operating system）、行動應用程式商店（程式平台業者，app store），以及第三方業者，比如資料分析業者和廣告業者。首先，設備製造商會在設備中裝置多種不同的感應器，包含陀螺儀(gyroscope)、數位式羅盤(digital compass)、加速計(accelerometer)、照相機（camera）、麥克風（microphone）等[14]，這些感應器都可以用以蒐集個人資料。智慧型裝置的作業系統則可藉由行動應用程式介面（Application Programming Interfaces, APIs）接收這些硬體感應器所蒐集到的各種資訊。從上下游供應鏈觀之，設備製造商和作業系統業者可說已為行動應用程式蒐集使用者個人資料，在軟硬體架構方面打下必要的基礎。

行動應用程式開發商是蒐集使用者個人資料的主要發動者。行動應用程式的設計，事實上決定了該程式對於隱私權的保護程度，以及對於使用者個人資料的蒐集種類。另一方面，諸如 Apple 的 App Store[15]、Google Play[16]等應用程式平台業者，藉由建置、提供一個公開的銷售平台，讓應用程式開發商得以將各式各樣的應用程式上架至平台之上，吸引各方的潛在使用者下載使用。而平台業者為了加強平台功能，會從「平台」和「行動設備」蒐集特定面向的使用者統計資料，例如使用者的使用方式與習慣等[17]。就行動應用程式的行銷通路而言，程式開發

---

13 *ClickMode Enumeration*, MSDN, http://msdn.microsoft.com/zh-tw/library/system.windows.controls.clickmode(v=vs.100).aspx (last visited Nov. 5, 2013).

14 *W3C Technical Reports Index*, W3C WORKING DRAFT, http://www.w3.org/TR/2012/WD-proximity-20121206/ (last visited March. 28, 2013); *Sensor API Specification*, W3C WORKING DRAFT, https://dvcs.w3.org/hg/dap/raw-file/tip/sensor-api/Overview.html (last visited March. 28, 2013).

15 *See App Store Review Guidelines*, APPLE, http://images.worldofapple.com/appstoreguidelines_9910.pdf (last visited Aug. 11, 2013).

16 Android Market 開發人員發佈協議，GOOGLE PLAY，https://play.google.com/about/developer-distribution-agreement.html（最後瀏覽時間：2013 年 8 月 11 日）。

17 同前揭註。

商與平台業者直接面對下載使用行動應用程式的消費者，因此也成為隱私聲明或隱私設定是否向使用者充分揭露的關鍵所在。

行動應用開發商蒐集到的使用者個人資料，除了作為增益既有功能或研發新軟體之際可供參照的市場調查數據資料外，亦可提供給第三方業者，使之得以提供客製化的廣告，或是進行企業行銷所需要的使用者消費行為趨勢調查[18]，因此第三方業者也有可能從行動應用開發商手中取得使用者的個人資料。綜此，若要通盤解決行動隱私的問題，在規範架構上應該同時從設備製造商、應用程式開發商、應用程式平台業者、和第三方廣告業者等居於供應鏈上下游之不同型態業者一一著手，依其個別蒐集、使用個人資料的不同目的與態樣，制定相對應的隱私保護規範，方能有所成效。

2.1.3. 行動應用程式業者蒐集使用者個人資料的目的

在行動商務尚未來臨前的實體世界，業者藉由各種營業活動所創造的互動接觸機會，蒐集客戶的個人資料或使用習慣，並加以分析、販售給其他業者，其實並非新聞。諸如信用卡業者蒐集持卡人的消費習慣，並且施以進一步的商業分析與運用，或是報刊雜誌業者販售訂戶的名單等，皆為適例[19]。在行動商務時代，由於人們高度仰賴行動裝置，透過行動應用程式的自動蒐集與傳輸，業者對使用者個人資料的蒐集、儲存、使用、散布更加容易而徹底，甚至可以從手機電話或電子郵件地址，窺探使用者的生活習慣，因此對於使用者的隱私衝擊也更形嚴重。

為何行動應用程式業者要蒐集個人資料？整體而言，業者蒐集使用者的個資，有三個目的：其一，乃是為了行動應用程式本身運作、改良、客製化所需，以做為開發新軟體的基礎[20]；其二，有些業者將行動應用程式作為廣告加以行銷，例如食品業者 Kraft 開發一款名為 iFood 的應用程式，即為一種成功的廣告手法，提供使用者免費的食譜，讓使用者產生購買食材的想法和行動，也可藉此了解使用者食材採購的情況[21]；其三，則是將蒐集的個人資料經分析或整理後，賣給第三方業者如廣告商，獲取利潤[22]。換言之，行動應用程式的目的可得知，行動應用程式產業的主要收益，一方面是根據應用軟體本身獲取的利潤，另一方面則是從應用程式取得的使用者個人資料取得的獲利。然而，其實這三個目的全都指向同一個企業經營策略：一對一行銷（One-To-One Marketing）。

---

18 *Understanding Mobile Apps*, ONGUARDONLINE.GOV, http://www.onguardonline.gov/articles/0018-understanding-mobile-apps (last visited March. 28, 2013).

19 *See* Dawyer v. American Express Co., 652 N.E.2d 1351 (1995); *see also* Shibley v. Time, 341 N.E.2d 337 (1975).

20 *See* Nick Bilton, *3G Apple iOS Devices Are Storing Users' Location Data*, N.Y.TIMES (Apr. 20, 2011), http://bits.blogs.nytimes.com/2011/04/20/3g-apple-ios-devices-secretly-storing-users-location/; *see also* Nick Bilton, *Apple Updates Software to Fix Problems With Collecting Location Data*, N.Y. TIMES (May 4, 2011), http://bits.blogs.nytimes.com/2011/05/04/apple-ios-software-release-fixes-location-bug/.

21 *See* RODYN BLACKMAN, NONTRADITIONAL MEDIA IN MARKETING AND ADVERTISING 1-14, 153-69 (2013).

22 參考劉翰謙，走向免費的商用軟體，數位時代，http://www.bnext.com.tw/article/view/id/22985（最後瀏覽日期：2013 年 8 月 18 日）。

一對一行銷又稱為關係行銷（relationship marketing），或消費者關係管理（customer-relationship management），意指業者鎖定每一個目標消費者，根據業者所了解、掌握的消費者細節，改變業者本身對個別消費者的行為，設計或提供符合消費者需求的商品廣告，吸引消費者消費；更甚者，業者甚至可以形塑消費者的消費習慣，受到業者的影響而消費[23]。Don Peppers、Martha Rogers 和 Bob Dorf 三位業界人士，在 1999 年於哈佛商業評論（Harvard Business Review）提出一對一行銷經營評量的架構供企業自我檢視，有以下四個評量因素[24]：

(1) 識別出消費者（Identifying your customers）

業者須具備識別出消費者的能力，並盡可能取得越多消費者的細節越好，除了姓名和地址外，還要了解消費者的消費習慣和消費行為模式，例如喜歡什麼或不喜歡什麼。此外，業者亦必須隨時更新消費者的資料，才能隨時跟著消費者的偏好，調整行銷的策略。

(2) 將消費者差異化（Differentiating your customers）

業者根據其所蒐集的消費者資料，依據消費者不同的價值和需求，將顧客區分成不同的客群。使業者可得以針對不同的客群，提供不同程度、價位或時效的服務。

(3) 與消費者的互動（Interacting with your customers）

在業者得以「識別消費者」並「區隔消費者」後，業者應和消費者建立互動的模式，以隨時掌握消費者的反應。在科技的輔助下，業者可以藉由網案、應用程式、電子郵件或社群網站等管道，和消費者互動，因此業者與消費者的互動模式是一個有成本效率（cost-efficiency）的方式。

(4) 客製化業者的企業行為（Customizing your enterprise's behavior）

業者以上種種的行為和努力，所要追求的終極目標是：針對每一個消費者，提供不同的待遇、產品或服務。然而，業者的能力有限，因此盡可能利用大量的客製化（mass-customizing），將產品或服務分割成一個個的獨立模組，消費者可依照其不同的需求加以組合。

從一對一行銷的因素可以理解，為何有論者將一對一行銷策略，稱為當代廣告行銷的聖杯。因為無論業者的規模大或小，都可以依其能力使用各種科技管道蒐集和分析消費者的個人資料，並從和消費者的互動間，提供或形塑消費者的需

---

23 Don Peppers, Martha Rogers, & Bob Dorf, *Is Your Company Ready for One-to-one Marketing?*, HARVARD BUSINESS REVIEW January-February 151-160 (1999); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N. Y. U. L. REV. 1814, 1850 (2011).

24 Don Peppers, Martha Rogers, & Bob Dorf, *supra* note 23, 151-160 (1999). 另參見陳巧佩，企業導入顧客關係管理決策之研究，國立政治大學企業管理學系碩士論文，頁 22-25（2000）。

求[25]。同時，從一對一行銷也可了解，為何行動應用程式產業需要蒐集使用者的個人資料，因為消費者的資料是一對一行銷成功與否的關鍵。當業者可以識別出特定個人，掌握該消費者鉅細靡遺的個人資料和使用習慣，則業者越能分析出消費者的消費模式，而得以做出最聰明、最有賺頭的決策。行動裝置或行動應用程式成為業者的得力助手，因為二者皆為現代人們最常使用的硬體和軟體，都可以藉由追蹤以及和使用者互動，取得大量、多樣化的使用者資料。因此可以從中推導出以下二個結論：首先，由於業者為能滿足使用者的需求，因而開發出新的技術或產品，帶來科技的革新和進步；然而，當行動應用程式可廣泛且深入地掌握使用者的個人資料，也因而產生使用者隱私受到侵害的疑慮。

在此背景下，業者為了因應使用者對隱私保護的需求，而發展出切合市場實況與產業需求的個資保護機制。例如目前已有行動應用程式業者依照使用者之需求，進行主動告知，將個人資料蒐集種類標準化，並將隱私聲明簡明化，列舉出主要蒐集（collect）、分享（share）的個人資料，以落實使用者資訊自決之權利。此外，透過匿名化或去識別性的技術，處理業者所蒐集的個人資料，保護使用者的隱私。更甚者，業者亦會提供隱私設定供使用者保護其隱私，例如行動裝置使用者可決定是否要開啟 GPS，供應用程式蒐集其位置資訊。

2.2. 個人資料保護的目的

個人資料的保護目的，係藉由保障個人生活私密領域免於他人侵擾及個人資料之自主控制，以保護人民之人格自由發展與人性尊嚴，係為憲法第 22 條所涵蓋之人民基本權利[26]。或有認為無論在傳統商業市場、電子商務，乃至行動商務市場，業者蒐集的資料，例如位置資料、下載什麼軟體、或者消費資料，並非敏感性的個人資料[27]，理應不致造成對行動應用程式使用者或使用者的隱私權侵害，然而事實上並非如此。

個人資料的蒐集和彙整，為何會對個人隱私造成侵害？有認為可以從喬治歐威爾在其小說「1984」中，所形塑「老大哥正在看你（Big Brother is watching you）」的社會氛圍來觀察。Jerry Kang 教授認為監視會侵害資訊隱私的根本價值之一——人性尊嚴，他舉例說明監視對於個人的侵害程度和侵害原因。我們可以接受在生活中受到不經意的觀察和注視，因為我們知道這是生活中必然的社交接觸和互動。然而，我們並不希望有不想要的碰觸，因為我們對身體有自主權，拒絕或防範不必要的碰觸可以減少不必要的傷害，同時不必要的碰觸也會帶來人格尊嚴的威脅和緊繃。監視其實就如同一種不必要的身體碰觸，因為人民知道自己受到監視，為了避免與監視者產生不愉快的互動經驗，因而產生人民自我設限、自我

25 Don Peppers, Martha Rogers, & Bob Dorf, *supra* note 23, 155-56 (1999); RODYN BLACKMAN, *supra* note 21, at 1-14 (2013).

26 參見司法院釋字第 585、603 及 689 號解釋，以及個人資料保護法立法意旨。

27 敏感性或私密性的個人資料，參酌我國個人資料保護法第 6 條，係為：醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

檢查，產生自我內化的效果，有意識或潛意識地表現出符合監視者要求的外在型態，進而內化成為自我的人格，而損害其作為自尊自主之權利主體的人性尊嚴。此外，除了人民的人性尊嚴與資訊自決權受到擠壓與侵害之外，在資訊網路下的監視為何較一般日常生活中的監視，須要受到更嚴格的檢視？其原因有二：其一，資訊網路下的監視可以蒐集、彙整大量且廣泛的個人資料；其二，資訊網路下監視蒐集的個人資料，經濟且有效率，非公務機關可以輕易獲取所欲知悉之當事人的個人資料，並可以低廉的成本，在其他業者交換彼此蒐集的個人資料。[28]。

然而 Daniel Solove 教授則認為，相較於「老大哥」的監視，法蘭克・卡夫卡的「審判（The Trail）」更為符合現代交易環境之下個人資訊隱私所面臨的情況。當代的大型機構透過廣泛蒐集個人資訊，可以掌握個別人士各個層面的大量細節資訊，然而當事人自己卻完全不知道有多少私人底細掌握在諸多大型機構裡，也不清楚這些大型機構實際上如何使用其個人資料，因而產生對於個人資料無法控制掌握的無力感，並且惴惴不安，心生恐懼。簡言之，業者所建立的大型資料庫以及實務操作帶來的問題，在於剝奪當事人對其個人隱私處理的控制權。此外，不同業者處理個人資料的手法不同，無法如同 Jerry Kang 教授所言，僅以單一的監視行為來涵括之，況且並非所有受監視所得的個人資料，當事人都認為是私人的（private）個人資料，而對其隱私有所侵害[29]。舉例來說，業者所蒐集的個人資料，可能個別單筆來看不具任何意義，然而將當事人不同種類的個人資料匯聚在一起，組合、比對分析之後的結果，或許會揭穿當事人不想告人或希望保密的個人資訊[30]。譬如宗教信仰，或許不是非常私人的個人資料，但是當事人可能希望隱瞞、不欲人知。然而業者可以從行事曆記錄（例如齋戒月）、位置資訊（當事人對麥加的定位資訊）或者網頁瀏覽紀錄（例如線上閱讀可蘭經）等資料，判斷出當事人是伊斯蘭教徒。Richard Posner 法官曾在其法律經濟學的書中言道：「當人們認為隱私權受到侵害，其實是他們希望能夠擁有更多權力，來隱藏如果遭別人使用會不利於他們的個人資料」[31]。質言之，在資訊社會之中，使用者若無法有效得知自己有多少資訊和想法掌握在業者手中、會被如何利用，將因無知與無力控制而產生莫名的心理壓力[32]。

---

28 Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1259-65 (1998).

29 DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, 38 (2004). *See also* Daniel J. Solove, *Why Privacy Matters Even if You Have 'Nothing to Hide'*, THE CHRONICLE REVIEW (May 15, 2011), http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/.

30 *See* Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 754-60 (2008).

31 RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1983).

32 *Id.* at 36-55.

2.3. 我國個人資料保護法簡論

我國隱私權概念的形成與發展，最初乃是建立在民法人格權的基礎上[33]。在憲法層次，隱私權雖非我國憲法明文列舉的個人權利，然而司法院大法官第 293 號解釋、第 535 號解釋、第 585 號解釋、第 603 號解釋、以及第 689 號解釋，均明示隱私權為憲法基本權保護範疇之內。尤其釋字第 603 號解釋文中，將「隱私」概念區分為二：私領域不受侵擾之權，以及資訊自決之權。其中資訊自決權不僅對於公務機關具有拘束力，基於「基本權第三人效力」理論，對於非公務機關亦具有相當的約制作用。在該號理由書中，大法官亦陳明隱私權雖立基於人性尊嚴與人格權，然其並非受到絕對保護的權利。換言之，隱私保護需與公共利益相互權衡，而其個案審查密度，則取決於系爭個人資料之性質。在法律層面上，我國在 2010 年 5 月大幅翻修既有的「電腦處理個人資料保護法」，並且更名為「個人資料保護法」（以下簡稱個資法），大舉擴充對於國人隱私權與資訊自決權的法律保護，在同年 9 月 26 日公布個人資料保護法施行細則，並已於 2012 年 10 月正式施行。

在介紹行動應用程式與個人資料保護法的關係前，為了方便後續討論，本文欲在此節簡介個人資料保護法，分別分析和評論個資法的原則、中央目的事業主管機關的判斷、個資法的管轄範圍、以及個人資料蒐集、處理和利用的規範。

2.3.1. 個資法的原則—與 OECD 隱私準則八大原則的對照

我國在民國 101 年 10 月 1 日正式施行個人資料保護法，並於同年 9 月 26 日公布個人資料保護法施行細則。個人資料保護法參酌 OECD 隱私準則，依據八大原則分別訂定相對應之法律規範，包含保護客體、適用主體、通知和同意機制、當事人權利、行政監督、相關責任和團體訴訟。

經濟合作暨開發組織（The Organization for Economic Cooperation and Development，簡稱 OECD）於 1980 年提出的「隱私保護與個人資料跨境流動準則（OECD Guideline on the Protection of Privacy and Transborder Flows of Personal Data，後簡稱 OECD 隱私準則）」，所訂定之八項原則成為各國訂定個資或隱私法規的共通原理原則，實為重要[34]。以下，將交互介紹 OECD 隱私準則的八大原則與我國個資法的條文。

---

33 王澤鑑，「人格權法」，1 版，三民經銷，台北，頁 12（2012）。

34 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, at 7-14, http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Dec. 22, 2012). 另參見劉定基，「個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例（下）」，月旦法學雜誌，第 119 期，頁 40-41（2012）；李震山，「論資訊自決權」，「人性尊嚴與人權保護」，頁 249（2011）。

(1) 目的特定原則（Purpose Specification Principle）、蒐集限制原則（Collection Limitation Principle）和使用限制原則（Use Limitation Principle）

目的特定原則係指個人資料的蒐集必須目的特定，後續的蒐集不能與目的牴觸，若有變更亦應特定；蒐集限制原則係指，個人資料應透過合法、公平的方式蒐集，並通知當事人，取得同意；而使用限制原則為個人資料的揭露，應符合蒐集目的，除非得當事人的同意或依據法律的規定。換言之，前述三原則緊扣機關行為與目的間的關聯，亦即機關對個資的行為必須囿限於特定目的的範圍內，且該行為和木的間必須有相當關聯性。此三原則的主要內容，體現於個資法總則的第 5 條、公務機關對個人資料之蒐集、處理及利用的第 15 條和第 16 條、以及非公務機關對個人資料之蒐集、處理及利用的第 19 條和第 20 條。

個資法第 5 條將目的特定原則明文規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」並在第 15 條、第 16 條、第 19 條和第 20 條限制特定目的外的蒐集、處理或利用的情形。依據法務部函釋的見解：「公務機關與非公務機關於蒐集、處理及利用個人資料時，仍應受「必要範圍」及「正當合理關聯」之限制……依個別情形予以審認（法務部民國 103 年 01 月 22 日法檢字第 10304504440 號）。」。此外，關於「必要範圍」及「正當合理關聯」的判斷，法務部認為須符合比例原則，亦即應依個案考量系爭行為所採取的是否有助於目的之達成（適當性）？是否對當事人權益損害最少（必要性）？以及造成的損害和欲達成目的之利益間是否均衡、相當（衡量性）[35]？此外，在個資法第 53 條授權法務部會同中央目的事業主管機關指定本法所定特定目的及個人資料類別，法務部並於 2012 年 10 月 1 日公布「個人資料保護法之特定目的及個人資料之類別修正總說明及對照表」[36]。

針對敏感性個人資料，為確保當事人的隱私免受侵擾，特於個資法第 6 條規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」，原則上敏感性個人資料禁止蒐集、處理或利用，惟於下列情形得為利外：「一、法律明文規定；二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措；三、當事人自行公開或其他已合法公開之個人資料；四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。」（關於蒐集、處理或利用的細部討論，請參見 2.3.4）。

(2) 公開透明原則（Openness Principle）

公開透明原則意指個人資料的使用應公開透明，並有合理管道可得確認。依據個資法第 8 條和第 9 條規定，無論是公務機關或非公務機關，均須依照法定的告知項目向當事人說明。在蒐集、處理或利用當事人的個人資料前，應先陳明（1）業者的名稱；（2）蒐集的目的；（3）個人資料的類別；（4）個人資料利用的期間、

35 法務部民國 103 年 01 月 13 日法律字第 10303500480 號。

36 個人資料保護法之特定目的及個人資料之類別修正總說明及對照表，法務部，http://www.moj.gov.tw/ct.asp?xItem=283183&ctNode=28007&mp=001（最後瀏覽時間：2013 年 4 月 20 日）。

地區、對象及方式；以及（5）當事人依個資法得行使的①查詢或閱覽權；②請求製給複本權；③補正或更正權；④停止蒐集、處理或利用權；以及⑤刪除權依第三條規定得行使之權利及方式。此外，個資法第 7 條陳明若機關以當事人的同意作為特定目的外蒐集、處理或利用的允許時，應取得當事人的書面同意。

(3) 資料品質原則（Data Quality Principle）

資料品質原則係指蒐集資料須與使用目的有關聯，並求資料的正確與更新。此原則規範於個資法第 11 條第一項:「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。」以避免不正確的個人資料，影響當事人的權益。

(4) 個人參與原則（Individual Participation Principle）

個人參與原則為當事人資訊自決的體現，當事人得以確認、取得、救濟、和異議。在個資法第 3 條當事人就其個人資料具有五項權利，不得預先拋棄或以特約限制，包含：查詢或請求閱覽權；請求製給複製本權；請求補充或更正權；請求停止蒐集權、處理或利用權、以及請求刪除權[37]。

(5) 安全維護原則（Security Safeguards Principle）

安全維護原則，顧名思義即資料管理者為蒐集、處理、利用或傳輸時，須確保個人資料受到安全地保護。根據個人資料保護法第 27 條規定第一項，非公務機關都應該採取適當之安全措施，以防止個人資料被竊取、竄改、毀損、滅失或者洩漏。依目前個資法施行細則第 12 條第 2 項規定，適當之安全措施和所欲達成之個人資料保護目的間，須有適當比例為原則。適當之安全措施得包含以下內容：（1）成立管理組織，配置相當資源；（2）界定個人資料之範圍；（3）個人資料之風險評估及管理機制；（4）事故之預防、通報及應變機制；（5）個人資料蒐集、處理及利用之內部管理程序；（6）資料安全管理及人員管理；（7）認知宣導及教育訓練；（8）設備安全管理；（9）資料安全稽核機制；（10）必要之使用紀錄、軌跡資料及證據之保存；以及（11）個人資料安全維護之整體持續改善。至於細節性、具體的安全措施與個人資料檔案安全維護計畫或業務終止後個人資料處理辦法，個資法以法律授權的方式，委由中央目的事業主管機關指定，並訂定計畫和處理方法之標準[38]。

---

37 針對更正、補充、停止和刪除權利，於個資法第 11 條第二項至第五項有更詳盡的規範：「個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限（第二項）。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。但因執行職務或業務所必須或經當事人書面同意者，不在此限（第三項）。 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料（第四項）；因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象（第五項）。」。此外，於個資法第 13 條規定個人資料處理期限或處理期限延長。

38 例如經濟部工業局已經編製「個人資料法規遵循參考指引暨宣導手冊——資服業個資教戰手冊（以下簡稱資服業個資教戰手冊）」，供資訊服務業者作為個人資料管理機制作法建議，共有 13 個步驟：步驟一：訂定個人資料保護與管理政策；步驟二：成立個人資料保護管理執行小

(6) 課責原則（Accountability Principle）

課責原則意指資料管理者若違反需承擔責任，個資法針對違法者之課責，規定於個資法第五章。

表一：OECD 隱私準則八大原則與我國個人資料保護法之對照[39]

OECD 原則		內涵		個資法
目的特定原則	↔	蒐集個資之目的必須明確，並在目的內使用之	↔	§5, 15, 16, 19, 20
蒐集限制原則	↔	須以合法手段取得個資，並待當事人同意	↔	§5, 6, 15, 19, 53
使用限制原則	↔	除有特殊情形，不得為目的外之利用	↔	§5, 16, 20
公開透明原則	↔	就個資的蒐集、處理或利用須公開相關做法	↔	§7, 8, 9
資料品質原則	↔	個人資料須正確、完整且不斷更新	↔	§11
個人參與原則	↔	當事人得針對其個資行使權利	↔	§3, 10, 11, 13, 17
安全維護原則	↔	個人資料以適當的安全防護措施加以保護	↔	§12, 18, 27
課責原則	↔	資料擁有者採取相關措施來符合上述原則	↔	第五章罰則

2.3.2. 中央目的事業主管機關的判別

我國於個人資料保護採取單一立法、部門監督的規範政策。換言之，我國訂立個人資料保護法作為個資和資安保護的母法，而由個別產業的中央目的事業主管機關」，就其所負責產業負有個資保護督導檢查之責，並於業者有違個資法律規定時，課處罰責。

依據行政院 101 年 10 月 22 日院臺法揆字第 1010061195 號函，公告「個人資料保護法非公務機關之中央目的事業主管機關」，參考行政院主計總處對行業標準的分類，劃定各個產業相對應的中央目的事業主管機關[40]。以行動應用程式業者為例，在「個人資料保護法非公務機關之中央目的事業主管機關」中，「271 電腦及其週邊設備製造商」、「272 通訊傳播設備製造業」、「582 軟體出版業」、「620 電腦系統設計服務業」、和「639 其他資訊供應服務業」是較貼近行動應用程式業者的非公務機關項目，其中央目的事業主管機關均為經濟部工業局[41]。然

組；步驟三：製作個人資料管理作業時程表；步驟四：公告個人資料保護管理政策；步驟五：盤點法規命令以及相關主管機關之規範；步驟六：盤點個人資料；步驟七：進行個人資料風險評估並擬定風險對策；步驟八：配置相當資源；步驟九：訂定個人資料保護管理作業手冊；步驟十：實施個人資料保護管理教育訓練；步驟十一：運作個人資料保護與管理；步驟十二：檢視；步驟十三：持續改善。參見經濟部工業局，個人資料法規遵循參考指引暨宣導手冊——資服業個資教戰手冊，頁 14-20（2012），http://www.moeaidb.gov.tw/external/ctlr?PRO=information.InformationNewsList&t=2184（最後瀏覽時間：2013 年 8 月 20 日）。

39 參見經濟部工業局，個人資料法規遵循參考指引暨宣導手冊──資服業個資教戰手冊，頁 5（2012），http://www.moeaidb.gov.tw/external/ctlr?PRO=information.InformationNewsList&t=2184（最後瀏覽時間：2013 年 11 月 20 日）。

40 【執行措施】個人資料保護法非公務機關之中央目的事業主管機關，法務部個人資料保護專區，http://pipa.moj.gov.tw/cp.asp?xItem=1298&ctNode=431&mp=1（最後瀏覽時間：2013 年 5 月 23 日）。

41 經濟部主管個人資料保護法非公務機關之分工表，經濟部法規委員會，http://www.moea.gov.tw/Mns/colr/content/ContentLink.aspx?menu_id=6419（最後瀏覽時間：2013

而本文發現，由於中央目的事業主管機關是依照各事業體的「行業別」而認定，並非依其從事之業務內容而個案認定[42]，勢將導致兩個問題。

首先，隨著科技的革新和社會的發展，以行業別來做為中央目的事業主管機關的歸屬標準，恐導致有些服務或商業型態未能列舉其中，形成體制上的灰色地帶。其次，以行動應用程式為例，由於行動應用程式的種類多樣，內容多元，經濟部工業局是否可以完整涵蓋，而為確定之主管機關，不無疑問。如果中央目的事業主管機關目前尚無法確認，是否會發生「部門踢皮球」[43]的情形，形成「體制空白」，不免令人憂心[44]。

此外，個資法第 22 條至第 26 條對於非公務機關建立行政檢查制度，同法第 27 條第三項授權中央目的事業主管機關，應就非公務機關訂定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，訂定相關辦法加以規範[45]。惟目前辦法訂定進度落後，各部會應該加緊腳步。個資法為個人資料保護的母法，是為原則性、總括性的法律規範，各機關可藉由制定法律、行政規則，或是作成行政函釋、行政處分等方式，形成案例並累積實務見解，提供各領域業者具體的建議與規定。此外或者藉由出版年報或定期報告書，將對於業者的監督與調查結果予以公布，或是依照產業的特性提出檢討或建議報告，使人民得以知悉並注意個別產業可能帶來的隱私威脅。如此亦得以讓業者更為了解如何加強使用者之個資保護，以保障消費大眾的隱私權益。

2.3.3. 個資法的管轄範圍

依據個資法第 51 條第二項規定：「公務機關或非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」。立法者認為，現今數位社會下，很容易在我國領域外蒐集、處理或利用我國國民的個人資料。因此依據屬地主義的法理，為防範公務機關或非公務機關在我國領域外違法侵害國人個人資料之隱私權益，規避法律責任，因此明定在我國領域外，亦有本法之適用[46]。換言之，外國機關在我國領域外蒐集、處理或利用我國國民的個人資料者，適用我國個資法的規定，必須履行個資法的義務和規範[47]。

年 8 月 20 日）。

42 第二篇、個人資料保護法實務上注意事項 Q1. 個人資料保護法的「主管機關」所指為何？中小企業如何確定自身所屬行業的主管機關有哪些？，經濟部中小企業處，http://law.moeasmea.gov.tw/modules.php?name=km&file=article&sid=608（最後瀏覽時間：2013 年 8 月 20 日）。

43 部會踢皮球 檢舉個資案跑一年，自由時報，http://www.libertytimes.com.tw/2013/new/may/14/today-life7.htm（最後瀏覽時間：2013 年 5 月 23 日）。

44 參見劉靜怡，「不算進步的立法：「個人資料保護法」初步評析」，月旦法學雜誌，第 183 期，頁 164（2010）。

45 法務部針對個人資料保護法第 27 條第三項，提出「中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項」和「中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項逐點說明」，供中央目的事業主管機關訂定個資管理辦法。

46 個人資料保護法第 51 條立法理由。

47 本文對個資法的管轄範圍有所疑義，即便個資法的適用主體範圍包含我國與外國機關，外國機關實際上是否受我國個資法約束，不免打上問號。發生在英國的隱私侵害案件，或許可做

表二：個資法管轄範圍[48]

行為主體 / 行為地	我國機關	外國機關
我國領域內為之	適用 （屬地原則）	適用 （屬地原則）
我國領域外為之	適用 （個資法第 51 條第二項，保護原則）	不適用

2.3.4. 個人資料蒐集、處理和利用的規範

個資法針對非公務機關對個人資料的蒐集、處理與利用，分別規定在個資法第 19 條和第 20 條。非公務機關在蒐集或處理時除須符合特定目的外，並須符合法定情形[49]。而在利用個人資料時，原則上必須符合目的特定原則，然而在例外情況下，可為特定目的外之利用[50]。

關於個人資料蒐集目的與個人資料之類別，法務部會同相關主管機關於民國 85 年頒布「電腦處理個人資料保護法之特定目的及個人資料之類別」，並於個資公布後在 101 年 10 月修正，例示出 182 種特定目的，以及 134 種個人資料類別[51]。只要在特定目的下，自一般可得來源下取得使用者的個人資料，並在蒐集時，告知使用者：業者名稱、蒐集目的、個人資料類別、個人資料利用期間、地區、對象，並提供使用者查閱、複本、補充更正、停止蒐集、處理或利用以及刪除的權利，並使當事人得自由選擇是否提供個人資料下，取得使用者同意後，即可蒐

為借鏡。英國一群 iOS 用戶控訴 Google 藉由迴避設計，繞過手機 Safari 瀏覽器的隱私設定，而追蹤使用者的瀏覽資訊。不過 Google 主張服務均在美國加州運作，因此英國的隱私法規無法適用，英國法院不具管轄權。雖然英國法院尚在調查其是否具有管轄權，但透過本案可看出外國業者適用我國法律有很多挑戰和困難。*See Google wants UK privacy case tried abroad, lawyer claims*, BBC (Aug. 19, 2013), http://www.bbc.co.uk/news/technology-23756243; James Tozer, *UK law has no power over us, says Google: Outrage at search giant's arrogance in snooping case*, DAILY MAIL (12:04 GMT, Aug. 19, 2013) http://www.dailymail.co.uk/news/article-2396809/Google-says-UK-law-power-Outrage-search-giant-bypassing-privacy-settings.html. *See* also James Vincent, *Google claims that UK law does not apply to them*, THE INDEPENDENT (Aug.19, 2013), http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-claims-that-uk-law-does-not-apply-to-them-8774935.html.

本文以為，與其要求外國業者遵守我國個資法，卻因為我國鞭長莫及而無管制實益，倒不如中央目的事業主管機關定期彙整他國經審查認定有違該國個資或隱私相關法律的行動應用程式業者，供國人知悉，更能保護我國國民。

48 資訊工業策進會科技法律研究所，「個資保護 1.0」，頁 52（2013）。

49 個人資料保護法第 19 條：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。五、經當事人書面同意。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」。

50 可為特定目的外利用者，依個資法第 20 條規定，包括：法律設有明文規定；為增進公共利益；為免除當事人之生命、身體、自由或財產上之危險；為防止他人權益之重大危害；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識別特定當事人；或者經過當事人書面同意。

51 法務部，前揭註 36。

集、利用、揭露使用者的個人資料。若非公務機關違反本法之規定，依個資法第 29 條第二項，準用第 28 條第二項到第六項的規定，當事人得請求回復名譽、並取得相當或法定的賠償。同時，主管機關亦得依個資法第 48 條及第 50 條規定，分別課處業者及其負責人罰鍰，若經查發現業者涉及不法，可依個資法第 41 條追究其刑事責任。

2.4. 行動應用程式所蒐集之個人資料

個人資料形同適用個人資料保護法的通關密碼，決定了個人資料保護法的適用界線。因此探討如何保護行動應用程式使用者的隱私前，應先了解行動應用程式業者蒐集、處理、利用和揭露使用者資料的行為，是否適用個人資料保護法。尤其，行動應用程式蒐集多種類型的使用者資料，例如姓名、帳戶、通訊錄、位置資訊和手機識別碼等，是否每一種資料均為個人資料有檢討之必要。以下將從個人資料保護法對個人資料的定義出發，了解個人資料保護法的適用範圍。其次，現行個人資料保護法的個人資料定義，在面臨匿名技術和重新識別技術發達的挑戰下，反思個人資料的定義是否有檢討的必要。最後，檢驗行動應用程式所蒐集的資料，是否該當個人資料保護法的個人資料要件。

2.4.1. 個人資料的定義

究竟何為個人資料，係個人資料是否受到保護之前提。依據個資法第 2 條第一款規定：「個人資料：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。」從條文來看，立法者採取「例示和概括並用」的立法方式。在例示的部分，羅列日常生活中經常被蒐集、處理及利用之個人資料，相較於電腦處理個人資料保護法第 3 條第一款的規定，現行個資法新增加護照號碼、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式等個人資料態樣，使個資法保護範圍更為完善。

此外，雖例示方式較為明確，且已羅列多達 19 種的個人資料種類，然而未免掛一漏萬，無法包攝其他可以特定出當事人的個人資料類型。因此，以「其他得以直接或間接方式識別該人之資料」之概括規定方式，涵蓋其他形式的個人資料，以求周延。分析本款規定之條文結構，尤其是最後的概括規定，本法所保護的個人資料必須具備四項要件：個人、資料、個人與資料的關聯性、以及可以直接或間接方式加以識別[52]。

(1) 個人

個人資料所指的「個人」，亦即個人資料之本人[53]，依個資法施行細則第 2 條規定，僅限於現生存之自然人（包含本國人與外國人）、將來非死產的胎兒（民法第 7 條），以及法人的資料中包含自然人資料者。其中，個資法僅保護現生存之自然人的原因在於，個資法立法目的之一即在保護屬於人格權之隱私權，而唯有生命之自然人方有隱私受侵害之恐懼情緒，因此法人的資料不在個資法保護之列。至於已死亡之人，已無恐懼其隱私權受侵害之可能，且其個人資料已成為歷

---

52 參考劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例（上），月旦法學教室第 115 期，頁 43-50（2012）。

53 個人資料保護法第 2 條第九款：當事人指個人資料之本人。

史，故非在個資法保護之列（法務部 100 年 9 月 22 日法律字第 1000022498 號函參照）[54]。然若死者的個人資料內，包含生存之自然人的個人資料，此時該尚生存的自然人之個人資料，自應受到個資法保護[55]。

(2) 資料

關於「資料」此一要件之意義，在個資法之中並未有明確規定。然而從個資法第 1 條的立法理由：「個資法的保護客體不再限於經電腦處理之個人資料，且本法規範行為除個人資料之處理外，將擴及至包括蒐集及利用行為。」可得知，基於希望全面擴大個資法適用範圍的立法意旨，因而不論其資料的性質（包含正確與否、是否為敏感性資料）、內容（包括數字、文字或影像等）、儲存方式（例如電腦、光碟、智慧型裝置、或紙本等）或是處理形式（包含電腦處理或人工處理），均可納入個人資料的保護範圍[56]。此外，個資法將個人資料區分為「一般性資訊」和「敏感性資訊」。依據個資法第 6 條規定，「敏感性資訊」包含醫療、基因、性生活、健康檢查及犯罪前科之個人資料；至於「一般性資訊」，則是「敏感性資訊」以外的個人資料[57]。

(3) 個人與資料的關聯性

再者，個人資料必須與當事人具有關聯性。關於關聯性的判斷因素，我國個人資料保護法和立法理由未有明確規定。若參酌歐盟個人資料保護指令第 29 條工作小組的意見書，此處應考量其內容（content）、使用目的（purpose）或結果（result）。此三者乃係為獨立的判斷要素，只要具備其中之一，即與當事人具有關聯性[58]。所謂從內容判斷，係指有些資料可以直接識別出當事人，例如手機拍攝出的照片，影像和當事人具有關聯性[59]。從目的判斷，則是指從物的角度出發，該物會被如何使用或將被如何使用。該意見書就此舉例解釋：公司的通話紀錄，對公司而言，可確認公司須繳之電話費金額；但對員工而言，通話紀錄可以證明員工和誰通過電話，以及電話通話的內容為何。因此對於不同的使用者，個人資料的使用目的就會有所不同[60]。至於從結果判斷，主要端視該個人資料對於個人可能帶來的影響為何。例如計程車定位資訊，可以讓計程車電台據以派送目前距離乘客位置最近的計程車載客。從蒐集位置資訊的目的觀之，計程車定位主要是為了提供顧客迅速即時的服務，並且節省油費和其他開銷。然而，位置資訊同時也讓計程車電台得以監控特定計程車司機的行為，譬如計程車司機是否遵守當地速限、載客時是否繞遠路等。因此從結果來看，該位置資訊對於計程車司機的個人權益仍然可能產生影響，因而該資訊仍可視為有關該司機之個人資料，因而受到個資法的保護[61]。

---

54 參前揭註 3，頁 43-45。另參酌陳建宇，淺談個人資料保護法，台灣法學第 215 期，頁 12（2013）。

55 參酌法務部 96 年 10 月 8 日法律決字第 0960030614 號函和法務部 100 年 9 月 26 日法律字第 1000017452 號函。另參見劉國佐／李世德，個人資料保護法釋義與實務——如何面臨個資保護的新時代，頁 17（2012）。

56 同前揭註 3，頁 45-46。

57 行政院尚未訂定個資法第 6 條的施行日期，目前尚未施行。

58 Opinion 4/2007 on the Concept of Personal Data, 2007 WP 136 (EC).

59 *Id.* at 10.

60 *Id.* at 10-11.

61 *Id.* at 11.

(4) 可以直接或間接方式加以識別

最後，資料必須得以透過以直接或間接方式（identified and identifiable）識別特定個人。所謂直接識別（identified），係指基於該個人資料，得以從群體之中將當事人與其他人加以區別（distinguished），例如姓名、照片、身分證字號等。至於間接識別（identifiable），則是指公務或非公務機關僅以該資料不能直接識別當事人，而須與其他資料進一步對照、組合、彼此連結，方能識別該特定之個人者[62]。換言之，當事人無法被直接識別時，透過該個人資料仍然可能間接識別出同一當事人[63]，例如透過工作或年齡等個人重要特徵的對照與組合，仍舊得以成功區辨出特定當事人。惟須注意，假若該資料雖可間接識別特定個人，然有查詢上困難或耗費過鉅的情況[64]，則應認為該資料屬於不可識別的資料，排除個資法的適用。由於較之於直接識別資料，間接識別較為模糊而有彈性，其範圍較直接識別來得更為廣泛。因此界定是否屬於間接識別資料，實為實務上判斷是否構成受保護個人資料的考量核心。

綜言之，判斷系爭資料是否該當個資法的個資定義時，「個人」、「資料」和「個人與資料的關聯性」等是較容易該當的要件。相對地，「可以直接或間接方式加以識別」則因識別性屬於籠統、抽象的概念，須通盤考量資料的性質與行為人蒐集、處理或利用的脈絡，因此較難判定，而為是否符合個資的關鍵要件。因此本文以為資料是否適用個資法的標準，應以該資料是否具有「識別性」作為主要判斷標準。

然而有論者質疑個資法對於個人資料的定義，例示的各種個人資料項目，是否得以識別特定當事人？若僅蒐集當事人的教育、職業與財務狀況，而未同時記載姓名、身分證統一編號等其他資料可以直接或間接識別該個人之相關資料時，由於單純的教育、職業與財務狀況無法識別當事人為何人，不禁懷疑是否仍須保護此類無法識別當事人的個人資料？例如民間人力銀行和政府為調查員工教育狀況和薪資的關聯，向民間企業索取不含薪資主體姓名及其他可資特定當事人的資料項目，則薪資和學歷是否仍受個資法保護[65]？因此，論者以為概括規定中「其他得以直接或間接方式識別該個人之資料」應作為例示規定的前提，並建議修正個資法第二條第一款之用語為：「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、社會活動等可識別及其他得以直接或間接方式識別該個人之資料」[66]。

然而本文以為無論是個資法所例示的 19 種個人資料項目，亦或是其他的個人資料，均須該當「個人」、「資料」、「個人與資料的關聯性」和「可以直接或間

62 個人資料保護法施行細則第三條。

63 *Id.* at 12.

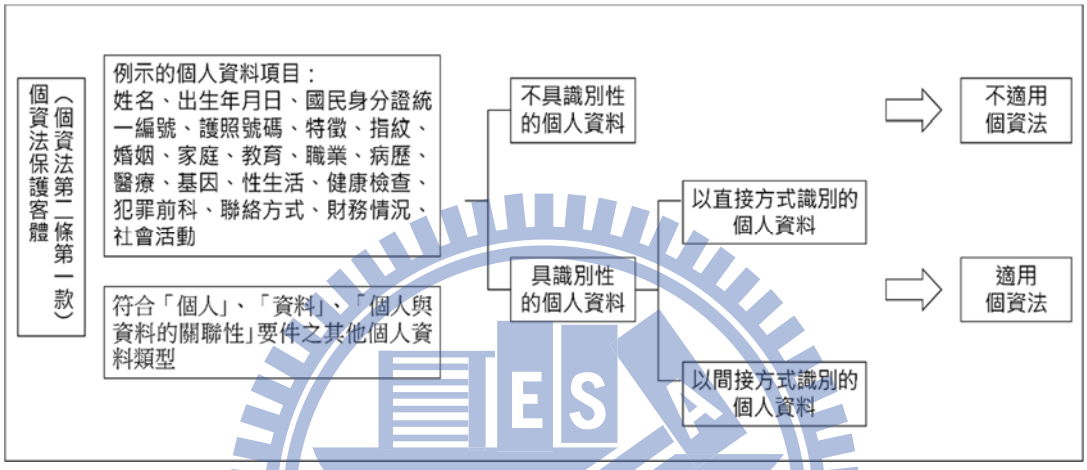
64 參考法務部民國 100 年 05 月 13 日法律字第 0999051927 號函，其要旨如下：「參照電腦處理個人資料保護法第 3 條、個人資料保護法第 2 條等規定，倘因悠遊卡技術上仍得透過比對記名卡卡號與內部資料庫系統得知特定持卡人個人資料，非屬查詢上有困難或耗費過鉅，該卡號即屬得以間接方式識別之個人資料。」既然在非屬查詢上有困難或耗費過鉅的情況下，可將悠遊卡號歸屬於間接方式識別之個人資料；則透過反面推論得知，假若該資料查詢上有困難或耗費過鉅的情況下，可認為該資料不屬於間接方式識別之個人資料，因為無法識別特定之個人，而不適用個人資料保護法。

65 蕭奕弘，論個人資料保護法的法制性問題，成大法學第 23 期，頁 160-165（2012）。

66 蕭奕弘，個人資料保護法之研究，司法研究年報第 29 輯第一篇，頁 90-93（2012）。

接方式加以識別」等四項要件，並非是從而，屬於 19 種個人資料項目之一，即適用個資法。易言之，19 種個人資料項目須具有識別性，方得為個資法的適用客體，因而不生論者所憂慮的問題。

總結以上，本文以為可將個人資料區分為識別性的個人資料和不具識別性的個人資料，前者受到個資法保護；反之後者則不在個資法規範內。其中，識別性的個人資料又可區分為以直接方式識別的個人資料以及以間接方式識別的個人資料二種。而個資法所例示的 19 種個人資料項目，須該當個人資料的四項要件，方得適用個資法，假若不具識別性而無法與特定當事人間產生連結，則不適用個資法（請見下圖一）。



圖一：個人資料保護法保護客體（作者自行整理繪製）

2.4.2. 個人資料定義的調整

誠如前文所述之個人資料的判斷流程，可觀察出一個問題：匿名化技術和重新匿名技術，是否會導致個人資料的界線模糊不清？具有識別性的個人資料經過匿名化處理，因為無法識別出特定當事人，喪失識別性而不受個資法保護。然而假若該匿名化資料又得輕易地重新識別，再度恢復為識別或可資識別的個人資料，又得以重新受到個資法保護，則個人資料的界線是否過於浮動？

特別在行動商務、雲端產業發達的時代，以行動應用程式產業為例，當使用者基於消費、資料儲存、應用程式使用等因素，將大量且各式各樣的個人資料提供給業者時，行動應用程式業者可能在利用使用者的個人資料時，或者將使用者的個人資料分享與第三者（諸如廣告業者或行銷分析業者）時，會以將使用者的個人資料為去除識別性或匿名的處理，來保證其可確保使用者的隱私不受侵擾[67]。以 Facebook 的行動應用程式為例，在說明 Facebook 如何利用使用者的個人資料時，強調：「除非我們已從中移除您的姓名或其他個人識別資訊，或是將您的資料與他人資料結合，使其不再與您相關聯之後，我們才會將資料提供給我們的廣告合作夥伴或客戶[68]。」；又或者是知名的照相、照片分享軟體 Instagram 為例，

67 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1708 (2010).

68 資料使用政策，Facebook，https://www.facebook.com/about/privacy/your-info（最後瀏覽日期：2013 年 10 月 22 日）。

在隱私權政策亦稱：「我們會分享您的資訊給第三者：我們會移除部分可識別您的資料，並以匿名資料分享給其他業者。我們也會結合您的資料和其他不再和您有關連的資訊，並將聚合後的資料分享給第三者[69]。」因此，本文希望探討重新識別技術對個人資料的定義帶來的衝擊和影響為何。

2.4.2.1 匿名化可確保隱私無虞

匿名，從字面意思來看，就是將當事人的名字隱藏起來。然而匿名的力量並非只是單純將當事人的名字隱匿起來。Helen Nissenbaum 教授認為匿名的作用，是截斷當事人的身分和其所為的行為間的連結，使第三者無法從資訊的內容辨別出資訊所指涉的當事人是誰。換言之，匿名所帶來的效果是：無法從資訊內容找出當事人（unreachability）[70]，也因此匿名化被稱為隱私促進的技術（Privacy Enhancing Technology, PET）之一[71]。

然而使用者是否即可認為，在匿名或移除識別性的保護傘下，即可確保我們的隱私？針對這個問題，可以從匿名或移除識別性的個人資料，是否可適用個人資料保護法出發，加以討論。假若該個人資料原本具有識別性，但「資料經過處理後或依其揭露方式無從識別特定當事人」，例如以代碼、匿名、隱藏部分資料或經其他類似手法處理過的個人資料（為求討論方便，以下將「資料經過處理後或依其揭露方式無從識別特定當事人」簡稱為匿名化個人資料）[72]，是否仍受到個人資料保護法保護？

首先，綜合觀察個人資料保護法和個人資料保護法施行細則，可發現當公務機關或非公務機關之學術研究機構，基於公共利益為統計或學術研究之目的而有必要，且已將識別性個人資料轉換成無法識別特定當事人之匿名化個人資料時，依照個人資料保護法，公務機關或非公務機關之學術研究機關，得例外享有個人資料保護法的義務免除，包含得免除間接蒐集個人資料之告知義務（第 9 條第二項第四款）、公務機關例外得於特定目的外利用個人資料（第 16 條但書第五款）、非公務機關得於特定目的內蒐集或處理個人資料（第 19 條第一項第四款）、以及非公務機關得為特定目的外利用個人資料（第 20 條第一項但書第五款）

然而當非公務機關、且非學術研究機關者，蒐集、處理或利用匿名化個人資料時，在此情形下是否適用個人資料保護法？從法條文義解釋觀之，既然該匿名化個人資料已經無從識別特定當事人，即意味著業者已切斷資料和當事人間的連結，不可能構成個資法第 2 條第一款之「可以直接或間接方式加以識別」之要件，

---

69 "Parties with whom we may share your information: We may remove parts of data that can identify you and share anonymized data with other parties. We may also combine your information with other information in a way that it is no longer associated with you and share that aggregated information.", *Privacy Policy*, INSTAGRAM, http://instagram.com/about/legal/privacy/ (last visited Oct. 22, 2013).

70 Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, 15 THE INFO. SOC'Y 141, 141-144 (1999).

71 *See* DANIEL SOLOVE, INFORMATION PRIVACY LAW 593-94 (2011).

72 參見個人資料保護法施行細則第 17 條。

因此應不受個人資料保護法之規範。從法務部所發布之行政函釋中，亦採取否定的見解，認為「如已匿名化或去識別化，而成為不能直接或間接識別個人之資料者（個資法第 2 條第一款及其施行細則第 3 條規定參照），自無個資法之適用」（法務部法律字第 10203503130 號），亦即「如將蒐集所得個人資料以匿名化或去識別化處理，而成為不能識別之資料，即無本法適用」（法律字第 10103104090 號）[73]。

從比較法途徑分析，無論是現行的歐盟個人資料保護指令，亦或是 2012 年 1 月 25 日公布的個人資料保護規則草案（The Proposed General Data Protection Regulation），均在前言部分陳明，由於匿名性資料不再具有可識別性（identifiable），因此不適用個人資料保護指令[74]。甚至在個人資料保護規則草案第 10 條中規定，如資料控制者（data controller）所處理的資料不允許資料控制者識別出自然人，資料控制者毋庸遵守本規則之任何規定[75]。

---

73 以「匿名」為關鍵字檢索法源法律網的判解函釋系統，可發現下列十則針對匿名化或去識別化處理之個人資料是否適用個資法的函釋，均一致認為當個人資料予以匿名化或去識別化處理，成為不能識別之資料，即無個資法適用：法務部民國 102 年 04 月 17 日法律字第 10203503130 號函、法務部民國 102 年 02 月 07 日法律字第 10100253980 號函、法務部民國 101 年 06 月 22 日法律字第 10103104090 號函、法務部民國 101 年 04 月 27 日法律字第 10103103240 號函、法務部民國 98 年 11 月 16 日法律決字第 0980047501 號函、法務部民國 96 年 06 月 21 日法律決字第 0960023899 號函、法務部民國 96 年 06 月 21 日法律決字第 0960022904 號函、法務部民國 94 年 11 月 01 日法律字第 0940033446 號函、法務部民國 92 年 09 月 03 日法律司字第 0920035657 號函、以及法務部民國 92 年 08 月 14 日行執一字第 0920005014 號函。

74 "Recital (26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible", *Directive 95/46/EC of The European Parliament And of The Council of 24 October 1995 on The Protection of Individuals With Regard to The Processing of Personal Data And on The Free Movement of Such Data*, EUR-LEX, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited Dec. 18, 2012);"Recital (23) The principles of protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable", *Proposal for a Directive of The European Parliament and of The Council on The Protection of Individuals With Regard to The Processing of Personal Data by Competent Authorities for The Purposes Of Prevention, Investigation, Detection or Prosecution of Criminal Offences or The Execution of Criminal Penalties, And The Free Movement of Such Data*, EUR-LEX, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited Oct. 21, 2013).

75 "Article 10 If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation", *Proposal for a Directive of The European Parliament and of The Council on The Protection of Individuals With Regard to The Processing of Personal Data by Competent Authorities for The Purposes Of Prevention, Investigation, Detection or Prosecution of Criminal Offences or The Execution of Criminal Penalties,*

此外，德國聯邦資料保護法（Federal Data Protection Act）亦將匿名化的個人資料排除於聯邦資料保護法的適用。從法條即可看出，德國在立法上，將匿名化個人資料和化名之個人資料，在定義和法律效果上有所區隔。匿名化個人資料規定於德國聯邦資料保護法第 3 條第六項，認為當個人資料為「匿名表現（rendering anonymous）」時，因個人資料不再得與特定當事人產生關連，如要產生連結需要耗費過鉅和耗時過久，因此不屬於個人資料，不受聯邦資料保護法保護[76]。換言之，匿名化個人資料的要件為，不可能從匿名化自資料追溯出可識別的個人。另一方面，化名之個人資料規定於德國聯邦資料保護法第 3 條第六項第（a）款，認為如果資料控制者僅以化名（aliasing）的方式，以符號取代當事人的姓名和其他可資識別的特徵，則因為該資料仍與特定當事人具有關聯性，因此受聯邦資料保護法保護[77]。簡言之，匿名化個人資料和化名之個人資料的區別實益在於，是否可適用聯邦資料保護法，僅化名之個人資料適格[78]。

從前述分析，可得出以下結論：當資料受到匿名化或去識別性處理後，因無法識別特定個人，不適用個人資料保護法。因此，假若行動應用程式業者在處理、利用或傳輸其所蒐集之個人資料前，已先將使用者的個人資料經過匿名化或去識別性之處理，則因該資料已經不再能和特定使用者產生連結，亦無從識別個人資料應歸屬於何人，因而可妥善保護使用者的隱私。顯而易見地，以上結論的立論基礎為：經過匿名化或去識別性的個人資料，無法輕易地重新識別，再追溯回可識別的特定個人。結論的前提假設為，重新識別技術在實施上有困難，因此難以將不具識別性的個人資料，恢復成具識別性的個人資料[79]。因此，匿名成為法律

And The Free Movement of Such Data, EUR-LEX, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited Oct. 21, 2013). *See* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW 65-67 (2007).

76 "(6) "Rendering anonymous" shall mean the alteration of personal data so that information concerning personal or material circumstances cannot be attributed to an identified or identifiable natural person or that such attribution would require a disproportionate amount of time, expense and effort.", BUNDESDATENSCHUTZGESETZ [BDSG] [FEDERAL DATA PROTECTION ACT], Sept. 1, 2009, BUNDESGESETZBLATT [BGBL] 1, 2814, as amended, *available at* http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile.

77 "(6a) "Aliasing" shall mean replacing the data subject's name and other identifying features with another identifier in order to make it impossible or extremely difficult to identify the data subject", , BUNDESDATENSCHUTZGESETZ [BDSG] [FEDERAL DATA PROTECTION ACT], Sept. 1, 2009, BUNDESGESETZBLATT [BGBL] 1, 2814, as amended, *available at* http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile.

78 將德國聯邦資料保護法對匿名化和化名的區分，與我國個人資料保護法對無從識別個人資料的規範進行比較，可發現我國個人資料保護法並未清楚區隔「匿名」和「化名」，尤其後者並未完全切斷當事人和資料的關聯，仍可有追溯識別當事人的可能。若公務機關或非公務機關之學術研究機構，可透過較簡便的「化名」即可免除資料主體的個資保護的義務，則顯不符合個資法的立法宗旨，因有修正之必要。參考邱文聰，從資訊自決與資訊隱私的概念區分——評「電腦處理個人資料保護法修正草案」的結構性問題，月旦法學雜誌第 168 期，頁 185-86（2009）。

79 *See* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 266-68 (2008); Paul Ohm, *supra* note 67, 1710-12 (2010).

和科技間的平衡點[80]，也成為業者和使用者間的平衡點，似乎只要將個人資料匿名化，一切隱私侵害的問題就解決了！

2.4.2.2　道高一尺，魔高一丈：重新識別技術打破匿名萬能的迷思

然而前述的假定，在科技快速進步，行銷手法著重於一對一行銷（one-to-one marketing）或行為行銷（behavioral marketing）的今天，受到強烈地挑戰。首先，個人資料保護和科技發展密不可分，重新識別技術（re-identification techniques）會日益進步、改良，不會一直停留在「重新識別匿名化個人資料是非常困難」的假定中。此外，行銷、廣告產業對「重新識別技術」有市場上地需求，行銷廣告業者須透過消費者的行為模式，設計出個人化或符合消費者需求的產品。當一對一的行銷手法成為主流時，將匿名化或去識別性的個人資料，重新還原成原本具有識別性的樣貌，是行銷業者迫切需要的技術[81]。是否可繼續固守「匿名即可確保隱私」的結論，即畫上一個大問號。

Paul Ohm 教授在「Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization」中[82]，率先打破匿名迷思，並進而質疑、甚至於否定以可識別的個人資料作為判斷是否適用個資法標準。在文章中，Paul Ohm 教授以外部資訊（outside information）和內部連結（inner join）二種重新識別技術，解釋匿名化的個人資料，如何重新識別並特定出個資所屬的當事人。外部資訊係指資料控制者所持有資料以外、當事人其他的個人資料，資料分析者藉由將外部資訊和匿名化個資彙整、比對的方式，而得追溯出特定的個人。電腦專家即指出，完美的匿名化技術的前提是，沒有其他任何外部資訊。一旦有外部資訊，則匿名化的保護傘就有被突破的可能，因此建議隱私相關法規應將外部資訊納入保護[83]。另一方面，內部連結猶如兩手交錯（crossed hand），可以藉由不同資料庫的綜合比對，破解經過匿名的個人資料，找到個人資料所屬的當事人。

總而言之，重新識別技術打破了個人資料的界線。首先，重新識別技術的興起，不僅可使原先匿名的個人資料，得以重新揭露；還可使原先認定為不可識別的個人資料，轉變為可識別的個人資料。其次，可識別的個人資料和不可識別的個人資料組合後，或者多種不可識別的個人資料聚合後，原先匿名的資料、去識別性的資料或者不可識別的個人資料，通通都有機會成為可識別的個人資料。因此，Paul Ohm 教授認為是否為個人資料的判斷，在匿名化和重新識別技術下，就像在玩打地鼠遊戲一般，資料游移在可識別個人資料或不可識別的個人資料間。亦即，個人資料保護法對個人資料定義的二分模式，受到挑戰。Daniel Solove 教授和 Paul Schwartz 教授也在「The PII Problem: Privacy and a New Concept of

80　*Supra* note 67, 1731-45 (2010).
81　*See* Paul M. Schwartz & Daniel J. Solove, *supra* note 23, 1818, 1841-59 (2011).
82　Paul Ohm, *supra* note 67.
83　Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy, *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

Personally Identifiable Information」文章中，呼應 Paul Ohm 教授對匿名不再能確保隱私的見解[84]。

此外，在歐陸法系和我國的個人資料保護法下，重新識別技術對匿名化個資會產生另一個問題：個人資料保護法的適用過度擴大。以我國的個人資料保護法為例，在概括條款中規定：「得以直接或間接方式識別該個人資料」。此時，只要任何原本已為匿名的個人資料，得以成功地重新識別出與匿名資料相對應地當事人，則該資料又重新受到資料保護法的保護。亦即，個人資料保護法涵蓋太多需要保護的資訊，使得在實務操作上過於綁手綁腳[85]，因為個人資料的界定不再固定不變，而是處於浮動的狀態，恐讓業者無所適從。此外，當個人資料過度擴張時，亦將會造成業者嚴重的負擔，因為只要資料具有識別性，則在處理、利用個人資料即須遵守個人資料保護法，而承受義務遵守的成本壓力。換言之，個人資料的二分法已經不再夠用，資料不一定能夠輕易的在可識別個人資料和不可識別個人資料間選邊站，而需要綜合考量不斷變動的科技、社會和企業的行為以及個案的脈絡。重新識別技術破壞了原先匿名所帶來法律和科技的平衡，蓋當法律涵蓋太多個人資料，則無法發揮效用；但涵蓋太少個人資料，又無法保護隱私[86]。總結以上分析，面對匿名化的個人資料，須綜合考量個案的脈絡（context）、運用重新識別技術的難易程度、以及企業的行為（corporate practice），不能一概而定，認為即不適用個人資料保護法[87]。

個人資料的定義和判斷，形同個人資料保護法適用的觸發點（trigger），界定了個人資料保護法規的適用界限和範圍。然而隨著科學技術不斷創新，不斷挑戰個人資料的界線下，既有的個人資料定義方法受到挑戰。在個人資料的判斷上，需符合個人資料存在的脈絡，以及考量對當事人隱私侵害的實質風險程度。此概念可運用於執法者判斷系爭資料是否適用個人資料保護法的情況，調整並舒緩個人資料定義僵化，無法與科技發展同步跟進的困境。

2.4.2.3 對個人資料的重新定義？

誠如前述理由，為了能使個資法的定義可以因應科技的發展，學者遂提出修正定義的方法。Paul Ohm 教授認為，在重新識別技術越來越容易破解匿名化個人資料下，既然個人資料無法明確定義或分類，倒不如直接揚棄可資識別之個人資料的概念，改以內容管制（the content of regulation）作為管制手法，從隱私侵害的角度出發，去了解資料受到重新識別的風險有多高，並提供以下五個造成隱私侵害風險的因素：第一，資料處理技術（data-handling techniques），以評估重新識別的風險高低；第二，私人相較於公開發表（private versus public release），將資料公開發表於大眾面前，因為公開發表於大眾匿名化個資重新識別的風險較高，因此應受到的規範密度應高於業者將資料私下分享給受信任的第三者；第三，擁有大量的個人資料（Quantity），過去個資法都偏重於個人資料的品質，然而當

---

84 *See* Paul M. Schwartz & Daniel J. Solove, *supra* note 23, 1836-48 (2011). 其他持相同見解者，例如：Omer Tene & Jules Polonetsky, *Big Data For All: Privacy And User Control In The Age Of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 257-59 (2013).

85 Paul M. Schwartz & Daniel J. Solove, *supra* note 23, 1827 (2011).

86 *See* Shuchi Chawla et al., *Toward Privacy in Public Databases*, 2 THEORY CRYPTOGRAPHY CONF. 363, 363 (2005).

87 *See* Paul M. Schwartz & Daniel J. Solove, *supra* note 23, 1841-45 (2011).

資料庫蒐集的個人資料越多，其可運用的外部資料就越多，也就越容易重新識別出資料當事人；第四，動機（motive），針對敏感性個人資料以及財務經濟的個人資料，需探究資料控制者的動機是否有重新識別的動機；以及第五，信任（trust），此為動機因素的延伸，須考量資料控制者是否可受信任[88]。

Paul M. Schwartz 教授和 Daniel J. Solove 教授則認為「可資識別的個人資料」普遍運用在各國的各個隱私相關法規中，直接揚棄此概念恐有困難。因此二氏提出「可資識別個人資料 2.0（PII 2.0）」的個人資料判斷標準。二氏提出 PII 2.0 的目的有三：其一，提供美國隱私法對個人資料的統一定義；其二，希望歐盟亦可採用 PII 2.0，改善包山包海的個資定義，調整隱私保護和科技發展的平衡；其三，希望依照可能洩漏個人資料的風險程度作為劃分，以對應對等的個資保護密度。以下為 PII 2.0 對個人資料所區分的三種判斷標準，以類似光譜的方式呈現，光譜的最左端為完全無識別風險的資訊，最右端則為識別的個人資料（identified personal data）。第一，識別的個人資料（Identified personal data），係指可依據該資料，直接指示特定的個人，具有最高的識別風險；第二，可資識別個人的個人資料（Identifiable personal data），係指可透過資料識別出特定個人，其中在此分類底下，若該個人資料具有實質風險可資識別當事人，則其保護密度和識別的個人資料相同；第三，不可識別個人的個人資料（Non-identifiable personal data），該資料可識別出個人的風險較低，難與個人產生連結，例如美國總居住人口的資料。其中，實質風險的判斷方式，應考量業者儲存資料期間的長短、相關科技的未來發展、和識別當事人的動機，憑藉以上脈絡加以綜合評價[89]。透過個人資料識別之實質風險，區分隱私保護的管制密度。

2.4.2.4　小結

個人資料的定義和判斷，形同個人資料保護法適用的觸發點（trigger），界定了個人資料保護法規的適用界限和範圍。然而隨著科學技術不斷創新，不斷挑戰個人資料的界線下，既有的個人資料定義方法受到挑戰。

Paul Ohm 教授主張將個人資料的概念廢棄，以內容管制的方法判斷隱私侵害風險的高低。然而廢除個人資料的概念，所要付出的代價是重新調整既存的個人資料保護法規，制度變動成本浩大。此外，改採內容管制的手段，雖可精準且具有彈性的判斷出系爭資料對當事人隱私侵害的風險，卻也同時意味著，個人資料保護法的範圍界線模糊。因為完全依照資料和當事人間存在的脈絡關係判斷，個案性質太強，僅憑藉數個隱私風險因素判斷，容易產生相同事實和個人資料，卻有不同的衡量結果，形成見解上或裁量上的矛盾。甚者，當事人、公務機關或非公務機關亦無法預見個人資料保護法的規範範圍。

另一方面，Daniel Solove 教授和 Paul Schwartz 教授提倡的 PII 2.0，雖然清楚地透過實質風險來區分不同的個資保護標準，然而實質風險的概念其實無異於傳統將個人資料區分為可識別和不可識別的分類方式，只是將界定個人資料的標

88　*See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1759-76 (2010).

89　Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N. Y. U. L. REV. 1814, 1877-79 (2011). See also Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1650-58 (2013).

準，做更細膩地畫分。易言之，可識別個人資料或不可識別個人資料間界線模糊的情況，同樣會發生在不同實質風險程度的個人資料標準間，未能完全解決個人資料界線浮動的問題。因此基於上述二種個人資料定義的修正方式或模型，似乎都還有持續發展的空間，本文以為並不適宜作為個人資料定義修法的參考或修正方向。更甚者，Paul Ohm 教授以及 Daniel Solove 教授和 Paul Schwartz 教授所提出的修正建議，均建立在美國尚無一套普遍適用的個人資料判斷標準，不同法規對於個人資料的定義有不同的要求與規定。然而我國已於個資法，針對個人資料的定義做出明確的規範，和美國法所面臨的問題不同，似不宜做為我國修法的主要參考基礎。

本文介紹此二篇文章的主要目的在於，無論是 Paul Ohm 教授的內容管制，亦或是 Daniel Solove 教授和 Paul Schwartz 教授提出的 PII 2.0 模型，均透漏出相同的訊息：在個人資料的判斷上，需符合個人資料存在的脈絡，以及考量對當事人隱私侵害的實質風險程度。此概念可運用於執法者判斷系爭資料是否適用個人資料保護法的情況，調整並舒緩個人資料定義僵化，無法與科技發展同步跟進的困境。因此面對匿名化的個人資料、經化名的個人資料、甚或是去連結的個人資料時，在判斷是否適用個人資料保護法時，應做更細緻化地判斷，綜合考量個案的脈絡（context）、運用重新識別技術的難易程度、以及企業的行為（corporate practice），方能與保護當事人個人資料與隱私之立法目的相合制。

2.4.3. 行動應用程式蒐集之個人資料

行動應用程式的種類繁多，所蒐集的個人資料大體上均可能落入個資法第 2 條第一款所規定之「得以直接或間接方式識別該人之資料」，在此爰將行動應用程式所蒐集、使用的個人資料主要類型，整理如下表三。

表三：行動應用程式可能蒐集之主要個人資料類型（作者自行整理）

使用者姓名	行動電話號碼
行事曆	網頁瀏覽紀錄
電話簿	健康或醫藥相關資訊
帳戶資訊	財務或付款相關資訊
通話紀錄	簡訊、訊息或電子郵件內容
電子郵件	已下載或已使用的應用程式
照片或影片	位置資訊（例如 GPS、Wifi 熱點定位）

行動數位時代下，智慧型裝置與應用程式可能蒐集、處理的個人資料，無論是通話紀錄（contact or call log）、文字訊息記錄（text messages）、電子郵件、位置資訊、財務資訊（banking details）、瀏覽歷史（browsing history）、照片和影片[90]等，雖非個人資料保護法所規定的敏感性個人資料，但事實上仍然屬於使用者

[90] Opinion 02/2013 on Apps on Smart Device, 2013 WP 202 (EC); *Privacy on The Go*, CALIFORNIA

的私密資訊（intimate information），與使用者的私領域具有非常密切的關連。尤其電話號碼、文字訊息這些資訊都是由智慧型裝置自動儲存[91]，假設行動應用程式可得加以蒐集，使用者根本無法設防。

首先，使用者姓名、通話紀錄、健康或醫藥相關資訊、財務或付款相關資訊，屬於個人資料保護法第 2 條第一款所例示的 19 種個人資料項目，通常能與帳戶資訊或電話等資料交叉比對、組合而得以適用個人資料保護法。尤其通話紀錄，係為發信人與受信人之社會活動之資料，應為發信人與受信人所共享之個人資料，屬於個資法規定所稱個人資料之範圍[92]。其次，照片或影片等資料，由於可從影像中透過臉部辨識技術特定出當事人，假若使用者並未將照片或影像公開，僅儲存於智慧型裝置中，則應屬於可直接識別的個人資料，受到個人料保護法保護。再者，至於通訊內容、文字訊息等通訊內容，可以藉由資料比對與組合而間接識別出使用者的身分，因此同樣可以受到個資法的保護。至於帳戶資訊、行事曆、WiFi 熱點、行動上網位置或者行動設備使用情形，或是行動應用程式使用情況等，雖未能直接識別出當事人，然而因為可與使用者註冊的資料結合、比對，而得以識別出特定個人，因此屬於可間接識別的個人資料，亦受到個資法保護。其中，關於行動電話號碼是否適用個人資料保護法，法務部有做出函釋，認為蒐集者如能將行動電話號碼與其他資料對照、組合、連結而得識別特定個人，即屬個人資料而有該法適用[93]。

以下，針對軌跡資料和位置資訊二種較具爭議性的個人資料，做出進一步的討論與說明。

(1) 軌跡資料：網頁瀏覽紀錄和已下載或已使用的應用程式

軌跡資料例如網頁瀏覽紀錄或已下載或已使用的應用程式紀錄，業者可藉由 cookies、URL 或其他數位追蹤方式[94]等，了解使用者的使用情況和習慣。亦即，軌跡資料係行動應用程式業者在蒐集、處理或利用過程中，所產生的衍生資料

DEPARTMENT OF JUSTICE, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (last visited March 28, 2013).

91 Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privay*, BURKELEY CENTER FOR LAWN & TECHNOLOGY RESEARCH PAPER, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405, (last visited Nov. 29, 2013).

92 法務部民國 91 年 10 月 28 日法律字第 0910037677 號函。

93 法務部民國 102 年 05 月 15 日法律字第 10203502260 號函。

94 由於在智慧型裝置中，業者除了在使用者行動瀏覽網路頁面時，可透過 cookies 追蹤使用者的瀏覽習慣，cookies 無法追蹤使用者的其他行為。因此業界開始開發新的數位追蹤方式（例如，Google 最近宣布其開始開發匿名識別碼），可追蹤行動裝置使用者的一舉一動，甚至可以掌控使用者手邊不同的裝置之使用方式和習慣，以提供客製化的廣告。舉例而言，假若使用者在禮拜一晚上用筆記型電腦搜尋哪一家年夜菜比較好吃，隔天當使用者使用行動應用程式時，廣告業者即可提供某餐廳年夜菜的廣告。*See* Claire Cain Miller, *Google to Pay $17 Million to Settle Privacy Case*, N.Y. TIMES (Nov. 18, 2013), http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html?_r=0.

（log files）。這些資料均可透過與其他資料的比對、組合，可與當事人產生連結，進而識別出特定個人，因此應為間接識別之個人資料[95]。此外，雖然軌跡資料並未規範於個人資料保護法的主文內，惟其有出現於個人資料保護法施行細則第12條關於安全維護措施的規定中，似可推知軌跡資料受個資法保護。

(2) 位置資訊（例如 GPS、WiFi 熱點定位）

行動應用程式業者可透過 GPS 或 WiFi 熱點得知使用者的所在位置，而其所蒐集的位置資訊，雖然無法直接和智慧型裝置相連結，而直接或間接識別出使用者。惟使用者通常在使用行動網路時，通常須註冊使用者的姓名、地址、銀行帳戶資訊，而可與使用者的位置資訊比對、組合，而得識別出使用者的身分。此外，每一隻手機都有獨得的號碼，例如國際行動設備辨識碼（International Mobile Equipment Identity number, IMEI）或國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI），亦可與位置資訊組合、比對而識別出使用者。再者，如果該行動應用程式為付費軟體，則使用者在購買時會提供信用卡卡號，一樣可以與位置資訊比對，而得特定出使用者為何人[96]。因此，位置資訊可能構成個資法第二條「得以間接方式識別該個人之資料」，而受到個資法之保護。

行動應用程式業者蒐集使用者多樣的個人資料，可從中探知使用者的私人生活，業者在處理和利用其所蒐集的個人資料時，應履行個資法所要求的義務。此外，業者不能再以個人資料經過匿名或或去識別性等方式處理，而認為可不用遵守個人資料保護法的規範，在重新識別技術越來越高超，匿名化個資一旦得重新識別出個資當事人，則仍須適用個人資料保護法。就法律層面上，雖然重新識別的個人資料須適用個資法，惟如果個人資料保護法的適用範圍過廣，將會導致科技發展遲緩，進而影響社會經濟的不良影響，因此實務在判斷匿名化或重新識別資料是否適用個人資料保護法時，應依照個案，綜合評估使用脈絡、運用重新識別技術的難易程度、以及對當事人隱私侵害的實質風險，盡量達到法律保護與科技發展間的平衡。

2.5. 行動應用程式與個人資料保護之關係

無論是採取「老大哥」或者「審判」作為隱私問題的隱喻，其實二派學者所要表達的共通概念，都是當事人對個人資料失去控制。綜合前文所述可知，行動應用程式的特性和風險是一體兩面，一方面行動應用程式提供多元種類的功能，並匯聚在同一個智慧型裝置中，十分便利，也加深了人們對智慧型裝置的黏著與依賴。然而，另一方面，有廣泛且多重的業者參與應用程式的提供和處理，並蒐集使用者大量且多種個人資料，記錄使用者的瀏覽資訊和使用習慣，招致使用者的隱私的危機。本文以下將分別從使用者與行動應用程式平台、開發商雙方之觀

95 相同見解，請參見劉佐國、李世德，個人資料保護法釋義與實務，頁 26-27（2012）。

96 *See* Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, 2011 WP 185 (EC).

點，討論行動應用程式與個人資料保護之關係，進一步剖析此一錯綜複雜的當代議題。

2.5.1. 使用者的觀點

使用者當然希望能使用到免費、方便又好用的行動應用程式，也因為這種心態而產生了隱私矛盾（privacy paradox），一方面很在意自己的隱私，希望自己的個人資料可獲得保護；但另一方面當業者提供更方便、更快速、更省錢、更好用和更安全的應用程式後，使用者反而會放棄可能功能較差，但對隱私較有保障的功能或應用程式[97]。

對於較著重隱私權的使用者而言，雖多數業者主動提供隱私權政策以及詳列權限清單（permissions）作為隱私聲明[98]，然而隨著隱私聲明逐漸法律化、技術化，多數使用者往往看不懂其中內容，或者根本懶得在小小的手機螢幕上看那密密麻麻的條款，而直接勾選「同意」。此同意的背後，實為使用者的「不」知悉！若認為使用者在此狀況下已知曉其個人資料將被利用之方式，而大幅降低其隱私合理期待與保護強度，個人資料保護勢將流於表面[99]。業者在隱私聲明的陳述過於概括或不明確，也是一大問題。例如 Google 在隱私權政策中指稱：「我們會將個人資訊提供給我們的關係企業或其他可信賴的公司或人員，請他們根據我們的指示，並遵守本《隱私權政策》和任何其他適當的保密和安全措施，代為處理這類資訊。」[100]然而究竟何謂「其他可信賴的公司或人員」，又有哪些公司或人員符合此處 Google 隱私權政策的要求，使用者無從得知，更遑論其閱讀隱私權政策之後，得以瞭解其個人資料最終會流向何方。事實上，目前許多行動應用程式開發商乃是個體戶，並不瞭解應該如何撰寫隱私權相關政策，卻仍然蒐集大量使用者的個人資訊，對使用者的隱私權益保障實乃為一大漏洞。

再者，隱私設定操作複雜、項目繁瑣，有些項目甚至是手機一買來就預先設定開啟或同意（如 Android 系統的定位設定）。一般使用者可能因沒耐性，或不

---

97 HELEN NISSEMBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 104-05 (2010). 相同見解可參考：Nicole A. Ozer, *Putting Online Privacy Above The Fold: Building A Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 220-231 (2012). *See also* MARY LOU ROBERTS & DEBRA ZAHAY, INTERNET MARKETING: INTERGRATING ONLINE AND OFFLINE STRATEGIES 412-19 (2013); John Deighton, *The Right to Be Let Alone*, 12 J. INTERACIVE MARKETING 2 (1998).

98 以 Google Play 商店為例，使用者在 Google Play 選擇欲下載的行動應用程式後，會出現行動應用程式介紹頁面，部分行動應用程式開發者會同時附上服務與使用條款（Terms of Service），以及隱私權政策的連結。當使用者按下「行動應用程式」下載鍵後，即出現權限清單，載明欲蒐集的資料，當使用者點選「接受並下載」，行動應用程式平台（在此為 Google Play 商店）與應用程式開發商即在使用者同意下，開始蒐集、使用、散布其個人資料。

99 Dave Asprey, *Oblivious Data Loss and the Wild West of Mobile App Security*, TREND CLOUD SECURITY BLOG (Apr. 12, 2012), http://cloud.trendmicro.com/oblivious-data-loss-and-the-wild-west-of-mobile-App-security/.

100 隱私權政策，Google，https://www.google.com.tw/intl/zh-TW/policies/privacy/（最後瀏覽日期：2013 年 4 月 23 日）。

知該如何設定或選擇退出（opt-out），而喪失個人資料自主控制的機會[101]。甚至應用程式每一次的更新，都有可能調整權限清單或者個人資料蒐集種類，使用者不一定能夠察覺其中的差異；尤其假若使用者讓應用程式自動更新，使用者更不會得知權限清單是否更動，而造成使用者原先同意使用個資的範圍，和實際使用個資的內容並不一致。最後，使用者難以憑藉一己之力，得知業者是否真如其隱私聲明所述，僅蒐集隱私聲明所列舉之資料，以及蒐集的資料究竟流去何方。由此觀之，在與行動應用程式互動過程中，使用者在目前的行動商務交易環境之中，在個資使用與保護方面經常被迫落居於被動、弱勢之一方。

2.5.2. 行動應用程式平台與開發業者的觀點

行動應用程式業者蒐集個人資料之目的，整體而言其一乃是為了行動應用程式本身運作、改良、客製化所需；其二則是作為開發新軟體的基礎；其三則是將蒐集的個人資料經分析或整理後，賣給第三方業者如廣告商，獲取利潤[102]。當代行動商務的一大特色乃是客製化，客製化的廣告為其具體展現形式其中之一。行動應用程式平台與開發業者的主要經濟收益，也正源自為第三方業者提供廣告所獲得的金錢收入。而就業者轉賣個資的情況而言，此時使用者之個人資料，在功能上猶如使用者免費使用該行動應用程式之金錢對價。

在此背景下，業者多半主張個資保護應該交由市場機制，透過業者間彼此競爭或是業者自律，自然形成切合市場實況與產業需求的個資保護機制。例如目前已有行動應用程式業者依照使用者之需求，進行主動告知，將個人資料蒐集種類標準化，並將通知簡明化，列舉出主要蒐集（collect）、分享（share）的個人資料，以落實使用者資訊自決之權利。然而，即便行動應用程式業者有意提供事前的隱私通知，鑑諸行動應用程式開發商多半是中小企業，甚至是個人工作者，其是否有能力自動自發地提供完善的隱私保護措施，不禁令人懷疑。按無論是事前的隱私聲明，抑或是事後的個人資料管理，均須耗費一定幅度的規劃建置與操作成本。目前市場上形形色色的應用程式開發商是否具有足夠能力與意願，透過彼此自律或是在市場壓力之下，自發性地建置足以維護使用者資訊自決與網路隱私的保護與告知機制，實在不無疑問。

2.6. 行動隱私的管制機制

當面對快速發展並改變人類文明與生活的資訊科技時，法律應採取何種管制途徑保護使用者的隱私，一直是各國政府和各界學者討論、爭辯的議題。因此，在探討應採取何種手段保護行動應用程式使用者的隱私前，先決問題是法律應採取何種管制途徑。誠如前文所述，從使用者和業者對行動應用程式和隱私關係的態度，可以粗略地觀察出二種科技管制政策的模式：市場機制和政府管制[103]。在進入下一個章節，比較歐盟、美國與國際層次對行動隱私的政策與回應前，本文欲先簡要地探討隱私保護的途徑與管制模式。

---

101 *Id.*

102 參考劉翰謙，走向免費的商用軟體，數位時代，http://www.bnext.com.tw/article/view/id/22985（最後瀏覽日期：2013 年 8 月 18 日）。

103 *See* Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J. L. & TECH. 229, 231-244 (2004).

政府管制模式的目的，在於強化使用者對個人資料的控制權力。政府可以透過訂立法規，明確規範資料的控制者如何蒐集、處理、利用、保存或傳輸，以及相關的法律義務；亦或是制定隱私標準，予以規範業者的行為模式。然而，政府管制機制為人所詬病的地方，在於政府介入管制往往會產生選擇性審查的結果，而偏好或歧視特定科技，造成市場扭曲的情況發生，剝奪使用者自主決定的機會[104]。此外，亦有認為政府已經事先替使用者決定隱私保護的程度，但部分使用者可能並不在意自己的隱私，形成政府管制過與家長式作風的情形[105]。因此，開始有訴諸市場機制，使用者和業者自行協調出隱私保護措施的聲浪。

市場機制的核心思想是：在使用者和業者的利益間取得權衡，協調出隱私保護的程度和密度。以行動應用程式下載為例，使用者將其保護隱私的態度，反射在選擇行動應用程式上。在市場機制下，使用者因為在意其隱私，因此會選擇下載較能妥善保護隱私的行動應用程式；同時，業者為能滿足使用者的需求以及吸引使用者的目光，提升市場競爭力與塑造商譽，因此自然而然會改善應用程式的隱私設定，加強自身的隱私操作措施。

Jerry Kang 教授認為，原則上可以透過契約的方式約定，僅能在功能上有必要的情況下，方得處理個人資料，加以保護使用者的隱私[106]。產業內的約束與自律，透過業者的倫理規範，亦為保護使用者隱私的方法。業者藉由張貼隱私權政策、隱私權標章（privacy statement）、甚至隱私權標識（privacy icon）[107]或科技輔助等模式，達到保護使用者隱私的結果[108]。

David Brin 教授在「透明社會：科技是否迫使我們在隱私和自由間做出選擇（The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom，中文譯本為：透明社會：個人隱私 vs. 資訊自由）」一書中，主張透明化或開放社會，是最符合市場機制，也最具有經濟效率的方法。如同美國的陽光法案或政府資訊公開法，政府掌握人民個人資料的同時，政府亦須公開其處理、利用人民個人資料的程序與措施，藉由彼此公開的方式，達到透明、公開的效果。同樣地，業者蒐集、了解使用者的個人資料的同時，業者亦須要對等地公開其如

104 劉靜怡，「社群網路時代的隱私困境：以 Facebook 為討論對象」，台大法學論叢，第 41 卷第 1 期，頁 27（2012）。*See* also Ming-Li Wang, *Information Privacy in a Network Society: Decision Making Amidst Constant Change*, 5 NAT'L TAIWAN U. L. REV. 127, 131-35 (2010).

105 *See* DANIEL J. SOLOVE, *supra* note 29, at 92.

106 *See supra* note 28, at 1256-68.

107 以隱私權標識（privacy icon）為例，Disconnect 公司（Disconnect, Inc）與 Mozilla 公司所領導的工作團隊研發，Ocupop 公司設計的出隱私權標示的產品。類似創用 CC（Common Creative）的概念，藉由不同的符號，告知使用者該網站蒐集個人資料的方式。*See Hover Over An Icon To Read Their Definitions*, DISCONNECT, INC, https://icons.disconnect.me/icons (last visited Dec. 19, 2012). *See also* Somini Sengupta, *Building an Iconography for Digital Privacy*, THE NEW YORK TIMES, http://bits.blogs.nytimes.com/2012/11/19/building-an-iconography-for-digital-privacy/?nl=technology&emc=edit_tu_20121120 (last visited Dec. 19, 2012). 另參見陳裕涵，網際空間中之隱私權保障—以社群網站為中心，國立台灣大學法律學院法律學研究所碩士論文，頁 144-49（2013）。

108 *See* DANIEL J. SOLOVE, *supra* note 29, at 79-80. *See also* Clark D. Asay, *Consumer Informtion Privacy and the Problems of Third-Party Disclosures*, 11 NW, J. TECH. & INTEEL. PROP. 321, 328 (2013).

何處理、利用和傳輸使用者的個人資料[109]。在對等公開、透明的情況下，業者和使用者的地位趨於平衡，使用者的隱私可以受到保護。綜前所述，可觀察到市場機制的支持者共同認為，透過市場機制可降低管制成本，透過使用者和業者間的協商，與業者彼此間的自律，即可協調出彼此都能接受的隱私保護機制。其次，市場機制可確保彈性，得隨時掌握市場的需求，而調整隱私保護的手段和方式[110]。

市場機制順利運作的前提是：市場確實可以提供使用者隱私的真正保護，惟此前提是否成立不無疑問。首先，藉由契約雖然確實能限制業者處理、利用、分享使用者個人資料的行為，然而契約的效力僅及於當事人和業者之間，無法涉及超出契約關係的第三方業者[111]。以行動應用程式下載為例，通常廣泛利用使用者個人資料者為第三方業者，如廣告業或是資料分析產業。然而使用者無法在下載應用程式時，得知第三方業者為何人，更不可能得知第三方業者的隱私操作內容。此際，使用者只能信任行動應用程式業者，確實會替使用者把關，將使用者的個人資料分享給可確保使用者隱私的第三方業者。其次，市場機制的前提建立在使用者和業者是對等的情況，然而實際上雙方處在不對等的地位。使用者難以明確、有效率地表達其所希望的隱私保護偏好，甚至於部分使用者不了解隱私對其的意義，而認為毋庸在意隱私。

此外，科技改變了社會模式，傳統的商務模式逐漸轉變為現在廣泛結合社群網路與網際網路的行動商務，使得業者與使用者的關係不對等的情況更趨嚴重。舉例而言，以免費社群通話軟體，當周遭親朋好友都在使用社群通話軟體，在群起效尤及外緣影響下[112]，即便對個人資料蒐集有所顧忌，多數人仍會下載。此時，市場制衡的關係減弱，使用者無法扮演監督與推動改善的角色。最後，在透明化以及業者自律的模式中，業者一般透過隱私通知告知使用者其隱私操作，惟隱私聲明的內容與範圍並不一定和實際上的隱私操作相同。此外，閱讀隱私聲明亦非多數使用者的習慣，在使用者沒有耐性閱讀隱私聲明，無法了解業者的隱私實踐，因此無法理性地選擇是否要使用業者提供的服務[113]。凡此種種促成隱私聲明的效度不足，令使用者和業者間存在資訊落差，而加重雙方地位之不平等。

綜言之，行動隱私的管制機制中，如果以光譜的方式呈現，光譜的最右端為完全的市場機制，最左端則是完全的政府管制。然而鑑於採取完全的市場機制或完全的政府管制，均無法同時兼顧保護使用者隱私和促進科技革新的利益。因此目前各國在採取行動隱私的管制政策時，均游移於光譜的中間區段：如歐盟和我

109 David Brin 著，蕭美惠譯，「透明社會：個人隱私 vs. 資訊自由」，頁 38-43（1999）。

110 劉靜怡，前揭註 104，頁 29-35（2012）。

111 *See* DANIEL J. SOLOVE, *supra* note 29, at 81.

112 所謂外緣影響係指，縱然人們嘗試要依理性行事，但是此能力會由於認知和資訊取得的侷限而受到限制，產生「受限理性」。當一個人的經濟行為受到交易本身以外的任何事物影響時，經濟學家稱之為「外緣影響」，例如從在車站跟著人潮走，到選擇手機的電信服務。參考鄧肯．華茲著，傅士哲、謝良瑜譯，「6 個人的小世界」，頁 241-51（2004）。

113 *See supra* note 29, at 83-85.

國者，採取以政府管制為主，市場機制為輔的管制機制；如美國者，則採取以市場機制為主，政府管制為輔的管制模式[114]。在第參章「歐盟、美國和國際層面對行動隱私的回應與法律政策」，可更清楚地觀察出歐盟、美國和國際層面上，在行動隱私管制機制方面，各採取的管制途徑。

114 翁清坤，「告知後同意與消費者個人資料之保護」，臺北大學法學論叢，第 87 期，頁 50（2013）。

三、　歐盟、美國和國際層面對行動隱私的回應與法律政策

在個人資料與隱私保護方面，目前國際間最具影響力，也最常受到相關組織與國家立法引用之國際規範原則者，厥為 OECD 隱私準則）」。惟此一準則雖然廣泛受到各國引用，然其並非正式之國際條約，亦尚未取得國際習慣法之地位，並不具有國際法上之法律拘束力，僅提供各國在國內法上自願參考遵循之用，無法在國際層次的隱私糾紛真正發生時，作為爭端解決所適用的準據法規範。

隨著網路科技與智慧型裝置日新月異，個人資料不再侷限於國界，進入全球化的範疇。以目前最熱門的 Candy Crush Saga 為例，開發者 King 公司為英國的社群遊戲（social game）業者，藉由多種平台（包含 Facebook、iOS 和 Android 平台），提供遊戲應用程式，供全球各地之智慧型裝置使用者日常遊樂之用[115]。由於目前尚無國際性的隱私規範可資遵循，King 公司設計、提供 Candy Crush Saga 之際，究竟應該適用哪一套或是哪一國家的個人資料保護法規？筆者在本部分將分別闡述歐盟、美國和國際層次上，在行動應用程式領域當前法制規範發展及對業者所提出的建議，並且附帶從應用程式個人資料傳遞之全球性特質與域外效力（extra-jurisdictional effect）出發，思量是否可透過國際合作加以因應。

115　*About us*, KING, http://about.king.com/about (last visited May 20, 2013).

3.1. 歐洲聯盟

3.1.1. 現行法：個人資料保護指令

歐洲國家於人權與基本自由保護公約（the Convention on the Protection of Human Rights and Fundamental Freedoms）第 8 條之中，共同肯認隱私權為基本人權之一[116]。歐洲聯盟（European Union, EU，以下簡稱歐盟）在 1995 年通過「歐洲議會暨理事會關於保護個人資料的處理與個人資料自由流通（95/46/EC）指令[117]」，簡稱個人資料保護指令（The Data Protection Directive），於 1995 年 10 月 24 日公布，1998 年 10 月 25 日於各會員國正式生效，以一貫、全面的法律保障會員國公民的隱私，共計七章。各會員國雖須遵守個人資料保護指令，惟仍可依各國國情，制定各自的個人資料保護法規，以徹底貫徹個人資料保護指令。個人資料保護指令直接對歐盟公民產生效果，一旦有侵害隱私權的情事發生，歐洲公民得向負責執行個人資料保護指令之歐盟機關，或其所屬的國家機關請求救濟。

歐盟近來推動個人資料保護指令的修正，並於 2012 年 1 月 25 日公布個人資料保護規則草案（The Proposed General Data Protection Regulation）。修正的理由主要有三：其一，基於各會員國在實踐個人資料保護上，步調逐漸出現差異；其二，隨著科技急速發展與全球化發展，對個人資料保護帶來新的挑戰，包含行動上網、定位資訊、以及電子商務，為使個人資料保護指令能足以因應數位時代的來臨，因此有修正的必要；其三，歐盟要確保業者提供服務予歐洲居民時，無論該業者是否為歐盟公司，均遵守個人資料保護指令之規定，以確保歐盟公民的隱私權得到妥適的保護[118]。

3.1.2. 對行動應用程式蒐集個人資料的因應

歐盟個人資料保護第 29 條工作小組（Article 29 Data Protection Working Party），在 2013 年 2 月 27 日公布對於智慧型設備（smart device）應用程式的意見書[119]。

---

116 「一、人人有權使他的私人和家庭生活，他的家庭和通信受到尊重。二、公共機關不得干預上述權利的行使，但是依照法律的干預以及在民主社會中為了國家安全，公共安全或國家的經濟福利的利益，為了防止混亂或犯罪、為了保護健康或道德、或為了保護他人的權利與自由，有必要進行干預者，不在此限。」，歐洲人權公約，社團法人中華人權協會，http://www.cahr.org.tw/lawdan_detail.php?nid=105（最後瀏覽時間：2013 年 4 月 14 日）。*See* European Convention on Human Right art. 8, *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf (last visited Nov. 29, 2013).

117 *Directive 95/46/EC of The European Parliament And of The Council of 24 October 1995 on The Protection of Individuals With Regard to The Processing of Personal Data And on The Free Movement of Such Data*, EUR-LEX, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited Dec. 18, 2012).

118 *Why do we need an EU data protection reform?*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (last visited March 29, 2013); *Speech: The EU's Data Protection reform: Decision-Time is Now*, EUROPA, http://europa.eu/rapid/press-release_SPEECH-13-197_en.htm (last visited March 29, 2013).

119 Opinion 02/2013 on Apps on Smart Device, 2013 WP 202 (EC).

意見書中指出行動應用程式對終端使用者（end user）個資保護所造成的主要風險有二：其一，欠缺透明性，因為多數應用程式業者未提供隱私權政策或給予事前充分的告知，以及缺乏對應用程式處理個人資料種類的認知；其二，資訊安全措施不足。

歐盟目前對於行動應用程式之個資蒐集規範，除了個人資料保護指令第七條對於處理個人資料應得當事人同意之規定外，主要係依據電子通訊隱私指令（Directive on Privacy and Electronic Communications, ePrivacy Directive，簡稱電子隱私指令）[120]前言第 24 段[121]和第 5 條第 3 項[122]的規定。依照該等規定，公共可用的電子通訊服務和公共通訊網絡內的任何資訊（any information），均受到該指令的保護和規範，且當事人個人資料受到保護的權利，均不得移轉或以契約放棄之。在本意見書中，第 29 條工作小組進一步將行動應用程式業者區分為四大類：應用程式開發商、作業系統商和設備製造商、應用程式商店和其他介入個人資料處理的參與者，分別提出對其個資蒐集活動之規範意見。

1. 應用程式開發商

應用程式開發商為主要的資料控制業者（data controller），同時為主要遵守歐盟個人資料保護指令的主體。其必須遵守電子隱私指令第 5 條第三項，事前告知（inform）使用者將會如何處理其個人資料。告知的內容包含：資料的種類或應用程式機會接近那些設備，並將這些資訊詳細且精準地寫在隱私聲明中。並且在資料外洩時，依照電子隱私指令的規定，應及時告知使用者。同時，程式開發商必須和作業系統與設備製造商合作，設計出既能清楚呈現隱私聲明，又可符合智慧型裝置介面和螢幕大小，方便使用者閱讀的告知方式。

---

120 Directive 2002/58/EC, 2002 O.J. (L 201) (EC).

121 (24) 使用者在電子通信網絡的最終設備，和儲存任何資訊設備，是使用者的部分私領域須受人權和基本自由的歐盟公約的保護。所謂間諜軟體（spyware）、網路爬蟲（Web Bugs）、隱藏識別字（hidden identifiers）和其他相似的設備可進入使用者的終端設備（terminal），使用者對近用資訊沒有認知，而儲存隱藏資訊或追蹤使用者的活動，恐嚴重侵擾使用者的隱私。上述設備對使用者的使用，應僅限於合法的目的，並讓使用者認知。“(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.”. *See id.*

122 3. 會員國應確認電子通訊網路設備的使用，在儲存資訊或進用訂閱者或使用者儲存在終端設備的資訊，僅允許於使訂閱者或使用者了解，根據電子隱私準則提供清楚和完整的資訊，包含處理的目的和提供拒絕資料控制者的權利。不應避免任何技術的儲存，或近用的目的僅為實施，或促進通過電子通信網路的傳送，或在絕對必要下，在訂閱者或使用者明顯的請求，提供資訊社會服務。“3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.”. *See id.* § 5(3).

除此之外，應用程式開發商亦應開發工具讓使用者得接近、修改其個人資料，或客製化其個人資料受到處理、利用的保存期間。在資料保存期間，程式開發商必須遵守個人資料保護指令和電子隱私指令的安全措施[123]。簡言之，應用程式開發商必須謹遵目的限制原則和安全義務，個資蒐集與處理之目的必須完全揭露，藉以強化使用者對個人資料的控制權力。

2. 作業系統和設備製造商

作業系統和設備製造商所處理資料，包括使用者一般性的資料（例如註冊資料）、設備自動產生的資訊、作業系統處理的個人資料、以及透過應用程式介面處理的個人資料。在某種程度上來說，作業系統和設備製造商也是資料控制者。因此，作業系統和設備製造商須定期更新應用程式介面，提供使用者充分的控制權，並在應用程式處理資料前，可行使有效的同意權，以貫徹「從設計著手保護隱私」（privacy by design）此重要原則[124]。其次，意見書要求本類業者應避免秘密監視使用者，並確保資訊安全以及安全的個人資料處理。其三，業者應提供有效且友善於使用者的措施，以避免使用者受到廣告業者或其他第三方業者追蹤。最後，本類業者應確保應用程式蒐集的任何一項個人資料，都和事前告知使用者的個人資料種類相同[125]。

3. 應用程式商店

應用程式商店一方面是資料控制者，負責前階段的付款手續，以及支援應用程式加購功能（in-app purchase），因而處理使用者登記的姓名、地址和財務資訊，甚至是信用卡卡號等直接可識別的個人資料。另一方面，應用程式商店主要扮演監督應用程式開發商的角色，兩者唇齒相依。因此程式商店除了要遵守歐盟個人資料保護指令和電子隱私指令的規範外，同時亦須確認應用程式開發商是否履行讓使用者知悉的義務，以及告知的內容是否與實際處理個人資料的情況相符。此外，此類業者應提供使用者意見平台，讓使用者得以抒發其使用應用程式的心得，以及回報安全或隱私的問題。最後，應用程式商店應和應用程式開發商合作，開發強化使用者控制個資的工具，例如指引使用者接近使用個人資料的符號。應用程式商店亦應提供遠端移除應用程式的功能，方便使用者移除應用程式。此類業者應提供使用者意見平台，讓使用者得以抒發其使用應用程式的心得，以及回報安全或隱私的問題。最重要的是，應用程式商店應提醒非歐盟的應用程式開發商，歐盟個人資料指令和相關法規的規定，例如同意的要求，以及將個人資料傳輸至非歐盟會員國的要求[126]。

4. 其他介入個人資料處理的參與者

其他介入個人資料處理的參與者，也就是所謂的第三方業者，包含廣告業者、資料分析業者和通訊服務業者，屬於資料處理者（data processor）。其藉由個人資

123 *Supra* note 119, at 9-10, 18, 27-28.

124 *See* Council Directive 95/46/EC, art. 16-17, 1995 O.J. (L281) 38 (EC). 其中個人資料保護指令前言第 46 段和第 17 條，提出「從設計著手保護隱私（Privacy by design）」的重要原則，係指在新產品或新服務的設計階段就要考慮個人資料保護問題。

125 *Supra* note 119, at 10, 11, 21, 29.

126 *Id.* at 11, 20-21, 28-29.

料的處理，來提供客製化的服務。廣告業者可以藉此提供符合使用者個人消費傾向的客製化廣告，以增加買氣與廣告點擊率。資料分析業者則可向應用程式業者提供客製化的報告，詳列使用者的使用習慣、應用程式的熱門度、應用程式的使用模式等。至於通訊服務業者，可以透過個資的蒐集和處理，決定各行動設備的預設模式和資訊安全，並且處理個別應用程式所使用的資料。

同時，第三方業者也是資料控制者，例如資料分析業者為能提供額外的應用程式熱門程度和客製化的建議，而蒐集許多個人資料。此時，本類型業者除了要遵守電子隱私指令第 5 條第三項事前同意的規定外，並應不得執行任何追蹤使用者個人資訊的程式，貫徹「Do Not Track」的機制。此外，廣告業者須分外注意，廣告的內容不得逾越使用者使用應用程式的情境脈絡（context），例如改變瀏覽器的設定或者置放圖示於智慧型裝置中[127]。

除了行動應用程式各參與者的責任與守法義務外，本意見書中另外揭示一大重點：同意與告知。同意的作成有三大要件：首先，使用者對同意權的行使有選擇權（freely given），得以選擇接受或拒絕業者處理使用者的個人資料；其次，使用者在同意前須受妥適的告知（informed），在應用程式下載前，業者即刻告知資料處理等相關資訊[128]，尤其假若業者蒐集的個人資料涉及敏感性資料，當事人應獲得知悉所做的同意，方為有效；其三，同意權的行使須特定（specific），概括式的同意不能視為有效[129]，業者依法須告知其蒐集、利用或處理個人資料的特定目的，並就該行為取得使用者的同意。此外，針對所蒐集的每一個種類的個人資料，都須取得相對應的使用者同意[130]。簡言之，業者的每一個通知內容必須特定，不得將多種通知內容包裹成一個通知，讓使用者作概括的同意；而且也不得將使用者的「下載」，視為個人資料蒐集的同意。

至於告知資訊的內容、方式和形式，根據個人資料保護指令第 10 條和第 11 條，各資料當事人有權知悉資料控制者的身分，是誰在處理當事人的個人資料；

---

127 *Id.* at 12-13, 21, 30.

128 意見書採取和美國聯邦交易委員會「行動隱私揭露——透過透明建立信任（Mobile Privacy Disclosures: Building Trust Through Transparency）」的幕僚報告（Staff Report）相同的見解。關於美國聯邦交易委員會對行動應用程式隱私保護內容，請參見本文 3.3.1.2。*See Supra* note 118, at 22.

129 意見書中舉例，使用者只是按下「同意下載」，不能視為有效同意，因為同意不能作為概括、形式性的授權。*See supra* note 119, at 15.

130 特定區分成時間的特定與內容的特定。就時間特定的部分，意見書中舉例，假若應用程式開發業者提供一個「附近有哪些餐廳」的應用程式，在使用者下載前，應用程式開發業者必須取得使用者的同意。例如開發業者須使用使用者的位置資訊，業者除了在下載前須取得使用者的同意外，在使用者使用應用程式的當下，亦須徵求使用者同意應用程式近用位置資訊，且該同意僅限於使用者使用應用程式的時候。就內容特定的部分，假若此係為通訊應用程式，會近用使用者的通訊錄，使用者必須有權利可以挑選使用者欲通訊的對象，而不是整個行動裝置通訊錄上所有人，都會出現在該通訊應用程式的聯絡人中。相對地，意見書亦提出不符合特定要求的同意範例，例如鬧鐘應用程式提供一個選項，讓使用者能透過口頭指令將鬧鐘靜音或啟動賴床模式。因此使用者對錄音的同意僅限用在鬧鐘鈴響時，任何在鬧鐘還沒響時的監控、錄音或收音已超出使用者的同意範圍，該行為係不法。*See id.*

此外，使用者也有權利知悉資料處理的種類、目的和方式。簡言之，業者的告知至少應把握 5W：誰在處理當事人的個人資料（Who）、應用程式開發商蒐集哪種個人資料（What）、為何要處理這些個人資料（Why）、這些資料是否會揭露與第三方業者（Whether）、以及使用者有哪些權利，包含撤銷同意權或刪除權（What）。然而若資料控制者能再提供蒐集或近用資料的比例性考量、資料保留期間的長度、將採取的資訊安全措施、以及業者處理個人資料符合歐盟法規（若為歐盟外地區，以美國為例，則闡明符合安全港條款），則更為妥當。

告知的內容除了使用者應用程式下載前揭露外，下載後也要提供使用者相關資訊，讓使用者得以隨時檢視隱私設定或個人資料處理內容。告知的內容必須得以接近，放在頁面中顯而易見的位置，且使用者可在應用程式商店中可對應用程式開發商，發表評論或意見。最後，每一個應用程式應提供可閱讀、好理解、且容易接近的隱私權政策，隱私權政策的內容至少須包含前述內容，並且為了方便行動設備使用者閱讀，可在下載頁面上，將隱私權政策的關鍵內容以簡要方式寫出，並附上隱私權政策完整版的連結，供使用者點閱[131]。

3.1.3. 小結

歐盟基於人性尊嚴與人格權的維護，將個人資料保護置於基本人權的高度[132]。歐盟的個人資料保護指令乃是其他國家經常效仿的立法方式，可以藉由單一立法和單一監督機關，妥善保護個人資料。但亦有論者對之提出批評，其一，歐盟個人資料保護指令的立法意旨一方面要保護個人資料，另一方面又試圖讓個人資料自由流通，自相矛盾[133]。另有論者認為，歐盟所採取的立法政策猶如唐吉軻德，將業者視作風車，處處都要提防。誠如第二章所述，業者蒐集資料除了私利外，亦將使用者的個人資料當作研發、改良的基礎，假若政府管制色彩濃厚，家長式作風下，介入資訊市場的運作，不一定符合資訊社會的期待與隱私意識，反而使科技業者捉襟肘見[134]。

無論是現行的指令規定或擬議中的規則草案，歐盟的個人資料保護指令均對業者告知與使用者同意設有嚴謹規定，對於人民的個人資料提供完善的保護。個人資料保護第 29 條工作小組在智慧型設備（smart device）應用程式的意見書中，也充分體現此一概念。意見書提供各類業者非常完整、具體和清楚的建議與適法準則，並將焦點著重在應用程式開發商的法律責任以及通知和同意機制。

---

131 *See* Opinion 10/2004 on More Harmonised Information Provisions, 2004 WP 100 (EC) at 4-5, 8-9; and *id.* at 23-24.

132 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L. J. 1151, 1164-71 (2004).

133 DANIEL SOLOVE, *supra* ntoe 71, at 1110 (2012).

134 *See* Peter Fleischer, *Don Quixote*, PETER FLEISCHER: PRIVACY...? (Feb. 17, 2013, 8:33 PM), http://peterfleischer.blogspot.tw/2013_02_01_archive.html.

然而歐盟此種規範方式，也令應用程式業者陷於艱困的處境。首先，誰是隱私聲明的預設閱讀對象[135]？隱私聲明寫得越詳盡，就代表隱私聲明的長度越長[136]，使用者閱讀的可能性也隨之大幅降低。如此一來，隱私聲明告知使用者的實際作用大幅下降，其主要功能反而轉變為政府介入管制的規範根據。從意見書似乎可觀察出，在歐盟現行管制架構之中，隱私聲明必須以兩階段方式呈現（layered notice）：告知使用者的主要方式為簡短的通知，除此之外另須提供隱私權政策，作為當事人進一步了解的輔助工具，以及政府監督、審查的標的[137]。再者，歐盟要求當事人的同意必須特定，不能概括同意。此種規範雖然可以藉由使用者每一次的同意，確保使用者的隱私，然而也增加業者的困擾和疑惑，例如：究竟特定同意的涵蓋範圍可以有多大？[138]此外，使用者在下載應用程式時，往往希望趕快使用應用程式，因此若業者提供過多的同意選項供使用者選擇，使用者是否會認真閱讀，而做出實質有效的同意？況且目前的應用程式業者仍採取「全盤接受，不然就不要用（take it or leave it）」的機制，使用者若在其中一個選項勾選不同意，將無法使用該應用程式。在此情況下，使用者若非常希望使用該應用程式，其所作出的同意，是否具有任意性，不免打上問號。

其次，工作小組意見書要求行動應用程式業者應肩負起監督並了解第三方業者處理使用者個人資料情況的責任，這是否會造成業者過大的壓力，形成過高的風險[139]？最後，工作小組的意見書本身雖然不具有法律拘束力，然而對於會員國國內法的實際影響為何，目前尚未明朗。不過英國在工作小組意見書公布後，已準備要對於國內應用程式開發商進行宣導，並且思考如何將其內容轉化為國內法，與本國法相容[140]。

---

135 Peter Fleischer, *Why Johnny can't read...a privacy policy*, PETER FLEISCHER: PRIVACY...? (March 27, 2013, 4:15 PM), http://peterfleischer.blogspot.tw/2013/03/why-johnny-cant-reada-privacy-policy.html.

136 以 Google 的隱私權政策為例，歐盟多國（包含法國、德國、英國、荷蘭、比利時、義大利、西班牙），均表示將對 Google 的隱私權政策進行審查，個人資料保護第 29 條工作小組也於 2012 年發函要求 Google 其修改隱私權政策，內容主要有三：隱私權政策未能提供充分的資料，包含資料使用的目的與資料種類；隱私權政策包含 60 多種 Google 功能，未能顯示 Google 實際之個人資料運作狀況，且縱有提供相關資料，也散見在不同的地方，使用者查閱不便；最後，Google 未訂有資料保存期限。各國審查將進行數月之久，其最終審查報告的建議方向與 Google 如何回應，值得繼續觀察。 *See Google Privacy Policy: Main Findings And Recommendations*, EU, https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/octubre/Recommendations_Google_EN.pdf (last visited April 22, 2013); *Letter Addressed to Google*, EU, http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/LetterAdressedToGoogle.pdf?__blob=publicationFile (last visited April 22, 2013).

137 Opinion 15/2011 on the Concept of Personal Data, 2011 WP 187 (EC) 20.

138 *See* Dan Cooper and Philippe Bradley, *EU Data Protection Working Party Sets out App Privacy Recommendations*, INSIDE PRIVACY (March 15, 2013), http://www.insideprivacy.com/international/european-union/eu-data-protection-working-party-sets-out-app-privacy-recommendations/. 相同見解可參考劉定基，「析論個人資料保護法上「當事人同意」的概念」，月旦法學雜誌第 128 期，頁 156-58（2013）。

139 *See id.*

140 Saira Nayak, *Response to EU Opinion on Mobile Apps*, TRUSTE BLOG (March. 14, 2013), HTTP://WWW.TRUSTE.COM/BLOG/2013/03/14/RESPONSE-TO-EU-OPINION-ON-MOBILE-APPS/.

3.2. 美國

美國將個人資訊保護議題，定義為「資訊隱私（information privacy）」[141]，在立法政策上，以尊重市場機制為主，政府管制為輔。美國傳統上以通知和同意機制（notice and consent）為主，最早起源於 1973 年聯邦衛生教育福利部（Department of Health, Education and Welfare）所提出的「公正資訊處理原則（Fair Information Practice Principle, FIPPs）」[142]。「公正資訊處理原則」內含五大子原則：通知／知情原則（notice/awareness），告知資料主體何時、如何、以及基於何種目的蒐集當事人的個人資訊；選擇／同意原則（choice/consent），當事人就如何蒐集任何可能被使用的個人資訊，具有選擇、同意權；接近／參與原則（access/participation），當事人可檢視其所受蒐集的個人資訊，並有機會更正或完整該資訊；資訊完整／安全原則（integrity/security），業者應妥善保護、保管消費者的個人資訊；以及執行／救濟原則（enforcement/redress）。公正資訊處理原則是美國無論聯邦層次或各州層次，均採用並且實際執行的政策與內容。

在聯邦層次上，美國採取部門（sectoral）立法，依照各部門所遭遇的不同狀況與立法需求，分別立法[143]。在各州層次上，部分州政府訂有專法規範網路個人資訊（personal information）蒐集[144]，本部分將以其中最具代表性的加州為例進行評介。

---

141 美國法上判斷是否受到隱私權保護的核心概念為「合理隱私期待」，其規範基礎為美國聯邦憲法增修條文第四條。此概念源自於 Katz v. United States 案，John Harland 大法官協同意見書對於多數意見的理由補充；其認為合理隱私期待的兩個前提要件為：（一）當事人主觀上必須表現對隱私有真正的期待；（二）其期待必須是社會認屬「合理的」。亦即不只考量到當事人主觀上是否具有隱私期待，社會上一般客觀的觀念也必須肯認此種隱私期待具合理性。參考簡郁庭，「個人資料揭露案例之研究－－以隱私權保障為中心」，國立臺灣大學社會科學院國家發展研究所碩士論文，頁 37（2008）。

142 *See* Fair Information Practice Principles, Federal Trade Commission, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited March 29, 2013); and JONATHAN D. HART, INTERNET LAW: A FIELD GUIDE 375 (2008). 公正資訊處理原則也影響了 1980 年 OECD 隱私準則和歐盟後來的立法。*See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1882 (2013). 另參見邱文聰，前揭註 78，頁 173（2009）。

143 參考周慧蓮，「資訊隱私保護爭議國際化」，月旦法學雜誌，第 104 期，頁 114（2004）；翁清坤，「論個人資料保護標準之全球化」，東吳法律學報，第 22 卷第 1 期，頁 23（2010）。

144 *See* HART, *supra* note 142, at 369.

3.2.1. 聯邦法層次

3.2.1.1. 一般網路消費者的隱私權保護

在涉及使用者的網路個人資訊蒐集議題，美國雖有個別部門立法可供援引[145]，然而至今聯邦層級尚無對於非公務機關個人資訊蒐集的概括式立法，僅針對兒童制訂了「兒童線上隱私保護法」（the Children's Online Privacy Protection Act, COPPA）[146]。因此，在遇到網路或行動商務隱私問題時，有賴聯邦交易委員會（Federal Trade Committee, FTC）擴張解釋聯邦交易委員會法第 5 條對於欺罔（deceptive）與不公平（unfair）行為的規範，而得以對於相關個資爭議進行管制。然而隱私管制須因應科技沿革而有所調整，為能更為妥適地保護消費者的隱私，近年來聯邦交易委員會與白宮分別提出新的解決方式與管制框架[147]。

聯邦交易委員會在 2012 年 3 月提出「保護快速變遷時代下的消費隱私——給業者和政策制定者的建議（Protecting Consumer Privacy in an Era of Rapid Change—Recommendations for Businesses and Policymakers）」之報告書[148]，詳列聯邦交易委員會目前執法的標準以及建議，並將重點置於業者在個人資料處理上的資訊透明，並且希望透過消費者選項的簡化（simplified consumer choice），以及隱私通知的即時提供，強化消費者的資訊自決權。

此外，2012 年 2 月美國白宮推出「消費者隱私權法案」（the Consumer Privacy Bill of Rights）[149]，特別針對私人機構在商業領域處理消費者個人資料加以規範，並宣稱即便法案未能獲得國會立法通過，仍希望以之成為聯邦消費者隱私權保護的基本體制與規範架構[150]。本法案的核心內容為消費者應具有個人資料的適當控制權，希望藉由清楚而簡單的隱私通知[151]，以及符合消費者認知的個人資料蒐集、使用和揭露的情境脈絡下[152]，對於使用者給予有意義的同意權。尤其以行動應用程式為例，由於一般智慧型裝置的螢幕都很小，消費者藉由小小螢幕閱讀完整隱私通知有其困難存在，因此業者應該考量智慧型裝置的特性，提供消費者最相關的資訊，並且將通知字體適度放大[153]。

---

145 包含「電腦詐欺與濫用法案（Computer Fraud and Abuse Act）」、「電子通訊隱私法（The Electronic Communications Privacy Act, ECPA）」、「聯邦交易委員會法（The Federal Trade Commission Act）」、「電訊傳播法（The Telecommunications Act）」、「電話用戶保護法（Telephone Consumer Protection Act）」、和「反垃圾郵件法（Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, CAN-SPAM）」、「自律規範（Self-Regulatory Codes）」、「影視隱私保護法（Video Privacy Protection Act）」等。*See* HART, *supra* note 142, at 375; Michael G. Rhodes and Charles A. Schwab, *Mobile Commerce: A Moving Target for Legal Compliance*, *in* UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW 1-31 (2012), *available at* http://www.cooley.com/files/Rhodes%20Excerpts.pdf (last visited Nov. 29, 2013).

146 *See* JONATHAN D. HART, *supra* note 142, at 375.

147 *See* Daniel J. Solove, *supra* note 142, at 1882 (2013).

148 FTC REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited Dec. 25, 2012).

149 THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited Dec. 26, 2012).

150 *Id.* at 5.

151 *Id*. at 14.

152 *Id*. at 15-19.

153 *Id*. at 15.

3.2.1.2. 對應用程式蒐集個人資訊的因應

為解決行動應用程式使用者的個人資訊受到業者不當的處理，聯邦交易委員會在 2013 年 2 月公布「行動隱私揭露——透過透明建立信任（Mobile Privacy Disclosures: Building Trust Through Transparency）」的幕僚報告（staff report）[154]。彙整四十年來處理隱私爭議的爭議，並參考加州檢察署於同年 1 月公布的行動隱私報告，以強調「透明化」（transparency）的方式保護使用者的隱私。該報告書中將行動業者分為四大類：平台（platform）或作業系統（operating system）、應用程式開發商、廣告業者或第三方業者，以及應用程式業者團體，分別規範行動科技招致的隱私風險。

1. 平台或作業系統

(1) 透過接近應用程式介面（Application Programming Interface, API），平台揭露資訊應用程式

平台或作業系統應對消費者提供即時揭露，並在應用程式接近使用者較敏感的內容，例如位置、通話照片、日曆、影片等之前，取得消費者明示同意。因為平台或作業系統猶如儀表板（dashboard）[155]，允許消費者在下載前後可先檢視應用程式將會接近那些資料內容。此外，該報告也建議平台或作業系統利用圖示來告知消費者應用程式現在正在接近使用某些資訊[156]。

(2) 平台監控應用程式

平台或作業系統應扮演監控的角色，因為消費者會期待、相信應用程式商店會對應用程式開發商進行監控。監視的內容包含：其一，和應用程式開發商間的契約中，增加條款要求應用程式開發商蒐集個資時應即時揭露，並在蒐集和分享敏感資訊前，先取得消費者的明示同意；其二，合理執行這些條款。除了監視之外，平台業者亦應該教育應用程式開發者應妥善保護消費者的隱私權[157]。

(3) 透明——應用程式檢審程序

平台業者在提供應用程是給消費者前，應使用不同的檢視程序。

---

154 聯邦交易委員會在報告中指出：「根據 2012 年最後一季的數據調查，全世界消費者總計擁有二億一千七百萬隻智慧型手機，消費者頻繁透過行動裝置為許多消費行為，過程中分享他們的生活資訊給多邊業者，包含無線網路業者、作業系統、分析業者、行動裝置製造商、應用程式開發者和廣告業者。」FEDERAL TRADE COM'N, MOBILE PRIVACY DISCLOSURE—BUILDING TRUST THROUGH TRANSPARENCY 15-18, *available at* http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm (last visited March 21, 2013). 此份幕僚報告延伸自 2012 年聯邦交易委員會所公布的「Marketing Your Mobile App: Get It Right from the Start」報告。*See FTC Publishes Guide to Help Mobile App Developers Observe Truth-in-Advertising, Privacy Principles*, FTC, http://www.ftc.gov/opa/2012/09/mobileapps.shtm (last visited April 20, 2013).

155 以 Google 為例，在「資訊主頁（Dashboard）」中詳列所有 Google 掌握的資料，和行動隱私較相關的，包含：帳戶、個人資料、Android 裝置、Play 商店、日曆、聯絡人等。資訊主頁，Google，https://www.google.com/dashboard/（最後瀏覽日期：2013 年 4 月 16 日）。

156 FEDERAL TRADE COM'N, *supra* note 154, at 15-18.

157 *Id.* at 18-20.

(4) 智慧型裝置之不追蹤（Do Not Track）措施

平台業者應提供智慧型手機使用者不追蹤機制，允許消費者透過智慧型手機瀏覽應用程式時，選擇預防廣告通路或其他第三方業者追蹤[158]。

2. 應用程式開發商

建議應用程式開發商提供隱私權政策，並確保該政策在應用程式商店是容易看到的。藉此完成即時揭露，以及蒐集、分享個人資訊前取得消費者的明示同意。此外，應用程式開發商可以加強和廣告通路或其他第三方業者的合作與溝通，了解廣告業者或第三方業者將處理那些個人資訊，以便能清楚、精確地揭露相關資訊給消費者。最後，建議應用程式開發商加入自律團體，諸如商會或公協會，藉此遵守該機構訂定的統一、簡易型式的隱私權揭露[159]。

3. 廣告業者或第三方業者

廣告業者或第三方業者未能直接面對消費者，因此應與應用程式業者溝通，使應用程式業者得以可信地揭露相關資訊予消費者[160]。

4. 應用程式業者團體

聯邦交易委員會主要認為，可以透過公協會等業者團體的力量，發展出標準化的圖示（icons）、標誌（badges）[161]和隱私權政策，此外業者團體同時也可擔負起教育應用程式業者的責任，協助隱私權業者保護消費者的隱私[162]。

聯邦交易委員會針對智慧型裝置的隱私議題之態度，可從 Path 和解案與 Goldenshores Technologies 公司和 Erik M. Geidl 和解案（以下簡稱 Goldenshore 和解案）來觀察。Path 為社交應用程式開發商，因未告知使用者，且未經使用者同意，蒐集使用者的通訊簿資訊；並且未經未成年使用者的父母同意，蒐集兒童的個人資料，同時違反聯邦交易委員會法和兒童線上隱私權保護法。最終 Path 以八十萬美金的罰鍰（civil penalty）與聯邦交易委員會達成和解。其中，擅自蒐集使用者通訊簿資訊的部分，係因 Path 在隱私權政策中僅表示會自動蒐集使用者的 IP 位置、作業系統、瀏覽型態、推薦連結的網址（address of referring site）、和活動相關紀錄（site activity information）等資料，但卻在使用者啟動應用程式後，自動蒐集並儲存使用者的通訊簿資訊，而有欺罔使用者的行為[163]。本案聯邦交易委員會所作成的和解協議內容和其公布的建議報告態度一致，均要求業者必須提供隱私權政策或通知，取得使用者同意，並要求業者應具體實踐其隱私權政策的內容。

---

158 *Id.* at 20-21.

159 *Id.* at 22-24.

160 *Id.* at 24-25.

161 聯邦交易委員會以 Moms With Apps 舉例，該應用程式提供隱私權標誌：其一，該應用程式是否會蒐集或分享資料；其二，應用程式是否包含廣告；其三，應用程式中是否會有任何購買行為；其四，應用程式是否會分享資料給社群網站；其五，應用程式是否會包含外部連結連至其他網站。*See*, *Id.* at 25-28.

162 *Id.* at 25-28.

163 U.S. v. Path, Inc., No. C 13 0448, slip op. at 9-15 (N.D. Cal). *See also* Press Release, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *available at* http://ftc.gov/opa/2013/02/path.shtm.

在 Goldenshore 和解案中，Erik M. Geidl 經營 Goldenshores Technologies 公司，開發一款名叫「Brightest Flashlight Free」的 Android 智慧型手機手電筒免費應用程式。Goldenshore 在隱私政策未揭露應用程式會將使用者精確的位置資訊和單一設備識別碼傳輸給第三方業者，包含廣告網絡。此外，該公司欺罔消費者，設置一個虛假的地理位址選項，讓使用者以為已經關閉傳輸地理位置的設定，然而該應用程式實際上會自動將地理資訊傳輸予第三方業者[164]。本案聯邦交易委員會要求業者必須修正隱私權政策，即時並完整地揭露所有蒐集的個人資料種類，並要求業者刪除先前以欺罔手法所蒐集的使用者個人資料[165]。

3.2.2. 州法層次——以加州為例

3.2.2.1. 一般個人資訊保護規定

加州於 2003 年訂定加州線上隱私保護法（The California Online Privacy Protection Act）。商業網站或線上服務業者凡透過網路對於住在加州的消費者，在瀏覽該商業網站或使用線上服務時，蒐集「可供識別的個人資訊（Personally Identifiable Information）」，應顯著地在網頁上張貼或提供隱私權政策[166]。隱私權政策須包含：標示業者所蒐集的個人資訊種類、提供並陳明消費者請求檢視或更改的管道，並且標註該隱私權政策的有效日期。隱私權政策如有任何更動應告知消費者[167]。所謂可供識別的個人資訊，包含姓名、地址（包括住家與其他實體地址，含街名、城市或鄉鎮名）、電子郵件地址、電話號碼、社會安全號碼，以及任何可供辨識，或可於線上或下線時連繫特定人之資訊[168]。

加州線上隱私法要求網站管理者或服務提供者，需主動張貼隱私權政策，並且置於網站首頁或最先出現的主要頁面（the first significant page），顯著地指引使用者知悉該隱私權政策的位置。隱私權政策必須：（1）釋明管理者或服務提供者蒐集有關使用者的個人可供辨識資訊類別，並釋明管理者或服務提供者可能會分享資訊之第三方清單；（2）描述使用者如何在網站上檢視或變更已蒐集之個人可供辨識資料；（3）描述管理者或服務提供者通知使用者隱私權政策實質改變的程序；以及（4）釋明隱私權政策的有效期日。若網站管理者或服務提供者之隱私權政策未符合上述要件，則牴觸加州線上隱私法[169]。

---

164 Press Release, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

165 In the Matter of Goldenshores Technologies, LLC, and Erik M. Geidl, No. 1323087 at 4-5, *available at* http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshoresorder.pdf.

166 Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22575 (a).

167 *Id.* § 22575 (b).

168 *Id.* Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22577 (a).

169 *Id.* § 22577 (b).

3.2.2.2. 對應用程式蒐集個人資訊的因應

為有效保護行動隱私權，加州檢察總長 Kamala D. Harris 和六大行動應用程式平台：亞馬遜、蘋果、Google、惠普、微軟和 RIM，達成協議以促進隱私保護、透明化和遵守線上隱私權法。協議內容主要規定，任何應用程式如有蒐集使用者的個人資訊，必須顯著地張貼隱私權政策或其他聲明，陳述如何蒐集、使用和分享個人資訊[170]。

在 2013 年 1 月，加州司法部公布由隱私執行保護單位（Privacy Enforcement and Protection Unit）[171]所提出的「Privacy on the Go 智慧型裝置隱私準則」[172]。此準則將行動應用程式業者區分為四大類：應用程式開發商、應用程式平台提供者（App Platform Providers）、廣告網絡（Advertising Network）、以及作業系統開發者（Operating System Developers）和行動通訊網路業者（Mobile Carriers）。

1. 應用程式開發商

首先應用開發業者在設計應用程式時，應一併考量隱私保護。第一步，建立一份個人資訊蒐集清單（data checklist），將應用程式可能蒐集、使用和揭露之可供識別的個人資訊列出。隨後，在設計應用程式時，考量這些個人資訊是否有蒐集的必要、對業者是否具有重要性，以及該應用程式將會如何處理這些個人資訊、會傳送給那些第三方業者、第三方業者會如何使用等。同時，基於資料蒐集限制原則，應避免或限制處理以下資料：和應用程式功能無關聯性的個人資訊、敏感性資料和 13 歲以下兒童的個人資訊。此外，在限制資料保存的考量下，在滿足應用程式功能後，不能長時間保存蒐集到的個人資訊。此準則希望藉由資料蒐集清單，在業者端建立一套隱私保護作法（privacy practice），除了確保使用者個人資訊的安全外，亦可符合聯邦及加州的隱私權規範[173]。

其次，此準則期待業者將隱私保護作法轉化為一般性隱私權政策，提供使用者完整、詳盡的描述，包含處理哪些個資、為何需要這些資料、如何處理、以及後續的傳送與分享情況。業者應將隱私權政策張貼在應用程式平台的頁面上，讓使用者容易點閱。同時，隱私權政策用語應清楚、簡白，隱私權政策的格式便於在智慧型裝置上閱讀，將最相關的隱私議題標明，或者透過圖示或標誌來陳述，讓使用者能一目了然[174]。

---

170 *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifiesmobile-app-developers-non-compliance (last visited Dec. 27, 2012).

171 加州司法部在 2012 年 7 月成立隱私執行保護單位（Privacy Enforcement and Protection Unit），負責具體落實聯邦和加州隱私權相關法案，並提供企業或私人相關隱私建議與指示。*See Privacy Enforcement and Protection*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, http://oag.ca.gov/privacy (last visited March 28, 2013).

172 CALIFORNIA DEPARTMENT OF JUSTICE, PRIVACY ON THE GO, *available at* http://oag.ca.gov/sites/all/files/pdfs/privac/privacy_on_the_go.pdf (last visited March 28, 2013).

173 *Id.* at 7-10.

174 *Id.* at 10-11.

再者，假如應用程式蒐集敏感性資料[175]、蒐集該可供識別的個人資訊與應用程式基本功能無關，或是當業者改變其隱私保護作法，加入新的、使用者無法預期的個人處理措施，或者將資料揭露予第三方業者（包含廣告業者）時，須以「特別通知（special notices）」，或者簡短的隱私聲明（short privacy statement）和隱私控制（privacy controls）告知[176]。

2. 應用程式平台提供者

首先，程式平台業者應給予使用者了解應用程式隱私保護作法的機會，因此應讓應用程式業者將其隱私權政策張貼在平台的頁面上。其次，平台業者也應提供應用程式使用者檢舉應用程式的管道，以便發現該應用程式有悖於隱私法規時，得以進行舉發。其三，平台業者應發揮教育應用程式業者和應用程式使用者的功能，一方面教育應用程式業者尊重使用者的隱私，另一方面也教育使用者應透過檢視隱私權政策與隱私選項，以保護自身隱私權益[177]。

3. 廣告網絡

廣告業者也須就所欲處理的個人資訊，提供隱私權政策，揭露予應用程式開發商，使其能間接轉知予使用者。同時，廣告的傳送不應超出應用程式的使用範圍，例如將廣告標示置於應用程式的桌面。最後應妥善保護個人資訊，維護其安全性[178]。

4. 作業系統開發者和行動通訊網路業者

對作業系統開發者而言，應建立全球隱私設定，允許使用者可控制個人資訊，以及行動設備可乘載應用程式。就行動通訊業者而言，則是藉由其與使用者之間持續的服務關係，教育使用者行動隱私，尤其是兒童行動隱私的觀念[179]。

3.2.3. 行動應用程式業者的回應

聯邦交易委員會 2013 年 2 月提出「行動隱私揭露——透過透明建立信任（Mobile Privacy Disclosures: Building Trust Through Transparency）」幕僚報告後，在美國聯邦商務部（Department of Commerce）「國家通訊與資訊局（National Telecommunication and Information Administration, NTIA）」協助下，由數十位科技遊說團體、應用程式開發業者聯盟與隱私權人士共同研討，並擬定出「促進行動應用程式實務透明化之簡短通知行為守則（Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices）（以下簡稱「行動 APP 守則」）」

175 敏感資料包含：文字訊息、通話紀錄或潛在隱私敏感設備紀錄，諸如相機、撥號機和麥克風。*Id.* at 12.
176 *Id.* at 12-13.
177 *Id.* at 14.
178 *Id.* at 15.
179 *Id.* at 16.

的草案[180]。由於本行為守則不具法律拘束力，行動應用程式開發商和其他相關業者，可自行決定是否遵循此守則，具有強烈的自我管制色彩。

值得注意的是，根據 2013 年 7 月 25 日最新版本的草案內容[181]，本守則所規定的簡短通知形式是以營養標示（nutrition label）作為藍本。具體而言，營養標示的通知是仿照食品的營養成分標籤，在使用者的介面上羅列基本的個人資料種類（例如電話、地理位置等），再特別標示出（highlight）業者所蒐集的個人資料種類及其內容、和哪些資料將分享給那些第三方業者（例如在有蒐集、使用和處理的個資種類旁打勾），讓使用者可以透過隱私通知的內容，決定是否同意蒐集或將資料分享給第三方業者[182]。本草案強調簡短通知不能取代隱私權政策，業者除了遵循行動 APP 守則外，也必須遵守隱私相關的法規規範。

本文以為，以營養標示作為簡短通知的藍本，雖為使用者所熟悉，且符合行動設備螢幕大小的呈現方式；然而若照目前本守則草案所提供的使用者介面範本，是否確實可讓使用者迅速理解其個人資料受到蒐集使用的狀況？如果能夠直接標示出將蒐集的個人資料，以成份標示（ingredient label）的方式標示，亦即直接列出業者實際上蒐集的個人資料項目，是否更可讓使用者一目瞭然，清楚迅速地掌握其個人資料可能受到侵犯的狀況？

營養標示和成分標示間簡短通知的形式區別在於，個人資料種類呈現的方式：前者是列出所有的個資種類，業者對其中幾項有蒐集的資料加以標示；後者則是業者僅列出其有蒐集的種類，未蒐集的個資則不列在簡短通知上。究竟簡短通知應採取營養標示或成分標示，或許需要進一步實證研究或是市場調查，來了解使用者的偏好。不過簡短通知如何能夠簡明而有效地提醒使用者注意其個人資料遭到業者利用的實際狀況，乃是當前行動隱私保護實務的關鍵所在。聯邦交易委員會對於此點若能進行全面性的仔細考量，研擬出具體有效的業者守則，對於使用者個資保護將可提供相當有價值的積極貢獻。

另外，由業者自行擬定行動 APP 守則，形成業者間的彼此約制效果，或許有助於隱私保護以及隱私設計模式的統一和形成。惟頗為奇怪之處在於，從草案以及相關文件觀察，無法得知究竟有哪些非政府組織及相關利益團體參與研擬。此外，除了簡短通知之外，行動 APP 守則草稿亦未建議業者必須提供隱私權政策，只言明假使業者有隱私權政策時，應指引使用者如何使用該隱私權政策。此

---

180 由於行動應用程式通知守則，尚在修改研擬中，且並非所有與會成員均簽屬此文件，因此仍為草案。Larry Magid, *Agreement Calls For Mobile App Privacy Disclosures (Updated)*, FORBES (July 25, 2013, 8:17PM), http://www.forbes.com/sites/larrymagid/2013/07/25/voluntary-industry-agreement-calls-for-mobile-app-privacy-disclosures-but-does-it-have-teeth/.

181 *Short Form Notice Code Of Conduct To Promote Transparency In Mobile App Practices*, NTIA (2013), http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf (last visited Nov. 29, 2013).

182 *NTIA Mobile App Transparency - UI Compositions*, NTIA, http://www.ntia.doc.gov/files/ntia/publications/ntia_ui_comps_update_7.23.pdf (last visited Aug. 28, 2013).

和聯邦交易委員會及加州司法部的建議報告並不相符。業者若遵循此守則，僅提供簡短通知，而漏未提供隱私權政策，仍有違反法律之虞（例如加州線上隱私權法），並不周延。

3.2.4. 小結

美國聯邦交易委員會和加州司法部，針對行動應用程式的隱私議題提出立場相近的研究報告。這兩份報告書也充分展現了美國對資訊隱私的態度與管制模式：市場取向[183]，講求資訊揭露和透明化。然而鑑於業者自律在隱私保護上的成效不彰，在講求隱私保護和科技發展兼籌並顧的同時，聯邦交易委員會和加州政府扮演監督業者的角色，並提出建議方案與行為準則，以強化行動應用程式使用者之個資保護。

在講求透明化的政策基調下，聯邦交易委員會建議、加州司法部要求業者提供即時、清楚的隱私權政策，然而在具體作法上有細微的不同。聯邦交易委員會希望可以設計出類似食品標示的隱私標誌，讓使用者得一目了然，知悉應用程式業者的隱私保護操作方式[184]；此外，更進一步希望由應用程式開發商或平台業者組成的公協會，可以提供隱私聲明的範本，以協助小型或個人應用程式開發商提供隱私權政策予使用者。在加州方面，則是在線上隱私法明定業者須提供隱私權政策，並且規定隱私權政策的要件與內容；此外，更建議業者依照加州線上隱私法的規範，形成最好的隱私保護作法（best practice），強調業者應從一開始設計應用程式時，就開始貫徹使用者的隱私保護（privacy by design）。然而，在加州司法部公布「Privacy on the Go 智慧型裝置隱私準則」後，諸多廣告聯盟即發函表示反對與抗議，認為該建議報告超出加州線上隱私法的條文規範與要求範圍，尤其是要求業者提供特別通知的建議，將使業者在研發、設計應用程式時綁手綁腳，增加業者的負擔與成本[185]。

本文發現在適用法上，加州線上隱私權保護法會出現法律適用和聯邦法先佔原則（preemption）的問題。首先關於法律適用的部分，加州線上隱私權保護法的規範主體為網站和線上服務提供者，行動應用程式是否可和一般的網站或線上服務畫上等號，不無疑問。此外，退步言之，縱使行動應用程式可適用線上隱私權保護法，然而若行動應用程式開發商非加州的公司，即便構成隱私侵害，是否可以加州線上隱私權法作為準據法，亦有疑問。其次關於聯邦法先佔原則的問題，可從 2012 年 12 月加州司法部依據加州線上隱私法向達美航空提起之訴訟加以

---

183 *See supra* note 132.

184 Steve Satterfield, *California AG Puts Mobile App Developers on Notice*, INSIDE PRIVACY (Nov. 1, 2012), http://www.insideprivacy.com/united-states/california-ag-puts-mobile-app-developers-on-notice/. *See* also Josephine Liu, *FTC Working on Privacy "Nutrition Label"; Industry Focusing on Icons*, INSIDE PRIVACY (Oct. 25, 2012), http://www.insideprivacy.com/united-states/federal-trade-commission/ftc-working-on-privacy-nutrition-label-industry-focusing-on-icons/ (last visited Nov. 29, 2013).

185 *See Re: Privacy on the Go – Recommendations for the Mobile Ecosystem*, http://gaia.adage.com/images/bin/pdf/TradeGroupLettertoCA1.10.13.pdf (last visited April 20, 2013).

觀察。加州司法部主張達美航空未提供行動應用程式的隱私權政策，且達美航空的網站隱私權政策未提及其所提供之應用程式，亦未說明該應用程式會蒐集使用者的個人資料[186]。加州地方法院認為本案應優先適用美國民航解除管制法案（Airline Deregulation Act of 1978），因此不適用加州線上隱私權保護法，而駁回起訴[187]。

同時，在使用者部分也有保護不足的疑慮。首先，聯邦交易委員會或加州司法部均要求業者提供隱私權政策，加州線上隱私法甚至明訂隱私權政策的要件和內容，然而兩者並未設定隱私權政策之最低揭露標準。因此隱私權政策雖然可能符合加州線上隱私法的規定，卻可能仍然無法保證確能有效保護使用者的隱私[188]。其次，若業者提供隱私權政策後，隱私保護的責任和風險承擔由誰負責？在 2012 年 12 月 18 日，聯邦通訊委員會（Federal Communications Commission）公布一份根據不同的作業系統所設計的智慧型手機安全檢查表（FCC Smartphone Security Checker），提供使用者自我保護隱私的機制。其中值得注意的是，聯邦通訊委員會在第五點要求使用者在下載應用程式前，應弄懂權限的內容，了解應用程式業者如何蒐集和處理個人資訊。此舉形同要求使用者於同意權限清單之後，必須自行承擔隱私受到侵害的風險，然而隱私聲明中的科技術語，並非使用者可得輕易理解[189]。因此有關隱私權政策的各項要求，似乎並未能根本改善使用者的隱私保護現況，這也是通知和同意機制所面臨的根本問題與困境。

3.3. 國際層次的因應

國際層次已察覺行動應用程式下載所引發的隱私問題，2013 年 8 月 OECD 的分支機構全球隱私執行機關網絡（Global Privacy Enforcement Network，以下簡稱 GPEN）發起第一波「網路隱私搜查（Internet Privacy Sweep）」，以隱私政策透明度為主題，檢視網站和行動應用程式的隱私政策揭露情況。此外，在 2013 年 9 月第三十五屆「國際資料保護與隱私權委員大會（The International Data Protection and Privacy Commissioners Conference）」公布「華沙宣言 ——應用程式生活化（Warsaw declaration on the "appification" of society），以下簡稱華沙宣言」，對行動應用程式的隱私議題做出回應。

---

186 Complaint, People v. Delta Airlines, Inc., No. CGC-12-526741 (Super. Ct. Cal. Dec. 6, 2012), *available at* http://www.lw.com/admin/Upload/Documents/Complaint.pdf (last visited Nov. 29, 2013).

187 *See* Tyler G. Newby & David Marty, *Privacy Litigation Alert: California Court Dismisses Attorney General's Mobile App Privacy Suit Against Delta, Offers Little Guidance*, FENWICK & WEST LLP, http://www.fenwick.com/publications/Pages/Privacy-Litigation-Alert-California-Court-Dismisses-Attorney-Generals-Mobile-App-Privacy-Suit-Against-Delta.aspx (last visited Aug. 29, 2013).

188 *See* Chris Jay Hoofnagle & Jennifer King, *Research Report: What Californians Understand About Privacy Offline* 3 (working paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075 (last visited Nov. 29, 2013).

189 H. Nissenbaum, *A Contextual Approach to Privacy Online*, DAEDALUS (Fall. 2011), at 36, *available at* http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf.

3.3.1 GPEN 的「網路隱私搜查」

3.3.1.1. GPEN 的「網路隱私搜查」簡介

鑑於三十年來隱私權保護型態的轉變，OECD 於 2007 年提出「跨境合作執行隱私保護法建議書」（Recommendation of the Council on Cross-border Co-operation in Enforcement of Laws Protecting Privacy），建議會員國之隱私執行機關互相交換經驗和合作，並於 2010 年 3 月成立「全球隱私執行機關網絡（the Global Privacy Enforcement Network, GPEN），以下簡稱 GPEN」，目前共有 32 個國家或地區的隱私執行機關參與，藉由資訊交換平台，以落實雙邊、多邊合作[190]。

GPEN 進行第一波「網路隱私搜查」，以「隱私操作透明度（Privacy Practice Transparency）」為主題，在 2013 年 5 月 6 日至 5 月 12 日期間，評估網站或行動應用程式是否適當公開隱私操作政策，讓使用者知悉業者如何利用、處理和傳輸其個人資料。針對「網路隱私搜查」，GPEN 聲明此行動並非深入地分析各網站或各個行動應用程式的隱私權政策內容，亦非調查網站或行動應用程式業者是否有隱私侵害事由。本行動的調查方式是以使用者的角度出發，模擬使用者在瀏覽網站或下載行動應用程式時，探究使用者是否可能接近、了解業者的隱私權政策之情況[191]。

---

190 *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, http://www.oecd.org/internet/ieconomy/38770483.pdf (last visited Nov. 29, 2013); *About the Network*, GLOBAL PRIVACY ENFORCEMENT NETWORK, https://www.privacyenforcement.net/ (last visited Nov. 20, 2013).

191 *See Global Privacy Enforcement Network Internet Privacy Sweep Questions and Answers*, THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, http://www.priv.gc.ca/media/nr-c/2013/nr-c_130506_qa_e.asp (last visited Nov. 20, 2013); *Results of the 2013 Global Privacy Enforcement Network Internet Privacy Sweep*, THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, http://www.priv.gc.ca/media/nr-c/2013/bg_130813_e.asp (last visited Nov. 20, 2013); *Results of the first GPEN Internet Privacy Sweep, COMMISSION FOR THE PROTECTION OF PRIVACY*, http://www.privacycommission.be/en/internet-privacy-sweep-2013 (last visited Nov. 20, 2013); *Privacy Commissioner: Website privacy policies are too long and complex*, THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex (last visited Nov. 20, 2013); *Global Privacy Enforcement Network Internet 'Privacy Sweep'*, OFFICE OF THE DATA PROTECTION COMMISSIONER, http://www.dataprotection.ie/documents/GPEN2013.pdf (last visited Nov. 20, 2013). 同時參考澳門個人資料保護辦公室，“互聯網私隱風險搜尋”報告，http://www.gpdp.gov.mo/cht/forms/sweepreport_ch.pdf（最後瀏覽日期：2013 年 11 月 20 日）；個人資料私隱專員公署，「全球私隱執法機關網絡」聯合公佈各地網上私隱政策透明度檢視結果，http://www.pcpd.org.hk/tc_chi/infocentre/press_20130814.htm（最後瀏覽日期：2013 年 11 月 20 日）。

「網路隱私搜查」行動共有 10 個國家、19 個隱私執行機關[192]參與該行動，在各自的管轄區域範圍內，共抽查 2276 個網站及行動應用程式。透過五大指標加以檢驗目前網站和應用程式張貼隱私權政策[193]的情況和效果，包含：(1) 是否具有隱私權政策；(2) 如果有隱私權政策，則該隱私權政策是否容易查閱；(3) 業者是否有提供聯繫方式；(4) 隱私權政策是否容易閱讀；(5) 隱私權政策的內容是否與網站或行動應用程式有關聯等[194]。針對調查結果，有一些值得注意的事項，首先 GPEN 針對網路隱私搜查行動僅提供大略的調查方針，並未具體要求搜查的細節，因此各國調查的風險評估標準不盡相同。例如各國對有隱私疑慮的行動應用程式或網站的比例不同，有隱私疑慮的網站比例從 25%到 90%都有。其次，雖 GPEN 希望各國的隱私執行機關針對其管轄範圍內的網站或行動應用程式進行調查，然各國的調查範圍不免重疊，因此某些網站或行動應用程式可能有重複評價的情況發生[195]。

3.3.1.2. 「網路隱私搜查」的全球調查結果

GPEN 的「網路隱私搜查」的全球調查結果，可分成二個部分：第一部分為調查結果的量化分析；第二部分則為隱私執行機關在進行「網路隱私搜查」時，所發現可供網路業者作為範本之「最好的隱私保護作法（Best practices）」[196]。

---

192 10 個國家、19 個隱私執行機關，包含：澳洲的澳洲資訊委員辦公室，Office of the Australian Information Commissioner）、加拿大的加拿大隱私委員辦公室（Office of the Privacy Commissioner of Canada）和英屬哥倫比亞資訊和隱私委員（Information and Privacy Commissioner of British Columbia）、愛沙尼亞的個人資料保護檢察署（Estonian Data Protection Inspectorate）、芬蘭的個人資料保護行政監察官署（Office of the Data Protection Ombudsman）、法國的國家資訊技術與自由委員會（Commission Nationale de l'Informatique et des Libertés）、德國的聯邦個人資料保護委員會（Federal Data Protection Commissio）、柏林個人資料保護委員會、(Data Protection Commissioner of Berlin）、萊茵蘭-普法爾茨個人資料保護委員會（Data Protection Commissioner of Rhineland-Palatinate (Rheinland-Pfalz)）、巴伐利亞個人資料監督機關（Data Protection Supervisory Authority of Bavaria）、黑森個人資料保護委員會（Data Protection Commissioner of Hesse）和布蘭登堡個人資料保護委員會、香港的個人資料私隱專員公署（Office of the Privacy Commissioner for Personal Data）、愛爾蘭的個人資料保護委員辦公室（Office of the Data Protection Commissioner）、澳門的個人資料保護辦公室（Office for Personal Data Protection, Government of Macao）、紐西蘭的隱私委員辦公室（Office of the Privacy Commissioner）、挪威的個人資料保護機構（Data Protection Authority）、英國的資訊委員辦公室（Information Commissioner's Office）、以及美國的聯邦交易委員會（Federal Trade Commission）。 *See Global Privacy Enforcement Network Internet Privacy Sweep Questions and Answers*, THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, http://www.priv.gc.ca/media/nr-c/2013/nr-c_130506_qa_e.asp (last visited Nov. 20, 2013).

193 GPEN 這裡所稱之隱私權政策，即本文所指之隱私聲明，惟為忠於 GPEN「網路隱私搜查」之用語，於此部分均使用「隱私權政策」之用語，併與敘明。

194 *See Global Privacy Enforcement Network Internet 'Privacy Sweep'*, OFFICE OF THE DATA PROTECTION COMMISSIONER, http://www.dataprotection.ie/documents/GPEN2013.pdf (last visited Nov. 20, 2013)。另參考香港個人資料私隱專員公署，「全球私隱執法機關網絡」聯合公佈各地網上私隱政策透明度檢視結果，http://www.pcpd.org.hk/tc_chi/infocentre/press_20130814.htm（最後瀏覽日期：2013 年 11 月 20 日）。

195 *Privacy Commissioner: Website privacy policies are too long and complex*, THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex (last visited Nov. 20, 2013).

196 主要參考加拿大隱私委員辦公室所公布之「網路隱私搜索」全球報告。 *See supra* note 192.

第一部分：調查結果的量化分析

1. 現在仍有相當比例的網路和行動應用程式業者（以下簡稱網路業者）未提供隱私權政策

網站和行動應用程式未提供隱私權政策聲明的比例佔 21%。從 77%提供隱私權政策的業者可發現，相較於中小型企業，大型的網路業者大部分都會提供隱私權政策。

2. 高達 1/3 隱私權政策的內容未提供相關資訊

1/3 的抽查個案未適當地提供相關資訊，許多都未「量身訂做」地編寫符合業者隱私操作的隱私權政策，僅提供有限的資訊告知使用者業者如何蒐集、利用和揭露使用者的個人資料。甚至部分個案中，隱私權政策的內容過分概括，並未交代業者如何蒐集和利用使用者的個人資料。

3. 大約 1/3 的隱私權政策的閱讀性堪慮

大約 33%的隱私權政策難以閱讀，大部分只抄襲相關的法律用語。對一般使用者而言，業者未能清楚且簡明的說明其隱私操作的內容，讓使用者難以清楚地理解個人資料是如何蒐集及利用。

4. 行動應用程式隱私權政策的情況較傳統網站落後

調查結果顯示高達 92%的行動應用程式在隱私權政策的呈現方式上，出現多種疑慮。54%抽樣行動應用程式未提供隱私權政策，而有提供隱私權政策者，有部分個案僅提供超連結，供使用者點選後得以在業者的網站上瀏覽隱私權政策。更甚者，隱私權政策並未交代行動應用程式開發業者，如何透過行動應用成蒐集、利用使用者的個人資料。

第二部分：「最好的隱私保護做法（Best practices）」之範本

1. 易於查閱、簡單好讀而且含有隱私相關的資訊內容，使使用者有興趣去了解、閱讀，註明使用者的權責，清楚交代如何蒐集資料、業者的使用目的，以及資料是否會與第三方業者分享共用。如此作法，可確實達到隱私權政策的透明功能。

2. 部分的隱私權政策會以好懂、容易理解的方式，使一般的使用者可理解隱私權政策的內容，例如：用語淺白、簡明易懂的解釋、善用標題、簡短的段落、常見問與答、以及以表列的方式表達隱私操作之內容和重點。

3. 將近八成的網路業者在隱私權政策中，列明聯絡人資料，讓使用者可向其查詢隱私相關的事宜。此外，更會提供不同的聯絡方式，例如：地址、電話、及／或電子郵件，確保使用者和網路業者間的溝通沒有障礙。

4. 部分的網路業者，針對行動應用程式和行動網站，特意編寫相應的隱私權政政策，具體說明業者的隱私操作，而非只是單純提供超連結連接到現有的網站隱私權政策。此外，為了配合行動裝置的小尺寸螢幕，GPEN 鼓勵業者研發可妥善傳達隱私權政策的方法，方便行動裝置使用者閱讀。

3.3.1.3. 小結

GPEN 發起「網路隱私搜查」行動，其目的是為了試水溫（temperature gauge），藉由廣泛的搜查以初步了解未提供隱私權政策的網站和行動應用程式比例仍偏高，且大部分有提供隱私權政策者，隱私權政策都有不易接近、不易閱讀和未能清楚揭露業者隱私操作的情況。

GPEN 的宗旨是藉由網站和行動應用程式隱私權政策的抽查結果，促使公眾和業界加強對隱私權保護和責任的意識，並遵守隱私保護相關法律的規範。此外，更希冀藉有本次行動，提升各國隱私執行機關的合作，共同確定推廣教育和執法行動的方向。經過本次調查，多個隱私執行機關（例如香港[197]、澳門[198]和澳洲[199]）開始針對其管轄範圍內，持續關注網站和行動應用程式業者提供隱私權政策的情況，並提出相對應的政策以解決網路隱私、行動隱私的問題。甚至於香港個人資料私隱專員公署，在 2013 年公布手機程式「起你底」的調查報告，認為該行動應用程式讓使用者得以搜尋個人的訴訟案件及破產資料，已嚴重侵犯資料當事人的隱私。因此，香港個人資料私隱專員公署發出執行通知，要求資料庫營運者 Glorious Destiny Investment Limited（GDI）停止向應用程式提供系爭資料，GDI 已於 2013 年 8 月 7 日起遵從指令[200]。

3.3.2 第三十五屆國際資料保護與隱私權委員大會之「華沙宣言」

國際資料保護與隱私權委員大會係成立於 1979 年，並於同年召開第一次會議，僅限設有獨立專責之隱私監督機關得參加會議，並邀請隱私專家或隱私相關的非政府間國際組織參與討論。會議中，各國的隱私專責機關探討個人資料保護的措施，以及針對新型態的隱私侵害議題進行討論[201]。

在 2013 年 9 月 24 日，第三十五屆國際資料保護與隱私權委員大會通過「華沙宣言」，針對應用程式生活化所招致的隱私侵害風險，加以回應。宣言中要求

197 香港個人資料私隱專員公署，「全球私隱執法機關網絡」聯合公佈各地網上私隱政策透明度檢視結果，http://www.pcpd.org.hk/tc_chi/infocentre/press_20130814.htm（最後瀏覽日期：2013 年 11 月 20 日）。

198 澳門個人資料保護辦公室，“互聯網私隱風險搜尋”報告，http://www.gpdp.gov.mo/cht/forms/sweepreport_ch.pdf（最後瀏覽日期：2013 年 11 月 20 日）。

199 *Supra* note 195.

200 香港個人資料私隱專員公署，調查報告：手機程式「起你底」嚴重侵犯個人資料私隱，（最後瀏覽日期：2013 年 11 月 20 日）。

201 *About the Conference*, THE INTERNATIONAL DATA PROTECTION AND PRIVACY COMMISSIONERS CONFERENCE, https://privacyconference2013.org/About_the_Conference_ (last visited Nov. 20, 2013).

行動應用程式開發業者，應遵守現行的個人資料保護原則，本文將宣言的要求整理成以下三點：

1. 從設計著手保護隱私：

行動應用程式開發商於開發應用程式時，即應將隱私保護納入應用程式設計中。一方面可保障使用者的隱私權；另一方面，使用者因為隱私權受到保障，因而提升對業者的信任度，使業者可享有競爭優勢。

2. 揭露隱私操作，並取得使用者同意

行動應用程式開發商應對使用者揭露其隱私操作內容，例如告知其蒐集使用者何種個人資料，並取得使用者的同意。本原則亦適用於第三方業者，如廣告網絡（ad networks），假使行動應用程式開發商有透過第三方業者的設備蒐集個人資料，亦應告知使用者，取得使用者同意。

3. 蒐集之目的限制原則

行動應用程式開發商應清楚了解，為了何種目的蒐集和利用使用者的個人資料，並且不可蒐集超出目的範圍的個人資料。

除此之外，宣言中亦要求作業系統業者和行動應用程式平台業者，應肩負起保護使用者隱私權的責任。由於行動應用程式平台業者提供並維護行動應用程式市場的框架，因此平台業者負有特別的責任以保護使用者的隱私。另外，國際資料保護與隱私權委員大會也鼓勵業界推動隱私權標章（privacy seal）或其他認證制度，做為業者自行監督、自律的方法。

總言之，國際資料保護與隱私權委員大會所公布的華沙宣言，其實就是彙整歐盟和美國所提出的意見報告之內容，偏向透過業者的自律和加強透明度，增加使用者對自身個人資料的控制權力。

3.3.3小結

GPEN 的「網路隱私搜查」的結果，主要是發現問題，並且僅於報告中，透過整理最佳隱私操作作為範例，建議隱私執行機關和相關業者遵循。同樣的，國際資料保護與隱私權委員大會所公布的華沙宣言，也僅以最寬泛、籠統的方式，建議行動應用程式產業業者應遵循全球共通的隱私保護原則。總言之，二者僅能做到拋磚引玉，喚起各界對行動應用程式隱私議題的注意，並未提供實質、具體且明確的幫助。因此，在國際層次上，尚無統一的行動應用程式隱私保護標準，提供世界各地行動應用程式業者遵循和參考。

3.4. 主導法規（Lead Regulator）與國際合作

從上述分析可以看出，歐陸法和美國法雖皆著重於增進隱私保護的透明程度，然而歐盟著重於應用程式開發商的管制，美國則著重於應用程式平台業者的把關功能。此外，保護取向亦不同，歐盟偏重使用者的保護，藉由法律規範和行政審查，確保業者蒐集、利用使用者的個人資料未超出目的範圍內，偏向政府管制途徑；相對地，美國偏向業者的彈性和發展，認為蒐集個人資料是可接受且具有潛在利益的，因此只要透過行政監督確保業者的行為未與使用者的基本權牴觸即可，偏向市場機制途徑[202]。由於隱私權與個人資料保護，具有濃厚的文化與民族性色彩，因此各國立法規範情況不一。然因網路無國界的特性，各國內國法事實上均具有域外效力，業者同時面對多個具有實質差異的國內法規範，不僅無所適從，而且受有各國隱私主管機關交互審查之不必要煩擾[203]。Google 全球隱私顧問 Peter Fleischer 遂提倡「主導法規（lead regulator）」，主張應建立全球化的隱私保護標準，以降低業者的遵循成本[204]。目前具有主導法規之姿者，應為 OECD 隱私準則莫屬。尤其在 2013 年 7 月 11 日，OECD 通過「隱私保護與個人資料跨境流動準則建議（Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data，簡稱 OECD 隱私準則修正）」，修正 1980 年所公布的八大隱私原則，以因應現今多重行為者藉由創新的科技技術，得以大量蒐集、利用和儲存個人資料，所造成的隱私風險和威脅[205]。

在本次修正中，OECD 引進三個新的概念：（1）國家隱私策略（national privacy strategies），指引會員國如何在國內實踐 OECD 隱私準則的八大原則；（2）隱私管理程序（privacy management programmes），認為資料控制者均應實行隱私管理程序，包含資料風險評估、內部監控、以及在有重大資安漏洞侵害個人資料時，應通知隱私主管機關或相關單位；（3）資料安全漏洞通知（data security breach notification），資料控制者應在發生資訊安全闕漏時，通知隱私主管機關和當事人[206]。可發現，強化課責原則是本次 OCED 的修正重點。

然而 OECD 隱私準則強調其僅為最低隱私標準，各會員國可以依國情和隱私保護需求，調整法律規範的內容和方向[207]。此外，由於 OECD 具有軟法之特性，在國際法上並不具有法律拘束力，究其實僅具有建議與自願遵循之效果。縱

---

202 DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 14-15 (2005).

203 *See* DANIEL J. SOLOVE, *supra* note 71, at 998-1003 (2012).

204 *See* Peter Fleischer, *It's time for a "lead regulator" in Europe*, PETER FLEISCHER: PRIVACY...? (Aug. 16, 2012, 9:02 AM), http://peterfleischer.blogspot.tw/2012/08/its-time-for-lead-regulator-in-europe.
html *(last visited Nov. 29, 2013)*.

205 *The OECD Privacy Framework*, OECD, at 3, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited Nov. 8, 2013).

206 *Id.* at 16-17, 23-35.

207 *See id.* at 55.

使會員國未能依照該準則之指引修改內國法，亦無違反國際法義務或遭到制裁之虞。

國際間近來一直有調和不同隱私規範的聲浪，例如國際資料保護與隱私權委員大會自 2005 年起，持續提出草案或共同提議（joint proposal）促成國際隱私規範的和諧[208]。筆者認為，國際間若能制定具有法律拘束力之國際條約，推動各國隱私與個資法律保護和諧化（harmonization），使締約國必須遵照該條約之規定訂定或修正內國法，降低國與國之間在個人資料保護規範上的歧異性，不僅可促進資料的國際流動，亦可有助於科技的革新，應屬行動隱私保護領域值得大力推動的努力目標。正如同歐盟各國雖然各自訂立符合國情需求的隱私權保護法規，然其法條精神與規範方向仍然遵守歐盟的個人資料保護指令。因此若能在 OECD 原有架構之下，或是在其他相關國際組織的支持下，締結具有拘束力的個人資料保護國際條約，應可大幅緩解目前各國立法分歧的困窘現況[209]。惟須注意，雖然建立一套國際的隱私保護規制，是隱私保護發展的終極目標。然而由於隱私議題有別於貿易或公共衛生等議題，各國可為了共通的目的或可共享的利益達成共識；相反的，隱私議題雖為人類的基本權，然而因國情、隱私管制途徑以及對個人資料蒐集、利用的態度相異，國與國間對各自隱私規範的誤解或歧見，將成為通往隱私和個資保護調和的絆腳石[210]。

208 *See id.* at 111-12.

209 參見翁清坤，前揭註 143，頁 46-54（2010）。

210 *See* Christopher Kuner, *"You Just Don't Understand": The Current EU–U.S. Privacy Battles*, PRIVACY PERSPECTIVE (Feb. 28, 2013), https://www.privacyassociation.org/privacy_perspectives/contributors/kuner_christopher (last visited Nov. 29, 2013); Christopher Kuner, *The Transatlantic Divide Over Data Privacy Rights,* PRIVACY PERSPECTIVE (May 20, 2013), https://www.privacyassociation.org/privacy_perspectives/post/the_transatlantic_divide_over_data_privacy_rights (last visited Nov. 29, 2013).

四、 量化研究：我國民眾使用行動應用程式的隱私意識調查

綜觀前述比較法分析結果，可以發現無論是以完整保護公民隱私為宗旨的歐盟，或者採取市場機制和業者自律的美國，亦或是國際政府組織，均共通認為：改善「通知和同意」機制是目前舒緩隱私和科技間緊張關係的手段。歐盟、美國和國際組織公布的報告或數據，也以調整通知的內容和呈現方法作為核心措施。此異曲同工的結果，其實不難想像，也十分合理。蓋公開透明原則是否具體落實，關乎使用者是否能在資訊適當揭露後，理性決定是否願意提供個人資料予業者。亦即業者是否履行通知義務，會影響到使用者能否有效決定個人資料揭露的內容和使用流向，進而做出是否同意業者可蒐集、使用、和傳送與第三方業者。

我國個資法就非公務機關之「告知與同意」機制，分別規定於第 7 條（書面同意之內涵）、第 8 條（直接蒐集個人資料之告知義務）、第 19 條（非公務機關蒐集或處理個人資料之要件）和第 20 條（非公務機關利用個人資料之除外情形）之中。行動應用程式產業在蒐集、處理或利用當事人的個人資料前，應先陳明（1）業者的名稱；（2）蒐集的目的；（3）個人資料的類別；（4）個人資料利用的期間、地區、對象及方式；以及（5）當事人依個資法得行使的①查詢或閱覽權；②請求製給複本權；③補正或更正權；④停止蒐集、處理或利用權；以及⑤刪除權依第三條規定得行使之權利及方式。惟就告知的形式和呈現的方法，我國中央目的事業主管機關並未以意見報告提出明確的建議（如同歐盟第 29 條工作小組的意見書），也並未以法律或者法律授權的法規命令做出確切的規定和要求。因此，本文希望透過問卷研究，談討我國國人對現今常用的隱私聲明之看法與了解程度。

甚者，參考 Jennifer M. Urban、Chris Jay Hoofnagle 和 Su Li 三位學者在 2012 年 7 月共同發表「Mobile Phones and Privacy」，針對美國的行動通訊裝置和行動應用程式使用者，進行隱私風險意識的調查[211]。此外，Pew Research Center's Internet & American Life Project 機構所製作的 Privacy and Data Management on Mobile Devices 報告[212]，報告中針對美國行動裝置使用者的資訊隱私和資訊安全意識進行調查。在這兩份報告的啟發下，筆者認為要對我國行動應用程式使用者的隱私和個人資料提出保護規範，應從了解我國使用者對行動應用程式的使用習慣和隱私意識開始。因此，量化研究以「通知和同意」機制為主題，調查我國行動應用程式使用者的個人資料意識，以及現行隱私聲明的效度。

---

211 *Supra* note 91, at 6-24.

212 Jan Lauren Boyles, Aaron Smith & Mary Madden, *Privacy and Data Management on Mobile Devices*, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES, 6-8 (2012), http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

在「通知和同意」機制下，行動應用程式業者通常以隱私權政策或揭示應用程式權限（Permission，應用程式權限，以下以「權限清單」稱之）作為隱私聲明的體現。因此，本文想要從行動應用程式使用者對「隱私權政策」和「權限清單」的閱讀情況和了解程度，來探知隱私聲明是否發揮應有的功用。其次，本文亦欲探討我國行動應用程式使用者在行動應用程式蒐集其個資的事情上的態度或隱私意識為何。因此，基於以上疑問，本文在量化研究上，採取問卷調查法，蒐集行動應用程式使用者，就其藉由行動通訊裝置使用行動應用程式的經驗，探討下列問題：(一)使用者閱讀隱私聲明的情況；(二)使用者對隱私聲明的了解程度；(三)隱私聲明的效能；以及(四)使用者對行動應用程式蒐集其個人資料的介意程度。筆者將分別針對此四大問題，設計問卷內容，並分析統計結果，進行更進一步的討論。

4.1. 研究方法

量化研究採取問卷調查方法，採樣範圍母群體為行動應用程式使用者，就「使用頻率最高」的智慧型裝置為作答對象。為保護作答者的隱私，並希望藉由匿名的問卷方式，讓使用者可以安心地依照其使用習慣和隱私態度作答，故採取不記名的問卷設計。

根據資策會提供的 2012 年第一季手機門號調查中[213]，2012 年第一季的行動上網數據用戶為 1,993 萬戶 ，若針對行動上網用戶進行抽樣，根據統計學的抽樣誤差公式[214]，在 95%信心水準和抽樣誤差在正負 5 個百分點以內時，必須抽取 384 位使用者為樣本[215]。

本份問卷係於 2013 年 2 月 5 日至 2013 年 3 月 15 日，分別透過紙本和網路蒐集樣本，徵求智慧型設備使用者填寫問券。網路問卷發放於（1）筆者和友人的 Facebook 臉書塗鴉牆；（2）BBS 批踢踢實業坊的「Q_ary」板（問卷板）、「Master_D」(碩士板)、「Android」板和「StupidClown」（笨板）上；(3）透過政大外交系和前鼎光電公司、傳承光電公司、歐英克科技公司、和歐霖光通公司的內部電子郵件公告，共計回收 213 份問卷。本問卷網路問卷使用 Google 提供的問卷系統設計。紙本問卷發放於（1）蘆竹鄉立幼兒園、(2）桃園縣縣立內壢國中、(3）台北市立松山高中、(4）國立交通大學科技法律研究所、和（5）親朋

---

213 2012 年第一季手機門號調查，經濟部工業局寬頻網通產業整合推動計畫，http://www.communications.org.tw/communications/page.php?pg=detail&unit=4306&cone=2&ctwo=22（最後瀏覽日期：2013 年 10 月 9 日）。

214 $$N_s = \frac{(N_p)(p)(1-p)}{(N_p-1)(B/C)^2 + (p)(1-p)}$$ （Ns = 須完成的樣本數；Np = 母群體規模；(p)(1-p)：母群體異質性程度；B：可容忍的抽樣誤差；C：可接受的信賴區間 95%，所對應的 Z 分數，亦即 1.96），羅清俊，社會科學研究方法：打開天窗說量化，頁 82-83（2010）。

215 *Sample Size Calculator*, CREATIVE RESEARCH SYSTEMS, http://www.surveysystem.com/sscalc.htm (last visited Oct. 9, 2013).

好友，共計回收 240 份問卷。因此，網路問卷和紙本問卷加總後，共回收 453 份問卷。然而，453 份問卷須扣除 13 份無法使用的問卷，包含：8 份空白問卷、以及 5 份問卷未填選使用何種行動應用程式平台，且最近三個月內未使用和下載任何行動用程式。因此，有效問卷總計 430 份，本文將以此作為研究基礎。

表四為使用者的組成以及性質，女性使用者共計 250 人，占 58%；男性使用者共計 180 人，占 42%。使用者年齡集中在 13 歲到 34 歲之間，共 293 人；使用者的就業情況，學生占 212 人，就業人士占 202 人。此外，使用者教育程度部分，使用者普遍擁有大學、大專院校以上的學歷，教育程度為大學、大專院校者共 187 人，碩士者為 116 人。

表四：我國行動應用程式使用者樣本組成及性質（樣本數：430 份）

	%
性別	
男	42
女	58
年齡	
未滿 13 歲	1
13-17 歲	23
18-24 歲	26
25-34 歲	28
35-44 歲	14
45-54 歲	6
55 歲以上	2
教育程度	
國中以下	13
高中、職	13
大學、大專院校	44
碩士	27
博士	3
就業狀態	
學生	49
就業中（正職／兼職）	47
待業中／家管	3
已退休	0 （1 人）
主修／專長	
其他科系	48
無	26
法律相關科系	16
資訊相關科系	10

月收入	
不知道／不方便作答	20
未滿新台幣一萬元	31
新台幣一萬元以上，未滿新台幣二萬元	7
新台幣二萬元以上，未滿新台幣三萬元	7
新台幣三萬元以上，未滿新台幣四萬元	7
新台幣四萬元以上，未滿新台幣五萬元	5
新台幣五萬元以上，未滿新台幣六萬元	5
新台幣六萬元以上，未滿新台幣七萬元	6
新台幣七萬元以上，未滿新台幣八萬元	6
新台幣八萬元以上，未滿新台幣九萬元	2
新台幣九萬元以上，未滿新台幣十萬元	0 （2 人）
新台幣十萬元以上	4

4.2. 問卷設計

依據研究目的，將問卷分成四大部分：（一）使用者的基本資料調查；（二）行動通訊裝置的行動應用程式背景資料；（三）應用程式的隱私聲明；以及（四）使用者對行動應用程式蒐集個人資料的態度。題目設計上依題目適性，兼採敘述性與解釋性調查[216]。針對使用者的個人背景以及使用行動應用程式的情況，採取敘述行調查；針對行動應用程式中隱私聲明的閱讀情況和理解程度，為獲得較多的資訊，因此透過一系列的問題調查使用者的態度和看法。因此，依照題目的需要，採取半開放式的問卷設計，除提供固定的選項外，使用者也可勾選「其他」，填答個人的意見或看法。

此外，考量行動應用程式平台所提供的隱私聲明不同，只有 Google Android Market／Google Play 和 Windows Store 在使用者下載行動應用程式前，會先揭示該應用程式所需要的權限，並在使用者同意後，才得以下載；而 Apple App Store 或 Nokia Ovi Store 的隱私通知政策上，並未在使用者下載前揭示權限清單。因此在詢問使用者對權限清單的看法時，問卷採取漏斗式的設計[217]，僅詢問 Google Android Market／Google Play 和 Windows Store 的使用者關於權限清單的問題。再者，針對「使用者在安裝行動應用程式前，是否會閱讀隱私權政策或權限清單」、「對隱私權政策或權限清單內容了解程度」以及「是否介意行動應用程式蒐集使用者個人資料」等問題，亦採取漏斗式的設計，針對其填答的內容，分別設計相對應的子問題，以探求使用者填選的原因。

216 羅清俊，前揭註 214，頁 65-66（2010）。

217 關於問卷設計和編寫，主要參考以下書籍：羅清俊，社會科學研究方法：打開天窗說量化，頁 64-106（2010）；內田治、醍醐朝美，徐華錂譯，問卷調查應用入門，（2000）；吳明隆，論文寫作與量化研究（2011）；Robert A. Peterson，王國川譯，如何編制優質的問卷（2010）。

4.3. 問卷結果分析

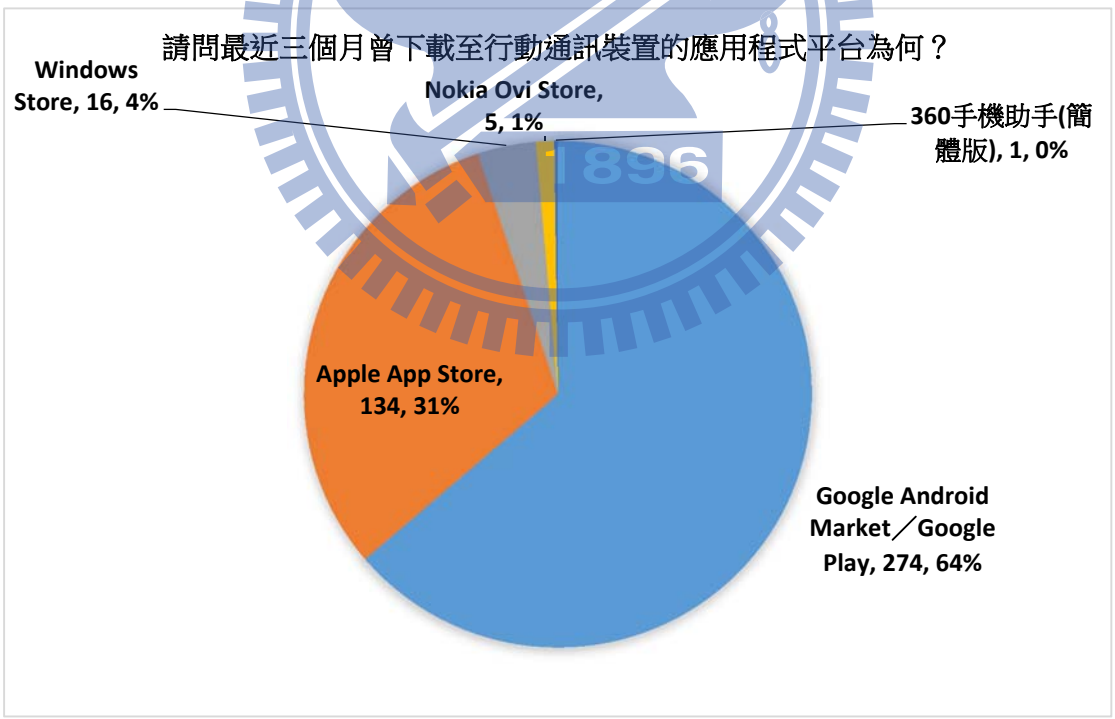
4.3.1. 行動通訊裝置的行動應用程式背景資料

為能了解使用者最常接觸和使用的行動應用程式平台和行動應用程式為何，因此詢問使用者最近三個月曾下載至智慧型裝置的應用程式為何、最近三個月內最常使用的行動應用程式類型、以及最近三個月曾經下載那些行動應用程式。為使使用者了解何謂行動通訊裝置，在問卷問題前，先針對行動通訊裝置為定義：「提供類似於個人電腦的功能，或是能下載行動應用程式的裝置，包含智慧型手機或平板電腦。」同時，假設使用者手邊同時有許多種行動裝置，煩請使用者以「使用頻率最高者」為作答對象。

4.3.1.1. 64%的使用者，自 Google Android Market／Google Play 下載應用程式

為了解使用者最近三個月內使用的行動應用程式平台為何，羅列目前使用者可能使用的行動應用程式平台，包含 Apple App Store、Google Android Market／Google Play、Nokia Ovi Store、Windows Store 和其他等。從問卷的結果分析得知，使用者中 64%使用 Google Android Market／Google Play、31%使用 Apple App Store（參見圖二）。

圖二：行動應用程式平台使用情況



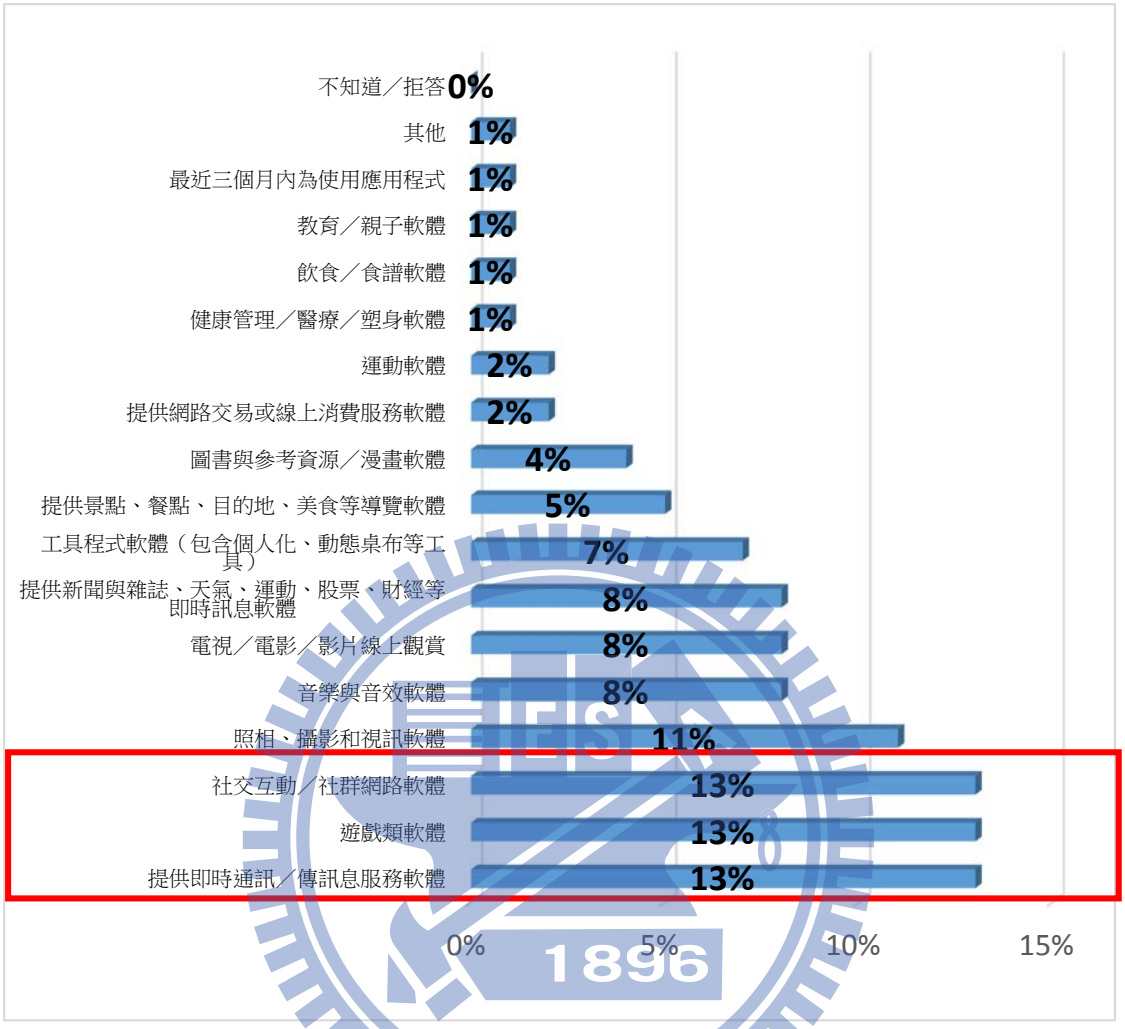
4.3.1.2. 使用者最近三個月內曾經下載的行動應用程式類型和最常使用的行動應用程式類型

自 Apple App Store[218]、Google Android Market／Google Play[219]、Nokia Ovi Store[220]和 Windows Store[221]四大主要行動應用程式平台所提供的應用程式種類，整理出以下 15 種類型提供受訪填選，包含：運動軟體、遊戲類軟體、教育／親子軟體、音樂與音效軟體、飲食／食譜軟體、照片、攝影和視訊軟體、社交互動／社群網路軟體、電視／電影／影片線上觀賞、健康管理／醫療／塑身軟體、圖書與參考資源／漫畫軟體、提供即時通訊／傳訊息服務軟體、提供網路交易或線上消費服務軟體、提供景點、餐點、目的地、美食等導覽軟體、工具程式軟體（包含個人化、動態桌布等工具）、以及提供新聞與雜誌、天氣、運動、股票、財經等即時訊息軟體，並提供「其他」此一選項，供使用者填寫不屬於上述 15 種類型的其他行動應用程式。再者，由於使用者可能最近三個月內未使用或未下載行動應用程式，或者使用者不知道或不願回答其所使用或下載的應用程式有哪些，是故選項中設有「不知道／拒答」、「最近三個月內未使用應用程式」、「最近三個月內未下載應用程式」，提供使用者填答。最後，由於使用者最近三個月內「最常使用」和「曾經下載」的應用程式可能不只一個，因此這兩道題目均為複選題。

從圖三可看出，使用人數最多的行動應用程式前三名分別為：提供即時通訊／傳訊息服務軟體（13%）、遊戲類軟（13%）、社交互動／社群網路軟體（13%）。另外，「其他」選項中，包含以下的行動應用程式：衛星定位導航軟體（1 人）、記帳（2 人）、交通資訊、地圖(純地圖非導覽)、閱讀電子書（TXT 等）程式（1 人）、公車到站訊息（1 人）、法源（1 人）、和字典（1 人）。

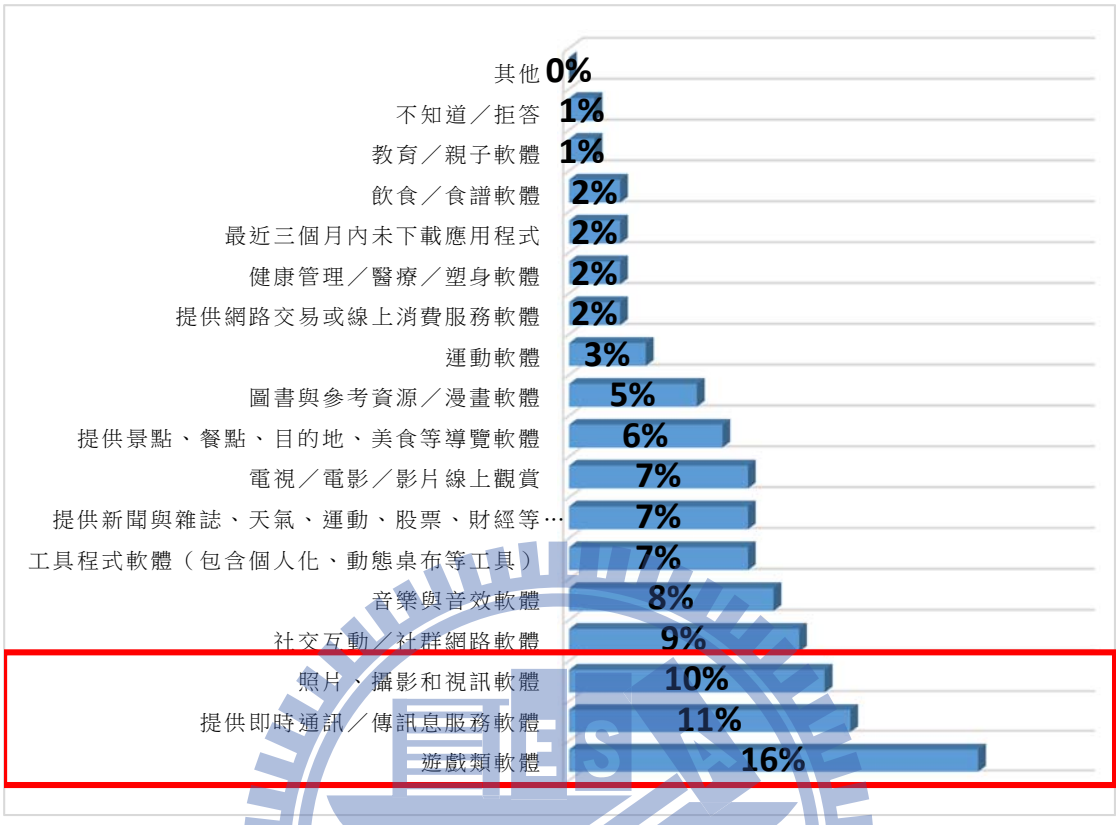
218 *iTunes Preview*, APPLE INC., https://itunes.apple.com/us/genre/ios/id36?mt=8 (last visited Oct. 10, 2013).
219 *Google Play*, GOOGLE, https://play.google.com/store (last visited Oct. 10, 2013).
220 *Ovi Store*, NOKIA, http://store.ovi.com/ (last visited Oct. 10, 2013).
221 *Windows Phone*, MICROSOFT, http://www.windowsphone.com/en-us/store (last visited Oct. 10, 2013).

圖三：最近三個月內，使用者最常使用的行動應用程式類型



另一方面，從圖四可得知使用者最近三個月內曾經下載的行動應用程式中，下載人數最多的應用程式前三名分別為：遊戲類軟體（16%）、提供即時通訊／傳訊息服務軟體（11%）、以及照片、攝影和視訊軟體（10%）。此外，「其他」選項中，包含以下的行動應用程式：有更新的應用程式（1 人）、GPS 導航（1 人）、以及日曆、文件管理（1 人）。

圖四：最近三個月內，使用者曾經下載的行動應用程式類型



4.3.2. 使用者閱讀隱私聲明的情況

隱私權政策和權限清單為業者對使用者呈現隱私聲明的方法之一，讓使用者在下載行動應用程式前，得以了解業者在使用者使用應用程式的同時，應用程式可能會如何蒐集、使用使用者的個人資料，以及如何將使用者的個人資料分享給第三方業者。因此，使用者是否閱讀業者提供的隱私權政策或權限清單，以及使用者是否了解其內容，攸關使用者在下載行動應用程式前，是否可知悉業者隱私操作的情況。

大部分業者會以張貼隱私權政策，做為提供隱私聲明的方式。在業者有隱私權政策的情況下，應用程式平台會在行動應用程式說明頁面張貼隱私權政策的網頁連結，讓使用者得以閱讀隱私權政策。為探究我國使用者閱讀隱私權政策的狀況，在詢問使用者相關問題前，先以臉書的隱私權政策為範本[222]，供使用者了解何謂隱私權政策。

以 Facebook（臉書）應用程式的隱私權政策為例，內容包含：

- 我們所收到的資訊以及如何使用的規範（瞭解本網站收到的資訊種類，以及資訊使用方式。）；
- 在 Facebook 上分享和搜尋您（瞭解可以協助控制您在 facebook.com 資訊的隱私設定。）；

222 *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Oct. 10, 2013).

- 其他網站和應用程式（瞭解社交外掛程式之類的應用程式，以及您和您的朋友在 Facebook 使用遊戲、應用程式和網站時的資訊分享方式。）；
- 廣告和動態贊助的運作方式（查看不必和廣告商分享您的資訊就能提供廣告的運作方式，並瞭解我們如何搭配廣告和社群脈絡，如動態消息風格的動態贊助。）；
- Cookie、像素和其他系統技術（瞭解 cookie、像素和工具（如本機儲存）如何使用來提供您各種服務、功能和相關廣告及內容。）；
- 其他您需要瞭解的資訊（瞭解我們對此政策所做的更改以及更多詳情。）。

此外，Google Play 和 Microsoft Store 兩個應用程式平台，均透過揭示「權限清單作為提供使用者隱私聲明的另一種方式。在使用者安裝應用程式前，行動應用程式會主動揭示並羅列該應用程式所需要的所有權限，使用者同意「接受」所有權限後，才得以下載應用程式；相反地，若使用者拒絕「接受」應用程式所需要的權限，使用者即無法下載該應用程式。

為知悉我國使用者閱讀權限清單的狀況，在詢問使用者相關問題前，先以 Google Play 上臉書提供的權限清單作為範本[223]，供使用者了解隱私權政策為何。

「權限清單」是在安裝下載前，行動應用程式會先跳出一個視窗，告知行動應用程式下載後，會要求使用者授予怎樣的權限。以 Facebook（臉書）應用程式為例，權限清單會有：

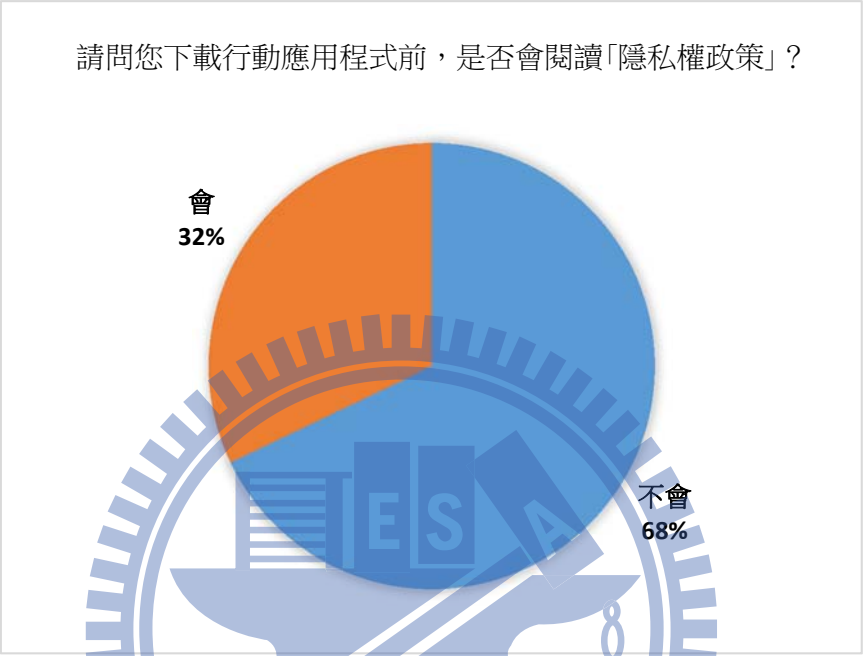
- 您的帳戶（建立帳戶及設定密碼、新增或移除帳戶）；
- 硬體控制介面（拍照和拍攝影片）；
- 您的位置資訊（概略位置（以網路為基準、精確位置（以 GPS 和網路為基準））；
- 網路通訊（完整網路存取權）；
- 您的個人資訊（讀取您的聯絡人、修改您的聯絡人）；
- 手機通話（讀取手機狀態和識別碼）；
- 儲存空間（修改或刪除 USB 儲存裝置的內容、修改或刪除 SD 卡的內容）；
- 系統工具（防止平板電腦進入休眠狀態；防止手機進入休眠狀態、開啟及關閉同步功能）；
- 您的帳戶（尋找裝置上的帳戶）；
- 硬體控制介面（控制震動）；
- 網路通訊（查看 WIFI 連線、查看網路連線、接收網際網路資料）；
- 系統工具（讀取同步處理設定）；
- 預設（測試能否存取受保護的儲存裝置；測試能否存取受保護的儲存裝置、寫入通話紀錄、讀取通話紀錄）。

223 *Facebook*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.facebook.katana&hl=zh-TW (last visited Oct. 10, 2013).

4.3.2.1. 68%的使用者「不會」閱讀隱私權政策

根據問卷結果分析，68%的使用者（292 人）在下載行動應用程式前，不會閱讀隱私權政策；僅 32%的使用者（138 人）閱讀隱私權政策（請見圖五）。

圖五：使用者閱讀隱私權政策的情況



為進一步探究使用者不讀隱私權政策的原因，遂詢問「不會」閱讀隱私權政策的使用者，造成他們「不讀」隱私權政策最主要的原因為何，並提供下列選項供使用者填答，包含：「字體太小」、「敘述太冗長」、「語言非繁體中文」、「不知道有隱私權政策」、「找不到隱私權政策的位置」、「內容看不懂：有太多資訊術語」、「內容看不懂：有太多法律詞彙」、「等不及，想趕快使用應用程式」、「使用者沒辦法改變隱私權政策，看了也沒有用」、以及「其他」。由於使用者不閱讀隱私權政策的原因可能不只一個，因此本題為複選題，並限定使用者最多選三個原因，以便讓使用者不讀隱私權政策的原因，更趨明確。

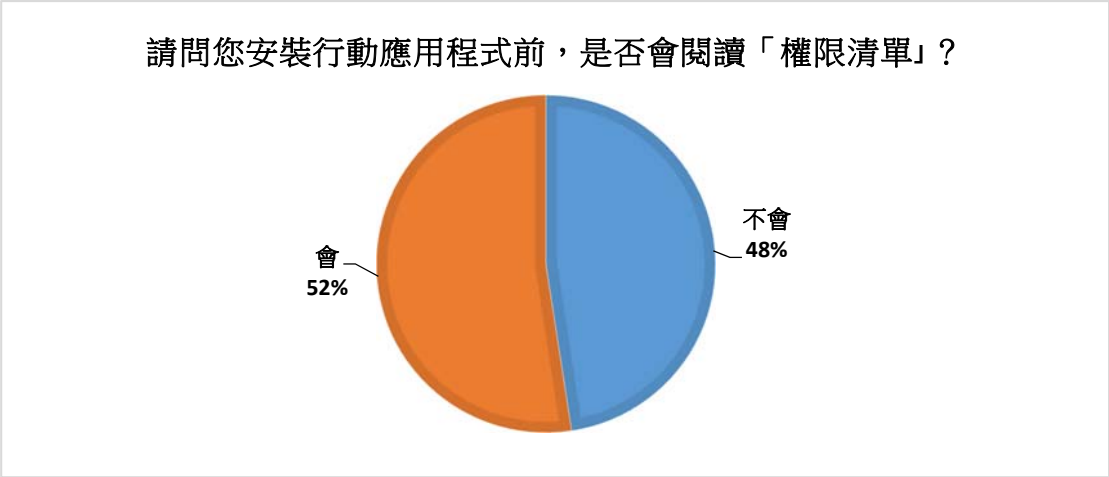
從圖六可發現，292 位不會閱讀隱私權政策的使用者中，有高達 223 位使用者認為隱私權政策的敘述太冗長，導致其不願意閱讀隱私權政策；有 124 位使用者不讀隱私權政策的原因在於「等不及，想趕快使用應用程式」；以及有 115 位使用者認為「使用者沒辦法改變隱私權政策，看了也沒有用」。此外，亦有部份使用者認為隱私權政策的字體太小，以及內容過於艱澀，充斥太多法律詞彙和資訊術語，是讓他們不閱讀隱私權政策的理由。

圖六：使用者不讀隱私權政策的主要原因

4.3.2.2. 52%的使用者「會」閱讀權限清單

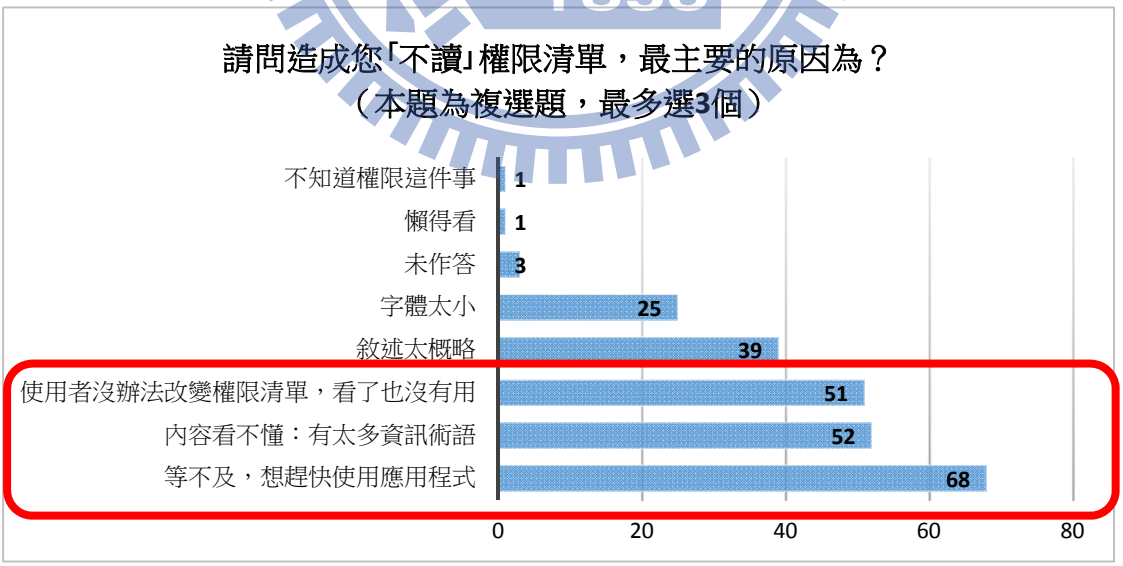
在 288 位使用 Google Play 或 Microsoft Store 下載應用程式的使用者中，有 52%的使用者在安裝行動應用程式前，會閱讀權限清單（請參見圖七）。

圖七：權限清單的閱讀情況



為進一步探究使用者不讀權限清單的原因，遂詢問「不會」閱讀權限清單的使用者，造成他們「不讀」權限清單最主要的原因為何，並提供下列選項供使用者填答，包含：「字體太小」、「敘述太概略」、「內容看不懂：有太多資訊術語」、「等不及，想趕快使用應用程式」、「使用者沒辦法改變權限清單，看了也沒有用」、以及「其他」。由於使用者不閱讀權限清單的原因可能不只一個，因此本題為複選題，並限定使用者最多選三個原因，以便讓使用者不讀隱私權政策的原因，更趨明確。

圖八：不讀權限清單的主要原因



從中可發現，縱然業者在使用者安裝應用程式前，主動提供使用者權限清單，增加使用者閱讀隱私通知，知悉業者隱私操作的機會。然而，使用者是否確實接收隱私通知的內容，是否在了解權限清單的內容後，再行按下「接受」鍵，仍有疑慮。從問卷調查結果可知，在 137 位使用者中，28%的使用者因為「等不及，想

趕快使用應用程式」，而不會閱讀權限清單。有 22%的使用者因為看不懂權限清單中的資訊術語，因而不會閱讀權限清單。此外，21%的使用者認為使用者沒辦法改變應單，看了也沒有用，所以在安裝行動應用程式前，不會閱讀權限清單（詳細人數統計，請見圖八）。

4.3.2.3. 閱讀隱私聲明和使用者年齡間的關聯性

本文將使用者的年齡設定為變數後，再行分析閱讀隱私權政策和閱讀權限清單的情況：

1. 隱私權政策和使用者年齡間的關聯程度

將使用者的年齡設定為變數後再行分析，可以發現隨著使用者的年齡增長，在下載行動應用程式前「會」閱讀隱私權的比例提升。尤其，以 25 歲作為界線，25 歲以上的使用者，在下載行動應用程式前會閱讀隱私權政策的比例達 41.75%；25 歲以下的使用者，則僅有 24%的使用者會閱讀隱私權政策（請參見表五）。

表五：使用者年齡和閱讀隱私權政策的關聯性

	下載行動應用程式前，是否會閱讀「隱私權政策」？		
使用者年齡	**不會**	**會**	**總計**
未滿 13 歲	6 人 (100%)	0 人 (0%)	6
13-17 歲	70 人 (78%)	29 人 (22%)	99 人
18-24 歲	82 人 (74%)	29 人 (26%)	111 人
25-34 歲	78 人 (64%)	44 人 (36%)	122 人
35-44 歲	39 人 (65%)	21 人 (35%)	60 人
45-54 歲	13 人 (54%)	11 人 (46%)	24 人
55 歲以上	4 人 (50%)	4 人 (50%)	8 人
總計	**292 人 (68%)**	**138 人 (32%)**	**430 人**

在下載應用程式前會先閱讀隱私權政策且 25 歲以上的受訪者共有 80 人。進一步探究他們的教育程度和就業狀況，可發現 99%受有大學、大專院校以上的教育水平；此外，90%的受訪者為就業人士（請參見表六）。

表六：25 歲以上且下載行動應用程式前會先閱讀隱私權政策之受訪者的教育程度與就業狀況比較表

	待業中／家管		合計	就業中（正職／兼職）				合計	學生		合計	總計
受訪者年齡	大學、大專院校	碩士		高中、職	大學、大專院校	碩士	博士		碩士	博士		
25-34 歲		1	**1**		23	14		**37**	5	1	**6**	**44**
35-44 歲				1	15	4	1	**21**				**21**
45-54 歲	1		**1**		5	5		**10**				**11**
55 歲以上					2	2		**4**				**4**
總計	**1**	**1**	**2**	**1**	**45**	**25**	**1**	**72**	**5**	**1**	**6**	**80**

2. 權限清單與年齡間的關聯性

以年齡作為變數，Google Android Market／Google Play 和 Windows Store 的使用者共 288 位，其中三位受訪者未回答本題，故分析樣本為 285 人。可發現閱讀權限清單的情況並未如隱私權政策一般，在安裝行動應用程式前會閱讀權限清單的比例，隨著年齡增長而提升，可以 25 歲作為界線加以觀察。然而從表八可發現，18 歲到 54 歲的受訪者中，過半數的使用者會閱讀權限清單。

表七：使用者年齡和閱讀權限清單的關聯性

	閱讀權限清單的情況		
年齡	**不會**	**會**	**總計**
未滿 13 歲	3 人 (100%)	0 人 (0%)	3 人
13-17 歲	51 人 (66%)	26 人 (34%)	77 人
18-24 歲	27 人 (35%)	49 人 (65%)	76 人
25-34 歲	29 人 (38%)	47 人 (62%)	76 人
35-44 歲	17 人 (50%)	16 人 (50%)	33 人
45-54 歲	5 人 (38%)	8 人 (62%)	13 人
55 歲以上	5 人 (71%)	2 人 (29%)	7 人
總計	**137 人 (48%)**	**148 人 (52%)**	**285 人**

在下載應用程式前會先閱讀權限清單的受訪者中，18 歲到 54 歲的使用者中共有 120 人。進一步探究他們的教育程度和就業狀況，可發現 89%受有大學、大專院校以上的教育水平（請參見表八）。

表八：18 歲到 54 歲且下載行動應用程式前會先閱讀權限清單之受訪者的教育程度與就業狀況比較表

	待業中／家管			合計	就業中（正職／兼職）				合計	學生			合計	總計
受訪者年齡	大學、大專院校	碩士	博士		高中、職	大學、大專院校	碩士	博士		大學、大專院校	碩士	博士		
18-24 歲	1			**1**	1	7			**8**	25	15		**40**	**49**
25-34 歲	1	1	1	**3**		18	15		**33**		9	2	**11**	**47**
35-44 歲					1	8	3	3	**15**			1	**1**	**16**
45-54 歲											7	1	**8**	**8**
總計	**2**	**1**	**1**	**4**	**2**	**23**	**18**	**3**	**56**	**25**	**31**	**4**	**60**	**120**

本文認為，在下載行動應用程式前，使用者「會」閱讀隱私權政策、「會」閱讀權限清單的比例，會普遍集中在 25 歲以上，應該與使用者的心智年齡、教育程度和就業狀態有關。

首先，從心理學的角度，少年和青少年傾向在不能確定後果的情況下，選擇做出決定，這樣的行為稱為風險行為（Risky Behaviors）。Margo Garner 教授和 Laurece Steinberg 教授在其合寫的文章「Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: An Experimental Study」中，發現 13-16 歲的青少年和 18-22 歲的少年相較於 24 歲以上的成年人，更傾向於做出風險行為或做出風險決定[224]。尤其，青少年和少年容易受到群體行為（group behaviors）的影響，決定是否要做某件事情的判斷因素，是在於同儕前看起來是否夠酷或者是否和他們一樣，而不在意該行為是否會招致負面的後果，特別是這樣的負面影響通常不會立即發生。因此，青年和少年族群通常較不在乎個人資料，隱私意識也較成年人薄弱[225]。隨著心智的成熟，成年人在行為前，比較會考量做與不做的利弊得失，權衡之後再行動。因此，未避免個人資料受到不當的利用或資料外洩，隱私意識會有所提升。是故，在本文的量化研究中可發現，未滿 25 歲的受訪者在下載行動應用程式前會閱讀隱私權政策的比例低於 25 歲以上的受訪者。

224 Margo Garner & Laurece Steinberg, *Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: An Experimental Study*, 41 DEVELOPMENTAL PSYCHOLOGY 625, 625-35 (2005), *available at* http://www.temple.edu/psychology/lds/documents/PeerInfluenceonRisk-TakingDP.pdf.

225 Chris Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?*, at 5, *available at* http://ssrn.com/abstract=1589864 or http://dx.doi.org/10.2139/ssrn.1589864.

其次，從教育的角度觀察，由於隱私權政策用語和內容較為專業和艱澀，受過高等教育者，有較充足的智識去理解隱私權政策的內容，以及判斷業者的隱私操作是否合理，因而增加閱讀隱私權政策的動力。再者，由於行動通訊裝置的便利性，就業人士在工作上或日常生活愈發依賴智慧型裝置，例如儲存客戶和親朋好友電話的通訊簿、記錄何時開會的行事曆、行動商務的購物紀錄、或記載老闆交代任務的備忘錄等。根據 Jennifer M. Urban、Chris Jay Hoofnagle、Su Li 三位學者在 2012 年 7 月共同發表「Mobile Phones and Privacy」的調查報告中，可得知行動通訊裝置使用者認為存在智慧型裝置的個人資料是具有私人性的（private），其私人的程度不亞於家用電腦[226]。當越多私人的資料存在行動通訊裝置中，尤其這些資訊可能涉及商業機密，使用者會更加注意行動通訊裝置和行動應用程式的隱私操作。因而藉由閱讀隱私權政策，加以審核、確認該行動應用程式是否真地可以確保其隱私，以及會蒐集那些個人資料、會如何使用和傳送其個人資料

4.3.2.4. 綜合分析

綜合比較前述統計分析結果可發現，隱私權政策的閱讀情況和權限清單的閱讀情況相較，較多使用者在下載應用程式前會閱讀權限清單，本文認為這可能和呈現權限清單的方式有關。

使用者在安裝行動應用程式前，必須先同意權限清單的內容，才得以安裝應用程式。亦即，應用程式平台形同強迫使用者，在下載應用程式前，須先確認是否接受應用程式所需要的權限，對應用程式所可能蒐集或使用者的個人資訊有所了解後，再行安裝行動應用程式。此舉，和隱私權政策的呈現模式相異。隱私權政策需要使用者主動地點閱應用程式提供的隱私權政策之網頁連結，連結到業者的隱私權政策網頁後，使用者才得以知悉隱私權政策的內容。簡言之，隱私通知在內容呈現上，權限清單是業者主動地揭露，而隱私權政策則是被動地呈現。正因如此，使用者閱讀權限清單的機會增加，會閱讀權限清單的比例也較高。

此外，比較使用者不看隱私權政策和不讀權限清單的前三大主要原因，可以發現皆有「等不及，想趕快使用應用程式」和「使用者沒辦法改變隱私權政策／權限清單，看了也沒有用」這兩個原因。從上述結果可將使用者不讀隱私聲明的原因區分為兩個面向：第一，隱私聲明的呈現有缺陷；第二，使用者無法改變業者對隱私操作的現況，而放棄閱讀隱私聲明。

首先，一般業者提供隱私聲明內容並不口語，一般使用者不一定能在短時間內，快速掌握隱私聲明中提到的每一個法律詞彙和資訊術語的定義與涵義。易言之，隱私聲明過於艱澀，使用者會有需要花時間閱讀隱私聲明的預期心理，因而不讀隱私聲明。更關鍵的原因在於，使用者必然是有功能上的需求，才會安裝或使用具有特定功能的行動應用程式。此時，在下載行動應用程式、享受應用程式功能前，還要花時間閱讀難懂的隱私聲明，未免強人所難。尤其隱私權政策在呈現上，均為提供連結至業者網站上的隱私權政策頁面的網址，而非專門為行動應

226 *Supra* note 211, 8-9.

用程式編寫的隱私權政策頁面。然而，一般網頁上的隱私權政策，多半都有字數多且字體小的特性，而這樣的特性，在行動通訊裝置上會更加明顯，因為行動通訊裝置的螢幕肯定比一般電腦的螢幕小上許多，造成使用者閱讀上的不便。

其次，使用者無法調整隱私聲明的內容，也是使用者不會閱讀隱私通知的主因。造成使用者覺得「使用者沒辦法改變隱私權政策／權限清單，看了也沒有用」的原因，或許可從某位使用者的留言略知一二：「user 處於相對弱勢，應有適當的法規與辦法以規範業者的行為」。因此，使用者和業者地位不對等，只有業者可以決定隱私聲明的內容，並依照業者的想法更新隱私聲明的內容，使用者對隱私聲明的內容無置喙的權力。

4.3.3. 使用者對隱私聲明的了解程度

針對下載行動應用程式前會閱讀隱私聲明的使用者，進一步調查使用者對隱私聲明的了解程度。藉由五點等級量表，來量化使用者的了解程度，以「完全不了解」為 1 分、「完全瞭解」為 5 分作為評分基礎，讓使用者依據其閱讀隱私聲明的了解程度作答。

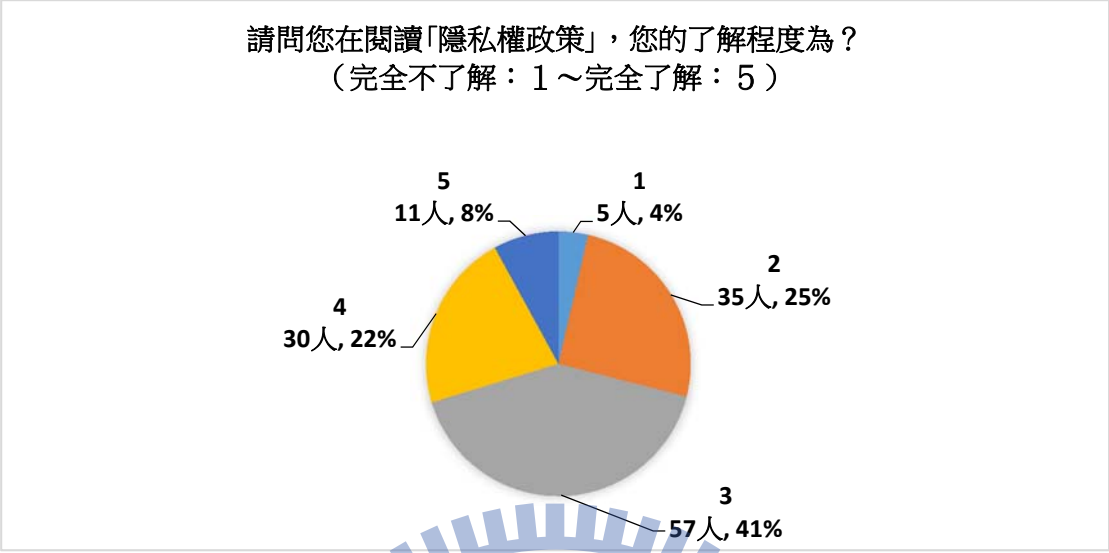
此外，對於選填「1 分」和「2 分」的使用者，由於其對隱私聲明的內容傾向不了解，遂詢問致使使用者「看不懂」隱私聲明的最主要原因為何，並提供特定選項供使用者選擇。在隱私權政策的部分，看不懂的原因有：「敘述太冗長」、「語言非繁體中文」、「內容看不懂：有太多法律詞彙」、「內容看不懂：有太多資訊術語」、「不理解個人資料蒐集與應用程式功能間的關聯」、以及提供使用者填寫其他原因的選項「其他」。另一方面，在權限清單的部分，看不懂的主要原因有：「敘述太概略」、「內容看不懂：有太多資訊術語」、「不知道權限清單對我會造成什麼影響」、「不理解個人資料蒐集與應用程式功能間的關聯」、以及提供使用者填寫其他原因的選項「其他」。由於使用者看不懂隱私通知的理由可能不只一個，因此本題採取複選的題型設計，並限定使用者最多只能選填三個原因，以便讓使用者看不懂隱私權政策的原因，更趨明確。

最後，針對填選「3 分」、「4 分」和「5 分」的使用者，表示其對隱私通知具有一定的了解程度。因此，進一步詢問在他們了解隱私通知的情況下，認為隱私通知對使用者自行保護個人資料的幫助程度有多少，藉以了解隱私通知的效能。本題採取五點等級量表，以「非常沒有用」為 1 分到「非常有用」為 5 分作為評分基礎，讓使用者依據其認為隱私通知，能提供使用者自行保護個人資料的幫助程度作答。

4.3.3.1. 使用者對隱私權政策的了解程度

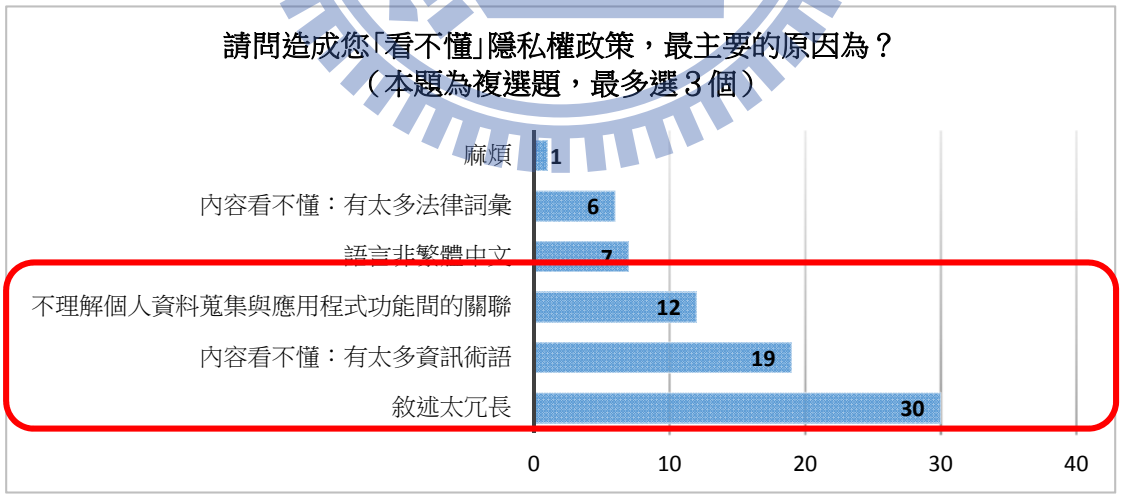
從圖九可知，勾選「1 分」的使用者有 5 位；「2 分」的使用者有 35 位、「3 分」的使用者有 57 位；「4 分」的使用者有 30 位；以及「5 分」的使用者有 11 位。總計，使用者認為對隱私權政策的了解程度，平均分數為 3.05 分。

圖九：使用者閱讀隱私權政策的了解程度



在填選「1 分」和「2 分」，偏向看不懂隱私權政策的 40 位使用者中，有 30 位認為因為隱私權政策的敘述太冗長，是造成使用者看不懂隱私權政策的主要原因。換言之，因為隱私權政策的字數過多、篇幅過長，致使看不懂隱私權政策的人數比例高達 75%。另外，有將近半成、共計 19 位使用者，因為看不懂隱私權政策中提到的資訊術語，而無法理解隱私權政策的內容（請見圖十）。

圖十：使用者看不懂隱私權政策的主要原因

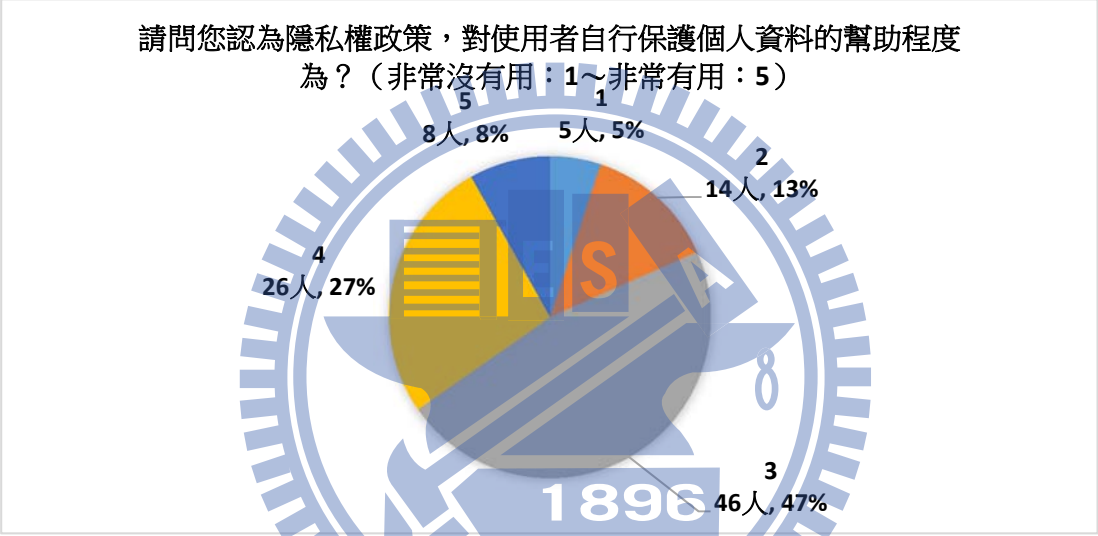


從問卷分析中，可以發現一個有趣的結果：「不讀」隱私權政策和「看不懂」隱私權政策的使用者，填選出來人數最多的主要原因均為「敘述太冗長」。本文以為這並非巧合，使用者多半很難在行動通訊裝置的小螢幕上，閱讀篇幅過長的隱私權政策；即便讀了，也可能看了後面，忘了前面，因而無法了解隱私權政策的意涵和內容。因此，本文可以得到一個簡單的結論，要改善使用者閱讀隱私權政策

的情況，應先改變隱私權政策在行動通訊裝置上的呈現方式，設計成讓使用者願意讀、容易讀、且容易理解的形式。

另外，針對 98 位填選「3 分」、「4 分」和「5 分」的使用者，詢問在他們了解隱私權政策的情況下，認為隱私權政策是否對使用者自行保護個人資料帶來幫助。從圖十一的統計數據可得知，勾選「1 分」的使用者有 5 位；「2 分」的使用者有 13 位、「3 分」的使用者有 46 位；「4 分」的使用者有 26 位；以及「5 分」的使用者有 8 位。因此在 98 位使用者中，認為隱私權政策提供幫助的程度，平均分數為 3.19 分。

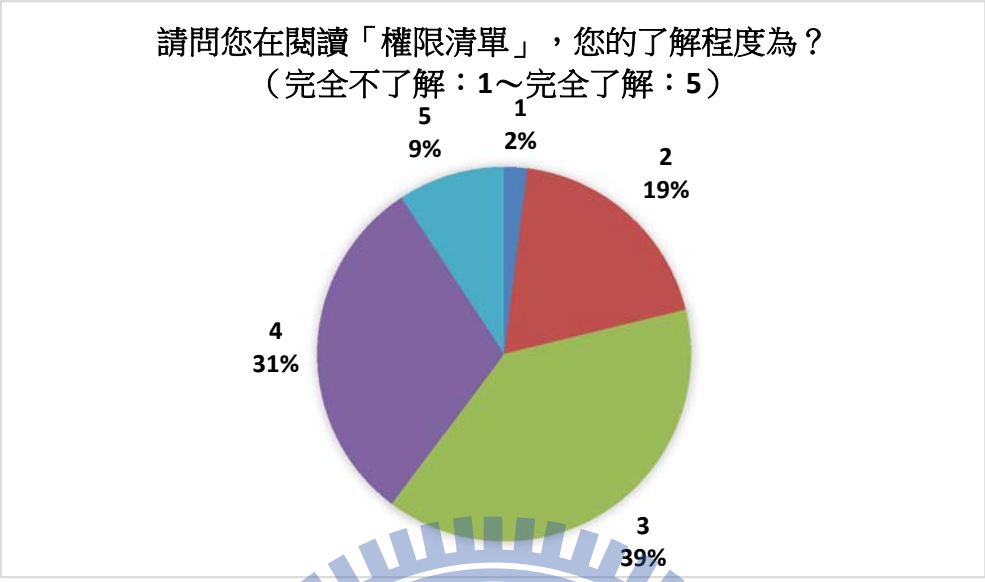
圖十一：隱私權政策對使用者自行保護個人資料的幫助程度



4.3.3.2. 使用者對權限清單的了解程度

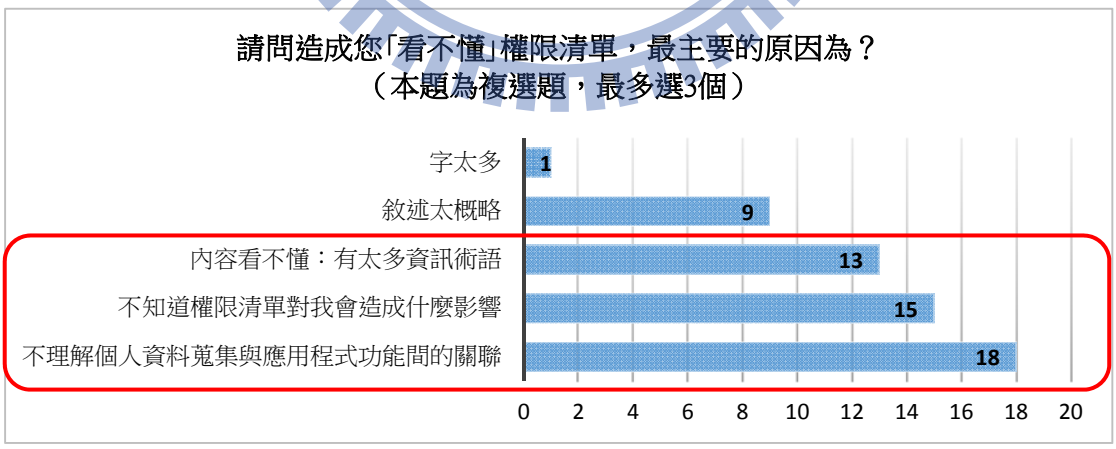
對於使用者了解權限清單內容的程度分析，勾選「1 分」的使用者有 3 位；「2 分」的使用者有 29 位、「3 分」的使用者有 59 位；「4 分」的使用者有 46 位；以及「5 分」的使用者有 14 位。因此，151 位使用者對權限清單的了解程度，平均分數為 3.26 分。

圖十二：權限清單的了解程度



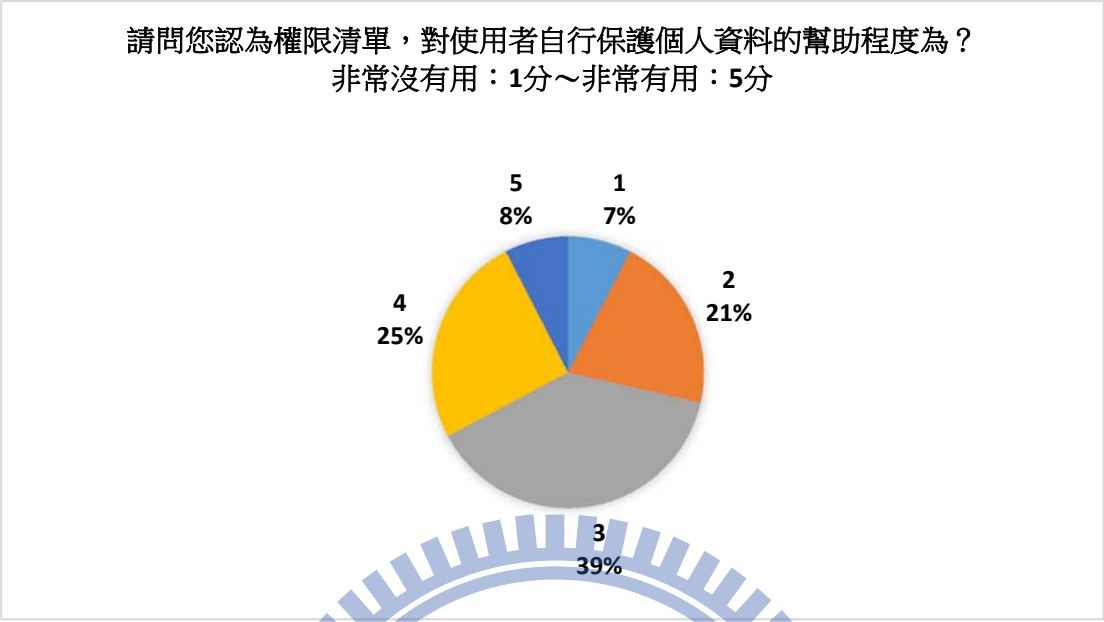
從圖十三可發現，看不懂權限清單的 32 位使用者中，有 18 位使用者認為造成他們看不懂權限清單的主要原因，在於「不理解個人資料蒐集與應用程式功能間的關聯」。換言之，使用者無法理解為什麼行動應用程式提供的功能，需要權限清單中列舉的權限，例如遊戲類型的應用程式，需要位置資訊。單純從權限清單的內容，使用者只能知道該應用程式需要那些權限，但無法從權限清單中了解，為何業者需要這些權限和個人資料。此外，有 15 位使用者不知道權限清單的內容，會對使用者造成什麼影響；13 位使用者因為不理解權限清單中的資訊術語，而看不懂權限清單。

圖十三：使與者看不懂權限清單的主要原因



針對 119 位填選「3 分」、「4 分」和「5 分」的使用者，詢問在他們了解權限清單的情況下，認為權限清單對使用者自行保護個人資料的幫助程度有多少，從圖十四可知，勾選「1 分」的使用者有 9 位；「2 分」的使用者有 25 位、「3 分」的使用者有 46 位；「4 分」的使用者有 30 位；以及「5 分」的使用者有 9 位。平均而言，119 位使用者認為權限清單的幫助程度為 3.04 分。

圖十四：權限清單對使用者自行保護個人資料的幫助程度



4.3.3.3. 綜合分析

從針對在安裝行動應用程式前，會閱讀隱私通知的使用者所得出的統計結果，可發現隱私權政策和權限清單反映出類似的情況：會閱讀隱私通知的使用者，對隱私通知內容的了解程度大約是 3 分；而針對隱私通知內容偏向了解的使用者，對於隱私通知對使用者自行保護個人資料的幫助程度也落在 3 分左右。蓋隱私通知的目的，在於將業者的內部隱私通知公開化、透明化，讓使用者得以了解業者的隱私操作，進而判斷是否要安裝應用程式。亦即，隱私通知理應對使用者的資訊自決權的施展有所幫助，可以協助使用者決定自身個人資料是否被蒐集、使用或分享給第三方業者。

然而，從統計結果可得知，多數的使用者安裝行動應用程式前，並不會閱讀隱私通知。又針對會閱讀隱私通知的使用者而言，使用者對隱私通知的理解程度，以及隱私通知對使用者自我管理個人資料的幫助，都達到剛好及格的分數。從問卷結果可推知，隱私通知未能完全發揮告知使用者的功能。

4.3.4. 隱私聲明對使用者安裝應用程式意願的影響

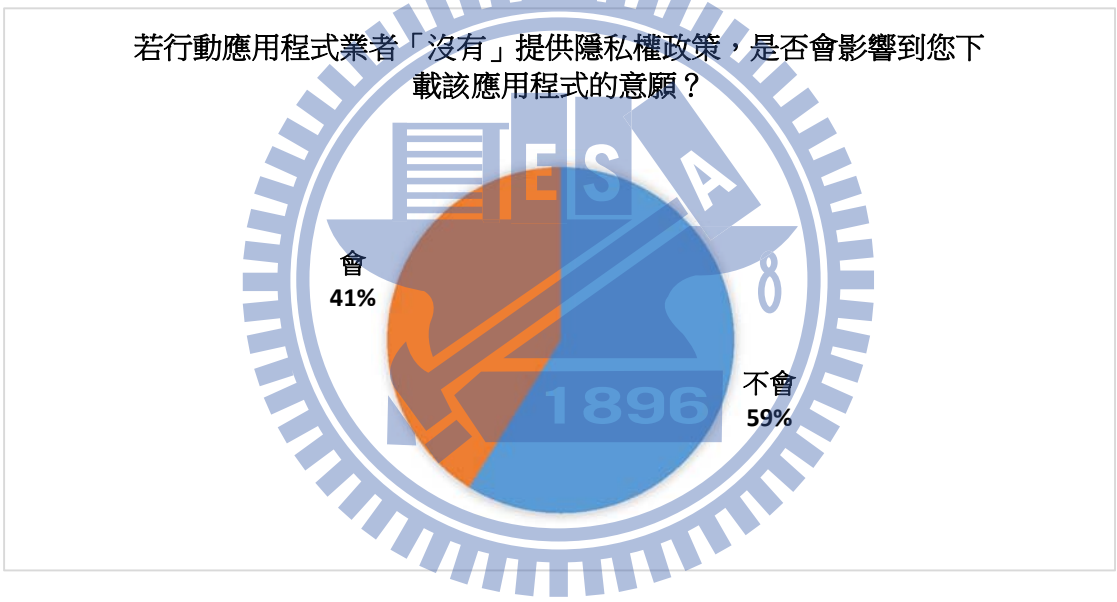
為能藉由了解使用者在安裝應用程式時的習慣，探究隱私聲明對使用者的影響程度，遂詢問使用者「若行動應用程式業者沒有提供隱私權政策，是否會影響到您下載該應用程式的意願？」、「行動應用程式權限清單上，列舉的項目數量，是否會影響您下載應用程式的意願？」，從使用者的回答來分析隱私聲明是否會影養使用者安裝行動應用程式。

4.3.4.1. 「沒有」隱私權政策不會影響使用者下載應用程式的意願

根據 Future of Privacy Forum 機構 2012 年 6 月的統計，在 iOS App Store、Google Play 和 Kindle Fire Appstire 中最受歡迎前 150 名的應用程式，61.3%會提供隱私權政策[227]。因此，在並非所有應用程式都會提供隱私權政策的情況下，筆者希望透過了解我使用者是否會因為應用程式「沒有」提供隱私權政策，而影響行動應用程式下載的意願。換言之，隱私權政策的有無，是否為使用者下載應用程式與否的判斷指標？

統計問卷結果發現，答案是否定的，行動應用程式業者未提供隱私權政策，不會影響其下載應用程式意願的使用者。從圖十五可知，59%的使用者認為隱私權政策的有無，並非是否下載行動應用程式的判斷因素之一。

圖十五：隱私權政策存在與否和應用程式下載意願的關聯



4.3.4.2. 權限清單列舉的權限數量，會影響使用者下載應用程式的意願

當 52%的使用者在安裝應用程式前會閱讀權限清單時，行動應用程式需要的權限多寡，是否會影響使用者的下載意願？舉例而言，假設使用者欲安裝可以觀看電視連續劇的應用程式，當應用程式需要使用者授予 8 個權限，包含：儲存（允許應用程式寫入內部儲存空間）、網路通訊（允許應用程式建立網路設定）、位置（使用者的約略位置）、系統工具（防止手機進入待命狀態）、通話次數（允許應用程式存許裝置的電話功能資料）、網路通訊（接收網路資料）、帳戶（發現已知帳戶）以及硬體控制（控制震動）[228]，使用者在知悉權限內容後，是否會因

227 FPF MOBILE APPS STUDY, FUTURE OF PRIVACY FORUM, 1-2, *available at* http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf (last visited Oct. 10, 2013).

228 電視連續劇 (最新台劇、韓劇、大陸劇、日劇)，Google Play，https://play.google.com/store/apps/details?id=com.jumplife.tvdrama（最後瀏覽日期：2013 年 10 月

為應用程式需要的數量很多，且應用程式會蒐集使用者的通話紀錄、位置資訊和帳戶資訊，而決定不安裝該應用程式？

從圖十六可發現，答案是肯定的。應用程式所需要的權限數量，會影響使用者的下載意願。53%的使用者會因為權限清單列舉的數量，而影響其安裝應用程式的意願。

圖十六：應用程式權限清單列舉的權限數量和使用者下載意願關係

4.3.4.3. 綜合分析

隱私權政策和權限清單皆屬於隱私聲明，然而使用者受其影響的程度卻不同。從上述統計分析可得知，使用者較不會以隱私權政策的有無，作為判斷該應用程式是否可以下載的標準；然而使用者較會因為權限清單上的權限數量，決定是否安裝應用程式。本文以為，造成差異的原因在於隱私權政策和權限清單的呈現方式不同。

隱私權政策看似可有可無的原因，可以從大部分的使用者不閱讀隱私權政策之情況，略知一二。當 68%的使用者不閱讀隱私權政策，就表示有 68%的使用者並不知悉隱私權政策的內容，因而在下載行動應用程式前，就不會將業者的隱私操作內容，作為是否下載的考量因素。此外，並非所有應用程式業者均提供隱私權政策[229]。

相對地，在 Google Play 和 Microsoft Store 的應用程式平台上，每一個應用程式都會提供權限清單，而且使用者在安裝應用程式前，需先按下「接受」鍵後，

10 日）。

229 *See supra* note 227.

方能下載應用程式的情況下，因此有 58%的使用者會閱讀權限清單。縱然承研究報告顯示，使用者對權限清單內容的了解程度平均分數只有 3.26 分，然而使用者仍可從權限清單羅列的權限數量和權限的名稱，了解行動應用程式會蒐集或使用使用者那些個人資料。因此，權限清單的權限多寡，相較於隱私權政策的存否，較可以影響使用者的行動應用程式下載意願。

4.3.5. 使用者對行動應用程式蒐集其個人資料的介意程度

在問卷的最後部分，希望了解使用者是否介意行動應用程式蒐集其個人資料，藉以探知我國行動應用程式使用者的隱私意識。在本部分，將詢問使用者「最不想被蒐集的個人資料為何」、「對業者蒐集個人資料的介意程度」、以及介意或不介意的原因。

4.3.5.1. 使用者最不想被蒐集的個人資料：財務或付款相關資訊

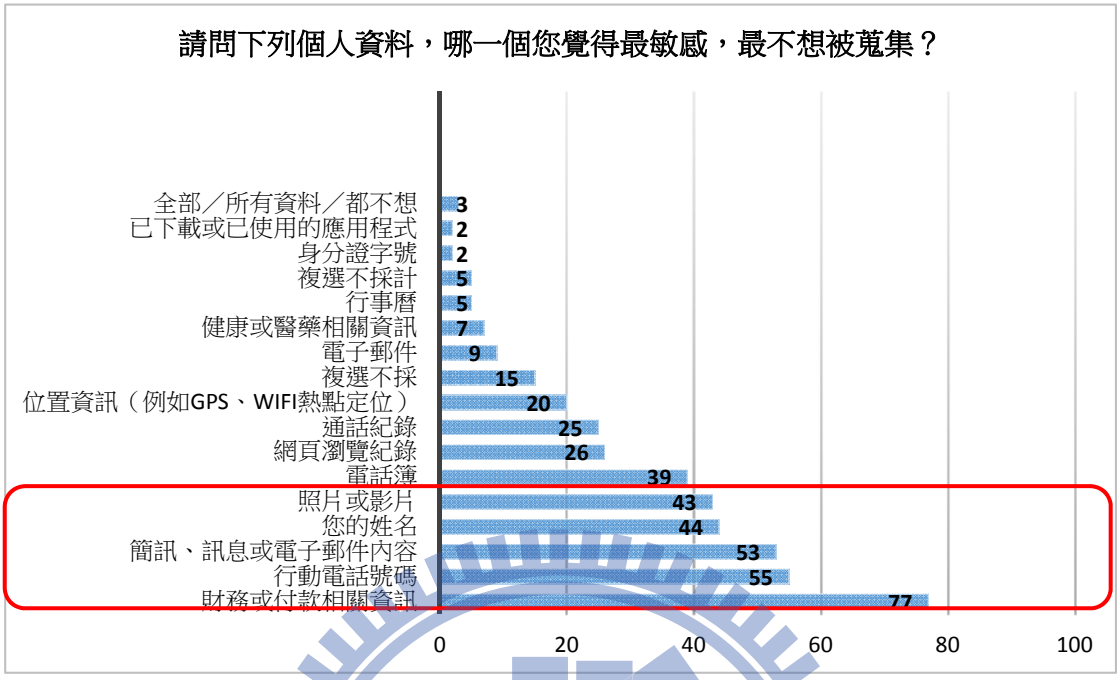
為了解我國行動應用程式使用者，認為何種個人資料是最敏感或最私人的資料，最不想要行動應用程式業者加以蒐集，以了解在使用者最在意那些個人資料，須提供較多的保護。因此筆者將行動應用程式所蒐集、使用的個人資料主要類型，整理如下表九，並提供「其他」此一選項，供使用者填寫不屬於下表 14 種類型的其他個人資料。由於希望使用者可以選出最不想被蒐集的個人資料，因此本題涉及為單選題，使用者僅能選擇一種個人資料。

表九：行動應用程式可能蒐集之主要個人資料類型（作者自行整理）

使用者姓名	行動電話號碼
行事曆	網頁瀏覽紀錄
電話簿	健康或醫藥相關資訊
帳戶資訊	財務或付款相關資訊
通話紀錄	簡訊、訊息或電子郵件內容
電子郵件	已下載或已使用的應用程式
照片或影片	位置資訊（例如 GPS、Wifi 熱點定位）

根據統計資料顯示，使用者最不想被蒐集的個人資料前五名為：「財務或付款相關資訊」、「行動電話號碼」、「簡訊、訊息或電子郵件內容」、「使用者的姓名」、以及「照片或影片」。除了「姓名」和「照片或影片」為可以直接識別出當事人的個人資料外，其餘個人資料均屬於可間接識別的個人資料。

圖十七：使用者最不想被蒐集的個人資料

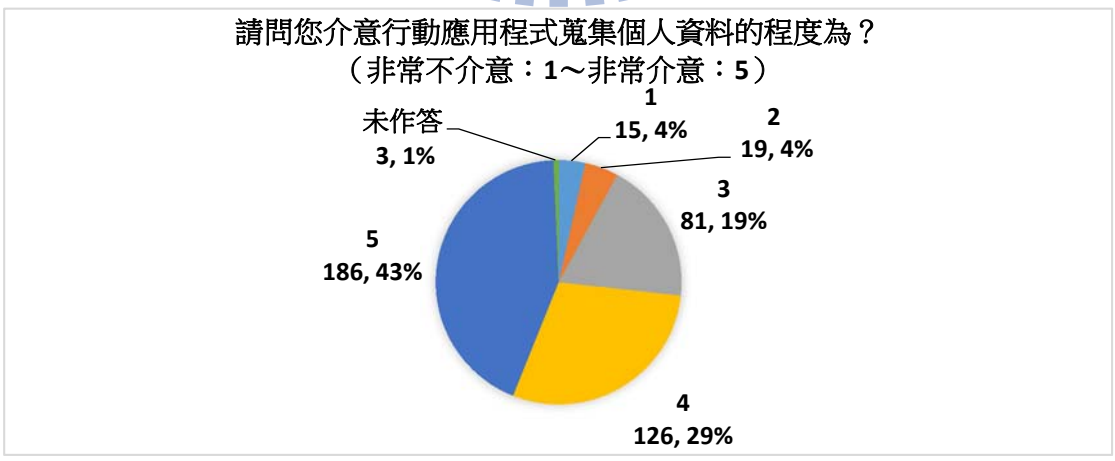


4.3.5.2. 使用者對行動應用程式蒐集其個人資料的介意程度

藉由五點等級量表，來量化使用者的對行動應用程式業者蒐集其個人資料的介意程度，了解使用者的隱私意識。以「非常不介意」為 1 分、「非常介意」為 5 分作為評分基礎，讓使用者依據其介意程度作答。

從研究結果可發現，有 53%的使用者填選「5 分」，表示其非常介意業者蒐集其個人資料。此外，填選 3 分以上的使用者佔全體使用者的 91%，足見使用者十分在意其個人資料被蒐集或使用。

圖十八：使用者對行動應用程式蒐集其個人資料的介意程度



對於選填「1 分」和「2 分」的使用者，對行動應用程式蒐集其個人資料傾向不介意，遂詢問致使使用者「不介意」的最主要原因為何，並提供特定選項供使用者選擇，包含：「行動應用程式的功能性更重要」、「不知道行動應用程式會蒐集個

人資料」、「行動應用程式所蒐集的個人資料不重要」、「反正沒辦法更改／拒絕個人資料的蒐集，就算了」、「行動應用程式蒐集個人資料，對我不會造成太大損害或不便」、以及提供使用者填寫其他原因的選項「其他」。由於使用者不介意的理由可能不只一個，因此本題採取複選的題型設計，並限定使用者最多只能選填三個原因，以便讓使用者不介意個人資料被蒐集的原因，更趨明確。

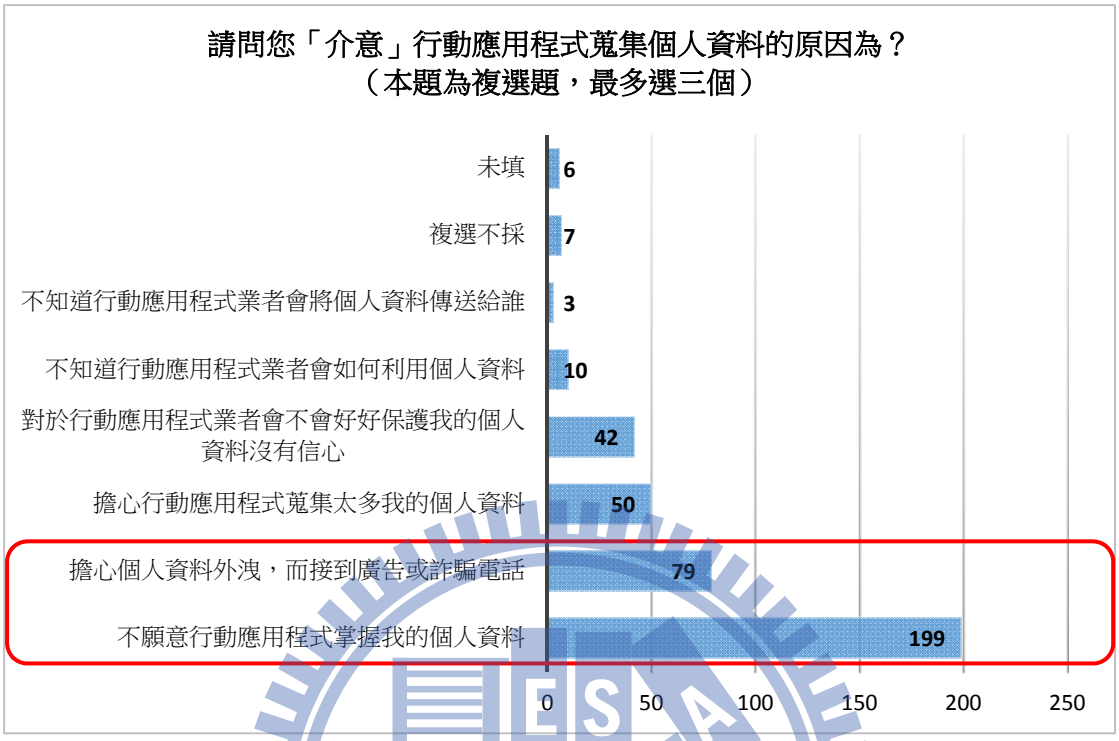
從圖十九可以發現，36 位表示不介意個人資料被蒐集的使用者中，有 29%的使用者認為「行動應用程式蒐集個人資料，對我不會造成太大損害或不便」，有23%的使用者認為「反正沒辦法更改／拒絕個人資料的蒐集，就算了」。從研究結果可以發現，因為使用者的消極態度，而無感於行動應用程式業者蒐集個人資料，或無力改變個人資料的蒐集，所以使用者不介意行動應用程式業者蒐集個人資料的原因。

圖十九：使用者不介意行動應用程式蒐集個人資料的原因

最後，針對填選「3 分」、「4 分」和「5 分」的使用者，傾向介意行動應用程式蒐集個人資料。因此，進一步詢問使用者介意的原因，並提供特定選項供使用者選擇，包含：「不願意行動應用程式掌握我的個人資料」、「擔心行動應用程式蒐集太多我的個人資料」、「擔心個人資料外洩，而接到廣告或詐騙電話」、「不知道行動應用程式業者會如何利用個人資料」、「不知道行動應用程式業者會將個人資料傳送給誰」、「對於行動應用程式業者會不會好好保護我的個人資料沒有信心」，以及提供使用者填寫其他原因的選項「其他」。由於使用者不介意的理由可能不只一個，因此本題採取複選的題型設計，並限定使用者最多只能選填三個原因，以便讓使用者不介意個人資料被蒐集的原因，更趨明確。

從圖二十發現，介意行動應用程式蒐集個人資料的 393 位使用者中，有高達50%的使用者認為介意的原因在於「不願意行動應用程式掌握我的個人資料」。此外，亦有 20%的使用者因為「擔心個人資料外洩，而接到廣告或詐騙電話」。

圖二十：使用者介意行動應用程式蒐集個人資料的原因



4.4. 小結

總結以上的研究結果，可發現一個有趣的現象：雖然高達 91%的使用者介意行動應用程式業者的蒐集其個人資料，然而僅有 32%的使用者會閱讀隱私權政策，以及 52%的使用者會閱讀權限清單。為何使用者不藉由閱讀隱私通知，加以確認業者的隱私操作是否會侵害其個人資料，卻十分介意行動應用程式蒐集使用者的個人資料？這看似衝突的結果，其實並不矛盾。本文以為可以從使用者不讀或看不懂隱私通知的原因，理出頭緒。

表十：使用者不閱讀或看不懂隱私通知的原因

		隱私通知	
		隱私權政策	權限清單
使用者不閱讀的原因	1	敘述太冗長	等不及，想趕快使用應用程式
	2	等不及，想趕快使用應用程式	內容看不懂：有太多資訊術語
	3	使用者沒辦法改變隱私權政策，看了也沒有用	使用者沒辦法改變隱私權政策，看了也沒有用
使用者看不懂的原因	1	敘述太冗長	不理解個人資料蒐集與應用程式功能間的關聯
	2	內容看不懂：有太多資訊術語	不知道權限清單對我造成什麼影響
	3	不理解個人資料蒐集與應用程式功能間的關聯	內容看不懂：有太多資訊術語

從表十可發現，使用者不閱讀或看不懂的原因，可以區分為二類：隱私通知的呈現方式和使用者的弱勢地位。蓋冗長又充斥太多資訊術語的隱私通知，並非對使用者友善地資訊告知；同時，也讓使用者為了能盡快享受應用程式的功能，而放棄閱讀隱私通知，直接安裝行動應用程式，使得隱私通知無法發揮其告知使用者的功能。再者，隱私通知通常不會解釋為何業者需要特定的個人資料，亦讓使用者在資訊不充足的情況下，無法理性地判斷行動應用程式蒐集個人資料的行為是否合理，而無法有效的保護其個人資料，因此，使用者雖然介意行動應用程式業者蒐集其個人資料，惟因為隱私通知的閱讀門檻提高，使用者難以了解隱私通知的內容，因而不讀隱私通知。

歸納量化研究分析可得出一個共通的問題：現行的通知和同意機制究竟出現什麼問題？為何通知和同意機制未能發揮「揭露業者隱私操作的資訊」的功能？為何使用者難以憑藉隱私通知的幫助，自行判斷安裝行動應用程式後，個人隱私是否會受侵害之風險？從前述的分析似乎可以發現主要的問題出在：不是人人都看得懂隱私聲明，隱私聲明的呈現方式有改進的必要。其次，如何舒緩業者和使用者間的資訊落差和磋商地位，亦是另一大課題。本文將在第五章「行動隱私下通知和同意（notice-and-consent）機制的落實與挑戰」進行更深入的分析與探討。

五、　行動隱私下通知和同意（notice-and-consent）機制的落實與挑戰

從外國立法例觀察，歐盟和美國在處理隱私議題上，雖採取不同的管制手段，然而在面對行動隱私議題時，皆採取加強透明公開原則、提升通知和同意（notice-and-consent）機制實踐的解決途徑。在國際層次上，從 GPEN 的「網路隱私搜查」結果可知，行動應用程式提供隱私聲明的比例偏低，且縱使有提供隱私聲明，也有多重疑慮而未能達到揭露、資訊透明的效果（例如未提供相關資訊或難以閱讀）。回到國內層次，從第四章的問卷量化結果，也反映出隱私聲明有本質上的弊病與問題，因為隱私聲明的呈現方式不佳，以及使用者和業者間資訊不對等，因此導致使用者不讀隱私聲明或看不懂隱私聲明的結果。因此本文以為，如果要改善行動應用程式隱私的保護，首要關鍵應從改善通知和同意機制著手。

通知和同意機制乃為公開透明原則（Openness Principle）的實踐，其成為最具主導性的隱私保護手段[230]，原因在於通知和同意機制的背後，有兩大思想基礎：其一，隱私權是控制自我資訊的權利，由使用者自行決定是否同意，實為資訊自主、資訊自決的體現[231]。其二，由於業者和使用者之間存有一對價關係，業者提供應用程式，使用者提供個人資料，因此從市場效率的角度出發，理性且自主的使用者在不受第三者干擾之下，應可做出對於自身最適切、有利的決定，而此一個別決定所集合而成的整體分布狀況，可使市場運作與資源分配達到最有效率的地步[232]。換言之，由業者提供資訊透明的環境，讓使用者得以對自身資料如何保護做出最適當的選擇，展現出對自我隱私的控制與體現個人自主的意識[233]。至於貫徹通知和同意機制最常見的方式，則為隱私聲明。通知和同意機制雖有以上理論背景與理想支持，然其運作實務發展至今，效能低落與無效率的問題卻越來越明顯。

5.1　通知和同意機制的困境與挑戰

通知和同意機制長期成為各國隱私權法的核心，其賦予業者告知使用者特定涉及隱私事項的義務，提供當事人對其個人資料有知悉、接近和同意的權利。同時，使用者的同意，也讓業者在蒐集、使用和揭露該當事人之個人資料時，具有正當性基礎。因此，通知和同意機制似乎是一個相當中立且公平的立法政策與管制方式。然而本機制有效運作的前提，必須建立在使用者全盤了解隱私聲明內容，並得以做出理性、對自己最有利決策的背景之上。惟此機制經過多年實踐至今，

230　*Supra* note 147, at 1881.
231　*See* ALAN WESTIN, PRIVACY AND FREEDOM (1967); *see also* DANIEL SOLOVE, *supra* note 71, at 42-45.
232　*Supra* note 189, at 34.
233　*See* Charles Fried, *Privacy*, 77 YALE L. J. 475, 483 (1968).

由於業者的實際權力和影響力越來越大，處理個人資料的電腦化技術也不斷推陳出新，較之以往越發有效迅速而徹底，使用者對科技的了解和掌握，不一定能跟得上技術的發展步調。因而業者與使用者之間的資訊落差與權力不對等，原先通知和同意機制所蘊含的公平與中立已逐漸崩壞與失衡。

難題一：詰屈聱牙的隱私權政策

隱私聲明作為通知的方式之一，其內容多半猶如老太婆的裹腳布又臭又長。用字抽象、過於法律性不說，其中還有相當多科技術語，需要使用者耐著性子、花時間去閱讀，並需要較高教育水平才得以理解[234]。以 Google 隱私權政策繁體中文版為例，總共 4357 個字，雖然 Google 稱「我們盡可能地以簡單易懂的文字表達」，但許多用字遣詞還是會讓使用者閱讀時產生疑惑。例如：「裝置資訊我們會收集裝置專屬資訊 (例如您的硬體型號、作業系統版本、裝置的唯一識別碼，以及電話號碼等行動網路資訊)。Google 會將您的裝置識別碼或電話號碼與您的『Google 帳戶』建立連結。」[235]。雖然 Google 提供關鍵詞語的說明，但也只有解釋個人資訊、Google 帳戶、Cookie、匿名識別字、IP 位址、伺服器記錄、敏感個人資訊、非個人身分識別資訊、像素標記等詞語，並沒有提供「硬體型號、作業系統版本、裝置的唯一識別碼」這三個詞的解釋。此外，為何裝置識別碼或電話號碼與您的「Google 帳戶」須做連結，連結後會帶來怎樣的效果或影響？雖然乍看之下，隱私權政策裡每個字詞都看得懂，然而如果再細想一下，一般的使用者是否真能看得懂？所用詞語是否明確？正如同聯邦交易委員會主任委員 Jon Leibowitz 在一次演講指出：「隱私權政策看起來是個好點子，但實務上來看……消費者不會去注意、閱讀或了解隱私權政策」[236]。事實上，使用者不僅經常不讀隱私權政策、不瞭解隱私權政策的內容；即便他們想讀，也的確讀了，但是隱私權政策若如天書般難以看懂，也往往讓他們選擇放棄[237]。

此外，業者時常調整隱私聲明，這也讓使用者十分困擾，即便業者在更改實有通知時有通知使用者，然而使用者一般而言難以理解變更的內容、原因以及影響[238]。再者，使用者在閱讀隱私聲明時還有語言障礙，許多外國行動應用程式業

234 *See supra* note 147, at 1883-86; *supra* note 189, at 35; Jeff Sovern, *Opting in, Opting Out, or No Options at All: the Fight for Control of Personal Information*, 74 WASH . L. REV. 1033 (1999). 另可參考本文第 4.3.2.3 節關於「閱讀隱私聲明和使用者年齡間的關聯性」之討論。

235 參見主要條款，Google，https://www.google.com.tw/intl/zh-TW/policies/privacy/key-terms/（最後瀏覽日期：2013 年 4 月 23 日）；隱私權政策，Google，https://www.google.com.tw/intl/zh-TW/policies/privacy/（最後瀏覽日期：2013 年 4 月 23 日）。

236 "Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies.", Jon Leibowitz, Comm'r, Fed. Trade Comm'n, So Private, So Public: Individuals, The Internet & The Paradox Of Behavioral Marketing, Remarks at the FTC Town Hall Meeting on "Ehavioral Advertising: Tracking, Targeting & Technology" (Nov. 1, 2007), at 4, *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf (last visited Nov. 29, 2013).

237 *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Dosclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 333-334 (2013).

238 *See supra* note 189, at 36; *Google Privacy Policy: Main Findings And Recommendations*, EU, https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/oct

者雖然提供隱私聲明，但所用語言為英文或日文，對我國使用者而言是另一大障礙。縱然部分行動應用程式的隱私聲明已經翻譯成中文，然而隱私聲明的內容不一定和原文版的隱私聲明內容完全一致，因此額外衍生隱私聲明的差別待遇[239]。

難題二：使用者的隱私矛盾

隱私聲明的詰屈聱牙，使用者閱讀隱私聲明的意願大幅降低，進而導致很多人不會選擇退出業者蒐集、使用或揭露其個人資料[240]。這代表使用者不在乎自己的隱私嗎？其實不然。從研究資料和量化研究的圖表十八來看，使用者其實很在乎個人資料的保護[241]，只是使用者可能不知道該怎麼保護隱私，或者是使用者寧願相信業者提供的隱私設定或保護，而同意分享資料在應用程式平台上[242]。這個隱私矛盾，使通知和同意機制未能發揮預期的功用。換言之，使用者實際上並沒有接收和了解告知的內容，未能有效評估在同意後所帶來的利弊得失，因此其所作成的同意決定並非理性考慮之下的結果[243]。

難題三：涉及多方業者

在資訊時代下，涉及處理個人資料的業者太多，以行動應用程式領域為例，總共有四大類的業者：行動應用程式開發商、平台業者、設備業者以及第三方業者，每一個種類的業者都有無數的個別業者，每一個別業者都會蒐集、使用和揭露使用者各種種類的個人資料。因此，使用者其實不能控制和掌握究竟有多少業者正在處理、保有其個人資料。再來，即便每個業者均提供使用者看得懂的隱私聲明，然而由於參與應用程式服務的業者太多，業者提供的隱私聲明也多，使用者仍然無法一一看完，同意和通知機制也無法有效落實[244]。

難題四：個人資料聚合之後的弊病

即便同意和通知機制有效落實，使用者在充分告知下做出理性的決定，然而這並不保證使用者的隱私受到完整的保護。以應用程式為例，一個應用程式會蒐集很多個人資料，例如位置資訊、帳戶等，雖非我國個資法第 6 條所規定的敏感性資訊，然而這些中性的資料經過匯集或分析後，仍然可能顯示當事人的敏感資

ubre/Recommendations_Google_EN.pdf (last visited April 22, 2013).

239 *See* Blasé Ur, Manya Sleeper, Lorrie Faith Cranor, *{Privacy, Privacidad, „Foreign Language>>} Policies in Social Media: Providing Translated Privacy Notice*, 9 I/S: J.L. & POL'Y FOR INFO. SOC'Y 201 (2013).

240 *See* Eric Goldman, *The Privacy Hoax*, FORBES.COM (Oct. 14, 2002), http://www.forbes.com/forbes/2002/1014/042.html (last visited Nov. 29, 2013).

241 *See* Chris Jay Hoofnagle, et al., *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*, SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 (last visited April 23, 2013).

242 *See* Alessandro Acquisti and Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf (last visited April 23, 2013).

243 *See supra* note 97, at 104-05.

244 *See supra* note 147, at 1888-89.

料[245]，甚至可以掌握當事人長期的行動軌跡[246]。換言之，使用者難以預見可能招致的隱私侵害，而在下載應用程式前評估隱私風險[247]。

難題五：業者和使用者的實力落差

使用者和業者間處於不平等的權力地位，既無力更改隱私權條款，也無法和業者進行條款磋商，完全沒有議價能力和談判空間。鑒於業者多半提供「全盤接受，不然就不要用（take it or leave it）」的兩種選項，因此使用者多半屈服於業者免費或低價提供應用程式的優惠，而表示同意。這產生一個疑問，當事人在當前現實環境中，是否真能自由、自主地選擇是否行使同意權？這也成為通知和同意機制的終極挑戰。

難題六：行動裝置的硬體侷限

在第二章「行動裝置簡介」中，本文介紹行動裝置有二個主要限制：小型螢幕和只能手滑，沒有滑鼠和鍵盤。從第三章歐盟、美國和 GPEN 提出的意見書和報告觀察，可發現此二限制嚴重影響行動應用程式呈現隱私聲明的方式。如果行動應用程式的隱私聲明，仍沿用電腦網頁瀏覽的呈現模式，例如字小而多、篇幅過長等，會減少隱私聲明的可讀性。此外，如果行動應用程式業者，以張貼網址連結的方式，提供使用者閱讀隱私聲明，又或者提供隱私設定讓使用者自行調整，則若連結和設定難以透過指尖輕鬆操作，一樣會降低隱私保護和揭露的效力。

前述六個難題，基本上是站在使用者的角度，檢驗通知和同意機制的運作現況。然而不禁要問：為何隱私聲明無法有效發揮透明化的作用？在市場機制下，使用者有隱私保護的需求，為何業者仍無法很好地回應？既然業者握有最多資訊，為何業者無法揭露隱私操作的內容？為何無法陳明使用者可能面臨到隱私風險？面對這些問題，如果直接以「業者為自己牟利最大化作為考量，因此犧牲使用者的隱私」作為上述問題的回答，恐有過於速斷之虞。

首先，「難題一：詰屈聱牙的隱私權政策」、「難題二：使用者的隱私矛盾」、「難題三：涉及多方業者」和「難題六：行動裝置的硬體侷限」其實是一體的問題，因為冗長或過於專業、不方便以行動裝置閱讀的隱私聲明，造成隱私聲明可讀性降低。隱私聲明雖然在法律上不具有拘束力[248]，惟從前述歐盟和美國對業者進行

---

245 例如臉書的按讚，根據劍橋大學與微軟研究人員共同合作一項研究，從使用者按讚的內容，可以分析出使用者的性向、種族、政治傾向、宗教信仰。臉書按個讚，性向、智商全曝光，天下雜誌，http://www.cw.com.tw/article/article.action?id=5047757（最後瀏覽日期：2013 年 4 月 23 日）；Robert Lee Hotz, *When 'Likes' Can Shed Light*, THE WALL STREET JOURNAL (March 11, 2013, 7:25 PM), http://online.wsj.com/article/SB10001424127887324096404578354533010958940.html?mod=WSJ_Tech_LEFTTopNews (last visited Nov. 29, 2013).

246 司法院大法官第 603 號解釋林子儀大法官協同意見書第 60 頁。

247 *See* Nicole A. Ozer, *supra* note 97, at 228-230.

248 *See* In Re Northwest Airlines Privacy Litigation, 2004 WL 1278459 (D. Minn. 2004), *available at* http://www.steptoe.com/assets/attachments/488.pdf; Dwyer v. American Express Co., 652 N.E.2d 1351 (1995).

隱私保護審查的案件可以知悉，隱私聲明是最先、最關鍵的審查標的，也是業者受行政處罰的依據。試想，業者何必擬定隱私聲明讓主管機關有審查的機會，搬石頭來砸自己的腳？又即便不具拘束力，隱私聲明也是使用者在隱私爭訟時，得作為事實陳述的根據，對業者亦為不利。甚者，在行動應用程式產業中，開發業者通常是個體戶或小型公司，要自行擬定一份好讀又合乎法規、隱私保護的隱私聲明，難謂易事。

再者，關於「難題四：個人資料聚合之後的弊病」，看似中性的資料，經過聚合後，究竟將帶來使用者何種隱私風險，未必是業者事前得預見和知悉。科技發展快速下，資料分析技術的革新導致部分中性的資料、甚或是不具識別性的個人資料，經過排列組合而得以特定當事人。舉例而言，美國傳統實務見解認為部分的郵遞區號（zip code，例如完整的郵遞區號有五碼，業者僅蒐集前三碼）不該當可資識別的個人資料，因為郵遞區號僅能特定當事人所在區域，不能識別出特定當事人。然而，近來有越來越多州法院[249]認為，即便是部分的郵遞區號，經過資料分析比對後，有相當高比例能特定出當事人，因此郵遞區號為可資識別的個人資料。此外，誠如第 2.4 節的分析，重新識別技術的快速沿革，同樣導致即便業者已經透過去識別性或匿名的方式將個人資料轉化為單純的資料，卻因為重新識別技術而破解、還原個人資料的識別性，因而導致個人資料認定產生識別風險（risk-identification）。因此，假使業者已對所蒐集的資料或個人資料，為符合當時最佳隱私保護技術的處理時，聚合後所致的隱私風險如完全由業者承擔，似不恰當。

基於上述使用者面對的困境，以及業者的難題，究竟通知和同意機制應如何調整或進化，以改善業者和使用者間的隱私保護衝突和矛盾，是本章所欲探討的對象。在討論解決方案前，先就我國的通知和同意機制進行討論。

5.2 我國的通知和同意機制

司法院大法官第 603 號解釋揭示：「就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之利用有知悉與控制權及資料記載錯誤之更正權」。另外許宗力大法官和曾有田大法官在協同意見書中，亦表示：「惟有使人民事先知悉其個人資料所以被蒐集之目的，並使國家之資訊使用受蒐集目的所拘束，方能正當化國家之取得人民個人資訊，並防止國家濫用所取得之人民個人資訊，而憲法對人民資訊隱私權之保障才不會落空[250]。」綜言之，實踐本號解釋所揭櫫的個人資料自主權之保護，即確保個人在充分告知、了解個人資料蒐集的目的後，得自由任意的做出選擇或表示同意，以實現人民的資訊自決權，此即通知和同意機制的具體內涵。

---

249 *See* Tyler v. Michaels Stores, Inc., Civ. No. 11-10920-WGY (D. Mass. Jan. 6, 2012); Pineda v. Williams-Sonoma, 51 CAL. 4TH 524, 246 P.3D 612, 120 CAL. RPTR. 3D 531 (Cal. Feb. 10, 2011). *See* also Angelique Carson, *ZIP Codes: Are Courts Set To Protect Consumers from Marketing?*, IAPP (May 1, 2013), https://www.privacyassociation.org/publications/2013_05_01_zip_codes_are_courts_set_to_protect_consumers_from_marketing.

250 司法院大法官第 603 號解釋許宗力大法官和曾有田大法官協同意見書，第 75-76 頁。

我國個人資料保護法有關於非公務機關之告知與同意的定義與基本要求，分別規定於第 7 條（書面同意之內涵）、第 8 條（直接蒐集個人資料之告知義務）、第 19 條（非公務機關蒐集或處理個人資料之要件）和第 20 條（非公務機關利用個人資料之除外情形）之中。

5.2.1 告知義務

告知的方式依照個資法施行細則第 16 條的規定，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。依據個資法第 8 條，告知的內容包含：（1）非公務機關的名稱；（2）蒐集的目的；（3）個人資料的類別[251]；（4）個人資料利用的期間、地區、對象及方式；以及（5）當事人依第三條規定得行使之權利及方式[252]。在直接蒐集的情況下，非公務機關須告知當事人得自由選擇是否提供個人資料，以及當事人若不提供個人資料時，將會有何種權益的影響。至於告知的時點，因直接蒐集和間接蒐集之不同有所差異；在直接蒐集的情況下，業者應於「蒐集時」告知法定事項。而在間接蒐集的情況下，業者應於「處理及利用前」向當事人告知個人資料的來源，以及第 8 條第一項第一款至第五款所列法定告知事項。在特定情況下，假如非公務機關有法定可免為告知之情由，則可免除告知義務，不為通知（參個人資料保護法第 8 條和第 9 條）。

告知有二個功能：首先，提供足夠的資訊，使當事人得以預先知悉個人資料如果受到蒐集、處理或利用後，可能遇到的隱私風險，對業者的行為得以產生隱私保護的期待；其次，確定當事人同意的範圍，當事人僅需針對已受告知的部分，表示同意。惟在部分特別情形下，或已有法律規定，或當事人已明知，履行第一項告知義務恐有礙職務之執行或無必要[253]，因此得於特定情況下免除業者的告知義務的部分，在直接向當事人蒐集時，依照個資法第 8 條第二項規定，共有五種例外情形業者可免為告知，包含「一、依法律規定得免告知；二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要；三、告知將妨害公務機關執行法定職務；四、告知將妨害第三人之重大利益；以及五、當事人明知應告知之內容。」。在間接向當事人蒐集時，依照同法第 9 條第二項規定，除前述五種情況外，還有四種額外情形業者可以免除告知義務，包括「一、當事人自行公開或其他已合法公開之個人資料；二、不能向當事人或其法定代理人為告知；三、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限；四、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。」。由於告知義務的免除，連帶影響

---

251 法務部，個人資料保護法之特定目的及個人資料之類別，http://mojlaw.moj.gov.tw/LawContentDetails.aspx?id=FL010631（最後瀏覽時間：2013 年 4 月 20 日）。有論者認為在個人資料保護法修正後，適用主體已不再限於公務機關，非公務機關由於處理的業務不同，個人資料類別應保有彈性和抽象性，以便精確反映個案的蒐集目的和個人資料項目，毋庸延續舊法時代共同指定特定目的及資料類別的作法，有檢討之必要。參見劉定基，前揭註 76，頁 159。

252 個資法第三條規定的當事人權利包括：（1）查詢或閱覽權；（2）請求製給複本權；（3）補正或更正權；（4）停止蒐集、處理或利用權；以及（5）刪除權。

253 個資法第八條的立法理由。

到使用者的同意權以及個資法賦予之權利行使，因此對於告知義務免除有以下二點值得討論。

首先，個資法第 8 條第二項第四款「告知將妨害第三人之重大利益」，惟立法理由並未如第 8 條第二項第一款至第三款等免除告知事由，舉例說明免除的理由。由於免除告知義務即剝奪當事人「知」的權利，而實際上亦難以想像何等情況，會因為告知的行為而危及第三人的重大利益；亦不明瞭所謂的「重大利益」所謂何物？資料蒐集者如以此款作為免除告知的理由，應證明所受侵害的利益為何，是否達到重大的程度；同時，中央目的事業主管機關亦應嚴格審查此款，與當事人的隱私做權衡比較，確保資料蒐集者無濫用或誤用本款之免除事由[254]。

延伸而論，除了重大利益此一法律不明確概念外，公共利益亦為個資法中，例外規定常見的事由，諸如個資法中第 9 條第二項第五款「大眾傳播業者基於新聞報導之公益目的而蒐集個人資料」得免除告知義務、第 19 條第一項第六款非公務機關得「與公共利益有關」下蒐集和處理當事人的個人資料、以及第 20 條非公務機關得「為增進公共利益」下得於特定目的外利用當事人的個人資料，這些例外條款的構成要件「公共利益」，均屬高度不確定的法律概念。第 9 條之公益目的涉及新聞自由與言論自由，與本文所欲探討之行動應用程式較無關聯，暫且不論。然而第 19 條與第 20 條所涉及的公共利益，於此處有討論之必要。

公共利益條款涉及法律明確性原則與授權明確性原則，劉靜怡教授認為此公益目的須考量二個重點：首先，從比較法制中，由法院透過司法案例建立公益目的的判斷原則，並在個案的隱私利益與公共利益間衡量與權衡；其次，由於個資法採取「多頭馬車」的執法模式，由各中央目的事業主管機關針對管轄事業為行政檢查，則在公共利益的判斷上，不免會產生不一致或矛盾的界定和判斷[255]。此外，立法院三讀通過個資法時，中國國民黨黨團和民主進步黨黨團提出相同之附帶決議：「有關本法之不確定法律概念，例如公共利益，一般可得知資料來源，顯有更值得保護之重大利益，公開場所或公開活動等，由政府機關邀請民間團體、學者專家等共同研議於施行細則中確定，避免個人隱私保護與資料運用之社會利益衝突[256]。」惟於現行個資法施行細則中，並未有關於公共利益的判斷標準之相關規定，未能解決立法過程中，立法者對公共利益此一不確定法律概念可能招致爭議之憂慮[257]。

綜言之無論是「重大利益」亦或是「公共利益」，此等概念外延不明確且難以確認，在實務審查上恐須高度仰賴個案判斷。如此在不同個案之間，不僅無法形成清楚明確而可通盤適用的一般性認定標準，在個案解釋適用時亦可能遭逢缺乏可資參照之實體基準，因而不易作出合理認定之現實困境。

254 參見劉定基，前揭註 97，頁 161。

255 劉靜怡，前揭註 44，頁 156-62（2010）。

256 「有關本法之不確定法律概念，例如公共利益，一般可得知資料來源，顯有更值得保護之重大利益，公開場所或公開活動等，由政府機關邀請民間團體、學者專家等共同研議於施行細則中確定，避免個人隱私保護與資料運用之社會利益衝突」，立法院公報，99 卷 29 期 3794 號一冊，頁 168，http://lis.ly.gov.tw/lgcgi/lypdftxt?09902901;0159;0168（最後瀏覽時間：2014 年 1 月 9 日）。

257 劉靜怡，前揭註 44，頁 156（2010）。

其次，關於個資法第 8 條第二項第五款，在當事人明知應告知之內容時，蒐集者得免除告知之義務。立法理由係認為既然當事人已明瞭蒐集者的告知事項，自無必要重複告知，節省蒐集者之告知成本。然而立法理由係假定當事人全盤了解告知內容，然而有時候可能會發生當事人僅能掌握部分告知內容，對其他部分不知情的情況。例如使用者在下載行動應用程式前，可能僅得知行動應用程式業者會蒐集哪幾種個人資料，然而不一定了解業者會如何處理、利用或保存其個人資料。因此有論者以為，此例外應限縮於當事人實際知悉、可預見的告知內容；針對未能知悉、預見的部分，蒐集者仍應履行告知義務[258]。

5.2.2 當事人的同意

非公務機關對一般個人資料的蒐集或處理以及利用，應有特定目的，並須符合個資法第 19 條和第 20 條所列的特定法定事由之一者，方得合法的蒐集、處理或利用當事人的個人資料，因此當事人的同意固然重要，仍僅為可能事由，而並非合法蒐集、處理或利用個人資料的唯一要件。關於同意的時點，從個資法第 7 條第一項的法條用語可得知，當事人僅得為事前之允許，而不可為事後的承認。此外，當事人有效的同意僅表示當事人同意業者在特定目的內，得以蒐集、處理或利用其個人資料，而非免除業者在個資法中所須負擔的義務與責任。

關於當事人表示同意的方式，依據個資法第 7 條第一項和施行細則第 14 條的規定，當事人經蒐集者告知個資法應告知事項後，所為允許應以書面，或依電子簽章法第 4 條第二項規定，以電子文件為之[259]。換言之，當事人僅得以書面方式表示同意，不得以口頭、或默示不作為表示同意。雖然書面同意是較為嚴謹的表示方式[260]，惟不免過於僵化，無法因應不同的情況、場合而做調整[261]。舉例而言，飯店在房客報到時告知當日下午茶時間，飯店的咖啡廳會安排專人攝影，將從作品中挑選照片作為廣告之用。如果房客願意被拍攝，則歡迎房客參與此活動；若不願意被拍攝，則飯店另行安排房客到另一個餐廳用餐。假使房客在下午時分至咖啡廳用餐，縱然房客並沒有以書面的形式表達同意，然房客的行動即可推論其同意接受飯店的拍攝[262]。因此，本文以為認定「當事人的同意」是否有效，不應該只單純審查表示同意的「形式」，而應從同意的「實質內涵」加以判斷，例如在充分告知後方得為同意[263]。因為我國就同意的實質要件，並沒有明確的規範會實務見解，因此本文參酌歐盟對同意的要件或標準進行分析和闡述。

歐盟個人資料保護指令第 29 條工作小組的意見書，認為同意有四項要件[264]。首先，當事人應自由地作出同意，亦即須當事人的同意須具有任意性，不受詐欺、

---

258 劉定基，前揭註 76，頁 161-62；資訊工業策進會科技法律研究所，「個資保護 1.0」，頁 72（2013）。

259 參考呂丁旺，淺析修正「個人資料保護法」，月旦法學雜誌第 183 期，頁 135-36（2010）。

260 參考翁清坤，前揭註 114，頁 74-75（2013）。

261 參考劉定基，前揭註 138，頁 151-53（2013）。

262 Opinion 15/2011 on the Definition of Consent at 23, 2011 WP 187 (EC).

263 誠如林子儀大法官在司法院大法官第 603 號解釋所作之協同意見書中表示「蓋資訊隱私權重要的意義之一，在於尊重、保護個人自主選擇的權利，但有意義的選擇須事先獲得充分翔實的資訊。」，司法院大法官第 603 號解釋林子儀大法官協同意見書，頁 65。

264 其實歐盟個人資料保護指令第 29 條工作小組的意見書中，同意應該有五項要件，包含得以任何形式表示及表明同意，惟此項要件與我國個人資料保護法之規定不符，因此僅闡述其餘的四項要件。

脅迫或承受任何不利的情況下作出同意，且當事人亦可毫無顧慮地撤銷同意[265]。其次，須為具體、特定的同意，意即業者以好懂、清晰的詞語，準確地言明業者將蒐集、處理或利用當事人個人資料的範圍與結果，讓當事人對業者的行為有合理的期待，並依此特定範圍表示同意。換言之，同意必須有具體的相對性，同意不可涵蓋資料控制者「任何合法目的」，而應確切地指涉某一具體、明確的目的，進而為必要且合理的資料處理[266]。

其三，告知後的同意，第 29 條工作小組認為須符合二種要求：（1）資訊的品質，業者提供蒐集、處理或利用等資訊的方式，必須以通俗的文字、不使用術語、以及易懂且清晰的言語，以當事人可理解的方式表達；（2）資訊的近用性和可見性，該資訊直接提供與當事人，且須以顯眼且全面的方式提供，例如以彈出式的對話框、分級式的揭露或者隱私設定選項等，供當事人閱讀[267]。其四，應於蒐集、處理或利用等行為「前」取得當事人的同意，方能充分地保障當事人的權利[268]。惟若資訊控制者行為之特定目的轉變時，亦得於處理資料進行中徵求當事人的同意[269]。

總結本文對我國個資法的通知和同意機制之討論，除了個資法所規定的應告知內容以及書面同意外，本文分別就通知和同意二項義務提出建議。首先，告知的部分，建議盡量限縮免除告知義務的範圍，就公共利益等抽象名詞以增訂施行細則或行政函令等方式使之明確。另一方面，同意的有效與否，先決條件是應先充分、以可閱讀的方式告知當事人，在使當事人在自由、任意地情況下，表明同意。同意的方面，應著重於同意的實質內涵，判斷當事人的同意是否具備「任意性」、「具體明確」、以及「已先為告知」等實質內涵。此外，本文認為，假若當事人的同意已具備實質內涵，縱然未以書面方式表達同意，或可認為當事人已同意業者為合法的蒐集、處理或利用其個資。換言之，個資法似乎可就同意為要式規定進行鬆綁。

5.3 通知和同意機制的調整與修正

長久以來，隱私法或個人資料保護法過度依賴通知和同意機制，然而即便業者符合我國個資法的規範，此機制在實踐上卻遇到前述多種問題，而無法達成預想的目標。面對此一困境，本文認為可分成二個階段對本機制進行修正：在第一階段，先改善當前的問題，調整揭露的方式；在第二階段，透過業者的隱私聲明呈現方式，改善業者和使用者間的資訊落差，確保使用者知的權利；在第三階段，藉由喚起使用者的隱私自覺，成為業者實踐隱私保護的壓力與動力。

265 *Supra* note 262, at 12.
266 *Id.* at 17-18.
267 *Id.* at 20.
268 *Id.* at 9.
269 *Id.* at 34.

第一階段：改善現況

有論者認為，將部分業者採取的選擇退出（opt-out）機制，轉為選擇加入（opt-in）機制，並且即時提供告知與加入選項，讓使用者有權決定同意與否。一方面相較於選擇退出機制，選擇加入機制更為貼近使用者的偏好；另一方面也可減少交易成本，提高效率[270]。在一般網路中，選擇加入機制已相當普遍，然而在行動應用程式仍有相當程度未採取選擇加入機制模式，或者業者雖採取選擇加入機制，卻因為隱私設定不甚明顯，讓使用者不易察覺或不知情，而未能變更、調整隱私設定。因此，本文就選擇加入機制的強化，提出二項建議。

首先或可採取依照使用者選擇加入的程度，決定應用程式提供服務功能的範圍。以導航應用程式為例，現在多直接開啟定位系統，蒐集使用者所在位置，以便規劃使用者前往目的地的路線。若使用者不想被定位，須自行變更系統設定。然而，一般使用者並不知道定位系統已經開啟，或是不知道如何變更隱私設定。因此若調整為選擇加入機制，使用者一開始即知悉應用程式會蒐集位置資訊，若使用者一開始未同意開啟定位並讓應用程式知悉其位置，則應用程式只能提供一般地圖查詢與路線規劃功能，無法進行定位，亦無法提供導航功能。此設計可讓使用者免於陷入「全盤接受，不然就不要用（take it or leave it）」的困境，而能更自由地行使其同意權。

其次，在下載、開啟行動應用程式時，或許可先顯示隱私設定的頁面[271]。雖然許多應用程式都有隱私設定的頁面，然而使用者不一定知悉，因而即使業者採取選擇加入機制，亦因為使用者不知道隱私設定的位置，而形同虛設。本文以為此為業者和使用者雙贏的措施，讓使用者得以在使用應用程式前，先行操作、設定隱私選項，或許更能強化對使用者的通知與隱私保護。另一方面，業者亦可從中增加蒐集使用者個資的機會和正當性，例如照相應用程式軟體可於隱私設定詢問是否可蒐集位置資訊，如使用者選擇「開啟」，業者即得蒐集位置資訊（當然，如果業者可附帶告知蒐集位置資訊的原因，會更加完善）。此外，業者也得因此減輕隱私風險的負擔，因為相關隱私設定已為使用者所知悉，如此方能貫徹選擇加入機制。

然而上述兩種措施，仍存在著通知和同意機制的問題，使用者如果真的無法了解隱私聲明的內涵，選擇進入或選擇退出對於使用者而言即無太大差異。此外，業者還是可以用迂迴曲折的語句和詞彙，或是運用資訊、權力不對等的優勢，讓使用者選擇進入並且同意業者處理個人資料。

---

270 *See* Jeff Sovern, *supra* note 234, at 1072-94, 1101-15 (1999).

271 筆者在操作行動應用程式時，發現某些較具規模的行動應用程式業者，在首次開啟行動應用程事時，會先顯示該應用程式的隱私聲明，這是通知和同意機制的進步。因此如能在呈現隱私聲明後，進一步顯示隱私設定的頁面，供使用者操作和調整，對使用者的隱私保護可更趨完整。

第二階段：改善資訊落差

本文以為，造成通知和同意機制運作失靈的癥結點，在於使用者和應用程式業者之間的資訊落差。Helen Nisssembaum 教授將隱私法中的通知和同意機制，和醫療照護系統下的通知和同意機制加以比較，探究為何同樣存在資訊落差，醫療照護體系下的通知和同意機制卻運作得比較好？依其研究，原因在於醫療照護體系裡有許多其他的輔助機制足以維繫外科手術的品質，並且確保對於已知的風險事前據實告知。無論是醫師的專業知識與長期執業經驗，醫師執照對於醫術的保證，醫療界的同儕監督，以及醫師及醫療機構欠缺對於病患福祉及健康不利的誘因等，都能讓病患對其抱持希望與信心[272]。而在動手術之前，醫生會以告知書詳細陳述病患開刀的風險與成效，病患得以依據成功機率以及復原程度來評估是否要動刀。即便醫生陳述的醫療術語或治療細節並非一般民眾得以馬上理解，由於事關病患之生命與健康，病患也會主動自行查詢並了解相關資訊。如果病患原本醫生的評估有所疑慮，也可能轉請另一位醫生再次進行檢查與診斷，以確實瞭解其所面臨的醫療風險。由此看來，病患願意投注於醫療風險資訊上的時間與成本，也比行動隱私要高出得多，這也有助於舒緩原本存在於醫師與病患之間的資訊不對等。

然而回頭來看行動隱私的通知和同意機制，最大的困境即在於業者和使用者間並未存在相同的輔助確保機制，能讓使用者相信業者在隱私保護方面的專業與全心關注，以及業者確實會落實執行其所聲稱的隱私保護措施。此外，行動應用程式有時無法說換就換，這也是業者與使用者之間權力不對等的另一來源。例如手機購買之後，無法變更作業系統；而對於具有群聚使用特性的行動應用程式，譬如親朋好友都使用某一社交或訊息軟體，當事人很難因其隱私保護不周而轉換使用另一同類型軟體。再者，當事人對於隱私權，往往未能投入與生命、身體或健康權同等的關心與注意，因此在資訊取得及消弭資訊不對等的努力上，與前述的手術醫療情境有明顯的落差。

針對改善資訊落差，有論者認為可以將隱私聲明作成隱私標示，猶如營養標示等圖示[273]，讓使用者一眼就可以了解內容，以提高透明度，這也是目前美國政府推行的政策方向。本文認為，除了營養標示模式外，或許可以採取成份標示的模式，列出該應用程式蒐集、分享的個人資料項目，以及接收個資的第三方業者種類，讓使用者一目了然。然而，無論採用哪一種通知模式，隱私標示的設計必須符合當地人民對於個人資料處理的心態和意向，此處必須引進社會科學與心理學的實證研究成果與統計數據，以便使隱私標示的運用得以符合使用者與業者間的互動脈絡與模式[274]。隱私標示除了方便使用者一目瞭然外，也方便業者踐行隱

272 *Supra* note 189, at 36. 另參見劉宏恩，「基因研究與人權保護」，基因科技倫理與法律—生物醫學研究的自律、他律與國家規範，頁 258-59（2009）。

273 *Supra* note 189, at 35.

274 *See supra* note 147, at 19; *see also id.* at 43-45.

私保護。尤其應用程式業者多為中小型企業，個人創作者亦在所多有，如能有一完善、統一的隱私標示機制，可方便業者遵循個人資料保護規範，減少執行成本。此外，隱私標示需要政府長期推動，形成各行各業共同的隱私保護制度，以便讓業者和使用者清楚瞭解該標示的意涵，並且有助於確保業者的隱私操作和標籤揭露內容一致。除此之外，本文建議可透過簡要的隱私聲明告知使用者為何業者須蒐集該種個人資料，更能貫徹通知機制。其中，簡要的隱私聲明亦可透過業者公協會的力量，擬定出統一的範本或範例，供個別業者參考或援用，減輕業者提供隱私聲明的壓力和困難度。

第三階段：提升使用者的隱私自覺

從本文量化分析中可得知，使用者不閱讀隱私聲明的原因有二：「隱私聲明難以閱讀外」和「等不及，想趕快使用應用程式」。其中，「隱私聲明難以閱讀外」凸顯業者在揭露隱私聲明的不足，此可藉由業者改變、調整隱私聲明呈現方式和內容（前述二個階段）予以改善、解決。另一方面，「等不及，想趕快使用應用程式」，則顯示出使用者對個人隱私的意識較為遲鈍或較不理性，無法將蒐集個資和個人隱私產生緊密的連結而有所警覺[275]。所謂遲鈍是指，使用者雖然在意自身隱私，也具有隱私意識，但無法在個資可能蒐集、處理或利用時，快速反射出隱私有侵害之虞的想法，進而主張法律所保障的權利和請求；而不理性則是指，使用者可能基於行動應用程式的「免費」或「低價」而降低選擇的理性，忽略了行動應用程式可能招致的隱私風險[276]。無論是遲鈍或不理性，都彰顯了使用者的隱私自覺尚待加強。因此本文以為，提升使用者的隱私自覺，亦是強化使用者隱私自決的重要環節

首先，可藉由學校教育，自小培養學生的隱私意識，例如在小學或國中的課程中，納入隱私與資訊社會的內容，建立校內的行動社群應用程式軟體，讓學生一方面可以實際操作社群軟體；另一方面亦可將行動應用程式軟體所蒐集資料的分析結果告訴學生，讓學生知道個資蒐集後可能帶來的隱私風險與影響。其次，則是從社會著手，藉由新聞媒體或政府的力量，喚起使用者的隱私意識。在科技快速進步、廣泛傳播的現在，越來越多媒體或管道著重於科技技術和產品的報導，有助於縮短業者和使用者間的資訊落差，並喚起使用者的隱私意識和危機感[277]。而當政府對隱私議題表示關心，並積極為行政檢查，審查隱私侵害案件時，亦可以讓社會產生隱私自覺。藉由提升社會的隱私自覺，而可以增加使用者對業者的籌碼，促使業者強化隱私設計和內容。

---

275 參見莊庭瑞，個人資料保護在台灣：誰的事務？，國家政策季刊第二卷第一期，頁 59-60（2003）。

276 *See* Nicole A. Ozer, *supra* note 97, at 226-228.

277 *See* Nicole A. Ozer, *supra* note 97, at 240-242.

在上述三個階段中，中央目的事業主管機關扮演關鍵的角色[278]。我國既於個資法第 22 條至第 27 條規範中央目的事業主管機關之行政檢查事項，則主管機關應積極使用行政檢查的權力，審查並發現業者的隱私侵害行為，而非被動地等到隱私危害已然發生，才予以回應。此外，行政檢查後，就違法業者主管機關應公開行政檢查的完整報告與結果，使其他行動應用程式業者得以預見行政檢查的脈絡與方式，自我檢查、反省自身的隱私設定和個資保護措施。同時，使用者亦得以透過行政檢查報告，了解那些業者的隱私保護措施較佳或較不完善，作為是否下載、使用的依據。

附帶一提，依個資法第 26 條，如檢查結果未發現有違法情事，經徵得被檢查之非公務機關同意，得公布檢查結果。根據本條之立法理由，公布合法業者的檢查結果，似在確保行政檢查之公信力[279]。惟本文以為，公布檢查結果之目的並非維持行政機關的公信力，而係建立行政檢查的慣例，讓業者得以掌握行政機關檢查的方向與內涵。同時，公布檢查結果亦可讓使用者知悉業者在隱私設計與保護的表現，得以作為判斷是否下載應用程式之依據。因此，合法業者就公開檢查結果之同意權可做限縮解釋，僅就檢查結果公開之範圍為同意或拒絕。換言之，原則上應公開行政檢查之報告（審理內容）與結果（合法），僅在業者認為公開檢查報告，可能揭露其營業秘密或招致不利影響時，例外僅公開行政檢查之最終合法結果

甚者，由於行動應用程式業、資訊分析和隱私保護技術的發展一日千里，除了業者隨時要跟上科技的脈動，調整隱私設計和操作外，政府亦應隨時留意技術研發的趨勢，適時公開主管機關的態度和立場，或者召開公聽會或研討會，與產業界就特定新興科技的個資保護方法進行意見交換和討論，並提供相關書面報告供使用者注意，並供業者參考。

最重要也最關鍵的是主管機關揭露行政檢查的標準與立場，開誠布公地告知行政檢查的步驟和衡量標準、要素，使業者得以預見。本文建議主管機關的審查可綜合考量個案的脈絡、隱私保護技術、企業的行為、以及業者製造的隱私風險是否當時業者可得預見，減輕業者所承擔的識別風險，方能在保護使用者隱私和業者利益間取得平衡。

278 *See* Ming-Li Wang, *Information Privacy in a Network Society: Decision Making Amidst Constant Change*, 5 NAT'L TAIWAN U. L. REV. 127, 146 (2010).

279 個資法第 26 條立法理由：「一、本條新增。二、檢查結果雖未發現有違法情事，中央目的事業主管機關或直轄市、縣（市）政府（檢查機關），經徵得被檢查之非公務機關同意，仍得公布檢查結果，以昭公信，爰為本條規定。」

六、 我國個人資料保護法有關行動應用程式之隱私保護

針對行動應用程式下載所導致之個人資料處理，業者應如何適用我國個人資料保護法（以下簡稱個資法）？又我國主管機關應如何因應行動應用程式產業所引發的隱私疑慮，保護我國的使用者個人資料和隱私不受侵害？本文試圖草擬對行動應用程式產業的個資法適用建議，期能達拋磚引玉之效果，喚起各界對行動隱私的重視與關注，強化對行動應用程式使用者的個人資料保護。

6.1 行動應用程式的個資保護

依照個資法第 19 條，直接蒐集、處理或利用使用者個人資料之行動程式產業業者（非公務機關），須遵守我國個人資料保護法的規範，並踐行個資法之法定義務。以下將分別探討應用程式開發商、作業系統商和設備製造商、應用程式商店、以及其他介入個人資料的參與者，在其產業、設備特性下，提供四種行動應用程式產業之業者，應如何適用我國個人資料保護法之建議。

6.1.1. 應用程式開發商

應用程式開發業者係為行動應用程式中，蒐集、處理、利用和傳輸使用者個人資料的核心關鍵。首先，行動應用程式開發商應揭示其身分以及連絡方式，供使用者面臨隱私爭議或問題時，得立即向開發商反映，尋求解決（個資法第 8 條）。其次，行動應用程式建議主動、積極地提供隱私聲明，告知使用者蒐集個人資料的種類、蒐集的目的以及將個人資料傳輸與何種第三方業者（個資法第 8 條）。隱私聲明的形式，必須符合行動裝置的螢幕大小，字體大小和篇幅應方便、友善使用者閱讀。行動應用程式開發商可以產業規模凝聚共識，以統一的規格呈現隱私聲明的方式，例如採取成分標示模式，羅列所有蒐集的個人資料種類；以營養成份模式，勾選所蒐集個人資料種類；或者研發隱私標示，方便使用者閱讀和理解。此外，亦可就說明蒐集個資源因的簡短隱私聲明，藉由行動應用程式產業與中央目的事業主管機關的協商下，擬定隱私聲明的範例或擬稿，供行動應用程式業者參考或引用。

其中，隱私聲明的形式如以隱私權政策呈現，不單純只以超連結連接到網頁版的隱私權政策，而建議設計行動版本的隱私權政策頁面，方能有助於使用者利用行動裝置閱讀隱私權政策，了解應用程式開發商的隱私操作。由於我國通行的文字為中文繁體，為有助於我國使用者閱讀隱私權政策，因此隱私權政策建議以繁體中文呈現。國外的行動應用程式開發商，將外語的隱私權政策或通知，逐字逐句翻譯成繁體中文，不可因為轉換為中文版本，而有內容上的缺漏或省略[280]。最重要的是，隱私權政策能確實、清楚地介紹應用程式開發商實際的隱私操作，開發商更應具體落實其隱私操作。

280 本文以為語言轉換應非難事，線上已有多種語言翻譯轉換的程式可供使用。

應用程式開發商在設計應用程式之初，將使用者的隱私保護納入程式設計中。尤其，開發商應將個人資料保護法第 3 條所規定的當事人權利，設計為隱私設定，供使用者得輕易地接近、修改、客製化其個人資料的期限和內容（個資法第 11 條）。另外建議行動應用程式得於使用者初次開啟行動應用程式時，先顯示出隱私設定頁面，供使用者自行調整與操作，強化選擇進入的模式。

此外，行動應用程式開發商可與行動應用程式商店合作，以簡明、易懂的話語定義個人資料的內容和專有名詞，例如以「問答集」的方式解釋何謂 cookies，業者蒐集 cookies 的目的為何，幫助使用者了解業者的隱私操作和目的。最後，假使有隱私風險和資安漏洞的情況發生，行動應用程式開發商應立即以適當的方式通知主管機關和當事人，並立即補救（個資法第 12 條）。

6.1.2. 作業系統商和設備製造商

作業系統商和設備製造商可透過內建的感應器或追蹤數位程式，蒐集使用者的個人資料，因此應遵守個資法的規範。因此，建議作業系統商和設備製造商在設計或調整產品時，將隱私保護納入產品設計中，提供使用者得自行設定隱私功能。在全新的行動裝置開機啟用時，針對隱私相關的功能設定，例如 GPS 功能開關、系統自動更新等，可從現在讓使用者選擇退出的措施，改為讓使用者選擇進入的方法，以確保使用者對其個資的控制。此外，業者提供使用者解除安裝的功能，讓使用者得以刪除自行下載的行動應用程式和行動裝置預先安裝的行動應用程式。惟行動裝置預先安裝的行動應用程式，可能與行動裝置的運作有密切關聯，業者可以隱私通知的方式，告知使用者假使刪除應用程式可能的後果，由使用者自行決定是否刪除。

6.1.3. 應用程式商店

應用程式商店一方面為蒐集者，因此應用程式商店應遵守我國個資法，告知使用者其蒐集的個人資料種類、目的、處理和利用的方式、以及傳輸與那些第三方業者（個資法第 8 條）。

另一方面，由於應用程式商店類似於零貨商的角色，提供平台讓行動應用程式業者得以申請上架、陳列，因而應用程式商店掌有行動應用程式是否可上架的決定權。因此建議應用程式開發商監督應用程式開發商是否履行隱私保護規範，並作為應用程式開發商和使用者間的平台，提供開發商張貼聯絡方式和隱私聲明的空間，並轉達使用者對應用程式開發商的心得、意見和評價，並提供評分或評價，讓使用者得據此作為下載應用程式與否的參考依據。簡言之，應用程式商店在行動應用程式下載、使用中，扮演舉足輕重的角色。

6.1.4. 其他介入個人資料的參與者

其他介入個人資料的參與者（簡稱第三方業者），包含廣告業者或資料分析產業，雖間接蒐集使者的個人資料，無法直接和使用者接觸，仍應遵守個資法的規範。惟在第三方業者處理、利用和傳輸使用者的個人資料時，仍應讓使用者知悉、了解和接受。因此，第三方業者可透過應用程式開發商，向使用者轉達其隱私通知和隱私操作。同時，應用程式開發商在傳輸使用者個人資料時，代替使用者把關，將個人資料分享給隱私保護程度相當的第三方業者，確保使用者的安全。然而應用程式開發商無法替第三方業者的隱私操作背書，應用程式開發商得將其合作的第三方業者名單公開，讓使用者得自行檢視第三方業者的隱私操作。

6.2 修法政策建議

6.2.1 增加個資法適用主體：納入「協助」蒐集個資的媒介業者

從比較法分析中可發現，歐盟和美國均寄望行動應用程式商店得以扮演守門員的角色，監督行動應用程式開發商是否確實履行隱私保護規範。然而行動應用程式商店是否有監督義務？又應用程式商店並未直接或間接蒐集個資，是否適用個資法？換言之，應用程式商店處於媒介的地位，提供開發業者得蒐集使用者個資的機會，甚或是開發業者蒐集使用個人資料的幫助者，針對應用程式商店的地位，法律應如何規範？從我國個資法的條文中，應用程式商店似乎在個資法規範射程外，不適用個資法。

因此當行動應用程式商店僅單純立於媒介地位時，我國可透過兩種方法要求行動應用程式商店為監督行動應用程式開發商的行為：第一種方法，透過業者自律或市場管制等方式，促使行動應用程式商店扮演好守門員的角色；第二種方式，修訂現行個資法，擴張個資法適用主體，納入「協助」蒐集個資的業者，進而得以管制應用程式商店，規定其監督行動應用程式開發商的義務。

本文以為透過修法方式較為可行，理由如下：首先應用程式商店為大型業者，甚至是掌控行動應用程式市場者，在球員兼裁判的情況下，難以發揮業者自律和市場管制的功能。再者，相對於行動應用程式開發商多為個人或小型業者，應用程式商店的規模，更容易也更較可能接受主管機關的管制或規範。其次，應用程式商店直接或間接地從應用程式中獲取高額利潤，因此賦予應用程式商店監督開發商的責任並未過苛。此外，應用程式商店在踐行監督責任後，其所上架的應用程式符合法定的個資保護要求，可提升應用程式商店和使用者的信任關係，而吸引使用者使用和下載，對應用程式商店有所助益。其三，應用程式商店對於開發商具有相當影響力，應用程式商店可透過上架流程或限制等規定，要求開發商就其應用程式設計加以調整。尤其行動應用程式開發商多為外國機關，我國中央目的事業主管機關難以審查外國開發商是否遵守個資法，如果能透過賦予應用程式商店法定監督義務，而得以間接管制應用程式開發商，不僅更具管制效率且更能

保護我國行動應用程式使用者。最後，納入「協助」蒐集個資的媒介業者，不僅有助於行動應用程式業的隱私管制，在雲端產業或行動支付業等有賴第三方媒介業者協助個資蒐集的產業亦有適用。因此本文建議個資法納入「協助」蒐集個人資料的機關，該等業者除須遵守個資法總則的規範外，更可於分則中要求協助蒐集個資的機關的監督義務，強化行動應用程式商店守門員的角色，進而保護使用者的行動隱私。

6.2.2 中央目的事業主管機關應公開行政檢查的標準與審查報告

就行動應用程式的個人資料保護議題，我國目前缺乏依照行動應用程式產業特性的個人資料保護框架，或是具體之教戰守則。雖然經濟部工業局已經編製「個人資料法規遵循參考指引暨宣導手冊——資服業個資教戰手冊（以下簡稱資服業個資教戰手冊）」，供資訊服務業者作為個資指引，似乎可作為行動應用程式業者的個資管理參考。然而很可惜的是，教戰手冊的內容主要在於介紹個人資料保護法的內容與條文釋義，以及提供個人資料管理機制與管理流程的建議，雖然設有「資訊服務業者應注意事項常見問答」的章節，但內容流於泛泛且過於簡略，多半仍然停留在個資法的法條解釋，並未針對個別產業的特性，提出個人資料保護的框架性建議。例如在這本教戰手冊中，雖然特別針對雲端服務業者提出個資處理的問與答，但僅著重在「個人資料的國際傳輸」，對於雲端資料的儲存或是通知和同意的具體型態等個資保護實務重要問題，均未提出更具體的建議[281]。

從美國與歐盟的意見書或報告可發現，意見書的內容應該針對產業的特性，依據相關法律或原則，提出具體的個人資料保護框架與建議。由於行動應用程式產業有別於一般網路產業，有不同的業者參與，包含製造商、平台業者和開發商，應個別賦予不同的個資保護責任。尤有甚者，智慧型裝置經常同時搭載數個行動應用程式，蒐集使用者多種類型的個人資料，主管機關應該針對此種產業特性，提供具體的建議與個資保護方針。再者，由於行動應用程式開發商多為中小型企業或個人創作者，在使用者個資保護方面欠缺足夠的知識與能力，亟需政府專責單位給予具體可行的詳細指引，以供業者與使用者遵守和參考。最後，主管機關應妥善進行行政監督，中央目的事業各個主管機關應公開其行政檢查的標準，供業者得以預見並行修改，並針對有隱私疑慮的行動應用程式產業業者進行調查，並將審查結果公開，讓使用者得以了解可以信任或不可信賴那些業者。透過審查報告的公開，亦可督促業者提升隱私保護的設計和呈現，可收一石二鳥之效。

總結以上，我國政府首先應就我國行動應用程式使者的隱私意識、決定下載的動機、與同意隱私權政策的內容，接受業者蒐集、利用和揭露個人資料的態度等，進行全面性調查，以確保隱私保護之規範內容與國內使用者交易習慣和使用脈絡兩相符合。其次，應透過編製行動隱私保護意見書之方式，將告知、特定目的和同意等三個法律要件與管制密度，清楚加以闡述，並與行動應用程式的現況加以緊急結合。最後，在政策方向上，應該力求業者隱私通知能夠做到簡明扼要，

281 前揭註 39，頁 26-27。

並且研究發展符合我國民情的隱私標示，教育業者在設計應用程式之初，就將隱私保護機制落實於程式設計之中，同時並教育使用者如何在充滿個資侵害陷阱的行動商務環境之下，應該如何自保。

七、 結論

隨著智慧型裝置的普及，以及行動應用程式產業的蓬勃發展，正如美國國家安全局前雇員 Edward Snowden 所言：「我們的口袋裡裝有各種感應器，我們的行蹤時刻受到追蹤[282]」，人們的生活和智慧型裝置與行動應用程式越來越密切。然而在行動應用程式得以蒐集廣泛且深入的個人資料時，會因為以下二種情況而侵害使用者的隱私。首先，若行動應用程式產業業者未能在使用者下載程式前，以清楚易懂的方式，充分揭露蒐集個人資料的種類、蒐集的目的、以及可能將資料分享給那些第三方業者，則使用者因為不知悉業者的行為，而無法掌控其個人資料的流向，而無法確保自己的隱私。其次，縱然業者以隱私聲明的方式，載列業者的隱私操作和行為，並提供使用者各項隱私保護的保證以及隱私設定，惟若業者的隱私實踐和操作，卻未依照其所揭示的隱私聲明或隱私設定，在此陽奉陰違的情況下，仍然侵害使用者的隱私，且因為欺罔使用者的信任，對使用者隱私的傷害更甚於第一種情況。這二種情況的共通點皆在於因為使用者的不知情，削弱使用者對個人資料的控制力，而危害自身的隱私，而這也是本文所欲探究、解決的議題。

首先本文透過問卷調查以及量化分析，了解我國的行動應用程式使用者對行動應用程式隱私聲明的了解程度，可發現僅有少數的使用者在下載程式前，會閱讀隱私通知；且看懂隱私聲明的比例也偏低。此外，進一步探究為何不閱讀隱私通知或看不懂隱私通知的原因，亦可發現隱私通知的長度和隱私通知的術語艱澀等原因，皆使得閱讀隱私通知的門檻提高。因此本文發現保護行動應用程式使用者的隱私的首要關鍵，應該從改善隱私聲明的運作方式下手。

本文量化的結論，亦和歐盟、美國對行動隱私的討論和所採取的政策相同。從比較法途徑分析可發現，歐盟在個人資料保護指令中，本身就有針對通知義務與同意進行規範，在「對於智慧型設備（smart device）應用程式的意見書」中，則是闡述各行動應用程式業者應如何履行法定義務。另一方面，美國對於行動應用程式產業的隱私保護建議，則偏向透過業者的自律以及產業公會的力量，制定出產業內部的規範和「隱私聲明」的統一型態，例如建立標誌或者圖像，便利使用者得以閱讀此等統一的通知模式，了解業者的隱私實踐。然而無論管制行動隱私的途徑是採取以政府管制為主的歐盟，亦或是以市場機制為主的美國，均可發現為能增加使用者對個人資料的控制與自主權利，皆透過修正現行「通知和同意機制」著手。此外，針對行動應用程式開發商、行動設備製造商、作業系統商、行動應用程式商店、以及第三方業者等，分別提出強化使用者自主控制力或者增

282 史諾登上電視 籲團結抵監控，聯合晚報，http://udn.com/NEWS/WORLD/WOR3/8385635.shtml（最後瀏覽時間：2013 年 12 月 31 日）。

進使用者閱讀隱私聲明程度的解決方式。更甚者，GPEN 的「網路隱私搜查」和第三十五屆國際資料保護與隱私權委員大會的「華沙宣言」，亦認為應從改善現行通知和同意機制下手。

本文根據量化研究以及文獻閱讀，認為現行通知和同意機制的弊病在於以下五點原因：（1）詰屈聱牙的隱私聲明，隱私聲明不僅又長又艱澀，而且有時還有語言不通的問題，導致使用者難以理解隱私聲明的內容；（2）使用者的隱私矛盾，雖然使用者在意自身隱私，但因為無法了解業者的隱私操作，因而不能確實、理性地評估下載應用程式後可能招致的隱私風險；（3）涉及多方業者，由於一個智慧型裝置涉及多方且多種行動應用程式產業業者，難以期待使用者每一次下載或使用應用程式前，能一一閱讀且理性地判斷業者的隱私實踐是否確能保護其隱私；（4）個人資料聚合之後的弊病，使用者可能以為行動應用程式業者所蒐集的資料，都是無關緊要或無傷大雅的個人資料不甚要緊，然而當中性的資料經會交叉分析後，可能會顯示當事人的機密資訊或行為軌跡，造成隱私的侵害；（5）業者和使用者的實力落差，使用者不僅和業者間存在資訊落差，還因為使用者不具有磋商籌碼和談判空間，而無法改變業者的隱私聲明與操作；以及（6）行動裝置的硬體侷限，因為螢幕的大小以及觸控式的操作，限制了隱私聲明的呈現與揭示。

既然問題的根本在於使用者的不知情，則因朝向拉近業者和使用者間的資訊落差的方向解決。本文認為可分成三個階段修正現行的通知和同意機制。在第一階段，先改善當前的問題，調整揭露的方式。首先，盡可能採取選擇加入的模式，提供使用者自行決定應用程式蒐集資料或提供服務的程度；此外，盡可能簡化隱私通知的內容，以淺顯易懂的語言，避免運用術語來解釋、描述業者蒐集個人資料的種類、目的、關聯性以及合作的第三方業者名單。在第二階段，透過改變隱私聲明的揭示方式，根本解決通知和同意機制的問題。在第三階段，則是透過教育、媒體和主管機關積極為行政檢查的力量，喚起使用者的隱私自覺。

最後，針對行動應用程式適用我國個人資料保護法時，面臨到的困難有二：個資法無法規範行動應用程式商店與中央目的事業主管機關不明確。首先，行動應用程式商店如僅為行動應用程式開發商蒐集個人資料的助手時，並不具有個資法之主體適格，不受個資法拘束。然而行動應用程式商店立於個資蒐集的關鍵地位，如未能予以規範，將形成隱私保護的漏洞。因此本文建議透過修法，納入「協助」蒐集個資的媒介業者為適用主體，明文規範其監督義務。

其次，雖得以從產業分類推測行動應用程式的主管機關為經濟部工業局，惟工業局管轄的產業範圍既多且雜，是否真的能有效監督、審查行動應用程式產業的隱私實踐，大有疑問。其次，縱然主管機關明確，然而主管機關如果未能提出完整的審查標準、主動審查違反個人資料保護法的業者、亦或是將審查報告公開，一方面業者無法了解主管機關的立場和態度，另一方面人民亦無法借助政府審查的力量，監督、了解業者的隱私實踐是否符合個資法，是否確實能保障自己的隱私。因此，本文建議政府應先針對我國的行動應用程式進行隱私意識與隱私通知模式的調查，藉以探究我國使用者與業者間的互動脈絡與模式，得以掌握如何設

計隱私聲明的表示方式，以及政府應以何種標準審查行動應用程式產業業者的隱私操作。此外，中央目的事業主管機關應揭示其為行政審查的標準與方向，納入綜合的實質要素包含個案的脈絡、隱私保護技術、企業的行為、以及業者製造的隱私風險是否當時業者可得預見等，以在業者和使用者間取得平衡。行政檢查後，公開行政檢查結果，供業者得以預見檢查的內容與方法，而加以因應與檢討。

總結以上，鑒於個人資料保護與人性自主與人格保護密不可分，本議題應從通知和同意機制的修正，以及減少業者和使用者間的資訊落差，增進個人資料處理的透明度著手。我國政府在此議題上，可依照個人資料法的規範以及我國國人使用行動設備和行動應用程式的習慣，給予業者符合行動應用程式特性的框架性建議，依照不同的行動應用程式業者類型，提供適合其特性的個別建議。同時，行動應用程式業者亦應自發地運用公協會或產業會議等方式，自行約定隱私設計的最佳模式，以及進行通知和同意機制的改革。蓋唯有業者最能快速掌握科技的發展與脈動。透過自我管制的方式保護使用者的隱私，不僅是最有效率的管制模式和手段，還可以提升業者的信譽與形象，更可以避免個資的爭訟。最後，使用者應該提升隱私意識，透過閱讀隱私聲明和確實地行使同意，了解自己個人資料的動向與使用方式，更應監督業者是否具體落實隱私聲明的內容，以保障自身隱私權利。在行動商務與行動應用程式愈發蓬勃發展，以及行動支付、行動商務逐漸成為主流之際，個人資料濫用、侵害個人隱私的情況只會愈演愈甚，低頭族不該也不必只因行動應用程式的便利或有趣，而向隱私低頭。

參考文獻

一、中文參考文獻

(一) 專書

1. David Brin 著，蕭美惠譯，《透明社會：個人隱私 vs. 資訊自由》，先覺出版社（1999）。
2. Robert A. Peterson，王國川譯，《如何編制優質的問卷》，五南出版社（2010）。
3. 内田治、醍醐朝美，徐華鍥譯，《問卷調查應用入門》，小知堂出版社（2000）。
4. 王澤鑑，《人格權法》，1 版，三民經銷，台北（2012）。
5. 吳明隆，《論文寫作與量化研究》，五南出版社（2011）。
6. 李震山，《人性尊嚴與人權保護》，4 版，元照出版（2011）。
7. 林建廷、李元生，《行動商務概論實務與應用：無所不在的雲端運算、行動裝置、RFID 與物聯網》，碁峰出版（2012）。
8. 恰克．馬丁，許瑞宋譯，《決戰第三螢幕——隨時、定位、互動、行動時代緊貼顧客的行銷與消費新模式》，天下文化（2011）。
9. 資訊工業策進會科技法律研究所，《個資保護 1.0》，書林出版（2013）。
10. 劉宏恩，「基因研究與人權保護」，《基因科技倫理與法律—生物醫學研究的自律、他律與國家規範》，元照出版（2009）。
11. 劉國佐、李世德，《個人資料保護法釋義與實務——如何面臨個資保護的新時代》，碁峰出版（2012）。
12. 鄧肯．華茲著，傅士哲、謝良瑜譯，《6 個人的小世界》，大塊文化（2004）。
13. 蕭奕弘，《個人資料保護法之研究》，司法研究年報第 29 輯第一篇（2012）。
14. 羅清俊，《社會科學研究方法：打開天窗說量化》，2 版，威仕曼文化（2010）。

(二) 期刊論文

1. 呂丁旺，淺析修正「個人資料保護法」，《月旦法學雜誌》，第 183 期（2010）。
2. 周慧蓮，「資訊隱私保護爭議國際化」，《月旦法學雜誌》，第 104 期（2004）。
3. 邱文聰，「從資訊自決與資訊隱私的概念區分——評「電腦處理個人資料保護法修正草案」的結構性問題」，《月旦法學雜誌》，第 168 期（2009）。
4. 莊庭瑞，「個人資料保護在台灣：誰的事務？」，《國家政策季刊》，第二卷第一期（2003）。
5. 翁清坤，「告知後同意與消費者個人資料之保護」，《臺北大學法學論叢》，第 87 期（2013）。
6. 翁清坤，「論個人資料保護標準之全球化」，《東吳法律學報》，第 22 卷第 1 期（2010）。
7. 陳建宇，淺談個人資料保護法，《台灣法學》，第 215 期（2013）。

8. 劉定基，「析論個人資料保護法上「當事人同意」的概念」，《月旦法學雜誌》，第 128 期（2013）。
9. 劉定基，「個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例（下）」，《月旦法學雜誌》，第 119 期（2012）。
10. 劉定基，「個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例（上）」，《月旦法學教室》，第 115 期（2012）。
11. 劉靜怡，「不算進步的立法：「個人資料保護法」初步評析」，《月旦法學雜誌》，第 183 期（2010）。
12. 劉靜怡，「社群網路時代的隱私困境：以 Facebook 為討論對象」，《台大法學論叢》，第 41 卷第 1 期（2012）。
13. 蕭奕弘，「論個人資料保護法的法制性問題」，《成大法學第 23 期》（2012）。

(三) 中文學位論文

1. 陳巧佩，《企業導入顧客關係管理決策之研究》，國立政治大學企業管理學系碩士論文（2000）。
2. 陳裕涵，《網際空間中之隱私權保障—以社群網站為中心》，國立台灣大學法律學院法律學研究所碩士論文（2013）。
3. 董顯康，《行動商務廣告中資訊隱私之研究》，國立臺灣大學國家發展研究所碩士論文（2011）。
4. 簡郁庭，《個人資料揭露案例之研究－－以隱私權保障為中心》，國立臺灣大學社會科學院國家發展研究所碩士論文（2008）。

(四) 網頁文獻

1. 【執行措施】個人資料保護法非公務機關之中央目的事業主管機關，法務部個人資料保護專區，http://pipa.moj.gov.tw/cp.asp?xItem=1298&ctNode=431&mp=1（最後瀏覽時間：2013 年 5 月 23 日）。
2. Android Market 開發人員發佈協議，Google Play，https://play.google.com/about/developer-distribution-agreement.html（最後瀏覽時間：2013 年 8 月 11 日）。
3. 立法院公報，99 卷 29 期 3794 號一冊，http://lis.ly.gov.tw/lgcgi/lypdftxt?09902901;0159;0168（最後瀏覽時間：2014 年 1 月 9 日）。
4. 主要條款，Google，https://www.google.com.tw/intl/zh-TW/policies/privacy/key-terms/（最後瀏覽日期：2013 年 4 月 23 日）。
5. 史諾登上電視 籲團結抵監控，聯合晚報，http://udn.com/NEWS/WORLD/WOR3/8385635.shtml（最後瀏覽時間：2013 年 12 月 31 日）。

6. 司法院大法官第 585 號解釋。
7. 司法院大法官第 603 號解釋。
8. 司法院大法官第 603 號解釋林子儀大法官協同意見書。
9. 司法院大法官第 603 號解釋許宗力大法官和曾有田大法官協同意見書。
10. 司法院大法官第 689 號解釋。
11. 法務部 100 年 9 月 26 日法律字第 1000017452 號函。
12. 法務部 96 年 10 月 8 日法律決字第 0960030614 號函。
13. 法務部民國 100 年 05 月 13 日法律字第 0999051927 號函。
14. 法務部民國 101 年 04 月 27 日法律字第 10103103240 號函。
15. 法務部民國 101 年 06 月 22 日法律字第 10103104090 號函。
16. 法務部民國 102 年 02 月 07 日法律字第 10100253980 號函。
17. 法務部民國 102 年 04 月 17 日法律字第 10203503130 號函。
18. 法務部民國 102 年 05 月 15 日法律字第 10203502260 號函。
19. 法務部民國 91 年 10 月 28 日法律字第 0910037677 號函。
20. 法務部民國 92 年 08 月 14 日行執一字第 0920005014 號函。
21. 法務部民國 92 年 09 月 03 日法律司字第 0920035657 號函。
22. 法務部民國 94 年 11 月 01 日法律字第 0940033446 號函。
23. 法務部民國 96 年 06 月 21 日法律決字第 0960022904 號函。
24. 法務部民國 96 年 06 月 21 日法律決字第 0960023899 號函。
25. 法務部民國 98 年 11 月 16 日法律決字第 0980047501 號函。
26. 香港個人資料私隱專員公署，調查報告：手機程式「起你底」嚴重侵犯個人資料私隱，（最後瀏覽日期：2013 年 11 月 20 日）。
27. 個人資料私隱專員公署，「全球私隱執法機關網絡」聯合公佈各地網上私隱政策透明度檢視結果，http://www.pcpd.org.hk/tc_chi/infocentre/press_20130814.htm（最後瀏覽日期：2013 年 11 月 20 日）。
28. 個人資料保護法之特定目的及個人資料之類別修正總說明及對照表，法務部，http://www.moj.gov.tw/ct.asp?xItem=283183&ctNode=28007&mp=001（最後瀏覽時間：2013 年 4 月 20 日）。
29. 第二篇、個人資料保護法實務上注意事項 Q1. 個人資料保護法的「主管機關」所指為何？中小企業如何確定自身所屬行業的主管機關有哪些？，經濟部中小企業處，http://law.moeasmea.gov.tw/modules.php?name=km&file=article&sid=608（最後瀏覽時間：2013 年 8 月 20 日）。
30. 部會踢皮球 檢舉個資案跑一年，自由時報，http://www.libertytimes.com.tw/2013/new/may/14/today-life7.htm（最後瀏覽時間：2013 年 5 月 23 日）。
31. 經濟部工業局，個人資料法規遵循參考指引暨宣導手冊——資服業個資教戰

手冊（2012），http://www.moeaidb.gov.tw/external/ctlr?PRO=information.InformationNewsList&t=2184（最後瀏覽時間：2013 年 8 月 20 日）。
32. 經濟部工業局寬頻網通產業整合推動計畫，http://www.communications.org.tw/communications/page.php?pg=detail&unit=4306&cone=2&ctwo=22（最後瀏覽日期：2013 年 10 月 9 日）。
33. 經濟部主管個人資料保護法非公務機關之分工表，經濟部法規委員會，http://www.moea.gov.tw/Mns/colr/content/ContentLink.aspx?menu_id=6419（最後瀏覽時間：2013 年 8 月 20 日）。
34. 資料使用政策，Facebook，https://www.facebook.com/about/privacy/your-info（最後瀏覽日期：2013 年 10 月 22 日）。
35. 資訊主頁，Google，https://www.google.com/dashboard/（最後瀏覽日期：2013 年 4 月 16 日）。
36. 電視連續劇（最新台劇、韓劇、大陸劇、日劇），Google Play，https://play.google.com/store/apps/details?id=com.jumplife.tvdrama（最後瀏覽日期：2013 年 10 月 10 日）。
37. 劉翰謙，走向免費的商用軟體，數位時代，http://www.bnext.com.tw/article/view/id/22985（最後瀏覽日期：2013 年 8 月 18 日）。
38. 歐洲人權公約，社團法人中華人權協會，http://www.cahr.org.tw/lawdan_detail.php?nid=105（最後瀏覽時間：2013 年 4 月 14 日）。
39. 鄭逸寧，成功的企業 App 必須貼近使用情境，達到使用者、裝置、周遭環境、網路之間的互動效果，並有效解決使用者面臨的問題，iThome，http://www.ithome.com.tw/itadm/article.php?c=73463&s=1（最後瀏覽時間：2013 年 8 月 11 日）。
40. 澳門個人資料保護辦公室，“互聯網私隱風險搜尋”報告，http://www.gpdp.gov.mo/cht/forms/sweepreport_ch.pdf（最後瀏覽日期：2013 年 11 月 20 日）。
41. 盧沛樺，App 出包 個資法未必管得到，聯合新聞網，http://mag.udn.com/mag/digital/storypage.jsp?f_MAIN_ID=322&f_SUB_ID=2920&f_ART_ID=470562（最後瀏覽時間：2013 年 8 月 20 日）。
42. 臉書按個讚，性向、智商全曝光，天下雜誌，http://www.cw.com.tw/article/article.action?id=5047757（最後瀏覽日期：2013 年 4 月 23 日）。
43. 隱私權政策，Google，https://www.google.com.tw/intl/zh-TW/policies/privacy/（最後瀏覽日期：2013 年 4 月 23 日）。

二、外文參考文獻

(一) 專書

1. BLACKMAN, RODYN, NONTRADITIONAL MEDIA IN MARKETING AND ADVERTISING (2013).
2. CALIFORNIA DEPARTMENT OF JUSTICE, PRIVACY ON THE GO, *available at* http://oag.ca.gov/sites/all/files/pdfs/privac/privacy_on_the_go.pdf (last visited March 28, 2013).
3. FEDERAL TRADE COM'N, MOBILE PRIVACY DISCLOSURE—BUILDING TRUST THROUGH TRANSPARENCY, *available at* http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm (last visited March 21, 2013).
4. FTC REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited Dec. 25, 2012).
5. HART, JONATHAN D. HART, INTERNET LAW: A FIELD GUIDE (2008).
6. HEISENBERG, DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION (2005).
7. Karstens, B. et al., *Presenting Large an Complex Information Sets on Mobile Handhelds*, in E-COMMERCE AND M-COMMERCE TECHNOLOGIES (Mehdi Khosrow-Pour ed., 2005).
8. KUNER,CHRISTOPHER, EUROPEAN DATA PROTECTION LAW (2007).
9. NISSEMBAUM, HELEN NISSEMBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).
10. POSNER, RICHARD A. POSNER, THE ECONOMICS OF JUSTICE (1983).
11. Rhodes, Michael G. Rhodes and Charles A. Schwab, *Mobile Commerce: A Moving Target for Legal Compliance*, *in* UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW (2012).
12. ROBERTS, MARY LOU & DEBRA ZAHAY, INTERNET MARKETING: INTERGRATING ONLINE AND OFFLINE STRATEGIES (2013).
13. SOLOVE, DANIEL J., INFORMATION PRIVACY LAW (2012).
14. SOLOVE, DANIEL J., THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).
15. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited Dec. 26, 2012).
16. WESTIN, ALAN, PRIVACY AND FREEDOM (1967).

17. YELTON, ANDROMEDA, BRIDGING THE DIGITAL DIVIDE WITH MOBILE SERVICE (2012).

(二) 期刊論文

1. Asay, Clark D., *Consumer Informtion Privacy and the Problems of Third-Party Disclosures*, 11 NW, J. TECH. & INTEEL. PROP. 321 (2013).
2. Charles, Fried, *Privacy*, 77 YALE L. J. 475 (1968).
3. Deighton, John, *The Right to Be Let Alone*, 12 J. INTERACIVE MARKETING 2 (1998).
4. Hoofnagle, Chris Jay & Jennifer King, *Research Report: What Californians Understand About Privacy Offline* 3 (working paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075 (last visited Dec. 10, 2013).
5. Hoofnagle, Chris Jay, et al., *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*, SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 (last visited April 23, 2013).
6. Kang, Jerry & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J. L. & TECH. 229 (2004).
7. Kang, Jerry, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998).
8. Nissenbaum, Helen, *The Meaning of Anonymity in an Information Age*, 15 THE INFO. SOC'Y 141 (1999).
9. Nissenbaum, Hellen, *A Contextual Approach to Privacy Online*, DAEDALUS, Fall. 2011, *available at* http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf (last visited Dec. 10, 2013).
10. Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).
11. Ozer, Nicole A., *Putting Online Privacy Above The Fold: Building A Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 220-231 (2012).
12. Peppers, Don, Martha Rogers, & Bob Dorf, *Is Your Company Ready for One-to-one Marketing?*, HARVARD BUSINESS REVIEW January-February 151-160 (1999).
13. Rubinstein, Ira S. et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261 (2008).
14. Sanderson, Steven, *Build a Better Mobile Browsing Experience*, MSDN MAGAZINE, (July 2011).
15. Schwartz, Paul M. & Daniel J. Solove, *The PII Problem: Privacy and a New*

Concept of Personally Identifiable Information, 86 N. Y. U. L. REV. 1814 (2011).

16. Schwartz, Paul M., *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623 (2013).
17. Solove, Daniel J., *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2008).
18. Solove, Daniel J., *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013).
19. Sovern, Jeff, *Opting in, Opting Out, or No Options at All: the Fight for Control of Personal Information*, 74 WASH . L. REV. 1033 (1999).
20. Tene, Omer & Jules Polonetsky, *Big Data For All: Privacy And User Control In The Age Of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013).
21. Ur, Blasé, Manya Sleeper, *Lorrie Faith Cranor, {Privacy, Privacidad, „Foreign Language>>} Policies in Social Media: Providing Translated Privacy Notice*, 9 I/S: J.L. & POL'Y FOR INFO. SOC'Y 201 (2013).
22. Urban, Jennifer M., Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privay*, BURKELEY CENTER FOR LAWN & TECHNOLOGY RESEARCH PAPER, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405 (last visited Dec. 10, 2013).
23. Wang, Ming-Li, *Information Privacy in a Network Society: Decision Making Amidst Constant Change*, 5 NAT'L TAIWAN U. L. REV. 127, 146 (2010).
24. Whitman, James Q., *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L. J. 1151 (2004).

(三) 其他外文參考文獻

1. *About the Conference*, The International Data Protection and Privacy Commissioners Conference, https://privacyconference2013.org/About_the_Conference_ (last visited Nov. 20, 2013).
2. *About the IAPP*, IAPP, https://www.privacyassociation.org/about_iapp/ (last visited Aug. 18, 2013).
3. *About the Network*, Global Privacy Enforcement Network, https://www.privacyenforcement.net/ (last visited Nov. 20, 2013).
4. *About us*, KING, http://about.king.com/about (last visited May 20, 2013).
5. Acquisti, Alessandro and Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf (last visited April 23, 2013).
6. *App Store Review Guidelines*, APPLE, http://images.worldofapple.com/appstoreguidelines_9910.pdf (last visited Aug.

11, 2013).

7. Asprey, Dave, *Oblivious Data Loss and the Wild West of Mobile App Security*, TREND CLOUD SECURITY BLOG (Apr. 12, 2012), http://cloud.trendmicro.com/oblivious-data-loss-and-the-wild-west-of-mobile-App-security/ (last visited Dec. 10, 2013).
8. *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifiesmobile-app-developers-non-compliance (last visited Dec. 27, 2012).
9. Bilton, Nick, *Apple Updates Software to Fix Problems With Collecting Location Data*, N.Y. TIMES, May 4, 2011, http://bits.blogs.nytimes.com/2011/05/04/apple-ios-software-release-fixes-location-bug/.
10. Boyles, Jan Lauren, Aaron Smith & Mary Madden, *Privacy and Data Management on Mobile Devices*, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012), http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.
11. BUNDESDATENSCHUTZGESETZ [BDSG] [FEDERAL DATA PROTECTION ACT], Sept. 1, 2009, BUNDESGESETZBLATT [BGBL] 1, 2814, as amended, *available at* http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile.
12. Carson, Angelique, *ZIP Codes: Are Courts Set To Protect Consumers from Marketing?*, IAPP (May 1, 2013), https://www.privacyassociation.org/publications/2013_05_01_zip_codes_are_courts_set_to_protect_consumers_from_marketing.
13. Chawla, Shuchi et al., *Toward Privacy in Public Databases*, 2 THEORY CRYPTOGRAPHY CONF. 363 (2005).
14. *ClickMode Enumeration*, MSDN, http://msdn.microsoft.com/zh-tw/library/system.windows.controls.clickmode(v=vs.100).aspx (last visited Nov. 5, 2013).
15. Complaint, People v. Delta Airlines, Inc., No. CGC-12-526741 (Super. Ct. Cal. Dec. 6, 2012), *available at* http://www.lw.com/admin/Upload/Documents/Complaint.pdf (last visited Dec. 10, 2013).
16. Cooper, Dan and Philippe Bradley, *EU Data Protection Working Party Sets out App Privacy Recommendations*, INSIDE PRIVACY (March 15, 2013), http://www.insideprivacy.com/international/european-union/eu-data-protection-working-party-sets-out-app-privacy-recommendations/ (last visited Dec. 10,

2013).
17. Council Directive 95/46/EC, 1995 O.J. (L281) 38 (EC).
18. Data Use Policy, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Oct. 10, 2013).
19. Dawyer v. American Express Co., 652 N.E.2d 1351 (1995).
20. Directive 2002/58/EC, 2002 O.J. (L 201) (EC).
21. *Directive 95/46/EC of The European Parliament And of The Council of 24 October 1995 on The Protection of Individuals With Regard to The Processing of Personal Data And on The Free Movement of Such Data*, EUR-LEX, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited Dec. 18, 2012).
22. European Convention on Human Right, *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf (last visited Dec. 10, 2013).
23. Facebook, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.facebook.katana&hl=zh-TW (last visited Oct. 10, 2013).
24. Fair Information Practice Principles, Federal Trade Commission, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited March 29, 2013).
25. Fleischer, Peter, *Don Quixote*, PETER FLEISCHER: PRIVACY...? (Feb. 17, 2013, 8:33 PM), http://peterfleischer.blogspot.tw/2013_02_01_archive.html (last visited Dec. 10, 2013).
26. Fleischer, Peter, *It's time for a "lead regulator" in Europe*, PETER FLEISCHER: PRIVACY...? (Aug. 16, 2012, 9:02 AM), http://peterfleischer.blogspot.tw/2012/08/its-time-for-lead-regulator-in-europe (last visited Dec. 10, 2013).
27. Fleischer, Peter, *Why Johnny can't read...a privacy policy*, PETER FLEISCHER: PRIVACY...? (March 27, 2013, 4:15 PM), http://peterfleischer.blogspot.tw/2013/03/why-johnny-cant-reada-privacy-policy.html (last visited Dec. 10, 2013).
28. *FTC Publishes Guide to Help Mobile App Developers Observe Truth-in-Advertising, Privacy Principles*, FTC, http://www.ftc.gov/opa/2012/09/mobileapps.shtm (last visited April 20, 2013).
29. Garner, Margo & Laurece Steinberg, *Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: An Experimental Study*, DEVELOPMENTAL PSYCHOLOGY (2005), *available at* http://www.temple.edu/psychology/lds/documents/PeerInfluenceonRisk-TakingDP.pdf.

30. *Global Privacy Enforcement Network Internet 'Privacy Sweep'*, Office of the Data Protection Commissioner, http://www.dataprotection.ie/documents/GPEN2013.pdf (last visited Nov. 20, 2013).
31. *Global Privacy Enforcement Network Internet Privacy Sweep Questions and Answers*, The Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/media/nr-c/2013/nr-c_130506_qa_e.asp (last visited Nov. 20, 2013).
32. *Glossary*, IAPP, https://www.privacyassociation.org/resource_center/privacy_glossary/#P (last visited Aug. 18, 2013).
33. Goldman, Eric, *The Privacy Hoax*, FORBES.COM (Oct. 14, 2002), http://www.forbes.com/forbes/2002/1014/042.html (last visited Dec. 10, 2013).
34. *Google Play*, GOOGLE, https://play.google.com/store (last visited Oct. 10, 2013).
35. *Google Privacy Policy: Main Findings And Recommendations*, EU, https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/octubre/Recommendations_Google_EN.pdf (last visited April 22, 2013).
36. *Google wants UK privacy case tried abroad, lawyer claims*, BBC (Aug. 19, 2013), http://www.bbc.co.uk/news/technology-23756243 (last visited Dec. 10, 2013).
37. Hoofnagle, Chris, Jennifer King, Su Li & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?*, *available at* http://ssrn.com/abstract=1589864.
38. Hotz, Robert Lee, *When 'Likes' Can Shed Light*, THE WALL STREET JOURNAL (March 11, 2013, 7:25 PM), http://online.wsj.com/article/SB10001424127887324096404578354533010958940.html?mod=WSJ_Tech_LEFTTopNews (last visited Dec. 10, 2013).
39. Hover Over An Icon To Read Their Definitions, Disconnect, Inc, https://icons.disconnect.me/icons (last visited Dec. 19, 2012).
40. In the Matter of Goldenshores Technologies, LLC, and Erik M. Geidl, No. 132 3087, *available at* http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshoresorder.pdf.
41. *iTunes Preview*, APPLE INC., https://itunes.apple.com/us/genre/ios/id36?mt=8 (last visited Oct. 10, 2013).
42. *June 2012 FPF Mobile Apps Study*, FUTURE OF PRIVACY FORUM, (2012), http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf (last visited Dec. 10, 2013).

43. Kuner, Christopher, *"You Just Don't Understand": The Current EU–U.S. Privacy Battles*, PRIVACY PERSPECTIVE (Feb. 28, 2013), https://www.privacyassociation.org/privacy_perspectives/contributors/kuner_christopher (last visited Nov. 29, 2013).
44. Kuner, Christopher, *The Transatlantic Divide Over Data Privacy Rights,* PRIVACY PERSPECTIVE (May 20, 2013), https://www.privacyassociation.org/privacy_perspectives/post/the_transatlantic_divide_over_data_privacy_rights (last visited Nov. 29, 2013).
45. Leibowitz, Jon, Comm'r, Fed. Trade Comm'n, So Private, So Public: Individuals, The Internet & The Paradox Of Behavioral Marketing, Remarks at the FTC Town Hall Meeting on "Ehavioral Advertising: Tracking, Targeting & Technology" (Nov. 1, 2007), *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf (last visited Dec. 10, 2013).
46. *Letter Addressed to Google*, EU, http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/LetterAdressedToGoogle.pdf?__blob=publicationFile (last visited April 22, 2013).
47. Liu, Josephine, *FTC Working on Privacy "Nutrition Label"; Industry Focusing on Icons*, INSIDE PRIVACY (Oct. 25, 2012), http://www.insideprivacy.com/united-states/federal-trade-commission/ftc-working-on-privacy-nutrition-label-industry-focusing-on-icons/ (last visited Dec. 10, 2013).
48. Magid, Larry, *Agreement Calls For Mobile App Privacy Disclosures (Updated)*, FORBES (July 25, 2013, 8:17PM), http://www.forbes.com/sites/larrymagid/2013/07/25/voluntary-industry-agreement-calls-for-mobile-app-privacy-disclosures-but-does-it-have-teeth/ (last visited Dec. 10, 2013).
49. Magid, Larry, *App Privacy Issues Deeply Troubling*, THE HUFFINGTON POST, Feb. 21, 2012, http://www.huffingtonpost.com/larry-magid/iphone-app-privacy_b_1290529.html; *What They Know – Mobile*, THE WALL STREET JOURNAL, http://blogs.wsj.com/wtk-mobile/ (last visited March 30, 2013).
50. Miller, Claire Cain, *Google to Pay $17 Million to Settle Privacy Case*, N.Y. TIMES (Nov. 18, 2013), http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html?_r=0.
51. Narayanan, Arvind & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy, *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.
52. Nayak, Saira, *Response to EU Opinion on Mobile Apps*, TRUSTE BLOG (March. 14,

2013), HTTP://WWW.TRUSTE.COM/BLOG/2013/03/14/RESPONSE-TO-EU-OPINION-ON-MOBILE-APPS/ (last visited Dec. 10, 2013).

53. Newby, Tyler G. & David Marty, *Privacy Litigation Alert: California Court Dismisses Attorney General's Mobile App Privacy Suit Against Delta, Offers Little Guidance*, FENWICK & WEST LLP, http://www.fenwick.com/publications/Pages/Privacy-Litigation-Alert-California-Court-Dismisses-Attorney-Generals-Mobile-App-Privacy-Suit-Against-Delta.aspx (last visited Aug. 29, 2013).
54. Nick Bilton, *3G Apple iOS Devices Are Storing Users' Location Data*, N.Y.TIMES, Apr. 20, 2011, http://bits.blogs.nytimes.com/2011/04/20/3g-apple-ios-devices-secretly-storing-users-location/.
55. *NTIA Mobile App Transparency - UI Compositions*, NTIA, http://www.ntia.doc.gov/files/ntia/publications/ntia_ui_comps_update_7.23.pdf (last visited Aug. 28, 2013).
56. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Dec. 22, 2012).
57. *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, http://www.oecd.org/internet/ieconomy/38770483.pdf (last visited Nov. 29, 2013).
58. Olson, Jeremy, *How To Succeed With Your Mobile App*, SMASHING MAGAZINE, Nov. 7, 2012, http://mobile.smashingmagazine.com/2012/11/07/succeed-with-your-app/ (last visited Dec. 10, 2013).
59. Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22575 (a).
60. Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22577 (a).
61. Opinion 02/2013 on Apps on Smart Device, 2013 WP 202 (EC).
62. Opinion 10/2004 on More Harmonised Information Provisions, 2004 WP 100 (EC).
63. Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, 2011 WP 185 (EC).
64. Opinion 15/2011 on the Definition of Consent at 23, 2011 WP 187 (EC).
65. Opinion 4/2007 on the Concept of Personal Data, 2007 WP 136 (EC).
66. *Ovi Store*, NOKIA, http://store.ovi.com/ (last visited Oct. 10, 2013).
67. Press Release, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers* (Dec. 5, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.
68. Press Release, *Path Social Networking App Settles FTC Charges it Deceived*

Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *available at* http://ftc.gov/opa/2013/02/path.shtm (last visited Dec. 10, 2013).

69. *Privacy Commissioner: Website privacy policies are too long and complex*, THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex (last visited Nov. 20, 2013).
70. *Privacy Enforcement and Protection*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, http://oag.ca.gov/privacy (last visited March 28, 2013).
71. *Privacy Policy*, INSTAGRAM, http://instagram.com/about/legal/privacy/ (last visited Oct. 22, 2013).
72. *Proposal for a Directive of The European Parliament and of The Council on The Protection of Individuals With Regard to The Processing of Personal Data by Competent Authorities for The Purposes Of Prevention, Investigation, Detection or Prosecution of Criminal Offences or The Execution of Criminal Penalties, And The Free Movement of Such Data*, EUR-LEX, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited Oct. 21, 2013).
73. *Re: Privacy on the Go – Recommendations for the Mobile Ecosystem*, http://gaia.adage.com/images/bin/pdf/TradeGroupLettertoCA1.10.13.pdf (last visited April 20, 2013).
74. *Results of the 2013 Global Privacy Enforcement Network Internet Privacy Sweep*, THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, http://www.priv.gc.ca/media/nr-c/2013/bg_130813_e.asp (last visited Nov. 20, 2013).
75. *Results of the first GPEN Internet Privacy Sweep,* COMMISSION FOR THE PROTECTION OF PRIVACY, http://www.privacycommission.be/en/internet-privacy-sweep-2013 (last visited Nov. 20, 2013).
76. *Sample Size Calculator*, CREATIVE RESEARCH SYSTEMS, http://www.surveysystem.com/sscalc.htm (last visited Oct. 9, 2013).
77. Satterfield, Steve, *California AG Puts Mobile App Developers on Notice*, INSIDE PRIVACY (Nov. 1, 2012), http://www.insideprivacy.com/united-states/california-ag-puts-mobile-app-developers-on-notice/ (last visited Dec. 10, 2013).
78. Sengupta, Somini, *Building an Iconography for Digital Privacy*, THE NEW YORK TIMES, http://bits.blogs.nytimes.com/2012/11/19/building-an-iconography-for-digital-privacy/?nl=technology&emc=edit_tu_20121120 (last visited Dec. 19, 2012).

79. *Sensor API Specification*, W3C Working Draft, https://dvcs.w3.org/hg/dap/raw-file/tip/sensor-api/Overview.html (last visited March. 28, 2013).
80. Shibley v. Time, 341 N.E.2d 337 (1975).
81. *Short Form Notice Code Of Conduct To Promote Transparency In Mobile App Practices*, NTIA (2013), http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf (last visited Dec. 10, 2013).
82. Solove, Daniel J., *Why Privacy Matters Even if You Have 'Nothing to Hide'*, THE CHRONICLE REVIEW (May 15, 2011), http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/ (last visited Dec. 10, 2013).
83. *Speech: The EU's Data Protection reform: Decision-Time is Now*, EUROPA, http://europa.eu/rapid/press-release_SPEECH-13-197_en.htm (last visited March 29, 2013).
84. *The OECD Privacy Framework*, OECD , http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited Nov. 8, 2013).
85. Tozer, James, *UK law has no power over us, says Google: Outrage at search giant's arrogance in snooping case*, DAILY MAIL (12:04 GMT, Aug. 19, 2013) http://www.dailymail.co.uk/news/article-2396809/Google-says-UK-law-power-Outrage-search-giant-bypassing-privacy-settings.html (last visited Dec. 10, 2013).
86. Tsukayama, Hayley, *California attorney general warns app makers over user privacy*, THE WASHINGTON POST, Oct. 30, 2012, http://www.washingtonpost.com/blogs/post-tech/post/california-attorney-general-warns-app-makers-over-user-privacy/2012/10/30/33ac9afc-22cd-11e2-8448-81b1ce7d6978_blog.html?wpisrc=nl_tech.html (last visited Dec. 10, 2013).
87. Tyler v. Michaels Stores, Inc., Civ. No. 11-10920-WGY (D. Mass. Jan. 6, 2012). Pineda v. Williams-Sonoma, 51 CAL. 4TH 524, 246 P.3D 612, 120 CAL. RPTR. 3D 531 (Cal. Feb. 10, 2011).
88. U.S. v. Path, Inc., No. C 13 0448, slip op. (N.D. Cal).
89. *Understanding Mobile Apps*, ONGUARDONLINE.GOV, http://www.onguardonline.gov/articles/0018-understanding-mobile-apps (last visited March. 28, 2013).
90. Vincent, James, Google claims that UK law does not apply to them, THE INDEPENDENT (Aug.19, 2013), http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-claims-that-uk-law-does-not-apply-to-them-8774935.html.
91. *W3C Technical Reports Index*, W3C WORKING DRAFT, http://www.w3.org/TR/2012/WD-proximity-20121206/ (last visited March. 28, 2013).

92. *Why do we need an EU data protection reform?*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (last visited March 29, 2013).
93. *Windows Phone*, MICROSOFT, http://www.windowsphone.com/en-us/store (last visited Oct. 10, 2013).

附錄：**「行動商務的個人資料保護－以行動應用程式為核心」紙本問卷調查**

受訪者，您好：

這是一份「行動商務的個人資料保護－－以行動應用程式為核心」的紙本問卷調查，由國立交通大學科技法律研究所學生鄭忻忻擔任研究訪問者，十分感謝您撥冗填寫問卷。

本問卷採樣範圍母群體為**行動應用程式**（亦即通稱的 App.）使用者，就**「使用頻率最高」**的智慧型手機或平板電腦為作答對象。本問卷的目的主要是藉由調查應用程式的個人資料保護措施，以了解使用者的個人資料意識，以及現行保護措施的效度，作為相關研究之用。

這一份問卷每一題都是**必答題**，但問卷不長，只需要花幾分鐘的時間填寫，您的回答對本研究非常珍貴。本問卷的原始內容，保證不會讓第三者得知，問卷的結果將用在碩士論文上，並以匿名統計數據的方式呈現，以確保您的隱私，請您放心填答。

感謝您撥冗填寫，並祝事事如意！

國立交通大學科技法律研究所
指導教授：王立達老師
研究生　：鄭忻忻　　敬上

第一部分：行動通訊裝置的行動應用程式背景資料

行動通訊裝置定義為「提供類似於個人電腦的功能，或是能下載行動應用程式的裝置」，包含智慧型手機或平板電腦。假設使用者手邊同時有許多種行動裝置，煩請以**「使用頻率最高者」**為作答對象。

1. 請問最近三個月曾下載至行動通訊裝置的應用程式平台為何？

☐ Apple App Store　　☐ Google Android Market／Google Play

☐ Nokia Ovi Store　　☐ Windows Store

☐ 其他：_____

2. 請問您最近三個月內，最常使用的行動應用程式（App.） 類型？（本題為「**複選題**」）

- ☐ 最近三個月內未使用應用程式
- ☐ 運動軟體
- ☐ 遊戲類軟體
- ☐ 教育／親子軟體
- ☐ 音樂與音效軟體
- ☐ 飲食／食譜軟體
- ☐ 照片、攝影和視訊軟體
- ☐ 社交互動／社群網路軟體
- ☐ 電視／電影／影片線上觀賞
- ☐ 健康管理／醫療／塑身軟體
- ☐ 圖書與參考資源／漫畫軟體
- ☐ 提供即時通訊／傳訊息服務軟體
- ☐ 提供網路交易或線上消費服務軟體
- ☐ 提供景點、餐點、目的地、美食等導覽軟體
- ☐ 工具程式軟體（包含個人化、動態桌布等工具）
- ☐ 提供新聞與雜誌、天氣、運動、股票、財經等即時訊息軟體
- ☐ 不知道／拒答
- ☐ 其他：_____

3. 請問您最近三個月內，曾經下載那些行動應用程式（App.） 類型？（本題為「**複選題**」）

- ☐ 最近三個月內未下載應用程式
- ☐ 運動軟體
- ☐ 遊戲類軟體
- ☐ 教育／親子軟體
- ☐ 音樂與音效軟體
- ☐ 飲食／食譜軟體
- ☐ 照片、攝影和視訊軟體
- ☐ 社交互動／社群網路軟體
- ☐ 電視／電影／影片線上觀賞
- ☐ 健康管理／醫療／塑身軟體
- ☐ 圖書與參考資源／漫畫軟體
- ☐ 提供即時通訊／傳訊息服務軟體
- ☐ 提供網路交易或線上消費服務軟體
- ☐ 提供景點、餐點、目的地、美食等導覽軟體
- ☐ 工具程式軟體（包含個人化、動態桌布等工具）
- ☐ 提供新聞與雜誌、天氣、運動、股票、財經等即時訊息軟體
- ☐ 不知道／拒答
- ☐ 其他：_____

第二部分：應用程式的「隱私權政策」

一、「隱私權政策」的使用者意識

以 Facebook（臉書）應用程式的隱私權政策為例，內容包含：

- 我們所收到的資訊以及如何使用的規範（瞭解本網站收到的資訊種類，以及資訊使用方式。）；
- 在 Facebook 上分享和搜尋您（瞭解可以協助控制您在 facebook.com 資訊的隱私設定。）；
- 其他網站和應用程式（瞭解社交外掛程式之類的應用程式，以及您和您的朋友在 Facebook 使用遊戲、應用程式和網站時的資訊分享方式。）；
- 廣告和動態贊助的運作方式（查看不必和廣告商分享您的資訊就能提供廣告的運作方式，並瞭解我們如何搭配廣告和社群脈絡，如動態消息風格的動態贊助。）；
- Cookie、像素和其他系統技術（瞭解 cookie、像素和工具（如本機儲存）如何使用來提供您各種服務、功能和相關廣告及內容。）；
- 其他您需要瞭解的資訊（瞭解我們對此政策所做的更改以及更多詳情。）。

1. 請問您下載行動應用程式前，是否會閱讀「隱私權政策」？

☐ 會　　☐ 不會（請跳至**第 3 題**作答）

2. 請問您在閱讀「隱私權政策」，您的了解程度為？（完全不了解：1～完全了解：5）

☐ 1（請跳至**第 4 題**作答）　　☐ 4（請跳至**第 5 題**作答）

☐ 2（請跳至**第 4 題**作答）　　☐ 5（請跳至**第 5 題**作答）

☐ 3（請跳至**第 5 題**作答）

3. 請問造成您「不讀」隱私權政策，最主要的原因為？（本題為**複選題**，最多選 3 個）

☐ 字體太小　　☐ 內容看不懂：有太多資訊術語

☐ 敘述太冗長　　☐ 內容看不懂：有太多法律詞彙

☐ 語言非繁體中文　　☐ 等不及，想趕快使用應用程式

☐ 不知道有隱私權政策　　☐ 使用者沒辦法改變隱私權政策，看了也沒有用

☐ 找不到隱私權政策的位置　　☐ 其他：_____

（答畢，請跳至**第 6 題**作答）

4. 請問造成您「看不懂」隱私權政策，最主要的原因為？（本題為**複選題**，最多選 3 個）

☐ 敘述太冗長
☐ 內容看不懂：有太多資訊術語
☐ 語言非繁體中文
☐ 不理解個人資料蒐集與應用程式功能間的關聯
☐ 內容看不懂：有太多法律詞彙
☐ 其他：_____

（答畢，請跳至**第 6 題**作答）

5. 請問您認為隱私權政策，對使用者自行保護個人資料的幫助程度為？

	1	2	3	4	5	
非常沒有用	☐	☐	☐	☐	☐	非常有用

6. 若行動應用程式業者「**沒有**」提供隱私權政策，是否會影響到您下載該應用程式的意願？

☐ 會
☐ 不會

二、「隱私權政策」的定性

請問您認為「隱私權政策」的性質是什麼？

☐ 契約或類似契約（同時拘束應用程式開發業者和平台業者，以及使用者）
☐ 聲明（僅通知性質，對業者和使用者沒有拘束力）
☐ 其他：_____

第三部分：行動應用程式的「權限清單」

Apple App Store 或 Nokia Ovi Store 使用者請跳至<u>第四部份（第７頁）</u>作答

「權限清單」是在安裝下載前，行動應用程式會先跳出一個視窗，告知行動應用程式下載後，會要求使用者授予怎樣的權限。以 Facebook（臉書）應用程式為例，權限清單會有：

- 您的帳戶（建立帳戶及設定密碼、新增或移除帳戶）；
- 硬體控制介面（拍照和拍攝影片）；
- 您的位置資訊（概略位置 (以網路為基準、精確位置 (以 GPS 和網路為基準))；
- 網路通訊（完整網路存取權）；
- 您的個人資訊（讀取您的聯絡人、修改您的聯絡人）；
- 手機通話（讀取手機狀態和識別碼）；
- 儲存空間（修改或刪除 USB 儲存裝置的內容、修改或刪除 SD 卡的內容）；
- 系統工具（防止平板電腦進入休眠狀態；防止手機進入休眠狀態、開啟及關閉同步功能）；
- 您的帳戶（尋找裝置上的帳戶）；
- 硬體控制介面（控制震動）；
- 網路通訊（查看 WIFI 連線、查看網路連線、接收網際網路資料）；
- 系統工具（讀取同步處理設定）；
- 預設（測試能否存取受保護的儲存裝置；測試能否存取受保護的儲存裝置、寫入通話紀錄、讀取通話紀錄）。

一、「權限清單」的使用者意識

1. 請問您安裝行動應用程式前，是否會閱讀「權限清單」？

☐ 會　　☐ 不會（請跳至**第３題**作答）

2. 請問您在閱讀「權限清單」，您的了解程度為？（完全不了解：1～完全了解：5）

☐ 1（請跳至**第４題**作答）　　☐ 4（請跳至**第５題**作答）

☐ 2（請跳至**第４題**作答）　　☐ 5（請跳至**第５題**作答）

☐ 3（請跳至**第５題**作答）

3. 請問造成您「不讀」權限清單，最主要的原因為？（本題為**複選題**，最多選 3 個）

☐ 字體太小
☐ 等不及，想趕快使用應用程式
☐ 敘述太概略
☐ 使用者沒辦法改變權限清單，看了也沒有用
☐ 內容看不懂：有太多資訊術語
☐ 其他：_____

（答畢，請跳至**第 6 題**作答）

4. 請問造成您「看不懂」權限清單，最主要的原因為？（本題為**複選題**，最多選 3 個）

☐ 敘述太概略
☐ 內容看不懂：有太多資訊術語
☐ 不知道權限清單對我會造成什麼影響
☐ 不理解個人資料蒐集與應用程式功能間的關聯
☐ 其他：_____（答畢，請跳至**第 6 題**作答）

5. 請問您認為權限清單，對使用者自行保護個人資料的幫助程度為？

	1	2	3	4	5	
非常沒有用	☐	☐	☐	☐	☐	非常有用

6. 行動應用程式權限清單上，列舉的項目數量，是否會影響您下載應用程式的意願？

☐ 會
☐ 不會

二、「權限清單」的定性

請問您認為「權限清單」的性質是什麼？

☐ 契約或類似契約（同時拘束應用程式開發業者和平台業者，以及使用者）
☐ 聲明（僅通知性質，對業者和使用者沒有拘束力）
☐ 其他：_____

第四部分：使用者對行動應用程式蒐集個人資料的態度

1. 請問下列個人資料，哪一個您覺得最敏感，最不想被蒐集？（本題為**「單選題」**）

☐ 您的姓名
☐ 行事曆
☐ 電話簿
☐ 通話紀錄
☐ 電子郵件
☐ 照片或影片
☐ 行動電話號碼
☐ 網頁瀏覽紀錄
☐ 健康或醫藥相關資訊
☐ 財務或付款相關資訊
☐ 簡訊、訊息或電子郵件內容
☐ 已下載或已使用的應用程式
☐ 位置資訊（例如 GPS、Wifi 熱點定位）
☐ 其他：_____

2. 請問您介意行動應用程式蒐集個人資料的程度為？（非常不介意：1～非常介意：5）

☐ 1（請跳至**第3題**作答）
☐ 2（請跳至**第3題**作答）
☐ 3（請跳至**第4題**作答）
☐ 4（請跳至**第4題**作答）
☐ 5（請跳至**第4題**作答）

3. 請問您「不介意」行動應用程式蒐集個人資料的原因為？（本題為**「複選題」**，最多選3個）

☐ 行動應用程式的功能性更重要
☐ 不知道行動應用程式會蒐集個人資料
☐ 行動應用程式所蒐集的個人資料不重要
☐ 反正沒辦法更改／拒絕個人資料的蒐集，就算了
☐ 行動應用程式蒐集個人資料，對我不會造成太大損害或不便
☐ 其他：_____

（答畢，請跳至**第五部分（第8頁）**作答）

4. 請問您「介意」行動應用程式蒐集個人資料的原因為？（本題為**「複選題」**，最多選 3 個）

☐ 不願意行動應用程式掌握我的個人資料

☐ 擔心行動應用程式蒐集太多我的個人資料

☐ 擔心個人資料外洩，而接到廣告或詐騙電話

☐ 其他：_____

☐ 不知道行動應用程式業者會如何利用個人資料

☐ 不知道行動應用程式業者會將個人資料傳送給誰

☐ 對於行動應用程式業者會不會好好保護我的個人資料沒有信心

第五部分：受訪者基本資料

1. 請問您的性別？

☐ 女　　☐ 男

2. 請問您的教育程度為？

☐ 國中以下　　☐ 碩士

☐ 高中、職　　☐ 博士

☐ 大學、大專院校

3. 請問您的就業狀態？

☐ 學生　　☐ 待業中／家管

☐ 就業中（正職／兼職）　　☐ 已退休

4. 請問您的主修或專長是？（若您目前為就讀高中職以下的學生，煩請填「無」，謝謝！）

☐ 法律相關科系　　☐ 其他科系

☐ 資訊相關科系　　☐ 無

5. 請問您的月收入多少？

☐ 未滿新台幣一萬元　　☐ 新台幣六萬元以上，未滿新台幣七萬元

☐ 新台幣一萬元以上，未滿新台幣二萬元　　☐ 新台幣七萬元以上，未滿新台幣八萬元

☐ 新台幣二萬元以上，未滿新台幣三萬元　　☐ 新台幣八萬元以上，未滿新台幣九萬元

☐ 新台幣三萬元以上，未滿新台幣四萬元　　☐ 新台幣九萬元以上，未滿新台幣十萬元

☐ 新台幣四萬元以上，未滿新台幣五萬元　　☐ 新台幣十萬元以上

☐ 新台幣五萬元以上，未滿新台幣六萬元　　☐ 不知道／不方便作答

6. 請問您的年齡？

☐ 未滿 13 歲（請至**第七部分（第 9 頁）**作答）
☐ 13-18 歲
☐ 18-24 歲
☐ 25-34 歲
☐ 35-44 歲
☐ 45-54 歲
☐ 55 歲以上

7. 請問您是否有未滿 13 歲的小孩？

☐ 是（請繼續作答）
☐ 否（作答完畢，如有任何建議，請至最後一頁不吝賜教，謝謝！）

第六部分：兒童隱私權保護與行動應用程式

1. 請問您的小孩在下載行動應用程式前，是否須經過您的同意？

☐ 是（請繼續作答）
☐ 否（作答完畢，如有任何建議，請至最後一頁不吝賜教，謝謝！）

2. 請問須經過您同意的理由，最主要的因素為？（本題為**「單選題」**）

☐ 過濾應用程式的內容
☐ 擔心應用程式須要付費
☐ 擔心應用程式會蒐集小孩的個人資料

3. 請問您在同意小孩下載應用程式前，是否會閱讀「隱私權政策」和「權限清單」？

若您是 Apple App Store 或 Nolia Ovi Store 的使用者，請只要考量是否會閱讀「隱私權政策」即可。

☐ 是（請繼續作答）
☐ 否（作答完畢，如有任何建議，請至最後一頁不吝賜教，謝謝！）

4. 請問「隱私權政策」的內容，影響到您同意小孩下載的程度為？

	1	2	3	4	5	
影響程度非常低	☐	☐	☐	☐	☐	影響程度非常高

5. 請問「權限清單」的內容，影響到您同意小孩下載的程度為？

（若您是 Apple App Store 或 Nolia Ovi Store 的使用者，本題不用作答。）

	1	2	3	4	5	
影響程度非常低	☐	☐	☐	☐	☐	影響程度非常高

第七部分：兒童隱私權保護與行動應用程式

請問您在下載行動應用程式前，是否須經過父母的同意？

☐ 是　　☐ 否

非常感謝您的作答，煩請不吝給予建議與指教。

祝您蛇年順利，事事如意！