

資訊隱私權之重塑——以行動商務為例

林雅惠

摘要

隨著全球無線通訊的蓬勃發展及手機普及率的提昇，結合無線通訊與網際網路的行動網路（mobile Internet）服務成爲最被看好的明星產業，而在行動商務中新興的定位服務（Location Based Service, LBS）——電信業者可透過基地台來確定用戶的所在位置，並將用戶當時所在地點及附近地區的資訊，下載至用戶的手機螢幕上等服務，使得個人資訊於有線與無線的傳輸過程中，無可避免地會暴露於業者手中。本文分爲以下部分探討：1.由傳統對於隱私權界定出發，與美國法上判例及成文法等規定來形塑（architect）現代資訊隱私之內涵：在網際網路社會中，傳統的公私領域分界欲趨模糊，我們所強調的隱私權保護應放在網路社會文化與價值規範的脈絡下討論，方得正確掌握其內涵。2.傳統上對於隱私權侵害的過失賠償機制（liability regime），也逐漸因隱私權的財產化，而將其視爲具有市場價值且可作爲交易客體（property regime），由此資訊所有人由消極被動之地位，轉向積極主張自我控制資料權利，故將隱私權視作財產利益之機制，落實在行動商務的交易中，有其重要意義。3.最後藉由成本分析方法來檢視在定位系統服務的價值鏈中可能會產生個人資訊隱私權侵害之問題，並檢討建議我國電信法、電腦處理個人資料保護法、電信業電腦處理個人資料管理辦法、刑法及其他法規中對於個人電子資訊與隱私權保障之相關規範。

關鍵字：行動商務、定位服務、資訊隱私權、成本分析、電腦處理個人資料保護法

資策會科技法律中心研究員；世新大學法律研究所碩士，2003；yhlin@iii.org.tw。
投稿日：2002 年 11 月 29 日；採用日：2003 年 11 月 14 日

Cite as: 1 Tech L. Rev. 93 (2004)

The Architecture of Information Privacy: Legal Analysis on Location Based Services

Ya-Hui Lin

Abstract

More and more carriers purchase commercial location service solutions from location commerce platform providers that integrate network-based or GPS technologies with applications and content to deliver services to an end-user wireless device. Application providers develop services like news delivery, weather forecasting, restaurant or movie guides, location-based couponing and other commerce-related wireless programming. To match consumers with merchants effectively in the location services environment, application providers may develop a profile of an end-user's interests and then access content sources matching those interests with favorite products. This comment addresses fundamental privacy concerns raised by the Location Based Services (LBS). First, it provides a brief explanation of how location-tracking technology works and describes ways that wireless carriers and non-carriers will use the technology to deliver location-based services. This section also provides a general overview of consumer privacy concerns that flow from using this technology. Second, this comment proposes a solution—a property regime for personal data replaces today's liability regime to

achieve a sound regulatory framework of data protection. Finally, this comment examines the privacy infringement occurred in the value chain of location based services and suggests additional legislations enacted in Telecommunications Act, Data Protection Act, Criminal Act and other related regulations in Taiwan.

Keywords: privacy, Location Based Services (LBS), Telecommunications Act

1. 前言

進入 21 世紀的今天，隨著全球無線通訊的蓬勃發展及手機普及率的提昇，使用網際網路已不再侷限於傳統的有線環境，結合無線通訊與網際網路的行動網路（mobile Internet）服務成爲最被看好的明星產業¹，而隨之引發的行動商務（mobile commerce）交易安全等議題亦值得加以關注。由目前的行動電話、寬頻上網、無線網路，甚或家中的各項家電用品都逐漸具備連網能力，未來網際網路不僅是人與人之間的通道，結合行動通訊的機動性後，這種的生活形態將會深深影響社會領域的架構轉型。

這個新的市場是由行動通信業者（mobile operators），其他服務提供者（service/content providers），與消費者等三個構面所組成，行動業者非僅爲傳統意義上的訊號傳遞者，而應定位爲價值的傳遞者，即將行動網路轉變成爲解決消費者在生活與工作上各種需求的解決方案，亦即一個提供金融、理財、交通、娛樂、資訊等服務的平台，並滿足消費者在現實與精神上的需求²。由電子商務到行動商務，除了市場環境成熟、無線通訊技術改良、高速分封數據服務（GPRS）、第三代行動通訊系統（3G）所擴增的頻寬等因素外，行動商務仍有其困難重重之處，在技術面上，目前尙未建立一個統一的行動通訊標準³，在市場層面上，無線通訊連網的普及率太低，且設備與

¹ 根據美國 Jupiter Communications 於 2000 年底所發布的報告顯示，預估至 2003 年全球使用手機上網的用戶數，將由 2000 年的 110 萬成長到 7,940 萬人。另根據 IDC 市場調查預估，全球行動電子商務營收將自 2000 年的 40 億美元成長至 2005 年的 2,100 億美元的龐大商機。轉引自，楊舜仁，〈行動商務的發展趨勢與個人應用〉〈http://www.efunction.com.tw/info/info_5-2.htm〉（造訪日期：2004 年 2 月 23 日）。

² 黃明珠，〈後行動通訊時代之經營模式〉，《萬國法律》，119 期，頁 46（2001）。

³ 目前行動電話系統爲第二代（2G）系統，如 GSM、CDMA 等，爲無線窄頻（narrow band）系統，另有與 GSM 系統相容之 GPRS（2.5G）作爲邁入第三代行動通訊之過

服務費用過於昂貴，但最重要的因素仍是消費者的信心無法建立——無線交易的安全性考量，這點在電子商務的方案中多依加密、認證等方式處理，而在行動商務中，除結合電子安全交易系統（SET／SSL 機制⁴）與無線上網技術（WAP／WTLS）等技術層面的做法外，但若涉及使用者之個人資料使用，又應如何規範？但此種生活便利性所帶來的隱憂是，使用者必須暴露其詳細的個人資料及所在位置，以回傳至基地台，因此行動商務在發展時如何兼顧網路交易安全與個人隱私權之保護，與消費者接受此種交易模式之意願緊緊相扣。

由於科技發展及智慧型資料蒐集系統的發展，對於隱私權之定義須由傳統上不受干擾的期待，轉向為個人資料利用之充份控制的概念，我們可將資訊隱私權大抵上定義為「個人、團體或機構可自我決定其自身資訊於何時、如何，以及以何種方式被他人知曉」⁵。但於在規範資訊隱私權的工作上，由於今日之資訊具有跨國境的特色，此外更重要的是應如何平衡——個人對於自身資訊之擁有之利益，以及商業團體於獲取或使用個人資料後應給付個人之對價（並應區分自願或非自願性），使得資訊隱私權與傳統隱私權之發

渡。第三代行動通訊標準依國際電信聯盟（ITU）所制訂之 IMT-2000 需具備以下特性：1.行動通信的通信容量與服務品質與固接式網路相同，語音質量與 ADPCM 之 32Kbps 同等；2.實行國際漫遊；3.能提供 2Mbps 的傳輸速率。但其規格提案卻仍未統一，主要有由美國電信產業聯合會（TIA）所提出的 CDMA2000，以及日本無線工商聯合會（ARIB）所提出之 W-CDMA。W-CDMA 可沿用目前歐規 GSM 的無線基地台等基礎設備，而 CDMA2000 則是現階段 CDMAOne 規格延伸，在北美、韓國及大陸較占優勢，但無法與現今採用 TDMA 系統（如 GSM）相容。東名編著，《行動通訊發展》，頁 6-3、12（2001）。

⁴ SSL (Secure Socket Layer) 是由 Netscape 首先發表的網路資料安全傳輸協定，其利用公開金鑰的加密技術 (RSA) 來作為用戶端與主機端在傳送機密資料時的加密協定，包含：1.訊息加解密，2.伺服器識別（運用數位憑證），3.用戶識別（運用數位憑證）。同前註，頁 8-11。

⁵ Kalinda Basho, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?* 88 CAL. L. REV. 1507, 1509 (2000).

展，無論在定義，或適用上逐漸分道揚鑣。

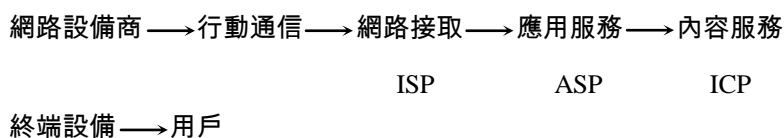
本文擬由傳統對於隱私權界定出發，並美國法判例及成文法等規定一併釐清現代資訊隱私之內涵，藉由成本分析方法，嘗試衡平個人資訊利益與資訊揭露之社會利益。

2. 行動商務之隱私權議題

2.1 行動商務之價值鍊

行動商務乃是利用行動通信裝置，如手機、PDA 等，結合無線通訊與有線網路所進行之商務相關行為，依其應用對象可分為消費者服務與企業服務，但若以其應用層面觀之，大致可區分為⁶：1.通訊，2.資訊，3.個人資訊管理，4.行動消費，5.行動工作。目前 2.5G 技術約可滿足至第 3 層面，而有關第 4、5 層面需整合電腦網路與無線通訊及相關金流與商業服務應用，仍有部分頻寬與技術的限制，目前正在快速發展中。而與電子商務相較下，其具備「移動性」、「即時性」等特性，此外，行動商務以資訊科技（information technology）技術服務作為其基礎，在網際網路部分仍透過 ISP 與固網通信業者接續，適用 TCP/IP 通訊協定，但於無線接續方式，則有不同通訊協定，如 GSM、GPRS、CDMA2000、W-CDMA。

傳統的電信價值鏈中，主要是由網路設備商、行動通信業者及終端設備商所組成，但結合有線與無線的行動通訊價值鏈上則如下圖示⁷：



⁶ 楊舜仁，前揭註 1。

⁷ 黃明珠，前揭註 2，頁 47。

尤其是行動商務中新興的定位服務 (Location Based Service, LBS) 更是電信業者未來的商機所在⁸。電信業者可透過基地台來確定用戶的所在位置，並將用戶當時所在地點及附近地區的資訊，下載至用戶的手機螢幕上。目前如日本 NTT DoCoMo 已於 2001 年 7 月 2 日開始提供 i-mode 用戶一項名為「i-Area」新手機功能，該用戶得透過手機的定位來查詢個人相近的資訊，而國內如中華電信與 GIS (地理資訊系統) 廠商九福科技合作推出行動地圖服務，遠傳電信推出以手機直撥「*131#」或使用 FET WAP 上網查訊之行動嚮導服務，以及台灣大哥大推出 828 隨身美食家服務等⁹。這些定位服務根據所使用技術可分為：1.網路，2.GPS。前者是透過行動基地台來確定用戶位置，而後者是使用衛星定位系統 (Global Position System)¹⁰，目

⁸ 以 GPS 定位服務為例，預估到 2005 年將會達到每年 600 億元營收。*Wireless World Will Drive GPS Application*, NEW ALLIED BUSINESS INTELLIGENCE STUDY BUSINESS WIRE (Dec. 13, 2000).

⁹ 陳世運，〈行動定位系統服務熱潮登場〉，Find，2001 年 9 月 12 日，<http://www.find.org.tw/trend_disp.asp?trend_id=1181>。

¹⁰ GPS 是由美國國防部發展出的 24 顆距地表 20,183 公里高空的衛星群，以 55 度等角均勻地分布在 6 個軌道面上，並以 11 小時 58 分的週期環繞地球運轉所組成的全球衛星定位系統 (Global Positioning System, GPS)，在每一顆衛星上都載有位置及時間訊號，只要用戶端裝設 GPS 設備，無論何地都可接收到至少 5 顆衛星的訊號。GPS 定位系統是利用衛星基本三角定位原理，GPS 接受裝置以量測無線電信號的傳輸時間來量測距離。由每顆衛星的所在位置，測量每顆衛星至接受器間距離，即可算出接受器所在位置之三維空間座標值。使用者只要利用接受裝置接收到 3 個衛星信號，就可以定出使用者所在之位置。一般的 GPS 都是利用接受裝置接收到 4 個以上衛星信號，來定出使用者所在之位置及高度。

目前 GPS 接受裝置定位的精度，利用差分定位 (differential) 技術其精度可達到 2-5 公尺左右，甚至可達到更精確之定位。現在全球計有 5 個地面衛星監控站，負責傳送衛星瞬時常數 (Ephemeris Constant) 及時脈偏差 (clock offsets) 之修正，讓衛星能及時提供接收器使用者更精確之定位運用。這些地面衛星監控站，分布於瓜加林島、科羅拉多泉、夏威夷、亞森欣島、底亞歌加西亞等地。在各種應用範圍中，通信手機 (cell phone) 定位系統市場方面，未來如能將 GPS 定位系統功能加入或是融入通信手機之中，提高通信手機應用功能，使通信手機也具有定位功能。對於找尋

前國內電信業者多採取行動基地台定位方式，但如中華電信與九福科技合作推出之行動地圖服務，則是採用 GPS 定位技術，配合 GIS 電子地圖即可得知用戶的位置¹¹，本文僅以行動基地台定位技術為討論範疇。

2.2 定位服務之隱私權侵害

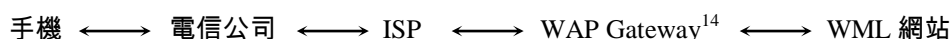
定位系統的價值鏈中，由上圖中之行動通信業者，網路接取業者，應用開發公司及設備供應商皆是此服務成功的關鍵。根據電信產業顧問公司 Ovnm 估計，到了 2005 年，全世界會有 12 億的行動電話使用者，其中約有 4 億 5 千人會使用某種類型的定位服務¹²。當電信業者利用正在興起的全球衛星定位服務（GPS），即不需透過國外當地的電信業者來找到自己用戶位置所在，但以網路為基礎的定位技術，則漫遊協定是不可或缺的，無論如何，電信業者知悉用戶的所在地，各種行動商務的機會便隨之而來。而在定位服務中，若為用戶主動申請者，則其定位資訊之控管及法律爭議，會直至行動電信業者為契約約定外使用時才產生；但若是業者主動發送廣告之情況，會涉及用戶是否願意接收手機上傳遞的廣告或其他資訊（若是業者主動發送廣告），與用戶是否願意暴露自身位置此二問題，前者較單純，可透過降低費率等方式事前與用戶協議，提高其接受程度，此可能涉及財產權侵害；惟後者，關於用戶位置之資訊取得，一方面這是定位服務之前提，另一方面，獲得此資訊並不限於行動通信業者，尚包括網路接取業者（ISP），

人員位置之定位，及提供如滑雪者、健行者、大自然愛好者及登山者利用 GPS 定位系統功能找到目的地及回家之最短路徑。美國政府相關單位計畫在 2001 年 10 月 1 日後，將所生產之通信手機全面具有 GPS 定位系統功能，此計畫對於通信手機及 GPS 定位系統製造業者將是一個未來商機。安守中，《GPS 全球衛星定位系統入門》，頁 50-53（2002）。

¹¹ 電子地圖搭配全球定位系統之服務，目前國內的九福科技與康訊科技有此類產品問市，九福科技公司〈<http://www.geoinfor.com.tw>〉（造訪日期：2004 年 2 月 23 日）。

¹² 高秀美，〈正視行動電子商務安全問題〉，Cnet 〈http://www.nii.org.tw/cnt/ECNews/ColumnArticle/article_138.htm〉（造訪日期：2004 年 2 月 23 日）。

其流程如下圖¹³：



而安全性的考量，除了在無線設備與基地台間，亦應包括由基地台與交換中心連接實體網路層上的安全。但 WAP 的網際網路接取管道，卻有一個潛在的弱點，就是當 WTLS（用以確保無線設備與 WAP 閘道間連接的協定¹⁵）轉換到連接 WAP 閘道跟網路伺服器的 SSL 協定，其保護便終止，亦即所有的加密資料到了 WAP Gateway 都會被再還原一次，無法做到點對點的加密¹⁶。

在定位服務中，用戶個人資料因無線與有線的傳輸過程，無可避免的會暴露在電信業者及網路接取業者手中，有學者就將這種定位技術戲稱為「電子狗標籤」（digital dog tags）¹⁷，其實不難理解個人定位資訊即是個人生活習慣的相互對照，例如在網路上透過消費者所瀏覽的網站、購買的商品、訂閱的雜誌，已可側寫出一個消費者的電子足跡（electronic footprints），進而追溯以得知其生活品味、興趣及思想，而定位服務所產生的憂慮正和此點相同，除了行動電信業者可能會根據個人定位資訊來寄送出許多個人化廣告外，更值得我們關注的是個人定位資訊若洩露給第三人，如其他市場商人、司法部門、雇主甚或犯罪者時，所造成的隱私權侵害將會被擴散，而可能戕害了我們的其他生命、自由、財產或工作的基本權利。在個人隱私權的規範

¹³ 東名，前揭註 3，頁 8-10。

¹⁴ WAP Gateway 閘道器，用以連結兩種不同協定的設備，在兩者間作協定的轉換，以搭起無線與有線的橋樑。

¹⁵ WTLS 為 WAP 協定中的安全機制，提供傳輸層（Transport Layer）以上的資料安全防護，即是將 SSL 延伸到無線通訊的環境下。

¹⁶ 在 WAP1.2 版後已改善此缺點。

¹⁷ Keith Perine, *Talking About Wireless Privacy*, THE INDUSTRY STANDARD (2000).

面上，究應如何保障，實為資訊時代裡的重大挑戰，以下以美國法為例，先針對資訊隱私之學說及法院實務發展作介紹，以為我國立法之借鏡。

3. 資訊隱私權之發展

3.1 資訊隱私權之意義

何謂隱私權？隱私權作為法律上之權利乃始於 1890 年 Warren 和 Brandeis 所著 *The Right To Privacy*¹⁸ 該文中，將隱私權界定為「不受干擾」，其文義應包含被刺探或揭露之干擾之排除，與其他生活干擾行為之排除，然其定義過於抽象，而學者 Ken Gormley 針對美國歷史上隱私權法之觀察，所得出 4 點隱私之文義上的界定或可有助於吾等對於隱私權概念的進一步掌握及分析¹⁹：1. 個人性格或特質之表達，即界定其為人類特質之權利。2. 個人自治權，即形成個人擁有思想、行動與決定之自由。3. 規範自身資訊及控制與其他人交往之能力。4. 秘密，匿名與獨處。而以上四種界定方式是無法截然分開觀察，因個人在上述第三種界定中，決定去公開自身資訊——重點在於控制資訊——必然會反映出其個人特質與得識別之外觀，因而會牽涉到第一種界定；而若為強迫性公開資訊，則會損及其個人自決權，則涉及第二種界定方式。

傳統上所討論之隱私權與現今資訊時代所探討之隱私權，有何相異之處？本文需先作前提性的解釋：在過去，儘管我們個人的出生紀錄、教育紀錄、就醫紀錄、保險單紀錄、買賣紀錄等是可被知悉或散布的，但若要將這些資料完整蒐集的過程卻是繁瑣且複雜的，或許也僅有政府可負荷此等高成本的事務，然而在網路化的社會中，我們每日均將自己的紀錄以電子化足跡散布各地，因而我們所需擔憂的不僅是隱私權受侵害的問題——消極防禦面

¹⁸ Warren & Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890).

¹⁹ Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1408 (1992).

向，更應注意的是我們對於自身資訊的自我決定權已慢慢喪失——積極主動面向²⁰。這乃是網路社會本身之特性所致：1.表達特殊性：網路傳播方式易於傳統人際傳播方式，而有其特殊之表達符號或指令。2.匿名性：網路之虛擬空間使得使用者，得以暱稱或代號相互聯繫交往。3.跨國性：由於網路網網相連，使得網路服務具有全球性之性質。4.自治性：虛擬世界之生活評價及管理，多賴網際網路公民的自治及自律。5.普及性：網路使用者即為網路資訊提供者，普及接近使用（universal access）為各國資訊基礎建設（National Information Instruction, NII）之一個基本目標²¹。一百年前 Warren 和 Brandeis 為隱私權辯護時，曾經警告「無數的機械設備預示著，將來有一天，我們在密室中的低語，將會如同在屋頂大聲宣告般。²²」而於科技匯流的今日，我們所面臨的隱私權議題已超越數十年前的形態²³，不僅因平台（platform）的差異（今日的資訊隱私權侵害多是透過網際網路，其與傳統之實體侵害不同，故如 Prosser 所歸納之四類形態是否得繼續適用，抑或網際網路社會應自行發展一套標準？）所造成隱私權侵害之即時性及廣泛性，更重要的是個人對於自身資訊的主動掌控能力。

所謂「資訊隱私權」，有認為乃指：「非侷限於不讓他人取得我們的個人資訊，而是應該擴張到由我們自己控制個人資訊的使用與流向」，亦有認為其意義在於「在沒有通知當事人並獲得其書面同意之前，資料持有者不可

²⁰ Joel R. Reidenberg, *Restoring America's Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771, 774 (1999).

²¹ 劉靜怡，〈網路上資訊隱私權保障問題之研究〉，〈<http://www.cyberlawyer.com.tw/alan4-0801.html>〉（造訪日期：2004年2月23日）。

²² Ellen Alderman & Caroline Kennedy 著，吳懿婷譯，《隱私的權利》，商周出版公司，頁439（2001）。

²³ 1960年 Prosser 就美國眾多判例及學說中，整理出四種隱私權侵害的態樣：1.侵入原告的獨處，2.公開原告難堪的私人事實，3.令原告受到錯誤的公眾印象，4.為被告的利益，自原告姓名或其他處獲利。William L. Prosser, *Privacy: A legal analysis*, 48 CAL. L. REV. 383, 389-407 (1960).

以將當事人爲某特定目的所提供的資料用在另一個目的上」²⁴。資訊隱私權的核心概念在於個人掌握資料之產出、利用與查核權利，且爲該個人資料的使用範圍的參與決定者。在此概念上，資訊隱私權與傳統隱私權用以對抗國家對於私人之隱私侵害，亦即一消極防禦性質不同，其特徵在於已具有積極請求權的性質，此種明白告知及參與決定的個人資料支配權，正是現代個人資料保護制度的最重要機制之一²⁵。

3.2 美國法院判例之發展

隱私權並非美國憲法上之明文，在當初制憲之際，制憲者也難以想像到現代高科技的通訊設備，如行動電話、筆記型電腦，甚至全球電腦網路對於現代人之日常生活是如此息息相關吧！因此我們所必須面臨的迫切問題是：在數位時代裡，我們應如何保障資訊隱私權以維護個人自治權？

美國聯邦法院首先於 1973 年 *Roe v. Wade* 案²⁶中引發隱私權本質的討論，指出隱私權不僅指個人資料的控制，亦包括個人發展上重要決定的自主。而嗣後 1977 年的 *Whalen v. Roe* 案²⁷更是資訊隱私權上最重要之判決，

²⁴ 劉靜怡，前揭註 21。

²⁵ 同前註。

²⁶ *Roe v. Wade*, 410 U.S. 113 (1973).

²⁷ *Whalen v. Roe*, 429 U.S. 589 (1977). 本案涉及 1972 年紐約州議會所通過之藥物控制法（*New York State Controlled Substances Act of 1972*），該法為加強控制同時流通於合法市場與非法市場之藥物，規定關於最危險藥物之處方，應用紐約州特別印製的官方表格，該表格並要求載名開具處方之醫師，提供該藥物之藥局，藥物名稱及藥量，與病人姓名、地址及年齡。這些資料一份交由紐約州健康部門，並輸入電腦處理保存 5 年，5 年後表格被銷毀，病人資料禁止公開，且只有有限的州健康部門官員或調查人員得接觸這些資料。於聯邦地院提起本案之原告為一群經常接受前述第二類最危險藥物的病人及開具這些藥物的醫師，其主張紐約州 1972 年藥物控制法追蹤接受第二類藥物病人之規定違憲。聯邦地院基於「醫師與病人關係為憲法保障之隱私權範圍所及」，以及該範圍確因紐約州 1972 年藥物控制法對於第二類藥物所採取「不必要而過於廣泛」的病人追蹤規定所受侵害，禁止受原告質疑之條款的執行。但美國最高法院則是推翻這項地院判決。轉引自，陳起行，〈資訊隱私權法理探討

Stevens 大法官針對藥物控制法可能侵犯憲法所保障之「隱私範圍」(zone of privacy) 提出兩點看法：其一，避免公開個人事務的個人利益——在新法執行期間，並無任何經驗可以證明有不當揭露的事實，且將這些資訊揭露於州健康部門，並不足以自動構成對於個人隱私之侵害。其二，獨立做出某種重要決定的利益（追蹤使用危險藥物病人的做法是否會影響病人就診之決定）——藥物控制法並未阻卻大眾接觸這些藥物，且未要求州官員或第三者參與診療，在合法的藥量內，藥物之使用全權由醫師與病人決定，故病人獨立決定的權利並未受損。故本案涉及之州政府在個人資料的處理上展現了適當之保護，並無必要決定無理揭露 (unwarranted disclosure) 的問題，而不足以構成侵害憲法第 14 條修正案對於任何權利或自由的保護。此外 Brennen 大法官也指出，本案判決不及於所有個人電腦資料檔案之使用，如建立個人素描 (personal profile) 及電腦紀錄比對 (computer matching) 則非本案判決範圍所及。而另位 Stewart 大法官在不同意見書中也強調，無憲法上的隱私權，只有憲法所保障的個人隱私區域，這些區域與個人住家，個人間之親密關係有密切關聯²⁸。美國聯邦法院嘗試在「個人隱私權利利益」與「個人資訊公開之公共利益」間所作的權衡測試法 (Balancing Test)，亦在嗣後的資訊隱私權案件中被多加適用。

在 *Nixon v. Administration of General Service* 案²⁹中，法院重申 *Whalen* 案之權衡測試法，認為本案中保存爭議資料的公共利益大於原告保存個人資料之利益。但此後，聯邦最高法院並未對資訊隱私權做出任何說明，只留給地方法院去決定如何在個人隱私權與公共利益間劃下一條分界線。

另外在 1999 年美國聯邦第九上訴巡迴法院針對 *United States v. McIver*³⁰，無搜查令之放置 GPS 追蹤裝置 (GPS-based tracking device) 所引

——以美國法為中心》，《政大法學評論》，64 期，頁 316-317 (2000)。

²⁸ 同前註，頁 319-320。

²⁹ *Nixon v. Administration of General Service*, 33 U.S. 425 (1977) .

³⁰ *United States v. McIver*, 186 F.3d 1119, 1126-1127 (9th Cir. 1999) .

發違反第 4 修正案之隱私權爭議，該法院認為該裝置是放在被追蹤者的汽車底盤下，而底盤是屬於汽車外部範圍，故這部分並無合理的隱私權期待，不構成第 4 修正案之搜索或扣押。

然由上述美國法院判例觀察，均僅限於禁止政府對於人民隱私權之違法侵害，但人民受其他私人或團體之隱私權侵害往往是更嚴重的。而於許多案例中，法院的態度卻表示，個人對於其銀行來往紀錄、電話號碼，及其他受第三人持有之個人資訊，並無合理的隱私權期待。例如在 *United States v. Miller* 案³¹中，法院並不傾向將憲法上之隱私權保護擴及金融紀錄，判決中指出，本案中顧客瞭解到將其財務交易紀錄向銀行公開，乃是為了享受銀行之服務，依此，顧客對於其金融紀錄並無一合理之隱私權期待。故在以上案例中，銀行顧客若為自願性揭露其金融紀錄，則其需承受洩露於第三者之風險³²。

而當網際網路成為普遍的媒介時，對於網際網路上的隱私權是否受到憲法保障，則仍是個問題，但在網際網路的時代中，我們已將許多個人資訊於公共領域中公開，只是其公開形態有所不同，例如透過電話交談的內容是受到憲法保障³³，但銀行之金融交易紀錄卻並未受到保護，這種歧異的保護在科技匯流下勢必會受到極大的挑戰³⁴。

³¹ *United States v. Miller*, 425 U.S. 435 (1976) .

³² 美國國會隨即於 1978 年制訂了金融隱私法 (Financial Privacy Act)，對於聯邦政府機關接觸銀行內個人帳戶資料有詳盡規定，但不及於私的環節。除少數州法對於銀行業個人資料的隱私保障有規定外，銀行業的自治規定亦為保障個人隱私之重要依據，並且重視客戶銀行內個人資料之保障漸成為銀行業者競爭上之利器。陳起行，前揭註 27，頁 330。

³³ 例如：帕序利等人訴北方電信公司案——1998 年北方電信公司那什維爾電話裝備製造工廠的員工發現他們的雇主一直都在竊聽他們，834 名員工以侵犯聯邦及州法律為理由（包括侵犯隱私權）向公司提起訴訟，本案於 1992 年 6 月和解，北方電力公司同意支付 20 萬美元作為賠償 (*Parish et al. v. Northern Telecom, Tennessee* 1992)，*Alderman & Kennedy*，前揭註 22，頁 437。

³⁴ 在電信資訊傳播科技匯流後，我們可利用網路電話與他人交談，亦得從事買賣，銀

3.3 美國立法之發展

儘管美國法院試圖透過判決、判例去形成隱私權之類型，但法院仍跟不上資訊發展的腳步，以及因此所亟待解決的個人資訊保護等議題。近來，美國立法嘗試在政府與私人間所擁有資料的規範間，以及法人對於其顧客及雇員所擁有之資料的規範間，做出分界，但一來美國資訊隱私之聯邦法律主要規範聯邦政府，不及州及私人企業，再者美國資訊隱私立法欠缺全盤規劃，一致適用各個環節，亦為值得詬病之處。故對於美國資訊隱私規範模式之理解，包含聯邦法律、州法律、普通法、工業自治，以及公司內部之行事規則，均應作動態的整體性觀察³⁵。

1974 年聯邦隱私法（The Privacy Act of 1974）是第一個美國國會所通過之隱私保護法案，對於聯邦政府處理及使用個人資料規範十分詳盡，也建立一隱私保護觀察委員會（Privacy Protection Study Commission）針對該法之個人隱私保護作定期之觀察與報告。而 1986 年電子通訊隱私法（The Electric Communication Privacy Act, ECPA）主要是針對網路監聽（聲音訊息）以及電子郵件（非聲音訊息）之隱私權保護。ECPA 對於公共傳播系統中之聲音訊息（voice message）傳遞提供了最佳的保護，即傳播系統的提供者不能於用戶間互相交談時故意介入干擾，也不能檢查用戶之間於交談後儲存於傳播系統中之內容。因此，依 ECPA 之規定，ISP 業者似乎對網路電話的用戶不論於線上交談時或訊息靜態儲存時均不可自行加以監聽。而針對非

行或票據等交易之電子商務行為，此時的平台（platform）已非如傳統形態可以分割以觀，則法律應如何分別規範？

³⁵ 美國資訊隱私立法主要針對政府部門，而私環節部分則由少數聯邦特定立法、州法、普通法，乃至於公司內規及工業自治等多重管道動態地發展，如 1977 年美國最高法院有關資訊隱私的 *Whalen* 案判決也並未授與任何憲法上的權利。*Whalen*, 429 U.S. at 323. 而這項規範哲學的核心在於政府只有在競爭不平衡時才介入，但於有限政府之原則下，其介入並非干涉，而是協助私人方式以及個人選擇的發展，使得隱私的價值及保護得以實現。FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* 129 (1997).

聲音訊息 (non-voice message)，即是指電子郵件檔案、文字或圖形的傳輸、以文字傳輸為主的 BBS 站交談區，或是 Internet 的即時交談區。而 ECPA 在此即規定除非系統管理者與網路使用者間有事先的約定，否則針對正在傳輸的非聲音訊息，系統管理者不能介入，但是若已經處於儲存的狀態，網路的系統管理者可以檢查，而所謂的儲存狀態包含了儲存於系統管理者電腦中等待存取及用戶之間私人對談的紀錄，因此 ECPA 並未賦予網路用戶就處於儲存狀態訊息保有隱私的權利，但是原則上他們不得將所見到的訊息交與第三人，除非是執法單位，但是仍有例外，網路系統管理者必須於閱讀訊息之後，有足夠的理由相信違法的活動正在進行，才得將訊息展現於執法單位，而執法單位所能檢查的訊息之限度，也只及於確定系統管理者所產生疑問的範圍。

此外，1988 年電腦比對及隱私權保護法 (Computer Matching and Privacy Act of 1988) 主要是針對「例行使用」³⁶問題——蒐集個人資料之目的與其使用目的之間是否相當之判斷，涉及行政效率之判斷以及個人隱私權之保護，故本法規定需設資料正直理事會 (Data Integrity Board)，並要求於資料比對後，如欲對個人採取不利行動前，必須經過獨立之查證。

在 1996 年美國電信法第 222 條中亦明文規定³⁷：「關於消費者資訊的隱私權保護，電信業者 (telecommunications carrier) 有義務去保護關於消費者之私人資訊的隱密性。」電信法中針對電信業者在蒐集消費者私人網路資訊 (The Consumer Proprietary Network Information, CPNI) 後之使用、公開，有嚴格的限制，而 CPNI 包括了個人位置、發話目的地、電信服務使用量及個人其他相關資訊等³⁸。並於 1999 年經無線通訊及公共安全法

³⁶ 依據 1974 年美國隱私法規定，政府機關官員則不得向他人或其他機關公開個人紀錄，除非係例行使用。例行使用係指：就公開某項紀錄而言，其使用之目的與原先蒐集之目的相同。

³⁷ 47 U.S.C. 222(a) (2000).

³⁸ 47 U.S.C.222(c)(1) (2000).

(Wireless Communications and Public Safety Act, WCPSA)³⁹的增補，包括 CPNI 之定位資訊的解釋，乃指「任何電信服務的顧客在使用一個訂購的電信服務時所產生的資訊，包括數量 (quantity)、技術結構 (technical configuration)、種類 (type)、目的 (destination)、位置 (location) 以及使用的總數 (amount) 等」，而業者僅可因為與顧客之間的業務關係 (carrier-customer relationship) 而利用這些資訊。資訊包括了顧客所收到的那些由電信業者所發送之電信局服務或長途電話服務帳單；但 CPNI 不包括訂戶的名單資訊 (subscriber list information)⁴⁰。並明訂電信服務提供者在公開或使其他人知悉用戶之位置資訊前須經其事前同意授權 (express prior authorization)，但對於該程序並未有詳細規定，故 FCC 近來已開始制訂相關「合理使用定位資訊準則」(fair location information practices)⁴¹。

由於無線通訊及公共安全法第 222 條中規定，電信業者在使用 CPNI 之前必須獲得顧客的同意，或由顧客書面 (written) 指定資訊揭露的對象⁴²，究該事前同意授權之方式為何，法條中並未有詳細規定，故按 FCC 所發布之第二版 CPNI Order (Second Report and Order and Further Notice of Proposed Rulemaking)⁴³，FCC 決定採用 opt-in 方式來作為業者獲得顧客同意的機制，規定業者在使用顧客 CPNI 之前必須以書面、口頭同意或利用電子設備方式獲得顧客的預先同意後才得以使用顧客的 CPNI。但在後續的 *U.S. West v. FCC* 一案中⁴⁴，針對 opt-in 方式⁴⁵是否違反業者所受憲法第 1 修

³⁹ Pub. L. No. 106-81, 113 Stat. 1288-1289 (1999).

⁴⁰ 47 U.S.C. §222(h)(1).

⁴¹ Comments of Cingular Wireless, LLC, In Matter of Cellular Telecommunications Industry Association's Petition for Rulemaking To Establish Fair Location Information Practices (Apr. 6, 2001), <<http://gullfoss.fcc.gov/cgi-bin/websql/prod/ecfs/comsrch<uscore>v2.hts.Last>>.

⁴² 47 U.S.C. §222(c)(2).

⁴³ 47 C.F.R. pt. 64, subpt. U (1998).

⁴⁴ *U.S. West, Inc. v. Federal Communications Commission, And United States Of America*,

正案保障之爭議則廣泛討論，在本案中 FCC 主張其僅禁止上訴者利用 CPNI 挑選顧客而非妨礙上訴者與顧客通訊或限制上訴者與顧客談話的內容，但法院認為，有效率的言論有兩個構成要素：說者與聽者。只要是對要素中任何一方作限制，就是限制言論。因此法院認為 FCC 的 CPNI 管制限制了言論，並且認為業者利用 CPNI 促銷是一種商業行為，因此認定 FCC 的管制違反商業言論自由。法院將 FCC 的 CPNI 相關條例視為對商業言論的規範並說明，即使是電信業者內部言論，只要不直接涉及商業交易行為，一樣算是商業言論，也因此適用第 1 修正案的保護範圍。

4. 資訊隱私權再檢討

由隱私權發展之歷史觀之，Warren 和 Brandeis 在其論文中點出了「不可侵犯的人格」作為隱私權所保障之價值，其乃根植於人性尊嚴的要求，惟於其論述中隱私權僅限於不被揭露的權利，其作用十分被動。再由美國判例及立法以觀，由 1965 年 *Griswold* 案、*Roe* 案及 *Whalen* 案以來，美國聯邦最高法院藉由投影理論（penumbra approach）將隱私權明確界定為憲法保障之基本權利，並將自主性導入其中，肯認個人對於自身事物的最終決定權（*Whalen* 案），在立法上也從保障消極的不被揭露，進而保障個人的資訊自主權，個人對於政府和他人所持有的資訊享有一定之控制權，其目的不僅在於保證資訊之自主性，更使個人成為可以掌握資訊流通的主體。

惟資訊隱私權與傳統概念下之隱私權其保護之目的是否同為維護人性尊嚴？此外，無論是傳統概念或現代資訊社會之隱私權侵害（或資訊掌握自主權），均會涉及公開之公共利益與不公開之個人利益的權衡必要，或可借用

182 F.3d 1224 (10th Cir. 1999).

⁴⁵ Opt-in 機制強調業者必須在顧客確實被告知後取得顧客預先同意才得以使用顧客的 CPNI。相反的即是 opt-out 機制，業者得以採用各種通知方式通知顧客 CPNI 的使用，在經過一定回覆期限後，若顧客未回覆 opt-out 通知，則代表顧客同意授權業者使用 CPNI。

美國聯邦最高法院在 *Whalen* 案中所作的權衡測試法之嘗試，以尋求隱私權之平衡。最後，在隱私權侵害類型上，因科技發展致使平台產生差異，是否仍得適用古典的侵害類型分類標準？抑或有形成網路社會自身分類標準之必要，而其內涵如何？

4.1 資訊隱私權保護之目的

首先，我們需試圖來回答一個問題：為何社會賦予個人、法人或團體去決定其自身與他人間之溝通交往（何時、如何，及以何種內容）之權利⁴⁶？這個問題對於隱私權的探討具有極大意義，究竟隱私權即為其價值本身，或是其為達到其他目的之工具性手段？學說上，亦大致可分為這兩種看法，即隱私權是一種基本權利，與隱私權是一項工具性權利。

前者，如 Warren、Brandeis、Bloustein 及 Blackmun 等人，他們將隱私權看做人格權，自由或人性尊嚴之一部分，而後者，如 Westin、Gavison、Fried 及 Rubenfield 等人，他們視隱私權為一種方法，用以達成其他目標，這些目標包括民主社會之維持、個人之社會參與、個人之自我調適，以及對於國家權利之限制等。由於此種工具性的看法，隱私權的價值依附在其所欲成就之目標上，且基於此等目標之達成，隱私權若與其他價值產生衝突時，則得退讓⁴⁷。

以上兩種說法均有其理論基礎，亦反映了隱私權的價值及功能，但就前者之主張由康德對人的看法——人為自身的目的——之理論，故在公私的區別上，個人領域為目的，公共領域為達成個人目的之工具，而不應該反過來支配個人領域。但單純之隱私是沒有意義的，如同 Cate 所說的：「過度對隱私權的要求似乎只是種臨床精神病的表徵⁴⁸。」因為社會用以保護隱私之

⁴⁶ See CATE, *supra* note 35, at 23.

⁴⁷ 詹文凱，《隱私權之研究》，台灣大學法律研究所博士論文，頁 174（1998）。

⁴⁸ “In fact, the obsessive quest for privacy has been called a symptom of clinical neurosis.” Cate, *supra* note 35, at 44.

利益是反映在社會利益所欲達成之結果本身，而非隱私上。隱私權確實為個人尊嚴之展現，但若非作為達成其他目標之手段，隱私權之意義將蕩然無存。此外，在資訊隱私權上，公私領域的界限難以繼續維持，我們無法用實體空間作為劃分的界限，網路社會所創造出來的虛擬空間，應由其自身特性所形成之社會價值與文化規範來創造新的境界⁴⁹。

故將隱私權視為一工具性之權利似較妥當，而其目的在促使其他更高的價值達成——促進「尊重、愛、友誼及信賴」⁵⁰，以下我們可由兩個面向——價值與成本——來檢視隱私權的內涵（以資訊隱私權為討論對象）⁵¹：

4.1.1 價值

若將隱私當作達成其他目的之手段，則其扮演之角色為何？資訊隱私對於個人及團體等之價值又是如何？

1. 自治

自治在作為隱私權之價值上是十分重要的，因隱私對於個人發展是不可或缺的。若我們沒有機會與自己的思想或情感獨處，則我們如何從事思維工作？而此種私人空間的需求，以帶動個人發展、觀念，及意見的形成，乃是民主制度的前提要件。

2. 由公共領域中之解放

隱私權對於個人之所以重要的原因在於，其提供了情緒紓解的機會，使得個人的一舉一動可以跳脫出公共的注視，自由地宣洩其憤怒，悲傷，挫折及其他的情緒反應，而無須擔心可能帶來的後果。

3. 自我評價與自我決定權

隱私帶來了個人獨處的機會，而這對於創造是十分重要的，因為個人需

⁴⁹ Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 557-561 (1998).

⁵⁰ Charles Fried, *Privacy*, 89 YALE L. J. 373, 475-477 (1980).

⁵¹ See Cate, *supra* note 35, at 24-30.

要時間及空間來檢視評價其所面臨與接收到的各項資訊，而深思熟慮後再決定其應採行的適當行為，在這個過程中，個人也能對於自身的價值——由所接收的私密對話到一般公開的行為、對話等資訊——重新評估。

4.有限且受保護的溝通

因個人需要與其所信賴之人分享秘密事務，並藉由分享的程度來建立與他人間之親密關係，因而隱私權提供了個人在與他人溝通之際，得以暢所欲言其所思所感。

4.1.2 成本

在現代社會中，隱私權是生活品質中重要的構成因素，無論是對個人或團體，皆需支付相當的成本，如同 Richard Posner 所說的：「隱私資訊的需求來自於兩方面，一方面是要刺探資訊的一方，這些人需要獲得個人資訊以供對個人評斷之依據，另一方面則是需利用誤導的資訊來進行交易⁵²。」由經濟學的角度觀之，對於個人資訊之揭露需要成本，則相對取得資訊即為效益，故隱私應為一種權利，然隱私的市場價值如何，應交由市場法則來決定。例如個人提供個人資料給業者時，該業者以告知蒐集該筆資料乃為郵寄特定名單為目的，則業者為獲得該筆資料所提供給當事人之對價——即為成本，則雙方在交易中所獲得之利益必然大於所付出之成本（否則交易不會成立），故此筆交易乃是對於資源作了有效率的利用。然與市場交易無關之隱私，如家庭，婚姻或子女關係等身分關係，則與經濟利益無關，惟其涉及或與交易目的牽連時，如第三人向夫或妻請求財產上給付，則此時夫妻婚姻關係存續與否則與市場交易有牽連關係，此種個人資訊之揭露即具市場價值。此外，應釐清的一點在於，個人對其資訊之控制目的並非在於商業價值，而是個人主體之表現，因隱私權縱作為一工具性權利，為其欲促成之目標仍為信賴、自尊、愛與友誼，而人性尊嚴為隱私權之發展內涵，非其保護目的本

⁵² Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 397 (1978).

身。

儘管隱私權具有上述的利益，但可能會擾亂社會結構。它一方面承認了個人擁有隱私權，則必然在決定是否揭露自身資訊時會侵害他人的權利。故隱私權無可避免的會面臨社會中許多重要利益的相互衝突，例如言論自由、私人財產保護、犯罪處罰及政府行政效率等問題。舉實例來說，我們在商店中以信用卡消費，若政府為保護個人隱私權而不許商家持有客戶相關的信用卡資料，則對於我們來說是相當不方便的，但若透過顧客主動且自願提供相關資料的機制，則可解決這些問題；因而在生活中，快速的信用交易、郵件傳送，或透過電話網路的郵購及無數便利的生活形態，均是因為犧牲了某程度的隱私權所致。

隱私權並非一絕對的概念，並非絕對的有利或有害，其價值可能因所欲達成之目標而深遠或細微，例如：對某人資訊未揭露之隱私權保護，可能使不適任之人獲得一份工作，則對於該人來說是具有價值的，但相反地對於整個社會而言是花費成本。又例如，隱私權可保障個人不受垃圾郵件的干擾，但對於某些人而言，可能會因接收這些郵件而受到經濟上的利益。因此隱私權之價值或成本並非絕對的截然可分，個人的隱私權利益可能與他人或社會之其他利益衝突，甚至與其自身的他種利益衝突。而美國聯邦最高法院試圖在 *Whalen* 案中建立的權衡測試法⁵³，即先檢視是否有實質侵害之效果，若無則政府可被推定無隱私權侵害之行爲，若有實質侵害效果，則需進一步檢視是否有迫切之政府利益，得以爲合憲之理由；然而這種個案式的利益衡量方式仍未提供我們一套檢驗標準，因此我們仍應回歸隱私權本質的探求，並

⁵³ 在 *Whalen v. Roe* 案中，Brennen 大法官僅指出，本案由於政府在處理個人資料上持嚴謹態度，對於所蒐集的個人資訊有很周全的保護，政府因此不必證明受指責的法律（藥物控制法）是控制藥物濫用所絕對必須。但若政府之法律確實有侵害之效果（a statute that did effect such a deprivation），則該法必須有助於政府迫切利益才合於憲法之規定。*Roe v. Wade*, 410 U.S. 113 (1973); *Eisenstadt v. Baird*, 405 U.S. 438, 464 (1962).

將資訊隱私權與傳統隱私權做出區隔觀察，才能確實尋找出解決的途徑。

4.2 資訊隱私權保護之形塑

由隱私的角度加以觀察，資訊技術對於隱私可能會構成的威脅同時存在於對人民資訊的取得，以及取得資訊後不當之使用或再處理，而由積極面觀察，資訊隱私權應包括：1.個人資料的取得及蒐集，2.個人資料保存，管理及利用，3.個人資料之閱覽，訂正請求權。因而將資訊隱私權歸於侵權法上之範疇已有不足，如同 Lawrence Lessig 所言：「網路上隱私權的威脅有兩類，第一種是如何定義有效的侵入（efficient invasion）？第二種是如何定義監視（monitoring）？由於科技的發展，在區分搜尋與監視界限已日趨模糊⁵⁴。」因而隱私權之概念，可分為消極意義與積極意義。前者強調個人私生活事務不受恣意公開干擾之權利；後者則是個人資料控制支配權，亦即賦予個人對其個人資料之蒐集利用發動權、停止權、內容提示權、更正權等；換言之，個人對於其個人資料應有主動積極控制支配之權利。而關於個人資訊之內涵及外延約可歸納如下四種⁵⁵：

1.個人屬性的隱私權（Privacy of a Person's Persona）

如一個人的姓名、身分、肖像、聲音等，由於其直接涉及個人領域之第一層次，而可謂「直接」之個人屬性，為隱私權保護之首要對象。

2.個人資料的隱私權（Privacy of Data about a Person）

當個人屬性被抽離成文字之描述或紀錄，如個人的消費習慣、病歷、宗教信仰、財務資料、工作、前科等紀錄，若其指涉之客體為獨一且個人化（unique and personal），則此等資料即含有高度之個人特性而常能辨識該個人之本體，此可謂「間接」之個人屬性而亦應以隱私權加以保護。

3.通訊內容的隱私權（Privacy of a Person's Communications）

⁵⁴ Lawrence Lessig, Code and other laws of cyberspace 150 (1999).

⁵⁵ Thomas F. Smedinghoff, Online law 269-270 (1996).

個人之思想與感情，原本存於內心之中，不易為人所辯識；惟當與外界藉由電子通訊媒介（如網路）溝通時，即易於暴露於他人之窺探之下，故此通訊內容亦應加以保護，以助成個人人格之完整發展。

4. 匿名之隱私權（Anonymity）

匿名發表在歷史上一直都扮演著重要的角色，這種方式常可以保障讓人願意對於社會制度提出一些批評。畢竟，群體生活中，集體之價值未必與個人之想法相符，此種落差常易引發個人以匿名方式表達其意見之需求。此種匿名權利之適度容許，常能鼓勵個人之參與感，並保護其自由之創造力空間；而就群體而言，亦常能藉由自由表達，而獲得進步之動力。

隨著社會轉型，傳統上以個人尊嚴為概念的隱私權逐漸模糊在公私領域重疊的界限上，亦即原本透過社會文化的規範所形成之界限，卻因科技的特性打破了以物理空間為據的概念，正如哈伯瑪斯在其著作「公共領域的結構轉型」序言中指出：「隨著電子媒體的興起，娛樂與訊息的不斷交融，所有的領域趨於集中化，……具有操縱力量的傳媒褫奪了公眾性原則的中立特徵，大眾傳媒影響了公共領域的結構，同時又統領了公共領域⁵⁶。」因而在新興科技的生活中，網際網路自身特性所形成的社會價值與文化規範恰另建構了新的界限，如 Lessig 主張應形塑（architecture）一套屬於網路文化的規範，他認為對於隱私權保護的觀念應該逐漸揚棄過去以賠償機制（liability regime）為中心的思想，而以財產機制（property regime）的觀念取代。賠償機制需當事人對故意過失及損害因果關係負舉證責任，另一方面受損害之隱私權價值通常僅限於一般理性之人所應受賠償之額度，但隱私權常帶有一情感上連結（a sentimental attachment），受侵害者之隱私權價值是主觀的，以一般客觀合理經驗判斷並不妥當。然若引入財產機制，係將個人隱私權視為可交易之客體，交易雙方可透過事前的約定明確地訂出雙方的權利義務，其特徵在於協議（negotiation），賦予當事人對於其資訊的控制權及價值決定

⁵⁶ 哈伯瑪斯，《公共領域的結構轉型》，頁 15（1999）。

權，於此隱私權所內含之自治與價值決定權亦同受保障，並且透過市場機制的手，使得雙方均可達成其合理且滿意交易（at a price that makes neither party worse off）⁵⁷。現今的賠償機制僅止於保護事後的交易安全，而財產機制卻預先賦予當事人選擇權，不僅可使隱私權的主觀價值受到較佳的保障，另可降低事後無盡的訴訟紛爭數量。而在適用財產機制上，並非對於所有的私人資料皆有保護，例如涉及不實或對他人產生損害等資訊則不在此限；並且財產機制的採行，在技術層面需確保透過當下網際網路或行動通訊的平台，交易當事人雙方具備合理可期待的協議環境（透過機器為之，非人與人間實體接觸而為協議），且隱私權可有效受到保護，則此機制方有落實之可能。

5. 我國定位服務之隱私權相關立法檢討

在定位服務中，用戶個人資料因無線與有線的傳輸過程，無可避免的會暴露在電信業者及網路接取業者手中，在個人隱私權的規範面上，應區分為資料儲存，與資料利用兩方面。對傳輸安全性之維護及相關責任歸屬，依照電信法第 6 條：「……電信業者並應採適當並必要之措施，以保障其處理通信之秘密。」按電信事業分為第一類電信與第二類電信，故行動通信業者自受電信法規範，而 ISP 為第二類電信事業，亦受規範。而電信法第 6 條所謂「適當且必要措施」乃是一不確定法律概念，其內容非明確即可理解，且若電信事業怠於為該義務，或其防止措施不足防止損害發生，該用戶除經契約求償外（舉證上不易），電信法上並無明訂違反之相關罰則（對於電信業者似無其他行政或刑事上之處罰）。以下就電腦處理個人資料保護法（以下簡稱個資法）之相關規定介紹⁵⁸：

⁵⁷ See LESSIG, *supra* note 54, at 160-161.

⁵⁸ 關於定位資訊之利用責任上可能涉及刑法第 318 條之 1，及民事上契約責任與侵權責任，惟本文僅就電信相關法規部分處理。

5.1 事前

行動商務中用戶之資料無可避免地會受到業者掌握，依個資法第 18 條：「非公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之：一、當事人同意。二、與當事人有契約或類似契約之關係而對當事人權益無侵害之虞者……」若依本條，是否用戶與電信業者簽訂租約後，即可推定用戶放棄其個人資料的控制與利用？此點與前述美國判例中針對銀行金融紀錄，客戶為享受銀行之服務，則對其金融紀錄無合理的隱私權期待之立論相近，蓋於租用契約中關於用戶資料處理部分，應屬於民法第 153 條第 2 項非必要之點，未經表示同意者，推定契約成立。

5.2 事後

然該租用契約之成立並非即可正當化業者對於個人資料之使用，因用戶對於其自身資訊有一財產上利益（業者得就用戶所在位置傳送消費者鄰近之資訊與廣告）。

5.2.1 資料儲存

針對個人資料儲存部分，於個資法中並未課與非公務機關一保存及維護義務，但依電信業電腦處理個人資料管理辦法第 12 條第 1 及 2 項則明訂電信業者有一維護保存個人資料檔案之義務，並於個人資料檔案之安全維護計畫標準中，明文個人資料建檔，設定密碼與製作使用紀錄；個人資料應儲存於軟式磁碟片上並定期拷貝；非經允准不得刺探或使用個人資料；以及個人資料檔案使用完畢，不得留在電腦終端機上。但可參考美國電子通訊隱私法中，針對聲音及非聲音訊息為不同的規範，尤其是針對 ISP 系統管理者介入或檢查之程序，以及資料儲存之期限等，宜增修於本條第 2 項之個人資料檔案之安全維護計畫標準中。此外本辦法第 10 條中規定用戶得向電信業者為確認個人資料存在，請求製給副本，請求補充或更正，請求停止電腦處理或利用，以及請求刪除之權利，且上揭權利不得預先拋棄或以特約免除，此正

符合個資法之立法目的，在於避免人格權受侵害，並促進個人資料之合理使用。

5.2.2 資料利用

依個資法第 6 條規定，個人資料之利用需尊重當事人權益，不得逾越特定目的之必要範圍。故雖用戶已同意使行動業者知悉其所在位置，並藉此發送相關廣告資訊，但該同意僅限於特定目的之必要範圍，即定位服務上，故若行動業者將用戶之位置資訊蒐集並作其他用途者，則逾越個資法第 6 條之特定目的及必要範圍之限制。於此，個人資訊並不因業者所提供之對價（較低之電話費率）而產生耗盡，故若未經當事人第二次同意，意圖為自己或第三人不法之利益或損害當事人權益，對於個人資料為非法輸出、干擾……行動通信業者及 ISP 業者需依個資法第 34 條，處三年以下有期徒刑，拘役或科新台幣 5 萬元以下罰金。此外，若有違反個資法其他規定，致當事人權益受損者，電信業者亦應依個資法第 28 條負損害賠償責任。

6. 結論

21 世紀以來，電腦及通訊技術發展及社會轉型，人與人之間的相互關係也隨著科技發展而愈形緊密，網際網路無國界，表現特殊性、普及性及其即時廣泛性的特色，也使得傳統的公私領域分界欲趨模糊，我們所強調的隱私權保護亦應放在轉型社會的脈絡下討論，方得正確掌握其內涵。而傳統上對於隱私權侵害的過失賠償機制（liability regime），也逐漸因隱私權的財產化，而將其視為具有市場價值且可作為交易客體（property regime），由此資訊所有人由消極被動之地位，轉向積極主張自我控制資料權利，此正符合資訊隱私權的中心思想：個人不僅是個人資料產出的最初來源，也是其正確性、完整性的最後查核者，以及該個人資料的使用範圍的參與決定者。

而藉由價值釐清與成本分析，資訊隱私權不宜再視為最終利益，毋寧只是為達成其他目標之工具性手段，但其所內含之自治，情緒紓解，自我價值

與決定權，以及溝通限制與保護之價值，仍為人性不可侵犯性之延伸，衡量其與社會上其他利益之關係，而可做出退讓。最後，資訊持有或產出人之隱私權保護，與公共利益之間的權衡，雖由 Whalen 案中是否可以是否具迫切政府利益為斷，惟此種不確定法律概念之適用仍較模糊，就網路社會文化與價值形塑一套規範實有必要，而將隱私權是作財產利益之機制，落實在行動商務的交易中，有其重要意義，將隱私權交由當事人與業者間協議，不僅可真正彰顯出隱私權的價值，亦符合隱私權所欲追求的自治及自我決定的價值，最重要的是能與網路發展的精神相符。

參考文獻

中文書籍

- ALDERMAN, ELLEN & KENNEDY, CAROLINE 著，吳懿婷譯，《隱私的權利》，商周出版公司（2001）。
- 安守中，《GPS 全球衛星定位系統入門》，全華科技出版公司，頁 50-53（2002）。
- 哈伯瑪斯，《公共領域的結構轉型》，學林出版社譯，頁 15（1999）。
- 東名編著，《行動通訊發展》，文魁資訊有限公司（2001）。
- 詹文凱，《隱私權之研究》，台灣大學法律研究所博士論文（1998）。

英文書籍

- AGRE, PHILIP E. & ROTENBERG, MARC, TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (1997).
- CATE, FRED H., PRIVACY IN THE INFORMATION AGE 150 (1997).
- LESSIG, LAWRENCE, CODE AND OTHER LAWS OF CYBERSPACE (1999).
- SMEDINGHOFF, THOMAS F., ONLINE LAW (1996).

WANG, YU-CHI, *PRIVACY IN THE COMPUTER AGE: ISSUES RELATED TO COMPUTER MATCHING AND THE INTERNET* (1997).

中文論文

- 林發立，〈行動商務與交易安全〉，《萬國法律》（2001）。
- 徐鳳美，〈行動商務行不行〉，《網路通訊》（2002）。
- 黃三榮，〈行動商務（Mobile Commerce）之法律入門〉，《萬國法律》（2001）。
- _____，〈W-CDMA：行動商務（M-commerce）基盤之一〉，《萬國法律》（2001）。
- 黃明珠，〈後行動通訊時代之經營模式〉，《萬國法律》（2001）。
- 陳志遠，〈行動 IP 網路之四大應用〉，《網路通訊》（2002）。
- 陳起行，〈資訊隱私權法理探討——以美國法為中心〉，《政大法學評論》，64 期（2001）。
- 劉瑞華、林福興，〈電子商務的交易成本分析〉，《產業論壇》，3 卷，1 期（2001）。
- 簡榮宗，〈網路業者處理個人資料的法律須知〉，《網路通訊》（2002）。

英文論文

- Basho, Kalinda, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?* 88 CALI. L. REV. 1507 (2000).
- Fried, Charles, *Privacy*, 89 YALE L.J. 373 (1980).
- Gormley, Ken, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335 (1992).
- Posner, Richard A., *The Right of Privacy*, 12 GA. L. REV. 393 (1978).
- Prosser, William L., *Privacy: A legal analysis*, 48 CAL. L. REV. 383 (1960).
- Reidenberg, Joel R., *Restoring America's Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771 (1999).
- Renenger, Aaron, *Satellite Tracking and the Right to Privacy*, 53 HASTING L.J. 549 (2002).
- Schauer, Frederick, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555 (1998).
- Traupman, Ellen, *Who Knows Where You Are? Privacy and Wireless Services*, 10 COMMLAW CONSPECTUS 133 (2001).
- Warren & Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890).

其他

- 吳建興，〈m-Commerce 安全嗎？從 WAP 的安全性談起〉，〈http://www.find.org.tw/trend_disp.asp?trend_id=1167〉。
- 高秀美，〈正視行動電子商務安全問題〉，〈http://www.nii.org.tw/cnt/ECNews/ColumnArticle/article_138.htm〉。
- _____，〈行動電子商務之起飛時機〉，〈http://www.nii.org.tw/cnt/ECNews/ColumnArticle/article_145.htm〉。
- _____，〈Mobile EC 成功之道——確立消費模式與安全機制〉，〈http://www.nii.org.tw/cnt/ECNews/ColumnArticle/article_132.htm〉。
- 陳世運，〈行動網路發展現況初探〉，〈http://www.find.org.tw/trend_disp.asp?trend_id=1163〉。
- _____，〈第三代無線通訊面面觀〉，〈http://www.find.org.tw/trend_disp.asp?trend_id=1165〉。
- _____，〈行動定位系統服務熱潮登場〉，〈http://www.find.org.tw/trend_disp.asp?trend_id=1181〉。
- _____，〈GPRS 應用服務驅動行動上網市場〉，〈http://www.find.org.tw/trend_disp.asp?trend_id=1180〉。
- 楊舜仁，〈行動商務的發展趨勢與個人應用〉，〈http://www.efunction.com.tw/info/info_5-2.htm〉。
- 劉靜怡，〈網路上資訊隱私權保障問題之研究〉，〈<http://www.cyberlawyer.com.tw/alan4-0801.html>〉。