

電子商務個人資料保護法制之研究

陳仲麟

2001/6/12

第一章 前言.....	1
第二章 電子商務與個人資料保護概說.....	1
第一節 電子商務概說.....	1
第一項 電子商務之意義.....	1
第二項 電子商務之類別.....	2
第三項 電子商務之發展概況.....	3
第二節 隱私權與個人資料保護概說.....	4
第一項 隱私權之意義與發展.....	4
第一款 隱私權概念之發展.....	4
第二款 隱私權的定義.....	4
第三款 隱私權在憲法上之地位.....	6
第二項 個人資料權之形成與確立.....	7
第一款 個人資料權之形成.....	7
第二款 個人資料權之意義及內涵.....	8
第三款 個人資料權在憲法上之地位.....	10
第三節 電子商務與個人資料保護之聯繫.....	11
第一項 電子化、網路化之特徵 - 以個人資料保護為中心之發掘.....	11
第二項 電子商務對個人資料的需求性.....	12
第三項 國家在電子商務中個人資料保護問題之角色扮演.....	13
第四項 個人資料保護法制之形塑.....	14
第三章 不同層次資訊處理之個人資料保護問題.....	16
第一節 個人資料之取得層次.....	16
第一項 網路新興技術所產生的特殊取得可能.....	16
第二項 個人資料蒐集之目的拘束.....	17
第三項 限制蒐集之思考.....	17
第四項 對我國法制之檢視.....	18
第二節 個人資料之利用層次.....	20
第一項 個人資料之限制利用.....	20
第二項 對我國法制之檢視.....	21
第三節 個人資料之儲存管理層次.....	21
第一項 安全保護問題.....	21
第二項 完整正確及個人參與問題.....	23

第三項 對我國法制之檢視.....	24
第一款 安全保護問題.....	24
第二款 完整正確及個人參與問題.....	25
第四節 個人資料之傳遞層次.....	25
第一項 個人資料之流動.....	25
第二項 對我國法制之檢視.....	26
第四章 不同性質資訊內容之個人資料保護問題.....	28
第一節 敏感性資料之析出.....	28
第二節 對我國法制之檢視.....	29
第五章 監督及救濟制度之設計.....	29
第一節 監督及救濟制度作為規範實現之確保.....	29
第一項 監督制度.....	29
第二項 救濟制度.....	30
第二節 對我國法制之檢視.....	31
第一項 監督制度.....	31
第二項 救濟制度.....	34
第六章 結論.....	36

第一章 前言

隨著網路科技的突飛猛進，電子商務也迅速地成為非常熱門的議題，但在電子化、網路化的環境，以及電子商務對個人資料的需求性之下，個人資料保護的問題就相當值得重視。而現實上也發生不少個人資料洩漏的案例，引起許多討論。本文希望能藉著理論與現行法的探討，為相關問題盡一點拋磚引玉的微勞。

個人資料保護措施除了法律的制度規範外，可能還有業者自律、教育使用者、使用科技裝置等等面向，但本文在範圍上限縮於法制層面，對其他方面較無法顧及，這樣的切割或許並非妥適，但限於能力和篇幅只得從權；另外，本文只討論關於「國內」個人資料保護問題，跨國性的個人資料保護其實也是非常重要而待研究的領域，但同樣限於能力及篇幅只有割捨，合先敘明。

關於本文架構，第二章先就電子商務、個人資料保護的概念作說明，並將二者相連結，本文的問題點及此一問題的討論價值，在此也就呼之欲出了；第三章則探討不同層次資料處理當中，個人資料保護的問題，應遵守什麼樣的原則，並檢視我國電腦處理個人資料保護法的規定；第四章則是涉及「不同資料內容」是否應使國家受不同拘束之問題；最後，要使上述規範得以實現，必須要依賴妥善的監督及救濟制度設計，此部份將在第五章論及。

第二章 電子商務與個人資料保護概

說

第一節 電子商務概說

第一項 電子商務之意義

所謂電子商務，目前尚無一致性的定義，一般而言，電子商務係整合了網路通訊資料庫管理以及安全防護等新技術，以支援商業流程及商品、服務的交換為目的，是網際網路全球資訊網或其他加值網路上的商業交易應用，可提供商品及服務的線上資訊傳輸、交易與支付功能；Zwass 將電子商務定義為：「藉由通訊

網路以分享企業資訊、維持企業關係並執行企業交易。」¹Kalakota 及 Whinston 亦稱：「普遍的用法，是將電子商務用來泛指利用今日的電腦網路，或是明日即將由無數網路所組成的所謂資訊高速公路（Information Superhighway），來銷售和購買資訊、產品、服務等行為。」²

由這樣的定義我們可以分析出，電子商務係為追求降低成本，增進商品及服務的品質，加強服務提供效率的「商務」目的，在現代科技進展下應運而生的產物，而其所採取的手段，主要就是「電子化」和「網路化」二項概念；所謂電子化，係指將既有的非電子程序，搬移到電子的平台上，以減少紙上作業，利用電腦的強大功能處理資訊，以增加內部的業務處理效率；所謂網路化，係透過電腦與電腦的連結，促進資訊的流通，進一步增進企業流程最佳化、生產流程自動化的效果，並且利用網際網路，蒐集、傳遞資訊，與消費者或其他事業達成更佳的互動。因此簡單地說，電子商務顧名思義即「電子」及「商務」兩項要素所組成，而此處所稱「電子」，其實指涉「電子化」及「網路化」兩項概念。

第二項 電子商務之類別

上述定義的說明其實仍然十分抽象，以下藉由電子商務類別的概略敘述，希望能對電子商務能有稍微具體一些的認識：³

1. 顧客對企業（Consumer-to-Business）：任何商號或企業皆可在網際網路上建立自己的網站及電子商務經營網頁，直接與來自世界各地的客戶或供應商進行交易，不受時間與空間的限制。一般消費者或企業型客戶也可以經由網路查詢、訂購商品、取得服務，並透過交易及支付機制付款，直接下載電子化商品或經由傳統及新興物流通路取得實體貨品。
2. 企業組織內部（Intra-Business）：企業組織內部的電子商務機制則以組織及作業通訊為主，如銷售點、總公司間的銷售、訂購及促銷訊息傳遞，部門間各類電子文件之瀏覽與交換，員工間溝通討論及電子會議，群體工作流程管理等。
3. 企業對企業（Business-to-Business）：企業與企業間的電子商務機制則以企業策略聯盟整體營運網路的交易執行與資訊流通為主，如零售、物流、製造等產業間的供應鏈管理，以及與金融業連線之電子資金移轉作業等。

¹ 余千智等，電子商務總論，1999.4，頁 2-3，台北，智勝（1999/4）

² Ravi Kalakota & Andrew B. Whinston 著，查修傑、連麗真、陳雪美譯，電子商務概論，頁 2，台北，紅螞蟻（1999/6 二刷）

³ 余千智等，電子商務總論，1999.4，頁 3-4，台北，智勝（1999/4）

第三項 電子商務之發展概況

電子商務的興起雖只是近幾年的事，但對全球經濟和社會的衝擊卻是相當深遠。由於這項革命性的改變，使得企業的經營可以更有效率，社會大眾可以在任何時間、任何地點進行消費，整個國家的經濟活動因而可以更為活絡。除了說電子商務的交易金額，發展潛力將是相當驚人外，電子商務對經濟發展的最大貢獻，應該是在於其對企業經營面所產生的衝擊，經由效率的提升，企業的競爭力可以大幅改善，因而促進整體經濟的成長。因此，各國政府都紛紛採取政策措施，來促進電子商務的發展。

網際網路的源起是在美國，加上美國政府在 1993 年開始的國家資訊基礎建設（National Information Infrastructure；NII）計劃下對電子商務的大力推動，使得電子商務的發展也是以美國最為盛行。而為了不讓美國專美於前，以及體認到電子商務的發展對整個經濟可能產生的重大貢獻，OECD 組織中的其他國家如日本、歐盟國家、紐西蘭、澳洲也都在政府的推動下，快速發展。⁴

我國在電子商務的發展算是比較慢，就網際網路的使用來說，自從一九九四年我國「國家資訊通信基本建設推動方案」（NII）開始推動以後，網路化的議題逐漸發熱，電子商務亦在網路潮流的趨勢中開展。而除了民間的自行摸索開拓外，此一新興領域的發展也特別需求各項條件的配合，例如政府的扶助、市場開放程度、相管法制的健全化等等，因此國家扮演的角色即相當重要；在我國 NII 計劃中亦將「協助企業應用電子商務」作為一重點，並曾於一九九八年十一月在 APEC 會議中提出「中華民國電子商務政策綱領」，說明我國推動電子商務的原則與措施，也參與 APEC APII 連網及電子商務之跨國合作計畫⁵。相關制度與措施勢必持續浮現，電子商務的發展正方興未艾。

⁴ 參照曾銘深，國際間推動電子商務之作法探討，http://www.moea.gov.tw/~ecobook/season/sag5_2/sag2-a5.htm（2001/4/26 瀏覽）；關於各國電子商務發展另可參照何全德，Internet 電子商務發展現況，http://www.find.org.tw/oriineews/focus/ec_trend/main.htm（2001/4/26 瀏覽）；林芬柔，日本電子商務推動政策及市場發展概況，http://www.find.org.tw/trend_disp.asp?trend_id=1120（2001/4/26 瀏覽）

⁵ 關於我國 NII 發展現況，參照 NII 專案推動小組，NII 發展現況，<http://www.nii.gov.tw/status/develop.htm>（2000/2/27 瀏覽）；關於我國政府推動電子商務的計畫，參照經濟部商業司，E.Commerce 網際網路商業應用計畫，<http://www.ec.org.tw/co-2.asp>（2000/2/27 瀏覽）；關於我國電子商務政策綱領，參照經濟部國貿局，中華台北電子商務政策綱領，http://www.moeaboft.gov.tw/impt_issue/impt_6/ec-rept-1.htm（2000/2/27 瀏覽）

第二節 隱私權與個人資料保護概說

第一項 隱私權之意義與發展

第一款 隱私權概念之發展

隱私權的概念，原本並不存在於傳統西方思想中，在實務偶有使用此一名稱時，亦未見對其概念有任何說明。真正將隱私權當作一項獨立概念加以探討者，應始於一八九一年 Harvard Law Review 上刊載之 The Right to Privacy 一文，二位作者 Warren 和 Brandeis 於文中從習慣法上對誹謗和著作權相關的規範，導引出個人對於因其情感表達而成的文書和作品有決定是否公諸於世的權利；並界定隱私權為「生活的權利」(right to life)和「不受干擾的權利」(right to be let alone)，內容為個人對其自身事務公開揭露的決定權利，其所保障的是個人的「思想、情緒和感受」。在界限上，則指出「公共利益」和「同意」是兩項主要限制。這許多論點對後來的實務和學說至今仍有相當之影響⁶。

對於隱私權的概念發展和內容，如果以美國法院的判決為主要觀察對象，可以歸納出以下的面向：⁷

A 個人空間隱私權：包含個人的物理空間和心理空間不受侵擾的權利。具體言之，有搜索扣押、侵入住宅、噪音、強迫收聽收看等議題。

B 資訊隱私權：包含個人資料和通訊不被揭露的權利。具體言之，在個人資訊方面有個人肖像、聲音、過去經歷（尤其犯罪記錄）、醫療記錄、財務資料、一般人事資料、犯罪被害人資料、招致誤導的情節等課題；在通訊隱私權方面有測謊、郵件、通話等面向的討論。

C 個人自主性隱私權：即個人私生活的自我決定權，包含生育、家庭和個人切身事務等三方面之自主權。具體言之，生育自主性包括避孕、中止懷孕、懷孕和生育、強制絕育、代理孕母等議題；家庭自主性包括子女教養、結婚與離婚、家庭關係等方面的議題；個人自主性包括性行為、猥褻行為或物品、藥物使用、個人形象、個人姓名、自殺和安樂死等方面的討論。

第二款 隱私權的定義

隱私權是個面貌相對尚未明晰的權利，學者採取的解釋可謂百家爭鳴，莫衷

⁶ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 13,19 (1998.7)

⁷ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 47-121 (1998.7)

一是，本文則選擇以下的定義：

隱私權是對個人領域的事務（即隱私）的控制權

對這項定義簡單說明如下，即它的主體是個人；客體是個人事務；作用則是控制，也就是個人對其自身事務的掌控和自主。

首先，主體是人，由於個人間彼此是獨立而平等的，所以各自享有一定活動空間，其生活型態和內容不致與他人完全重疊。即使再親密或密切的兩人間，仍存在有互相不能支配的部分。又，在此所指的人應是自然人，因為自然人有情感和理性，需要國家保障其情感之安定、生活之追尋和價值尊嚴的維持。至於法人，一方面它是擬制的，非實存的，所以難以想像它會有情感或精神上的需求，另一方面，法人的組成、目的、業務和所產生的作用，與公眾均有密切關係，人們組織法人在於遂行某種公共目的，即使是以營利為目的的公司，其設計也是為了使更多人能夠參予經濟活動、規避市場風險（想想公司許多資訊反而要求公示，應可顯現其公共性）。法人也有秘密，但秘密並非就是隱私，國家機密所欲維護的是國家社會的存續，營業秘密所欲維護的是對於生產技術的投資和持有者的交換利益，這些都是屬於公共領域內的事務，而非在突顯和保障「個人」的差異和尊嚴。

其次，隱私權的客體是「個人領域的事務」也就是「隱私」。所謂私人領域，是個人生活中與公眾無關的部分，是個人追求自我發展和實踐自我理念的領域，包括對其自我的認知、自我形象的建立、生活的形成、生命目標的尋求等，是個人生活中實質的、終極的及目的性的部分，由個人的價值、情感和自我認知所支配。「私人領域」與相對的「公共領域」之界分，和 Mill 的「涉己的」與「涉他的」十分接近，其說明亦可作為我們判斷的工具，Mill 主張的是，個人的行為不涉及自身以外之他人的利益，即涉己的部分。但人際的關聯甚為複雜，個人的一舉一動在情感上、好惡上、利益上常會影響他人，所以 Mill 又認為「所謂只影響本人者，是指其影響為直接的、最初的」。進一步要說明的，個人領域除了是個人在參與公共領域時偶爾抽身的避風港，更重要的是，它是個人參與公共事務的目的，公共領域的決定，目的在於提供成員更好的條件以遂行其個人領域的生活。若不是如此，公共領域的決定將脫離了成員利益，成為漫無目的的機器，甚至危及成員原有的個人領域，使個人喪失獨立存在的價值。

最後，隱私權的作用「控制權」，指對個人領域事務的自我決定的資格和能力。個人可以將自身事務開放，使他人或公眾知悉、參與，也可以封閉其個人領域，排除他人或公共權利的介入或支配。這種選擇的權利是個人對其自身事務處理的權利。賦予個人控制的權利，便是讓個人可以決定在何時、何地、何種程度下，何人可以知悉或參與其自身事務的部分，以便維持個人的獨立和不受支配。這種自主和控制的意思可以表現在下面的例子中：在侵入住居的情形，隱私權所保護的是屋主對其住居所的控制權，而非單純的安寧、隔離狀態，否則在住宅內舉行宴會時有人闖入，就沒有造成隱私權侵害；又如在個人資訊情形，如果蒐集和第一次揭露構成不法侵害，按照控制的定義，自第一次揭露而取得個人資訊者

仍不能將取得之資訊再為揭露，因為不論是第幾次揭露都是侵害個人對其自身資訊的控制權。

上述的定義，幾乎已將隱私權的概念提昇至與近代關於自由的理解相當的境界，為何採取如此廣泛，涉及所有個人事務的概念？原因在於隱私權的意義自發展初始至今，一直圍繞著不受干涉、不受支配的原則，保障居家生活免受侵擾、個人形象免受利用、個人資訊免受揭露、個人特定行為免受干涉；在這些事務表象背後，均隱含個人對其生活、自身事務的自主、控制的欲求，因此隱私權真正的意義，應是對於此一自我控制的欲求的承認。只有給予個人完整的控制權，才能通盤理解，為何這許多看似無關的議題都被納入隱私權範疇中。⁸

第三款 隱私權在憲法上之地位

隱私權的根據，也就是主張保護隱私權的理由，主要就在於個人尊嚴的理念。所謂的人性尊嚴，意指每個人均應有作為人的尊嚴，受國家的尊重和保護。其核心內容有二：一、人本身即是目的，不得被要求或視為一種工具（物體）或手段，人若被物化，自然無尊嚴可言。二、人得以自治（律）自決，不應處於被操控的他治（律）他決的地位，一個人在權利行使的正當範圍內若乏自治自決的機會，人亦將喪失其尊嚴⁹。由這樣的原則可以分析出，個人是目的，是有尊嚴的存在，而自主是這項存在的基礎。自主、自治或自決等概念相對於被支配、宰制，和「以個人為目的」的原則相呼應，成為個人尊嚴的基礎。而由於每個人自主的個體，均不受他人之干涉，所以個人僅就自己的事務有自主的權利。公共事務是公眾共同的事務，非個人自身的事務，所以個人沒有單獨決定的權利。這樣的結論正好和前面所定義的隱私權 對個人領域內事務的控制權相符合。可以證明隱私權即是自主的權利，是人性尊嚴不可缺少的基礎¹⁰。

我國憲法並無如德國基本法般以人性尊嚴作為權利保障基礎的明確規定，但近年來或許受到外國憲法思想之影響，增修條文和實務上均出現人性尊嚴之文字。例如憲法增修條文第十條第六項：「國家應維護婦女之人格尊嚴，保障婦女之人身安全」釋字第三七二號解釋：「維護人格尊嚴與確保人身安全，為我國憲法保障人民自由權利之基本理念」釋字第四 號解釋：「俾能實現個人自由、發展人格及維護尊嚴」釋字第四九 號解釋：「服兵役之義務，並無違反人性尊嚴亦未動搖憲法價值體系之基礎」可見人性尊嚴的理念在我國亦已受到承認，而可以之作為統合個人自由權利的基本精神。故而，隱私權就可以在我國憲法上找到存立的基礎。

⁸ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 137-162（1998.7）

⁹ 參照陳清秀，憲法上人性尊嚴，收錄於現代國家與憲法，頁 94；李震山，論資訊自決權，收錄於現代國家與憲法，頁 719。

¹⁰ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 190-193（1998.7）

接下來的問題是，承認隱私權為憲法保障的權利，是將隱私權當作一項個別的基本權利，或者是統括諸多自由權利的指導性概念？從人性尊嚴加以引申，個人享有參與公共決策的權利和決定自己事務的自由，後者即為隱私權的意涵，故隱私權是以許多自由權利的上位概念方式存在，基本上它應是解釋和適用各項自由權利時的指導原則，而非單一的權利，又由於憲法上所明定的自由權利並不窮盡個人事務的範圍，所以隱私權的概念又具有補充的具體化權利的性質。因此在方法上，就不宜自憲法第二十二條尋求隱私權的保障，而可採美國聯邦最高法院在 Grisword 案中的方式，藉各項自由權利保障的內容和範圍，交織成為一個貫通各項自由權利的「隱私區域」。例如在同性戀的問題上，憲法雖未予明文保障，但自人身自由、居住自由、思想自由、秘密通訊自由、生存權等，應可推出個人感情和家庭生活方式應受尊重的結論，進而得出同性戀行為是個人自主的範圍，非國家權利所能干涉¹¹。

第二項 個人資料權之形成與確立

第一款 個人資料權之形成

盜取他人關於其個人之秘密而加以公開之情形，在向來隱私權之領域內，本屬隱私權侵害之一種，但在自動化資訊處理方法革新以後之今日，隱私之概念發生變動，以往未必稱得上秘密、保護需求性較弱的個人資料，已可認為包含在隱私權的範圍中。蓋在資訊社會，任何掌握資訊工具之人，均很容易地無須得該資料關係人之同意而取得其個人資料，同時，亦無須經該關係人之同意而極其便捷地予以保存、流通、使用或銷毀，尤有進者，資訊業持有關於他人隱私之資料，不但早已不屬資料關係人同意與否之問題，反而已經是可能知悉他人是否有關於其自己隱私資料與否的問題，如此，在今天若未能對於自動化資訊處理體系予以相當之法律上規範，則個人因此而遭受的隱私權損害，自當遠較往昔之隱私權侵害更為複雜而且深刻，同時隱私權之理論方面，若未能針對自動化資訊處理之革新從事因應之改變與充實，則所謂隱私權之保護，自屬有名無實¹²。

亦且，由於一般人對電子媒體的個人隱私權，在意識型態上甚為薄弱；而資料處理者任意擷取窺視或組合他人資料，用以滿足個人之好奇心或私人需求卻不以為杵；復以有權蒐集、管理個人資料之權利者，僅持超平常心看待大量的個人資料而不加以尊重。在此三極化交相影響下，透過電腦特有之快速精確的分析比對處理技術，使得個人資料所受侵害程度日益加深。即便是以匿名之方式為個人

¹¹ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 285-286（1998.7）

¹² 相關說明參照翁岳生等，資訊立法之研究，行政院研究發展考核委員會委託研究，頁 39-40（1994/7）

資料之處理，在現今之資訊處理技術水準下，表面上無法破壞之匿名性，已可經由簡單之程序重新擬人化；經由相關資訊之附加，個人同一性重建之界限被繼續地降低，建立每個人廣泛且仔細之概像 - 亦即個人人格之剖面圖 - 並使個人形同「透明人」成為可能¹³。

個人資料是否應予保護？如果應予保護法律上如何應對？凡此問題並非電腦問世之後才發生之問題，但不可否認地，電腦的使用使此等問題之發生更形頻繁，加害程度更形深刻、廣泛¹⁴。就在上述資訊處理的特性與發展下，個人資料保護問題愈行受到重視，個人資料權亦於焉浮現。

第二款 個人資料權之意義及內涵

要了解個人資料的意義，首先必須掌握何謂「個人資料」。所謂個人資料或稱個人資訊，根據學者Raymond Wacks所下的定義，係指「有關於個人的事實、通訊和意見，被合理地期待為私密的或敏感的，因而對於它們的收集、使用或流傳會想加以阻止或限制。」¹⁵德國「聯邦個人資料保護法」第二條之定義為「關於特定或得特定之自然人屬人或屬事之個別資料。」¹⁶歐盟1995資料保護指令第二條定義為「指有關識別或足資識別自然人（資料當事人）之任何資訊；足資識別之人指直接或間接能予識別者，特別是以參考識別號碼或以其身體、生理、精神、經濟、文化或社會屬性之一項或多項特定因素。」¹⁷美國一九七四年隱私權法 a 條第四款對「紀錄」(record) 的定義為「有關一個人之任何單項性、累積性或集合性之資料，包括但不限於其教育、財務處理、醫療過程，及犯罪或職業經歷等，並包括其姓名、識別號碼、象徵或其他個人之特定表徵，諸如一手指指印、聲音音帶，或一張照片等資料在內。」¹⁸我國「電腦處理個人資料保護法」（以下簡稱個資法）第三條第一款之定義為「自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」

故從我國規定出發，兼採例示規定較純粹的抽象規定為佳，但所謂「足資識別該個人之資料」則有欠明確，語意上似在表明須有證明個人身分之作用，而有一點語焉不詳，尤其在一些新興的個別資料未在條文列舉之列者，例如E-mail信

¹³ 葉淑芳，行政資訊公開之研究 - 以隱私權益之保障為中心，中興大學法研所碩士論文，頁 144-145 (1999/7)

¹⁴ 參照朱柏松，個人資料保護之研究 - 近代隱私權概念之形成與發展 (上)，法學叢刊，一一四期，頁 75；朱柏松，資訊時代的新權利 - 個人資料權，中信通訊，一八一期，頁 93 (1991/9)

¹⁵ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 65 (1998.7)

¹⁶ 德國「聯邦個人資料保護法」的中譯，參閱林錫堯譯，德國聯邦個人資料保護法，法學叢刊，三十六卷四期，頁 1-18。

¹⁷ 歐盟 1995 年資料保護指令之中譯，參照熊愛卿、詹文凱合譯，歐盟 1995 年資料保護指令，收錄於熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，附錄 (2000/7)。

¹⁸ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 65 (1998.7)

箱、domain name網域名稱等，是否屬於應受保護的個人資料就會發生疑問。所謂「足資識別該個人之資料」究竟應如何解釋，如果比較德國法的定義，其強調「個人關聯性」，若當事人是不特定的，也就是蒐集單位及其所得指揮之人員，均無法確定資料所關聯之個人為何者，那就不是該條所稱的個人資料¹⁹；歐盟指令的定義則也有我國個資法「足資識別」的文字，不過它進一步將足資識別放寬包括「間接」能予識別者。

然而，「間接能予識別」其實還是很不清楚的概念，國內的論述似乎並沒有看到非常明白的解釋，本文認為，解釋上至少應以從寬為原則，因為就個資法例示的項目而言，許多事項例如教育、職業、健康、財務情況、社會活動等，如果不是和姓名、身分證統一編號等資料扣合在一起，事實上也欠缺確是那一個人的能力，卻已明文受到保護；何況某項資料本身雖不能指涉其所有人，但透過與其他資料的比對或連結，就可能發生個人關聯性，而保護個人資料某種程度也就是在避免這種風險；甚至我們可以說，個人資料即使是最典型的身分證字號或姓名，單獨來看都可能是無意義、不造成損害的，但問題就在當它們被和其他資料連結時，將有造成損害的危險，而判斷是否存在此種風險，也就是判斷是否為個人資料所要負擔的功能，其結果，只要是與個人相關的資訊均有產生此種風險的可能，因此也就均應被評價為個人資料，至於是否真的造成損害，則是另一問題而非判斷個人資料所應承擔的作用。

在具體的認定上例如IP位址，一般認為其僅為數字之組合，且歸屬於機構或組織而非個人所擁有，應該不能認為屬足資識別個人之資料²⁰，但如果是個人申請的IP位址則似乎有被認為個人資料的可能；又如cookies²¹所蒐集的網路活動資料，姑且不論有解釋為例示的「社會活動」之可能，至少和病歷、財務情況、社會活動等歷史記錄具有同質性，而且cookies可以識別出是同一電腦再度光臨，而可能解釋為間接識別使用者，遑論其與其他資訊扣合之機會甚大，比如加入會員輸入的會員資料、寄網上文章給朋友輸入的E-mail信箱、購買東西輸入的信用卡號碼等。

在釐清個人資料的定義後，個人資料權的意義也就呼之欲出。和隱私權可界定為對隱私的控制權一樣，個人資料權也就是對個人資料的控制權。主體是個人，客體是前述的個人資料，而作用則是控制，也就是對個人資料的掌握和自主，個人可以將其個人資料事務開放，使他人或公眾知悉、參與，也可以將其封閉，排除他人或國家的介入或支配。賦予個人控制的權利，就是讓個人可以決定在何時、何地、何種程度下，何人可以知悉或參與其個人資料的成分。

¹⁹ 參照洪榮彬，資訊時代之資料處理與資料保護——以德國聯邦個人資料保護法為中心，輔仁大學法研所碩士論文，頁77（1993/6）

²⁰ 認為IP位址不在個資法保障範圍者，參照陳家駿等，我國網際網路管理辦法建議草案之訂定，交通部電信總局委託研究，頁166（1998/7）；簡榮宗，網路上資訊隱私權保障問題之研究，http://tawanic.com/alan/alan4-08_6-2.html（2001/2/16 瀏覽）

²¹ 關於cookies技術本文在第三章第一節第一項有略作說明。

從此出發，可認知個人資料權的內涵，應包括國家或他人不得任意蒐集個人資料，否則即破壞個人對其資料之自主和掌握；即令在當事人同意下獲取資訊，亦應在符合當事人認知之範圍內為運用，否則亦超出當事人之控制而違反個人資料權；尤其不應容許任意揭露和公開，蓋此種對隱私侵害的明顯化，在向來隱私權之保護即已被理解。

當然，個人對其資料並無所謂絕對、無法加以限制的控制權；畢竟個人不可能遠離社會而獨居於陰暗的角落，必須考量其在社會團體內發展、依賴聯絡交往之人格。在這樣的社會活動中，不可避免部分個人資料在部分人間流轉，這種輕微的脫離控制例如朋友把自己的姓名、生日告知另一朋友，不應認為係侵害個人資料權²²。不過，由於國家沒有人際交往的問題，也就沒有此種因素之考慮，毋寧應儘可能避免蒐集資訊，除非是在正當社會公益的考量下，方允許對人民個人資料權為合比例的限制。

第三款 個人資料權在憲法上之地位

個人資料的蒐集和揭露，會使個人私密的不欲人知的面貌暴露出來，而造成當事人困窘和感情上的傷害；更深一層地，在個人資料被揭露的情形，被侵害者所喪失的不只是資訊的自主權，更是因為他人對其行為的品評而喪失個人生活的自由，特別是採取不同於主流價值的生活空間。個人原本可以自由地去營造和形成自己的生活型態，偏偏在個人資訊被揭露情形，使社會主流價值侵入個人生活，嚴重者可能導致對個人自由和創造力的扼殺，否定以「個人」方式存在之可能，使每個人在被公開的主流價值下而標準化。也因此允許個人資料任意蒐集，將使個人時時有被監視的恐懼，無法隨心所欲地生活，甚至喪失安全感，在無法擺脫被監視的狀況下，往往被迫對自身的行為和生活方式做出改變，使其行為和生活的自主權受到妨害²³；而愈倚賴用個人資料來對人作理解，也離獨立有尊嚴的「個人」愈遠，人們不再是認識你這個人，而是將你化約為符號、資料而為了解和評價。

因此，無論從人性尊嚴或隱私權 對個人領域的事務的控制權的角度觀之，均應肯認個人資料權應受憲法的保障，在現代資訊社會尤然。隱私權乃作為一上位概念，本身並不由憲法第二十二條呈現，而是具有解釋、適用已明文規定之權利的指引作用，並補充具體化未列舉或隨時代發展出的權利，也就是說，當某一型態個人領域的控制權，日見形塑成熟，即可透過隱私權的價值在二十二條予以承認，本文認為個人資料權基於前述的保護正當性及成熟性，就是此種操作的極

²² 所以歐盟 1995 資料保護指令第三條就將「自然人單純為個人或家計活動者」排除於適用範圍之外。歐盟 1995 年資料保護指令之中譯，參照熊愛卿、詹文凱合譯，歐盟 1995 年資料保護指令，收錄於熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，附錄（2000/7）

²³ 參照詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 276-277（1998.7）

佳範例。

第三節 電子商務與個人資料保護之 聯繫

第一項 電子化、網路化之特徵 - 以個人資料保 護為中心之發掘

在前述第一章第一節的定義中已論及，電子商務以電子化與網路化為要素，而電子化與網路化具有以下的特徵，使個人資料保護更具重要性以及需求特殊之因應：²⁴

1. 掌握資訊工具及能力者易取得他人資料：掌握專門技術或網路工具者，有能力在一般人不知不覺中即取得大量他人資訊。
2. 資訊易傳遞、集中：電子資料容易複製，又佔空間極小，較傳統檔案容易傳遞、集中。尤其在網路化之情形下，傳送極為容易，甚且跨越國界。
3. 資料易予分析、整合：電子資料容易使用電腦程式予以分析，而資訊系統所具備與強調和其他系統的相容性，使各種不同形式的資料更容易在不同系統中處理和整合。
4. 資料可迅速、不留痕跡地變更、洗除：按個鍵即可不留痕跡地把記錄變更或洗除，也因此一有塗改、變造不易察覺或追究。
5. 資料防護不易：傳統之檔案可以經由警衛的看守或上鎖等措施加以防護，使無關人員不易接觸；但電腦檔案則不然，因其處理須經過許多專門步驟，而增加了接觸的人數，且在網路化情形下，須防止駭客入侵，更增加安全上的風險。
6. 對資料保護意識的低落：一般人對電子媒體的個人隱私權，在意識型態上甚為薄弱；而資料處理者任意擷取窺視或組合他人資料，用以滿足個人之好奇心或私人需求卻不以為杵；復以有權蒐集、管理個人資料之權利者，僅持超平常心看待大量的個人資料而不加以尊重。

²⁴ 相關特徵之觀察可參照洪榮彬，資訊時代之資料處理與資料保護——以德國聯邦個人資料保護法為中心，輔仁大學法研所碩士論文，頁 14(1993/6)；熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，頁 49-51(2000/7)；葉淑芳，行政資訊公開之研究——以隱私權益之保障為中心，中興大學法研所碩士論文，頁 144-145(1999/7)

第二項 電子商務對個人資料的需求性

前項電子化、網路化的特徵觀察，著眼於電子化、網路化本身的性格，但不可忽略，電子商務還有「商務」此一要素，而當電子化、網路化和商務連結在一起時，就個人資料保護的角度而言，又會產生什麼樣的化學變化？

首先，個人資料的提供與獲取，在電子商務先天上就是不可避免的。傳統的交易型態出賣人可以對買受人一無所知，只要拿到錢就好了，但在電子商務的交易型態，相對人並不是現實地出現在眼前，如何確知是誰跟我交易，是不是真能獲得給付，即成為問題，因此勢必要有個人資料的交通，才能使網路上交易成為可能，信用卡卡號的提供就是現實上最普遍的例子。

更進一步的，電子商務經營者除了要吸引顧客進入該網站瀏覽並且有購物行為外，同時為了要達成一對一行銷並提昇客戶的消費忠誠度，常常想盡各種方法蒐集個人資料，以試圖描繪出顧客的好惡輪廓，藉由個人化的服務，增強其競爭力。而此種作法在電子商務之所以特別鮮明，可以從消極面和積極面加以說明：

25

1. 消極面：在網站可替代性過高的網路消費環境下，為求能成功的留住消費者，常常需要以此種行銷方式提供消費者個人化的服務。
2. 積極面：關係行銷的利益雖然很好，但是這種行銷方式在過去所耗費的成本過大，因此常常不被納入經營策略的考量中。但是現今由於網路化與電子化的特徵，可大量、迅速、輕易的處理個人資料，尤其新興資訊科技諸如 cookies 的興起，更容易蒐集消費者的資訊，此種經營方式即易於實現。

就因為在電子商務的環境之下，個人資料的重要性非同以往，個人資料可以說成為網路公司的重要資產，這從 Amazon 新的隱私權政策表示，客戶的個人資料可能會被當作公司資產的一部份轉移給收購的公司²⁶，以及二嫌犯趁選舉熱潮之際，號稱有一千五百萬筆選舉人名冊，規劃出各選區選舉人之詳細資料，利用網路招攬及主動投寄各候選人來進行販售²⁷等案例可以清楚看出。

也因為個人資料的重要性非同以往，個人資料的保護問題也就特別受到重視，據報導，從一份美國商業周刊所進行的調查指出，個人隱私權是消費者決定上網購物的最大障礙，甚至為了維護個人隱私權，拒絕登錄在未明確提出消費者隱私權保護政策的網站，有些網路使用者更為了自保，以假資料上網登錄²⁸。

²⁵ 參照邱建勳，從電子商務之面向探討網路資訊隱私權，
http://www.elitelaw.com/paperread.asp?paper_no=971（2001/5/1 瀏覽）

²⁶ Patricia Jacobus，隱私權團體：亞馬遜政策有騙客戶之嫌，CNET 新聞專區，
<http://www.taiwan.cnet.com/news/ec/story/0,2000022589,11014061,00.htm>（2001/4/26 瀏覽）

²⁷ 李科逸，從網路販賣名冊看個人隱私之保護，<http://www.crime.org.tw/data01-a1401.html>
（2001/4/26 瀏覽）

²⁸ 吳芬滿，網路隱私權與個人化服務的矛盾，

從第一項及本項的討論可知，電子商務中個人資料保護的問題，具有特殊探討的價值，因此，在學者及實務對電子商務的討論，以及各國的做法中，個人資料保護已成不可或缺的重要議題。

第三項 國家在電子商務中個人資料保護問題之 角色扮演

從上一項的討論中可知，電子商務因其電子化、網路化之特性，對個人資料保護造成較以往更為劇烈的衝擊，更強的保障需求性亦於焉浮現；而在前節本文亦已確認，個人資料權應從憲法第二十二條生成，作為憲法所保障的基本人權，則在此認知下，國家對於電子商務中的個人資料保護問題，應扮演如何之角色呢？

按向來見解認為，基本權的規範對象為國家，主要的效果表現在人民可主張排除國家對其之侵害，也就是基本權的防禦功能；而電子商務的個人資料保護問題所涉及的，是私人與私人間的關係，並非國家對人民的侵害。不過，學說上亦認為，基本權同時也是一種「客觀的價值秩序」，也就是說，從基本權利中抽繹出的客觀價值決定，可放射至所有法律領域，成為立法機關、行政機關與司法機關行使職權時所應遵循的重要準繩；並在此概念下發展出的「保護義務功能」，要求國家保護人民之基本權利免於自然力或第三人之侵害，以促進基本權利之實現，其表現型態，乃在立法者負有制定保護性法律之任務，行政權負有執行保護性規範之義務，司法者以保護義務為標準，審查立法者與行政權之作為或不作為，或審理民事案件作成裁判。²⁹

值得注意的是，與防禦功能以國家之侵害為對象不同，保護義務功能所涉及的問題，說是私人對私人的侵害，毋寧說是私人之間的權利衝突更為精確，畢竟保護了某人的權利，同時也是限制了他人的自由。以本文的背景而言，在前節第二項第二款最後即曾指出，個人沒有絕對、無法限制的個人資料控制權，仍須顧及個人社會交往之利益；同時，可能也涉及對自己網站設備的控制（財產權）、藉個人資料追求經濟利益（工作權）、促進資訊交流追求真理（言論自由）等等

<http://www.ectimes.org.tw/searchshow.asp?id=916&freetext=網路隱私權與個人化服務的矛盾>
&subject= (2001/4/26 瀏覽)

²⁹ 關於基本權利的功能體系，可參照李建良，基本權利理論體系之構成及其思考層次，人文及社會科學集刊，九卷一期，頁 39 以下（1997/3）；許宗力，基本權的功能與司法審查，收錄於憲法與法治國行政，頁 153 以下（1999/3）；林錫堯，西德法上基本權之性質與效力及憲法訴願之客體，憲政時代，十卷一期，頁 24-26。關於保護義務功能，參照李建良，基本權利理論體系之構成及其思考層次，人文及社會科學集刊，九卷一期，頁 49-50（1997/3）；Christian Starck，李建良譯，基本權利之保護義務，政大法學評論，五十八期，頁 33 以下（1997/12）；許宗力，基本權的功能與司法審查，收錄於憲法與法治國行政，頁 164-168（1999/3）。

的價值。如果把電子商務的經濟利益視為一概括的價值，更可以做如下的討論：徹底保護了個人資料權，則業者動輒得咎，將會扼殺了電子商務的發展；但全力促進電子商務，又可能對個人資料權造成嚴重的侵害，而且回過頭來，消費者顧慮隱私問題而躊躇不前，對電子商務發展反而不利³⁰。因此，保護義務功能就需求立法者作利益的調和，妥善設計，透過立法的方式加以實現。

特別在個人資料保護的問題上，由前節第二項第二款的定義可知，個人資料權係對自己個人資料的控制權，甲強行獲取乙的個人資料當然造成乙個人資料權的損害，即令非強行獲取，而是透過迂迴、隱密的方式知悉，也仍然是造成乙對其個人資料控制權的妨礙；又假設甲在乙的同意下獲得乙的個人資料，在現實上擁有對該資料的支配地位，是否即可任意加以使用、傳送甚至揭露予他人？從前述對個人資料權內涵的認識可知，乙將其資訊交付與甲，並非當然表示其權利已然消失，毋寧其保護要求及當事人對該資訊的控制權，仍應附著其上，持續地發生效力。因此，個人資料的取得、管理、使用實為一整體性的問題，應予全盤思考，甚至國家應創設一制度和程序，對人民個人資料之保護為周全規劃，方能使人民個人資料權真正獲得實現，這可認為是基本權的制度保障或程序保障功能的要求。

第四項 個人資料保護法制之形塑

承前項，為保障人民個人資料權，國家須建構一定的法制，而在建構此一法制時，有待將個人資料權的內涵進一步具體化，成為一般性的理念或原則，並調和其他利益，形塑出原則底下細緻的規範。關於個人資料保護立法的原則，參酌他國立法例及國際間的發展趨勢，本文擬以經濟合作與開發組織(Organization for Economic Cooperation and Development, OECD)一九八一年提出的「有關個人資料之國際流通及隱私權保護準則」中，關於國內個人資料保護的八項原則，作為主要的依據；雖然該準則年代較為久遠，但作為上位的立法原則，依然經得起考驗，並且實際上對各國的法制幾乎都產生深刻的影響，而可以該八項原則作為理解各國規定的基礎³¹。試將該八原則略述如下：³²

³⁰ 關於個人資料保護與電子商務的衝突，其實也表現在歐盟與美國不同社會、文化背景下，法制的差異上，歐盟重視前者，故採取嚴格的措施加以保障，美國傾向後者，故政策上一直希望以業者自律的方式來解決，而立法遲緩。參照簡榮宗，網路上資訊隱私權保障問題之研究，http://tawanic.com/alan/alan4-08_5-3.html（2001/2/16 瀏覽）

³¹ 美國一九七四年隱私權法及英國一九八四年自動化處理個人資訊之利用與其提供於公務規範法之原則，與 OECD 八原則均有類似之處，且相比之下似以 OECD 較完整，前述美、英立法原則參照林子儀，網路與隱私權，資訊科技與法律課程大綱與簡介，<http://www.cc.ntu.edu.tw/~cyberlaw/J4.html>（2001/5/1 瀏覽）；另外，美國一九七四隱私權法、德國一九九一年聯邦個人資料保護法、日本一九八八年有關行政機關電子計算機自動化處理個人資料保護法等立法例，均可以 OECD 八原則加以理解，參照許文義，個人資料保護法論，頁 170-171, 175-176, 178-179，台北，三民（2001/1）關於國際規範及各國立法介紹，可參照許文義，個人資料保護法論，頁 161 以下，台北，三民（2001/1）；簡榮宗，網路上資訊隱私權保障問題

1. 限制蒐集原則：有關個人資料之蒐集，原則上應加以限制；資料之蒐集應適法，並應依公正之手段為之，必要時，並通知當事人或得其同意後，始得為之。質言之，蒐集個人資料應合法、公平，並得資料當事人之同意或告知當事人。
2. 資料內容完整、正確原則：個人資料於特定目的之利用範圍內，應力求正確、完整及最新之狀態。
3. 目的明確化原則：個人資料於蒐集時，目的應明確化；其後之利用亦不得抵觸最初蒐集之目的；於目的變更時亦應予明確化。
4. 限制利用原則：個人資料之利用，除法律另有規定或當事人同意外，不得為特定目的以外之利用。
5. 安全保護原則：個人資料為防止遺失、不法之接觸、破壞、使用、變更或公開之危險，應採取合理之安全保護措施。
6. 公開原則：對於個人資料蒐集、自動機械化、處理及有關政策之制定，應對一般人公開之，例如資料管理人姓名及聯絡處、資料之種類、特定目的等事項，均宜公開。
7. 個人參與原則：資料之本人有權對他人持有自己之資料，行使一定程序之控制。個人有下列權利：(1)向資料管理人或其他人確保有關自己之資料是否被保有；(2)資料本人於合理期間內，如有必要時以不過度之費用，依合理方法，以自己亦了解之形式，知悉有關自己之資料；(3)資料本人於提出有關答覆或閱覽卷宗之要求而被拒絕時，能夠要求告知被拒絕之理由，並得對之提起異議；(4)可對有關自己之資料提起異議，如認異議有理由時，應將其資料予以刪除、變更、完全化與補正。
8. 責任原則：資料管理人應負遵守前述原則之責任。

另外，歐盟一九九五年個人資料保護指令採取的原則，與上述也有互通之處，但延續歐洲議會一九八一年有關個人資料自動化處理保護個人公約的「敏感性資料禁止處理原則」，則應特別予以注意。

針對個人資料的保護，我國已於一九九五年通過「電腦處理個人資料保護法」，在這方面可說已有法制成形，但該法仍存在甚多問題，與本文相關之部分將在下面分別檢討。討論的基礎雖說是上述各項原則，不過本文絕非將上述內容直接、僵硬地套用，毋寧各項原則的具體內涵仍須經過理論上的檢視，並參考其他立法例之規定，合先敘明。

在體系上，OECD 原則 1.到 7.，涉及的是「不同層次的資訊處理」，可稱之

之研究，http://tawanic.com/alan/alan4-08_5-2.html（2001/2/16 瀏覽）；翁岳生等，資訊立法之研究，行政院研究發展考核委員會委託研究，頁 48 以下（1994/7）

³² 關於 OECD 八項原則的說明參照許文義，個人資料保護法論，頁 162-163，台北，三民（2001/1）；李鴻禧，資訊、憲法、隱私權——資訊化社會與人權問題之探討，收錄於憲法與人權，頁 489-490；黃三榮，個人資料之保護——兼評我國電腦處理個人資料保護法，資訊法務透析，頁 40-41（1998/1）

為縱向的分析；另一方面還有橫向的分析，也就是「不同資料內容」是否應使國家受不同拘束之問題，歐盟指令的「敏感性資料禁止處理原則」將在此論及；最後，原則 8.責任原則促使我們注意，要使上述規範有意義，必須要依賴妥善的監督及救濟制度設計。因此下文的開展，就將以「不同層次資訊處理之個人資料保護問題」、「不同性質資訊內容之個人資料保護問題」及「監督及救濟制度之設計」為架構。

第三章 不同層次資訊處理之個人資料保護問題

第一節 個人資料之取得層次

第一項 網路新興技術所產生的特殊取得可能

以往，對個人資料的獲得，多係來自本人有意識地交付，但隨者網際網路之普遍使用，以及網路上活動相關技術的發展，使得蒐集他人資訊的可能途徑大幅增加，亦且發生質變。

透過網路相關科技的運用，可以記錄個人在網路上的電子腳印，也就是各種網路上活動所產生的資料，包括所拜訪過的網站、消費習慣、閱讀習慣，甚至信用紀錄、通訊紀錄等等不一而足。其中近來最受矚目，引起最多爭議的網路個人資料蒐集工具，可能非 Cookies 莫屬了。Cookies 本身是一個電腦檔案，其運作模式為：只要某一特定網路使用者拜訪或進入設有 Cookies 裝置的網站，此一網站的 server 會主動要求該使用者的瀏覽器出示一個特定的 ID（即 Cookies），如果該使用者的瀏覽器無法提供該 ID，網站的 server 便會自動送出這個 ID 到該網路使用者的硬碟理，記錄使用者日後在該網站上所從事的活動，甚且通常和網站所收集到的其他資訊，例如使用者確認（user authentication）資料，進行相互整合，以進一步發揮追蹤使用者網路活動的功能；甚至，也可形同使用者購物袋上所附著的記錄器，記錄使用者在網站上所購買的商品（例如網路書店 Amazon 即使用此種 shopping basket system）除了 Cookies 之外，類似資訊科技其實不勝枚舉，例如：對每一特定造訪者進行再度造訪次數的記錄（New Visitor Counting）；對網路使用者在網站上所瀏覽的特定網頁或網頁中之特定部分予以記錄（Behavior Tracking）；具有追蹤與歸類網路使用者特定網路興趣或所須網路資訊

內容之功能的 Push Technology 或 Agent Technology 等，均有或高或低侵入個人私領域的能力³³。

Cookies 此類技術的發達，固然創造了一些便利性及個人化的服務，但對個人隱私的衝擊也十分強烈。透過對個人網路活動的記錄累積，可以描繪出一個人的網路形象，使他人侵入個人的宗教認同、政治偏好、性別傾向等私領域之範圍，甚至流入不當的用途，而更嚴重的是，這些蒐集行為都是在我們不知不覺中，甚至可以說是在對網路「匿名性」的誤解中，而被完成。這使得網路活動者對其個人資料失去掌握，也使他人的蒐集資訊行為不易監督。

例如知名電子商務網站 Amazon、DoubleClick 等，均使用 cookies。據報導，美國聯邦貿易協會（FTC）更指出，雖然有八成以上的網站會收集網路使用者的個人資料，但僅有 14% 的網站會告知消費者其收錄個人資料的行為，更只有少之又少的網站會明確地告訴使用者該網站的隱私權保護政策。可見問題的嚴重性。

第二項 個人資料蒐集之目的拘束

目的明確化原則：個人資料於蒐集時，目的應明確化；其後之利用亦不得抵觸最初蒐集之目的；於目的變更時亦應予明確化。

這一原則之意旨與下面二、1 提及的「限制利用原則」相關聯，合併而言可以說就是「目的拘束原則」。目的拘束在個人資料保護法中非常重要，是一在德國經聯邦憲法法院肯認之原則，可以說是個人資料蒐集或處理的核心要件³⁴。

第三項 限制蒐集之思考

由於電子化、網路化所產生對個人資料權的重大威脅，我們對於收集個人資訊一事，應該重新檢視。也就是說，以往有些取得個人資料之情形，我們覺得沒什麼大不了，但到了資訊時代情況已大不相同，便捷的資訊流動、功能強大的比對分析，更不要說管理許多人的各式資料，對任何一企業而言，都不是非常容易的事，甚至在電子商務的環境下，個人資料代表財產價值，利之所趨如何期待管理者會為資料所有人著想？不管在後端的管制技術以及法制規範多完善，個人資料權仍處在很大的危險中。因此除了在資料的管理、傳遞和揭露的規範方面努力外，是否在一開始的資料取得就應採取更嚴格的控制，值得我們反省。

詳言之，對於國家蒐集個人資訊既是對人民權利的侵害，本應符合比例原則，而在狹義比例原則也就是衡平性的判斷上，應體認收集個人資訊後我們所要

³³ 參照劉靜怡，從 Cookies 以及類似資訊科技的使用淺論網際網路上的個人資料隱私保護問題，資訊法務透析，頁 24-26（1997/10）

³⁴ 參照許文義，個人資料保護法論，頁 225-226，台北，三民（2001/1）

付出的代價，意義上已與以往不同，因此需要更強烈的政府利益，才能正當化國家對個人資訊的蒐集行為。「限制蒐集原則」應由此處加以思考，甚至說是採取「必要性原則」，盡量避免資料之蒐集，也就是說，只有在個人侵害屬可以忍受，且處理之利益超過個人之損害時，方得被容許，此時蒐集個人資料便應掌握其項目與內容在必要的範圍內³⁵。

第四項 對我國法制之檢視

首先，就 Cookies 及類似資訊技術的問題而言，本文認為應有個資法之適用可能。Cookies 所蒐集的資訊，如在個資法第三條第一款列舉範圍內者自無疑問，若是 E-mail 信箱，本文認為具有表徵個人之作用且與個人密切相關，類似姓名、地址之作用，應屬受保護的個人資料³⁶；IP 位址本文在參、二、2 個人資料權部分已說明；最大宗的網路活動記錄（瀏覽網站那部分、停留時間長短、從事何種交易行為等等），本文亦在參、二、2 以多項理由認為應屬於受保護的個人資料。因此，非公務機關至少應受個資法的約束，不能任意使用 Cookies 或類似技術來取得人民資訊。

其次，個資法第六條規定：「個人資料之蒐集或利用，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。」第十八條規定：「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 經當事人書面同意者。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。三 已公開之資料且無害於當事人之重大利益者。四 為學術研究而有必要且無害於當事人之重大利益者。五 依本法第三條第七款第二目有關之法規及其他法律有特別規定者。」第十九條規定：「非公務機關未經目的事業主管機關依本法登記並發給執照者，不得為個人資料之蒐集、電腦處理或國際傳遞及利用。徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人，應經目的事業主管機關許可並經登記及發給執照。前二項之登記程序、許可要件及收費標準，由中央目的事業主管機關定之。」可說是限制蒐集原則、目的明確化原則的落實。

值得討論的是，第十八條第二款所謂「與當事人有契約或類似契約之關係」，似並非僅指有關個人資料蒐集之契約，否則適用第一款即為已足，但契約千萬種，不分類型與內容均可免責，個人資料保護豈非落空？或謂尚有後段「對當事人權益無侵害之虞者」來把關，但問題是不論何種形式的個人資料蒐集，恐怕都難說「對當事人權益無侵害之虞者」，蓋每一筆資料或許無害，但如果和其他某

³⁵ 認為我國個資法將來應遵循的原則包括「必要性原則」，參照熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，頁 225,233,248（2000/7）

³⁶ 認為 E-mail 在個資法保障範圍者，參照陳家駿等，我國網際網路管理辦法建議草案之訂定，交通部電信總局委託研究，頁 166（1998/7）

些資料連結，或將許多細微的資料累積、分析，就可能造成極大的侵害，而個人資料保護在資訊時代的意義，正是要避免此種危險，因此有謂「沒有無利益之資料」、「舉凡資料蒐集、處理或利用等行為均具干預性質」即此之謂，就算還是認為有篩選作用，如此不確定概念，也是不易掌握，因此，第二款兩項要件均不妥當，放在一起也無法正當化，實有檢討必要。第三、四款所謂「無害當事人之重大利益」也有類似的問題，均值再予探究。³⁷

如果參考德國法上的解釋，或許可以得到一些啟發。德國聯邦個人資料保護法第二十八條規定，「有左列情形之一者，得儲存、變更或傳遞個人資料，或以利用個人資料為執行自己業務目的之方法：一 在與當事人間之契約關係或類似契約之信任關係之目的範圍內。」所謂在目的範圍內該法並為詳細規定，必須由文件來加以闡釋，一般認為只要其儲存和利用資料，係用以完成當事人基於該契約所應履行義務和行使權利之必要者，即為本法所許可，例如：在勞工契約中，依據該契約所為之資料傳遞行為，只有當其係因勞工契約、或補充勞工契約之團體協約或其他勞工法律規定所必要者，才許可之；又如，在一項訂購家具之買賣契約中，為了送貨及徵信買者之信用度所進行之資料儲存行為，亦為本法所許；總之，契約關係之目的範圍，通常可由契約履行之情況中研判出來；而類似契約之信任關係之目的範圍，則可由締約關係人與其締約準備階段之情況推論出其特定之範圍；因此關於當事人之私人領域、嗜好之資料，由於均已超出契約目的範圍，所以其儲存或利用均非本法所許可；最後尚須注意的是，若在當事人和儲存單位存在多種契約關係時，必須依各個不同契約關係之進展來進行研判，唯有在具體之契約關係範圍內，始得為儲存和利用行為，例如信貸機構之員工向公司本身進行貸款行為時（此時乃居於顧客之地位），則關於其帳戶之收支情況之資料，即不得利用於其與信貸機構間之勞工契約關係之範圍內，從事人事評鑑之行為，殆此時其帳戶相關資料之使用已超出原先之使用範圍（信貸契約之範圍），其嗣後使用於勞工契約中，須重新審查其必要性及是否為本款所許可。³⁸這樣的操作在現實上是否有陳義過高，或是有模糊空間不易掌握等問題，當然不是沒有討論的餘地，但至少使我們思考，以所謂「有契約或類似契約之關係」當作合法化蒐集處理個人資料的理由，應該要是在促進契約或類似契約關係之實現所必須者，才有合理化的可能，我國的規定是否要做這樣的限縮解釋，相當值得考慮，若認為超出文義，就顯然有修正的需要。

另外，第十八條第一款的「書面同意」，產生一問題，即在網路上進行的點選或填寫行為，算不算書面？在進入電子化時代後，電子文件不符合民法上「書面」的要求就成為問題，由於和傳統書面的理解有異，電子簽章法草案就此有特別加以規定，不過在何種情況下承認有書面效力有爭論，最終的立法結果仍待觀

³⁷ 相關檢討意見可參照許文義，個人資料保護法論，頁 242，台北，三民（2001/1）；黃三榮，個人資料之保護——兼評我國電腦處理個人資料保護法，資訊法務透析，頁 48（1998/1）

³⁸ 洪榮彬，資訊時代之資料處理與資料保護——以德國聯邦個人資料保護法為中心，輔仁大學法研所碩士論文，頁 239-240（1993/6）

察；在還沒立法之前，恐怕就很難說在網路上的點選或填寫是書面，尤其一般討論民法上書面要求的理由，不外使當事人慎重以及作為證明之用，就前者而言，網路使用者通常很少會去詳讀那一大堆文字的隱私權條款，使之慎重的期待恐怕會落空一大半，就後者而言，網路使用者並不保有該份隱私權條款，哪一份是當初同意的那一份，將來也不可能舉證，因此解釋成不是書面，似乎也很合理；但另一方面，電子商務既以網路作為交易的工具，幾乎必然採取網頁上請求同意的方式，期待業者對每個人去簽同意書，幾乎是不太可能的事，因此此種書面要求，在電子商務上是否是不切實際，有檢討的空間。當然，由於第十八條有其他款的事由（尤其第二款），這個問題也許還不會很嚴重。不過第一款的同意和第二款的契約畢竟是指涉不同的東西，前者指對蒐集個人資料的同意，後者則指雙方為其他目的訂立的契約，不是關於個人資料蒐集使用的契約，在這裡附帶澄清。

最後，關於第六條的概括條款，謂應「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。」應從限制蒐集之思考來加以理解。在現行電子商務的活動狀況，可發現對個人資料的蒐集幾乎到了瘋狂的程度，有沒有用不管，先全部蒐集了再說，有沒有逾越其蒐集目的的「必要」範圍，就非常問題，但消費者為了購買該項商品，對網路商店要求必須填寫的各項資料只好一一填入，這樣的同意真的是完全的自由意志，業者的要求真的完全符合誠信原則，也令人懷疑。

第二節 個人資料之利用層次

第一項 個人資料之限制利用

業者獲得他人個人資料後，是否就可以任意使用，或仍要受一定原則的拘束？

從資訊被取得人的觀點，他人預見其所提供之資訊將在怎麼樣的範圍內被使用，而斟酌提供一定之資訊。如果業者在利用資訊時逾越了取得人被告知、所理解的目的範圍，則非被取得人所預見，如果當初能預見此種利用，是否仍會提供相同資訊，則有疑問。因此，逾越取得目的使用人資訊，明顯損害被取得人對其資訊的控制權，此種行為應予禁止。³⁹

從上述的理由我們可以得出，對他人個人資料的運用應遵循「限制利用原則」，也就是個人資料不應供作蒐集目的以外之其他目的之利用，除非經過資料主體之同意或依據法律之規定。簡言之，利用應於目的範圍內。

另外，對不完整、錯誤的個人資料為使用，其結果可能有害於當事人的實體

³⁹ 參照林子儀，「資訊取得法」立法政策與法治之研究，收錄於氏著，權力分立與憲政發展，初版，頁 205-206。

利益，對其個人資料權亦可能造成傷害，蓋「誤導」本屬隱私權侵害的一種態樣⁴⁰。故應遵循「資料內容完整、正確原則」，也就是個人資料之利用，於其利用目的之必要範圍內，必須保持正確、完全和最新。

第二項 對我國法制之檢視

個資法第二十三條規定：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用：一 為增進公共利益者。二 為免除當事人之生命、身體、自由或財產上之急迫危險者。三 為防止他人權益之重大危害而有必要者。四 當事人書面同意者。」

就「應於蒐集之特定目的必要範圍內為之」而言，與「目的明確化原則」、「限制利用原則」相符，不過例外規定充斥過於模糊的不確定法律概念，恐怕有稀釋個人資料保護之問題，如第一款所謂「增進公共利益」就可說出手全無部位，幾近包山包海，應有細緻化的可能。⁴¹

第三節 個人資料之儲存管理層次

第一項 安全保護問題

由於資料電子化之後，可以輕易而迅速地複製、清除，或不留痕跡地變更大量資料，如果未加妥善管制，對資料安全性會造成很大的風險。在網路化的情形，由於大量資料將利用開放式公共網路進行傳輸，資料很容易在中途遭人截取，而資料庫及內部網路亦可能遭駭客侵入，使個人資料保護威脅倍增。

例如美國麻州有一青少年入侵機場的網路系統，切斷塔台的通訊服務，造成進入機場的飛機無法打開機場跑道的燈；美國一電腦駭客因不滿某法官的裁決，故而侵入電腦系統將法官的考績竄改；美國一銀行職員將客戶存款的零頭尾數挪到自己的帳戶裡，聚沙成塔後獲取巨額財富⁴²。我國亦發生許多現實案例，例如刑事警察局發現在破獲的色情網站及網路駭客案件中，有將近八成設有「木馬程式」。網路使用者從網站下載共享軟體或進入色情網站下載或曾被電腦駭客入侵，即可能被植入木馬程式，導致電腦內的資料完全曝光；三名高中生利用

⁴⁰ 關於 William L. Prosser 教授對隱私權侵害的分類，參照林子儀，網路與隱私權，資訊科技與法律課程大綱與簡介，〈<http://www.cc.ntu.edu.tw/~cyberlaw/J4.html>〉；詹文凱，隱私權之研究，台灣大學法研所博士論文，頁 26-27（1998/7）

⁴¹ 相關評論參照黃三榮，個人資料之保護 兼評我國電腦處理個人資料保護法，資訊法務透析，頁 49（1998/1）；許文義，個人資料保護法論，頁 188，台北，三民（2001/1）

⁴² 蔡美智，電腦駭客入侵的法律問題，資訊與電腦，二一七期，頁 65,67（1998/8）

Subseven 以及 Netspy 之用戶端「特洛伊木馬程式」，侵入網路上不特定第三人電腦，以遠端遙控的方式，取得他人電腦的主控權，竊取電腦內部的檔案、網路撥接帳號及密碼等重要資料，再利用該撥接帳號上網，造成被害人上網費用暴增；離職的張姓網路工程師，因先前追求該公司黃姓女同事遭拒，欲得知黃女男友的身份，涉嫌以「社交工程法」(social engineering)入侵公司電腦，截取公司及所有員工的電子郵件，並且假冒調查局之名，在網路上散發黃女之黑函；⁴³中國信託商業銀行發生信用卡資料外洩事件，可能係偽卡銀行與員工掛勾所致⁴⁴；曾發生網友緣於好奇上 Google 搜索引擎輸入自己名字測試，發現自己之前曾於智富網所登錄之資料（包括姓名、住址、年齡、身分證字號等），居然隨意就可在網路上被搜尋到，而感到驚訝不已⁴⁵。凡此例子均可見網路資訊安全保護問題的嚴重性。

故在個人資料保護上導引出「安全保護原則」，即對於個人資料之佚失、不當接觸、破壞、利用、修改、開示等危險，必須藉合理之安全保護措施加以保護。

德國聯邦個人資料保護法第九條第一句，即要求「應採取技術上與組織上之必要措施，以確保本法之執行」，其附件對「自動化處理個人資料」更要求須一所以保護個人資料之種類，採行下列「個別保護措施」：⁴⁶

- A 入口管制：防止無權者擅入處理個人資料之資料處理設備內。
- B 出口管制：防止擅自閱讀、複印、變更或搬走資料庫。
- C 輸入管制：防止擅自投入儲存機及擅自認知、變更或消除已儲存之個人資料。
- D 使用者管制：防止無權者擅自利用以資料傳遞設施傳遞資料之資料處理系統。
- E 取用管制：確保有權利用資料處理系統者只能取用其權限內之個人資料。
- F 傳遞管制：確保能檢定並確認，個人資料經由資料傳遞設施可能傳遞至何處所。
- G 投入管制：確保事後能檢定並確認，那些個人資料於何時由何人投入資料處理系統。
- H 委託管制：確保受委託處理之個人資料能僅依委託人之指示為處理。
- I 運送管制：防止在傳遞個人資料以及運送資料庫時該資料被擅自閱讀、變更或消除。
- J 組織管制：使官署或營業之內部組織能符合資料保護之特殊要求。

由該法第九條組織上與技術上之措施，本不論自動化或非自動化資料處理均

⁴³ 非色情網站 網路犯罪防治網，案例摘要，<http://www.crime.org.tw/data01.htm#13>（2001/4/26 瀏覽）

⁴⁴ 羅惠馨，中信銀如何逃過醜聞風暴，http://www.pchome.com.tw/ebusinessweekly/024/ebusinessweekly_22-1.html（2001/4/26 瀏覽）

⁴⁵ 李科逸，從智富網事件看網路新興趨勢對社會規範之衝擊，http://tech.smartnet.com.tw/article/art_cont_1.asp?art_no=20010328016（2001/4/26 瀏覽）。本文作者自己就曾發生，在 Google 上存在我參加某研討會報名個人資料的網頁頁庫存檔，去函 Google 未獲回應，經向該研討會主辦單位要求向 Google 反映後，方才移除。

⁴⁶ 德國「聯邦個人資料保護法」的中譯，參閱林錫堯譯，德國聯邦個人資料保護法，法學叢刊，三十六卷四期，頁 1-18；關於各項個別保護措施的具體內容，參照洪榮彬，資訊時代之資料處理與資料保護——以德國聯邦個人資料保護法為中心，輔仁大學法研所碩士論文，頁 127-133（1993/6）

在要求之列，第九條第一句附件之個別保護措施卻只適用於「自動化處理個人資料」，可見已體會電子化對資料保護的衝擊，並針對此點為特殊設計。

另外，歐盟一九九五年資料保護指令第十七條亦規定，「保管人應設置適當技術及組織設施，以防止個人資料遭受災害或不法破壞、滅失、竄改、無權揭露或存取，尤以經由網路傳遞及其他非法形式之處理。」與德國法之規定意旨相同，而「該等設施，經考量技術狀況與實施成本，應確保對其所處理資料之風險與所需保護之性質，具有相當之安全水準」之規定，似乎更意味著資料保管人具有積極義務使自己一直掌握最新的安全資訊，以確保符合相當的安全水準⁴⁷。

第二項 完整正確及個人參與問題

取得他人個人資料後，雖實體上脫離個人掌握，但就個人資料權之理念而言，個人始終為個人資料之權利主體，仍應保有對其之控制權，這除了表現在不得任意使用、傳遞、揭露等面向外，亦表現在資料所有人有權知悉資料蒐集者對其資訊掌握之狀況、對不正確之資料有權更正、對使用目的消失之資料有權主張消除等面向。前者本文於其他章節說明，後者則列於此處資料的管理層次，稱為完整正確及個人參與問題予以討論。

人們如果對自己的資訊，是否以及在何範圍內被他人所保有，毫不知情，則後續的參與權和監督權皆無由發動；若資料蒐集者持有之資訊不正確，將可能據此作出錯誤決定，個人會被錯誤認識，亦可能因資料管理者的決定而受害；對不法取得的資料，應予消除當無疑問，對使用目的已經消失的資料，鑒於取得個人資料本身即是對個人資料權的一種侵犯，以及持續的保有就代表持續的危險，亦應予以消除。

上述理由導引出所謂「公開原則」及「個人參加原則」。「公開原則」指關於個人資料的蒐集、管理者、儲存場所、資料類型與性質、利用目的等事項應予公開；藉此個人得了解其資訊是否遭蒐集、儲存、利用等，方能進一步實現對其個人資料的控制權。「個人參加原則」，其內涵就 OECD 一九八一年提出的個人資料保護原則，則包含如下：⁴⁸

- A 本人就有關自己之資訊資料，得向資訊資料管理人或他人，要求確認是否保有。
- B 本人就有關自己之資料，於合理期間內，以不過高之費用為限由本人支付，依用合理之方式，藉本人容易瞭解之形式，得加以了解。
- C 就前兩項權利之行使遭受拒絕時，有關個人得對其拒絕理由提出異議。

⁴⁷ 參照熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，頁 168（2000/7）；歐盟 1995 年資料保護指令之中譯，參照熊愛卿、詹文凱合譯，歐盟 1995 年資料保護指令，收錄於熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，附錄（2000/7）

⁴⁸ 參照李鴻禧，資訊、憲法、隱私權——資訊化社會與人權問題之探討，收錄於憲法與人權，頁 489-490；黃三榮，個人資料之保護——兼評我國電腦處理個人資料保護法，資訊法務透析，頁 41（1998/1）

D 就有關自己之資訊資料之訛誤，申明異議而被認許時，得要求資料之消除、修改、重新完成或補充。

再參考德國聯邦個人資料保護法之規定，包括下列權利或要求：⁴⁹

A 請求告知權：應依當事人之申請，告知左列事項：一 已儲存之關於其個人之資料，包括資料來源及接受者。二 儲存目的。

B 資料之更正請求權：個人資料不正確者，應予更正。文卷內之個人資料經確認為不正確，或當事人對其正確性有爭執者，應於文卷內註明之，或依其他方法記錄之。

C 資料之封鎖請求權：當事人對資料檔內之個人資料正確性有爭執，而未確認其係正確或不正確者，應予封鎖。

D 資料之消除請求權：資料檔內之個人資料有左列情形之一者，應予消除：一 不法儲存者。二 儲存單位執行其主管職務已無了解其該個人資料之必要者。

E 輾轉通知之義務：基於保障當事人正當利益之必要，不正確資料之更正、爭執性資料之封鎖即因不法儲存而消除或封鎖資料時，均應通知在經常傳遞範圍內接收該資料之傳遞而為儲存之單位。

該法第六條並規定：「當事人之告知與更正、消除或封鎖之權利，不得以法律行為予以排除或限制。」使當事人的法律地位更具實質意義。

第三項 對我國法制之檢視

第一款 安全保護問題

個資法對安全保護僅有第十七條規定：「公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」而非公務機關依第二十六條準用之。

個資法施行細則第三十四條規定：「公務機關保有個人資料檔案者，應訂定電腦處理個人資料安全維護法令，其內容應包括資料安全、資料稽核，設備管理及其他安全維護等事項。」而非公務機關依第三十五條準用之。

個資法第二十條第一項第十、十一款分別規定，個人資料檔案維護負責人之姓名、個人資料檔案安全維護計畫，為登記應記載之事項，同條第五項規定第一項第十一款之個人資料檔案安全維護計畫之標準，由中央目的事業主管機關定之。

上述規定均屬十分概括，未如德國聯邦個人資料保護法規範細緻，亦似未體會組織與技術上措施的科技性和發展性，對是否採取足夠的技術、組織上之措施

⁴⁹ 參照洪榮彬，資訊時代之資料處理與資料保護——以德國聯邦個人資料保護法為中心，輔仁大學法研所碩士論文，頁 177-191（1993/6）

又無任何效果或監督規定，是否足以保障個人資料的安全性，實堪懷疑。

第二款 完整正確及個人參與問題

「資料內容完整、正確原則」落實在個資法第十三條，可值贊同，附帶提及。

個資法的公開原則落實在第二十一條及第二十二條等條文，要求將第二十條第一項第一到十款之事項於政府公報公告並登載於當地新聞紙，以及備置簿冊供查閱，而第二十條底一到十款所列事項包括「一 申請人（即該非公務機關）之姓名、住、居所。如係法人或非法人團體，其名稱、主事務所、分事務所或營業所及其代表人或管理人之姓名、住、居所。二 個人資料檔案名稱。三 個人資料檔案保有之特定目的。四 個人資料之類別。五 個人資料之範圍。六 個人資料檔案之保有期限。七 個人資料之蒐集方法。八 個人資料檔案之利用範圍。九 國際傳遞個人資料之直接收受者。一 個人資料檔案維護負責人之姓名。」規定尚稱允洽。

個人參與原則部分，個資法第四條規定：「當事人就其個人資料依本法規定行使之左列權利，不得預先拋棄或以特約限制之：一 查詢及請求閱覽。二 請求製給複製本。三 請求補充或更正。四 請求停止電腦處理及利用。五 請求刪除。」

查詢及請求閱覽權 第十二條（第二十六條準用）。

請求製給複製本權 第十二條（第二十六條準用）。

請求補充或更正權 第十三條第一項（第二十六條準用）。

請求停止電腦處理及利用權 第十三條第二項（第二十六條準用）。

請求刪除權 第十三條第三項（第二十六條準用）。

相關條文尚有第十五（第二十六條準用）十六第一項（第二十六條準用）三十二條及施行細則二十三、二十四條第一項（第三十五條準用）二十五條（第三十五條準用）二十六條等。規定與德國法相似且亦不惶多讓。

第四節 個人資料之傳遞層次

第一項 個人資料之流動

就資訊的流通利用而言，各業者當然希望能獲取他人個人資料愈多愈好，也就希望能從其他業者處獲得或彼此分享個人資料。尤其個人資料在電子商務的環境底下，具有財產價值，如前面提及 Amazon 新的隱私權政策表示，客戶的個人資料可能會被當作公司資產的一部份轉移給收購的公司；剛屆滿週年便旋即關

門的 Toysmart.com 將其公司資產出清，其中就包括了該公司的顧客名單⁵⁰，已可見將個人資料轉售的例子所在多有。但從個人資料權的角度觀察，允許企業間任意傳遞就有商榷的餘地。

首先就「資訊的取得」面向而言，前曾論及應在一定條件下，並受目的明確原則拘束，但倘若允許個私人間資料可以隨意流通，則對資料取得的限制就失去意義；在甲業者傳遞資料給乙業者的過程中，乙業者其實就相當於資料的取得，如果獲取該項資訊本非其權限範圍，如何能夠允許呢。

就「資料的利用」面向而言，業者應只能在蒐集目的範圍內為利用，前已論及，則前述乙業者的利用及其目的，勢必非當事人當初所能預見，也就同樣違反了限制利用原則。

就「資料的管理」面向而言，資料的管理者原應確保資料不外洩，倘若業者間資料可以任意交流，此一保護也就產生漏洞。

第二項 對我國法制之檢視

個資法對個人資料的傳遞並未以個別條文規定，但個資法第三條第三款定義「電腦處理」指「使用電腦或或自動化機器為資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理。」傳遞就被包含在電腦處理的概念中；但同條第五款又定義「利用」為「指公務機關或非公務機關將其保有之個人資料檔案為內部使用或提供當事人以外之第三人。」又把「提供當事人以外之第三人」納入利用的概念中，則因為電腦處理將適用第十八條⁵¹，利用則應適用第二十三條⁵²，在此發生問題。就文意上而言，二者都可說得通，德國聯邦個人資料保護法第三條是將「傳遞」定義為示之第三者的行為⁵³，歐盟1995年資料保護指令第二條定義「處理」包括「蒐集、記錄、組織、儲存、改編或變更、檢索、諮詢、利用、經傳送揭露、散布或其他產生效用、排列或組合、凍結、刪除或銷毀之作

⁵⁰ 丁源宏，顧客名單轉售？高度商業化背後的道德疑慮，

<http://www.ectimes.org.tw/searchshow.asp?id=950&freetext=&subject=顧客名單轉售？高度商業化背後的道德疑慮>（2001/4/28 瀏覽）

⁵¹ 個資法第十八條規定：「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 經當事人書面同意者。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。三 已公開之資料且無害於當事人之重大利益者。四 為學術研究而有必要且無害於當事人之重大利益者。五 依本法第三條第七款第二目有關之法規及其他法律有特別規定者。」

⁵² 第二十三條規定：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用：一 為增進公共利益者。二 為免除當事人之生命、身體、自由或財產上之急迫危險者。三 為防止他人權益之重大危害而有必要者。四 當事人書面同意者。」

⁵³ 「傳遞，指將已儲存或經資料處理所獲得之個人資料，依左列方式示之第三者：a.由儲存單位將資料傳達於接收者，b.由接收者從儲存單位查閱或截取原已備妥之資料。」德國「聯邦個人資料保護法」的中譯，參閱林錫堯譯，德國聯邦個人資料保護法，法學叢刊，三十六卷四期，頁1-18

業或整組作業方式。」⁵⁴ 則若參考此二外國立法例的解釋，就會採取前說，國內亦有學者認為應適用個資法第十八條者⁵⁵，而且，在公務機關對公務機關傳遞之情形，能否解釋為第三人會發生問題⁵⁶，若要求理解上的一致，可能也會傾向此說；但另一方面，「提供當事人以外之第三人」屬利用又十分清楚，國內亦有採後說者⁵⁷。本文提出另外兩種想法，在甲業者傳遞個人資料給乙業者這樣的例子中，甲的行為比較類似利用，而乙的行為則等於是蒐集，因此一種解法是認為，就甲而言要合法傳遞，理論上應符合關於利用的規定，就乙而言要合法收受，則應符合關於蒐集的規定，故甲應遵守第二十三條，乙應遵守第十八條，之所以提出此一想法，乃鑒於傳遞可能是一涉及雙方的行為，假如是在一存在交付、受領的情況下，似乎雙方都有責任才是，如果要免責，就應分別符合利用、蒐集的規定；至於在單方行為的情況，例如甲單純的公開揭露他人個人資料，就應該論斷甲違法傳遞的責任，乙雖然可能藉此知悉他人個人資料，但似乎不應加以非難，個資法第十八條第三款「已公開之資料且無害於當事人之重大利益者」且有特定目的，似即可作為合法化的依據。第二種解法是認為，甲的行為符合利用的規定，或乙的行為符合蒐集的規定，只要其一具備即為合法，因為既然甲可以合法傳遞，這時我們還認為乙不能合法取得，豈不是相互矛盾，例如甲為盡其契約義務，請乙履行輔助，且被認為是在目的的必要範圍內的話，仍要乙負違法之責似乎不是很合理；相反地，如果乙可以合法蒐集，那他從甲那邊獲取個人資料，並沒有造成當事人的損害，似乎也不應令甲負違法之責。此二說應採何者為妥，本文尚無確定想法。

以上述兩見解檢討電子商務下常見的行為，例如任意將個人資料出售、交換是非法，應該是沒有問題的。不過，倘若甲是將所掌有的個人資料隨同其與消費者間之契約賣給乙，則未必被評價為違法，因為甲當初既然是為履行契約提供消費者特定服務而蒐集個人資料，當該契約移轉給乙時，將個人資料隨同移轉給乙，反有助服務的繼續履行，而在當初蒐集的目的範圍內，故符合第二十三條；又乙因為受移轉成為與消費者間契約的當事人，就能符合第十八條第二款之情形，且是為促進該契約目的而為的蒐集（如果當初甲蒐集個人資料的合法性沒有問題的話）；這似乎是合理的解釋。至於甲在移轉契約後，本身對個人資料的蒐集目的已經消失，繼續保有個人資料已失去正當性，根據個資法第二十六條準用第十三條，應依職權或當事人之請求，刪除或停止電腦處理及利用該資料。

⁵⁴ 歐盟 1995 年資料保護指令之中譯，參照熊愛卿、詹文凱合譯，歐盟 1995 年資料保護指令，收錄於熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，附錄（2000/7）

⁵⁵ 參照許文義，個人資料保護法論，頁 252-256,261，台北，三民（2001/1）

⁵⁶ 根據電腦處理個人資料保護法施行細則第六條規定：「本法第三條第五款所稱第三人，指保有個人資料檔案之公務機關或非公務機關以外之自然人、法人或其他團體。但不包括受委託處理資料之團體或個人。」看起來公務機關提供給公務機關似乎就不算提供給第三人，但這樣就會變成提供給公務機關和提供給非公務機關發生分流的現象，相較於德國規定的「人或單位」以及歐盟的「任何自然人或法人、公務機關、機構或其他團體」，恐怕是立法疏漏。

⁵⁷ 參照簡榮宗，網路上資訊隱私權保障問題之研究，http://taiwanic.com/alan/alan4-08_6-2.html（2001/2/16 瀏覽）

第四章 不同性質資訊內容之個人資料保護問題

第一節 敏感性資料之析出

對在各式各樣不同性質的個人資料，是否都合適相同對待，採取相同程度的保護措施？是否存在更核心，更具有保護需求性之個人資料種類？確是我們在個人資料保護已有相當認知之情況下，應該進一步思考的問題。或許能夠因此將個人資料權更予細緻化，而達到最佳的保護效果。

依資料內容而定是否限制或異其限制之立法例，在挪威的「私人註冊法」即已出現⁵⁸。其後的歐盟 1995 資料保護指令，更以「敏感性資料禁止處理原則」作為對各會員國之要求。此一原則之理念，應係認為個人資料，有關於個人身心之基本資料，如人種、個人思想、政治或宗教信仰、精神等資料，稱為「隱私權之固有資料」，除此以外敏感性較低之資料，稱為「隱私權之外延資料」，前者原則上應禁止蒐集處理，後者則無如此嚴格限制⁵⁹。

該指令第八條規定，「凡揭示種族血源、政治意向、宗教或哲學信仰、工會會員資格等之個人資料及涉及個人醫療或性生活等資料，會員國皆應禁止處理之。」⁶⁰由於此類資料最具敏感性，牽涉強烈之價值取向或利害關係，也就最有可能發生主流價值介入個人自由意志的情形，尤其本不應以此類資料當作對個人差別待遇之依據，考量此種因素而能認為正當連結實甚罕見，可是事實上，若使他人可以任意掌握此類資料，將不易避免此種歧視情況發生，蓋是否參雜不當連結本屬不易察覺，此類資料更均牽涉強烈之價值取向或利害關係，強求維持客觀中立，不如根本性地禁止處理；另外就個人醫療或性生活等資料，具特別深度的私密性，故亦納入禁止處理之範圍。不過當然，所謂禁止其實只是原則，仍然存在一些必要的例外情形，規定允許就敏感性資料為處理。

該指令中還有第二種敏感性資料，即「關於犯罪、刑事判決或保安處分等資

⁵⁸ 參照翁岳生等，資訊立法之研究，行政院研究發展考核委員會委託研究，頁 134（1994/7）

⁵⁹ 參照黃三榮，個人資料之保護 兼評我國電腦處理個人資料保護法，資訊法務透析，頁 45（1998/1）

⁶⁰ 所謂「處理」依該指令第二條之定義包括「蒐集、記錄、組織、儲存、改編或變更、檢索、諮詢、利用、經傳送揭露、散布或其他產生效用、排列或組合、凍結、刪除或銷毀之作業或整組作業方式。」所以從蒐集階段即已禁止矣。歐盟 1995 年資料保護指令之中譯，參照熊愛卿、詹文凱合譯，歐盟 1995 年資料保護指令，收錄於熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，附錄（2000/7）

料」，其處理，「限由公務機關監管下進行之，或國家法律已提供適當特定之安全維護措施者，會員國得訂定例外條款。但刑案有罪判決之完整記錄，應限由公務機關監管。」

第二節 對我國法制之檢視

個資法並未區分不同的個人資料給予不同的保護，就前述敏感性資料禁止處理原則之理念觀之，即有不足之處。採取該項原則，除了對隱私權保障強度更大外，某個角度來看也可以更有效率，因為反正敏感性資料就一律禁止蒐集，那就不會有後續的種種麻煩和擔憂；但另一方面，此項原則又不可能沒有例外，對其處理假如又要為不同的設計，反增添法制上的複雜性，尤其區分出敏感性資料，或許只是一小步，像歐盟指令又有第二類敏感性資料，又受不同程度的保護，這或許也是我們不能完全不去考慮的。而對不同內容資料給予不同保護，必須建基於我們對隱私、個人資料權更深的理解，當我們對什麼性質的資料的疏忽會造成什麼樣的傷害、對什麼性質的資料應給予何種強度的保護等問題，愈來愈清楚的時候，我們就可設計出更妥善的制度，這是我們勢必應予努力的方向。

第五章 監督及救濟制度之設計

第一節 監督及救濟制度作為規範實

現之確保

在前述不同層次的資訊處理，我們已經檢視了相關應遵守的原則及個資法的規定，法規仍有改進空間是一回事，但畢竟已有一定的法制可為保護的依據，不過，這些規範能不能發揮效果，相當大程度仍繫於監督及救濟的制度，因為要求非公務機關如何如何、禁止非公務機關如何如何，當他不遵守時如果沒有一定控制的手段，這些要求或禁止就只是空中樓閣。

第一項 監督制度

就監督制度而言，可以分為內部監督和外部監督，前者是業者的自我檢查作

用，後者則是行政機關的監督作用。

而各國立法例對於監督機關之設置，可分為：A 設立獨立之監督官或委員會；B 僅由原行政機關自行監督。而欲其真正發揮制度功能，達到管制之效用，有賴具有相當權能，並且有超然地位的機構加以推動予監督始可奏效，尤其，資訊處理深具科技專業性，一般機關監督能力恐怕有所不足，這也是各國立法中甚多設有此類機關（採 A）的原因⁶¹。

關於其他國家的監督制度設計，以下介紹德國及瑞典二個例子。德國聯邦個人資料保護法就非公務領域之保護監督制度，設計多層的監督系統，由業務保護資料監察人（以下簡稱資料保護人）擔任「自我監督」之工作，企業參決會擔任「集體監督」之任務，以及由國家監督機關擔任「外部監督」之工作。該法於一九九一年修正時，將資料保護人擔任內部監督制度之任務予以確立並加強不得任意撤換之規定，以強化其獨立行使監督權之能力。關於資料保護人之任免、義務、組織及任務該法有詳盡之規定。⁶²相較於對公務機關監督所設計的「資料保護監察使」，資料保護人受任於業者，權力遠遠不及，但或許是因為就公務機關而言，機關監督是內部，所以有創設獨立保護監察使之需要，但對非公務機關而言，機關監督是外部，所以認為不需要具超然獨立地位之資料保護監察使的設置吧。

瑞典改正資訊法則規定有「資料檢查院」，由政府選任之主席以及財經、民眾所選任之十名董事予以組成，並不受行政機關之監督與支配，尤其，其對任何資訊處理機關所為資訊處理行為之監督與檢查，在該法之領域內有絕對效力。其權威性更超過德國之資料保護監察使⁶³。

歐盟 1995 資料保護指令第二十八條亦規定：「各會員國應設立一或多個公務機關，負責監督會員國依據本指令所訂定之法規於其境內之適用情形。該等機關應完全獨立行使職權。」並明確要求該等機關應被賦予調查權、有效干預權、參加訴訟或移送司法機關之權力等⁶⁴。

第二項 救濟制度

在救濟制度方面，固然，針對資訊時代之特性，資料保護法強調防免個人資料保護之風險，而要求採取種種預先之措施，但不可否認事後法律責任之追究仍屬必要，才能達成個人資料權的周全保護。不過，若在民、刑法原已存在保護隱私法益規定的情況下，是否有必要製造不同的構成要件和責任內容？存在爭論

⁶¹ 參照黃三榮，個人資料之保護——兼評我國電腦處理個人資料保護法，資訊法務透析，頁 51（1998/1）；翁岳生等，資訊立法之研究，行政院研究發展考核委員會委託研究，頁 138（1994/7）

⁶² 參照洪榮彬，資訊時代之資料處理與資料保護——以德國聯邦個人資料保護法為中心，輔仁大學法研所碩士論文，頁 275（1993/6）

⁶³ 參照翁岳生等，資訊立法之研究，行政院研究發展考核委員會委託研究，頁 139-140（1994/7）

⁶⁴ 歐盟 1995 年資料保護指令之中譯，參照熊愛卿、詹文凱合譯，歐盟 1995 年資料保護指令，收錄於熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，附錄（2000/7）

⁶⁵。本文認為，即便傳統民、刑法典已有保護隱私法益之規定，其條文必仍屬抽象概括，什麼情形算侵害「隱私」，什麼東西叫「秘密」，本有解釋空間，而在資訊時代變換萬千的事實態樣下，如果沒有較為具體的標準，法官一定會有無從下手之感，甚至淪為恣意而令人民無所適從⁶⁶；如同上位的隱私權概念已經走到具體的個人資料權，抽象的保護規定也應該在個人資料權的面貌下去具體形塑，尤其在要求或禁止的規定已經做成的情形下，將這些誠命的違反和損害的價值作某種連結，應該是很可以考慮的方式。不過，刑罰的採取總是應該較為謙抑，特別是此種新興權益的保護，某種程度的違犯被認為是「犯罪」，是不是符合一般人民的法律感情？可能還是值得思考的問題。

第二節 對我國法制之檢視

第一項 監督制度

在我國個資法下，行政監督之機關為目的事業主管機關，如無目的事業主管機關，依個資法第四十二條第二項，由法務部負責。監督手段部分，包括登記或許可、行政檢查及扣押，以及行政處罰或其他不利益處分等。

首先，個資法第十九條規定：「非公務機關未經目的事業主管機關依本法登記並發給執照者，不得為個人資料之蒐集、電腦處理或國際傳遞及利用。徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人，應經目的事業主管機關許可並經登記及發給執照。前二項之登記程序、許可要件及收費標準，由中央目的事業主管機關定之。」要求非公務機關若欲為個人資料之蒐集處理，一定要先經登記並發給執照的程序，否則不得為之，對徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人，甚至是採取許可制。而依第二十條第二、三項，於業務終止時應為終止登記，並將其保有個人資料之處理方法陳報目的事業主管機關核准。而違反前開第十九條規定者，依第三十八條目的事業主管機關處負責人新台幣二萬元以上十萬元以下罰鍰，並令限期改正，逾期未改正者，按次處罰之。而違反第二十條第二項者，依第三十九條，由目的事業主管機關限期改正，逾期未改正者，按次處負責人新臺幣一萬元以上五萬元以下罰鍰，情節重大者甚至可撤銷許可或登記。其目的在透過登記或許可之方式，掌握非公務機關蒐集、處理個人資料之相關資訊，便於之後的追蹤和監督。

其次，個資法第二十五條規定：「目的事業主管機關，認有必要時，得派員

⁶⁵ 相關討論參照翁岳生等，資訊立法之研究，行政院研究發展考核委員會委託研究，頁 142-144（1994/7）

⁶⁶ 參照陳仲麟，電腦處理個人資料保護法與民、刑法的縱橫交錯，全國律師，第四卷第十二期，頁 34-35（2000/12）。

攜帶證明文件，對於應受其許可或登記之非公務機關，就本法規定之相關事項命其提供有關資料或為其他必要之配合措施，並得進入檢查。經發現有違反本法規定之資料，得扣押之。對於前項之命令、檢查或扣押，非公務機關不得規避、妨礙或拒絕。」而對於該命令、檢查或扣押若規避、妨礙或拒絕，依第四十條，由目的事業主管機關，按次處負責人新臺幣一萬元以上五萬元以下罰鍰。目的乃在透過行政檢查之方式，實際查悉非公務機關有無違反個資法之情事。

其他如違反個資法中對個人資料保護之各項規定，分別情形依第三十八、三十九、四十條，可能施以罰鍰、限期改正處分、撤銷許可或登記等效果，凡此均係藉由行政機關的處罰或其他不利益處分，督促非公務機關遵守個資法之規定。故上述規定與前述第三章資訊的取得、利用、管理、傳遞等層次均有相關。

不過，首須注意的是，個資法的適用對象並非所有的私人，也就是說，非屬個資法適用對象者，不管上述監督規定如何，其實都與之無涉。個資法第三條第七款對非公務機關的定義為「公務機關以外之左列事業、團體或個人：（一）徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。（二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。（三）其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」因此，從事電子商務的業者，如果屬於上數列舉之事業、團體或個人，就受個資法規範，反之則否。

問題是所謂的「電信業」會不會包括所有的電子商務經營網站呢？依電信法第十一條規定，「電信事業分為第一類電信事業及第二類電信事業。第一類電信事業指設置電信機線設備，提供電信服務之事業。前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。第二類電信事業指第一類電信事業以外之電信事業。」由於電信法對於電信事業之範圍未明確加以界定，因此，必須由登記實務來判斷什麼樣的網站屬於第二類電信事業的範圍。依據交通部電信總局所公布的經營第二類電信事業申請書之附件「經營業務申報表」中，將第二類電信事業區分為語音類、數據類及視訊類，其中與網站最相關的是數據類，包括：

- (a)網際網路接取業務(Internet access service)；
- (b)X.25 分封交換數據通信業務(X.25 Packet switched data network service)；
- (c)線上資訊業務(On-line information service)如資訊儲存、檢索及資訊處理業務；
- (d)電子文件業務(Electronic mail service)，如電子文件存送業務；
- (e)電子佈告欄業務(BBS)；
- (f)電子資料交換業務(Electronic Data Interchange service)；
- (g)數據網路業務(Data network service)如文字處理編輯功能、資料格式與編輯通信協定之處理及轉換業務；
- (h)交易服務業務(Data transaction service)，如航空訂位系統業務、遠端交易業務；
- (i)傳真存轉業務(Store & forward facsimile service)；
- (j)國內衛星小型地球電臺數據網路業務(VSAT data network service)；

- (k)寬頻交換(數據部分)通信業務；
- (l)數據交換通信業務；
- (m)其他。

前述各項分類中，(a)、(c)、(h) 等項很明顯地將ISP、入口（搜尋）網站業者、遠端交易系統（一般所稱電子商務業務應均包括在內）這些網站經營歸屬於第二類電信事業，至於一般ICP，若僅單純提供內容而不涉及交易，原則上是不屬於第二類電信事業。然而，依目前網路世界的生態來看，經營者雖然有不少是屬於第二類電信事業，但於交通部電信總局所公告已登記之家數卻非常少，且多屬於ISP業者，經營電子商務的業者雖然多如牛毛，但是已依法進行登記的卻寥寥無幾。⁶⁷不過，無論是否已經向電信總局進行登記經許可，在解釋上，只要已經有經營前述業務的事實，就應該被歸類為第二類電信事業，也就要受到個資法的規範才對，則如採取此種解釋，從事電子商務之事業，均會因解為電信業而受個資法的規範。

當然，個資法的「電信業」是否如此解釋仍有待法院的確認，畢竟一般觀念中的電信範圍並沒有那麼廣。不過更根本的問題是，個資法如此限縮其適用範圍，當年或許是為了新法實施，不欲打擊過廣，以利推行，也或許是鑑於行政管制能量不足，故僅以對個人資料需求較大之產業為對象，但就法理上而言，法律關心的重點應是在法益的保護，一個侵害法益的行為即使不是特定行業所為，法律也應予限制，一個非法益侵害的行為就算是特定行業所為，也不該成為限制的對象；因此，即使政府認為現階段其管制能量不足，沒辦法顧及所有的事業，而將登記、監督等行政管制措施侷限於侵害可能性較大的特定行業，也不該讓民事求償和刑事處罰都受到此種限制，因為法益的侵害和行業別無關，民、刑案件也和行政機關的施政便宜考量無涉，如此區分只是又突然增加法體系的紊亂罷了。一個對不同業者違反平等的差別待遇，假如沒有足以通過比例原則的政府利益，那恐怕就有違憲的嫌疑了⁶⁸。總之，基於行政便宜性和資源分配的效率考量，一部份的行政管制監督措施（如登記等）是有容許設一定限制的可能，但就行為限制的部分，例如要求蒐集個人資料要有特定目的經當事人同意云云，為什麼有些人應遵守，有些人卻不必？當該等規定遭到違反時，對有些人行政機關為什麼就無法處罰？實在沒什麼道理。故對於個資法的適用範圍，論者多有認為應擴大者⁶⁹；據報載，法務部的修正草案，亦朝向將「化外之業」納入的方向⁷⁰。

接下來，關於監督機關，我國仍由原已工作飽和、未見專業能力與素養，更欠缺超然獨立地位之一般公務員，擔任監督工作，執行成效實堪懷疑，故論者均

⁶⁷ 劉承愚、賴文智、顏雅倫，網路事業經營必讀，頁 161-163，台北，元照（2001/5）

⁶⁸ 陳仲麟，電腦處理個人資料保護法與民、刑法的縱橫交錯，全國律師，第四卷第十二期，頁 34（2000/12）

⁶⁹ 參照簡榮宗，網路上資訊隱私權保障問題之研究，http://taiwanic.com/alan/alan4-08_7-2.html（2001/2/16 瀏覽）；陳仲麟，電腦處理個人資料保護法與民、刑法的縱橫交錯，全國律師，第四卷第十二期，頁 34（2000/12）；熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，頁 232（2000/7）

⁷⁰ 自由時報，2001/4/16

主張應考慮設置獨立機關以發揮監督作用⁷¹。

第二項 救濟制度

關於個資法適用範圍之問題於本節前項已經提及，假如認為從事電子商務業者均屬個資法規範對象，則各種救濟制度在本文尚稱單純；倘若認為可能存在不屬個資法規範對象的業者，則民、刑事責任體系將十分混亂。本文暫採前說，故對後說情形下的民、刑事責任體系⁷²略而不提，合先敘明。

行政途徑：本節前項述及各種行政監督措施，其終極目的也在維護人民的個人資料權，不過上述行政監督措施，固然是機關的法律義務，但若要說當事人有公法上請求權，恐怕就有問題。例外是在個資法第三十二條，雖是以行政處分手段實現，但係人民請求救濟的途徑之一，故本文於此說明，該條規定：「當事人向非公務機關行使第四條所定之權利，經拒絕後，當事人得於拒絕後或期限屆滿後二十日內，以書面向其目的事業主管機關請求為適當之處理。前項目的事業主管機關應於收受請求後二個月內，將處理結果以書面通知請求人。認其請求有理由者，並應限期命該非公務機關改正之。」第四條也就是當事人對其個人資料一查詢及請求閱覽、二 請求製給複製本、三 請求補充或更正、四 請求停止電腦處理及利用、五 請求刪除之權利；故倘若非公務機關拒絕當事人這些請求，當事人可以向目的事業主管機關請求救濟，主管機關應限期命非公務機關改正。

民事賠償：個資法第二十八條規定：「非公務機關違反本法規定，致當事人權受損害者，應負損害賠償責任。但能證明其無故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第五項之規定。」此為民法侵權行為的特別規定，採取的是中間責任，受害人無須證明非公務機關有侵權的故意過失，除非該非公務機關證明其無故意或過失，才能免責。另，個資法對賠償額有特別限制，時效亦與民法不完全相同，附帶提及。

刑事責任：個資法第三十三條規定：「意圖營利違反 第十八條、第十九條第一項、第二項、第二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金。」第十八條為非公務機關對個人資料蒐集或電腦處理所作的規範，而所謂「電腦處理」依第三條第三款規定，包括使用電腦或自動化機器為資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理，第二十三條則是關於非公務機

⁷¹ 參照洪榮彬，資訊時代之資料處理與資料保護——以德國聯邦個人資料保護法為中心，輔仁大學法研所碩士論文，頁 355（1993/6）；黃三榮，個人資料之保護——兼評我國電腦處理個人資料保護法，資訊法務透析，頁 51（1998/1）；翁岳生等，資訊立法之研究，行政院研究發展考核委員會委託研究，頁 138（1994/7）；簡榮宗，網路上資訊隱私權保障問題之研究，http://taiwanic.com/alan/alan4-08_7-2.html（2001/2/16 搜尋）；熊愛卿，網際網路個人資料保護之研究，台灣大學法研所博士論文，頁 233（2000/7）。

⁷² 對此可參照陳仲麟，電腦處理個人資料保護法與民、刑法的縱橫交錯，全國律師，第四卷第十二期，頁 34-35（2000/12）。

關對個人資料利用之規範，故凡此類行為業者意圖營利違反第十八條、第二十三條之規定致生他人損害，應受刑罰制裁，故本條與前述第三章資訊的取得、利用、管理、傳遞等層次均有相關；另外，違反第十九條登記或許可之規定，及第二十四條對國際傳遞及利用之限制命令者，亦同此刑罰效果。附帶提及刑法第三百十八條之一的洩漏電腦秘密罪，與此可能構成法條競合，適用個資法規定已足。

第三十四條則規定：「意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法輸出、干擾、變更、刪除或以其他非法方法妨害個人資料檔案之正確，致生損害於他人者，處三年以下有期徒刑、拘役或科新臺幣五萬元以下罰金。」主要係在確保個人資料的正確性不受破壞，而與前述第三章第三節資訊的管理層次的安全保護問題相關，且對象除非公務機關本身之外，亦在嚇阻第三人侵入非公務機關電腦系統為破壞行為。與安全保護部分相關者，除了個資法第三十四條是規範妨礙個人資料正確性行為，若是偷窺個人資料檔案，有可能解釋為構成刑法第三百十五條妨害書信秘密罪：「無故開拆或隱匿他人之封緘信函、文書、圖畫者，處拘役或三千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。」⁷³若是複製檔案，則可能解釋為構成刑法第三百二十條竊盜罪：「意圖為自己或第三人不法之所有，而竊取他人之動產者，為竊盜罪，處五年以下有期徒刑、拘役或五百元以下罰金。」因為刑法第三百二十三條規定：「電能、熱能及其他能量或電磁紀錄，關於本章之罪，以動產論。」另外若檔案內容是著作權法保護的客體，亦有著作權法第九十一條重製罪之問題⁷⁴。

第三十五條：「公務員假借職務上之權力、機會或方法，犯前二條之罪者，加重其刑至二分之一。」第三十六條：「本章之罪，須告訴乃論。」第三十七條：「犯本章之罪，其他法律有較重處罰規定者，從其規定。」

⁷³ 參照蔡美智，電腦駭客入侵的法律問題，資訊與電腦，二一七期，頁 66；但黃榮堅教授認為會有一些解釋上的問題，首先，並不是所有的電磁紀錄都是文書，不是文書的就無法以本條加以規範，其次，封緘應該是針對日常生活中實體的信函而言，對於電磁紀錄沒有所謂的封緘，即使對電磁紀錄經過加密處理，其作用等同於信函或文書的封緘，但條文的用字就是如此，不能不加以考慮。當然，在立法者之主觀意願及立法之客觀需求的因素下，此一文字的擴張解釋在現實上是勢所難免，到最後真正必須認真以對的倒是，至少在解釋上，參考德國刑法條文之規定，被入侵之行為客體如果是屬於電磁紀錄，必須是特別經過加密處理的（而且具有文書性質的）電磁紀錄，參照黃榮堅，刑法增修後的電腦犯罪問題，收錄於罪與刑，頁 312-313（1998/10）

⁷⁴ 參照蔡美智，電腦駭客入侵的法律問題，資訊與電腦，二一七期，頁 67；但黃榮堅教授認為，竊盜罪當中所謂竊取，刑法上的解釋是，破壞原持有人的持有支配關係而建立新的持有支配關係，然而在竊取電磁紀錄的情形（事實上指的應該就是重製），原持有人並未因此喪失他對電磁紀錄內容的持有支配關係，因此不管把電磁紀錄做怎麼樣的解釋，這一條文的適用可能性都有問題，解決的方法是，我們可以把竊取的定義修改為僅以建立新的持有支配關係為要件，而不必以破壞原來的持有支配關係為要件，參照黃榮堅，刑法增修後的電腦犯罪問題，收錄於罪與刑，頁 314-316（1998/10）。另外黃榮堅教授又認為此一規定會被著作權法架空，因為不是著作權法保護的客體就不是值得保護的財產利益，也不應論以竊盜罪，但本文認為未必如此，至少個人資料的集合可能不是著作，卻具有財產利益（除了隱私利益外也是有財產價值的）。

第六章 結論

本文的小小貢獻，大概就是將電子商務底下個人資料保護的問題，作一個概括的瀏覽吧。除了對電子商務稍作介紹，再來就是從上到下，形塑隱私權具體化到個人資料權，再具體化到法制應有的原理原則，並以此為基礎，分別就縱向、橫向層面的個人資料保護，作理論、外國法制及我國規定的探討。

本文將隱私權定義為對個人領域的事務的控制權，並在這樣的上位概念下提出個人資料權的權利型態，以之作為個人資料保護的基礎。由於電子商務環境所具有的特性，對個人資料權產生深度衝擊，吾人須對此種環境下的個人資料保護投以更多的關注，國家亦應建立妥善法制以促進個人資料權的實現。

在處理個人資料的不同階段，將遭遇不同的問題及需要不同之因應措施，故本文區分資訊的取得、利用、儲存管理及傳遞等層次加以討論。在資訊的取得部分，鑒於電子化網路化對個人資料所帶來的威脅，應採取限制蒐集原則，我國個資法之規定就此尚有改進的餘地；在資訊的利用階段，應採取限制利用原則，個資法之規定充斥過多抽象概念，對個人資料保護尚嫌不足；在資訊的管理面，個資法就安全保護上僅簡略規範，有再思考的空間；關於資訊的傳遞，個資法因未直接規定，但解釋上仍應受第十八條規範。最後，徒法不足以自行，沒有具實效的監督、救濟制度，不管如何的良法美制都將落空，就此個資法是否應引進獨立監督機關之設置值得考慮。

另一方面，是否應該就不同性質的個人資料保護，給予不同的制度規範，是進一步應思考的問題，找出核心的敏感性資料值得參考，但或許也只是個開始。

當然，本文的觀察其實仍十分簡陋，對個資法的檢討並不全面，在隱私權與國家追求的其他利益的衡量上，尤感難以負荷，權利的保護必須付出代價，畢竟是我們需時時刻刻放在心上的；特別是，自己回首再讀本文，有一種強烈的無力感，個資法施行已快要六年了，但它的理想和現實的落差是多麼地大，即使我們將來將許多規定上的缺失和不足都補完了，真的就能讓我們享有個人資料免於侵害的自由嗎？或是這種傳統的管制手段已經江郎才盡，有待在管制理論上重新思考？我不知道。只能說，權利的保護總是不斷從抽象走向具體，從粗糙走向精緻的吧，對權利實現有益的方向，還是我們應選擇的路，在享受科技所帶來的便利時，應體會這把雙面刃亦給我們傷害，資訊科技應是為人而服務，當它鬆動了人性尊嚴的個人價值追求時，我們須以戒慎恐懼的態度嚴肅面對，這應該是沒有疑問的吧。