RDEC-RES-097-010（委託研究報告）

政府機關強化個人資料保護措施之研究

行政院研究考核發展委員會編印
中華民國九十八年十月

（本報告內容及建議，純屬研究小組意見，不代表本會意見）

RDEC-RES-097-010（委託研究報告）

政府機關強化個人資料保護措施之研究

受委託單位：東吳大學

研究主持人：林桓副教授

協同主持人：余啓民副教授

研　究　員：簡榮宗、葉奇鑫

行政院研究考核發展委員會編印

中華民國九十八年十月

II

目　次

表　次

圖　次

提　要

<研究緣起>

隨著電子科技日益精進，利用電腦蒐集、處理及利用個人資料日益普遍，攸關個人隱私等足資辨識個人之資料保護更形重要。然而，在英國「隱私國際」與美國「電子隱私資訊中心」公布 2007 年國際隱私權評比，第一次被評比的台灣，成績落後，值得重視。又，近來國內多次傳出個人資料經由網路或電視購物外洩或詐騙情形，突顯了台灣公、私部門應強化對於個人資料保護的重要性。故確有必要先瞭解目前台灣公務機關、非公務機關在蒐集、處理及運用個人資料時，可能會產生遭遇到那些問題，而目前各部會在面對非公務機關於蒐集、處理及運用個人資料時，究竟應該扮演什麼樣的角色及如何進行監督。實值探究。

許多先進國家如美國、歐盟、德國、日本等均訂有個人資料保護相關法制配套，對於推動個人資料保護之組織、法制及配套措施等已累積相當的經驗，足資我國借鏡。本研究有必要參考國外推動經驗，探討如何強化政府機關在蒐集、處理及運用民眾個人資料保護的具體作法與配套措施，

<研究經過 研究方法>

本研究計畫經初步利用法源法律網蒐集新聞事件(個案分析法)並統計後決定重要爭點(歷史文獻分析法)，之後側重就醫及就學資訊、網路購物、金融、電信等作爲主要縱向議題探討進行，另加入資訊安全角度加以衡量，並輔以國外法例深入進行問題分析與建議（比較分析法）。另參酌專家訪談結論後(專家訪談法)，形成具體結論與建議事項，以供各部會施政參考運用。

<重要發現及主要建議>

我國政府機關針對強化個人資料保護雖已卓具成效，但部分法制及行政配套措施及執行面仍未臻完備，本研究提供如下建議，謹供未來相關施政之參考。

一、立法部分

(一)短程建議

1. 對於個資法修正之進一步建議

個資法修正草案歷經多個會期未能順利通過三讀，雖對於個人資料保護面向有所缺憾，但反由補強充實面觀之，卻是對於法律完備度的潛在契機。建議新法案送交立院審議時能就本研究提出之問題，進一步釐清增訂：

(1)特殊敏感性個人資料的定義範圍(草案第 6 條)之再釐清。條文中之醫療、基因及健康檢查三者間之關係，建議於立法說明中，詳析其區別實益，以杜未來適用疑慮。

(2)草案第 15 條有關公務機關得依特定目的，爲個人資料之蒐集與處理一節，明訂三種例外情況。建議應尊重當事人之資訊自決權，對於「於執行法定職務之必要範圍內」及「對當事人權益無侵害時」的兩種情況，仍應考慮須經當事人書面同意之告知，而不可直接對個人資料予以蒐集或處理。

(3)草案第 16 條有關公務機關得爲特定目的外之個人資料之利用的七種例外情況，有待進一步檢視其是否過於寬鬆，並設計監督機制，以避免對個人資料利用之浮濫。

(4)對於草案第 19 條及第 20 條有關非公務機關對於個人資料之蒐集、處理及利用之例外規定，亦建議一併予以配合調整檢視。

（主辦單位：法務部；協辦單位：行政院衛生署）

(二）中、長程建議

1. 對於資訊安全法制位階調整化之建議摘錄爲建議宜將其法源提升至法律的法位階層次

如本章第一節所述，我國目前有關資訊安全之法制，多均以行政規

則定之。建議(資通安全會報)宜將其法源提升至法律的法位階層次，並建議參考 OECD 指導原則等外國立法例，以提高資訊安全的重視程度。而一旦有了法律位階的設計後，未來該法律之主管機關爲何(國家通訊傳播委員會？)，亦須審慎評估。

（主辦單位：行政院資通安全會報　協辦單位：國家通訊傳播委員會）

2. 對於個別產業管理相關法制建議

個資法草案已將非公務機關的適用行業(「八大行業」)別予以打破，進而全面適用於所有行業，但爲因應現行個資法之規定，原「八大行業」多有細部規定有關個人資料保護之處理原則(如電信業電腦處理個人資料管理辦法)，未來個資法全面適用各非公務機關之行業時，現行相關處理原則及管理辦法勢必要重行檢視及調整，另針對特殊產業，是否仍有必要(如就醫資訊相關產業)，另行訂定新的處理原則，亦爲個資法通過施行時之一大考驗，建議主管機關(法務部)即早透過公聽方式，獲致共識，以爲因應。

（主辦單位：法務部; 協辦單位：行政院衛生署、國家通訊傳播委員會、行政院金融監督管理委員會、教育部）

3. 電子簽章法之配合檢視

本研究建議未來爲有效管控個人資料之保護、杜絕不當個資外洩，宜採用憑證安全機制。然現行自然人憑證之推廣應用面如將擴及其他應用，勢必牽涉原自然人憑證之憑證作業基準或憑證互通應用，建議於電子簽章法修法(經濟部商業司)時，配套評估考量。

（主辦單位：經濟部商業司; 協辦單位：經濟部工業局）

二、行政部分

(一)短程建議

1. 輔導獎勵之建議

本研究中引用德國及日本有關隱私標章認證制度之推行，建議相關單位(研考會、經濟部、內政部、財政部、金管會、法務部等)，審慎評估。在非公務機關標章制度推廣方面，經濟部或可藉由商業登記之便進行，在公務機關部分，內政部主管業務(如戶政、警政等資料)繁雜，事涉個人資料保護強化者較多，另有關金融隱私部分亦建議財政部及金管會共同研議，故建議由個資法中央主管機關之法務部會同上述部會共同研商規劃。

（主辦單位：法務部;協辦單位：行政院研究發展考核委員會、經濟部、內政部、財政部、行政院金融監督管理委員會）

2. 監督機制之建議

無論前述之隱私標章認證制度是否在我國順利推展，個資法草案通過，全面適用於所有行業後，對於較易造成個資外洩之電信業或無店面零售業等，相關主管機關均有必要對於其管理及監督機制及法規進行調整。

(主辦單位：經濟部; 協辦單位：行政院消費者保護委員會）

（二）中、長程建議

1. 組織建置之建議

本章第二節有關公務機關部分建議時，所提出之「資訊保護官(類似機制）」設置，建議由行政院做整體及各級機關組織調整時之參考。以目前就學資訊個人資料外洩事件頻繁爲例，或全非資訊安全設備建置之問題，反多爲人爲因素所致。而此問題之發生，在於整個資訊安全「規劃、執行、檢查、改善」流程中，對於「檢查」及「改善」階段中，欠缺有效監督機制所致。以各級學校或相關學術單位爲例，主管機關(教育部)確依規劃階段要求所屬各級學校完成一定資安標準認證，然實際操作時由於欠缺監督檢查機制，造成學校內徒有認證之名，而無資安保護之實。故，本研究建議，除依現行規

定要求各級機關行政副首長爲資安負責人外，更應積極規劃類似「資訊保護官(類似機制)」之相關人員，以收監督實效。

（主辦單位：行政院人事行政局；協辦單位：行政院研究發展考核委員會、教育部、交通部、行政院行政院金融監督管理委員會、行政院衛生署）

2. 預算補助之建議

承上所述，監督檢查人力之編制，涉及人事預算之編列。另對於非公務機關之中小企業，是否考慮資安強化建置之補助(行政院經建會)，有待進一步檢討規劃。所謂「徒法不足以自行」，個人資料之保護雖有相關法律做爲後盾，然在數位匯流的時代中，降低個人資料外洩，仍有賴設備及技術面之偵測、預警及防堵。另在各級機關設備經費預算編列上，有否考量設計一定比例之資安預算，以維設備採購及維護之基本預算。

（主辦單位：行政院經濟建設委員會；協辦單位：經濟部、教育部、行政院衛生署）

第一章　緒論

第一節 研究主旨（主題、緣起及預期目標）

隨著電子科技日益精進，利用電腦蒐集、處理及利用個人資料日益普遍，攸關個人隱私等足資辨識個人之資料保護更形重要。然而，在英國「隱私國際」與美國「電子隱私資訊中心」公布 2007 年國際隱私權評比[1]，第一次被評比的台灣，成績落後，值得重視。台灣在該評比中被認爲有以下幾項重點：(1)隱私權保障未於憲法條文中明訂保護，而是散見於其他權利保護中;(2)有資料保護之特別法律; (3)資料外洩導致相關犯罪;(4)非法監聽情況嚴重，而合法監聽數量一年內超過 25,000 件，不過合法的定義過於寬鬆造成人權保障不周;(5)紙本的身份證件被要求指紋身份辨識，並且已發展自然人憑證制度且發卡量已超過百萬; (6) 健保卡已採用晶片卡，並且晶片儲存相關病歷資料; (7)居留超過三個月之外國人必須進行愛滋病(HIV)的強制檢測，如發現爲帶原者將強制驅逐; (8)政府現正積極推定無線射頻身份辨識(Radio Frequency Identification)相關技術發展與應用。 針對上述國際評比對於台灣的描述，可謂真假參半。我國政府實際上於近年來刻正積極進行個人隱私的保護。針對國際評比之指稱，簡述國內發展如下：

一、我國憲法本文及增修條文之規定，雖並未明文保障隱私權，但釋字第二九三號解釋首次肯認隱私權存在，大法官言及並正面肯定維護人民之隱私權。此項解釋具有幾個重要意義：肯定隱私權是憲法上的權利，屬憲法第二二條人民之其他自由及權利，應受憲法之保障；隱私權的保護，並非絕對，爲防止妨礙他人自由，避免緊急危難，維持社會秩序或增進公共利益之必要，得以法律限制之(憲法第二三條)。後釋字五三五號解釋文再次明確使用隱私權，並確認隱私權爲憲法二二條概括基本權所保障。釋字五八五號解釋理由書提及「保障個人生活秘密空間免於他人侵擾及個人權利之自主控制」爲隱私權保護之內容，後釋字六零三號解釋並明確定義何爲資訊隱私權，再次確

[1] 詳如網址：http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597

認其亦受憲法二二條保障[2]。

二、台灣雖在 84 年已頒行「電腦處理個人資料保護法」(以下簡稱『個資法』)，惟僅適用於部分行業，且該法執行、監理、處罰的權責又分散在各部會，以致該法之落實確有待努力。配合第 7 屆立法院改選後，法務部已重行將前開法案名稱修正爲「個人資料保護法」草案，擴大保護客體並強化個人資料保護規範，立法院已經針對法務部提出之行政院版草案進行二讀程序，本會期預計通過該法律。除法制面外，機關間協調、組織功能提升以及完善配套措施等層面亦值得關注。

三、個人資料外洩情事確有發生，從個資法的分類言，公務機關與非公務機關均有發生，其中非公務機關部分，依舊法分類觀之，又以電信業及金融業較爲民眾所關切，的確是有待解決的議題。

四、健保晶片(IC)卡運用一節，健保卡的正式名稱是「健康保險憑證」，其用途只在證明就醫者爲被保險人的事實。之前使用的紙卡設計，即已符合這樣的需求，民間其他醫療保險憑證的設計，也是如此。健保局規劃的健保ＩＣ卡，其實是結合了「保險憑證」、「醫療紀錄」以及「身分識別證件」的功能。這種連結造成用肉眼不能檢視其內容正確性的ＩＣ來製作，會有侵害被保險人權益之虞。故健保ＩＣ卡對個人隱私的侵犯，就其癥結，在於個人不能決定其晶卡片上的記載項目及其內容正確性；在於個人無法控制其個人醫療資料在系統中的私密性[3]。其實在實務運作上，參與全民健保的民眾，如果希望就醫記錄需要做保密，不希望被其它醫療院所讀取，可設定 4 到 6 位數的密碼，民眾只要前往投保單位例如區公所或是大型醫院的公共資訊服務站，利用健保卡機設定後，就醫時，除非患者輸入密碼，否則醫師無法讀取就醫記錄。特別是 AIDS 及精神疾病的病患隱私更被注意，患者也可以選擇不登錄在健保卡裡。密碼保護原爲政府保護民眾的隱私而設，但有些喜歡逛醫院的患者，會有重複治療的問題，導致浪費醫療資源。一旦設定密碼後，除非患者

[2] 「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並爲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，隱私權乃爲不可或缺之基本權利，而受憲法第二十二條所保障」。參見大法官會議第 603 號解釋文。

[3] 莊庭瑞，從健保 IC 卡談個人資料保護，自由時報 91.08.06 自由廣場，http://www.tahr.org.tw/site/PDPA/Juang.htm

輸入密碼，否則醫師無從得知就醫紀錄與用藥情形，若病患習慣尋求多間醫院不同醫師診治致重複治療，反有損健康；如同金融卡一般，民眾只要按錯三次密碼，將導致鎖卡，必須繳回原卡到健保轄區分局。[4]

五、針對 HIV 檢測一節，其爭點在於後天免疫缺乏症候群防治條例第十八條之規定，針對上述條文之指摘，其實仔細研究該條例修法的立法重點可以清楚理解，該條例已有通盤檢討以因應後天免疫缺乏症候群之疫情變化需求，爲強調人權保障之精神，於立法意旨中增列保障人類免疫缺乏病毒感染者之權益等文字；另有鑑於感染者屢發生被棄養、被拒絕提供醫療等情事，爰增列感染者之安養、居住、就醫及隱私等基本權利，均予保障；增訂中央主管機關應邀人類免疫缺乏病毒感染者權益促進團體、相關學者或專家、民間相關機構代表及目的事業主管機關代表，與推動人類免疫缺乏病毒傳染防治及感染者權益保障事項；新增醫事機構及醫事人員不得拒絕提供感染者必要之服務、保護感染者隱私權及基本人權、檢驗前應提供諮詢及知後同意始得抽血檢驗等。[5]

更且甚者，近來國內多次傳出個人資料經由網路或電視購物外洩或詐騙情形，突顯了台灣公、私部門應強化對於個人資料保護的重要性。因此，我們確有必要先瞭解目前台灣公務機關、非公務機關在蒐集、處理及運用個人資料時，可能會產生遭遇到那些問題；而目前各部會在面對非公務機關於蒐集、處理及運用個人資料時，究竟應該扮演什麼樣的角色及如何進行監督。此外，許多先進國家如美國、歐盟、德國、日本等均訂有個人資料保護相關法制配套，對於推動個人資料保護之組織、法制及配套措施等已累積相當的經驗，足資我國借鏡。因此，有必要參考國外推動經驗，探討如何強化政府機關在蒐集、處理及運用民眾個人資料保護的具體作法與配套措施，本研究計畫經初步利用法源法律網蒐集新聞事件並統計後決定，研究將側重醫療及教育資訊、網路購物、金融、電信等作爲主要縱向議題探討進行，並深入進行問題分析與建議。

[4] 健保 IC 卡可設密碼保護就診隱私，http://discuz.club1069.com/redirect.php?tid=187148&goto=lastpost

[5] 參見立法理由說明，人類免疫缺乏病毒傳染防治及感染者權益保障條例，法源法律網，http://db.lawbank.com.tw/FLAW/FLAWDAT01.asp?lsid=FL013990

本研究之預期目標爲：

一、 檢視公務機關蒐集、處理及運用個人資料之現況及遭遇之問題。

民眾就醫（醫療健保記錄及病歷碼不當外洩）、就學相關個人資料（如近來大考中心資料外洩、指考及基測學生資料遭補習班不當利用等），在處理及運用上目前常因外洩而讓私人業者不當運用，致影響或侵害民眾隱私，未來除於技術、資安上有效管控外，並檢討是否應設計法規以爲因應，

二、檢視非公務機關蒐集、處理及運用個人資料之現況及遭遇之問題。

網路購物、電信資訊及金融個人資料近年來頻遭不肖人士濫用，以網路購物爲例，現行之消費者保護法針對企業經營者責任、電腦處理個人資料保護法及其修正草案中所涉之個人資料範圍、以及居於行政指導地位的「電子商務消費者保護綱領」等均爲就個人資料的隱私權保護加強保護，而有必要檢視分析，以電信資料爲例，濫發商業簡訊的問題已隨著數位匯流與行動商務的定址化服務（location based services）益形嚴重而有必要予以管理，

三、檢討各相關主管機關對非公務機關蒐集、處理及運用個人資料之監督機制。

此部分將以即將通過之個人資料保護法作爲分析重點。

四、就上開蒐集、處理及運用個人資料態樣，並參考主要國家個人資料保護之發趨勢，研提我國民眾關注之個人資料保護議題，進行問題分析、研提具體建議或配套措施。

第二節 研究主題背景及有關研究之檢討

在本計畫中所提之相關議題，將先針對我國「隱私權」定義、發展沿革及議題因應等做一釐清。

一、在隱私權方面

隱私權此一概念繼受自英美法，今日已成爲法治國的普世價值。從隱私權的起源觀察，在猶太與羅馬法時代就已出現。於19世紀，美國Cooley法官

於定義侵權行爲態樣時首先點出個人應保有獨處、不受外人干擾的權利(The Person has the right to be let alone.)，後Warren與Brandeis在其基礎上建立隱私權概念。其主張侵害個人應有保持秘密，不受公眾干擾的權利，不論在身體方面或名譽方面，甚至擴及到情感、精神等，對私人與家庭生活造成的侵害亦屬隱私權範圍，若隱私權遭受侵害，可以構成一項訴因。隱私權(Privacy)一名亦由是而來，除Warren與Brandeis所提出之獨處權理論外，美國法上又發展出其他理論闡釋隱私權。除美國外，資訊科技的進步也在其他國度造成衝擊，大屠殺陰影下的德國雖然沒有完整的隱私權體系，德國聯邦憲法法院卻也透過人口普查案判決自一般人格權進一步闡釋發展出資訊自決權理論，亦即所有的個人資料均受到保護。

資訊自決權賦予個人自我保護個人資訊資料以阻止政府機構、公司企業等不當收集、處理、傳播、利用個人資訊的權利，承認每個人對涉及個人資料提供、利用的過程皆有積極參與和自我決定、以抗拒他人恣意干涉的積極自由權，亦即所謂資訊自決權，是指個人基本上有自行決定是否將其個人資料交付與提供他人使用之權利，可拘束國家機關，並基於第三人效力理論及於私法關係，真正體現了對個人尊嚴的充分尊重。個人資料之資訊隱私權，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使用有知悉與控制權及資料記載錯誤之更正權。

二、在現有相關法制發展部分

第一項 經濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）

OECD 早於 1980 年 10 月已通過個人隱私資料保護基準(Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[6])。許多國家以該基準作爲資料保護立法的基礎。歸納該份基準，可整理出八項原則[7]。

[6] 資料來源：http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html 。

[7] 資訊服務業者配合政府公權力提供客戶資料之法制研究，頁 17-18。另可參考 OECD 網站

(一)、 限制蒐集原則（Collection Limitation Principle）

個人資料蒐集應有限制，資料之蒐集需依合法及公正之手段，且於適當之情形，應通知資料之主體及取得其同意。亦即，關於個人資料之蒐集，其蒐集對象應有界限，蒐集方法亦應有所限制。

(二)、 資料內容完整、正確原則（Data Quality Principle）

蒐集個人資料時，蒐集之資料內容，必須與蒐集使用之目的有關；而且在合乎原來蒐集目的下，做必要而合乎適當程度之蒐集；使該當資料完全正確，與蒐集時實際情形吻合。

(三)、 資料利用目的明確化原則(Purpose Specification Principle）

個人資料之蒐集目的，至遲於蒐集時必須明確化，且於其後資料之利用，不得與該當蒐集目的之達成有所衝突，於目的變更後亦應明確化。簡言之，蒐集目的必須明確化，且利用時應受該目的之限制。

(四)、 限制利用原則（Use Limitation Principle）

個人資料不應供作蒐集目的以外之其他目的之開示利用或其他使用，除非經過資料主體之同意或依據法律之規定。簡言之，利用應於蒐集目的範圍內。

(五)、 安全保護原則（Security Safeguards Principle）

對於個人資料之迭失，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。如組織管理及密碼化等安全措施之講求。

：

（1）http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html 。

（2）http://www.oecd.org/document/1/0,3343,en_2649_34255_28863233_1_1_1_1,00.html 。

（3）http://www.oecd.org/document/50/0,3343,en_2649_34267_2514994_1_1_1_1,00.html 下載OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders http://www.oecd.org/dataoecd/24/33/2956464.pdf 。

(六)、 公開原則（Openness Principle）

個人資料之蒐集作成，在實務上應採公開原則；而資料管理人之特定、資料之貯存場所之決定，個人資料之內容與性質、及其主要利用目的等，也應以公開方式確定；這種公開方式及政策，並應先以法律明定之。

(七)、 個人參加原則（Individual Participation Principle）

個人關於自己之資料，有如下之權利：得向資料管理者或其他人確認是否持有關於自己之資料；關於自己之資料得於合理期間內，於必要情形下以不過當之費用，用合理之方法，藉本身容易了解之情形，加以了解。並就前開權利之行使，如遭受拒絕時，得對其拒絕理由提出異議。且於異議成立時，得要求資料之消除、修改、完全及補充。

(八)、 責任原則（Accountability Principle）：

資料之管理人，應負責任，遵守上述諸原則，並採取各種措施，使諸原則能產生實際效果。

第二項 亞太經濟合作會議(Asian-Pacific Economic Cooperation, APEC)

由於未經授權而使用的個人資訊恐將會阻礙線上交易的成長和限制資訊社會的發展。由電子商務指導小組（APEC Electronic Commerce Steering Group）[8]於 2003 年初成立個人資料隱私權保護分組（Data Privacy Sub-Group），研擬制訂 APEC 隱私權保護原則（APEC Privacy Principles）以供該區域內之企業、消費大眾、法律協會以及保護隱私權的專家做參考，並希望藉此能在大力推動電子商務的同時，也建立起消費者的信任與信心。該隱私權保護分組完成 APEC 隱私權保護原則草案之擬定，並於 2004 年 11 月間經 APEC 部長級會議通過，成為 APEC 各會員國有關個人資料保護之最高指導綱領。

[8] 資訊服務業者配合政府公權力提供客戶資料之法制研究，頁 18-19。另可參考網站 http://www.pmc.gov.au/privacy/apec/meetings.cfm 有 2007 First Data Privacy Meeting 相關資料。

APEC 隱私權保護原則共有九大原則。

(一)、 避免損害原則（Preventing Harm）：有關個人資料之蒐集、處理與利用，不得損害當事人之權益。

(二)、 告知原則（Notice）：資料蒐集者蒐集個人資料時，應告知當事人蒐集者名稱、蒐集資料之目的、種類與用途等必要事項。

(三)、 限制蒐集原則（Collection limitation）：蒐集個人資料應符合蒐集之目的，且不得逾越必要之範圍，與目的無關之資料，不得任意蒐集。

(四)、 利用個人資料原則（Uses of Personal Information）：有關個人資料之利用，應符合當初蒐集目的之必要範圍內，未經當事人同意或另有法律規定，該資料不得作其他利用。

(五)、 當事人選擇原則（Choice）：有關個人資料之蒐集或利用，當事人有權得選擇「進入」（OPT-IN）或「退出」（OPT-OUT）模式，資料蒐集者或保有者應尊重當事人之選擇。

(六)、 個人資料完整原則（Integrity of Personal Information）：保有個人資料檔案者，有責任隨時更新或補充資料，力求該資料之完整正確，避免當事人因不正確之資料，讓其權益遭受損害。

(七)、 安全維護原則（Security Safeguards）：保有個人資料檔案者，應採取必要之安全維護措施，避免個人資料被偷竊、遺失、毀損或外洩。

(八)、 當事人查詢及更正原則（Access and Correction）：當事人隨時有權查詢或閱覽其個人資料，如發現有錯誤或欠缺者，得請求補充或更正。

(九)、 責任原則（Accountability）：對於違法蒐集或利用個人資料者，應課以法律責任，以保護資料當事人之權益。

第三項　歐盟

歐洲方面[9]，其個人資料保護的立法基礎主要源於 1950 年的歐洲人權保護公約第 8 條 (Article 8 of European Convention for the Protection of Human Rights and Fundamental Freedoms；ECHR)，該公約明文釋明人民之私生活及家庭生活應受到尊重，公部門須有法律授權或基於國家安全、經濟福祉等公益考量之必要情況下方得干涉人民之上述權利。上述意旨於歐盟理事會 (Council of Europe) 頒布的「個人資料自動化處理保護公約」(Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[10]) 再次重申，並正式產生一定的法效力，不過由於該公約亦未對一些重要名詞具體定義，各國制定之內國法基於解釋疑義導致規範標準不一，因此該公約對於隱私保護的法效力實屬有限[11]。於是歐洲議會（European Parliament）又通過歐盟保護個人資料的指令[12]，該指令正式生效後，歐盟將禁止將個人資料傳送至保護個人資料不足的國家或地區。

該指令明白賦予個人參與資訊處理的權利及隱私權受侵害時之損害賠償請求權，並落實執法機關的建置，其中對於資料傳輸至第三國的高度標準[13]，更使得指令的重要性倍增。該指令之主要內容包括一般條款、個人資料處理原則、資料當事人權利、資料控管人責任及監督機制。其中，一般條款係就

[9] 資訊服務業者配合政府公權力提供客戶資料之法制研究，頁 20。歐盟最新(2008-08-30) JOC_2008_224_R_0050_01 請參 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:224:0050:0056:EN:PDF

[10] See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 全文置於 http://www2.echo.lu/legal/en/dataprot/counceur/ conv.html （最後瀏覽日期 2009.6.30）。

[11] 周慧蓮，英國個人資料保護最新案例發展及其對我國法制之啓示，資策會科技法律中心科技法律透析，民國 94 年 1 月。

[12] 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, Official Journal of the European Communities of 23 November 1995 No. L. 281, p. 31. http://www2.echo.lu/legal/en/dataprot/ directiv/directiv.html （最後瀏覽日期 2009.6.30）

[13] 於「個人資料保護指令」當中，歐體特別要求對於將個人資料移轉或傳送至第三國情形，除非該第三國對於個人資料有適當程度（adequate level）之保護，否則將不被允許。由於歐體之個人資料保護指令條以極高立法標準對個人資料提供廣泛之保護，同時還限制個人資料移送至第三國之情形，因此與美國之立法立場有所歧異。劉靜怡，資訊隱私權保護的國際化爭議－從個人資料保護體制的規範協調到國際貿易規範的適用，月旦法學雜誌第 86 期，民國 91 年 7 月；周慧蓮，資訊隱私保護爭議之國際化，月旦法學雜誌第 99 期，民國 93 年 1 月。

立法目的、保護客體、適用主體及名詞定義等加以說明。立法目的方面，指令明白揭櫫係爲保障自然人之基本權與自由，建立最低隱私保護標準，調和各會員國間關於隱私保護立法之分歧，一方面保障會員國境內之個人資訊隱私權，一方面防止他人假隱私保護之名妨害資料流通。保護客體及於以自動化及非自動化方式處理之個人資料，但對於以非自動化方式處理之資料的保護設有一定要件限制。適用主體則兼及於公、私部門。資料處理原則方面，包括限制蒐集、資料內容完整、目的明確、限制利用等諸原則，另有敏感性資料妥善處理原則。本指令所賦予當事人之權利，除了一般常見的受告知權、資料近用權 (Right of Access)、修改或刪除權等，尚有異議權及自動個別決定拒絕權 (rights in relation to automated decision taking)。所謂異議權係指基於公益等因素而合法揭露當事人資料時，當事人得基於特殊情況之重大正當理由提出異議，異議有理由時，資料控管人即應除去相關資料。而自動個別決定拒絕權則指當事人得拒絕僅以自動化資料處理方式，就個人特定事項如工作表現、信用、可靠度、品行等爲評量，而做成對其具有法律效果或重大影響之決定。資料控管人責任主要可略分爲二：一爲資安維護責任，另一則爲損害賠償責任。至於監督機制，則以成立專責主管機關，賦予其檢查、調查、監管、參加訴訟等權限。

第三節 研究方法與過程

一、 文獻探討及法制分析

科技與法律制度的發展，多有其時間軸的延續性。所謂「古爲今鑑」，透過歷史觀察及重新思考金融付款機制的沿革及其意義，將可避免未來做出不符合歷史發展長流的制度設計。故本研究擬於相關文獻整理、分析時，側重隱私權與科技發展等與新興網路服務業(網路購物、電信及金融等)運作的歷史文獻，從探索過去的環境與衝擊，找出未來因應之建議方向。

二、 案例類型化研究

本研究擬援引「法律的生命不是邏輯，而是經驗。」的務實精神，將個案透過類型化方式，進行整理與分析，以符合法政策研究的主流方法論與應

用，更能突顯東吳法律系一貫強調英美法案例實證教學之旨。具體申言之，本研究擬利用法源法律網(http://www.lawbank.com.tw)的[法律要聞]資料庫蒐整近年來因科技快速發展利用所產生的消費資料提供相關爭議案例的整理、分析，依各該行爲所涉及之議題及國內發展趨勢加以類型化，並進一步研析在既有的法制架構(法源法律網[法規新訊]的資料庫)下，檢討個案處理的妥當性，藉此尋求可能解決問題之取向與方法，以期研究成果能與現實社會之需求契合。

三、比較法研究

由於數位匯流及網際網路的全球化發展，世界各國的制度同樣面臨挑戰與因應。爲釐清可能爭議及有效提出解決對策，比較各國法制誠有其必要。有鑒於此，本研究擬以網路資源搜尋方式，蒐集、整理歐盟、美國等相關發展及法制，輔以最新期刊論文之文獻意見，做爲本研究比較法的理論基礎。

第二章　隱私權之發展、資訊隱私與個人資料保護

第一節　前言

個人資料之資訊隱私權，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使用有知悉與控制權及資料記載錯誤之更正權。[14]

在電腦普遍運用之後，個人資料的蒐集、處理與利用更是容易。這種趨勢無疑地已強烈威脅到個人資料的隱密性，當個人資料輕易地暴露於有心人的侵襲與操控之後，個人隱私及其權益尊嚴不免飽受威脅。於是傳統上對隱私權保障的思考，乃轉向以「資料保護」（Data Protection）爲重心的思路上，「資訊隱私權」（Information Privacy）的概念乃因應而生，以對抗資訊時代中隱私權所受之衝擊。所謂「資訊隱私權」，有認爲乃指「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」，亦有認爲其意義在於「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」。簡而言之，資訊隱私權的中心思想乃在於：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。由此可見，資訊隱私權所別於古典隱私權之消極防禦性質者，在於其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，亦爲現代個人資料保護重要機制之一。

近來多次傳出個人資料經由網路或電視購物外洩或詐騙情形，更突顯了台灣公私部門應強化對於個人資料保護的重要性。因此，我們確有必要先瞭解目前台灣公務機關、非公務機關在蒐集、處理及運用個人資料時，可能會產生遭遇到那些問題；而目前各部會在面對非公務機關於蒐集、處理及運用個人資料時，究竟應該扮演什麼樣的角色及如何進行監督。此外，許多先進

[14] 大法官釋字第 603 號。

國家如美國、德國、日本等均訂有個人資料保護相關法制配套，對於推動個人資料保護之組織、法制及配套措施等已累積相當的經驗，足資我國借鏡。因此，有必要參考國外推動經驗，探討如何強化政府機關在蒐集、處理及運用民眾個人資料保護的具體作法與配套措施，特別可以從民眾關注的角度選定至少 4 項議題來探討個人資料保護議題，並深入進行問題分析與建議。本研究計畫經初步利用法源法律網蒐集新聞事件並統計後決定，研究將側重醫療及教育資訊、網路購物、金融、電信等作爲主要縱向議題探討進行，並深入進行問題分析與建議。

隱私權之概念，可分爲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。如前所述，資訊隱私權屬於積極意義的隱私權，個人資訊的主體者享有相關權利，惟其具體內容究竟爲何？試析述如下：

一、個人資訊的取得、蒐集

個人資訊的處理，密切關係到個人基本人權的保障。縱使，基於法律授權的公權力行爲，也應受憲法上一定的約束，更何況非政府機關的商業蒐集。因此，對於個人資訊的取得、蒐集，必須以適法、手段公正，且在達成目的之最小限度範圍內始得爲之。而允許蒐集的個人資料範圍也應予限制，例如思想、言論等與個人基本人權相關之資料，原則上禁止蒐集[15]。

二、個人資訊的保有、管理、利用

關於個人資訊的保有、管理、利用，基本上與前述資訊之蒐集相同，要兼顧「必要性」及「手段正當性」。惟應特別注意的是，縱使資訊取得，蒐集手段正當，但若用於蒐集目的以外，則仍構成隱私權之侵害。例如美國於 1974 年通過的隱私權法即規定，行政機關蒐集個人資訊後，除非有該法所列之例外情形，否則其公開或移轉須經紀錄關係人之書面申請或同意。此種限

[15] 參見簡榮宗，網路上資訊隱私權保障問題之研究，http://www.cyberlawyer.com.tw/alan4-08_3-4.html（最後瀏覽日期 2009.6.30）

制第二次利用的規定，正是此原則的實現[16]。

三、個人資訊之閱覽、訂正請求權

政府在今日積極國家的運作之下，適時的介入國民生活，將是無法避免而被容忍的。相對的，國民也不得不提供個人資訊。但隨著電腦科技的進步，個人的資訊隨時可能經由傳輸到達他人的手中，在此種情形下，若不賦予人民「確認個人資訊提供」之權利，則無異使個人置身於「無法確知自己是否成爲被評價對象」的狀態之中。因此，人民對於自己是否成爲他人之評價對象，或評價之基礎是否正確等確認手段之閱覽權便十分重要。而且，基於評價個人資訊正確之要求，一但發現資訊不正確時，個人當然亦享有要求訂正之權利[17]。

由上述對於「資訊隱私權」權利性的理解可知，「資訊取得、蒐集的限制」以及「資訊保有、管理、利用的規定」，係排除來自第三者干涉之權利，屬於自由權排他性的一部份。而「資訊閱覽」或「資訊訂正」，則係某種作爲的請求，在權利的性質上屬於請求權的一種。因此，資訊隱私權如傳統的隱私權一樣，其權利性除排除干涉的自由權性質外，還兼有請求權的性質。

第二節　隱私權相關法制簡介

第一項　美國

隱私權此一概念繼受自英美法，今日已成爲法治國的普世價值[18]。從隱私權的起源觀察，在猶太與羅馬法時代就已出現[19]。於 19 世紀，美國 Cooley

---

[16] 見前註。

[17] 見前註。

[18] 世界人權宣言第十二條：「任何人的私生活、家庭、住宅和通信不得任意干涉，他的榮譽和名譽不得加以攻擊。人人有權享受法律保護，以免受這種干涉或攻擊。」

[19] 當時係用 Injuria 一字表達侵害隱私爲傷害（injury）與暴行（outrage），其包含現代侵權行爲的概念，進一步衍生爲故意輕視人格的行爲。參見 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY 1 （1st ed. 1987）.

法官於定義侵權行為態樣時，首先點出個人應保有獨處、不受外人干擾的權利（The Person has the right to be let alone.）[20]，後 Warren 法官與 Brandeis 法官在其基礎上建立隱私權概念。其主張個人應有保持秘密，不受公眾干擾的權利，不論在身體方面或名譽方面，甚至擴及到情感、精神等，對私人與家庭生活造成的侵害亦屬隱私權範圍，若隱私權遭受侵害，可以構成一項訴因（Cause of Action）[21]。隱私權（Privacy）一名亦由是而來，除 Warren 法官與 Brandeis 法官所提出之獨處權理論外，美國法上又發展出其他理論闡釋隱私權[22]。隱私權的起源隱於「家是個人的城堡」（An Englishman's house is his castle）的觀念，本質上是「守密」，後 Prosser 教授整理案例法上曾發生隱私權侵害案件為以下四種態樣，並成為通說[23]。雖然 Prosser 教授之四態樣區分已成為通說，但由於隱私權並非一單一明確的權利，而為多種不同法律與理論所建構的法律空間，故適用於具體個案時，仍必須依賴法院主觀性的判斷。

---

[20] THOMAS M. COOLEY, THE LAW OF TORTS 29 （1888）.

[21] SAMUEL D. WARREN & LOUIS D. BRANDEIS, *The Right to Privacy*, 4 HARV. L. REV. 193 （1890）.

[22] 如親密關係自治說，其將公眾社會生活與私人生活或私密性關係作一分界，劃分出專屬於個人的「親密關係」加以保障，避免他人、社會、國家或其他公眾人物的侵入；「一般人格權理論」認為人格之獨立不受侵擾在現實生活的呈現，其環繞而成的共同指向即是人格的自我實現，目的在保持個人人格之完整；「資訊保留權理論」認為隱私權應只限於為將文字化、關於個人自己之資訊保密而不與人知之狀態。關於隱私權於美國法上的發展請參見：詹文凱，《隱私權之研究》，台灣大學法律學研究所博士論文， 1998 年 6 月。林建中，《隱私權概念之再思考— 關於概念範圍、定義及權利形成方法》，台灣大學法律學研究所碩士論文，1999 年 1 月，藍培青，《隱私權在美國演進歷程之研究》，淡江大學美國研究所博士論文，1997 年 5 月。

[23] （1） 使他人處於人為誤解情況之隱私權之侵害（Placing him in a False Light in the Public Eyes）－編造不實情節而扭曲他人形象，受到公眾誤解。此類型侵害與誹謗罪相類似，差別在於誹謗罪之要件必須具備惡意，但隱私權侵害並不需要。（2） 對他人生活安謐所為之隱私權侵害（Intrusion upon the Plaintiff Seclusion or Solitude or into his Private Affairs）。侵擾他人私密生活（intrusion）－此類侵害行為包括：未經同意而侵入他人生活，包括非法侵入他人住宅、臥房、非法搜索人的身體與住宅、用設備偷看他人在房間內的活動、未受許可而私拆他人信件等行為。如果這些侵擾對任何人而言都是高度冒犯與難以容忍的，便屬於隱私權侵害。（3） 公開他人之姓名、肖像或揭發其他不願為他人所知悉之私人資料所為之隱私權侵害（Publicity Given to his Name or Likeness or to private Information about him）－公開令本人感到困窘的私密事實（private facts）。此種侵權型態是指，未經許可而將他人的私生活或私人事務公諸於世，令當事人感到難堪與困窘。被公開的事實必須符合秘密性，亦即，不是眾所週知之事。公開已公諸於眾的資訊，並非隱私權之侵害。（4） 基於商業上之目的，侵犯他人人格所致之隱私權之侵害（the Commercial Appropriation of Element of his Personality）－為牟利而盜用他人姓名（簽名）與其他形象、特徵之盜用（misappropriation）。 See WILLIAM L. PROSSER, *Privacy*, 48 CAL. L. REV. 3 （1960）.

自西元 1960 年代始，美國公部門與私部門開始逐漸引入資訊設備，藉由資訊設備的快速性與便利性處理大量資料，當時的功能仍在檔案輔助，1970 年代初始，大量資訊自動化設備問世進入企業，企業中的 IT 系統開始提供管理上的效能，藉由查詢資料提供即時且精確的資訊，使管理者掌握組織運作狀況，做出適當的決策，公、私部門所掌握的資料與處理、利用方法越見增加，民眾對於此種現象產生警覺，要求保護隱私[24]。但若欲將此種資訊蒐集行爲歸入前述之四種隱私權侵害類型時，要件難以相符，確有所扞格。正因傳統隱私權理論無法因應資訊時代的需求，爲保護個人資料，在美國法中於隱私權的範疇下衍生資訊隱私權（Information Privacy），隱私權已不只是「獨處的權利」。透過隱私權保障的賦予，維護個人自主性（Personal Autonomy）以及個人的身分認同（Personal Identity），達到維護個人某本尊嚴（Personal Dignity）的目的[25]。隱私權已擴充爲一可「控制自身資訊的權利」[26]。資訊隱私權除了包含個人事務不受他人公開干擾的消極權利外，並應包括在沒有通知當事人並獲得其同意之前，不得逕行蒐集當事人之個人資料以及資料持有者不可將當事人爲某特定目的所提供的資料用在其他目的。

第二項　德國

除美國外，德國聯邦憲法法院也透過人口普查案判決自一般人格權進一步闡釋發展出資訊自決權理論，亦即所有的個人資料均受到保護。資訊自決權賦予個人自我保護個人資訊資料以阻止政府機構、公司企業等不當收集、處理、傳播、利用個人資訊的權利，承認每個人對涉及個人資料提供、利用的過程皆有積極參與和自我決定、以抗拒他人恣意干涉的積極自由權，亦即所謂資訊自決權，是指個人基本上有自行決定是否將其個人資料交付與提供他人使用之權利，可拘束國家機關，並基於第三人效力理論及於私法關係，真正體現了對個人尊嚴的充分尊重。個人資料之資訊隱私權，乃保障人民決

[24] 政府早已存有人民的資料，私部門也開始進行相同的行爲，相對應於 George Orwell 的不朽名著 1984 中的「老大哥」（Big Brothers），學者創造出「小大哥」（Little Brothers）這個名詞描述公、私部門均進行個人資料蒐集的行爲。參見 JEFFREY ROTHFEDER, PRIVACY FOR SALE: HOW COMPUTERIZATION HAS MADE EVERYONE'S LIFE AN OPEN SECRET（1992）.

[25] 劉靜怡，網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河，資訊管理研究，第四卷，頁 144-145，2002 年。

[26] U.S v. Westinghouse Electric Co., 638 F.2d 576 （1980）

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使用有知悉與控制權及資料記載錯誤之更正權。為保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損，德國於 1977 年 1 月 27 日即制定「資料處理個人資料濫用防制法」(Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung)，簡稱「聯邦資料保護法」(Bundesdatenschutzgesetz)，並行之有年。後因歐洲聯盟成立，為轉置歐盟指令、保障個人資料及資訊自由流通，而於 2001 年 5 月 18 日修正其內容。最近一次修正日期為 2003 年 1 月 14 日，修法目的旨在保障個人資料自主權，並落實歐盟有關建立共同資料保護標準之指令[27]。

第三項　英國

在英國方面，因應歐盟於 1995 年頒定之「個人資料保護指令(95/46/EC)」，英國於 1998 年施行新版之資料保護法 (Data Protection Act of 1998)[28]，並於 2000 年 3 月 1 日正式生效施行，取代 1984 年的資料保護法。由於 1984 年資料保護法之保護客體僅及於經電腦處理之個人資料，為配合歐盟指令，1998 年之資料保護法擴大將人工資料納入保護客體，但為避免衝擊過大，1998 年資料保護法遂分兩階段實施，分別於 2001 年 10 月 24 日、2007 年 10 月 24 日逐步納入部分人工資料，使其非因該法之施行而隨即落入該法的保護範疇，造成資料控管人(data controller) 之過度負擔。茲將本法中其他規定簡要介紹如下[29]：

本法雖擴大將人工資料 (或謂非經自動化設備處理之資料) 一併納入保護客體，但非謂所有之人工資料均受本法保護，依本法規定，受本法保護之人工資料，須該筆資料為相關建檔系統 (relevant filing system) 之一部，或意圖作為相關建檔之一部。所謂相關建檔系統即指該筆資料之組織方式

[27] 參考立法院網站各國法律發展，http://npl.ly.gov.tw/do/www/billIntroductionContent?id=19 1.資料保護法(德文版)：http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg03.htm 2.資料保護法(英文版)：http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg01_eng.htm

[28] 全文請參考<http://www.hmso.gov.uk/acts/acts1998/19980029.htm#aofs >

[29] 周慧蓮，英國個人資料保護最新案例發展及其對我國法制之啓示，資策會科技法律中心科技法律透析，民國 94 年 1 月。

係與該個人相關或涉及該個人之評等，且其組織方式將致關於特定個人之資料易於被接近使用[30]。根據英國個人資料保護署 (Information Commissioner) 發布之法律指導 (Legal Guidance)[31]之說明，決定人工資料是否屬於該法之保護客體，應考量下列兩項因素：其一，必須存在一組(a set of)或一群(a grouping)關於個人之資訊 (information)，這些資訊可以是藉著不同的識別符號加以表徵，不一定要同時出現於同一份文件中，亦無須放置於同一個檔案櫃或同一地點；甚者，該組資訊亦不一定非得要由資料控管人所屬組織集中控管。其二，該組資訊係易於取得的；換句話說，資料控管人所屬組織中之一個以上的人可因其職務而隨時近用該資訊。當然，本法律指導亦特別指出，某筆人工資料是否爲本法之保護客體，判斷不易，須就具體個案及當事人利益等各面向綜合審酌。

除了擴大保護人工資料，本法立有八個資料保護原則，分別爲：1. 個人資料須經公平且合法處理；2. 個人資料須於合法且特定目的下方可取得，且不得爲目的外使用；3. 個人資料僅得於必要範圍內蒐集、利用；4. 個人資料應維持其正確性與即時性 (up-to-date)；5. 個人資料之原蒐集目的消滅時，該筆資料即不得再留存；6. 個人資料之處理應與本法所賦予之當事人權利相配合；7. 應採取適當的科技或組織措施以維護資料安全；8. 不得將個人資料傳輸至個人資料保護法制未達適當標準之第三國。資料控管人必須對於其掌有之資料處理，踐行上述八項原則。

本法賦予資料當事人之權利，共計有六：資料近用權、損害防止請求權 (Prevention of processing causing damage or distress)、直銷拒絕權 (Right to prevent processing for purposes of direct marketing)、自動個別決定拒絕權、損害賠償請求權、訂正權。其中，最重要者當爲資料近用權，資料當事人可透過書面請求 (該書面請求亦可透過電子方式傳輸) 並於支付適當費用後，要求資料控管人提示其是否處理該當事人之資料，如果

[30] Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

[31] Data Protection Act 1998 Legal Guidance, available at < http://www.dataprotection.gov.uk >

是，資料控管人回覆資料當事人之際，應一併告知該筆個人資料爲何、處理目的以及揭露對象。至於損害防止請求權爲，倘當事人合理相信資料控管人所爲之資料處理將造成實質、毫無理由的損害或痛苦(substantial unwarranted damage or distress)，其可要求資料控管人於合理時間內停止資料處理。當資料控管人以直銷爲目的而爲資料處理時，當事人可於事前防止或事後拒絕。至於自動決定拒絕權，與歐盟之個人資料保護指令之規定相同。此外，本法依循歐盟之個人資料保護指令，設有專責機關，負責處理個人資料相關事件，包括促進資料控管人對於本法的踐行、適時公布本法實施報告，促成業者自律規範、國際合作、受理特定業者依本法須爲之登記事項、定期向國會報告、追訴違反本法規範者等等。

第四項　日本

日本約到 20 世紀 50 年代後，隱私權方受到日本學者的重視；而 1964 年東京地方法院作成的「宴之後」(宴のあと）判決[32]，更使得隱私權成爲日本各界廣泛談論的話題[33]。70 年代部分隱私權保護團體爲了反對日本政府規劃的「國民總編號制度」，曾提出了「個人資料保護自治條例模範綱要」，學者也在此時開始倡議進行隱私保護立法。1980 年經濟合作開發組織發布了「隱私保護與個人資料跨境流通指導原則」(Guidelines On the Protection of Privacy and Transborder Flows of Personal Data)，提出個人資料保護的八大原則[34]，而「歐洲理事會」(Council of Europe）[35]亦於次年發布「個人資料自動化處理保護協定」(Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data)；其中，日本因身爲 OECD 指導原則簽署國之一，爲因應法制化的需求，該國政府遂於當時的「行政管理廳」(政管理庁）轄下，成立了「隱私保護研究會」(プライバシー保護研究会)，並於 1982 年提出了知名的「個人資料處理之隱私保護對策

[32] 判時 285 号 12 頁、判夕 165 号 184 頁。

[33] 参堀部 政男，個人情報保護に関する国際動向と日本の対応，法とコンピュータ，第 26 期，頁 5，2008 年 7 月。

[34] OECD 揭櫫的八大原則請參後節說明，分別爲：1、蒐集限制原則；2、資料內容正確性原則；3、目的明確化原則；4、利用限制之原則；5、安全保護原則；6、公開之原則；7、個人參與原則；及 8、責任原則。詳參次節說明。

[35] 當時仍屬「歐州共同體」(European Communities）時代。

」(個人データの処理に伴うプライバシー保護対策)報告[36]。

經過漫長的討論，日本國會於 1988 年 12 月制定了「行政機關電腦處理個人資料保護法」(行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律)，然而，該法僅規範公部門，而未及於一般的私人企業與個人。1995 年歐盟(European Union, EU)發布「個人資料保護指令」[37]，要求各成員國應於 1998 年 10 月 24 日前將法案內容轉化爲內國法外，並嚴格禁止成員國將個人資料輸往資料保護水平較低的國家。有感於既有法令的不足，日本政府於「高度資通訊社會推進本部」(即後來的 IT 戰略本部)下先後成立了「個人資料保護檢討部會」及「個人資料保護法制化專門委員會」，並於 2001 年 3 月完成了「個人資料保護法」草案[38]。在歷經多次檢討與修正後，日本國會於 2003 年 5 月通過「個人資料保護法」[39]，並於 2005 年 4 月 1 日全面實施，成爲現階段日本在私部門個人資料保護最爲重要的法律規範[40]。

日本個人資料保護法的主要內容：它適用於處理 5000 人以上資料的所有機構或個人，這些機構或個人在處理資料時，必須遵守下面規範：(1) 告知個人它收集資料的目的；(2) 不得以不當手段取得資料；(3) 保證資料有安全防護，不會被遺失、被非法取用；(4) 未經個人同意不得提供給第三者；(5) 不得拒絕個人要求修正、補充、刪除其資料的要求；(6) 不得拒絕個人要求停止使用其資料的要求；(7) 所有機構必須成立申訴單位，處理對資料

[36] 參堀部 政男，前揭文，註 3，頁 6。

[37] 歐盟「個人資料保護指令」，全名爲”European Union's Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data”.

[38] 參淵邊 善彥、五十嵐 敦編，個人情報管理ハンドブック，商事法務出版，第 2 版第 1 刷，頁 5，2008 年 4 月。日本行政機關之電腦處理個人資料保護法歷經多年實施之後，日本總理於 1999 年 6 月 28 日參議院會議中就住民基本台帳法修正法案答辯時指出，日本政府將對現行個人資料保護方式進行全面檢討，並儘速將民間機構納入個人資料保護法規範範疇；同年 7 月 23 日日本高度情報社會推進本部首度召集「個人資料保護檢討部會」，就現行個人資料保護相關法令系統進行全面檢討，並提出確立個人資料保護機制中之核心基本原則與制定一基本法等相關意見。至 2000 年 10 月，個人資料保護法制專門委員會提出「個人資料保護基本法大綱」，並於 2001 年 3 月經內閣會議通過，正式提報國會進行審議。

[39] 除「個人情報保護法」外，當時亦同步通過「行政機關個人情報保護法」、「獨立行政法人個人情報保護法」、「資訊公開及個人情報保護審查會設置法」及「行政機關個人情報保護法施行整備法」等關連法案。

[40] 參淵邊 善彥、五十嵐 敦編，前揭書，註 8，頁 6。

處理不當的申訴案件。

於日本個人資料保護法案中，不論是行政機關或是民間機構，只要有利用個人資料者，都受到此法之規範；因此，日本政府制定一般性規範，意即所謂的「基本原則」，作爲各機構之標準。此外，特別是對於使用電腦或資料庫等儲存利用個人資料之相關單位(個人資料利用事業者)，亦設定「個人資料利用事業者之義務」規定，訂定具體且明確之規範。以公務機關之個人資料處理而言，在昭和六十三年已制定「行政機關電腦處理個人資料保護法」，然而爲配合「個人資料保護法案」之制定，因此已於國會中提出相關之個人資料保護法案，除了對原先「行政機關之電腦處理個人資料保護法」之修正案外，另提出「獨立行政法人資料保護法案」、「資料公開與資料保護審查會設立法案」、「行政機關之個人資料保護法施行相關法律準備之法案」[41]等，以加強個人資料保護法之完整性。

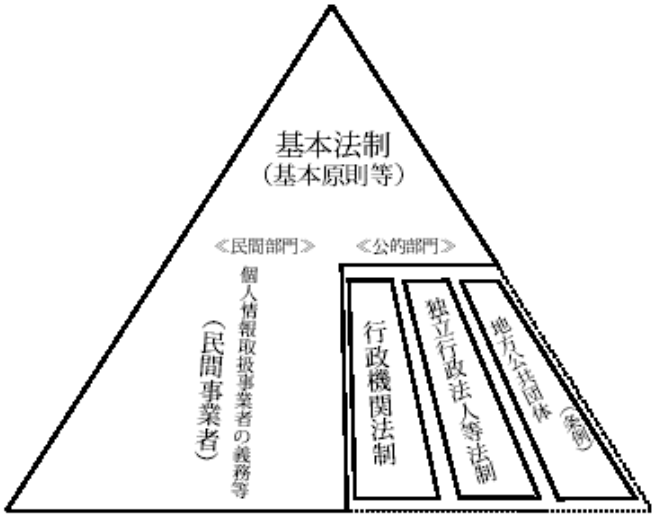


圖 1、個人資料保護之法制體系

註、資料來源

日本總務省行政管理局

[41] 行政機関等個人情報保護４法案の概要，日本總務省行政管理局，http://www.soumu.go.jp/gyoukan/kanri/kenkyu_f.htm。

在尊重個人人格之理念下，慎重處理暨利用個人資料，係爲制訂日本個人資料保護法案之基本考量；因此（1）資料利用目的之限制、（2）資料之適當取得、（3）確保資料正確性、（4）確保資料安全性、（5）確保資料之透明度，即爲本法案之五項基本原則。爲保護所有個人、團體、法人以及機關個人資料，依據上述五項基本原則，本法案朝向制定適當處理及利用個人資料之方向而努力，且實務上何種資料之處理與利用始可視爲恰當，以及對於公益活動或正當事業活動之必要性亦加以評估後，於個人資料保護之必要範圍內予以判斷，爲制訂本法案之相關考量因素。

以金融機構業務而言[42]，顧客資料保護方面有著分期付款販售法（割賦販売法）或是貸款業法（貸金業法）等法律上的規定，金融檢查手冊或是金融事務指導原則等監督行政上之規定，以及業界自行訂定規範等各種不同之法令規定。一般而言，由於金融機構對於顧客資料有保密義務，故非正當理由將顧客資料提供給第三者之情形，是不被認可的，因此金融業朝向訂定共通的基本原則思考；此外，即使是顧客資料中有關個人資料的部分，亦有業界自訂的規範，或是如財團法人金融資訊中心(財団法人金融情報システムセンター，The Center for Financial Industry Information Systems，簡稱FISC)、壽險業與損害保險業或是信用資料機構等機構所訂定更爲詳細的個人資料保護指導方針。

[42] 顧客情報の取扱いに関する諸問題—個人情報保護法案を踏まえて—，金融法務事情 No. 1642，2002.5.5。

第三章　個人資料保護與資訊安全之立法與分析

第一節 現行之電腦處理個人資料保護法

近來，台灣的民眾普遍碰到的問題，包括詐騙集團的電話，電子信箱裡的垃圾郵件，都是個人資料處理運用氾濫的結果。公家或私人機溝的個人資料大量流出或是販賣個人資料營利行業的興起，都造成社會大眾對個人資料處理感到不安。爲使社會大眾得以安心享受科技技術帶來的便利，所有先進國家的政府都早已注意及此，紛紛訂定「個人資料保護法」(Personal Information Protection Act)。像 APEC 這類國際組織更把訂定個人資料保護的國際性規範，以及促進國際間合作列爲重要討論議題已如前章簡介。我國早在民國 84 年即訂定「電腦處理個人資料保護法」，並在 85 年公佈「電腦處理個人資料保護法施行細則」，明訂「徵信業、電信業、醫院、學校、金融業、證券業、保險業、大眾傳播業」等八大行業必須遵守。雖然我國的法條比其它國家要更嚴厲（例如：第 27 條規定「 賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。」罰金遠高於其它國家。)，但很快就被發現不敷社會的需求[43]。

現行之電腦處理個人資料保護法，顧名思義，其保護客體僅及於使用電腦或自動化機器[44]爲資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理之個人資料，非經電腦或自動化設備處理之資料，或謂人工資料，非屬本法保護範疇。而根據本法定義，所謂個人資料係指自然人之姓名、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。再次佐證，單純人工處理之資料、法人或非法人團體之資料均不納入電腦處理個人資

[43] 爲人詬病者包括： (1)只適用於八大行業(因此，影帶出租業的客戶資料不受保護)，(2)只有用電腦處裡的資料受規範(因此，收集、販賣通訊錄的資料，只要不用電腦處理就不算犯罪)，(3) 只有在圖利情況下洩漏資料才有罪(因此，老師提供學生名單給開補習班的朋友，只要沒收錢就無罪)。

[44] 根據電腦處理個人資料保護法施行細則第 5 條規定：「本法第 3 條第 3 款所稱自動化機器，指具有類似電腦功能，而能接受指令、程式或其他指示自動進行事件處理之機器。」

料保護法保護範疇。過去法務部對於保護客體僅侷限於經電腦處理之個人資料所爲的解釋理由主要有三：1．立法之初，社會各界對於個人資料保護之意識薄弱，且未來執法效能亦仍屬混沌、2．非經電腦處理之資料仍受民法、刑法等相關法制之保護、3．參酌外國立法例，日本與英國亦採之。

個資法之規範主體可分爲公務機關與非公務機關兩種。公務機關係指依法行使公權力之中央或地方機關。非公務機關原則上僅及於徵信業及以蒐集或電腦處理個人資料爲主要業務之團體或個人、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業等，學界間稱此爲「八大行業」。至於非屬個資法八大行業的其他企業，只能依據個資法第3條第7款第三目，由法務部會同中央目的事業主管機關，以指定的方式納入個資法規範。根據法務部歷年來頒布的行政函釋，目前經指定納入個資法第 3 條第 7 款第三目的團體計有：期貨業、台北市產物、人壽保險商業同業公會、中華民國產物保險商業同業公會、中華民國人壽保險商業同業公會、財團法人台灣更生保護會、財團法人犯罪被害人保護協會、不動產仲介經紀業、利用電腦網路開放個人資料登錄之就業服務業、登記資本額爲新臺幣一千萬元(含) 以上之股份有限公司之組織型態，且有採會員制爲行銷方式之百貨公司業及零售式量販業、除語文類科外之文理類補習班[45]。

關於個人資料之蒐集、處理與利用等原則，公務機關方面，因設有「對當事人權利無侵害之虞者」此一要件[46]，造成公務機關對於個人資料之蒐集、處理及利用要件相當寬鬆。就非公務機關方面，根據個資法第 18、19 條，非公務機關經目的事業主管機關依本法登記並發給執照後，對個人資料之蒐集或電腦處理，須有特定目的並符合下列情形之一時，方得爲之：1．經當事人書面同意者、2．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、3．已公開之資料且無害於當事人之重大利益者、4．爲學術研究而有必要且無害於當事人之重大利益者、5．依本法第 3 條第 7 款第二目有關

[45] 參法務部全球資訊網 http://www.moj.gov.tw/ct.asp?xItem=108068&ctNode=26436&mp=001

[46] 電腦處理個人資料保護法第 7 條第 1 項第 3 款參照。

之法規及其他法律有特別規定者。另根據第 20 條，非公務機關向目的事業主管機關登記時，應具申請書並載明：1．申請人之姓名、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。2．個人資料檔案名稱。3．個人資料檔案保有之特定目的。4．個人資料之類別。5．個人資料之範圍。6．個人資料檔案之保有期限。7．個人資料之蒐集方法。8．個人資料檔案之利用範圍。9．國際傳遞個人資料之直接收受者。10．個人資料檔案維護負責人之姓名。11．個人資料檔案安全維護計畫。關於電腦處理個人資料保護法的特定目的，爲個資法規範非公務機關處理個人資料之核心要件，禁止單純儲存或毫無目的地蒐集利用個人資料，亦禁止變更原蒐集利用目的而爲其他目的之資料處理，此舉不但可減少機關不必要的蒐集費用，更可確實保護當事人的資訊隱私權。法務部已於民國 85 年 8 月 7 日公布「電腦處理個人資料保護法之特定目的」，計有 101 項，諸如行銷、客戶管理、統計調查與分析、經營電信業務與電信加值網路服務等。另根據電腦處理個人資料保護法施行細則第 30 條，個資法第 20 條所指之書面同意應爲事前書面同意[47]。至於本法所謂之類似契約關係之情形有二：一爲非公務機關與當事人間於契約成立前，爲訂定契約或進行交易爲目的，所爲接觸，磋商所形成之信賴關係。另一爲契約因無效、撤銷、解除、終止或履行而消滅時，非公務機關與當事人爲行使權利，履行義務或確保個人資料完整性之目的所形成之連繫關係[48]。

當事人權利方面，根據個資法第 4 條，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：1．查詢及請求閱覽、2．請求製給複製本、3．請求補充或更正、4．請求停止電腦處理及利用、5．請求刪除。因此，非公務機關應維護個人資料之正確，並應依當事人之請求適時更正或補充之。個人資料正確性有爭議者，公務機關應依職權或當事人之請求停止電腦處理及利用。個人資料電腦處理之特定目的消失或期限屆滿時，非公務機關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。

[47] 電腦處理個人資料保護法施行細則第 30 條：「非公務機關基於特定目的，爲取得當事人書面同意，於初次洽詢時，檢附爲特定目的蒐集、電腦處理或利用之相關資料，連同得於所定相當期間表示反對意思之書面，經本人或其法定代理人收受，而未於所定期間內爲反對之意思表示者，推定其已有同意之表示。」

[48] 參考電腦處理個人資料保護法施行細則第 32 條第 2 項。

當事人得於上述請求拒絕後或期限屆滿後二十日內，以書面向其監督機關請求爲適當之處理。

個資法對於資料傳輸至第三國亦有類似歐盟指令之規範，第 24 條規定非公務機關爲國際傳遞及利用個人資料，而有下列情形之一者，目的事業主管機關得限制之：涉及國家重大利益者、國際條約或協定有特別規定者、接受國對於個人資料之保護未有完善之法令，致有損當事人權益之虞者、以迂迴方法向第三國傳遞或利用個人資料規避本法者。但實務上並未見具體案例。

另依據現行電腦處理個人資料保護法第 3 條第 1 款之定義，本法所稱之個人資料係指「指自然人之姓名、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。」準此，人工資料當然不在本法保護客體中，本文前已敘及。事實上，經非自動化設備處理、單純人工處理之個人資料亦可能因處理人之故意過失致生當事人之損害，舉例而言，時下銀行爲推廣各類金融卡，均廣招業務員於街頭招攬行人辦卡，倘若當事人於街頭填寫的資料未送回銀行以自動化設備處理前，即遭不肖業務員自行蒐集利用；又或者徵信社負責人爲竊錄民眾電話而於民眾住宅外電話分線盤鐵盒內裝設錄音設備[49]，電腦處理個人資料保護法於此例中對當事人的保障均顯不周。

此外，何謂「足資識別該個人之資料」，本法未有具體說明。電話號碼、基因資訊、個人使用電信設備所生之傳輸訊息，如電子郵件帳號、歷史紀錄檔 (log files) 與位址資訊 (location data) 等可否解釋爲「足資識別該個人之資料」而納入電腦處理個人資料保護法的保護範疇，容有討論空間。實務上，曾認定電子郵件帳號非屬本法所稱之個人資料，因而作出不起訴處分[50]。倘依此推論，個人使用電信設備所生之傳輸訊息，如電子郵件帳號、歷史紀錄檔與位址資訊似乎都不屬於現行法所定義之個人資料。

[49] 根據台灣高等法院 86 年法律座談會結論，所謂自動化設備應指類似電腦之機器，而電腦之構造以積體電路爲主，與一般電話並不相同。

[50] 台灣新竹地方法院不起訴書，科技法律透析，民國 88 年 7 月。

第二節「個人資料保護法」草案

電腦處理個人資料保護法（以下簡稱「個資法」），其立法目的就是在保護民眾的個人資料隱私。根據個資法，不論公務或非公務機關，對於個人資料的蒐集、利用都必須尊重當事人的權益，並不得逾越取得該資料之特定目的必要範圍；資料處理時，除應與蒐集之特定目的相符外，當事人有請求維護資料的正確性、停止利用或刪除該資料的權利；而保有個人資料檔案者，有指定專人依相關法令辦理安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏的義務，違反者，當事人得提出損害賠償訴訟等。而現行個資法在適用上最大的爭議，在其適用範圍僅限於徵信業、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業等所謂的「八大行業」，而不及於一般事業及個人；且保護之客體，只限於經電腦處理之個人資料。新法將改名爲「個人資料保護法」（以下簡稱「新法」），刪除現行個資法中對非公務機行業別之限制，將適用之主體擴大至自然人、法人、公務與非公務機關等；並擴大保護客體至紙本處理的個人資料；增加犯罪前科、健康檢查、醫療、性生活及基因等 5 類「敏感性資料」，嚴格規範其蒐集處理與利用等等。其中企業需特別注意者，爲新法賦予企業更重的個人資料安全維護責任，並賦予目的事業主管機關更大的介入查核權限。

個資法修正草案主要是針對前述個資法的缺漏進行修正：

一、 刪除非公務機關行業別之限制並擴大適用範圍：

任何自然人、法人、機構或其他團體，除單純爲個人或家庭活動等私生活目的之情形外，皆適用個資法。除落實民法有關避免人格權受侵害之相關規定，並促進個人資料合法利用等立法原旨。

二、 增訂資料蒐集使用者之告知義務：

爲保護個人資料當事人的資訊自主權，及得知資料係被何人蒐集及所蒐集範圍、用途等，公務機關及非公務機關在蒐集資料時，不論是直接或間接蒐集，除符合得免告知情形外，均須明確告知當事人蒐集機關、蒐集目的、資料類別、資料來源等相關事項。

三、 增訂敏感性資料蒐集之限制：

有關犯罪前科、醫療、基因、性生活及健康檢查等五類個人資料，因性質特殊或事涉敏感，比一般個人資料有受更嚴格保護之必要。因而此五類個人資料除基於特定目的並符合法規明文規定，或經當事人書面同意，或當事人自行公開等要件外，原則上不得任意蒐集，或以電腦處理及利用。

四、 增訂團體訴訟：

如公益性法人的章程中，訂有保護個人資料爲其宗旨之一者，該公益性法人得接受當事人委任，代爲行使依個資法得主張之權利及提起訴訟。此條文的增訂，是期待藉由民間專責團體之參與，減少民眾行使權利之負擔，進而樂於行使權利。另外，爲鼓勵民眾多利用公益性法人代爲行使權利，以提高行政效率與節省資源，公益性法人得就同一原因事實，接受 20 人以上之委任，代爲向公務機關行使權利或提起民事訴訟，得免除相關費用或得減免裁判費用。

五、 提高損害賠償金額：

爲使公務機關與非公務機關對個人資料之蒐集及利用能謹慎爲之，並使被害人能得到較高額度的賠償，明定違反個資法規定，侵害當事人權利時，被害人雖不能證明非財產上的損害，亦得請求新台幣 2 萬元至 10 萬元的損害賠償，並對同一侵害原因事實，將賠償金額上限提高爲新台幣 5 千萬元。

另從資安角度觀之，個資法修正草案中，亦包括以下修正重點：

一、 新增機關對當事人主動通知之安全責任

有鑑於國內屢次爆發大規模的個人資料外洩案，資料主體當事人卻因爲欠缺得知資料被外洩途徑可能性，而導致權益受損卻無法主張權利的狀況，新法特別賦予公務或非公務機關，當其所蒐集之個人資料有被竊取、洩漏、竄改或遭其他方式之侵害時，有以適當方式（如電話、信函、公告請當事人上網或電話查詢等）迅速通知當事人之責任；違反規定而隱匿不爲通知者，主管機關得限期改正，並得按次處以新台幣 2 萬元以上 20 萬元以下之行政罰鍰。

二、 增列向第三國（地區）傳輸個人資料限制

雖然現行個資法即有對國際傳輸之限制，但由於對「國際」傳輸之認定有爭議，實務上，企業爲降低作業成本而將資訊作業迂迴傳輸至中國大陸或離島地區處理，忽視對客戶個人資料保護責任的情形頗爲嚴重。爲避免認定之爭議影響對個人資料之保護，新法特別將「地區」之文字納入，以收明確之效。未來企業進行資訊作業委外時必須注意，違者並得課予罰鍰。

三、 機關應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

現行個資法對機關資訊安全作業之規定，僅見於第 17 條與第 26 條，要求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、滅失或洩漏等。但各機關如何辦理、落實資訊安全維護工作？機關資訊安全維護事項指涉的內涵究竟爲何？由於現行個資並未明確規範，需另行參照各目的事業主管機關頒訂之相關法令，在各目的事業主管機關認知不同情況下，實務上各企業對資訊安全維護工作的認知並不相同。

也由於各企業對安全管理之需求與風險承擔能力不盡相同，新法將要求受指定之機關（如銀行、電信、保險等），應根據中央目的事業主管機關所定之標準，訂定各機關之個人資料檔案安全維護計畫、與業務終止後之個人資料處理方法。此外，雖然法條並未明訂，但中央目的事業主管機關未來在依職權進行行政檢查時，企業是否符合這些安全維護計畫與資料處理方法所訂步驟，應可望成爲判斷責任歸屬之重要依據。本條規定，預期可有效提升企業資訊安全風險意識，並擴大企業對資安咨詢服務業之需求。

四、 強化行政檢查權

現行個資法在適用上的另一個缺陷，在於主管機關不明。雖然許多國家針對個人資料保護之議題，已設有特別之專責機構（如英國設有個人資料保護署 Information commissioner），但考量各行業已有目的事業主管機關，且個人資料之蒐集、處理與利用應屬各該事業之附屬業務

，新法因此不另設專責主管機關，而是明確賦予中央目的事業主管機關與直轄市、縣(市)政府有強制檢查與處分權。當其發現非公務機關違反規定，或有必要時，得派員進入該非公務機關進行檢查，或要求說明、提供資料；認有違法情事時，對檢查時所發現得沒入或可爲證據之資料或檔案，得強制扣留或複製，被檢查者不得規避、妨礙或拒絕。本條規定之立意雖佳，但由於新法賦予中央目的事業主管機關、直轄市、縣(市)政府與司法搜索扣押行爲類同之權限，引發立委們的顧慮。

五、 新增機關代表人同受行政處罰規定

本條新增，但對企業之影響預計將頗爲深遠。因爲只要非公務機關（企業法人）依新法受有行政罰鍰之處罰時，企業之代表人、管理人、或其他代表權人對各該違反本法規定之行爲（包括個人資料應採使適當安全措施之義務），視爲有疏失；除能證明以盡防止義務者外，應並受同一額度罰鍰之處罰。

第四章　公務機關就醫資訊及就學資訊管控與監督

第一節 公務機關對於就醫資訊之蒐集、處理、利用及保全

第一項 問題之發現及提出

一、疾病管制局肺結核資料外洩案[51]

疾病管制局接獲某報記者通知，可在網路上查詢到該局結核病患名單。疾管局獲知後立即依據行政院資訊安全相關規定，成立緊急因應小組，迅速查明原因，進行危機處理，管制損害。經查，本次事件共有 953 名結核病患姓名、居住縣市等個人資料外漏，判斷外漏時間約一週。出境管制名單可從 Google 搜尋引擎，透過已知結核管制病患姓名搜尋，所幸必須已知結核病患姓名，否則無法搜尋到資料，判斷資料尚未廣泛流傳。經初步了解，係因系統設計出現瑕疵，致具系統權限者於使用查詢功能時，遭 Google 擷取造成。是否有駭客或植入木馬程式所造成，仍待查明。該局晚間八時四十五分已緊急將該份名單自網路移除，並立即聯繫 Google 移除庫存頁面，關閉伺服器進行檢修，尋找外漏的原因。該局表示：

1、對於部分名單的外漏，向當事人慎重道歉，若有當事人因此權益受 損，該局將負起責任。

2、本案屬資安事件，該局已依資安全管理程序，陳報國家資通安全會報通報應變組，目前暫停系統服務，並立即修改程式弱點，將經過完整嚴密測試後才會再度上線。

3、呼籲從此次管道獲得個人資料的任何民眾，都應遵守傳染病防治法及個人隱私保護法之相關規定，不得洩露。

二、本案涉及之法律問題

[51] 自由電子報，開放肺結核個資，網搜曝光，2007.11.07 http://www.libertytimes.com.tw/2007/new/nov/17/today-life1.htm

就本案例看來，結核病人資料外洩似涉及疾病管制局內部資訊安全之管理、資料洩漏之當事人權益保障及尋求救濟等，該等問題屬於公務機關對於個人就醫資訊之蒐集、處理、利用、保全以及個人資訊之人格權保障等。本文以電腦處理個人資料保護法及個人資料保護法草案之內容，就適用主體、保護客體、個人資料保護請求權之保障、公務機關於就醫各階段取得資訊之態樣、我國對於醫療資訊隱私權之保護規範與現況等，進行分析說明，併行檢討草案對現行問題規範不足之處。

第二項　公務機關對於就醫資訊之蒐集、處理、利用及保全

一、適用主體：公務機關

依照個資法草案（以下簡稱「草案」）第 2 條第 7 款，「公務機關」係指「依法行使公權力之中央或地方機關或行政法人」，草案第 4 條規定，非公務機關委託蒐集、處理或利用個人資料者，於個資法適用範圍內，視同委託機關。由上述適用主體之定義觀之，包含必定涉及就醫資訊之醫療單位，亦含括全民健保之主管機關，其為辦理保險給付，必須依法蒐集所需醫療資訊；並含括各級公立學校，為辦理學生疫苗注射活動，可能須留存部分學生之醫療資訊等是[52]。

二、保護客體：

草案第 2 條第 1 款以例示加概括之方式，將「病歷」、「醫療」、「基因」、「性生活」、「健康檢查」，以及其他得以直接或間接識別該個人之醫療資料列為受個資法保護之就醫資訊；其中，草案第 6 條將「醫療」、「基因」、「性生活」，以及「健康檢查」列為特別需要受保護的特種資料。

非屬特種資料的就醫資訊，原則上得為蒐集、處理、利用，但須依誠實信用方法為之，且不得逾越特定目的之必要範圍，並應和蒐集之目的具有正當合理之關連，以免資料蒐集者巧立名目或理由，任意蒐集、處理或利用所

[52] 莊郁沁，論醫療隱私權之保障，國立台灣大學國家發展研究所碩士論文，2002 年，頁 42。

蒐集的資料[53]。

屬於特種資料的就醫資訊，依草案第 6 條規定，原則上不得蒐集、處理或利用；其原因在於，該等資料中有部分資料性質較爲特殊或具敏感性，如果任意蒐集、處理或利用，可能會造成社會不安，或對當事人造成難以彌補之傷害[54]。草案第 6 條保障之 5 種特種資料中，除了「犯罪紀錄」以外，其他皆可能被納入就醫資訊之範疇，應可推知就醫資訊本身即帶有特殊性、敏感性。

惟上述屬於特種資料之就醫資訊，其內涵爲何較其他資訊爲特殊、敏感？以下分就受到草案特別保護之特種資訊內涵爲簡單介紹，以釐清就醫資訊異於他種資訊而需特別受到保障之處[55]。

(一)、醫療資訊

1. 定義：

學術論文於討論醫療資訊時，多認爲包括，在醫療實踐的過程中，被動地「接收（receive）」由病人所提供的、與病人有關的資訊，以及主動地由醫療專業依據其醫學知識「生產（create）」與病人有關的資訊[56]。爲使病患能順利進入醫療過程，病患必須提供與個人健康狀態無直接關係之人口統計學資訊（如姓名、生日等）、個人辨識碼（如身份證字號）、財務資訊、得以幫助醫療專業判斷之求診原因（如受傷之原因是槍傷或是車禍…等）、症狀，以及家族病史。醫療專業因爲前述病患所提供之資訊，依據醫療專業所做出之護理紀錄、檢驗記錄、復健紀錄、身體檢查紀錄…等，亦屬醫療資訊之範疇[57]。

[53] 個人資料保護法草案第 5 條立法說明。

[54] 個人資料保護法草案第 6 條立法說明。

[55] 如下文所示，由於本文對於「醫療」資訊採取廣義定義，並認爲同屬特種資訊之「健康檢查」亦可被含括於「醫療」中，故對於「健康檢查」即不另行介紹。

[56] 吳昊，由醫療資訊隱私權之觀點論全民健保 IC 卡政策，國立台灣大學法律學研究所碩士論文，2001 年，頁 129；莊郁沁，論醫療隱私權之保障，國立台灣大學國家發展研究所碩士論文，2002 年，頁 23。

[57] 邱文聰，由醫療資訊談國家醫療權力的管制，國立台灣大學法律學系研究所碩士論文，1

2．特別保護醫療資訊隱私之理由：

醫療資訊本屬個人資訊之一部分，受到隱私權之保護乃屬當然，何以需要特別保護？此係因保障醫療資訊係出於保障個人人格自我形塑之權利，可以連結到人性尊嚴以及屬憲法基本權利層次之人格權保障使然[58]。由於個資法以保障「人格權」爲核心，包括消極面的資訊隱私不受侵犯，及積極面的個人資訊自決權，最終目的在於「尊重人格自我形塑之權利」。醫療資訊爲醫療專業對於個人健康狀況的專業性評斷，如果被評價爲不健康、或者曾經被評價爲不健康，醫療資訊尚會揭示導致不健康結果之可能原因，包括生活習慣、家庭背景、過去經歷等，而此等被醫療專業評價爲不健康之弱點，以及個人不欲人知的特殊生活習慣、家庭背景、過去經歷等，如能使他人輕易推知或遭到不當公開，極可能貶損外界對該人之評價，影響個人建構形象的可靠性，從而侵犯個人人格自我形塑之權利[59]。

3．本草案所指「醫療」資訊範圍是否與醫療法所稱「病歷」相等？

由上述醫療資訊之內涵觀之，醫療資訊包含範圍甚廣，而其內涵主要係由醫療法規定、由醫事人員[60]所製作的病歷[61]所構成；故如依本草案第 2 條第 1 款將醫療與病歷、基因、性生活，及健康檢查

998 年，頁 16。該文並依據資訊是否經過醫療專業處理，將資訊分爲「單純由病患提供之資訊（received）」，以及「經醫療專業處理後所生產之資訊（created）」；前者包括姓名、生日、身份證字號、財務狀況…等，後者則包括個人病史、家族病史、病患主訴…等；楊宗杰，醫療資訊隱私權侵害之研究－以健保 IC 卡政策爲例，南華大學公共行政政策研究所碩士論文，2006 年，頁 19。

[58] 李震山，電腦處理個人資料法之回顧與前瞻，中正法學集刊第 14 期，頁 6。

[59] 吳昊，由醫療資訊隱私權之觀點論全民健保 IC 卡政策，國立台灣大學法律學研究所碩士論文，2001 年，頁 140。

[60] 醫療法第 10 條，所稱醫事人員，係指領有中央主管機關核發之醫師、藥師、護理師、物理治療師、職能治療師、醫事檢驗師、醫事放射師、營養師、藥劑生、護士、助產士、物理治療生、職能治療生、醫事檢驗生、醫事放射士及其他醫事專門職業證書之人員。所稱醫師，則係指醫師法所稱之醫師、中醫師及牙醫師。

[61] 醫療法第 67 條第 2 項所稱病歷，係指醫師依醫師法執行業務所製作之病歷、各項檢查檢驗報告資料，以及其他各類醫事人員執行業務所製作之紀錄；醫療法第 69 條規定，醫療機構以電子文件方式製作及貯存之病歷，得免另以書面方式製作，已將電子病歷納入規範範圍，故已無電子醫療資訊形式之疑問。關於醫療資訊形式之疑問，請見吳昊，由醫療資訊隱私權之觀點論全民健保 IC 卡政策，國立台灣大學法律學研究所碩士論文，2001 年，頁 145；莊郁沁，論醫療隱私權之保障，國立台灣大學國家發展研究所碩士論文，2002 年，頁 44。

分別列示，則本草案所指醫療資訊，其語義應不包括病歷、基因、性生活，及健康檢查，遠較學說討論所稱之醫療資訊範圍爲小；惟如將病歷排除於醫療資訊之射程外，則在此所指、應受特殊保障之醫療資訊幾無其他殘餘內涵。

故本草案應明確界定其所指的「醫療」資訊範圍如何，以確定那個範圍以內的醫療資訊必須受到特殊保護，原則上不得任意蒐集、處理、利用；如將「醫療」資訊之範疇採取廣義的認定，其中除了病歷以外之其他醫療資訊仍有特別保護之必要，則如本草案將「醫療」資訊全部納入特種資訊，即無必要再將「病歷」與「醫療」併列，以免誤認「醫療」資訊之內涵不包括「病歷」。如將「醫療」資訊採取狹義認定，而僅侷限於醫療法所稱之「病歷」，兩者意涵既然相同，即無須再將「醫療」與「病歷」併列，保留其一即可；而屬於「病歷以外、屬廣義醫療資訊範圍內」的其他資訊，如有特殊保護必要，仍應納入特種資訊之範疇中加以保護[62]。

---

[62] 以美國於 2002 年公佈之「個人可辨識之健康資訊隱私標準（Standard for Privacy of individually Identifiable Health Information）」，以及其後公佈配套之「健康保險改革：安全標準（Health Insurance Reform: Security Standards）」與「健康保險改革：電子化資料傳輸標準及編碼（Health Insurance Reform: Electronic Data Transaction）」爲例，此三標準將就醫資訊區分爲以下三種：健康資訊（health information）、可辨識個人之健康資訊（individually identifiable information），以及受保護健康資訊（protected health information）。

其中，健康資訊爲最廣義之就醫資訊，包括任何口頭、書面、及電子化形式之資訊，由健康照護提供者、健康計畫、公衛主管機關、雇主、保險公司、學校、大學或資訊處理者所製造或接收，且內容有關個人過去、現在或未來之身體、心理或任何狀況之資訊，以及關於提供個人健康照護之資訊，與過去、現在或未來提供個人健康照護之付款資訊。

可辨識個人之健康資訊爲上述健康資訊之下位概念，限由健康照護提供者、健康計畫、雇主或資訊處理者製造或接收，並可藉之辨識記載主體或有合理基礎相信該資訊可以用於辨識該記載主體之身分者。

受保護健康資訊則爲可辨識個人之健康資訊的下位概念，爲可辨識個人之健康資訊中，非屬家庭教育及權利隱私法規範紀錄之其他資訊。

我國所稱最廣義的醫療資訊，應可和上述健康資訊相對照；所稱病歷，即爲由健康照護提供者者製造或接收之資訊。病歷以外之其他醫療資訊，即包含由健康計畫、公衛主管機關、雇主、保險公司、學校、大學或資訊處理者所製造或接收，且內容有關個人過去、現在或未來之身體、心理或任何狀況之資訊，以及關於提供個人健康照護之資訊，與過去、現在或未來提供個人健康照護之付款資訊。

莊郁沁，論醫療隱私權之保障，國立台灣大學國家發展研究所碩士論文，2002 年，頁 39-41。

如對醫療資訊採取廣義定義，則除病歷以外，上述由健康計畫、公衛主管機關、雇主、保險公司、學校、大學或資訊處理者所製造或接收，且內容有關個人過去、現在或未來之身體、

比對本次草案增修之部分，「醫療」、「基因」、「性生活」、「健康檢查」等就醫資訊係屬新增，如將「醫療」採取廣義定義，則本草案可以考慮將「病歷」及「健康檢查」兩個項目刪除，因爲僅規範「醫療」並採取廣義定義，即足以將「病歷」及「健康檢查」含括在內。

至於「基因」及「性生活」兩個項目，雖然「醫療」可能包含基因及性生活資料，但是基因及性生活資料並不必然全被包含於「醫療」資訊中[63]，毋寧認爲醫療，與基因及性生活之範圍有交集關係，基於基因及性生活資訊另有其特殊內涵存在，僅將醫療納入特種資訊保障，並不足以充分保障基因及性生活資訊，是以特種資訊中，與就醫資訊相關之部分，應將「醫療」、「基因」及「性生活」三者皆納入[64]。

（二）基因資訊

1. 定義

基因主係由核苷酸（nucleotide）組成的去氧核糖核酸（deoxyribonucleic acid, DNA）所構成，不同結構的核苷酸分別組成不同生物訊息的 DNA，而不同排列的 DNA 訊息決定不同的蛋白質結構與功能[65]，進而影響人體細胞的功能和角色；基因可謂人體藍圖，所帶有的序列不僅顯示親子間的遺傳關係，亦決定個人之成長

心理或任何狀況之資訊，以及關於提供個人健康照護之資訊，與過去、現在或未來提供個人健康照護之付款資訊…等資訊如符合特殊保護必要之要件，仍可將之納入特種資訊中保護。

[63] 如基因檢測公司所爲之基因檢測即可能不被病歷或醫療資訊之定義所涵蓋，而須另以規範保護。

[64] 至於爲了向健保局支領健保給付，而定期呈報健保局之診療紀錄，否應納入個資法之特種資訊予以保護，從而禁止其蒐集、利用、處理，本文認爲容有討論餘地；是否應納入特種資訊之保障，仍應回歸前述「人格權保障」，視呈報健保局之診療紀錄資訊之蒐集、處理、利用後果是否可能造成個人自我形塑權利之妨礙而定；認爲前開資訊應納入受保障醫療資訊之範圍者，請參見吳昊，由醫療資訊隱私權之觀點論全民健保 IC 卡政策，國立台灣大學法律學研究所碩士論文，2001 年，頁 145。

[65] 楊秀儀，基因診斷－當智慧使不上力量的時候，科學發展月刊第 378 期，2004 年，頁 7-8。轉引註自陳彥碩，論商業應用下基因檢測所涉法律議題，國立清華大學科技法律研究所碩士論文，2007 年，頁 13。

發育模式[66]。

基因資訊（genetic information）即爲存於人體細胞核中，決定每個人遺傳特徵的基本單位－基因－的遺傳訊息[67]。由於基因資訊可一定程度揭露個人健康資訊，其內容應屬相當私密之個人資訊，是一般多肯認基因資訊爲隱私權保障客體無疑；更有甚者，基因資訊尚顯示出部分家族遺傳性生物資訊，是以更應賦予相當保障[68]。基因資訊之利用，在目的上，可以供自己使用、提供公用或商業營利，或供學術研究之用；在方法上，可以公開、傳遞、比對或操作（如基因篩選、基因改造、基因治療…等）；在利用領域上，可及於教育、工作、醫療保險、婚姻、犯罪偵察等；基於電子科技之進步，個人資料跨國傳輸和利用亦有相應之規範[69]。

2．特別保護基因資訊之理由

由於基因資訊在一定程度上可以揭露個人健康情況及身體狀況，可爲個人身份辨識，亦顯露家族遺傳資訊，可以用來預測個人未來健康情形，如正確利用，可以協助司法鑑定、協尋失蹤人口、確定親子血緣、提升犯罪偵查效能、有助診療、預防基因變異所生疾病、研究發展新藥開發，並能帶來龐大商業利益，此危機因資訊正確運用所能帶來的正面效益例示。惟若基因資訊遭不當使用，除侵害個人人格自我形塑權之外，亦可能導致個人平等權、工作權、財產權受到侵害；以基因歧視（genetic discrimination）[70]爲例，

[66] See Nelson Cox, Lehninger Principle of Biochemistry, WORTH 276(4th ed. 2004). 轉引註自陳彥碩，論商業應用下基因檢測所涉法律議題，國立清華大學科技法律研究所碩士論文，2007 年，頁 13。

[67] 林子儀，基因資訊與基因隱私權－從保障隱私權的觀點論基因資訊的利用與法的規制，收錄於當代公法新論（中）翁岳生教授七秩誕辰祝壽論文集，2002 年，頁 694。

[68] 蔡明誠等著，基因檢測受試者同意書相關研究與討論，生物科技與法律研究通訊第 17/18 期，2003 年，頁 34。

[69] 如歐洲議會於 2002 年通過之個人資料保護與自由流通之指令（Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data）即產生域外效力（extra-jurisdictional effect）。相關論述，請參照周慧蓮，資訊隱私保護爭議之國際化，月旦法學雜誌第 104 期，2004 年，頁 112 以下。轉引註自李震山，基因科技發展與基本權利保障，收錄於多元、寬容與人權保障——以憲法未列舉權之保障爲重心，2005 年，頁 408。

[70] 美國眾議院於 2007 年 4 月 25 日通過反基因歧視法（Genetic Information Nondiscrimination

亦即，如經分析，某人的基因帶有遺傳性缺陷基因，如該資訊遭不當利用，可能在以下面向造成歧視[71]：(1) 教育上可能造成歧視：例如以基因評判智商，實施能力分班，或以基因分析性向，迫令爲一定方向之學習，侵害其受教育之自主性；(2) 工作上可能造成歧視：例如雇主考量其基因缺陷而限制其選擇職業自由、職位選擇自由、執行業務自由，甚而危及其生存權；(3) 醫療保險上可能造成歧視：醫療保險公司爲避免給付保險金，利用基因資訊對某些基因有缺陷之被保險人做過度限制，甚而影響其健康權、生命權；(4) 婚姻上可能產生歧視：如其基因缺陷被認爲對其擇偶結婚將產生不利後果，可能間接限制其婚姻權；(5) 犯罪者歧視：如某些犯罪者之基因特徵將成爲其標籤烙印，則該等犯罪者將更生不易；(6) 家族或族群之歧視：例如將有基因缺陷者之親屬擴大聯想爲遺傳性缺陷基因之帶因者，從而使該家族、甚或未出生之嬰兒受到社會烙印（stigma）。

以上對於基本權利之限制或侵害，多涉及一般人格權中之自我決定權及人性尊嚴，故基因資訊被認爲應受特殊保障[72]。惟爲避免對基因資訊利用過度限制造成科技發展之負面效用，於規範管制上即須衡量「運用基因資訊之風險」與「限制運用基因資訊之風險」[73]。

三、個人資料保護請求權保障之原則

Act, GINA)，避免雇主或保險業者僅透過基因篩檢，即拒絕雇用或承保某些具有特定基因、未來可能患有特定疾病之人。

資料來源：http://www.newscientist.com/article.ns?id=dn11787&feedId=online-news_rss20.（最後查閱日期：2009 年 6 月 30 日）

[71] 李震山，基因科技發展與基本權利保障，收錄於多元、寬容與人權保障——以憲法未列舉權之保障爲重心，2005 年，頁 408-410。

[72] 李崇僖，基因資訊隱私保護法理與規範，台灣本土法學雜誌第 91 期，2007 年，頁 75。

[73] 李震山教授即援引 Arthur Kuafmann 教授之觀點，指出「在生物科技的許多決策情況中，存在著一種以理性無法解決的衝突。…不僅贊成生物科技的實驗，即連反對的決定亦是一種冒險，因爲反對實驗可能錯失治癌症的機會。…如因倫理與法律無法提供解決衝突的合理決定標準，那麼依循以往方式所做成的決定，就必須加以容忍」，從而須「借風險決定理論及相關法社會學理論的支應，再融合正當法律程序之正義觀，或可活化規範管制之單向思考及封閉體系。」

李震山，基因科技發展與基本權利保障，收錄於多元、寬容與人權保障——以憲法未列舉權之保障爲重心，2005 年，頁 423。

（一）個人資料保護請求權保障之一般原則

草案修法總說明中，明白指出本草案係依據依據經濟合作及發展組織（OECD）於 1980 年 9 月 23 日通過之「保護隱私權及個人資料跨境流通綱領」(Guideline on the Protection of Privacy and Transborder Flows of Personal Data）[74]所揭示的個人資料保護八大原則，並參酌各國個人資料保護之立法例修正而成。此八大原則於電腦處理個人資料保護法立法時即已酌參，已屬我國個人資料保護請求權保障應予遵守之原則。惟除一般個人資訊之保障外，由於特種資訊之特殊性、敏感性，OECD 在對於保護隱私權及個人資料跨境流通綱領所提出之 detailed commends 中，針對具特殊性、敏感性之資料特別提出蒐集、處理規範，認爲某些具有特殊敏感性之資料，例如宗教信仰、前科紀錄等，對於該等資料之蒐集、利用須嚴格加以限制，甚或禁止該等資料之蒐集利用。

上述主張獲得歐洲部分立法例支持，如歐盟一九九五年資料保護指令（EU Data Protection Directive）第 8 條即規定，凡有關「種族血源」、「政治意向」、「宗教」或「哲學信仰」、「工會會員資格」等個人資料、及涉及「個人醫療」或「性生活」之資料，會員國皆應禁止處理，明確揭示了特定敏感資料的內涵[75]，並在例外的情況下允許對敏感資料進行處理[76]，例如與當事人利益相關之例外情形[77]、與公共利

[74] 資料來源：http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM（最後查閱日期：2009 年 6 月 30 日）

[75] 在此所列舉的高度敏感性資料，並不包括「犯罪紀錄或保安措施」。「犯罪紀錄或保安措施」雖亦屬另一種高度敏感性資料，原則上亦禁止處理，但其得處理之例外情形不若下述爲多，僅得於「公務機關監管下進行之，或國家法律已經提供適當而特定的安全維護措施時，會員國方得訂定例外條款，但刑案有罪判決之完整紀錄，仍應限由公務機關監管」；此種例外情形之訂定亦須通知歐盟執委會。此外，爲調和個人資料保護與表現自由，出於新聞或藝術表現目的之個人資料使用亦得訂定例外條款。

熊愛卿，網際網路個人資料保護之研究，國立台灣大學法律學研究所碩士論文，2000 年，頁 162-163。

[76] 法治斌，政府行政作爲與隱私權之探討，行政院研究發展考核委員會委託研究計畫，2000 年，頁 46-48。

[77] 例如獲得當事人明示同意，或者爲了保障當事人之重大利益，而當事人無法爲同意之意思表示時。

益有關之例外情形[78]、涉及特別種類非營利組織內之會員事項[79]、邏輯上須承認之例外情形[80]、與健康資料有關之例外情形[81]，以及涉及重大公益而不限資料種類之例外情形[82]等是[83]；該指令對歐盟會員國就指令所欲達成的目標具有拘束力，會員國得依自身情況，自行選擇形式和方法以達成指令目標[84]。

草案第 6 條新增特種資訊之保障，凡屬「醫療」、「基因」、「性生活」、「健康檢查」，以及「犯罪紀錄」之資訊皆屬受到特別保障之特種資訊，原則上禁止該等資訊之蒐集、處理或利用，符合但書條件之一者，方例外允許蒐集、處理或利用特種資料，即係採取前述立法例。

(二)、公務機關向個人取得資訊之特殊性

現代社會之資訊載具，除了以紙本記載個人資料外，出現大量個人資料以電腦蒐集、處理、保存，並經網際網路交換流通，從而，個人資料透過電腦及網際網路交換得以進行大規模整合；政府爲了達成種種行政目的、實現社會國給付社會福利之責任，在多方領域對個人資料進行蒐集、管理並使用，如政府將其所有的資料進行整合並建立起資料庫，可以想見該資料庫之龐大、個人資料內容之詳盡而鉅細靡遺；基於國家機器之巨大、資源之豐富，如未對於公務機關取得個人資料、其後對於該資料之利用、保存，以及公務機關間對於取得之個人資訊能否交換流通等事項加以限制規範，則個人隱私將可能面臨極

[78] 當國家對高度敏感性資料之處理訂有安全維護措施，且該處理係於國家法律授權範圍內，則資料保管人依其法定執掌，爲履行其義務或執行特定職權目的所必要時。

[79] 限於該處理不屬於非經當事人同意而向第三人爲揭露者。

[80] 即該資料已由當事人自行公開，或該資料之處理係爲了成立、行使或防禦其法律上主張之必要者。

[81] 即「爲防醫療、診斷之目的與看護或治療或醫療服務管理之規定所要求資料之處理」及「由醫療事業依國家法律或國家主管機關訂定之規則遵守專門職業保密規定或由第三人遵守同等保密義務而爲資料處理」。

[82] 即除前五類例外情形之外，如事涉重大公益，會員國「得依法律或主管機關規定，於有適當安全維護措施下，另定除外情形」，並將其另定之例外情形通知歐盟執委會。

[83] 熊愛卿，網際網路個人資料保護之研究，國立台灣大學法律學研究所碩士論文，2000 年，註 84，頁 161-162。

[84] 熊愛卿，網際網路個人資料保護之研究，國立台灣大學法律學研究所碩士論文，2000 年，註 84，頁 152。

巨大之侵害風險，個人形象可以透過鉅細靡遺的政府資料庫重新形塑，亦可能發生違反當初蒐集目的之個人資料使用[85]。

而人民之個人資料保護請求權係屬資訊權之一部，其內涵以「保護個人資訊隱私」及「資訊自我決定權」爲核心，兩者皆屬人格權之內容，並可連結至人性尊嚴保障；而關於基本權利之自由保障已不在侷限於外部領域，而擴及至因科技化與自動化而使國家逐漸有滲透、掌握可能的人民內部領域，爰此自由權利保護領域之擴張，認定基本權利干預之存在，即不應再如傳統憲法與行政法理論般，著眼於國家對人民造成不利益的行爲究係直接或間接、公開或隱密，而應認爲凡涉及國家對於個人資料之取得、儲存、處理與傳遞，即便在不爲當事人所知悉之情況，甚或僅在國家行政內部領域進行，因客觀上已造成對個人資料之除隱私化，以及除隱私化之持續化，故個別皆應以隱私之干預或限制視之，從而須分別得到法律授權，受法律限制[86]。

四、公務機關於就醫各階段取得資訊之態樣

（一）前言

由於我國推行全民健康保險政策，釋字第 524 號解釋將之定爲強制性社會保險，是以我國國民原則上皆爲全民健保之被保險人；我國全民健保推行之始，係採用紙卡作爲健康保險憑證，嗣後出於方便民眾就醫、提高醫療品質、健保經營效率之考量，決定推行健保 IC 卡[87]，至此，在全民健保體系下，國民之個人資訊自製作健保 IC 卡開始，即

[85] 關於公務機關間個人資訊之流通，學者林子儀教授亦認爲，基於保障個人之權益，原則上應該禁止政府機關見彼此互相流通其所取得之私人資訊，亦不建議將所有各級機關所取得之私人資訊完全集中於一中央管理之資料儲存庫。參見林子儀，「資訊取得法」立法政策與法制之研究，收錄於權力分立與憲政發展，1993 年，頁 208。

[86] 許宗力，民主法治國家的情報活動－重建情報法治的若干建議，收錄於法與國家權力，1996 年，頁 385。

[87] 健保 IC 卡除了取代以往健保卡紙卡之功能外，尚將兒童健康手冊、孕婦健康手冊和重大傷病證明卡一併納入健保 IC 卡中，除了可以記載持卡人的個人醫療費用、在保與繳費狀況外，保險對象也可以知道自己花費的部分負擔，醫院可以由累計的部分負擔，收到規定之全年住院部分負擔上限，即可不再收取，除了減少民眾負擔，也避免民眾必須先繳交部分負擔，等到次年再向健保局核退超過上限的麻煩。資料來源：中央健康保險局網站 http://www.nhi.gov.tw/webdata/webdata.asp?menu=9&menu_id=175&webdata_id=917&WD_ID=196. (最後查閱日期：2009 年 6 月 30 日)

置於國家掌控下。

在健保 IC 卡製卡發卡時，被保險人必須提供姓名、性別、出生年月日、身份證字號、電話、地址及身份證正反面影本，並可選擇卡片上是否印製相片；上述資料除健保局可接觸外，製卡廠商及投保單位與村里幹事亦可能接觸上述資訊，惟上述資訊係屬一般資訊，並非原則上禁止蒐集、處理、利用之特種資訊。被保險人持 IC 健保卡就醫時，須先將健保卡置入讀卡機中，確認持卡者為合法之在保人，並將就醫資料及費用紀錄登錄於 IC 內；所登錄的就醫資料包含[88]就醫類別為門診、住院、急診、同一療程或預防保健、主要診斷碼及次主要診斷碼並與重大傷病註記進行比對[89]、特定診療項目[90]，以及就醫費用紀錄[91]、保健服務資料[92]、孕婦產前檢查資料，及新生兒依附註記[93]。

被保險人持健保 IC 卡就醫時，就醫可用次數即自動扣減 1 次，可用次數小於 3 時，即可透過讀卡機進行健保 IC 卡更新，亦即透過讀卡機連線至健保總局查對被保險人之加保資格、繳費紀錄，並更新可就醫次數；醫事服務機構每日亦會上傳當日就醫資料至健保總局之就醫資訊蒐集伺服器，以利健保局為資料比對及補換卡資料重建。在就醫階段，健保 IC 卡持卡人之診斷碼、特定診療項目等皆會被記錄於健保 IC 卡中，雖係以代碼方式記載，但是並非無法解讀[94]，由此，個人之

[88] 以下健保 IC 卡之使用、資料更新等詳細說明，請參見衛生署中央健康保險局，徵求建議書文件第五章使用健保 IC 卡作業流程，頁 1-6；轉引註自吳昊，由醫療資訊隱私權之觀點論全民健保 IC 卡政策，國立台灣大學法律學研究所碩士論文，2001 年，頁 47-53。

[89] 如主要診斷碼或次主要診斷碼與持卡人之健保 IC 卡內登錄的重大傷病註記代碼相符時，該次就醫免部分負擔。

[90] 包括特定診療項目日期、醫療院所代碼、血型、過敏藥物、病史紀錄…等。

[91] 包括當次就醫總費用、當次就醫部分負擔金額、當年就醫總費用、當年就醫部分負擔總金額；如當年度住院部分負擔總金額達法定上限，保險對象能申請提前退費。

[92] 包括兒童保健、成人預防保健及子宮頸抹片檢查。

[93] 新生兒於辦理加入全民健保申報前，如需就醫，得依附於父母之健保 IC 卡內，限期一個月。

[94] 如全民健康保險研究資料庫即提供非學術研究者及學術研究者下載已經加密、無法辨識人別之民眾就醫資訊，包括醫療機構、藥品主檔、醫療費用、醫令清單、門診處方及治療明細、門診處方醫令明細…等，並提供譯碼簿供使用者下載。

該資料庫之源起係「中央健康保險局應學界之請託，在保障民眾隱私以及資料安全的前提下，於民國 89 年特委託國家衛生研究院以全民健保的資料為基礎，建立一個以學術研究為目

就醫資訊中，涉及該人之身心健康狀態、生理特徵或病史紀錄等，皆有完整判讀之可能；除了就醫資訊可能有被揭露之疑慮，對於健保 IC 卡中之就醫紀錄是否完整正確，一則肴於民眾之專業不足，一則因 IC 卡之讀取須經特定設備爲之，對於 IC 卡內之資料記載正確與否，民眾無從得知亦無從要求修改，對於資訊自決之保障似有不足；此外，對於 IC 卡內之醫療資訊用途是否超出當初蒐集之目的，一般民眾亦無從得知[95]。

（二）公務機關取得基因資訊之態樣：

目前，公務機關除依醫療法第 78 條爲人體試驗而取得檢體、依人體器官移植條例第 14 條[96]保存人體器官，從而有機會取得人體之基因資訊外，其他依法取得基因資訊之情況尚包含依去氧核醣核酸採樣條例，司法警察、檢察官、法院或軍事法庭出於提升犯罪偵查效能、協尋失蹤人口、協助司法鑑定…等目的[97]，請鑑定機構採樣並保存犯罪嫌

的之資訊資料庫，提供由中央健康保險局提供加密的資料檔案，經抽樣、分檔等步驟，建立新的資料庫給學術單位及非營利機構之學者專家進行醫藥衛生相關研究使用。行政院衛生署爲執行推動知識經濟，促進發展生物技術產業，以加強生物技術產業推動方案，要求提供國內衛生相關資料庫予產業界合理使用。爲避免資料相關當事人之權益受侵害，對資料之提供及運用有所規範，並制定「行政院衛生署及所屬機關提供產業界衛生相關資料庫使用作業要點」。

健保局提供上述資料之依據，似係依「中央健康保險局提供電腦處理個人資料作業要點」辦理，而依該作業要點第 1 條規定，其法源依據爲「電腦處理個人資料保護法」及其施行細則；電腦處理個人資料保護法第 8 條規定公務機關得基於某些情形爲特定目的以外之利用，而將「當事人同意」與「其他特殊情形」並列，形成擇一關係，亦即如有其他特殊情形，即便無當事人之書面同意，公務機關亦得對該資料爲蒐集目的以外之利用，其中即包含提供予他人爲學術研究。此種立法方式將告知後同意與其他公益理由並列，形同架空告知後同意，對於個人資訊自主權之維護是否適足，尚非無研究餘地。

[95] 此或因爲，對於「IC 卡內之就醫資訊會經加密後提供研究之用」這件事情，一般民眾並未經告知，在不知其資料被使用之情形下，更不可能發現其資料之使用是否超出當初蒐集之目的。

[96] 人體器官移植條例第 14 條：「爲妥善保存摘取之器官，以供移植之用，得設置人體器官保存庫；其設置，應經中央衛生主管機關之許可。前項人體器官保存庫，其設置之資格、條件、申請程序、應具備之設施、作業流程、許可之廢止及其他應遵行事項之管理辦法，由中央衛生主管機

關定之。第一項所稱人體器官保存，包括人體器官、組織、細胞之處理與保存，及以組織工程、基因工程技術對組織、細胞所爲處理及其衍生物之保存。人體器官保存，得酌收費用；其收費標準，由中央衛生主管機關定之。」

[97] 去氧核醣核酸採樣條例第 1 條：「爲維護人民安全、協助司法鑑定、協尋失蹤人口、確定親子血緣、提昇犯罪偵查效能、有效防制性犯罪，特制定本條例。本條例未規定者，適用其他有關法律之規定。」。

疑人之 DNA 資訊及樣本；如人體生物資料庫管理條例草案通過，則為達建立大規模人體生物資料庫，以發展生物科技產業之目的，公務機關得建立大規模人體生物資料庫，取得參與者之生物檢體、衍生資料、基因資料、體檢資料及其他與參與者有關之個人資料[98]。

上述基因資料來源係屬就醫資訊者，受到醫療法、人體器官移植條例之規範，惟醫療法與人體器官移植條例皆非專門針對基因資訊為保護之法律，對於與基因資訊相關之保障亦屬簡略，僅醫療法第 78 條至第 80 條[99]有對人體試驗之簡略規定，以及人體器官移植條例第 14 條對於捐贈器官之保存有簡單規定，此兩者與基因資訊之載體相關外，其他如去氧核醣核酸採樣條例，其主要係與司法鑑定及犯罪偵查相關，而與就醫資訊無涉[100]。

然而，醫療法與人體器官移植條例雖非專門針對基因資訊為保護之法律，就取得基因資訊仍須考量個人資料之保護，首重仍以取得「書面同意」為前提要件。依據醫療法第 79 條規定，醫療機構施行人體試

[98] 人體生物資料庫管理條例草案第 4 條。

[99] 醫療法第 78 條：「為提高國內醫療技術水準或預防疾病上之需要，教學醫院經擬定計畫，報請中央主管機關核准，或經中央主管機關委託者，得施行人體試驗。非教學醫院不得施行人體試驗。但醫療機構有特殊專長，經中央主管機關同意者，得準用前項規定。前二項人體試驗計畫，醫療機構應提經有關醫療科技人員、法律專家及社會工作人員會同審查通過；計畫變更時，亦同。」

醫療法第 79 條：「醫療機構施行人體試驗時，應善盡醫療上必要之注意，並應先取得接受試驗者之書面同意；受試驗者為無行為能力或限制行為能力人，應得其法定代理人之同意。前項書面，醫療機構應記載下列事項，並於接受試驗者同意前先行告知：一、試驗目的及方法。二、可能產生之副作用及危險。三、預期試驗效果。四、其他可能之治療方式及說明。五、接受試驗者得隨時撤回同意。」

醫療法第 80 條：「醫療機構施行人體試驗期間，應依中央主管機關之通知提出試驗情形報告；中央主管機關認有安全之虞者，醫療機構應即停止試驗。醫療機構於人體試驗施行完成時，應作成試驗報告，報請中央主管機關備查。」

[100] 去氧核醣核酸採樣條例第 9 條亦有為確定親子血緣之目的而得自費為採樣之規定，惟該規定之適用主體即為自費採樣之一般人，以及受託進行採樣之醫療機構；除此之外，其他的適用主體包括法院、檢察官、司法警察；得為採樣而得以取得資訊、保存樣本之機構，國內則僅有法務部之刑事警察局及調查局。由上述以觀，基因資訊與可能與廣義醫療資訊重疊之部分，僅包含由醫療機構所產出之基因資訊；實則此部分並非去氧核醣核酸採樣條例之重點，去氧核醣核酸條例之主要功用仍在犯罪偵查，以及司法鑑定…等方面。

驗時，除應善盡醫療上必要之注意，尚應先取得接受試驗者之書面同意並告知相關事項；又，依人體器官移植條例所爲摘取屍體或他人之器官施行移植手術，在保護當事人之資訊自決權下，原則上仍須以書面同意作爲前提要件，例如人體器官移植條例第 6 條至第 8 條之 1 規定[101]。在此，以書面同意作爲醫療機構進行人體試驗、取得基因資訊或摘取屍體及他人之器官施行移植手術之前提要件，似符合保護個人之資訊自決權，仍須注意者在於，當事人對於受告知之項目是否得以充分理解，在充分理解下相關事項下，方得使當事人之同意成爲有效之同意；當事人撤回同意後，是否一併將其個人資料銷毀，以免留存外洩；在管理、保存個人基因資訊之監督及控管是否安全不致外洩或遭侵入擷取等等，上述疑慮仍屬保護當事人之個人資訊自決權之相關範圍，不得不慎。

惟如人體生物資料庫管理條例草案一旦通過，將透過基因資訊所

[101] 人體器官移植條例第 6 條：「醫師自屍體摘取器官，以合於下列規定之一者爲限：一、死者生前以書面或遺囑同意者。二、死者最近親屬以書面同意者。三、死者生前爲捐贈之意思表示，經醫師二人以上之書面證明者。但死者身分不明或其最近親屬不同意者，不適用之。」

人體器官移植條例第 7 條：「非病死或可疑爲非病死之屍體，非經依法相驗，認爲無繼續勘驗之必要者，不得摘取其器官。但非病死之原因，診治醫師認定顯與摘取之器官無涉，且俟依法相驗，將延誤摘取時機者，經檢察官及最近親屬書面同意，得摘取之。」

人體器官移植條例第 8 條：「醫院自活體摘取器官施行移植手術，應合於下列規定：一、捐贈器官者須爲成年人，並應出具書面同意及其最近親屬二人以上之書面證明。二、摘取器官須注意捐贈者之生命安全，並以移植於其五親等以內之血親或配偶爲限。前項第二款所稱之配偶，應與捐贈器官者生有子女或結婚二年以上。但結婚滿一年後始經醫師診斷罹患移植適應症者，不在此限。成年人捐贈部分肝臟移植於其五親等以內之姻親，或滿十八歲之未成年人捐贈部分肝臟移植於其五親等以內之親屬，不受第一項第一款須爲成年人及第二款移植對象之限制。滿十八歲之未成年人捐贈肝臟，並應經其法定代理人出具書面同意。醫院自活體摘取器官施行移植手術，應對捐贈者予以詳細完整之心理、社會、醫學評估，經評估結果適合捐贈，且在無壓力下及無任何金錢或對價之交易行爲，自願捐贈器官，並提經其醫學倫理委員會審查通過，始得爲之。第三項之肝臟捐贈移植，醫院除應依前項規定辦理外，並應報經中央衛生主管機關許可，始得爲之。前項許可，中央衛生主管機關得邀請專家、學者組成委員會審議；委託經中央衛生主管機關指定之機構爲之時，亦同；其許可辦法，由中央衛生主管機關定之。」

人體器官移植條例第 8 條之 1：「前三條規定所稱最近親屬，其範圍如下：一、配偶。二、直系血親卑親屬。三、父母。四、兄弟姊妹。五、祖父母。六、曾祖父母或三親等旁系血親。七、一親等直系姻親。前項最近親屬依第六條第二款或第七條但書規定所爲書面同意，不得與死

者生前明示之意思相反。前項書面同意，最近親屬得以一人行之；最近親屬意思表示不一致時，依第一項各款先後定其順序。後順序者已爲書面同意時，先順序者如有不同之意思表示，應於器官摘取前以書面爲之。」

具有之高度人別辨識性對人格權產生極大衝擊。按人體生物資料庫管理條例草案之立法目的，即爲使大型人體生物資料庫之設置、營運及組織得有法源依據[102]；建立此等資料庫之最終目的，即在於透過研究資料庫中生物檢體所載資料，與健保資料庫及戶籍資料庫進行交叉比對，從而得出特定基因資料與特定疾病間是否具關連性之研究結果[103]。

如此等跨生物、醫療與戶籍等資料庫之個人資訊交換機制建立，對於生物科技及醫療技術或有很大助益，但是參與者個人身體、心理健康狀態及歷史，甚或其家族之病史資訊，皆可能在此龐大的資料庫中獲得，並可透過資料庫中的戶籍等一般性資料特定出該人之住址等資訊，人之圖像透過虛擬的資訊交換整合幾可具現，無論該圖像與其所欲建構之形象是否相吻合，是否有侵害人格權之疑慮，尚非無疑；對於個人資訊權之保障可能帶來的科學進步阻礙，亦應加以考慮。

五、對於個資法草案之檢討及建議

綜觀個資法草案就公務機關取得個人就醫資訊保障之規定，有如下幾點建議：

（一）個資法草案未針對「公務機關」與「非公務機關」取得個人資訊之本質進行區分：

公務機關蒐集、處理、利用個人資料，本質上屬國家公權力對於個人基本權利之限制、侵害，此際立法應規範者，爲國家自我節制公

[102] 人體生物資料庫管理草案第 1 條。

[103] 請參考「台灣社會需要什麼樣的個人資料保護？個資法相關法案座談會」第二場次會議錄音，政大法科所劉宏恩教授發言錄音，與現場與會者發言發問錄音中，衛生署代表羅彥清博士之發言。台灣人權促進會主辦，2008 年 9 月 27 日。

建制大規模生物資料庫係初步階段，目前由衛生署委由中研院進行建制，目標爲取得兩萬名參與者之生物檢體，第二階段以後所欲進行的，始爲上述的跨資料庫資訊交換；正因爲所取得的檢體資訊必須能和現實生活中的參與者健康狀況進行比對，建立資料庫才有其意義，故學者劉宏恩批評該條例草案中所採取的「去連結」措施根本不可能實行、亦無法透過「去連結」保障參與者之資訊隱私權。或許參與者於參與前必須有放棄其隱私權之覺悟，然而，如前所述，基因資訊並不只牽涉該個人之隱私，尚包含其家族其他成員之隱私，是否能單憑一人意志即得放棄，非無討論空間，而保障資訊隱私權之同時，亦應考量對生物科技進步可能造成之阻礙，而以倫理進行兩者之調和。

資料網址：http://www.tahr.org.tw/index.php/article/2008/08/29/608/.（最後查閱日期：2009 年 6 月 30 日）

權力之行使；相對地，對於非公務機關蒐集、處理、利用個人資料，本質上係屬私人將其他私人之人格權內涵物化爲具有商業價值之標的，國家對於私人人格權應擔負積極保障之任務，與前述國家自己爲個資蒐集使用者之消極角色實爲相反。個資法草案在同一部法律中同時規範公務機關與非公務機關，但是對於國家在此兩部分應扮演的角色、功能卻未有明確劃分。

（二）就醫資訊中，「病歷」與「醫療」資訊之定義、範圍區分不明：

如前所述，草案將「病歷」與「醫療」並列，似指兩者內涵不同，卻將「醫療」納入特種資訊中加以保障，則令人難以想像，如果醫療不包含病歷，則醫療之內涵還剩什麼，亦不能理解爲何病歷被排除在特種資訊之外。

（三）特種資料蒐集、處理、利用之除外條款過於寬鬆，誤解「告知後同意」與其他事由應爲「聯立」而非「擇一」關係：

草案第 6 條列舉 5 種理例外情況得蒐集、處理、利用特種資訊，包括法律明文規定、法律未禁止且當事人書面同意、執行法定職務所必要、當事人已公開或其他以合法公開資料，以及出於研究目的且已處理無從辨識當事人等例外情況。惟參酌國外立法例，即便有法律明文規定、執行法定職務所必要、當事人已公開或其他以合法公開資料，以及出於研究目的且已處理無從辨識當事人等例外情況，仍應取得當事人之同意，使得爲資料之蒐集、處理及利用；否則僅因法律規定、法定職務或有研究需要，即不需取得當事人同意，無異將當事人之資訊自決權架空，保障資訊自決權即形同具文。

（四）公務機關得否爲資訊蒐集以外之目的，而爲機關間資訊之交換、界限如何，草案第 16 條規定過於寬鬆：

如前所述，正由於國家機器之龐大、蒐集資料之範圍廣泛，對於國家蒐集、處理、使用個資才應爲節制之規定，始符合限制公權力、保障基本權利之本質；如依草案第 16 條規定，則國家得爲蒐集目的外使用之例外情況過多，甚至可能不必獲得當事人書面同意，只要有其他公益事由即足，對於國家限制過於寬鬆，個資保障可能不足。

（五）立委謝國樑提案版本第 9 條「邱毅條款」對於個資保護形成漏洞：

立委謝國樑提案版本第 9 條第 2 項第 6 款規定，民意代表基於質詢問政之目的而蒐集之個人資料，於處理或利用前免向當事人告知該個資來源（第 9 條第 1 項）、蒐集者名稱（第 8 條第 1 項第 1 款）、蒐集目的（第 8 條第 1 項第 2 款）、個資類別（第 8 條第 1 項第 3 款）、利用期間、地區、對象及方式（第 8 條第 1 項第 4 款），以及當事人有權得請求查詢、閱覽、製給複製本、補充或更正，以及請求停止蒐集、處理、利用或請求刪除（第 8 條第 1 項第 5 款）。該款新增之理由「各級民意代表質詢問政之資料，經常由第三者所提供，如需依第一項之規定向當事人告知資料來源，將造成實務上質詢與問政之困擾，故應予排除。」、「如當事人不認同蒐集機關適用本條第二項之規定而免爲告知時，得依本法第三條規定請求查詢或閱覽，被請求機關則應依第十三條規定辦理。當事人亦得以其蒐集不合法爲由，請求補爲告知，或依第十一條第四項規定，請求蒐集機關刪除、停止處理或利用該個人資料，併予敘明。」

該款之立法理由與其內容並不一致；既認爲透露資料來源將造成日後於立法院問政之困擾，則排除於利用前告知個人資料來源即已足，告知當事人第 8 條第 1 項第 1 至 5 款事項與透露資料來源係屬二事，立法理由中並未說明，即將當事人受前述事項告知之權利剝奪，並不妥適，有過度侵害個人資訊自決權之疑慮。此外，立法委員於國會殿堂質詢問政，常有電子媒體及平面媒體即時報導，如立法委員質詢問政，在當事人毫無預警之情況下即於媒體前公佈當事人之資料，則個人資料一旦被揭露，其隱私權所受之侵害即無從回復，如不課予立法委員於利用資料前爲告知義務，則個人對於此種公權力侵害個人資訊權之態樣即無從即時防範，亦即無法即時依第 3 條規定請求停止利用，無異於嚴重剝奪個人資訊自決權之核心內涵，與立法委員行使質詢權限相較，何者應予優先保障，容有充分討論之餘地。

（六）個資保護之監督機制不備：

草案對於個資保護之監督機制並不完備，亦未區分「公務機關」

與「非公務機關」之監督機制。對於非公務機關之監督機制採取分散式立法，由事業主管機關及各地方政府爲之，此種多頭馬車式的監督立法，加上賦予事業主管機關及各地方政府行政檢查之權限，產生了令狀主義開後門之疑慮，亦即搜索扣押假借行政檢查之名規避令狀之必要性，且事業主管機關及各地方政府皆得爲之，對於非公務機關之權利將造成極大影響。

對於公務機關之監督機制，草案中則未有規定，僅提示個資當事人得提起行政訴訟、請求國家賠償；惟個人資訊權受到侵害之態樣之形式特殊，受侵害之當事人的個人資訊常係在不自覺的情況下被違法蒐集、處理、利用，從而當事人對於侵害之發生更係難以察覺；此際，國家對於公權力侵害個人資訊權非不僅自我節制，自我監督檢查之機制亦爲闕如，反要求人民以自力救濟之方式對抗國家無形之侵害，實屬立法之缺漏。

（七）條文之可操作性：

如前所述，由於個資受侵害常發生於當事人不自覺的情況下，是以草案條文之可操作性如何，意即當事人得否透過個資法草案條文之操作確實保障其資訊權，尚待討論。

第三項　案例分析

首先，在本外洩案中，將患者之個人姓名、居住縣市、及病歷等均公告在網路之上，故當然符合電腦處理個人資料保護法（以下稱「個資法」）第 3 條第 1 款之規定受該法之保障。 另外，本次外洩案係屬於疾病管制局之業務範疇，故按個資法同條第 6 款之規定，疾病管制局係屬於公務機關，故應該適用個資法第二章「公務機關之資料處理」以下之規定。先就前階疾病管制局爲肺結核病人資料蒐集之行爲論之，傳染病爲第三類法定傳染病，且按傳染病防治法第 2 條和第 5 條之規定，衛生署疾病管制局按本法第 7 條之規定，因肺結核爲法定傳染病，按傳染病防治法第 5 條第 1 項之規定，中央主管機關，訂定傳

染病防治政策及計畫，包括預防接種、傳染病預防、流行疫情監視、通報、調查、檢驗、處理及措施。且按同法第 58 條與第 59 條之規定，中央主管機關疾病管制局為防止傳染病傳入、出國（境），得採行必要防疫、檢疫措施，且對未治癒且顯有傳染他人之虞之傳染病病人，通知入出國管理機關，限制其出國（境）。是故，疾病管制局為了監控肺結核疫情資訊，預防肺結核病人搭機擴散疫情而為蒐集肺結核病人之病歷資料，係屬於法令規定的職掌必要範圍之內，因此前階段蒐集肺結核病人資料之行政行為隸屬防疫特定目的之法定職權，故符合個資法第 7 條之規定[104]。又依個資法第 17 條之規定，疾病管制局應對該結核病人的個人資料指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏，本結核病人資料外洩一案，因維護系統設計出現瑕疵，致具系統權限者於使用查詢功能時，遭擷取造成，疾病管制局對此資料外洩一事，自有違個資法第 17 條之規定，資料外洩之當事人對此外洩一案所造成之損害，當可依個資法第 27 條及第 30 條規定，向疾病管制局請求損害賠償。

其次，本案例指出公務機關或非公務機關在合於個資法之規定下蒐集利用個人資料，對於個人資料之維護及保全，僅有個資法第 17 條及第 26 條準用第 17 條之規定，指定專人依相關法令辦理安全維護事項，如此規定過於簡略以及草率，並將公務機關以及非公務機關作一體之規範，如此規定是否妥適，則非無疑義。是故，個資法修正草案（名稱修正為個人資料保護法，以下簡稱「草案」）對此有所修正，區分公務機關及非公務機關辦理資料安全維護事項，在非公務機關辦理資料安全維護事項情形，中央目的事業主管機關得指定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，此規定於草案第 27 條[105]，並參其說明理由第 3 點[106]，由於非公務機關行業別限制取消

[104] 曾令嫻，論電子病歷流通與個人資料保護之研究-以告知後同意為中心，國立中正大學法律學研究所碩士論文，2006 年，頁 185。

[105] 草案第 27 條：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定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。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」

[106] 草案第 3 點立法說明：「由於非公務機關行業別限制取消，現行條文第二十條第五項業已刪除。然某些行業如銀行、電信、醫院、保險等，因保有大量且重要之個人資料檔案，其所負之安全保管責任應較一般行業為重，爰增訂第二項規定，授權中央目的事業主管機關得指定特定之非公務機關，要求其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，以加強管理，確保個人資料之安全維護。」

之故，某些行業如銀行、電信、醫院、保險等，因保有大量且重要之個人資料檔案，其所負之安全保管責任應較一般行業爲重，爰增訂中央目的事業主觀機關得指定特定非公務機關，要求其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，以加強管理，確保個人資料之安全維護。

再者，對於當事人因個人資料外洩而造成自身權益之損害，個資法於第四章規定損害賠償及其他救濟途徑，依個資法第 27 條及第 28 條分別規定公務機關及非公務機關在違反個資法規定之下，當事人得請求賠償之要件及其相關規定，並依個資法第 30 條規定，損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。是故，當事人如因個人資料之洩漏欲請求賠償，則須回歸於國家賠償法以及民法上的侵權行爲責任而請求損害賠償，在侵權行爲責任之認定，應須檢驗是否符合其成立要件，包含加害行爲、行爲須不法、須侵害他人權利、須致生損害、須有責任能力、須有故意過失等要件[107]，而該等要件除法律另有規定外，原則上須由主張權益受侵害者負舉證責任。在本外洩案中，可以預見當事人如欲請求損害賠償，勢必負起上述該等要件之舉證責任，惟，就個人資料之單純外洩，是否即符合權益受侵害的情形，抑或是須因個人資料外洩而遭受到權益之侵害，例如名譽權、財產權受侵害等，方符合上述侵權行爲之認定而得請求損害賠償，兩者間之認定似乎不甚明確。就草案而言，僅將個資法現行條文「致當事人權益受損害者」等文字，修正爲「侵害當事人權利者」，使其與國家賠償法與民法規定用語一致，並未就此問題多作修正。對此，在維護人性尊嚴與尊重人格自由發展，乃自由民主憲政之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並爲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，隱私權乃爲不可或缺之基本權利，而受憲法第 22 條所保障。[108]在上述憲法保障隱私權及個資法第 1 條以避免人格權受侵害之規定之下，爲擴大對隱私權及人格權之保障，應可認定個人資料在單純洩漏之下，即已侵害當事人之隱私權而受有損害，不須再於資料外洩後，證明自身何種權益因資料外洩而受到侵害。

[107] 侵權行爲之成立要件學說上分類或有不同，本文參考王澤鑑，侵權行爲法（1）2002 年版，頁 97 以下。

[108] 歷見大法官釋字第 603 號解釋、第 585 號解釋。

此外，在侵權行爲主觀要件上，當事人必須舉證證明公務機關或非公務機關在違反個資法的情況下對於個人資料之蒐集、處理、利用、保全及維護具有故意過失，就本案例而言，疾病管制局因其個人資料維護設計有所缺陷，致個人資料之外洩，疾病管制局就此侵害有無故意過失之舉證，一般民眾如何得知疾病管制局的內部維安設計管理之缺陷以及對於個人資料之洩漏是否具有故意過失，其得以何種方式舉證，實殊難想像，則當事人無法舉證疾病管制局對資料外洩具有故意過失，疾病管制局之侵權責任將無法構成，當事人權益之損害則無法獲得賠償。按個資法第 28 條規定，非公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但能證明其無故意或過失者，不在此限。個資法以推定責任之方式減輕當事人之舉證責任，使當事人獲得賠償之途徑將不再如此困難，實足肯定，惟此舉證責任減輕之規定僅適用於非公務機關，草案亦未將舉證責任減輕之規定列於公務機關(依草案第 27 條爲無過失的事變責任)得以一併適用，如此對當事人面對遭受公務機關之侵害時，將面對舉證責任之困難而終致求償無門，對當事人權益之保障，恐有不足之處。又，個人資料若遭竊取、竄改、滅失或洩漏之情形下， 其損害之範圍可能因公務機關、非公務機關或當事人之不自知，而將無限的蔓延及擴大，如此對當事人權益之侵害甚大致難以估計，而個資法並未對於侵害的立即排除多作規定，在草案中亦未見說明增訂，在侵害造成後的侵害排除規定，顯見闕漏及不足。

第二節 公務機關對就學資訊的管控與監督

第一項　問題之發現與提出

一、醫學系實習生強制篩檢愛滋案[109]

（一）案例事實

[109] 中華民國憲法第 8,22,23 條 ・人類免疫缺乏病毒傳染防治及感染者權益保障條例第 15,16,23 條 ・桃園縣管理娼妓自治條例第 6,19,22 條 ・後天免疫缺乏症候群防治條例施行細則第 3,5-7 條・各級學校防治後天免疫缺乏症候群處理要點第 4-7 條 ・署授疾 字第 0970000016 號。

日前發生醫學系實習生因感染愛滋遭醫學中心拒絕實習，全國公私立醫學校院院長會議後行文衛生署疾病管制局，詢問可否針對實習醫師強制篩檢？疾管局開會後實習醫師不是高危險群，強制篩檢恐將違法。另，為避免拒絕篩檢的實習醫師被貼標籤，也不建議以「知情同意」方式篩檢。 針對實習生或實習醫師強制篩檢的提議，由於涉及敏感人權爭議，及學生受教權保障，疾管局日前邀集專家學者、愛滋防治團體進行討論，最後決議不得要求強制篩檢，也不得要求提出檢驗證明。疾管局建議醫院、醫學院，以委員會或專案小組方式，發現學生、實習醫師感染者時，保護其隱私權，並提供就學權益保障、病情追蹤、病患風險評估等協助，保障醫病權益。

疾管局官員表示，近年來不只一位醫學生因感染愛滋病而在實習之前遇到「困擾」，也曾聽說醫學生被實習醫院拒絕的傳言。據了解，所涉及院校均保密處理，評估實習生的權益與臨床接觸病患的風險後，適度調整課程（如侵入性治療課程僅觀摩不動手等）。官員坦言，的確有部分醫院要求醫學系實習生應提供體檢證明或篩檢報告，但這已違法，不論學校或實習醫院，依法都不得要求進行愛滋篩檢或要學生提出相關檢驗證明。疾管局強調，根據人類免疫缺乏病毒傳染防治及感染者權益保障條例(之前稱為「後天免疫缺乏症候群防治條例」)第 15 條第 1 項規定，當衛生單位接獲報告或發現感染、或疑似感染愛滋，及與感染愛滋病毒者有性接觸者，應通知篩檢，逾期未受檢則強制篩檢。疾管局曾以行政院衛生署 97 年 1 月 18 日署授疾 0970000016 號函公告，基於感染風險、國內防疫與國防需要，「應」接受強制愛滋病毒檢查九大類對象，包括性工作者、嫖客、性病感染者、吸毒者、賣毒者、矯正機關收容人、外籍勞工、現役軍及義務役役男等族群，但不包括醫事人員，「連醫生也沒有全面篩檢」。

官員指出，除被公告須強制篩檢愛滋病毒的對象外，衛生機關不能對一般人強制篩檢。官員強調，台灣醫護人員高達數十萬人，歷年感染者僅三十七人，就比例而言，絕非高危險群，且一旦發現感染愛滋後，可調整為非侵入性治療的職務，包括放射科、病理解剖及檢查、衛教行政工作，減少感染機率。此外，與會專家認為，可預期國內從

事醫學相關職業的愛滋感染者「會越來越多」，建議應比照國外做法，醫院、校合作成立諮詢委員會，協助已知感染的醫學生或醫師，協調出能維護醫病雙方權益的具體臨床操作準則。

（二）本案所涉及之爭點

關於本案例而言，涉及到醫院、學校、或實習機關可否因特定之目的對實習生進行強制篩檢愛滋，並拒絕感染或疑似感染愛滋病的實習生進行實習之課程，而此等舉動是否違反個資法對個人資料之保障，以及影響實習生進行實習課程之受教權[110]等。

二、基測個資外洩案[111]

（一）案例事實

教育部委託博暐圖書網路公司辦理 97 年國中基測電腦處理作業，但博暐違法販售考生個資及成績，侵害考生權益，監察院通過糾正，指出教育部疏於監督，明顯怠忽職責。教育部主任秘書潘文忠對此表示，教育部尊重並接受建議，也會檢討改進。監察院調查發現，博暐公司趁取得考生個人基本資料及成績機會，將 97 年第一次國中基測考生個資及成績外洩，販賣給中南部 10 多家補教業者，並提供給 7 所私立高中作爲招生之用。

監察院指出，全案經高雄地檢署及台中地檢署分別偵查起訴，但高雄地檢署偵查又發現，博暐公司在承包 96 年國中基測電腦作業時，就曾經協助學生僞造假成績單。此外，93 年國中基測時，電腦作業承包廠商大正資訊網路公司也發生運用考生個資，寄發升學特輯給考

[110] 大法官釋字第 626 號解釋理由書：「…按人民受教育之權利，依其憲法規範基礎之不同，可區分爲「受國民教育之權利」及「受國民教育以外教育之權利」。前者明定於憲法第二十一條，旨在使人民得請求國家提供以國民教育爲內容之給付，國家亦有履行該項給付之義務。至於人民受國民教育以外教育之權利，固爲憲法第二十二條所保障（本院釋字第三八二號解釋參照），…」

[111] 2008-11-14/聯合報/C3 版/教育

生，顯示教育部辦理國中基測有很多疏失不當。監察院糾正案文指出，教育部未能預見國中基測試務繁雜且專業，每年由不同學校輪流主辦，易爲承包廠商壟斷，且未善盡監督電腦採購作業職責，又未能以93年考生個人資料外洩爲鑑，積極檢討改進，加強保密措施，以致於97年弊端擴大，教育部疏於監督，明顯怠忽職責。

潘文忠指出，當初教育部發現博暐有違法情事，即主動移送檢調調查，希望依法快速處理；在教育部內部也舉辦多次檢討會議，檢討流程及討論未來是否設專責機構處理等，以便進一步做好防護工作。教育部中教司司長蘇德祥則表示，教育部在事後已有積極改善作爲，明年考生的個人資料將送交政府專責單位，不再委由民間處理，不會有外洩問題(教育部目前已規劃成立基測專責單位，並自本(98)年起，委請國立台灣師範大學協助辦理試務電腦作業，加強保護考生個資)。

（二）本案所涉及之爭點

本案係爲教育部委託博暐圖書網路公司辦理97年國中基測電腦處理作業，涉及學生個人資料及成績之外洩，引發侵害隱私疑慮之探討議題。以下先就學生資訊之態樣與之管理方式爲簡介，再就上開各類資訊之管控監督爲介紹，最後再針對案例進行分析。

第二項　就學資訊之態樣與管理方式

一、教務[112]

教務行政工作主要包涵學籍資料管理、學生成績管理、課程排課管理、學生選課、教師研究、教師服務等，與學生就學資料較爲相關的，主係「學籍資料管理」與「學期成績管理」兩項。

（一）學籍資料

[112] 賴靜儀，從資訊自決權論學生資料保護，94年國立臺灣師範大學公民教育與活動領導學系碩士論文，頁128-138。

1．目的

學生學籍資料填寫建立之目的，係爲了將有關學生入學、輟學、復學、轉學、成績及學籍等資料予以統整以便於管理。

2．內容

包含學生在校之學號、姓名、身份證字號、性別、出生年月日、出生地、學生身份別、家長姓名、家長和學生的關係、監護人電話、戶籍地址…等。多屬於個人資料保護法草案中之一般資訊，其蒐集、處理、利用原則上並未受到禁止，惟仍須尊重當事人權益，依誠實信用方法爲之[113]。

3．管理方式

關於學籍資料之管理，以國民教育爲例，各地方政府依國民教育法施行細則第 20 條自訂學籍管理要點，各地方政府規範密度寬嚴不一；惟其內涵多包括學籍資料之建立、更正、保存方式與期限，以及學籍資料之調閱限制等項目。一般而言，學籍資料之管理多係由教務處註冊組負責。其中，關於學生學籍資料之調閱，原則上調閱對象應予限制，各地方政府多規定除依法調閱外，不得隨意出具相關資料。

（二） 學期成績

學期成績爲目前主要評量學生學習成果之指標，故於我國極受重視。包含學生姓名、各科之成績，以及排名；目前學校就學生成績之管理幾已電腦化，由任課老師上網填寫成績，有密碼者即可查閱相關電腦資料。國民小學及國民中學學生成績評量準則第 10 條規定，國民中小學學生成績評量結果及紀錄，應本保密及維護學生權益原則，非經學校、家長及學生本人同意，不得提供作爲非教育之用。

[113] 個人資料保護法草案第 5 條。

二、學務[114]

學務處與學生個人資料相關者，包括「學生獎懲缺曠紀錄」，以及「學生健康資料」。學生之獎懲紀錄中，一般多認爲「懲處」紀錄之公佈對於學生會造成較大心理壓力及影響，故如台北市、台北縣、高雄市皆規定關於學生之懲處紀錄以不公開爲原則。

學生健康資料之內容，則包含學生健康檢查紀錄、宿疾資料紀錄等，蒐集之目的則係作爲學生在校活動和教師教學時參考使用。惟學生健康資料內容亦與醫療資訊有所重疊，如健康檢查紀錄即屬個人資料保護法草案（以下簡稱個資法草案）第 6 條規定原則上禁止蒐集、處理、使用之特種資料，是應將學生健康資料內容納入醫療資訊範疇，適用較高密度保障。

三、輔導

輔導處與學生資料管理相關之工作包括建立完整學生輔導資料、實施心理測驗及行爲評量並登錄於學生綜合資料表供教師參考、實施認輔制度並建立相關輔導紀錄、處理中輟生相關業務並建立中輟學生相關檔案資料。

（一）中輟生資料建檔

1．中輟生通報及中輟生資料庫建檔流程

(1)中輟生通報流程

國中小學生如未經請假，而未到校上課達三日以上，或者轉學生未向轉入學校報到者，列爲中輟生，由學校立即填具通報單通報直轄市、縣（市）政府，並報請鄉（鎮、市、區）強迫入學委員會執行強迫入學事宜[115]。直轄市、縣（市）政府接獲學校通報之中輟生資料後，應於三日內彙報教育部。教育部應即將中途輟學而行蹤不明學生檔案資料函送內政部警政署。對於應入學而未入學、已入學而中途輟學或長期缺課之適齡國民因家庭清寒或家庭變故而不能入學者，學校應檢具該生及其家庭相關資料報請當地直轄市、縣

[114] 賴靜儀，從資訊自決權論學生資料保護，94 年國立臺灣師範大學公民教育與活動領導學系碩士論文，頁 139-142。

[115] 國民中小學中途輟學學生通報及復學輔導辦法第 2 條。

(市) 政府。直轄市、縣（市）政府接獲學校之通報，應立即指派社工人員調查，依社會福利法規予以特別救助，亦得請家庭教育中心提供親職教育之諮詢服務[116]。

內政部警政署接獲教育部函送之中途輟學而行蹤不明學生資料後，立即透過其資訊設施系統傳送各地警政單位，配合查尋。各地警政單位協尋查獲中途輟學而行蹤不明學生應即通知原就讀學校之主管教育及社政行政機關，會同學校及鄉（鎮、市、區）強迫入學委員會輔導學生復學。直轄市、縣（市）政府應指定聯絡人於非上班時間，即時受理警政單位通知，執行協助尋獲學生之復學事宜[117]。

(2)中輟生資料庫建檔流程[118]

直轄市、縣市教育廳局應督責所屬國民中小學建立「中途輟學學生檔案」(電腦系統檔），按學年度登錄校內中途輟學學生資料，包括輟學日期、輔導復學、回流輟學情形，並定期（按月）與縣市通報資料比對檢核；教育部（電算中心)則發展「國民中小學中途輟學學生通報及復學管理系統 Windows 版本」，自八十七學年度起全國連線使用，並與警政單位直接連線，使教育、警政，強迫入學委員會能夠同時即時掌握中途輟學學生資料。內政部警政署則儘速將中輟失蹤學生資料系統，發展爲巡警掌上型電腦通報資料，提供全國巡迴警察人員，同時通報協尋中輟失蹤學生，增進通報協尋時效，提高尋獲輔導復學比率。

(3)中輟生資料之管理方式

雖然國民中小學中途輟學學生通報及復學輔導辦法已說明中輟生資料建檔之必要及流程，但是對於建檔以後的利用、保存、期限、使用範圍…等規定卻付之闕如，僅能依據現行的電腦處理個人

[116] 國民中小學中途輟學學生通報及復學輔導辦法第 3 條。

[117] 國民中小學中途輟學學生通報及復學輔導辦法第 4 條。

[118] 教育部中途輟學學生通報及復學輔導方案第 4 條。

資料保護法、刑法等相關規定約束之；亦即，對於中輟生之資料建檔後，並未有法律或命令規範該等資料之管理方式。

2．建立中輟生資料庫可能產生的問題

(1)建立資料庫之法源依據

依據國民中小學中途輟學學生通報及復學輔導辦法第 1 條規定，該辦法之建立係依強迫入學條例及兒童及少年性交易防制條例第 11 條第 2 項規定訂定。

依據國民教育法第 2 條第 2 項之授權，立法者訂定了強迫入學條例，第 9 條並規定：「凡應入學而未入學、已入學而中途輟學或長期缺課之適齡國民，學校應報請鄉（鎮、市、區）強迫入學委員會派員作家庭訪問，勸告入學；其因家庭清寒或家庭變故而不能入學、已入學而中途輟學或長期缺課者，報請當地直轄市、縣（市）政府，依社會福利法規或以特別救助方式協助解決其困難。（第 1 項）前項適齡國民，除有第十二條、第十三條所定情形外，其父母或監護人經勸告後仍不送入學者，應由學校報請鄉（鎮、市、區）強迫入學委員會予以書面警告，並限期入學。（第 2 項）經警告並限期入學，仍不遵行者，由鄉（鎮、市、區）公所處一百元以下罰鍰，並限期入學；如未遵限入學，得繼續處罰至入學爲止。（第 3 項）」

由強迫入學條例觀之，該條例僅要求學校爲「通報」義務，並授權予鄉（鎮、市、區)爲書面警告、限期入學及連續課以罰鍰之權限，並未授權教育部建立全國性的中輟生之資料庫，亦未授權教育部將中輟生資料跨部會地提供給警政署。

兒童及少年性交易防制條例第 11 條第 2 項規定，教育部應於本條例施行後 6 個月內頒布中途輟學學生通報辦法；該條例亦僅授權教育部建立通報機制，並未授權教育部建立全國性的中輟生之資料庫，亦未授權教育部將中輟生資料跨部會地提供給警政署。

(2)建立中輟生資料庫並跨部會分享資訊可能引發之爭議

如上所述，教育部係依據教育部中途輟學學生通報及復學輔

導方案第 4 條建立全國的「國民中小學中途輟學學生通報及復學管理系統」並與警政單位連線，惟授權之母法僅要求建立通報系統，此授權是否能含括建立全國性的資料庫，以及與警政署連線，尚非無疑。

退一步言，建立通報系統之目的無非在於找回中輟生，使之復學，如認爲一定要建立全國性資料庫並與警政署連線，才有可能使得通報系統發揮其作用，則應取得法律位階之授權，而非僅以命令位階的輔導方案規定之。

按中輟學生之資料雖僅爲特定時間中，學生輟學日期、通報及輔導紀錄、復學日期、再度中輟情形、追蹤輔導紀錄等事實的紀錄，但是仍可能包含當事人不欲爲人知的資訊，例如中輟輔導紀錄中可能說明當事人中輟之原因，此爲當事人不欲人知者，即爲一例。

如認中輟生資料屬於個資法草案第 2 條第 1 款所指「得以直接或間接方式識別該個人之資料」，有個資法之適用，則當事人理應可以享有請求閱覽、製給複製本、請求補充或更正、停止蒐集處理利用， 以及請求刪除之權利，對於中輟生資料的使用，原則上亦應僅限於其蒐集目的範圍內；惟教育部中途輟學學生通報及復學輔導方案並未規定蒐集資料的保存使用期限，對於資料流向警方後的使用、管理亦未有所規定，對於個資保護尚難謂充分。

（二）學生綜合資料表[119]

學生綜合資料表係爲使教師有完整而正確的學生資料，以利日後教學、輔導學生之用，故於新生入學時，請新生填具 A 卡，包含以下項目：本人概況（身份證字號、生日、血型、住址、一般健康狀況、電話號碼…等）、家庭狀況（直系血親、家中排行、父母教育程度、父母職業…等）、學習狀況（如偏好科目、特殊專長、休閒興趣、智育成績…等）、畢業後計畫（如升學意願、將來職業志願…等）、生活適應

[119] 賴靜儀，從資訊自決權論學生資料保護，94 年國立臺灣師範大學公民教育與活動領導學系碩士論文，頁 143-150。

（如生活習慣、學習動機…等）、測驗紀錄（包括智力測驗、性向測驗、職業興趣測驗…等），以及其他資訊（如導師評語、留級及轉修復停升學異動紀錄…等）。

A 卡填畢後存放輔導處；B 卡則於每學期初發給學生填寫家庭狀況、自我認識、學習心得…等項目，並由導師、註冊組、生教組及資料組分別填寫導師評語、生活適應、重要輔導紀錄、成績考察紀錄、轉休復停學紀錄、獎懲紀錄、心理測驗紀錄..等項目，交由導師保管及登錄，學期結束時交回輔導處保管登錄檢閱。

除學生轉學者，學生綜合資料表以正本轉移外，其他如升學、就業時，學校僅會轉出 AB 兩表之影本，正本仍留存學校；依教育部之「學生綜合資料運用手冊」，正本應保存至少五年，含有學籍表之表格則應永久保存，並依班級裝訂成冊。

惟教師於學期中持有班上所有學生的 B 卡，對於教師保管 B 卡應注意之事項則未爲規定，是以教師只要於學期結束時交回輔導處即可，容易產生個資保護之漏洞。

（三）輔導紀錄[120]

輔導紀錄之做成目的，在於使輔導工作得以完整、順利進行，惟依「各級學校提供家庭教育諮商或輔導辦法」第 8 條規定，各級學校應將有重大違規事件或有特殊行爲之學生資料予以建檔，並記錄追蹤家長或監護人接受家庭教育諮商輔導情形，檔案資料並應妥善保管。

惟輔導紀錄雖由輔導處統一保管，對於保管之期限及其後的資料利用限制、是否銷毀…等事項則未有規定。

第三項　公務機關對各類就學資訊之管控與監督

依教育基本法第 9 條規定，教育事務原則上屬各地方政府之權限，中央

[120] 賴靜儀，從資訊自決權論學生資料保護，94 年國立臺灣師範大學公民教育與活動領導學系碩士論文，頁 163-166。

權限僅包含以下事項：一、教育制度之規劃設計；二、對地方教育事務之適法監督；三、執行全國性教育事務，並協調或協助各地方教育之發展；四、中央教育經費之分配與補助；五、設立並監督國立學校及其他教育機構；六、教育統計、評鑑與政策研究；七、促進教育事務之國際交流；八、依憲法規定對教育事業、教育工作者、少數民族及弱勢群體之教育事項，提供獎勵、扶助或促其發展。

關於學生就學資料之保障，應不屬於上述中央教育主管機關之權限，而屬各地方政府之權限；然則各地方政府對於學生就學資料之保障各有寬嚴不一之規定，或許由中央訂立一套最起碼的學生個人資料保護辦法，提供與地方政府參考，不失爲一種解決方式，如教育部編製的「學生綜合資料運用手冊」即爲許多學校制訂綜合資料表時的參考範本。

惟在決定公務機關對於就學資訊應採什麼樣的管控監督之前，必須先討論以下問題，即，學生的資訊權（包含資訊隱私及資訊自決）在學校中，是否因爲特別權力關係而受到限縮？如是，受限縮之界限爲何？

一、特別權力關係理論對於學生權利之已知影響

傳統特別權力關係是基於特別的法律原因，當事人之一方對於相對人在一定範圍內，有概括的命令強制之權利，相對人具有服從義務之法律關係；該法律關係爲具某種職務之人與國家統治權具有特別密切義務的特徵，例如公務員、軍人、學生及監獄受刑人，國家對於具有此等身分之人爲財產上或自由上的侵害，不僅不需有法律上的依據，一旦欲請求救濟，最多只能尋求內部申訴管道，而不能如一般人提起訴願或行政訴訟[121]。

惟經我國大法官數次做成解釋後，特別權力關係在我國已有鬆動，即便公務員、軍人、學生、受刑人等具特別身份者之基本權利仍應受憲法保障，如欲限制之，仍應受法律保留原則之拘束，對於權利之限制種類及程度，亦以使該特別權利機關達成必要任務爲限[122]。

[121] 法治斌，董保城，憲法新論，2004 年 10 月，台北：元照，頁 186。

[122] 法治斌，董保城，憲法新論，2004 年 10 月，台北：元照，頁 187。

首先，釋字第 380 號解釋先確認了「實質上發生限制學生畢業之效果」事項，應有法律保留原則之適用，揚棄了特別權力關係理論中，認爲無須以法律授權，即得以特別規則限制相對人自由權利之說法。

其次，釋字 382 號解釋鬆動了特別權力關係對於學生身份受剝奪時，所得採取救濟途徑的限制，認爲「對學生所爲退學或類此之處分行爲，足以改變其學生身分並損及其受教育之機會，自屬對人民憲法上受教育之權利有重大影響，此種處分行爲應爲訴願法及行政訴訟法上之行政處分。受處分之學生於用盡校內申訴途徑，未獲救濟者，自得依法提起訴願及行政訴訟。」

再者，釋字第 563 號解釋則進一步確認學生身份受到影響時，於窮盡校內申訴途徑後仍未獲得救濟者，仍可循訴願、行政訴訟之途徑請求救濟；惟釋字第 563 號解釋認爲「大學自治既受憲法制度性保障，則大學爲確保學位之授予具備一定之水準，自得於合理及必要之範圍內，訂定有關取得學位之資格條件」；如學生因不符取得學位之資格條件，自可依上述救濟途徑尋求救濟。

由上觀之，特別權利關係對於學生「身份關係」之限制已然鬆動，而有基本權利保障、法律保留原則之適用，並得爲訴願、行政訴訟，亦可聲請國家賠償；然而，除「身份關係」外，有關職務上之「經營管理關係」，只要在無礙身份關係之情況下，仍有特別權利關係之適用空間。

二、特別權力關係與學生資訊之蒐集、整理及利用

特別權力關係之鬆動已如前述，而學生資訊之蒐集、整理及利用與學生身份關係之得喪變更並無直接關係，應可認爲仍有特別權力關係之適用；惟於權利意識高漲之今日，如公務機關（如教育部）欲蒐集、處理、利用學生之個人資訊，是否可以逕依特別權力關係排除法律保留原則之適用，直接以命令爲學生個人資料之蒐集、處理及利用，尚非無疑。

毋寧認爲，公務機關欲蒐集、處理、利用學生個人資料時，原則上仍應依個資法之規定，此係因涉及學生基本權利之限制，仍應有法律依據[123]，惟基於學校與學生之間的營造物利用關係，學生對於其資訊權所享有之保障範

[123] 吳庚，行政法之理論與實用，2005 年 10 月，頁 222-223。

圍可能較爲限縮，不若個資法規定範圍爲廣。

三、個資法草案對於各類學生資訊蒐集、處理、利用之相關規定

（一）個資法草案對於公務機關蒐集、處理、利用一般個資之規範

1．蒐集

公務機關應有特定蒐集目的，並於執行法定職務必要範圍內、或經當事人書面同意、或對當事人權益無侵害時，始得蒐集處理個資（個資法草案第 15 條）；關於個資之利用，原則上亦以蒐集目的爲限，超出蒐集目的以外之利用，必須有下列情形之一始可：一、法律明文規定；二、爲維護國家安全或增進公共利益；三、爲免除當事人之生命、身體、自由或財產上之危險；四、爲防止他人權益之重大危害；五、公務機關或學術研究機構基於公共利益爲統計或學術研究而有必要；且資料經過處理後或依其揭露方式無從識別特定當事人；六、有利於當事人權益；七、經當事人書面同意（個資法草案第 16 條）。

公務機關於蒐集個資前，應向當事人爲下列事項之告知：一、公務機關或非公務機關名稱；二、蒐集之目的；三、個人資料之類別；四、個人資料利用之期間、地區、對象及方式；五、當事人依個資法第 3 條規定得行使之權利及方式；六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響（個資法草案第 8 條第 1 項）。

惟有下列情形之一者，公務機關得免爲上述事項之告知：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；五、當事人明知應告知之內容（個資法草案第 8 條第 2 項）。

2．處理或利用

公務機關處理或利用由他人提供之個資前，應向個資當事人爲下列事項告知：一、資料來源；二、公務機關或非公務機關名稱；三、蒐集之目的；四、個人資料之類別；五、個人資料利用之期間、地區、對象及方式；六、當事人依第三條規定得行使之權利及方式（個資法

草案第 9 條第 1 項）。

惟有下列情形之一者，公務機關得免爲上述事項之告知：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；五、當事人明知應告知之內容；六、當事人自行公開或其他已合法公開之個人資料；七、學術研究機構基於公共利益爲統計或學術研究之目的而有必要，且資料經處理後或依其揭露方式無從識別特定當事人；八、不能向當事人或其法定代理人爲告知；九、大眾傳播業者基於新聞報導之目的而蒐集個人資料（個資法草案第 9 條第 2 項）。

公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本（個資法草案第 10 條）。公務機關受理當事人上述之請求，應於 15 日內爲准駁之決定；必要時，得予延長，延長之期間不得逾 15 日，並應將其原因以書面通知請求人（個資法草案第 13 條）。查詢或請求閱覽個人資料或製給複製本者，公務機關得酌收必要成本費用（個資法草案第 14 條）。

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。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。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、停止處理或停止利用該個人資料。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。違法蒐集、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。因可歸責於公務機關之事由，未爲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（個資法草案第 11 條）。

3．保存

公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：一、個人資料檔案名稱。二、保有機關

名稱及聯絡方式。三、個人資料檔案保有之依據及特定目的。四、個人資料之類別（個資法草案第 17 條）。公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏（個資法草案第 18 條）。公務機關違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人（個資法草案第 12 條）。

4．小結

由上述個資法草案觀之，公務機關之行爲義務如下：

(1) 於蒐集個資階段應特定蒐集目的，並履行告知義務；

(2) 於處理及利用階段亦應履行告知義務，並應依當事人請求答覆查詢、提供閱覽、製給複製本，並應主動或依當事人請由爲資料之更正、補充、刪除、停止處理或停止利用，並於更正或補充後通知曾提供利用之對象[124]；

(3) 個資保存並應辦理安全維護，如因公務機關違反個資法草案之規定致個資外洩，公務機關應查明後通知當事人。

（二）個資法草案對於公務機關蒐集、處理、利用學生個資之規範

1．教務資訊

(1) 學籍資訊

如前所述，學籍資料之蒐集目的在於統整學生入學、輟學、復學、轉學、成績及學籍等資料，以便於管理，故於蒐集階段之

[124] 個資法草案第 11 條僅規定當個資有「更正」或「補充」時，始須通知曾提供利用之人個資已更正、補充；然而，公務機關依當事人請求，或公務機關主動刪除、停止處理或停止利用之情形，個資法草案反而未規定公務機關亦應通知曾提供利用之人該資料應刪除、停止處理或停止利用。

由於個資交付與公務機關以後，公務機關對於該個資有最密切之掌握，如當事人請求，或公務機關自行刪除、停止處理或停止利用時，公務機關應爲最有能力確保該個資徹底地被刪除、停止處理或利用之人，解釋上公務機關亦應負責通知曾提供利用之人，確保其確實刪除、停止處理或利用該個資。個資法草案就此雖未爲規定，但於解釋「刪除、停止處理或利用」時，應對之爲最廣義的解釋，亦即蒐集機關除了自行刪除、停止處理或利用外，亦應確保其他機關爲刪除、停止處理或利用。

目的已經特定;惟公務機關是否應爲個資法草案第 8 條第 1 項之告知,可能會因該資料之蒐集係出於公務機關執行法定職務所必要，而符合個資法草案第 8 條第 2 項免爲告知之要件。

於處理或利用階段,個資法並未要求公務機關另外再爲處理利用之告知,除非該資料並非由當事人提供,然學籍資料包含學生在校之學號、姓名、身份證字號、性別、出生年月日、出生地、學生身份別、家長姓名、家長和學生的關係、監護人電話、戶籍地址…等，多由個資當事人，亦即學生本人提供，故應無再告知之問題。

惟公務機關（尤其是學校）是否須依學生或其法定代理人之請求，爲資料之刪除、停止處理或利用，容有討論餘地，畢竟學校與學生之間涉及經營管理關係之事項,仍有特別權力關係之適用，個資法對於個人資訊權之保障可能因此有所限縮。

(2) 成績資訊

成績資訊應爲學生就學資訊當中，外洩誘因最強的資訊種類，觀諸近年社會上發生的數起學生就學資訊外洩案件，絕大部分皆爲成績外洩[125]；成績資訊之蒐集目的在於評量教學成效，應符合特定蒐集目的之要求，且蒐集成績資料係出於其法定職務之必要者，亦免爲個資法草案第 8 條第 1 項之告知。

於處理或利用階段，個資法並未要求公務機關另外再爲處理利用之告知，且學生成績即爲教師對學生學習成果之評量，難以想像存有第三人提供之可能，故應無處理、利用前再告知之問題。

惟公務機關（尤其是學校）是否須依學生或其法定代理人之

[125] 例如 2008 年發生的國中基測資料外洩事件，共有三種學生個資外洩之態樣：第一種，爲獲選爲基測電腦處理作業之博暐公司內部員工自內部電腦中下載考生資料,販售予補教業者；第二種，爲學校教職員自學校系統中竊取學生資料，販售予補教業者；第三種，則爲駭客入侵學校及大考中心網站，竊取資料後，再販售與補教業。

聯合報,《基測個資外洩案 竄改三推甄生成績 交換個資》,2008 年 6 月 26 日。資料來源：http://mag.udn.com/mag/campus/storypage.jsp?f_ART_ID=133171.（最後查閱日期：2009 年 6 月 30 日）

請求，爲成績資料之刪除、停止處理或利用，容有討論餘地，畢竟學校與學生之間涉及經營管理關係之事項，仍有特別權力關係之適用，個資法對於個人資訊權之保障可能因此有所限縮。

最爲重要的，係成績資訊保存管理之問題。個資法第 12 條及第 18 條雖然規定應由專人保管個資，如有違反個資法規定致個人資料外洩之情形並應查明後通知當事人，但是對於公務機關違反個資保存規定致學生個人資料外洩，個資法並未訂有相關處罰規定，僅能依刑法第 132 條公務員洩漏國防以外秘密罪論之。至於駭客入侵電腦竊取資料則僅能依刑法妨害電腦使用罪論之。

2．學務資訊

(1) 學生獎懲缺曠紀錄

學生獎懲缺曠紀錄主要目地在於管理學生出缺席情況，並紀錄學生特殊優良事蹟或應受責難之行爲，故於蒐集階段之目的已經特定；惟公務機關是否應爲個資法草案第 8 條第 1 項之告知，可能會因該資料之蒐集係出於公務機關執行法定職務所必要，而符合個資法草案第 8 條第 2 項免爲告知之要件。

於處理或利用階段，個資法並未要求公務機關另外再爲處理利用之告知，除非該資料係由第三人提供，然則出缺席紀錄係公務機關（尤其是校方）依據學生出席之事實所爲之紀錄，資訊之提供者並非學生亦非第三人，應無處理利用前再告知之問題。

惟公務機關（尤其是學校）是否須依學生或其法定代理人之請求，爲獎懲缺曠資料之刪除、停止處理或利用，容有討論餘地，畢竟學校與學生之間涉及經營管理關係之事項，仍有特別權力關係之適用，個資法對於個人資訊權之保障可能因此有所限縮。

(2) 學生健康檢查資料

健康檢查資料屬於應受特別保護之特種資訊，應將之劃歸醫療資訊範疇，適用較爲嚴格的個資保護規定。

3．輔導資訊

(1) 中輟生資料建檔

如前所述，中輟生資料庫建檔可能產生的種種問題，包括其建立可能超過母法授權範圍而有違反法律保留原則之虞；退一步言，縱不論資料庫之建立是否超過母法授權範圍，如認爲一定要建立全國性資料庫並與警政署連線，才有可能使得通報系統發揮其作用，則應取得法律位階之授權，而非僅以命令位階的輔導方案規定之。

對於中輟生資料的處理利用，亦應限於其原始蒐集目的；個資法草案雖然允許公務機關出於蒐集目的以外之目的使用個資，惟其條件過於寬鬆，例如「爲維護國家安全或增進公共利益」，實則只要公務機關想要爲蒐集目的以外之利用，都可循此解釋成「爲維護國家安全或增進公共利益」；故如國民中小學中途輟學學生通報及復學輔導辦法或其他相關辦法並未就警政署使用中輟生資料庫爲一定限制或管理，則對於中輟生個資保護尚難謂充分。

(2) 學生綜合資料表

學生綜合資料表之蒐集目的在於使教師有完整而正確的學生資料，以利日後教學、輔導學生之用，應符合特定蒐集目的之要求，且蒐集成績資料係出於其法定職務之必要者，亦免爲個資法草案第 8 條第 1 項之告知。

於處理或利用階段，個資法並未要求公務機關另外再爲處理利用之告知，除非該資料並非由當事人提供，然學生綜合資料表係由學生本人填寫，難以想像由第三人提供之情形，本應無處理利用前再告知之問題，惟學生綜合資料表之內容有部分甚涉及學生家屬，例如父母教育程度、父母職業、家庭經濟狀況…等，並非全都是僅與學生本人有關之資料，是以要對學生綜合資料表爲處理或利用前，是否應再告知當事人或其親屬，應視處理或利用之實質內容而定，斷無法以特別權力關係限制個資法在此部分之保障。

至於公務機關（尤其是學校）是否須依學生或其法定代理人之請求，爲資料之刪除、停止處理或利用，容有討論餘地，應視請求刪除、停止使用或利用之資料具體內容爲何；雖然學校與學生之間涉及經營管理關係之事項，仍有特別權力關係之適用，個資法對於個人資訊權之保障可能因此有所限縮，但是學生綜合資料表裡有部分資訊實爲他人資訊，如父母生日、年齡、職業、教育程度、家庭經濟狀況…等，特別權力關係能否限縮非專屬學生之個人資訊保障，尚非無疑。

(3) 輔導紀錄

輔導紀錄之做成目的，在於使輔導工作得以完整、順利進行，應符合特定蒐集目的之要求，且蒐集成績資料係出於其法定職務之必要者，亦免爲個資法草案第 8 條第 1 項之告知。

於處理或利用階段，個資法並未要求公務機關另外再爲處理利用之告知，除非該資料並非由當事人提供，惟學生輔導紀錄應爲學生與輔導老師共同完成，如同病歷係由病人提供病徵資訊，而藉由醫生專業知識所做成之診療紀錄，學生的輔導紀錄亦係由學生提供心理狀態之描述，而由輔導老師共同做成之紀錄，故應可認該資料部分係由當事人提供。爲如欲就輔導資料爲處理、利用，應視處理利用者爲誰、爲如何之處理利用而定，蓋因輔導紀錄可能涉及學生較爲私隱之事項，比起獎懲缺曠、成績資料更貼近人格權之核心，所受之保障密度不應與其他就學資料等同視之。

至於公務機關（尤其是學校）是否須依學生或其法定代理人之請求，爲資料之刪除、停止處理或利用，容有討論餘地，應視請求刪除、停止使用或利用之資料具體內容爲何；原本學校與學生之間涉及經營管理關係之事項，仍有特別權力關係之適用，個資法對於個人資訊權之保障可能因此有所限縮，但是如前所述，輔導資料可能較其他就學資訊更貼近人格權之核心，斷難僅因特別權力關係使個資法在此部分的保障受到限縮。

第四項 本案評析

一、醫學系實習生強制篩檢愛滋案

首先，按醫師法之規定，醫學系科[126]、中醫學系[127]、以及牙醫學系科[128]畢業實習期滿成績及格，領有畢業證書者，得應醫師、中醫師及牙醫師考試，且經醫師考試及格並依醫師法領有醫師證書者，得充醫師[129]。又於實習階段，實習醫生依照實習醫師實施制度要點[130]須至醫療機構，於醫師指導下執行醫

[126] 醫師法第 2 條：「具有下列資格之一者，得應醫師考試：一、公立或立案之私立大學、獨立學院或符合教育部採認規定之國外大學、獨立學院醫學系、科畢業，並經實習期滿成績及格，領有畢業證書者。二、八十四學年度以前入學之私立獨立學院七年制中醫學系畢業，經修習醫學必要課程及實習期滿成績及格，得有證明文件，且經中醫師考試及格，領有中醫師證書者。三、中醫學系選醫學系雙主修畢業，並經實習期滿成績及格，領有畢業證書，且經中醫師考試及格，領有中醫師證書者。前項第三款中醫學系選醫學系雙主修，除九十一學年度以前入學者外，其人數連同醫學系人數，不得超過教育部核定該校醫學生得招收人數。」

[127] 醫師法第 3 條：「具有下列資格之一者，得應中醫師考試：一、公立或立案之私立大學、獨立學院或符合教育部採認規定之國外大學、獨立學院中醫學系畢業，並經實習期滿成績及格，領有畢業證書者。二、本法修正施行前，經公立或立案之私立大學、獨立學院醫學系、科畢業，並修習中醫必要課程，得有證明文件，且經醫師考試及格，領有醫師證書者。三、醫學系選中醫學系雙主修畢業，並經實習期滿成績及格，領有畢業證書，且經醫師考試及格，領有醫師證書者。前項第三款醫學系選中醫學系雙主修，其人數連同中醫學系人數，不得超過教育部核定該校中醫學生得招收人數。經中醫師檢定考試及格者，限於中華民國一百年以前，得應中醫師特種考試。已領有僑中字中醫師證書者，應於中華民國九十四年十二月三十一日前經中醫師檢覈筆試及格，取得台中字中醫師證書，始得回國執業。」

[128] 醫師法第 4 條：「公立或立案之私立大學、獨立學院或符合教育部採認規定之國外大學、獨立學院牙醫學系、科畢業，並經實習期滿成績及格，領有畢業證書者，得應牙醫師考試。」

[129] 醫師法第 1 條：「中華民國人民經醫師考試及格並依本法領有醫師證書者，得充醫師。」

[130] 中華民國 93 年 9 月 9 日衛署醫字第 0930216396 號公告修正實習醫師制度實施要點：「一、為健全實習醫師制度，特訂定本要點。二、本要點所稱之實習醫師，係指公立或立案之私立大學、獨立學院或符合教育部採認規定之國外大學、獨立學院醫學系、中醫學系、牙醫學系畢業，並經實習期滿成績及格，領有畢業證書，繼續從事實習者。三、實習醫師得在下列醫療機構，於醫師指導下執行醫療業務：(1) 經醫院評鑑合格之醫院。(2) 經中醫醫院暨醫院附設中醫部門訪查合格之醫院。(3) 設有牙醫部門之醫院或經中央主管機關指定之牙醫診所。前項第三款所稱指定之牙醫診所，於中央主管機關未辦理指定前，各牙醫診所均視為指定之牙醫診所。四、醫院聘用實習醫師，以不超過醫院該類醫師員額之三分之一為限。五、實習醫師之實習期間，以取得畢業證書之日起六年為限。本要點於九十三年九月九日修正公告前，已於醫療機構擔任實習醫師者，前項實習年限以自本要點九十三年九月九日修正公告日起算。」

療業務，並經實習期滿成績及格，領有畢業證書，繼續從事實習者。是故，醫學系科、中醫學系、及牙醫學系科之學生，必須進行各系科所要求之實習課程，於實習期滿成績及格，領有畢業證書後，方得應試而領有醫師執照。該等實習課程爲 醫學系科、中醫學系、及牙醫學系科之學生欲畢業得應試資格之必修課程，因此，醫院、學校、或實習機構拒絕實習生之實習課程，將使該實習生無法完成必修課程，無法領取畢業證書，而不得參加醫師考試，取得醫師證書，故若醫院、學校、或實習機構在無法律明文規定下限制實習生之實習課程，將侵害各醫學系院學生之受教權。

然而，在本案例中關於個人資料之保護議題，即是醫院、學校、或實習機構得否因實習之課程特殊性（例如侵入性之醫療行爲等），而在病患受愛滋病感染的風險評估上，強制要求實習生必須接受愛滋病篩檢，將有感染或疑似感染愛滋病之實習生排除在實習課程外。

按個資法第 3 條第 7 款規定，學校或醫院該等實習機構屬於個資法定義下的非公務機關，又按個資法第 3 條第 1 款之規定，關於健康及病歷情況等均屬個人資料而受個資法規定之保障，因此，實習機構欲蒐集、處理或利用實習生之病歷或健康資料，必須符合個資法第 18 條[131]規定。惟該資料之蒐集或電腦處理，似乎難以符合個資法第 18 條各款情形所要求者，實習機構採取強制篩檢之手段，並非經當事人書面同意，或與當事人有契約或類似契約之關係、該等資料並非已公開之資料、亦非爲了學術研究，於此皆不符合個資法第 18 條第 1 款至第 4 款之規定，然而，依個資法第 18 條第 5 款之規定，實習機構得否以此作爲強制篩檢的合法性基礎，有所疑問。依照行政院衛生署疾病管制局衛署疾管愛字第 0960007798 號函文意旨指出,所有醫事相關人員(包括醫學院實習學生)，非法規中規範應接受人類免疫缺乏病毒檢查之對象，故醫學院校及實習醫院不得要求實學生進行愛滋病毒篩檢及提出相關檢驗證明[132]。又依各級學校防治後天免疫缺乏症候群處理要點第 7 點第 2 項規

[131] 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，不得爲之：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、爲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。」

[132] 行政院衛生署疾病管制局衛署疾管愛字第 0960007798 號函討論事項第 1 點決議：「1. 依據後天免疫缺乏症候群防治條例第 6-1 條及第 8 條、衛生署 93 年 4 月 16 日行政院衛生署署

定，學校不得藉由任何名義，要求當事人提出未感染人類免疫缺乏病毒之證明[133]。

參照上文意旨，醫院、學校或實習機構皆不得以任何理由要求實習生進行愛滋病毒篩檢或提出相關檢驗證明，是故，實習機構不得依個資法第 18 條第 5 款規定，要求實習生進行強制愛滋篩檢，否則將侵害實習生對自我資訊隱私權及資訊自主控制權。

就強制篩檢愛滋一案而言，係就當事人之健康狀況、醫療等方面之個人資料進行蒐集、處理或利用，該等個人資料較具有敏感性質，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。有鑑於此，草案認爲個人資料中有部分資料性質較爲特殊或具敏感性者，其蒐集、處理或利用應較一般個人資料更爲嚴格，故於草案第 6 條[134]修正其蒐集、處理或利用之要件，以加強保護個人之隱私權[135]。故就草案第 6 條各款以觀，實習機構強制對實習生進行愛滋篩檢，並非依法律明文規定、法律未明文禁止且經當事人書面同意、履行法定義務、當事人自行公開或已合法公開之個人資料、亦非基於醫療、衛生或犯罪預防目的，爲統計或學術研究而有必要等之情形，皆不符合草案第 6 條所列各款之情形，故實習機構不得對實習生進行強制篩檢愛滋。然草案對於特種資料蒐集、處理、利用之除外條款規定的仍

授字第 0930000341 號公告及各級學校防治後天免疫缺乏症候群處理要點，感染人類免疫缺乏病毒者之人格與合法權益應受尊重及保障，不得予以歧視，拒絕其就學、就醫、就業或予其他不公平之待遇。所有醫事相關人員(包括醫學院實習學生)，非法規中規範應接受人類免疫缺乏病毒檢查之對象，故醫學院校及實習醫院不得要求實學生進行愛滋病毒篩檢及提出相關檢驗證明。2. 建議醫學院校於醫學教育中加強愛滋病防治及感染愛滋病毒對後續執業之影響等知識，並建立相關諮商管道。」

[133] 各級學校防治後天免疫缺乏症候群處理要點，93 年 12 月 9 日台體字第 0930166116 號函。

[134] 草案第 6 條：「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。但有下列情形之一者，不在此限：一、法律明文規定。二、法律未明文禁止蒐集、處理或利用，且經當事人書面同意。三、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。四、當事人自行公開或其他已合法公開之個人資料。五、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，爲統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從識別特定當事人。」

[135] 草案第 6 條第 2 點說明：「按個人資料中有部分資料性質較爲特殊或具敏感性，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。是以，一九九五年歐盟資料保護指令(95/46/EC)、德國聯邦個人資料保護法第十三條及奧地利聯邦個人資料保護法等外國立法例，均有特種（敏感）資料不得任意蒐集、處理或利用之規定。經審酌我國國情與民眾之認知，爰規定有關醫療、基因、性生活、健康檢查及犯罪前科等五類個人資料，其蒐集、處理或利用應較一般個人資料更爲嚴格，須符合所列要件，始得爲之，以加強保護個人之隱私權益。又所稱「性生活」包括性取向等相關事項，併予敘明。」

過於寬鬆，當事人同意之要件僅列於其中一款，誤解「告知後同意」與其他事由應爲「聯立」而非「擇一」關係，僅因法律規定、法定職務或有研究需要，即不須取得當事人同意而得蒐集、處理、利用個人資料，無異將當事人之資訊自決權架空，保障資訊自決權恐將形同具文。

此外，一旦實習生拒絕接受愛滋檢測，實習機構或是學校得否以病患受感染之風險爲由，而排除學生有選取實習課程之機會。如此一來，學生因無法實習期滿而領有畢業證書，進而參加國家考試成爲醫師，對學生之受教權亦有所影響。在此方面，對於實習課程的改變以及調整，例如侵入性醫療課程僅觀摩不動手等，將學生之職務改變爲非侵入性醫療的職務，例如放射科、病理解剖及檢查、衛教行政工作等，以降低病患受感染之風險，實習課程之調整空間甚大，實非能僅因單純以病患有受感染愛滋之風險逕行對學生強制篩檢愛滋或排除學生實習之機會，如有此情形發生，學生僅能事後對醫院、學校或實習機構請求損害賠償，在事前個人資料已遭蒐集、處理或利用，因此受有歧視之對待或其他權益之損害，將形成難以彌補之損害，此等皆與個資法保障人格權之規範、憲法保障人民之資訊隱私權、資訊自主控制權、以及受教權等皆有違背，造成當事人權益損害難以估計及難以彌補。

二、基測個資外洩案

按個資法第 3 條第 6 款規定：「公務機關：指依法行使公權力之中央或地方機關。」、個資法草案第 2 條第 7 款規定：「公務機關：指依法行使公權力之中央或地方機關或行政法人。」、行政程序法第 2 條第 3 款規定：「受託行使公權力之個人或團體，於委託範圍內，視爲行政機關。」，是故，依上開法條規定，博暐公司受教育部委託依法辦理國中基本學力測驗電腦處理作業程序，既屬於行政程序法規定之行政機關，亦應屬於個資法下之公務機關，適用個資法上公務機關之資料處理，合先敘明。

本案中，博暐公司利用受教育部委託依法辦理國中基測電腦處理作業之機會，販售考生個資及成績等情，涉及違反個資法中保護個人隱私權及資訊自決權。學生因就學而產生之就學資料，主要係「學籍管理資料」與「學期成績管理資料」兩項，而學籍資料包含學生之姓名、出生年月日、身分證統

一編號等，學期成績管理資料則包含學生姓名、各科成績以及排名等等，皆應屬於個資法第 3 條第 1 款所稱之個人資料。又，教育部辦理國中基本學力測驗係依高中及高職多元入學方案、教育基本法第 9 條[136]、高級中學法第 3 條[137]及職業學校法第 4 條[138]之規定承辦，屬個資法第 7 條規定公務機關對個人資料之蒐集或電腦處理係於法令規定職掌必要範圍內者，故博暐公司受教育部委託辦理國中基本學力測驗電腦處理作業程序，亦屬於依法令職掌必要範圍內對個人資料之蒐集或電腦處理，符合個資法第 7 條之規定。是以，博暐公司取得考生之姓名、出生年月日、身分證統一編號、各科考試成績以及排名等等，均屬對個人資料之合法蒐集與處理。

按「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用：一、法令明文規定者。二、有正當理由而僅供內部使用者。三、為維護國家安全者。四、為增進公共利益者。五、為免除當事人之生命、身體、自由或財產上之急迫危險者。六、為防止他人權益之重大危害而有必要者。七、為學術研究而有必要且無害於當事人之重大利益者。八、有利於當事人權益者。九、當事人書面同意者。」、「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。」個資法第 8 條、第 17 條分別定有明文。是故，博暐公司既合法取得考生之個

[136] 教育基本法第 9 條：「中央政府之教育權限如下：一、教育制度之規劃設計。二、對地方教育事務之適法監督。三、執行全國性教育事務，並協調或協助各地方教育之發展。四、中央教育經費之分配與補助。五、設立並監督國立學校及其他教育機構。六、教育統計、評鑑與政策研究。

七、促進教育事務之國際交流。八、依憲法規定對教育事業、教育工作者、少數民族及弱勢群體之教育事項，提供獎勵、扶助或促其發展。前項列舉以外之教育事項，除法律另有規定外，其權限歸屬地方。」

[137] 高級中學法第 3 條：「高級中學入學資格，須具有國民中學畢業或同等學力者，經入學考試、推薦甄選、登記、直升、保送、申請或分發等方式入學。高級中學修業年限以三年為原則。第一項同等學力之標準，由中央主管教育行政機關定之；高級中學多元入學之各項辦法，由各級主管教育行政機關定之。」

[138] 職業學校法第 4 條：「職業學校學生入學資格，須具有國民中學畢業或同等學力者，其同等學力之標準，由教育部定之。職業學校應以多元方式辦理招生；其多元入學招生方式、實施區域、範圍、方法、招生對象、辦理時間、組織分工、名額比例及其他應遵行事項之辦法，由教育部定之。職業學校修業年限以三年為原則。性質特殊之類科，有增減修業年限之必要者，得由各該主管教育行政機關報請教育部核定之。職業學校應考查學生學業成績，學生學業成績優異者，得縮短其修業年限半年至一年；未在修業期限修滿應修學分者，得延長其修業年限二年。學生成績考查項目、方式、基準及其他相關事項之辦法，由教育部定之。」

人資料及成績排名等，在利用、處理、維護及監督方面，自應依上述個資法為之。然而，博暐公司竟為圖利，將 97 年度第一次國中基測考生個資及成績外洩，販賣給中南部 10 多家補教業者，並提供給 7 所私立高中作為招生之用，顯然已違反最初蒐集之目的以及為非法之目的外利用，並且，無視辦理安全維護事項，故意將個人資料洩漏，嚴重違反個資法之規定，侵害個人隱私權及資訊自決權甚鉅。

博暐公司上開違法行為，依個資法第 33 條至第 41 條規定，其相關違法之人最高可處以處三年以下有期徒刑、拘役或科新臺幣五萬元以下罰金，且其係屬於受託行使公權力之行政機關，為職務上之公務員，可加重其刑至二分之一。此外，遭公佈個人資料之學生，得以個資法第 4 章規定，請求賠償損害。按「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」、「損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。」個資法第 27 條、第 30 條分別定有明文。因此，揆諸上開說明，遭販售個人資料之考生得依上述規定，依國家賠償法規定向博暐公司及教育部請求損害賠償，以維個人權益之保障。惟依個資法第 5 條及其施行細則第 11 條第 2 項規定，博暐公司視同委託機關(按應為國立桃園高中)之人，當事人行使個資法之權利，仍應向國立桃園高中為之。

誠如前述，在保障人格權之議題下，維護人性尊嚴與尊重人格自由發展，乃自由民主憲政之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為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，隱私權乃為不可或缺之基本權利，而受

憲法第 22 條所保障[139]。個資法及草案係爲規範處理個人資料時，以避免人格權受侵害，並促進個人資料之合理利用之下而制定，對於人格權之保障與促進個人資料合理利用常會造成拉扯之局面，如何從中獲得平衡，並兼顧二者之目的，即爲個資法及草案最重要的核心重點。

[139] 歷見大法官釋字第 603 號解釋、第 585 號解釋。

第五章　非公務機關對於金融、電信、網路購物與消費隱私之保障

第一節 網路金融對個人資料之蒐集、處理、利用及保全

第一項　金融業之定義與範圍

依金融機構合併法之定義（第四條第一項），金融機構係指下列銀行業、證券及期貨業、保險業所包括之機構，及其他經主管機關核定之機構：[140](1)銀行業：包括銀行、信用合作社、農會信用部、票券金融公司、信用卡業務機構及郵政儲金匯業局。(2)證券業及期貨業：包括證券商、證券投資信託事業、證券投資顧問事業、證券金融事業、期貨商、槓桿交易商、期貨信託事業、期貨經理事業及期貨顧問事業。(3)保險業：包括保險公司及保險合作社。(4)信託業等。現行電腦處理個人資料保護法第三條第七項所指之非公務機關乃限定（一）徵信業及以蒐集或電腦處理個人資料爲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。而個資法草案則傾向普遍適用，刪除非公務機關八大行業別之限制，即任何自然人、法人或其他團體，除爲單純個人或家庭活動之目的，而蒐集、處理或利用個人資料外，皆須適用本法。（修正草案條文第 2 條第 8 款、第 50 條第 1 項），因此，由上述個資法所規定適用主體的定義觀之，涉及個人資料之金融機構，包含銀行、證券、保險及信託業，均應依法蒐集所需客戶資料。本研究之範圍將以銀行業爲主要範圍。

目前我國銀行享有金流處理機制中的特許地位[141]，且銀行法第二十九條

[140] 另依金融業申請電腦處理個人資料登記程序許可要件及收費標準第二條，該標準所稱之金融業，係指本國銀行、信託投資公司、外國銀行在台分行、票券金融公司、信用合作社、農會信用部、漁會信用部及其他經金融目的事業主管機關許可或核准設立之法人及團體。同法第三條規定，金融業申請爲個人資料之蒐集、電腦處理或國際傳遞及利用，應依本法第十九條及第二十條之規定，填具申請書向財政部辦理登記。以蒐集或電腦處理個人資料爲主要業務之金融業，爲前項之申請時並應經財政部之許可。

[141] 觀之銀行法第二十九條即規定非銀行不得經營收受存款、受託經理信託資金、公眾財產

第二項針對經營銀行間資金移轉帳務清算之「金融資訊服務事業」[142]亦須經主管機關許可，顯見金融業仍屬高度管制產業。至於網路銀行究竟要不要劃爲受高度管制的獨佔事業而受管制？從我國網路銀行的發展觀之，各家金融機構架設網路銀行的目的不外乎在微利時代如何加強競爭、提高利潤等考量，皆以原有實體銀行組織架構之思考擴展經營、服務業務通路，與國外單純以完全虛擬、無實體型態出現的網路銀行基本考量多所差異，故我國網路銀行業務開展可視爲乃以傳統銀行經營業務的另一型態，主管機關業納原先實體金融業高度管制的規範體系管理之。

第二項　金融業對個人資料的蒐集、處理、利用及保全

爲規範金融控股公司與其子公司及各子公司間進行業務或交易行爲、共同業務推廣、資訊交互運用或共用營業設備或場所之方式，並確保客戶權益，特依據金融控股公司法第四十三條第二項之規定，訂定「金融控股公司及其子公司自律規範（以下簡稱「自律規範」）」。（自律規範第一條）

一、蒐集：內容及程序

金融機構蒐集他人之資料，來自於與該金融機構往來的客戶，或客戶使用由該金融機構提供之服務或自各項行銷活動所取得的資料，或依相關法規，或他人自己公開之資料中獲得。客戶資料之分類，依自律規範第二條規定，包括基本資料(包括姓名、出生年月日、身份證統一編號、電話及地址等資料)、帳務資料(包括帳戶號碼或類似功能號碼、信用卡帳號、存款帳號、交易帳戶號碼、存借款及其他往來交易資料及財務情況等資料)、信用資料(包括退票記錄、註銷記錄、拒絕往來記錄及業務經營狀況等資料)、投資資料(包括投資或出售投資之標的、金額及時間等資料)、保險資料(包括投保保險種類、年期、保額、繳費方式、理賠狀況及拒保紀錄等相關資料)等。但各子公司可依其業務特性，增刪上述資料之分類與內容。

或辦理國內外匯兌業務。倘違反非銀行收受存款的限制，依同法第一百二十五條規定對其違反專業經營行爲處以刑罰併科罰金。足以得窺所謂高度管制之立論。

[142] 參照財政部 90/09/28 台財融(二)字第 0090719310 號令訂定之「銀行間資金移轉帳務清算之金融資訊服務事業許可及管理辦法」。

二、使用

爲提供客戶完整、便利及更多元的金融商品及服務，金融機構於法令允許之範圍內，得運用客戶之資料進行共同行銷活動。共同行銷，指同一金融控股公司之各子公司間，爲共同業務推廣行爲、共同使用客戶資料、共用營業設備、場所及人員或提供跨業之綜合性金融商品或服務。（自律規範第二條第一項）金融控股公司及其子公司應將所爲共同行銷行爲應遵守之規範，列入內部控制與內部稽核項目。（自律規範第九條）

三、揭露

金融控股公司與其子公司及各子公司間（自律規範第五條）、金融控股公司及其子公司與其他第三人（自律規範第六條）進行共同行銷，於揭露、轉介或交互運用客戶資料時，應依照下列規定辦理：

（一）、 符合法令或主管機關之規定者。

（二）、 經客戶簽訂契約或書面同意者。

（三）、 本規範第七條至第九條規定之事項。

依前項揭露、轉介或交互運用客戶資料，不得有損害客戶權益之情事。

除法令另有規定、經客戶簽訂契約或書面明示同意者外，揭露、轉介或交互運用之客戶資料不得含有客戶基本資料以外之帳務、信用、投資或保險資料。

因此，客戶資料之揭露、轉介及交互運用，均應依照相關法令辦理，除於該公司暨其各子公司及經客戶同意之第三人間進行揭露、轉介及交互運用外，不得向任何其他第三人爲之。

另自律規範第七條規定，金融控股公司與其子公司及各子公司間相互揭露客戶資料，或揭露客戶資料予其他第三人時，應訂定保密協定，並維護客戶資料之機密性或限制其用途。收受並運用資料之機構不得再向其他第三人揭露該等資料。資料係屬於可公開取得且無害於客戶之重大利益者，則不受前項之限制。

四、保存

依自律規範第八條，金融控股公司及其子公司除法令另有規定外，應向客戶揭露保密措施，該措施應包含下列內容：

（一）、 資料蒐集方式：金融控股公司之子公司取得客戶資料之方式。

（二）、 資料儲存及保管方式：金融控股公司之子公司取得客戶資料後，如何保存該等資料。

（三）、 資料安全及保護方法：金融控股公司之子公司有關資訊防火牆之建置方式及效果。

（四）、 資料分類、利用範圍及項目：依照本規範第二條第一項第二款之分類，揭露欲使用之資料性質及項目。

（五）、 資料利用目的：依照資料分類，說明對於不同性質資料使用之意圖。

（六）、 資料揭露對象：依照資料分類，說明對於不同性質資料揭露之對象。

（七）、 客戶資料變更修改方式：客戶有更改資料之需求，提供客戶修改之申請途徑。

（八）、 行使退出選擇權方式：金融控股公司及其子公司依照本規範第六條、第十一條所爲之行爲，客戶得通知金融控股公司或其子公司停止對其相關之資訊交互運用及共同業務推廣行爲。行使方式應於保密措施中揭露。揭露保密措施及其修訂內容應以書面或電子郵件方式通知客戶，另採公司網頁、營業處所內明顯位置張貼公告、大眾媒體公告或其他足以由主管機關認定爲已公開揭露之方式辦理。包括:

1、 資料儲存及保管方式

金融控股公司及所屬子公司取得客戶資料後，將依相關作業規範建 檔並儲存於資料庫，同時嚴格控管客戶資料之存取，任何未經該公

司及所屬子公司正式授權之人員不得蒐集、使用或保管客戶的資料。

2、 資料之安全及保護方法

自律規範第十六條規定，爲確保屬於客戶資料之安全及避免因不當運用而損害客戶之權益，金融控股公司之子公司應建立客戶資料庫，妥善儲存、保管及管理客戶相關資料，並建立該客戶資料庫之安全措施，僅被授權員工始可使用客戶資料。金融控股公司及所屬各子公司將採嚴格措施保護客戶資料，並遵照政府相關法令及資訊管理原則，置有嚴密之防火牆及防毒系統以防止不法侵入及惡意程式之破壞。資料之傳輸，除以安全加密的方式加以保護外，並依相關資料檔案管理措施保護資料安全[143]。

3、 資料變更修改方式

爲確保客戶資料之正確性及完整性，客戶資料如有變更，除契約或法令另有規定得以電子傳輸或電話方式通知外，應隨時以書面通知該公司所屬各子公司修改。

4、 客戶資料退出之選擇

自律規範第十一條規定，金融控股公司或其子公司於使用客戶資料從事共同業務推廣行爲時，應於接獲客戶通知停止使用其資料後，立即依其通知辦理。

客戶直接以電話或書面通知金融控股公司及所屬各子公司停止對其相關資料交互運用及共同業務推廣，該公司及所屬子公司將於接獲通知後立即依客戶之指示辦理，停止使用客戶資料之生效日爲接獲客戶通知後第五個營業日起生效。

[143] 根據美國聖地牙哥防詐欺組織－身份盜竊資源中心（Identity Theft Resource Center）統計，今(2008)年惡意攻擊是導致資料外洩的首要原因，近 13%是由於駭客入侵，15.6%是員工堅守自盜，21%是儲存有消費者資料的筆記型電腦或其它儲存媒體遺失，14%是意外公佈或傳播消費者數據，11%是由於包商失誤造成的。大紀元，美個資外洩嚴重 去年 1.2 億人身分被盜，2008/8/29，http://www.epochtimes.com/b5/8/8/29/n2244755.htm （last visited on 2009.6.30）

惟金融控股公司法部分條文修正案已於 2009 年 1 月 21 日經總統明令公布。本次修正包括原第四三條有關「共同業務推廣不得損害客戶權益」之規定。2005 年 1 月 1 日前除自律規範之限制外，金融控股公司子公司間之共同行銷行爲，未有限制，且得不事先許可，僅以備查方式即可[144]。2005 年 1 月 1 日後，金管會於「金融控股公司之子公司進行共同行銷時應遵循之相關規範」第一項規定，「子公司間進行跨業行銷之申請，由金融控股公司代爲向本會提出，並依所申請專業櫃檯之性質同時副知本會證券期貨局、保險局」[145]，但其究竟是否爲核准制，用語不甚明確。此次修正後之新法則限縮此一寬鬆規定而於第四三條第一項明文規定此一行爲「應由金融控股公司事先向主管機關申請核准」[146]。另前述有關舊法時期關於共同業務推廣及資訊交互運用等行爲委由自律規範訂定之規定亦遭刪除，取而代之者，關於此類行爲及其他應遵循事項之辦法，均由主管機關定之[147]，將原本自律規範之內容，均由法律或命令定之，以彌補其法位階之不足[148]。

另有關共同使用客戶資料一節，新法第四三條增列第二項明文定之[149]，即於共同使用客戶資料時，除個人基本資料外，應先經客戶書面同意，始得使用其往來交易資料及其他相關資料，且不得爲使用目的範圍外之蒐集或利用；一經客戶通知不得繼續共同使用時，應即停止共同使用[150]。

---

[144] 依財政部 91 年 3 月 11 日台財證字第 001539 號函，金融控股公司「子公司間進行跨業行銷之申請，由金融控股公司提出，並由本部以單一窗口方式受理，金融控股公司並應同時副知各業別之主管機關;該案件之核准採備查制，由原核准設立金融控股公司之主管機關負責辦理，准予備查時並副知他業主管機關」。

[145] 行政院金融監督管理委員會 95 年 11 月 19 日金管銀(六)字第 0936000587 號令。

[146] 新法第 43 條規定第 1 項：「金融控股公司之子公司進行共同行銷，應由金融控股公司事先向主管機關申請核准，且不得有損害其客戶權益之行爲。」

[147]新法第 43 條規定第 3 項：「依第一項規定申請核准應具備之條件、應檢附之書件、申請程序、可從事之業務範圍、資訊交互運用、共同設備、場所或人員之管理及其他應遵循事項之辦法，由主管機關定之。」

[148] 有論者以爲，凡事以法令規定，於金融業或消費者，均爲必有利．於核准制下，將申請核准之要件與程序及揭露之要求與應揭露事項以法令訂之即爲已足，他事項如共同行銷之行爲準則之訂定，仍保留予自律規範，而藉因資訊透明所促成之市場紀律強化，自然形成自律監督爲宜．參見張冠群，二ＯＯ九年一月金融控股公司法關於共同行銷及關係人交易與風險集中揭露之修正條文評析，月旦法學雜誌 (No. 168) 2009.5 頁 200.

[149] 本項修訂理由係參考美國聯邦準備理事會規則 P(Regulation P)之立法例，採客戶選擇退出(Opt-out)機制。詳見本章後述討論。

[150] 有關違反本項規定之罰則，請參見新法第 60 條。

第三項　對個人金融資料的蒐集、處理、利用及保全之美國立法例

一、金融服務業現代化法案 (Gramm-Leach-Bliley Financial Services Modernization Act of 1999, GLBA)

美國金融服務現代化法案，15 U.S.C. §6801~6809爲金融資訊與消費者保護重心，限制金融機構揭露客戶非公開的資訊 (discourse on nonpublic personal information) 予非分支機構之第三人 (nonaffiliated third parties) ，且要求金融機構對其所有客戶揭露該機構與分支機構與非分支機構之第三人資訊分享的隱私權政策與方法。[151]對非公開的個人資訊之保護，每個金融機構負有明確和長期尊重客戶隱私的義務，並保護客戶之非公開個人資訊的安全性和機密性。其中包含[152]

1. 告知 (Notice and Disclosure)

當金融機構與其消費者建立關係，在此關係存續期間，金融機構須每年以書面或電子檔的形式，清楚而明確地告知消費者有關其向相關和非相關第三人揭露非公開個人資訊的具體政策和實行。

2. 選擇(Choice)

消費者有選擇拒絕金融機構將其非公開個人資訊與非關聯協力廠商共用的權力,或拒絕部分非公開個人資訊與關聯機構共用,且消費者應得到金融機構關於如何行使這項選擇權的說明。

3. 安全(Security)

金融機構必須提高警惕,保證客戶資訊和記錄的安全和秘密性,防範那些可以預見的針對記錄的安全和完整性的威脅和危害，防止那些會對消費者產生實質損害和不便的未經授權而獲取、使用此類記錄的違法行爲。

4. 履行(Enforcement)

15 U.S.C. §6805爲履行法律, GLBA規定聯邦貿易委員會(FTC)等8個政府機構有執法權,這些政府機構按照各自的職能進行執法活動,頒佈規則和指

[151] 參考：電子金融服務與付款機制電子化管理規範研究，頁 140。

[152] See 15 U.S.C. §§6801-6805.

引。GLBA 規定了隱私保護的最低水準,但它並不排除各州對金融隱私進行更高水準保護的立法。實際上，已有一些州對金融機構與非關聯第三方共用資訊採用選入(opt in) 標準。

二、金融消費者資訊隱私權法 Regulation P- Privacy of consumer financial information

消費者金融資訊隱私權法[153]，在GLBA 授權下由美國之金融機構監理部會組成聯合工作小組制訂，將GLBA 之規範落實爲具體措施。立法目的乃要求金融機構提供消費者有關隱私權政策與執行資訊，描述金融機構在什麼情況下可以揭露客戶非公開的個人資料給非分支機構的第三人，以及提供消費者避免金融機構揭露其相關資訊的選擇權(opting out)措施。[154]

金融機構[155]必須提供清楚、明確反應其隱私權政策與執行的初次告知給將成爲金融機構顧客的個人以及消費者，金融機構原則上告知其顧客的時點不能晚於建立顧客關係時[156]，對消費者則必須在揭露任何消費者個人非公開資訊予非分支機構的第三人前告知之。但若金融機構沒有揭露任何消費者非公開的個人資訊或未與消費者建立顧客關係，就沒有告知的義務[157]。金融機構亦必須在與其顧客持續的關係中，每年向顧客提供清楚、明確反應其隱私權政策與執行的告知。若金融機構與顧客結束關係後，即毋須向其提供年度告知[158]。

---

[153] 12 C.F.R. 216. REGULATION P 將 GLBA 落實爲下述具體措施：一、金融機構需以明確、清楚且顯著的方式告知消費者關於金融機構在何種情況下，將會對分支機構或非分支機構之第三人揭露消費者非公開之個人資訊；二、金融機構需定期以明確、清楚且顯著的方式告知客戶金融機構的隱私權政策；三、金融機構需提供消費者得選擇個人資訊不被揭露的機制。轉引自林育廷，「淺談我國網路金融法治相關問題之研究」，科技法律透析，2001 年 2 月，頁 56。

[154] 參考：電子金融服務與付款機制電子化管理規範研究，頁 141。

[155] 必須遵守本規則的金融機構爲州體系成員的銀行、銀行控股公司、爲前二者之子公司或關係密切者(不包括非聯邦儲備體系者、由證交法管理的證券商、由投資公司法管理的投資公司等等)、外國銀行的州際代辦處與分社(其存款非由聯邦存款保險公司承保)和由外國銀行控制或持有的商務借貸公司等。

[156] 適時告知的例外規定 C.F.R.(§216.4(E))，如建立顧客關係非來自顧客的選擇，或適時提供告知會造成顧客交易的實質遲延且顧客同意事後再取得告知。

[157] 12 C.F.R.§216.4(A).(B).

[158] 12 C.F.R. § 216.5.

本規則下，金融機構必須提供清楚且足夠的事先通知且能夠完全反映其隱私權政策與執行給消費者(consumer)與顧客(customer)。金融機構對原來的客戶(existing customer)提供新的金融商品或服務時，也必須滿足事先足夠通知的要求。但若建立顧客關係非消費者自己的選擇，或者顧客同意延後獲通知，則可以延後通知。必須包含在隱私權通知裡的訊息有：[159]

1. 金融機構可能收集到有關個人的非公開資訊種類；

2.金融機構會揭露的個人非公開資訊；

3. 將對之揭露資訊之分支機構或非分支機構之第三人；

4.有關從前顧客非公開的個人資料被揭露的種類以及對之揭露的分支機構或非分支機構之第三人；

5. 若對非分支機構之第三人揭露個人非公開的資料需有一獨立通知(a separate statement)；

6. 向消費者解釋在本法規定下得選擇終止金融機構向非分支機構之第三人揭露關於其非公開之個人資料的權利；

7. 任何在公平信用評等法(the Fair Credit Reporting Act,15 U.S.C. 1681a(d)(2)(A)(iii))規定下的洩露、

8. 機構本身關於保護個人非公開資料機密及安全的政策與實踐；

9. 任何在§216.6 第二項中所必須揭露的事項[160]。

金融機構針對非顧客的消費者所給予簡短的選擇權初始告知，必須清楚(clear)、明確(conspicuous)地陳述其隱私權注意事項如何遵循法令，說明消費者如何透過合理方法行使上開選擇權利[161]。此所稱「合理方法」例如：提供消費者免付費電話或是在金融機構辦公室取得告知書的影印本。而在給予消費者的選擇權告知中，必須表明：1. 金融機構揭露或保留將消費者非公開之個人資訊揭露予非分支機構的第三人之權利;2. 消費者擁有終止揭露的

[159] 參考：電子金融服務與付款機制電子化管理規範研究，頁 141-143。

[160] 12 C.F.R.§216.6(B)

[161] 12 C.F.R.§216.6(D)(2).

選擇權，以及3. 消費者合理行使上述選擇權的方法[162]。合理行使選擇權的方法例如：在有關選擇權告知書中明顯標示出選擇權選項、在選擇權告知書裡附上回覆表格(a reply form)、提供行使選擇權的電子方式(例如寄發電子郵件或透過金融機構網站)、提供免付費電話供消費者做選擇[163]。消費者可以在任何時候行使選擇權[164]，而金融機構必須在接到消費者選擇權決定後在合理可執行的時間內立即遵守[165]。消費者所做的選擇決定，其效力將持續到消費者自行另以書面撤回爲止，而與同一人重新建立的顧客關係，將不適用於先前顧客關係中所爲的選擇[166]。金融機構不可直接或透過任何分支機構提供予消費者初次的隱私權告知內容外，揭露其他非公開個人資訊，除非：1. 金融機構已經對消費者提供清楚、明確描述修正的隱私權政策與執行的告知；2. 金融機構提供消費者再一次選擇機會；3. 在揭露消費者資料給非分支機構的第三人之前，曾經提給予消費者合理的機會(a reasonable opportunity)以行使選擇終止的權利，以及4. 若消費者沒有選擇終止揭露[167]的情形。[168]

金融機構必須滿足§216.4與§216.7的「告知」要件，並且在將個人非公開的資訊揭露予非分支機構的第三人之前，提供消費者選擇終止的機會；但消費者沒有選擇終止時，金融機構才可以例外地直接或透過分支機構揭露資訊。金融機構可以提供消費者個人非公開資訊揭露的部分終止權(partial opt out)[169]。針對資訊的再度揭露或重複使用限制，若金融機構因§216.14或§216.15例外規定而自其他非分支機構的金融機構取得個人非公開的資訊，則允許將此資訊揭露予資訊來源金融機構的分支機構、本身的分支機構或爲一定目的而使用。[170]

---

[162] 12 C.F.R.§216.7(A)(1).

[163] 12 C.F.R.§216.7(A)(2)(II).

[164] 12 C.F.R.§216.7(F).

[165] 12 C.F.R.§216.7(E).

[166] 12 C.F.R.§216.7(G).

[167] 12 C.F.R.§216.8(A).

[168] 參考：電子金融服務與付款機制電子化管理規範研究，頁 143-144。

[169] 12 C.F.R.§216.10.

[170] 參考：電子金融服務與付款機制電子化管理規範研究，頁 144。

若金融機構非因前揭 §216.14或 §216.15規定而取得資訊，金融機構得將該資訊揭露予資訊來源金融之分支機構、本身的分支機構或合法透露給任何與此資訊來源機構相關的任何個人。而在 §216.14 或§216.15 例外規定下取得資訊之非分支機構的第三人，該第三人可將此資訊揭露予其分支機構或爲一定目的而揭露使用。非因 §216.14 或§216.15 例外規定取得資訊之第三人，則得將資訊揭露予其分支機構與合法情況下可對之揭露的其他個人[171]。原則上，金融機構不得直接或透過分支機構，對非分支機構的第三人以電話銷售(telemarketing)、郵件銷售或其他電子郵件銷售目的，爲消費者帳戶金額、帳戶密碼、存款數額、信用卡密碼或交易數額的揭露。例外的情形，則是在金融機構將帳戶數額或密碼單獨揭露予其代理人或服務提供時，以便爲金融機構產品及服務的實現，或爲私人的信用卡計畫而揭露予顧客知悉的相關參與者，則允許揭露之[172]。

上開 §216.7與 §216.10的選擇權相關要求，在金融機構提供個人非公開的資訊予非分支機構的第三人，旨於使第三人對之提供服務(perform services)或以金融機構名義(functions on your behalf)時，則不適用。但此時金融機構必須滿足 §216.4 所指初次告知的要求，以及與第三人簽訂契約協議，禁止第三人在上述目的外揭露或使用金融機構所揭露之資訊，包括在 §216.14 或 §216.15 例外規定下以日常營業過程實踐這些目的。[173]

簡言之，若依本條規定經由共同行銷方式揭露非公開性之個人資訊予金融機構，且與該金融機構間之約定符合依本條中第(a)(1)(ii)款所規定，除因實施共同行銷或第216.14 或第216.15 條中所載之一般正常業務範圍內之共同行銷之例外情形，金融機構不得揭露或使用該非公開性的個人資訊[174]。至於 §216.4(a)(2)對消費者初次告知的規定，§216.7 與 §216.10 所稱選擇權規定，以及 §216.13 所指對服務提供者與共同行銷的要求，若金融機構揭露非公開的個人資訊乃與下列行爲有關，則例外不適用－爲達成、實現或執

[171] 12 C.F.R.§216.11.

[172] 12 C.F.R.§216.12.

[173] 參考：電子金融服務與付款機制電子化管理規範研究，頁 145。

[174] 12 C.F.R. § 216.13(A).同條(B)段規定服務(SERVICE)目的可以包括共同行銷(JOINT MARKETING)。

行來自消費者的要求或授權之必須(necessary to effect, administer, or enforce a transaction)、服務處理消費者要求及授權、處理消費者帳戶及私人信用卡問題、研議中或已進行的證券化(proposed or actual securitization)及次級市場買賣(secondary market sale)與關係到消費者交易的類似交易等[175]。另外，若取得消費者未撤回(revoked)之同意(consent)或指示[176]，或爲對抗實質及潛在的詐欺、非授權交易，或提供資訊予保險費率諮詢機構(insurance rate advisory organizations)、保證基金或金融機構之律師、會計師、審計人員，或爲了買賣、併購、交易或轉讓全部或部分營業，或遵守聯邦、州、當地法令及其他應適用的規定之目的，或爲了民刑事的調查(investigation)、傳喚(subpoena)、約談(summons)等，金融機構毋須適用 §216.4(a)(2)初次告知要求、§§216.7 與216.10 選擇權要求，以及 §216.13 對服務提供者和共同行銷之規定[177]。

綜前所述，進一步介紹過GLBA與Regulation P 的相關內容後，足知該等規則中金融機構必須在詳盡的程序規定下方可揭露消費者個人非公開的資訊，相較我國目前新修訂的「金融控股公司法」第四三條，似乎有所不同。蓋新法四三條第二項專侷限於金融控股公司之子公司相互間，且係爲共同行銷之目的所爲之資訊交互運用而設之限制。但美國法關於資訊利用與揭露之規定於關係企業間卻不適用，因希冀關係企業得藉客戶資訊之交戶利用來降低成本，而收經營之效。美國的Regulation P 對於極敏感之資料運用，採取原則明文禁止的立法，而我國新法則未對此設有限制，則是否意味個人之帳號、密碼等資料亦得經個人書面同意而使金融子公司交互運用？[178]

三、財務隱私權法 Right to Financial Privacy Act, 12 U.S.C. 3401 et seq.

財務隱私權之相關規範，原肇始於銀行秘密法的制訂造成金融機構很大

[175] 12 C.F.R.§216.14(A).此段中有關“NECESSARY TO EFFECT, ADMINISTER, OR ENFORCE A TRANSACTION”的解釋請參見(B)段。

[176] 12 C.F.R.§216.15(B)(2)：消費者可以撤回對揭露資訊的同意。

[177] 12 C.F.R.§216.15. 電子金融服務與付款機制電子化管理規範研究，頁 145-146。

[178]參見張冠群，二ＯＯ九年一月金融控股公司法關於共同行銷及關係人交易與風險集中揭露之修正條文評析，月旦法學雜誌 (No. 168) 2009.5 頁 204-205.

參考：電子金融服務與付款機制電子化管理規範研究，頁 146。

負擔，且無法滿足顧客對金融機構資訊保密的要求，故催生出財務隱私權法，以期在政府犯罪調查與財務隱私保障下取得平衡點。本法建立了將消費者金融紀錄對政府機關揭露的程序規定與例外，提供消費者在聯邦政府對金融機構監督下可以享有合理隱私權對待權利。[179]

政府若欲取得顧客的財務資料，必須符合五種方式規定[180]：

1. 經由顧客授權(customer has authorized such disclosure)、

2. 取得行政傳票或傳喚(an administrative subpoena or summons)、

3. 取得搜索票(search warrant)、

4. 取得司法傳票(judicial subpoena)、

5. 經由正式的書面請求(formal written request)。

惟金融機構或其主管、雇員、代理人通知政府當局，其持有可能有關違反法律或規則的資訊時，例外地排除上開方式規定的適用，上開揭露者毋須負任何法律責任。此外，金融機構為附隨於完整擔保利益，證明破產請求權，債務催收或處理關於政府貸款、貸款保證等之申請而提供紀錄[181]亦不在禁止之列。[182]

四、公平信用評等法案（Fair Credit Reporting Act, FCRA, 15 U.S.C. §1681 et seq）

公平信用評等法，係由美國聯邦貿易委員會(the Federal Trade Commission)專責執行，立法目的在要求消費者信用報告代理機構採用合理的程序，以符合消費者信用、個人與保險或其他金融資訊的機密性、正確性、中肯與適當使用，並確保公平、公正且尊重消費者隱私權。本法並建立修正消費者信用報告錯誤的程序，確保只在合法的商業目的下提供有關消費者報告。信用報告必須為判決、留置權、訴訟等保留七年，但為了破產事件應保

[179] 參考：電子金融服務與付款機制電子化管理規範研究，頁 146。

[180] 12 U.S.C.§3402.

[181] 12 U.S.C.§3403(C)(D).

[182] 參考：電子金融服務與付款機制電子化管理規範研究，頁 147。

留十年。本法並修正了TILA(Truth in Lending Act[183])誠實信貸法的規定，要求針對所有有關信用卡、賒帳卡的申請或要約，必須有新的揭露，包括每年利率(annual percentage rates)、定期會員費用(periodic membership fees)、最低限度的金融規費(minimum finance charges)以及餘額結算方法(the type of balance calculation method)。此法優先於各州州法適用[184]。

目前公平信用評等法，依據2003年「公平正確信用交易法」the Fair and Accurate Credit Transactions Act of 2003(FACTA) (PL 108-159, 12/04/03)所爲之部份修正，FACTA 要求聯邦貿易委員會和相關機構在2004年以FCRA 授權所制訂的規定來執行FCRA 中的修正條款[185]。除了上開法案提供消費者保護外，電子資金移轉法(EFTA[186])與誠實信貸法(TILA)都有消費者保護的相關部份規定。[187]

第四項　我國對於金融業客戶個人資料保護之現況

我國有關金融隱私部分的法制建構，除於消費者保護法第§4、11~17、22-1等條文中針對企業提供服務的消費者保護原則、定型化契約訂定與解釋原則與廣告揭露規定外；「個人電腦銀行業務及網路銀行業務服務契約範本」更建立主管機關爲電子金融的網路服務所爲的低度規範；電腦處理個人資料保護法§6、23(4)牽涉非金融機關對個人資料的利用；金融控股公司法§42、43、48、60[188]與銀行法§28IV、48II 成爲不同金融主體關於客戶金融資料保密與

[183] 15 U.S.C §§1601-1667f. (Amended as of January 1, 2001).

[184] *SEE* JONATHAN R. MACEY, GEOFEREY P. MILLER& RICHARD SCOTT CARNELL, BANKING LAW AND REGULATION, 3D, AT 172~173 (2001).電子金融服務與付款機制電子化管理規範研究，頁 147-148。

[185] 有關 FCRA 的全文與簡介，請參見聯邦貿易委員會(FTC)網站，網址：HTTP://WWW.FTC.GOV/PRIVACY/PRIVACYINITIATIVES/CREDIT.。電子金融服務與付款機制電子化管理規範研究，頁 148。

[186] Electronic Fund Transfer Act, 15 U.S.C. §1601

[187]如 EFTA 中§1693c 中規定對於消費者對於非經授權交易責任的事先揭露、§1693g(b)所設有關舉證責任分配規定中要求金融機構應負擔「主要的」舉證責任等，將消費者保護理念深入實踐於每一個金融交易。另外，誠實信貸法(TILA)認金融機構有提供資訊的義務，也是消費者保護的表現，值得參考。參電子金融服務與付款機制電子化管理規範研究，頁 148。

[188] 金控法隱私權規範的介紹與遺漏，請參照施峰達，「我國『金融檢查』與『財務隱私權』法制關連性之探討-以銀行業之監理爲中心」，中原大學財經法律學系碩士論文，91 年 1

使用的準則[189]。電子簽章法於2001年11月14日公布，2002年4月1日施行，其中鑑於憑證機構將大量蒐集、處理個人資料，亦在第十一條第二項將「保護當事人個人資料之方法與程序」明定爲憑證實務作業基準應載明事項之一。

上開規定或契約範本看似多元，其實彼此之間的相互勾稽就會造成資訊隱私權防護的漏洞。且保密義務規定不夠詳細，僅作原則性保密規範，似乎無法完全保障消費者資訊隱私權[190]。

第五項　國內外近來發生案例摘要

一、現金卡個資外洩詐欺集團[191]

內政部警政署刑事警察局宣布偵破，銀行客戶現金卡申請書資料外洩，遭詐騙集團冒辦信用卡盜刷案。而被媒體以頭版頭條方式，點名洩漏個人資料的銀行，總經理特別澄清表示，是代辦公司出問題[192]，卻要銀行背黑鍋，

月，頁 81~84。

[189] 不同金融機構主體違反保密義務的處罰應歸統一，金融機構對於顧客造成較大損害僅可做爲顧客求償的依據，而非差別處斷的依據。見前註 29 文章，頁 83。

[190] 例如，個資法第 23 條但書第四款規定下，金融機構多半在定型化契約中即取得客戶同意，得以將客戶資料爲銀行業務外的使用。又如，依網路下單相關規定，證券公司應要求客戶設定優質之安全密碼以申請交易憑證(電子簽章法規定必須以數位簽章爲之)，然實務作業上，富邦證券公司卻允許其營業員請客戶以簡易數字碼 12345678 申請，並交由富邦證券之營業員利用富邦證券公司網路進行期貨交易的下單動作，造成未經客戶授權下單(由下單 IP 位址看出下單電腦屬富邦網段)，賺取交易手續費。此例業經金管會處分在案，顯示金控集團，或由其客戶資料之互通方便，而可能有侵害消費顧客隱私之慮。更且甚者，於客戶主張侵害時，富邦期貨還未經客戶同意，利用客戶在富邦金控之交易資料(含富邦銀行及證券之開戶及通訊方式與交易記錄)做爲自己訴訟或非訟之抗辯，足見內控及監管之疏漏。

[191] 銀行法第 45.1,48,61.1,129 條 ・電腦處理個人資料保護法第 2,3,23,27,28 條 ・銀行內部控制及稽核制度實施辦法第 17,30,31 條 ・金融機構辦理現金卡業務應注意事項第 4,19-21 條 ・電腦處理個人資料保護法之特定目的及個人資料之類別第 1,2 條 ・臺灣高等法院暨所屬法院八十六年法律座談會民事類提案第二十四號 ・銀行現金卡個資外洩詐欺集團 刑事局破獲

[192] 翁姓男子原本在銀行委託的代辦公司任職，涉嫌趁職務之便，影印民眾申辦現金卡的個人資料，再以電子郵件轉賣給大陸詐騙集團，進行網路盜刷。由於申請表格上姓名、身分證字號、電話、職業等資料相當詳盡，還附上有申請人身分證正反面影本，以及附給銀行的財力證明、薪資扣繳憑單，讓詐騙集團很輕易地就能冒名向十多家銀行申辦信用卡。刑事局偵九隊日前將翁某逮捕。 依內政部警政署新聞發布：(一)刑事警察局偵九隊於網路巡邏時發現使用雅虎奇摩帳號 my68my78 者，在「光華螞蟻市場」網站刊登大量訊息「高收課本。紅綠本買賣～預付卡買賣～轉接～來信留聯絡方式 my68my78@yahoo.com.tw」、「出售奇摩拍賣帳號～要什麼評價的都有！可長期配合！！請來信 my68my78@yahoo.com.tw」，另以帳號 my68my78 於網路上清查後發現，該帳號使用人並於「跳蚤市場」網站有「高收課本紅綠本買賣，電話卡買賣，轉接來信留聯絡方式 my68my78@yahoo.com.tw」等訊息，研判該帳號使

相當不公平。

按姓名、出生年月日、身分證統一編號等個人資料，依據電腦處理個人資料保護法第 23 條本文規定，非公務機關利用時，應於蒐集的特定目的必要範圍內爲之。若因違反規定，致當事人權益受有損害，依同法第 28 條第 1 項本文規定應負損害賠償責任。依同條第 2 項適用同法第 27 條第 3 項規定，每人每一事件最高可獲賠新台幣十萬元。

此外，根據銀行法第 45 條之 1 第 1 項規定，各銀行均應建立適當有效的內部控制制度。參照金融機構辦理現金卡業務應注意事項第 21 點第 1 項規定，若金融機構辦理行銷涉及個人資料外洩等非法行爲，經查證屬實者，主管機關得視情節輕重，依相關規定予以處罰，必要時，得暫停或停止辦理現金卡業務。

二、網路銀行帳戶遭盜領 140 萬 銀行拒絕賠付[193]

用者乃是詐騙集團份子，於網路上張貼上述訊息收購人頭金融帳戶後再使用於犯罪行爲上以逃避警方追緝，影響社會治安甚鉅，刑事警察局偵九隊獲線後，即向局長黃茂穗報告，黃局長獲報後極爲重視，指示偵九隊全力偵辦，刑事警察真九隊即與台北市政府警察局信義分局偵查隊共組專案小組積極偵辦。（二）經專案小組追查相關資料，清查出涉案人乃居住於汐止市伯爵山莊內之翁○欽涉有重嫌，經向臺灣士林地方法院聲請搜索票，前往該嫌出入之特定地點，查扣信用卡卡號資料、民眾現金卡申請人資料、各家銀行信用貸款民眾申請資料等乙批、作案用手機等相關贓證物，其中現金卡申請人資料除了申請表格填有申請人基本姓名、身分證字號、本身持有電話、職業、公司資料外並有申請人聯絡人電話，更誇張的連申請人身分證正、反面影本，及附給該家銀行申請人爲證明財力持有的它家銀行信用卡正、反面影本資料及薪資扣繳憑單也一併被翁嫌以電子郵件寄給藏匿在大陸的信用卡盜刷集團因而外洩，經刑事警察局偵九隊向聯合信用卡中心查詢後，初步得知已有被害人資料被冒用申請別家銀行信用卡因而被盜刷成功；另從翁嫌電腦中清查出來的信用卡資料，發卡銀行分別有中信銀、花旗、荷蘭、國泰世華、玉山、慶豐、遠東、兆豐、台北富邦、聯邦、萬泰、新光、匯豐、華南、台灣銀行、中華、土銀、上海等１０幾家銀行，其中已有數十張卡有被盜刷紀錄，全案依詐欺、僞造文書、電腦及處理個人資料保護法、妨害秘密等罪嫌移送臺灣士林地方法院檢察署偵辦。（三）專案小組正清查該家銀行內部控管機制是否出現問題及相關業務承辦人員，有無勾結信用卡盜刷集團，導致客戶資料被委外的現金卡代辦公司外洩販賣給在大陸之信用卡盜刷集團，使客戶權利嚴重受損。爲杜絕個人資料外洩、人頭戶氾濫警方請大家不要隨便填寫個人資料調查表給他人；另特別呼籲銀行及信用卡中心應嚴格控管個人原始申請基本資料，因該申請資料有申請人詳細申請資料，一經外洩遭詐欺集團利用可能造成民眾重大損失。

[193] 銀行法第 42.1,125.3 條 ・防杜人頭帳戶範本第 1,2 條 ・個人網路銀行業務服務定型化契約範本第 1 條 ・防範歹徒猜中網路銀行客戶密碼之安全控管措施第 3,4 條 ・台財融（一）字第 0911000105 號 ・台融局（一）字第 0090723995 號 ・電話語音、網路銀行約定轉帳 隔日才生效法源編輯室 / 2007-04-30

網路金融詐騙猖獗，林姓男子開啓網路銀行帳戶，出國幾天卻遭盜轉新台幣一百四十萬餘元。然銀行認爲沒疏失而拒絕理賠[194]。警方指出，歹徒的手法日新月異，從「懶人密碼」到植入「木馬程式」不斷演變，民眾使用網銀更要小心謹慎。

就此案例，行政院金融監督管理委員會銀行局官員指出，根據個人網路銀行業務服務定型化契約範本第 13 條第 3 項規定，除非銀行證實客戶故意或過失，否則應先賠付，再報請檢調和警察單位調查處理，釐清責任。不過，銀行表示，如果可以確定林先生的損失是因爲機制錯誤，或被植入木馬程式而遭盜領，他們會負起責任，但也有可能是客戶沒盡到保守帳號、密碼等資料的責任，則不在賠償之列。而刑事警察局科技犯罪防治中心表示，根據調查，確實有駭客組成犯罪集團破解網路帳戶機制，但嫌犯是在大陸遙控犯案，除非他們回台灣，否則很難逮捕。警方提醒民眾，使用網路銀行要謹慎小心，除了要常更換密碼，上網時也應注意不明「釣魚」網站，當心洩漏個人資料，或被植入木馬程式，若有疑慮，可以上刑事局網站下載最新的防堵軟體。

爲防範民眾的網路銀行密碼被歹徒猜中，致權益受損，參照防範歹徒猜中網路銀行客戶密碼之安全控管措施第 4 點第 1 款規定，網路銀行「用戶代號」不得少於六位，若以身分證字號或帳號作爲識別，則應另行增設「使用者代號」以資識別；至於網銀「密碼」，依同點第 2 款規定，建議採英數字混合使用，宜包含大小寫英文字母或符號，不得訂爲相同的英數字或連號，且不得少於六位（若搭配交易密碼使用則不應少於四位）。

三、2.500 萬筆財稅個資疑似外洩[195]

[194] 受害的林先生說，他開設的網路帳戶，於二月十六日到十九日出國期間，歹徒利用ＯＴＰ非約定轉帳機制，四天內盜轉十六筆共一百四十萬三千八百元；他認爲銀行疏失，血汗錢平白無故受損。但該家銀行表示，網路銀行帳戶需三道認證機制，交易時也需要進一步確認，設計上沒有問題，由於此案件已進入司法程序，不認爲有必要先理賠給消費者。

[195] 電腦處理個人資料保護法第 17,27 條 ・電腦處理個人資料保護法之特定目的及個人資料之類別第 1,2 條 ・綜合所得稅電子結算申報作業要點第 1-3 條 ・各類所得資料網際網

根據媒體報導，2008 年底驚傳五百萬筆納稅義務人的資料可以透過點對點分享軟體輕鬆瀏覽，並在立法院財政委員會引起軒然大波。

立委在財委會針對個資疑似外洩與網路報稅安全進行質詢，財政部表示，造成個資外洩的問題，全因民眾使用點對點分享軟體，並非從財稅資料中心外洩出去。立委要求財政部三天到七天日內，必須針對未使用點對點分享軟體報稅民眾資料是否外洩，做出專案報告。

依照綜合所得稅電子結算申報作業要點第 2 點規定，納稅義務人利用網際網路辦理綜合所得稅結算申報及個人所得基本稅額申報，其通行碼有三種。內政部核發之自然人憑證、納稅義務人之「身分證統一編號」加上所得年度十二月三十一日戶口名簿上所載之「戶號」、其他經財政部審核通過之電子憑證。

從 2008 年五月報稅至今，已有十一萬件使用網路報稅，民眾在使用網路申報前，依上開規定，可申請自然人憑證或是金融機構憑證，若無憑證則可利用簡易網路申報，也就是用身分證統一編號加戶口名簿號碼，其中民眾若使用簡易網路申報，與網路點對點分享軟體時，財稅個資就極容易因爲分享而外洩出去，全屬於個人行爲所造成，非政府資料外露。

根據電腦處理個人資料保護法第 17 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。如果真是財政部的資安機制出現問題導致個人資料外洩，依同法第 27 條第 1 項規定，公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。即使被害人並非財產上的損害，依同條第 1 項規定，也可以請求慰撫金。

路申報作業要點第 1-3,5 條 ‧稽徵機關於結算申報期間辦理綜合所得稅納稅義務人查詢課稅年度所得資料作業要點第 6,7 條 ‧釋 字第 631 號 ‧財北國稅資 字第 0950210222 號 ‧法律決 字第 0940009245 號 ‧法律 字第 0910024855 號 ‧個資外洩事件 消保會將與法務部攜手防堵法源編輯室 / 2008-05-05

四、遏止網路釣魚 金管會提供金融業網站資料[196]

鑒於金融網路運用日益蓬勃發展，各金融服務事業所提供之商品及服務透過網際網路提供者愈形普及，爲便於社會大眾瀏覽金融相關網站，同時爲遏阻「網路釣魚」或「虛設網站」誘騙民眾誤上假網站，騙取個人資料或誤信假消息，增加金融網路業務風險，行政院金融監督管理委員會已於 98 年 8 月 24 日大幅改版首頁並增列及調整該會全球資訊網站首頁週邊單位內容，將週邊單位區分爲「金融資訊網站」、「本國公(協)會」、「外國相關網站」、「其他政府網站及相關活動專區」、「合法金融業網站連結」、「上市(櫃)、發行公司網站連結」及「金融發展研究基金專屬網頁」等七類，並呼籲民眾直接點選金管會網站（http://www.fscey.giv.tw/），以連結各類金融機構網址，俾確保相關金融業者網址之正確性及安全性。

五、美國 Heartland 金融交易系統遭駭 1 億筆資料恐外洩[197]

爲美國飯店、酒店，及零售業提供信用卡、薪水支付及相關付款處理服務的 Heartland Payment Systems 日前宣布，旗下付款處理系統被植入惡意程式，由於 Heartland 每月處理逾 1 億筆的交易，因此被視爲可能是有史以來最大宗的資料外洩事件。據了解，Heartland 接到 Visa 及 MasterCard 信用卡公司的通知，警告有可疑的信用卡交易活動，因此藉由法院稽核人員協助該公司進行調查，竟發現有惡意程式危害了 Heartland 網路上的資料，受影響的資料包括未加密的個人身份辨識碼（PIN）、用戶住址，及電話號碼等，所幸目前並未有商家資料或是社會安全碼外洩的消息。Heartland 總裁暨財務長 Robert H.B. Baldwin 表示，他們發現入侵的證據後，就馬上知會聯邦執法機構及金融卡業者，他們認爲此次的意外應該是來自於全球的網路詐欺行爲，現正與美國特勤局及司法部密切合作

[196] 網際網路等電子式交易型態交易資料保存規範第 1-2 條 ・證券商採網際網路等電子式交易型態交易所使用之交易主機應具備之相關受託買賣有價證券檢查點控制項目第 1 條 ・財政部國有財產局個人電腦及網路管理規範第 2,4,5,6,7,9 條 ・防範歹徒猜中網路銀行客戶密碼之安全控管措施第 2-5 條 ・台證交 字第 0930026521 號 ・全新買空賣空詐騙手法 盜奇摩帳號五百個/ 2007-11-19

[197] http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=4791 (2009.02.02)

中。此外，Heartland 亦建立一個相關網站，揭露此意外的相關資訊並建議持卡人特別注意每月的帳單及呈報可疑的行爲。

第六項 小結：未來建議方向

觀之美國財務隱私權法可知，金融機構對於客戶資訊之處理與利用，必須依一定行政或司法上之請求或是顧客之授權同意，然如爲舉發犯罪或其他金融運作之必須(如金融機構爲附隨於完整擔保利益，證明破產請求權，債務催收或處理關於政府貸款、貸款保證等之申請而提供紀錄)時，則可不受該等規定影響而爲一定之揭露。此種設計，對於金融客戶隱私權益保障方面，係爲一衡平公允作法，或值未來金管會因爲個資法修正後，制訂相關金融法規之參考，而避免因法條未臻詳盡規範例外情況，而遭致公益與私益權衡上之爭議困擾。另依美國公平信用評等法相關規定，消費客戶爲任何新申請時，對於其個人資料之蒐集、處理與利用，必須重新對其要求當事人之書面同意，此點也與我國個資法修正方向吻合，建議金管會於個資法通過後，應加強宣導。

金融機構當要開始自行建置或委外尋求供應商進行資安設備評選之前，應確保如下工作，包括文件、政策都已經備妥，切勿以爲有解決方案能全自動包辦[198]。

第一步：文件分類

如果文件沒有分類，系統也不知道要保護哪些類型的資料，分類的方式依照不同的企業營運型態而有所不同。最理想的狀態下，企業應該有自己的檔案伺服器，並依照不同的文件機敏程度而給予不同的分類。當然，也可以做所有文件的控管。

第二步：訂定存取權限管制

公司把文件都分類存放在檔案伺服器之後，想必會同時將權限管理同時

[198] 防制資料外洩評估實務 3 步驟
http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=4766 (2009.01.13)

執行，誰可以創造文件、誰可以存放到檔案夾、誰可以開啓、誰可以修改或刪除，都必須要有相對應的權限，一般而言都是對應到公司部門的職務職權與業務需求。重點在於，所有文件存取的過程都必須要能夠產生稽核記錄(Access Log)方可真正發揮效用。

第三步：從風險分析角度來評估 DLP

接下來，在防制資料外洩(DLP, Data Loss Prevention)的兩個重點在於資料外洩管道及資料外洩手法的防堵，必須規劃完整的資料外洩防範政策及評估 DLP 方案的功能需求爲何來製作 DLP 的需求與風險分析表，不同的方案對應到企業可能要面對的議題上，會有不同的優先需求程度。防制資料外洩解決方案並無一勞永逸的解決辦法，如果從資料本身來看，資料加密基本上算是根本之道，但困難點在於加密金鑰或密碼的管理機制，以及如何確保該加密的資料是確實被加密的。再者，就是落實管理辦法，以對使用者產生威嚇的作用。最後必須知道，資料永遠會有外洩的可能。所以，必須有一套相對應的資料外洩危機處理方案，包括如何偵測、追蹤外洩資料的發生，這就是另外一個未來的發展考量方向，也是一個企業善盡資料安全與客戶權益確保的必要作爲。

第二節　電信業對個人資料之蒐集、處理、利用及保全

第一項　我國電信業之發展

1987年當政府宣布用戶可自備電話機時起，台灣電信自由化露出第一道曙光，之後1989年放寬對電信網路利用，並逐步開放加值網路業務及第一類電信業務開放予民間經營等政策，直至2001年7月開放所有電信業務，使台灣電信市場邁入全面自由化之新局面。由於電信自由化政策，使得消費者逐漸得享受到物美價廉的通訊服務，而近年來通信服務市場之成長相當驚人，以行動電話爲例，其佔有率已超過百分之百。而隨著電信自由化，電信服務類型亦趨多元化，另加上通訊技術的日新月異，使得越來越多的服務內容，已不再侷限於原有傳統的電信語音服務。[199]因應電信、傳播與資訊科技匯流趨

[199] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 18。

勢，傳統分類方式已無法切合科技匯流與產業界線的變化，從而，如何爲一個較合適的分類模式以利管理，成爲各國相關管制機關所面臨之首要議題，歐盟執委會於其架構指令（Framework Directive，Directive 2002/21/EC)[200]之定義上，不以傳輸設施來區分電信、傳播或資訊產業，而改以電子通訊網路（electronic communications network）[201]來定義傳輸載具，所謂電子通訊網路係指以傳輸系統，及其所使用之交換或路由設備，或其他以有線、無線或其他電磁方式傳輸訊號，而這傳輸網路包括衛星網路、固定（迴路與封包交換，包括網際網路）、地面行動網路、電力纜線系統、無線廣播與電視廣播網路及有線電視網路，且不論其所傳輸之資訊型態爲何。我國爲順應通訊傳播業匯流之趨勢，於2004年1月7日通過的「通訊傳播基本法」第二條定義規定中，亦採功能別定義方式，將通訊傳播定義爲：以有線、無線、衛星或其他電子傳輸設施傳送聲音、影像、文字或數據者。而電信業可分爲第一類電信事業和第二類電信事業，根據電信法規定，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；第二類電信事業指第一類電信事業以外之電信事業。由此可知，第一類電信業者建置網路基礎建設，不屬於資訊服務業範圍，而第二類電信業者利用第一類電信業者的基礎建設，提供用戶網路接取及加值服務。

第二項　「通訊傳播業」與客戶資料隱私之關係

面對通訊傳播業之界線越來越模糊，跨業整合之現象將日趨普遍，在此情況下，通訊與傳播業者間資訊之互通頻繁應可預見，而消費者個人資訊將更加容易被濫用，爲保障個人隱私權有必要從整個通訊傳播領域爲探討，故本報告擬在通訊傳播匯流趨勢下，以我國通訊傳播基本法對通訊傳播之定義爲範疇，探討該領域對個人隱私權保護之規範。主要議題可包括個人資料隱私、資訊安全管理與維護、通訊秘密、未經邀約通訊等方面。[202]隨著行動商務的發展，個人對於通訊內容的需求更爲殷切，尤其行動商務的特色在於可以更明確掌握各用戶消費習慣，通訊傳播業者爲滿足消費者個人化之需求，

[200] Framework Directive (2002/21/EC) , OJ L 108, 24.4.2002, p.33,

[201] Framework Directive, Article 2(a)。

[202] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 20。

即必須利用所擁有之用戶個人資料與通訊資料，以提供該用戶最適化之服務。但便利用戶的服務，若未謹慎爲之，往往也是對個人隱私構成危害的服務[203]。所以隨著通訊服務的多樣化，個人資料被他人蒐集、利用與處理之機會也隨之日增下，通訊傳播業使用個人資料的行爲如果未經適當規範，即相當容易構成對個人資料隱私的威脅，如何將該資料爲有利之應用，並能兼顧用戶隱私權之保障，即屬重要。[204]

個人隱私保護也包括個人不受打擾的權利。在這個議題中以未經邀約之通訊中，最常被提到。所謂未經邀約(unsolicited)的通訊，即通訊一方未經另一方同意即主動利用通訊服務與之溝通，例如透過智慧型語音系統，以自動撥號或預錄音帶推銷商品、或利用電話傳真傳送商品傳單、或經網路發送的商業電子郵件。尤其電子通訊服務的發達使得資訊流通更加便利，但電子通訊發送訊息的低成本、快速、便利、甚至跨國界特性，若被濫用，也會成爲使用者困擾的來源，例如濫發商業電子郵件的行爲，不但對網路使用者帶來的相當大困擾；也極易因此發生行銷詐欺行爲，造成消費者損失。[205]

即便通訊傳播業者以符合蒐集、利用、處理的範圍使用用戶的個人資料，但隨著日常生活中電子通訊活動日漸頻繁，資訊安全的問題，例如個人資料的管理架構、干擾電腦電磁紀錄、妨害電腦使用等行爲，如果未經妥善處理或計畫，除了可能造成用戶對於使用通訊服務上的遲疑，也造成服務提供者經濟上的損失，而其對於用戶隱私的侵害，也是不言可喻。因此要保障個人資料完整性、免於遭到未經同意的使用與通訊過程中不受到干擾，也必須保護資訊安全。[206]

---

[203] 以定位資料所提供之服務爲例，通訊傳播業者可透過用戶資料之比對，得知該用戶之交友偏好，並就其所在位置提供符合其交友條件的用戶。但是如果未告知用戶經其同意，該用戶的行蹤即可能在不知情的情況下暴露給第三者。所以通訊傳播業者在提供客製化服務過程中，其蒐集資料與提供服務的方式，若在告知與同意上產生瑕疵，對重視個人隱私的用戶而言，即可能已經造成某程度的侵犯。

[204] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 20。

[205] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 20-21。

[206] 針對上述在通訊傳播業中，關於個人資訊隱私保護的議題，我國雖在個別領域諸如民法、刑法、電信法、廣播電視法、電腦處理個人資料保護法等中已分別有加以立法，但一方面保護法益與保護行爲分歧，在規範適用上有其整合上的必要；一方面通訊傳播業所提供的服務中所利用的個人資料，如流量資料、位置資料等有其特殊性，實難以用一般性規定，例如

第三項 電信業者對於客戶資料之蒐集、處理與利用

由前述有關通訊傳播業下數位匯流的論述可知，傳統電信與網路截然劃分的明確區隔將逐漸模糊。倘若法制規劃係以區別電信與網路爲前提，可能會使得由電信流入網路的個人資料，或由網路流入電信的個人資料，因爲無法可管，而成爲法規範真空的領域。有鑑於此，關於通訊傳播業個人資料保護的法制規劃，爲求其周延，或許可以跳脫傳統由產業別出發，分別就網路或電信產業思考的模式，轉而從資料的性質出發，依不同的資料性質，設計妥善的個人資料保護法制。[207]

將通訊傳播業中所涉及的個人資料加以類型化的意義在於：法規範必須針對事物的本質爲妥適的設計。對於同等事物，應爲同等對待；對於不同事物，應爲不同的對待，此乃法規範合理性基礎之所在。個人資料若依其類型之不同，某些類型的資料僅須提供較低限度的保障，而某些類型的資料則須以較高的標準加以保護，當法規範一概以單一標準予以保障時，其合理性即有可疑之處。[208]

事實上，在目前外國立法例中，已有依通訊業個人資料類型不同而設計不同規範者。例如歐盟隱私與電子通訊指令，即將資料分爲位置資料[209]與流量資料[210]、名錄資料[211]，以及來電顯示（calling line identification）[212]；美國電信法（47 U.S.C. §222）就客戶專屬網路資訊（customer proprietary network information）、總合統計資訊（aggregate information）、用戶

以個資法，加以全部涵括規範。參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 21。

[207] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 22。此外，1995 年，在一份針對美國國家資訊基礎建設隱私保護法制的研究報告中，已發現此一趨勢。U.S. DEPT. OF COMMERCE, NAT'L TELECOMM. AND INFO. ADM., PRIVACY AND THE NII：SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995), *available at* <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.>（last visited on 2009.6.30）.

[208] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 22。

[209] 第 9 條參照。

[210] 第 6 條參照。

[211] 第 12 條參照。

[212] 第 8 條參照。

名錄資訊（subscriber list information）有所界定。由以上外國立法例可看出，通訊業中，目前已經認定與個人隱私有關之資料，大致可分爲：與流量相關、與位置相關、與用戶有關（包含客戶目錄、名單、來電顯示），以及與非屬個人資訊之總合統計資料（即爲去個人化（de-identified））等類型。以下將分別就其內涵、特性予以說明。[213]

一、流量資料

流量資料，係指使用者使用通訊服務，在使用的過程中所發生的交易資料（transactional data），例如通話對象、持續時間、費率、經過的中繼點等。除了做爲計價（billing）的依據外，通訊業者亦可藉由蒐集此類資料，分析個別使用者的使用習慣、偏好，供行銷之用。流量資料對於個人隱私的重要意義在於其中蘊含著個人的人際網路、生活作息、消費偏好等資訊。此類資訊一旦爲他人所掌握，個人的交游、習慣、喜好，即無秘密可言，對隱私權之危害，不可謂不重大。[214]

從通訊業業者的角度而言，當業者掌握充分的流量資料後，就可以針對不同消費者的消費偏好、使用特性，採取多樣化的行銷策略，同時能兼顧成本與效益[215]。而從消費者的角度而言，對於通訊業者針對消費者個人需求，適時的提供新產品或新服務的訊息，供其作爲購買決策的參考，對某些人來說，這種服務能滿足其需求，因而接受意願較高。但相對的，有些人則可能只想使用目前的產品、服務，而不願接受新產品或服務的行銷活動訊息。對後者而言，過度的行銷廣告，可能是一種騷擾。[216]

其次，消費者爲確保其不致被超額收費，往往需要帳單上詳列其通訊明

[213] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 22-23。此外，美國曾發生一案例，大法官候選人及其家人在錄影帶出租店的交易紀錄被公開。令人訝異的不是被揭露的資訊，而是法制上連此類資料的保護都付之闕如。此一個案，終於導致美國於 1988 年通過 Video Privacy Act。

[214] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 23。

[215] 舉例而言，若電話公司的某位客戶較有撥打國際電話的需求，當該公司推出國際電話促銷方案時，便可特別向該名客戶發送促銷訊息，而能期待發生一定的效果。倘若電話公司不能區隔客戶類型，針對較有消費潛力的客戶推銷產品，可以預見其行銷的平均效果必然較爲低落。

[216] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 23-24。

細。但另一方面，消費者也可能會基於維護其通聯紀錄之隱私不被他人蓄意或偶然查知，而不希望帳單上有詳細的通聯紀錄。事實上，之所以會產生通聯紀錄，係因目前電話通訊仍是基於線路交換（circuit-switch）技術，依單次連線時間計費。在封包交換（packet-switch）的通訊網路，其計費基準則是以資料傳輸量計算，或是以定期不限時間連線之方式計費。在後者，並無產出詳細通聯紀錄之必要。[217]

從法律爭議的角度而言，流量資料可能是發生爭議時，作爲證明特定事實的重要證據。例如刑事訴訟證人於法庭上宣稱並不認識被告，但檢察官在電話通聯紀錄中卻發現證人與被告通話的紀錄，因此使得法院對於證人證詞的可信度發生懷疑，對於法官心證之形成具有一定的影響力。從犯罪偵查或國家安全維護的角度而言，檢調機關或國家情報機關，亦可能有取得特定人所爲或流向特定人之通聯紀錄的需求。國家取得此類個人資料，係侵害憲法保障之秘密通訊自由，故必須依法律規定，經法定程序取得此類個人資料，否則即屬違法。[218]

（1）美國 1996 年電信法對客戶資料隱私保護之規範

美國在1996年電信法（the Telecommunications Act of 1996）中，在第222條（47 U.S.C § 222）對於客戶個人資料的隱私有特別的規範。國會訂定第222條是期望能達到客戶隱私保護及促進電信市場競爭的雙重目的。電信業者（telecommunications carriers）有責任保護其他電信業者、設備製造商、客戶及轉售業務業者相關專屬資訊之隱密性[219]。第222條主要規範三種類型的資訊，一爲客戶專屬網路資料（Customer proprietary network information，以下簡稱CPNI），二是整合統計資訊（Aggregation information），三是用戶名錄資訊（Subscriber list information）。

（2）歐盟：電子通訊個人資料處理暨隱私權保護指令（2002/58/EC）

對於流量資料，指令之規定於第6條。「流量資料」的定義，是指以在電

[217] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 24。
[218] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 24。
[219] 47 U.S.C § 222(a).

子通訊網路中通訊傳輸爲目的、或爲帳務目的而處理的資料而言。這些由公共通訊網路或公共電子通訊服務提供者所處理及儲存，且與使用者及用戶相關之流量資料，當通訊傳輸的目的不再時，必須被刪除或匿名化處理。[220]另爲用戶帳務及互連費用所需的流量資料，指令亦規定得處理之，但必須是在得對帳單提出異議或得爲付款請求之期間內爲限。[221]此外，爲行銷電子通訊服務或提供加值服務之目的，若取得用戶或使用者的同意，公共電子通訊服務提供者得在目的之必要範圍及期間內處理流量資料，且亦應提供用戶或使用者撤銷同意之機會[222]。

指令同時規範告知之義務，即服務提供者必須告知用戶或使用者以下資訊：（a）所處理的流量資料之類型、（b）爲用戶帳務及互連費用之目的資料處理期間（c）及爲行銷或加值服務目的，在取的同意前告知行銷必要的期間。[223]此外，上述所爲之處理，必須限制是公共通訊網路服務（或公共電子通訊服務）提供者所授權之人員，且爲處理帳務、流量管理、客戶查詢、詐欺偵查、行銷電子通訊服務或提供加值服務目的之必要範圍內始得爲之[224]。

二、位置資料

位置資料係指使用者所使用的終端設備所在的地理位置，以及行進的方向、速度。[225]所謂的地理位置，除了包括精確的地表經度、緯度之外，尚包括終端設備於特定時點所連接的基地台（network cell）。由以上定義可知，位置資料並不必準確地指出終端設備於特定時點所在的精確位置，即使僅能說明終端設備於特定時點的位置的大概範圍，亦屬之。[226]

所謂的位置資料，主要應用如目前電信業所提供的定位服務。其基本運

[220] Art. 6 para. 1.

[221] Art. 6 para. 2.

[222] Art. 6 para. 3. 此部分翻譯參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 32。

[223] Art. 6 para. 4.

[224] Art. 6 para. 5. 此部分翻譯參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 32-33。

[225] 相關定義，參見前註歐盟指令第二條。

[226] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 24。

作原理係在中心網路上架設專門處理定位查詢的位置伺服器（location server），而發出定位詢問（position request）的應用程式可能來自於任何網路端點或是手機終端裝置，扮演客戶端（client）的角色。當位置伺服器收到定位查詢的訊號後，位置伺服器將透過電信網路的定位系統確定客戶端的正確位置，然後送出定位回應（position response）。[227]關於位置資料之蒐集、計算方式，因所採之技術爲有線通訊[228]與無線通訊[229]而有所區別。[230]

在有線通訊，終端設備須依賴線路連接使能發生作用，其位置通常在業者安裝之時即已確定，並有所記錄，相當明確。縱使消費者自行接線，其延伸範圍亦不脫離同一戶或同一大樓的範圍。但若使用者以原終端設備爲中繼點，於終端設備外自行延伸架設無線通訊網路，屆時，真正的最後終端設備將難以確認。[231]至於終端設備的行進方向及行進速度的位置資料，僅存在於無線通訊應用上，有線通訊下的固定式終端設備不可能產生此類資料。實際上，目前所謂的定位服務，主要都是針對無線行動通訊，在有線通訊，並無定位服務之需求。[232]

在無線通訊，關於終端設備的精確位置、行進方向或速度，必須經由計算才能獲得。若訊號發射及收受的基地台只有一個時，由於無線電波在空氣中會發生折射、反射，故接收方並不能藉由訊號接收來確認發送方的正確相對位置，只能藉由接收終端設備所發射出的訊號得知該終端設備正在基地台收發訊號的半徑範圍內。[233]若要獲得較確定的位置資料，須要藉由多點交叉

---

[227] 宏裕，位置定位服務深入探討（上），網路通訊，116 期，頁 114，2001 年 3 月。

[228] 就目前而言，有線通訊可傳遞數位訊號（如網路），也可傳遞類比訊號（如電話、電視），但透過訊號轉換技術，用類比訊號也可連接網際網路（如撥接上網），使用數位訊號也可講電話（Voice over IP）、看電視（Video on Demand）。目前數位電視亦已進入市場。由此可知，以數位訊號與類比訊號之差異來區隔市場、應用，將愈來愈困難。

[229] 無線通訊應用，亦可再細分爲行動通訊與非行動通訊技術。前者在使用者高速移動中仍可收發訊號；後者雖非完全不能於移動時收發訊號，但在移動速度較高的情況下，可能會發生訊號中斷。在目前，行動電話及無線電通訊屬於前者，而無線網路應用則屬後者。

[230] 服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 25。

[231] 以目前的網際網路應用爲例，消費者申請 ADSL 或 Cable Modem，在家中自行架設交換設備（不論是有線或無線），配合 Network Address Translation 技術，其網際網路連線的資源甚至可以讓數百公尺範圍內的鄰居共同分享。

[232] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 25。

[233] 在都會區，當基地台的半徑範圍不大的情況下，此種定位方式仍具實用性。宏裕，位置定位服務深入探討（中），網路通訊，117 期，頁 110，2001 年 4 月。

定位，其計算方法，是藉由三個基地台，由各自訊號發射及接收的時間差，算出終端設備與基地台的相對距離，再以終端設備與各基地台的相對距離爲半徑畫圓，取其交叉點，即爲終端設備的可能位置。在衛星定位系統（Global Position System, GPS），其原理亦大致相同，差別在於後者係由環繞地球的二十四顆衛星擔任基地台的角色[234]。

值得注意者，不僅是在電信服務業者提供的無線通訊服務（例如目前的GSM、PHS），或是GPS應用下才會產生位置資料。在無線網路上，亦可能有定位服務之需求。例如在博物館中，遊客可以藉由具備無線上網功能之PDA或手機，在每個展覽點接收展覽之詳細說明。事實上，無線網路服務下的定位技術，亦非不可行[235]。

在無線通訊技術，並非所有採用無線通訊技術的通訊方式均有產生位置資料的必要。例如，在使用者自行架設的區域無線網路（WLAN），發射及接收訊號的基地台（access point）縱使有多個，也沒有記錄位置資訊的必要，網路設備廠商亦不太可能開發出有記錄位置資料功能的基地台設備。[236]

位置資料對於個人隱私保護的意義在於：位置資料將使得個人何時位於何處的資訊不再爲個人所專有，而處於他人可得知的狀態。[237]就位置資料 對隱私權的負面影響而言，倘若位置資料之保護不足，消費者可能會因擔心其遷移位置之資訊爲人所知，而主動限制自己的行動。我國憲法雖保障人民有遷徙、旅行的自由，但僅係禁止國家以不當方式限制人民的自由、權利;至於因資料保護不當而導致人民自發性的限制自我行動，似乎難以納入憲法保障

[234] 宏裕，同前註，頁 117-8。參考轉引自：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 25-26。

[235] 蔡子傑、高紹華、李政霖，無線區域網路定位系統，中華民國資訊學會通訊，7 卷 1 期，頁 127-8，2004 年 3 月。參考轉引自：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 26。

[236] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 26。

[237] 在電影「全民公敵」（Enemy of the State）中，主角的位置資訊之所以隨時處於被監控的狀態，是因爲身上被裝置訊號發射器，其應用原理與通訊傳播業下的位置資料相同，但就法律上的意義而言，兩者並不相同。按前者所涉及的是國家偵查犯罪的手段是否合法（國家僅得在法律明文而有必要的情況下對特定人裝置訊號發射器，用以監控其位置），而後者則是通訊業者爲提供服務，必須處理、記錄每個消費者的位置資訊。兩者均涉及位置資料之處理及應用，但資料搜集的合法性要求並不相同。國內文獻在引用上開電影的背後意涵時，往往未明確區分技術應用與法律意義上的差異，易造成誤解，將國家偵查手段所涉及的隱私保障議題與通訊業隱私保障議題混雜在一起。

人民遷徙、旅行自由的範圍內。就其正面意義而言，位置資料係爲滿足人類社會生活所必須。在公益目的上，諸如犯罪偵查之證據取得，犯罪嫌疑人或刑案被告之逮捕，緊急危難之救助；在私益上，道路導引、即時消費資訊之提供，企業經營之內控等，均有賴即時而正確地蒐集位置資訊。由此可知，位置資料爲他人所持有，或許有害於個人隱私，但亦具有其正面意義。[238]

（1）歐盟：電子通訊個人資料處理暨隱私權保護指令（2002/58/EC）

所謂位置資料，指令的定義是指在電子通訊網路中處理、得以表明公共電子通訊服務使用者的終端設備所在地理位置之資料而言。一般而言，位置資料可能指使用者終端設備之經度、緯度和高度，亦可能爲其行進之方向、位置資料的正確程度等。在數位行動網路通訊系統，使用者終端設備所在地之位置資料經處理後，使通訊傳輸得以完成，這些資料爲流量資料之一種，爲指令第6條規範之範疇。然而，除了通訊傳輸所必要之位置資料外，數位行動網路能處理更爲精確的位置資料，而這些資料可提供加值服務所需之資訊，例如：提供駕駛個人化的交通資訊和駕駛方向。對此流量資料外更爲精確的位置資料，指令在第9條另爲規範[239]。

指令第9條的規範限於「非流量資料之位置資料」。公共通訊網路或公共電子通訊服務提供者處理這類位置資料，只能在經匿名化後始能爲之。或者須取得使用者或用戶的同意，在提供加值服務之必要範圍及期間內始得爲之，且服務提供者必須在取得同意前，告知用戶或使用者以下事項：（1）將處理的位置資料種類、（2）處理的用途及期間、（3）爲提供該加值服務，該資料是否會傳輸至第三者。此外，在取得使用者或用戶處理位置資料之同意時，必須讓使用者及用戶有機會能隨時撤銷其先前之同意[240]，並得繼續以簡單且免費的方式，在每一網路連結或每一通訊傳輸時，暫時地拒絕位置資料的處理[241]。同樣地，第9條亦限制只有經公共通訊網路、公共電子通訊服務提供者或提供加值服務的第三者授權之人員，且必須爲提供加值服務的必要

[238] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 26-27。

[239] 請參考 Directive 2002/58/EC 立法說明第（35）點.

[240] Art. 9 para. 1.

[241] Art. 9 para. 2.

範圍內，才能處理位置資料[242]。

（2）美國1996年電信法中之行動通訊與位置隱私（Location Privacy）

美國1996 年電信法(Telecommunications Act of 1996)中與隱私最相關的，就是Ttitle VII 的第222 條關於消費者資訊隱私之規定。每家電信傳輸業者有責任保護該電信傳輸業者及其他電信傳送業者、設備製造商、消費者的獨占機密，包含電信傳輸業者轉賣由其他電信傳輸業者所提供的電信服務。在九一一攻擊之後，美國通過「無線通訊與公眾安全法 (Wireless Communications and Public Safety Act of 1999) 」，要求所有在美國境內經營行動電話行動電信之業者，必須在行動電話中安裝GPS，以便定位追蹤。然而消費者消費時，其行動與所在地點亦爲其隱私之一部分，如可隨時被定位，亦有隱私遭受侵害之嫌。就此，2001年參議院提出的「位置隱私保護法 (Location Privacy Protection Act of 2001)」，要求提供無線位置服務的公司於收集位置資訊時，須通報用戶。該法案並禁止未經用戶許可而逕行收集或銷售資訊。[243]

在歐盟立法例部分，1995年公布的「關於個人資料處理以及此類資料自由流動的個人保護指令(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) 」中，即已令要求各成員國應以立法之途徑來管理個人資料，該指令適用於任何有關涉及個人資料之活動，包括蒐集、儲存及發表之行爲，且不論是自動或非自動化的資料蒐集方式。其個人資料定義之範圍則相當寬廣，舉凡足以辨識或可辨識個人身分者皆在內，且不限於文字、圖像、聲音、視像、影訊等。在2002年公布的「電子通訊隱私指令[Directive on Privacy and Electronic Communications (2002/58/EC)]」中，亦確立了以電子通訊中傳輸個人資料的隱私保障，應採技術中立(Technology-neutral)的原則。

[242] Art. 9 para. 3. 此部分翻譯參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 33。

[243] S 1164, Location Privacy Protection Act.

http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp

該指令第九條明確要求電信業者提公有關位置服務時，須符合opt-in consent之要求。而且客戶須能隨時撤回該同意。[244]

有關與位置有關的行動商務，日本的發展更早於美國及歐盟。1998 年郵政及電信部(Ministry of Posts and Telecommunications)公布了行動通訊個人資料保護辦法(Protection of Personal Data in Telecommunications Business)，對於使用位置資訊的客戶同意，建立了一套清楚的標準：行動通訊業者在未經客戶的同意下，不得將其位置資訊揭露予任何第三人。另外，在2003年5月通過的個人資料保護法(Personal Data Protection Law)，也確立了1998 年郵政及電信部的行動通訊個人資料保護辦法對於opt-in consent 的要求。[245]

在上述三個地區之中，日本對於以位置資訊爲基礎的服務活動之發展乃是最蓬勃的。其中一項原因即是因爲這些明確且清楚的法律規定，確實地保障了非緊急性的客戶的位置隱私資訊，也不妨礙此類商業服務之發展。由於位置資訊本身的敏感的特性，所以應該以有別於處理「客戶財產網路資訊(Customer Proprietary Network Information,CPNI)」，包括：時間、日期、通話時間、撥打電話號碼。CNPI 的程序及立法來保護這類的資訊。特別是讓消費者能清楚地知道：當他想購買以位置資訊爲目標的服務時，對於誰可以獲得此類的資訊或何時這些資訊會被揭露等。而法令在此時即扮演一個重要角色：負責提供一個標準，好讓業者、政府和其他相關的人清楚地知道自己的權利義務。通訊業者有很強烈的利益理由來促進這類服務的發展，而政府也有非常強烈的理由來規範這樣資訊的保障。所以這類的立法應達成：消費者如何授權誰得獲取位置資訊的規範：清楚、一致而且是技術中立的目標。[246]

[244] 參考：電子金融服務與付款機制電子化管理規範研究，頁 115-116。

[245] The Personal Information Protection Act (Law No. 57 of 2003), http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.參考：電子金融服務與付款機制電子化管理規範研究，頁 116 及 Jones Day—Personal Information Protection Law in Japan, http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=2920 (last visited on 2009.6.30)

[246] 參考：電子金融服務與付款機制電子化管理規範研究，頁 116-117。

三、用戶資料（subscription data）

用戶資料，係指消費者於通訊服務訂約（subscribe）時，所提供的個人相關資料。例如申請固網電話，用戶所填的申請單，可能須提供用戶姓名、身分證字號、出生日期、住址、戶籍地；如申請人爲法人，亦可能須提供事業登記字號。如用戶的繳費係採金融機構自動扣款，亦須提供金融機構帳戶號碼。在各種用戶資料中，最常見之應用即爲電話簿、查號臺及來電顯示。此外，警察、消防機關及醫護機構在急難救護上，亦常需要查詢用戶資料。[247]

（1）用戶公共名錄

A. 歐盟：電子通訊個人資料處理暨隱私權保護指令（2002/58/EC）（Directories of subscribers）

電子通訊用戶名錄廣泛地公開於大眾，基於自然人個人隱私權和法人對於其法律上利益之保護，用戶或使用者應有權利決定是否將其資料公布於名錄上。並且用戶名錄提供者除應告知用戶將其列於名錄外，並應告知用戶該名錄之目的及電子形式名錄之特殊使用功能，尤其是搜尋功能，例如：反向搜尋功能得讓使用者僅憑用戶的電話號碼搜尋到其姓名和住址[248]。對於用戶名錄，指令於第12條規範如下：

關於公開（或得由名錄查詢服務取得）之印刷或電子形式名錄，在名錄中得收錄個人資料，且以電子版名錄附加的搜尋功能爲基礎，可爲進一步的使用。對此會員國應確保用戶在被列入名錄前能接獲免費之告知[249]。且應確保給予用戶機會決定是否將個人資料收錄於公共名錄中，並確保用戶得修改、更正或取消該資料[250]。再則，上述的規範應適用於自然人之用戶，而會員國亦應確保，在共同體法架構下及可適用的國家立法下，應充分保護非自然人之用戶關於收錄進公共名錄的正當利益[251]。

[247] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 27。

[248] 請參考 Directive 2002/58/EC 立法說明第（38）點.

[249] Art. 12 para. 1.

[250] Art. 12 para. 2.

[251] Art. 12 para. 4. 此部分翻譯參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 34。

B. 台灣：

我國俗稱之電話簿，由於其印刷頁面傳統上係黃色，故又稱爲黃頁簿（yellow pages）。電話簿上所記載之號碼，主要係供一般公眾查詢。與傳統的黃頁簿應用相較，目前開放市場下的電話號碼查詢服務，關於個人資料之使用、揭露、更正，則是較大的問題。在過去，我國電信服務之供給係一家（中華電信）獨占經營，電話簿之印製，查號服務之提供，其中所有可供查詢之電話號碼均由其經營。目前，由於電信業開放經營執照。可以預見，其他電信業者若要印製電話簿或提供查號服務，不可能只以其客戶之電話號碼爲限，而須與其他同業競爭者共同分享資料。但我國電信法中並未規定業者間分享資料之義務或範圍。此外，共享之資料若要維持其正確性、即時性，並確保查詢服務之合法，勢必需要由一組織從事整合之任務，將各家電信業者所持有之資料加以統整，並採中央控管資料的流向，避免因分散管控，導致資料大量外洩，卻無從追究、歸責。[252]

（2）來電身份顯示

在整合式電信服務技術下，電信業者所提供之服務，已不止於提供通話連線。其他附加於通話連線的服務，例如指定轉接、來電顯示、定時鬧鈴等，在日常生活中亦非少見。來電顯示（calling number display, CND），則是其中與個人隱私較有關係的服務類型。來電顯示，在技術上必須國際與國內電信業者間之系統聯結、資料交換均能支援，方能使來電顯示應用普遍化。

對於受話方來說，某些人不願受到不明電話的打擾，因此會希望電信業者能提供來電顯示服務，以供其過濾、選擇是否接聽電話。但從發話方來說，亦可能有某些人希望能在不顯示發話方電話號碼的前提下，與受話方通話。由此可知，來電顯示涉及發話方(caller)不願其發話號碼被受話方(callee)得知的意願，以及受話方要求知悉發話方電話號碼的意願。雙方意願之衝突，應取得平衡。應注意的是，與其他類型的資料所涉及的隱私保護議題不同的是，來電顯示服務並無大量資料外洩的可能，此種特殊的資料應用型態，與

[252] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 27-28。

一般隱私保護議題所要處理的問題有相當差異，而有必要特別加以處理。[253]

A. 歐盟：電子通訊個人資料處理暨隱私權保護指令（2002/58/EC）

指令對於通話的身分顯示賦予用戶或使用者有拒絕顯示的權利，於第8條規分別就「發話線路身分顯示（calling line identification，即一般所謂來電顯示）」及「被連接線路身分顯示（connected line identification）」加以規定如下[254]：

（1）當提供發話線路身分顯示時，服務提供者必須提供發話方使用者（calling user）有機會能使用簡單且免費的方式，以每通電話爲基礎阻止身分顯示。而對於發話方用戶（calling subscriber）亦應以每一線路爲基礎，給予阻止身分顯示的機會。[255]

（2）當提供發話線路身分顯示時，服務提供者應提供受話方用戶機會，使用簡單且免費的方式以阻止來電的身分顯示。

（3）當提供發話線路身分顯示服務且在通話確立前即顯示身分，當發話方預先阻止身分顯示時，服務提供者應給予受話方用戶有機會，使用簡單方式拒絕來電。

（4）當提供被連接線路身分顯示時，服務提供者應給予受話用戶有機會，使用簡單且免費的方式，阻止將被連接線路的身分顯示給發話的使用者。

（5）其中（1）有關來電身分顯示的規定亦應適用於從共同體內撥打至第三國之通話。而（2）（3）（4）規定亦應適用於從第三國撥打進共同體內之通話。

（6）會員國應確保當提供發話連線（或被連接線路）身分顯示服務時，公共

[253] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 28-29。

[254] 此部分翻譯參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 34-35。

[255] Art. 8 para. 1: Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

電子通訊服務提供者應告知大眾此情形，並告知大眾上述規定。

在追蹤惡意或騷擾電話，或爲加速提供緊急服務，對於身分顯示之保護，指令亦設有例外之規定。指令第10條規定，會員國必須確保有透明的程序，以管理公共通訊網路（或公共電子通訊服務）提供者在下述例外情形時限制用戶或使用者隱私權保護之方法：

（1） 當用戶申請要求追蹤惡意或騷擾電話時，公共通訊網路（或公共電子通訊服務）提供者得暫時地不顧慮排除來電身分顯示的情形。而在此況下，依據國家法律規定，有關發話用戶的身分資料將被儲存，並由公共通訊網路（或公共電子通訊服務）提供者提供；

（2） 爲回應緊急電話，對於處理緊急電話之組織，公共通訊網路（或公共電子通訊服務）提供者，以每一線路爲基準，得不顧慮（1）排除來電身分顯示（2）暫時拒絕或未同意處理位置資料之情形。這些組織包含執法機關、救護服務及消防隊。[256]

四、總和統計資料（aggregation data）

總合統計資料，係指通訊業者於蒐集上述的訂約資料、流量資料、位置資料後，將資料中可確認個人身分的部分去除（de-identification），再將所有的資料匯總加以分析，做爲經營決策的參考。嚴格來說，總合統計資料已經非個人資料。但倘若總合統計資料去個人化的過程有瑕疵，可能使得個人資料被混雜在總合統計資料中被外洩。縱使資料去個人化的過程沒有瑕疵，倘若總合統計資料可以藉由交互查詢，與其他資料比對，仍有可能將總合統計資料回復爲個人資料，而找出特定人的個人資料。[257]

[256] 此部分翻譯參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 35。

[257] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 29。

第四項 2006 電子通訊資料保存指令

2006 年 3 月 15 日，歐洲議會提出「電子通訊資料保存指令」[258]。此一指令修正了歐盟 2002 年第 58 號有關個人資料處理與隱私保護之指令（Directive 2002/58/EC），強制公用電信事業經營者及網際網路服務提供者留存如發話號碼、用戶身份、某一 IP 位址之用戶身份個人資料，6 個月至 2 年的時間。其主要目的爲確保被留存的資料得於調查、偵查與告發重大犯罪時所利用。該指令於 5 月底生效，會員國應於 2007 年 9 月 15 日前完成轉置。該指令認爲各會員國得依本指令第五條（資料之範圍及定義）、第六條、第八條及第九條等規定爲個人資料揭露時應遵循民主社會的必須（Necessary）、適當（Appropriate）及比例（Proportionate）等原則，在符合特定公益目的（包括國家安全、公共安全防衛或基於防堵、調查、偵查及起訴有關刑事犯罪或未經授權利用電子通訊系統等原因）下爲之[259]。該指令第六條並明確規範基於特定目的保存個人資料爲一定公益之利用最長不得超過 24 個月；第八條規定了當有權機關調閱該等資料時，公用電信事業及網際網路服務提供者不得無故拖延（undue delay）；第九條則規定對於上述事項各會員國應設立專責監督機構。

在規範之目的與範圍部分，本指令之目的，主要是統合歐盟會員國賦予其國內電信業者或網路服務提供者，對所擁有通訊資料保存的義務，以確保這些通聯資料能即時被利用於協助檢警進行重大犯罪偵查與起訴。本指令所適用之範圍，僅包含所有自然人或法人之通聯資料與位置資料，以及其他用來識別發話者與受話者所必須的資料；並不得適用於通訊實質內容之保存。

[258] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[259] Article 15（1） of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of he rights and obligations provided for in Article 5, Article 6, Article 8（1）, （2）, （3） and （4）, and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security （i.e. State security）, defense, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications systems.

在資料保存內容部分，依其保存項目之不同，主要分爲 6 大類：（1）追查與識別通訊之資料；（2）識別通訊地點之資料；（3）識別通訊日期、時間與通聯時間長短之資料；（4）識別通訊類型之資料；（5）識別用戶所使用之溝通器材及可能使用器材之資料；以及（6）識別行動通訊位置之資料等。

以固定與行動電話通聯爲例，資料保存之內容包含發話者與受話者之電話號碼、姓名與地址、通話日期及起迄時間、所使用的通訊服務類型等等。對於行動電話的部分，額外需要紀錄發話者與受話者之國際行動使用者識別碼（IMSI）與國際行動裝置識別碼（IMEI）。若通話者所使用之行動電話，乃透過不知名的預付系統（預付卡）進行通聯時，則業者必須記錄該行動電話通話時之發話位置。網路提供者對於網路使用、電子郵件與網路電話的資料保存內容，則大致包含用戶 ID、發話者與受話者之姓名、地址、電話號碼，以及發話時之 IP 位址等。另外，尚須記錄網路使用者所使用之網路類型（如透過 xDSL 或 Cable）及所使用之網路服務（如是否使用其他加值服務）等。

在資料的保護與銷毀方面，依據本指令第六條之規定，各會員國需確保上述資料得保存 6 個月以上，但最多不得超過 24 個月。保存之資料因涉及人民隱私，若不慎外洩或被不當利用，將造成人民隱私的重大侵害，且影響程度不亞於即時通訊遭攔截所造成之侵害，故本指令特於第七條要求，對於被保存資料的保護等級，應等同於資料傳輸時的保護。而各國更應積極採取技術上或政策上之措施，以避免受保存之資料遭到有意或無意的遺失、破壞或刪除；而對於超過保存期限的資料，除非有特殊的情況，否則應立即銷毀。爲確保資料得以妥善保存不受侵害，在保存資料的提供與罰則方面，本指令第九條特別要求，各會員國應明確指定相關單位負責監督資料保存與運用之情形，且僅得爲有法律授權之使用者所使用。若有非經法律允許而故意使用或交換受保存之資料者，各國應制定有效且合適的刑罰，以嚇阻惡意或不當利用或儲存之行爲。各會員國除了需保護被保存的資料不被侵害外，更應確保有權使用的機關提出請求時，可即時取得所需之資料而不受到延誤。亦即，各會員國應要求業者，必須確保其保存之資料可隨時配合執法單位之調查而提出，以協助執法單位進行嚴重犯罪與恐怖嫌犯之調查時的參考利用。對於非經法律允許而故意使用或交換受保存之資料者，各國應制定有效且合適的罰則，包含行政處罰或是刑事處罰，以嚇阻受保存之資料遭到不當的利用或

儲存。

針對「電子通訊資料保存指令」，Article 29 Data Protection Working Party 建議認為此一指令對於資料之處理欠缺充分且特定之保護措施。因此建議各會員國應該採取以下幾項標準，制訂一體適用的八項準則：

1、目的特定（Purpose Specification）：公權力要求提供個人資料的目的必須特定。指令中「重大犯罪（Serious Crime）」一詞太過含混，應予以釐清。

2、接觸限制（Access Limitation）：要求提供個人資料的公權力機關應予以特定且必須限於必須因調查、偵查及起訴的機關，並公告周知該等機關的名單給民眾。對於調閱資料之記錄應呈報給監督機關以利有效監督。

3、資料最低調閱（Date Minimization）：資料調閱必須以最低必要為原則並詳列清單。如有清單異動，應採最低必要原則（Strict Necessity test）檢視。

4、資料探勘禁止（No Data Mining）：為調查、偵查及起訴犯罪之需所為之資料蒐集不得進行該資料之進一步探勘以維護民眾自由旅行及使用通信的權利不受犯罪嫌疑之影響。

5、有權接觸機關之司法或獨立檢驗（Judicial/Independent Scrutiny of Authorized Access）：調閱個人資料基本上是屬於個案（Case by Case）審查方式進行，且由特定機關為之並接受監督檢驗。是故，該等機關調閱資料時應詳載特定目的之個案需求及特定範圍資料之調閱。

6、業者保留資料之目的（Retention Purposes for Providers）：業者在保存客戶資料時，除因應公權力機關之特定需求目的外，不得以其他理由進行客戶資料之不當留存（Retention）。

7、系統分離（System Separation）進行因公權力機關需求為目的的客戶資料系統應與業者自行以商業目為資料儲存的系統分離。

8、安全維護（Security Measures）：指令中應更進一步對於資料留存

（Data Retention）的要求做規定，並要求業者對於技術及組織上的安全維護措施訂定依循的最低標準。

由於電子通訊資料保存指令的訂定，明顯增加電信與網路服務提供者的負擔，若政府單位未提供補助或透過租稅減免的方式提供協助，這些成本勢必會轉嫁至電信及網路使用者身上，造成用戶費用的提高，進而引起民眾之反彈[260]。故爲使「資料保存指令」推動更爲順利，歐盟學界與實務界均建議，歐盟會員國將本指令落實於該內國法律時，應考量到如何對業者進行補助，避免業者將額外之費用轉嫁到用戶身上，增加用戶之負擔。

第五項 電信業者因應相關機關（構）提供用戶資料及其相關法規檢視

一、電信業因應政府公權力對於用戶資料之提供

政府公權力常因犯罪偵查需要而向電信機構要求提供客戶資料，依據電信法第七條規定：

「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。

前項依法律規定查詢者不適用之；電信事業處理有關機關（構）查詢通信紀錄及使用者資料之作業程序，由電信總局訂定之[261]。

電信事業用戶查詢本人之通信紀錄，於電信事業之電信設備系統技術可行，並支付必要費用後，電信事業應提供之，不受第一項規定之限制；電信事業用戶查詢通信紀錄作業辦法[262]，由電信總局訂定之。」

---

[260] 爲配合國家的政策與法規，歐盟國家之電信及網路服務提供者勢必要增購更多的儲存設備，並且增加額外的人力與財力，以儲存並確保這些被保存之資料的安全；而爲避免資料遭遺失或毀損而無法補救，業者甚或需進一步思考是否透過異地備援的方式保存資料，避免因無法即時提供資料而受罰之情事。種種的配合措施，均需要付出額外成本，若政府單位未給予任何的補助或協助，將可能影響此類業者市場競爭。

[261] 電信事業處理有關機關(構)查詢電信使用者資料實施辦法於民國 88 年制訂公布（交通部電信總局電信公八八字第 50679710 號令），並於民國 91 年十二月修訂（交通部電信總局電信公字第 0910510088-0 號令）。本實施辦法中所稱之本辦法所稱使用者資料，係指電信使用者姓名或名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料爲限。詳參閱交通部電信總局相關網址

http://www.dgt.gov.tw/Chinese/Regulations/5.3/5.3.2/Query-user.shtml (最後瀏覽日期 200961.30)。

[262] 電信事業用戶查詢通信紀錄作業辦法已於民國 94 年六月二十四日由交通部電信總局公布。詳參閱交通部電信總局相關網址 http://www.dgt.gov.tw/Chinese/News-press/94/press-dgtnews-94

根據電信服務業者依據交通部電信總局規定的實施辦法所制訂出的處理原則來看，有以下情形時，公權力可向依法向電信事業查詢使用者資料，電信服務業者料以用戶申請各項電信業務所填列之資料爲限，提供一定資料：

1、司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者。

2、其他政府機關因執行公權力所需者。

3、與公眾生命安全有關之機關（構）爲緊急救助所需者。

但針對前(1)、(2）項之情況，公權力之政府機關必須敘明其法律依據。

在有關機關查詢電信通信記錄程序方面：

1、應先考量其必要性、合理性及比例相當原則，並應符合相關法律程序後，再備正式公文或附上電信通信紀錄查詢單，載明需查詢之電信號碼或姓名及其身分證統一編號、電信服務種類、法律依據、案由說明、查詢案號、資料用途、查詢機關(構)、機關(構)主管、連絡人、連絡電話或傳真機號碼、機關(構)加蓋印信及其首長署名、職章等，送該電信使用者所屬電信事業指定之受理單位辦理。對於案由特殊、情況緊急之查詢，得由法官、檢察官或查詢機關(構)之首長或經其授權之主管署名並加蓋職章及連絡人之資料，視同機關(構)正式公文書先傳真之，並經回叫確認爲之，查詢後應於三個工作日內補具正式公文或加蓋印信之電信使用者資料查詢單正本。前述之查詢，經查詢機關與電信事業雙方認證同意，得以經加密之電子郵件爲之，該電子郵件並視同正式公文或電信使用者資料查詢單正本。(實施辦法第五條）

2、查詢通信記錄，須載明欲查詢之電信號碼、通信紀錄種類、起迄時間、查詢依據或案號、資料用途、連絡人、連絡電話或傳真機號碼、及指定之列帳相關資料等，送指定之受理單位辦理。

3. 依實施辦法第八條規定，電信事業處理查詢使用者資料，應以不影響其營運作業，並依受理查詢日期先後之順序爲原則。但案情特殊、情況緊急之查詢，得優先處理。

4. 在查詢相關資料時有關收費方式方面，依中華電信之處理原則：(1) 單向發信通信紀錄：以每頁新臺幣十元計收。(2)雙向通信紀錄：以每號每日新臺幣一百二十元計收，查詢期間不滿一日以一日計收。(3)公權力機關查詢結果

0624.shtml (最後瀏覽日期 2009.6.30)。

後無資料者，仍需計費。法官、軍事審判官、檢察官、軍事檢察官或監察院、審計部及所屬審計機關依法查詢電信通信紀錄者，查詢費用得予減收或免收。

5. 電信機構依不同通信記錄，都有不同保存時限，提供資料僅在仍在保存期限內提供。在第一類電信事業通信紀錄之保存期限：(1)市內通信紀錄：最近三個月以內。(2)國際、國內長途通信紀錄，最近六個月以內。(3)行動通信通信紀錄：最近六個月以內。

對於第二類電信事業通信紀錄，依據交通部民國 94 年所發布的「第二類電信事業管理規則[263]」第 27 條則規定，電信業者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供其資料。業者對屬於語音單純轉售服務通訊紀錄或是網路電話服務通信紀錄者，應保存 6 個月。

在網際網路接取服務部分，對於撥接用戶識別帳號、通信日期、上下網時間紀錄與免費電子郵件信箱、網頁空間線上申請帳號時之來源 IP 位址，以及當時系統時間等紀錄，保存期間均爲 6 個月；ADSL 用戶與纜線數據機用戶之識別帳號、通信日期與上下網時間，以及張貼於留言版、貼圖區或新聞討論群組之內容來源 IP 位址及當時系統時間，則應保存 3 個月；電子郵件通信紀錄則爲 1 個月。

二、對於現行法規適用及個資法修正草案上之探討

針對公權力機關(構)要求電信業者提供客戶資料一節，係屬政府執行公權力的一種行政行爲。一般而言，行政行爲形式係將行爲獨立於具體事實而依程序方法、功能與法律效果所形成的結構。[264]將行政活動分配爲特定的行政行爲形式則須回溯到一體規制行爲前提與法律效果的特別規範基礎之上。如此，才可以解決不斷重複發生的法律問題。[265]

行政行爲之行爲形式原則上依循兩個步驟來建構體系：[266]

---

[263] 交通部交郵字第 09400850511 號令。

[264] P. Krause, Rechtsformen des Verwaltungshandelns, 1974, S. 14.

[265] *Eberhard Schmidt-Aßmann*, Die Lehre von den Rechtsformen des Verwaltungshandelns, DVBl. 1989, S. 533(534).

[266] Vgl. *Eberhard Schmidt-Aßmann*, Die Lehre von den Rechtsformen des Verwaltungshandelns, DVBl. 1989, S. 533 ff.; Fritz Ossenbühl, Die Handlungsformen der Verwaltung, JuS 1979, S. 681 ff.; Walter Pauly, Grundlagen einer Handlungsformenlehre im Verwaltungsrecht, in: Becker-Schwarze/Köck/Kupka/v. Schwanenflügel(Hrsg.), Wandel der Handlungsformen im Öffentlichen Recht, 1991, S. 25 ff.

第一個步驟對於可歸屬爲行政的所有行爲進行法的描述。這個步驟是作爲規範科學的法學對於經驗科學所確定的行爲概念所從事之法的規範性觀察。法學即以從事行爲概念之法的觀察與分析來對於行爲事實進行法的認識、判斷與操控。行政行爲在這樣的理解下，即是所有國家可規範歸屬行政之機關管理人行爲[267]

又如上所述，行政行爲之行爲形式理論脫離行政行爲之複雜事實擷取重要的個別要素，並分析其在行爲關連性的意義。[268] 公法學者在行爲概念下，整理了所有公法秩序的行爲類型。最重要的行爲形式被以高度抽象的概念呈現，以擔保其在眾多行政領域之所有個案中可以被適用。[269] 行爲形式將被定義、與他行爲形式區隔、賦予程序法的意義與提供正確權利救濟的分配[270]。

第二個步驟是分配特定行爲形式的法之要求與法律效果。這個步驟在建構行政所受法規範之拘束性與合法違法之法律效果體系。一般在這個步驟，會被討論的包括行爲形式的容許性、形式與實質的合法性及其所生的法律效果問題。然後就是相對人民的權利保護與行政行爲司法監督的問題。這些內容便結構了行政之行爲形式體系。

循著此一思考模式，要求資訊服務業者提供客戶資料，在行政法上之觀察，依序爲：有無要求資訊服務業者提供客戶資料的授權；有權要求資訊服務業者提供客戶資料之行政機關的行政行爲形式的選擇；組織、程序與方式等形式合法性的要求；行爲內容之實質合法性的要求等，其詳述如下：

一、有無要求資訊服務業者提供客戶資料之授權基礎

行政機關要求業者提供客戶資料之行爲同時涉及了「客戶」之資訊自決權與電信業者之工作權與財產權。故依憲法第廿三條規定之意旨，僅在法律

[267] Walter Pauly, Grundlagen einer Handlungsformenlehre im Verwaltungsrecht, in: Becker-Schwarze/Köck/Kupka/v. Schwanenflügel(Hrsg.), Wandel der Handlungsformen im Öffentlichen Recht, 1991, S. 25 (29).

[268] *Eberhard Schmidt-Aßmann*, Die Lehre von den Rechtsformen des Verwaltungshandelns, DVBl. 1989, S. 533.

[269] *Eberhard Schmidt-Aßmann*, Die Lehre von den Rechtsformen des Verwaltungshandelns, DVBl. 1989, S. 533(534).

[270] Water Pauly, Grundlagen einer Handlungsformenlehre im Verwaltungsrecht, in: in: Kathrin Becker-Schwarze/Wolfgang Köck/Thomas Kupka/ Matthias von Schwanenflügel (Hrsg.), Wandel der Handlungsformen im Öffentlichen Recht, 1991, S. 25.

明確規定或法律明確授權行政機關制訂法規命令，始得對之予以適當地限制。故在具體個案中，第一個思考的是：有無法律之具體授權？對此，針對行政機關要求資訊服務業者提供客戶資料之行爲所稱之法律授權，應同時具備對於「客戶」之資訊自決權與電信業者之工作權與財產權限制的雙重授權。

關於前者之授權，涉及個人之資訊自決基本權，對於個人資料的蒐集、處理與利用，有所謂「附許可保留的禁止（Verbot mit Erlaubnisvorbehalt）」之一般原則。易言之，法律以「規則—例外」關係的方式來呈現。即，除例外的被許可外，他人對於個人資料的處理，原則上是不被容許的。對此，德國聯邦資料保護法第四條第一項規定：「個人資料之蒐集、處理與利用僅於本法或其他法律許可、命令或當事人同意，始得爲之。」相對於此，我國電腦處理個人資料保護法第六條僅規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」又該法第七條復規定：「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，不得爲之：一、於法令規定職掌必要範圍內者。二、經當事人書面同意者。三、對當事人權益無侵害之虞者。」第八條規定：「公務機關對個人資料之利用，應於法令職掌必要範圍內爲之，並與蒐集之特定目的相符。但有左列情形之一者，得爲特定目的外之利用：一、法令明文規定者。二、有正當理由而僅供內部使用者。三、爲維護國家安全者。四、爲增進公共利益者。五、爲免除當事人之生命、身體、自由或財產上之急迫危險者。六、爲防止他人權益之重大危害而有必要者。七、爲學術研究而有必要且無害於當事人之重大利益者。八、有利於當事人權益者。九、當事人書面同意者。」足見其對於當事人個人資料之保護顯然不足。又對此，電腦處理個人資料保護法修正草案雖在其第五條修正爲：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法爲之，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。」但仍與「附許可保留的禁止」的要求有著一段距離。

又針對公務機關對於個人資料之蒐集、儲存、變更、利用，乃至於傳遞，什麼樣的個人資料保護之一般性規定，始能有效保護人民之資訊自決權？對此，德國聯邦個人資料保護法第十三條、第十四條與第十五條，分別就公務機關所爲之個人資料蒐集、儲存、變更、利用，乃至於傳遞，分別針對「直

接目的」與「爲其他目的」所容許之資料蒐集、儲存、變更、利用，乃至於傳遞行爲爲明確的規定，其規定如下：

德國聯邦個人資料保護法第十三條規定:「(1) 個人資料之認識於有關機關任務達成所必要者，得蒐集之。(1a) 法律有課予該機關報告義務或依其自願交付之規定者，得蒐集非由當事人而是由非公務機關之第三人所提供之個人資料。(2) 特殊個人資料蒐集(第三條第九項)有下列情形之之一者，始得爲之：1. 法律對其預爲規定或基於重要急迫之公益理由所必要者；2. 當事人依第 4a 條第三項之條件同意之;3.其對於當事人或第三人生命之重要利益所必要者，而當事人就生理上與法律上之特殊原因，無法爲同意者；4. 當事人已公開之個人資料；5. 公共安全重大之危害防止所必要者；6. 防止對於公共利益有重大危害或實現重大公益所急迫必要者；7. 衛生行政，就健康照護、醫療診斷之目的，所爲健康照護與治療所必要及經由醫事人員或其他人員，於守密義務下，所爲之資料處理者；8. 學術研究進行之必要，且研究計畫進行之學術利益大於當事人排除資料蒐集之利益，且研究目的，無法或僅得以不合比例之支出達成者；9. 有國防之急迫原因，或聯邦公務機關爲履行超國家或國家間之危機處理、阻止衝突領域或人道措施義務所必要者」

德國聯邦個人資料保護法第十四條規定：「(1)個人資料對於有關機關所管轄任務之完成所必要，且得達成資料蒐集之目的者，得儲存、變更或利用之。非已爲蒐集之資料，以儲存之目的爲限，始得變更或利用之。(2) 爲其他目的所爲之儲存、變更或利用，於下列情形之一者，始得爲之：1. 法律明文規定或急迫；2. 當事人同意；3. 明顯有利於當事人，且其不存在有對於其他目的之認識不爲同意之理由；4. 由於事實上的切入點存在著不正確，當事人所爲之說明必須被審查；5.爲一般取得或有關機關可得公開之資料，除當事人就目的變更之排除具有較大之值得保護的利益,；6. 對於公共利益有重大不利或公共安全有重大危害之防止或實現重大公益所必要;7. 對於犯罪行爲或違反社會秩序之行爲的訴追、刑罰或刑法第十一條第一項第八號所指之措施或青少年法院法所指感化教育的執行與強制執行或罰金決定之執行所必要；8. 對於他人權利嚴重影響之防止所必要；9. 學術研究進行之必要，且研究計畫進行之學術利益大於當事人目的變更排除之利益，且研究目的，無法或僅得以不合比例之支出達成者；(3) 不違反當事人之優先保護之利益

下，有關機關所為監理與監督權或審計之實施，組織調查之進行，非為其他目的處理與利用。此亦適用於教育與考試目的有關機關之處理或利用。(4) 資料保護監督、資料保全或普通企業保全之資料處理中心所儲存之個人資料，僅得依該目的利用之。(5) 為其他目的之特殊性質（第三條第九項）個人資料的儲存、變更或利用，有下列情形之一者，始得為之：1. 第十三條第二項第 1 至 6 號或第 9 號所得蒐集之條件具備者；2. 學術研究進行之必要，且研究計畫進行之學術利益大於當事人目的變更排除之利益，且研究目的，無法或僅得以不合比例之支出達成者；依第二句中所謂之公共利益衡量，應特別顧及研究計畫之學術利益。(6) 對於第十三條第二項第 7 號所指目的之特殊性質(第三條第九項)個人資料的儲存、變更或利用，第十三條第二項第 7 號所指人員有守密義務。

德國聯邦個人資料保護法第十四條規定：「 (1)公務機關之個人資料傳遞，有下列情形之一者，始得為之：1. 依資料被傳遞之第三者或傳遞機關職權所存在任務之履行所必要者；2. 符合第十四條得為利用之條件者；(2) 傳遞之容許性，傳遞機關承擔責任。基於資料傳遞第三者之請求所為之傳遞，其承擔責任。此類事件，除有傳遞許可之特殊原因外，傳遞機關僅審查，傳遞之請求是否為受資料傳遞之第三者的任務之內，第十條第四項不適用之。(3) 受資料傳遞之第三者，得就該傳遞所欲履行之目的處理與利用資料。為其他目的之處理與利用，僅在符合第十四條第二項之條件者，始得為之。(4) 對於公法宗教團體之個人資料的傳遞，於確認已具被資料保護措施下，第一至三項適用之。(5) 與依第一項得為傳遞之個人資料有關之當事人或另一第三人不可分割或須付出無法接受之支出始得分割之進一步的個人資料，當事人或第三人守密之權利利益非具有明顯優勢者，亦得傳遞之。但此一資料之利用，不得為之。(6) 第五項之規定，對於個人資料於公務機關內部之轉移，準用之。」

相對於此，我國電腦處理個人資料保護法第七條：「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、於法令規定職掌必要範圍內者。二、經當事人書面同意者。三、對當事人權益無侵害之虞者。」與該法第八條：「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得

爲特定目的外之利用：一、法令明文規定者。二、有正當理由而僅供內部使用者。三、爲維護國家安全者。四、爲增進公共利益者。五、爲免除當事人之生命、身體、自由或財產上之急迫危險者。六、爲防止他人權益之重大危害而有必要者。七、爲學術研究而有必要且無害於當事人之重大利益者。八、有利於當事人權益者。九、當事人書面同意者。」不論在個人資料之蒐集、處理與利用的規定未臻明確，對於資料傳遞之規定更付之闕如。至於，個人資料之蒐集、處理與利用的目的拘束、必要性要求與公務機關之衡量義務亦未有所規定。

又就個人資料保護法之性質而言，其實質上僅具有國家侵犯資訊自決權行爲之「援助法律（Auffanggesetz）」的地位[271]，即在法律未針對個人資料保護之特別規定時，始適用該法律。對此，基於規範清晰性（Normenklarheit）與比例原則（Verhältnismäßigkeit）有必要就領域之特殊性爲特別之個人資料保護規定。個人資料之處理規則得因此具體地、個別地、且正確地針對特殊行政任務之規範領域確定之。也由於個人資料保護法同時適用於所有行政領域，也因此有其界限。作爲一般程序法，其僅侷限在就個人資料處理之一般性原則而爲規定。具體的資訊程序，則交由具有領域特殊性之資料保護規定來規範，始能給予適當的方向。而此等性質之基本原則，如必要性、目的拘束性等，也建構出所謂個人資料處理之合法性基準。

由此可知，國家應盡可能針對不同領域之特殊性，規範出不同需求的所爲之個人資料保護相關法律規定。然而此種針對領域特殊性所爲之個別資料保護法的規範模式，在我國之立法技術上，仍未有所見。在未來，應鼓勵不同行政機關，就其個別行政任務之特殊性，制訂出符合該法領域之資料保護規範。而國家個別具體侵犯資訊自決權的行爲，也應由個別領域之「專法」來予以規定，始能作出較佳的法規範形成。

又顧及到「特殊性（Spezialität）」原則，關於資料處理與利用之許可構成要件，應優先從個別領域(bereichsspezifische)之相關資料保護規定觀察之[272]。我國雖未有所謂領域特殊性之資料保護規定，但對於個別具體之侵

[271] Vgl. Gola/Schomerus, BDSG (2002), § 1 Rn. 16. ; zu § 15 Rn. 6 BDSG ; Simitis, in: ders ., BDSG (2003), § 1 Rn. 107; zu § 15 I BDSG.

[272] 德國從 1980 年 8 月 16 日制訂之通報權框架法、1980 年 8 月 18 日制訂之社會法第十冊（

犯資訊自決權行爲，則多針對不同的行政任務，於特別法中有個別的授權。此種授權，或直接課予個人法律上承擔事實釐清之協力義務（Mitwirkungspflichten）；或授予行政機關資訊取得（Informationserhebung）、處理、利用與傳遞之權限。

以前者而言，包括當事人之申報義務（Anzeigepflichten），如公平交易法第十一條針對事業結合，向中央主管機關提出申報之義務；所得稅法等相關規定之納稅義務人稅捐繳納申報義務；銀行法中持股變動及設定質權與銀行虧損申報義務；金融控股公司法第十六條之同一人或同一關係人持有金融控股公司有表決權股份總數超過百分之十者之申報義務；針對第三人有時亦有申報義務之課予，如洗錢防制法第七條之「金融機構對於達一定金額以上之通貨交易」與第八條之「金融機構對疑似洗錢之交易」，向指定機構申報之義務等；又針對第三人有所謂的說明義務（Auskunftspflichten）與提供資料，包括帳冊（Buchführungs-）與報告（Aufzeichnungspflichten）等義務，如公平交易法第二十七條第一項與銀行法第四十五條之規定，但針對第三人之義務，均相對伴隨著行政機關之的陳述意見與提供資料請求權。

針對於行政機關要求業者提供客戶資料之授權，除電腦處理個人資料保護法第七條針對公務機關對個人資料之蒐集或電腦處理之概括授權外，個別行政法對於第三人之說明與資料提供義務各有其特別授權，如行政程序法第四十條針對行政機關之職權調查規定：「行政機關基於調查事實及證據之必要，得要求當事人或第三人提供必要之文書、資料或物品。」其他個別的法規授權，如稅捐稽徵法第三十條第一項：「 稅捐稽徵機關或財政部賦稅署指定之調查人員，爲調查課稅資料，得向有關機關、團體或個人進行調查，要求提示有關文件，或通知納稅義務人，到達其辦公處所備詢，被調查者不得拒絕。」；公平交易法第二十七條第一項第二款：「公平交易委員會依本法爲調查時，得依左列程序進行：二　通知有關機關、團體、事業或個人提出帳冊、文件及其他必要之資料或證物。」；通訊保障及監察法第十四條第二項及第三項規定：「電信事業及郵政機關（構）有協助執行通訊監察之義務，其通

社會資料保護）與 1980 年 3 月 6 日制訂之聯邦身份證法起，資料保護法由一般援助法律轉向於針對特殊領域提供個別較佳之法規範的形成。

訊系統應具有配合執行監察之功能。」「協助執行通訊監察之電信事業、郵政機關（構）於執行後，得請求執行機關支付必要之費用。其費額由交通部會同內政部、國防部及法務部定之。」

其他，如監察法第二十六條第一項：「監察院爲行使監察職權，得由監察委員持監察證或派員持調查證，赴各機關部隊公私團體調查檔案冊籍及其他有關文件，各該機關部隊或團體主管人員及其他關係人員不得拒絕，遇有詢問時應就詢問地點負責爲詳實之答覆，作成筆錄由受詢人署名簽押。」又警察職權行使法第十六條針對警察對於個人有關資料之傳遞規定：「警察於其行使職權之目的範圍內，必要時，得依其他機關之請求，傳遞與個人有關之資料。其他機關亦得依警察之請求，傳遞其保存與個人有關之資料。前項機關對其傳遞個人資料之正確性，應負責任。」

又針對授權的基礎，我們又該思考第二個問題：法律應該要規範或授權到什麼程度？

又依司法院釋字第六〇三號解釋之解釋文所示：「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使用有知悉與控制權及資料記載錯誤之更正權。」故國家應擔保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。亦應提供人民對其個人資料之使用得以知悉與控制及資料記載錯誤之更正的法制度。

又「憲法對資訊隱私權之保障雖非絕對，國家仍須符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。」

又國家基於特定重大公益之目的而有大規模蒐集、錄存如同「人民指紋」等個人資料、並有建立資料庫儲存之必要者，則「應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。」[273]誠如許宗力與曾有田大法官之協同意見書所

[273] 對此，解釋理由書復說明：「而爲確保個人主體性及人格發展之完整，保障人民之資訊隱私權，國家就其正當取得之個人資料，亦應確保其合於目的之正當使用及維護資訊安全，故國家蒐集資訊之目的，尤須明確以法律制定之。蓋惟有如此，方能使人民事先知悉其個人資料所以被蒐集之目的，及國家將如何使用所得資訊，並進而確認主管機關係以合乎法定蒐集目的之方式，正當使用人民之個人資訊。」

述：「對人民該項資訊隱私權，國家固非不得以法律限制之，然先決要件之一是，法律必須明確規定蒐集、使用人民資訊之目的，不僅禁止為供未來不特定目的使用而蒐集人民個人資訊，也不許將所蒐集之資訊作法定目的外之使用。蓋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。」

又關於個人資料之傳遞與利用，該協同意見書指出：「電腦處理個人資料保護法第八條明文容許政府機關對個人資訊得為特定目的外之使用，且所規定特定目的外使用之要件，諸如『有正當理由而僅供內部使用者』、『為維護國家安全』與『為增進公共利益者』等，也極為空泛、概括，實際上幾乎與空白授權無異，有使資訊隱私權有關『禁止為法定目的外之使用』之要求淪為具文之嫌。」試想，主管機關原先主張後又否認之「刑事偵查與維護治安」目的，均可輕易在「有正當理由」、「為維護國家安全」與「為增進公共利益者」等不確定法律概念的掩護下重新敗部復活，可見過於空泛、概括之使用目的規定，相較於完全沒有規定，對個人資訊隱私權之危險性並不遑多讓。是系爭規定在目的審查階段，就已難以在憲法保障人民資訊隱私權面前站得住腳。」而為國家安全與公共利益蒐集、使用個人資訊，應要求國家必須以更精確、依個別不同領域的資訊需求與相關情狀，密切剪裁蒐集、使用目的，藉以繩公權力於一定軌道，避免不當侵害人民資訊隱私。

再則，解釋文復要求「主管機關尤應配合當代科技發展，運用足以確保資訊正確及安全之方式為之，並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨。」故進可推知，就所有個人資料之蒐集與利用，亦應採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨。許宗力與曾有田大法官之協同意見書對此進一步闡釋以為：「資訊科技之發達，固使國家得以更快速、方便的自動化方式蒐集、儲存、利用與傳遞個人資訊，但同時也使儲存於國家資料庫中之個人資訊處於外洩或遭第三人竊取、盜用之更大風險中。是基於基本權的保護義務功能，國家有義務採取適當之組織與程序上保護措施，使個人資訊隱私權免於遭受第三人之侵害。同時基於當代資訊科技發展之開放性，國家並有義務不斷配合資訊科技發展的腳步，採取隨科技進步而升級之動態性的權利

保護措施，以有效保護人民之資訊隱私權。為確保此項目標之達成，國家所採取組織保護措施並應包括設置獨立、專業之資訊保護官(類似機制)，以幫助在資訊科技洪流中不具有自保能力之一般人民保護其個人資訊安全。」

又依大法官釋字第四四三號解釋理由書之意旨:「憲法所定人民之自由及權利範圍甚廣，凡不妨害社會秩序公共利益者，均受保障。惟並非一切自由及權利均無分軒輊受憲法毫無差別之保障：涉及人民關於剝奪人民生命或限制人民身體自由以外之其他自由權利之限制者，亦應由法律加以規定，如以法律授權主管機關發布命令為補充規定時，其授權應符合具體明確之原則。因此，對於個人資訊自決權乃至於持有個人資料之第三人之限制，得以法律授權主管機關發布命令為補充規定。只是，特定之授權法律規定，賦予行政機關那些權限，又其得課予相對人民那些義務？這是「授權明確性」的問題。

就此，交通部依據電信法第十七條第二項規定訂定「第二類電信事業管理規則」，該規則第二十七條第一項與第二項規定：「經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。前項電信內容之監察事項，依通訊保障及監察法規定辦理之。」有疑問的是：電信法第十七條第二項規定是否有為課予「經營者」「提供『客戶』資料」義務之授權？

還觀電信法第十七條第二項之規定亦僅規定：「第二類電信事業營業項目、技術規範與審驗項目、許可之方式、條件與程序、許可執照有效期間、營運之監督與管理及其他應遵行事項之管理規則，由交通部訂定之。」若依釋字第五三八號解釋，或可依法律整體解釋，推知立法者有意授權主管機關，就第二類電信事業者登記之要件、電信事業及其從業人員準則、主管機關之考核管理等事項，依其行政專業之考量，訂定法規命令，以資規範。但若涉及第二類電信事業者之財產權與營業自由之重大限制，為促進第二類電信事業者之健全發展並貫徹憲法關於人民權利之保障，仍應由法律或依法律明確授權之法規命令規定為妥。因此，該規則第二十七條第一項與第二項規定:「經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。」之規定，實應在電信法明定或明確授權交通部制訂法規命令，但關於人民行為或不行為的義務，受規範者之行為準則，個案事實是否屬於法律所欲規範之對象，應使一般受規範者所得預見（釋字第四三二號、第五二一號、第五九四號解釋參照)，若法律就電信監理關係之內容授權以命令為補充

規定者，其授權應具體明確，且須爲受規範者所能預見（釋字第五二四號解釋參照）。始符合法律明確性或授權明確性之人民「預見可能性」的要求。

除上述有關實質合法性之要求外，仍之規定必須注意程序合法性之要求。程序上，資訊自決權被侵犯之當事人與利害關係人之通知、當事人同意與否與當事人陳述機會是否給予。對此，我國現行電腦處理個人資料保護法對於公務機關或非公務機關從事個人資料蒐集、處理與利用的「程序」要求付之闕如，對於個人之資訊自決權之保護顯有不週[274]。

第六項　近期國內發生之案例

一、員警勾串徵信業者違法監聽 名人隱私不保[275]

臺灣板橋地方法院檢察署與刑事局、台北市刑警大隊共同破獲一個暴力討債集團。該集團透過徵信社，向電信業者員工以及松山分局的員警，以一筆新台幣二千元的代價購買個人資料。檢方偵訊十四名嫌犯，其中彭姓員警以十萬元交保，五名徵信業者則遭到聲押[276]。 本案涉及違反電信法第56條之

[274] 因此，電腦處理個人資料保護法修正草案第八條規定：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。有下列情形之一者，得免爲前項之告知：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。五、當事人明知應告知之內容。」

[275] 電信法第 6,7,56.1 條 ・中華民國刑法第 132,133,315.1,318.1 條 ・通訊保障及監察法第 2,24 條 ・電腦處理個人資料保護法第 7,8,18,23,33,35 條 ・法務部 (84) 檢 (二) 字第 0552 號
・臺灣高等法院暨所屬法院 84 年度法律座談會 刑事類第 8 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 19 號 ・電話竊聽、盜打真方便？ 電信箱輕易打開法源編輯室 / 2007-05-18

[276] 板橋地檢署日前接獲線報，指稱蔡姓男子及其手下涉嫌接受國內各大徵信業者委託，佯裝成中華電信員工，謊稱要修理電話，進入徵信社業者所提供的電話裝機地點，破壞電信箱後，夾線竊錄，每線收費四千五百元，錄滿每卷再收六百元，從民國九十五年迄今，不法所得高達三百五十五萬五千元，而違法監聽的對象還包括部分藝人和名人。檢警監控過程中，發現松山分局有員警與徵信業者有所聯繫，進而查出勾串不法。由於時值「靖紀專案」期間，刑事局在掌握有員警涉案後，即展開監控，並會同北市刑大偵五隊共同行動。板檢指出，台北市政府警察局松山分局彭姓偵查隊員與在遠傳電信上班的鄭姓員工，涉嫌違背職務販售民眾戶籍、車籍、出入境或電信基本資料給徵信業者，謀取不法利益。台北市警察局指出，去年十二月就發現彭姓員警涉案事實，因此，主動將線索提供給檢方，在彭姓員警交保後，已經先將他調到警備隊，等待後續偵辦，再做懲處。 檢警發動搜索同時，赫然發現竟有某一媒體記者正和業者「泡茶」，檢警也不排除有媒體與徵信業者掛勾，取得藝人、名人資料作爲跟蹤偷拍爆料依據。板檢強調，這次搜索共帶回二十二人偵訊。

1、通訊保障及監察法第24條第1項及第3項、電腦處理個人資料保護法第33條及刑法第132條第1項洩漏國防以外秘密等罪嫌，情節重大，檢方將深入追查，擴大偵辦。

二、行動電話個人資料安全 消保會將嚴格把關[277]

行政院消費者保護委員會（以下簡稱行政院消保會）日前接獲民眾申訴其身分資料遭冒用申辦行動電信預付卡門號，甚至因此被警方列爲犯罪嫌疑人，建議加強對電信業門號申辦者身分資料查證及把關責任云云。行政院消保會遂於 96 年 12 月 4 日上午邀集主管機關國家通訊傳播委員會（以下簡稱通傳會）、內政部警政署（以下簡稱警政署）、中華電信公司等九家電信業者及全虹、震旦等電信通路業者召開會議，除確認各電信業者因應可攜式門號規劃之「來電答鈴」識別語音均已建置完成外，並請各電信業者對消費者因常接到舊用戶親友來電造成困擾之情形，免費更換其他門號之服務。對冒用身分資料申辦行動電信門號部分，則請業者對所屬經銷商（加盟店）應定期及不定期查察是否落實申辦者須以本人雙證件正本辦理行動電話門號之申裝業務，如發現未依規定辦理者，應立即終止合約。

有關行動電信門號申辦作業規定,各電信業者表示對所屬合約經銷商(加盟店）之門市均會進行經常性定期及不定期之查察，或委託外聘公司進行私下查訪，了解有無落實申辦者證件審核工作，行政院消保會已要求渠等將 96 年度 1 至 11 月份查核資料送該會以作爲督導考核之參考。與其他行業相較，電信相關的個人資料管控流程已屬嚴格．然仍然發生上述新聞案例之情事，多屬人爲疏失及欠缺有效稽核流程所致．

第七項 小結

隨著日常生活中電子通訊活動日漸頻繁，資訊安全也成爲受到關心的議題，因爲缺乏安全的通訊環境，除了造成用戶使用信心的不足，與服務提供

[277]標題：個人資料安全 免驚～～行動電信門號申辦嚴格把關！新聞出處：行政院消費者保護委員會中華民國刑法第 210,212,216,217 條 ・行動通信業務管理規則第 35,72-74 條 ・行動通信業務管理規則第 76,77 條 ・行動電話業務營業規章範本第 1 條 ・院解 字第 3915 號 ・70 年 台上 字第 1107 號 ・95 年 訴 字第 1490 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 4 號 ・個人資料外洩引發詐騙 法務部：修法重懲 / 2007-12-18

者經濟上的損失，對於用戶隱私的侵害，也是不言可喻。資訊安全的目的在於保護資料的機密性(即確保只有經授權人才可接觸資訊)、完整性(即確保資訊與處理方法的完整與正確)與可用性(即確保資料於有需要時能加以存取)。在關於個人隱私保護上，保護資訊安全可保障個人資料完整性、免於遭到未經同意的使用與通訊過程中不受到干擾。現行個資法就個人資料之定義並不明確，並無法爲有效之保護，除列舉規定之自然人之姓名、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、財務情況較容易爲清楚之描述外，「社會活動」與「其他足資識別該個人之資料」之概括規定似乎仍不夠具體。如以本研究所提之位置資訊與行動電話號碼之部分，在現行法規中並無法有明確之解釋與立論依據。

但如上所述，目前提出之「個資法草案」中第二條第一款之規定[278]，將個人之「聯絡方式」列舉爲個人資料之一，於此可得知行動電話號碼於其保護範疇之內，且位置資料與流量資料，按同條之「其他得以直接或間接方式識別該個人之資料」之規定，於可識別該個人之情況下即受有保護。目前該草案雖尚未通過，但除草案之發展外，從外國立法例[279]之角度而言亦採類似之立場，以歐盟「隱私與電子通訊指令」之規定觀之，其對位置資料與流量資料皆有其保護之限制，故應肯認該兩者資料但於現行個資法下，應屬於「其他足資識別該個人之資料」。目前簡訊行動定位雖係採取 LBS 之技術，但其可透過電信名單爲篩選，更精準的定位收訊人所在之位置，此種行銷方式除可能確知收訊者所在之位置外，當傳輸方式受到攻擊時，即可能洩漏他人之位置資料；且透過其所寄發之簡訊，亦可能得知收訊者之生活範圍與習性，此等零碎式資料如遭有心人士使用，將可能拼湊出許多個人資訊。是故本文認爲對於位置資料是否屬於個人資料之部分，於現今法規範而言雖可能不受保護，但未來科技發展更迅速時，將可能產生更大之侵害，故此部分仍須相關機關加以認定與研討，擬定出相關對策，以保護個人之隱私與安全。目前

[278] 法務部所提出之個人資料保護法草案第 2 條第 1 款規定個人資料係指「自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」。

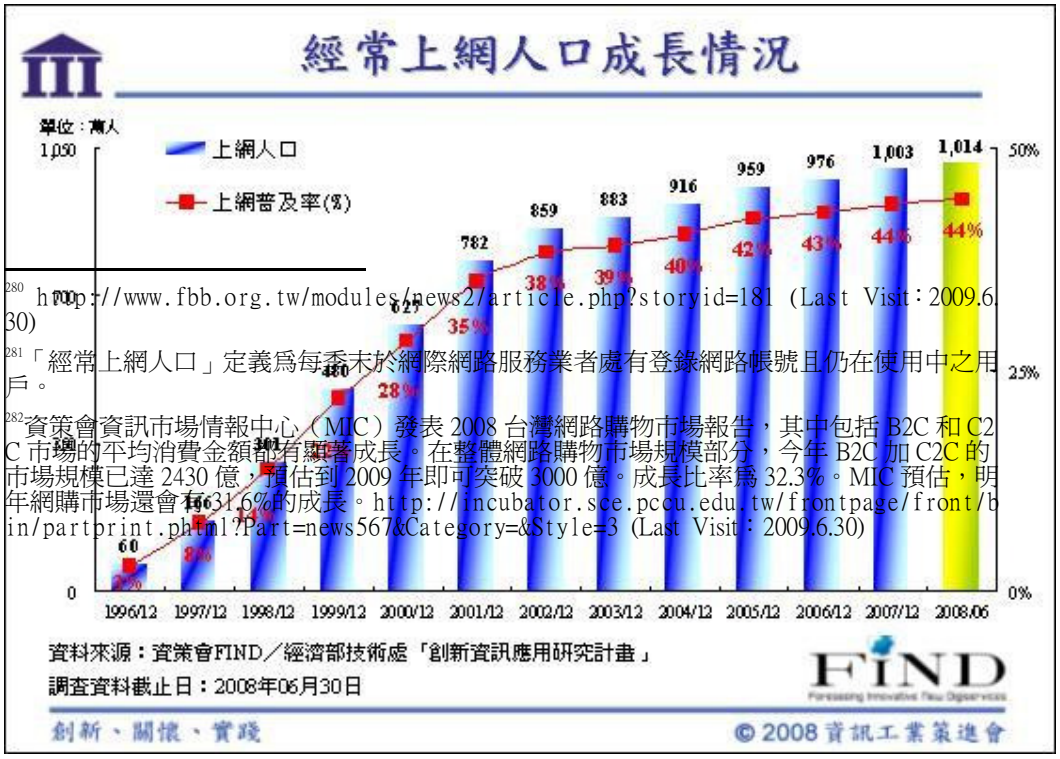
[279] Directive on privacy and electronic communications, DIRECTIVE 2002/58/CE, Article 9 and Article 6, 2002.07.31, p44-45, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF <last visited 2009.6.30>

因電信通訊所產生之資料，尚無管制之方法與規定，以致於此部分仍處於模糊地帶，而從「個人資料保護法草案」之方向似可管理，但是否適當則仍有討論空間。而本文認爲對於資料保護部分，應利用個別立法方式取代施行細則或是行政函釋等方式，始能讓保護更加周詳，以免造成「行政侵害立法」之情況發生。在具體制訂方向方面，建議採取前述有關歐盟「電子通訊資料保存指令」討論之具體八項準則，即「目的特定」、「接觸限制」、「資料最低調閱」、「資料探勘禁止」、「有權接觸機關之司法或獨立檢驗」、「業者保留資料之目的」、「系統分離」、「安全維護」。

第三節 網路購物

第一項、 我國電子商務之發展

近年來，台灣隨著網路基礎設備不斷提升、上網人數穩定成長，電子商務之發展亦隨之日趨壯大。根據 2008 年 6 月資策會 Find 所進行之「我國網際網路用戶數調查[280]」，我國經常上網人口[281]已達 1,014 萬人，而網路上進行之交易更高達 2430 億[282]，預估 2009 年即可突破 3000 億。以下將針對電子商務之交易形態、付費習慣、交易習慣個別介紹說明。



[280] http://www.fbb.org.tw/modules/news2/article.php?storyid=181 (Last Visit：2009.6.30)

[281]「經常上網人口」定義爲每季末於網際網路服務業者處有登錄網路帳號且仍在使用中之用戶。

[282]資策會資訊市場情報中心（MIC）發表 2008 台灣網路購物市場報告，其中包括 B2C 和 C2C 市場的平均消費金額都有顯著成長。在整體網路購物市場規模部分，今年 B2C 加 C2C 的市場規模已達 2430 億，預估到 2009 年即可突破 3000 億。成長比率爲 32.3%。MIC 預估，明年網購市場還會有31.6%的成長。http://incubator.sce.pccu.edu.tw/frontpage/front/bin/partprint.phtml?Part=news567&Category=&Style=3 (Last Visit：2009.6.30)

圖 2：我國網際網路用戶數調查

註、資料來源
資策會

一、 B2C 及 C2C 發展現況

網路交易本源自於學生之間透過電子佈告欄(BBS)上的跳蚤市場或二手市場版所發表之出售訊息，由於 BBS 的操作簡單方便、訊息傳遞快速，逐漸成爲買賣二手商品的重要管道。直到今日，BBS 上的交易活動仍不見式微，甚至成爲目前最爲火紅的團購訊息發佈地。日後 WWW 發展成瀏覽資訊的主流，1995 年美國工程師 Pierre Omidyar 爲了方便收集 PEZ 糖果，意外的開發了 ebay，於是最早的拍賣網站便因此形成。網路交易發展日趨專業，除了拍賣，各式各樣的電子商務網站也因應趨勢產生。根據交易形態，可區分爲 C2C (Customer-to-Consumer)及 B2C(Business-to-Consumer)。所謂 C2C 泛指透過網路公司所設置的交易平台，由消費者自行進行交易，例如：eBay、yahoo 拍賣、露天拍賣等等。拍賣發展初期，商品類型大多以二手商品、收藏品的流通爲主，且以競標的方式交易。當商品的競爭者多時，商品的結標價也就相對高。這樣的交易方式，買方雖想享受了競標的樂趣，但買賣方須等待結標期間截止，才能進行後續付款交貨等動作，對於多相同商品數要出售的賣家而言，並不方便。因此，又產生了「立刻買」(Buy It Now)機制，即買家看到商品，只要賣家提供「立刻買」，就可馬上下標購買，無須等待競標期間結束。透過「立刻買」機制，賣家不但可以快速出售商品，提高物品銷售數，買家也可以在第一時間購得商品。「立刻買」機制的產生，漸漸就形成之後 B2C 網站主要的商品交易機制。而 B2C 是指企業透過網際網路對消費者所提供的商業行爲或服務，如 Amazon、Pchome 線上購物、Yahoo 購物中心。也可說是 C2C 專業化後的另一結果。以 Yahoo 購物中心爲例，2007 年全年度營業額爲七十五億元，2008 年預估即將突破百億，營收規模可望與實體百貨公司並駕齊驅[283]。而 pchome 線上購物也不遑多讓，將產品觸角深入之民生必需品，2007 年 3 月正式推出以「24 小時到貨」號招之嶄新服務，搶佔電子商務大餅。目前這項 24 小時到貨的服務，每個月營收超過 2 億元[284]以上，成功打造出台灣第一個「速度經濟」模式。誰會想到這些柴米油鹽醬醋茶，在台

[283] http://tw.news.yahoo.com/article/url/d/a/081208/78/larnc.html(Last Visit：2009.6.30)

[284] http://event.pchome.com.tw/ipo/invent/2008/in2008_1119.htm(Last Visit：2009.6.30)

灣電子商務業者的努力下，也能有如此的經濟效應。在不景氣下，逆勢創造業績成長，在在顯示台灣在發展 B2C 這一塊，確實已掌握了致勝的 know-how。我們從幾方面來探討台灣 B2C 成功的要素：

- **產品觸角深入各種類**：產品種類夠多，才能讓消費者在第一時間搜尋到想要購買的商品並下單。矛盾的是，如果品項數又像量販店般的多，又會造成消費者得在搜尋結果頁翻頁過多而失去耐心，因此重質的品項種類及搜尋技術就顯得相對重要。

- **吸引人之商品展示圖片**：網路上的商品，摸不到也看不著實體，藉由精美的商品圖片、多角度拍攝、比例尺比對、近拍等等各種方式呈現，提供網友更精準的參考。如 Yahoo 購物中心展示女裝女鞋類商品時，會透過專業模特兒來穿搭服裝、女鞋。

- **網路行銷技術**：透過社群力量影響購物決策、eDM 發送、每日搶標活動、線上資訊展、週年慶。

- **擅用媒體效應**：最有名的例子即為 Payeasy 透過電視美容節目的置入性行銷，成功將自有品牌商品業績推廣。

- **靈活的付款方式供消費者選擇**：尤其為零利率分期付款信用卡刷卡服務，刺激突破網友心中的消費點。

- **快速且 e 化的物流配合**：線上物品即時追蹤、24 到貨服務、18 小時到貨服務。

- **系統化售後機制**：退換貨機制健全、享有七天鑑賞期。

C2C 初期因「競標」及「立刻買」模式，與 B2C 網站產生了基礎結構上的差異。近年來，部分網拍賣家經營朝專業化發展，甚至到最後，造就了新公司或新企業。再加上原本由實體通路轉向虛擬通路的商家，為地毯式的接觸潛在客戶，幾乎都會同時進入 B2C 與 C2C 市場。於是賣家跨界經營的趨勢愈來愈明顯，類 B2C 模式的產生，使得 B2C 與 C2C 的界線漸模糊。

二、 消費者付款習慣

線上購物基於交易方式不同，也導致不同的消費族群在選擇付款方式有

不同的偏好，根據資策會 MIC 研究顯示[285]，B2C 網友整體選擇在「便利商店代收款項」爲主要網購付款方式佔 39.1%，「線上信用卡全額支付」次之，佔 34.2%。而 C2C 主要以「銀行實體 ATM 轉帳/匯款」作爲主要付款方式，佔 46.8%，排名第二名爲「線上 ATM 轉帳」，佔 34.8%，「貨到付款」排名第三，佔 23.7%。不同的交易模式及環境，網友也因此發展出不一樣的付款習慣：

(一) **B2C 網站付款習慣**：

1. **便利商店代收款項：台灣便利商店密集度世界第一，平均兩千七百人就**有一家便利商店，便利商店服務項目越來越多，除了一般銷售，還可以郵寄物品、沖洗相片及代收款。EC 業者看準這點優勢，與便利超商配合，透過行銷包裝[286]，發展便利超商取貨之交易模式。消費者毋須先行付款，只要等待貨到通知，直接至所選定之超商付款取貨即可。此類交易模式，通常用於低單價商品。

2. 信用卡刷卡：根據 AC 尼爾森 2005 年全球消費者線上調查顯示，信用卡爲最受歡迎的線上付款工具。[287]信用卡付款除了擁有「先消費後付款」的好處外，在台灣購物網站業者的努力下，更將信用卡效益發展至極致。與各大發卡銀行合作配合，推出零利率分期付款及信用卡紅利點數折抵。消費者在無須額外手續費的情況下，只有持有信用卡，大多會選擇以信用卡作爲付款方式。

(二) **C2C 網站付款習慣**：

---

[285] 2007 網路購物市場趨勢前瞻 MIC (頁數：16&28)

[286] 會員可於購物網站上，僅需負擔便利商店物流費，即可免費索取商品。

[287] 在網路購物行爲中，**信用卡（59%）及銀行轉帳（23%）成爲全球網購族最常用付款的工具**。但不同國家有不同的付款工具，例如在歐洲的葡萄牙（35%）、希臘（31%）、西班牙（29%）及義大利（28%）等國，貨到付款（cash-on-delivery）是僅次於信用卡的常用的付款方式，而英國則有近一半的網路消費者則是使用簽帳卡。至於在一些亞太地區市場，貨到付款也是一種網購族喜好的付款方式。例如在印度（29%）與日本（25%），貨到付款即是僅次於信用卡付款的另一種常見付款方式。但中國卻很不一樣，最常使用的付款方式是貨到付款（34%）與銀行轉帳（31%）。信用卡（26%）只排名第三，而現金轉帳（23%）則緊接在後。而當被問及偏好何種付款方式時，信用卡（24%）則成爲僅次於貨到付款（32%）的付款方式，這就指出了在中國市場，網路上使用信用卡購物的需求尚未被滿足。

http://tw.cn.acnielsen.com/news/20051101.shtml (Last Visit：2009.6.30)

1. 實體 ATM 與 WebATM：根據 MIC 網拍付款方式資料顯示，ATM(包含實體 ATM 與 WebATM)仍是網友進行網拍交易時，最主要的付款方式。2006 年佔 78.6%，2007 年佔 81.6%，比例逐年增加。但深究其因，主要爲 WebATM 使用率的增長，由原本的 26.3%成長至 34.8%。WebATM 始推出之際，國內金融業網路資訊安全事件頻傳，網友們對於網路 ATM 之信心及安全度仍有疑慮，再加上使用 WebATM 尚須硬體讀卡機支援，因此雖然擁有無須出門即可轉帳之便利性，但仍無法成爲網拍族的最愛。不過近年在銀行業者極力推廣[288]下，短短一年內，網友對於 Webatm 接受度即有明顯的成長。主管機關及銀行公會也密集研討，透過機制有效管控網路轉帳之安全。如「金融卡插拔動作」、「螢幕鍵盤」、金融卡「非約定轉帳」單筆及單日限額等，都產生極佳的防駭防騙效果。

2. 貨到付款及面交：貨到付款及面交皆爲網拍低信任度交易環境下的產物，滿足部分不願先付款後收貨的網友，無須面對收不到物品的風險。但並非所有的網拍賣家都有提供貨到付款服務[289]，再加上此項服務須支付額外的手續費用，故大多用於較高單價之商品。而面交存在區域性問題，如居住在高雄之買家就無法與台北之賣家約定面交交易，因此並非所有交易都適用，主要提供此服務之賣家大多爲非專職賣家[290]。

[288]銀行設置實體 ATM 櫃檯成本不低，因此不少銀行紛紛開發網路 ATM(又稱 eATM 或 WebATM)服務，希望讓持有晶片金融卡的客戶，能夠通過網路 ATM 方式與銀行進行交易，不僅降低銀行運作成本，也透過活動推廣的方式，拉近銀行與客戶的關係，如玉山銀行推出幸福下午茶活動、國泰世華推出免費麥當勞美式咖啡兌換券及轉帳手續費折扣等來拉提各家 WebATM 之市佔率。

[289]貨到付款雖轉移買方收不到貨之交易風險，但相對的，反而提高提供此交易服務賣家出貨被退貨損失運費之風險。因此，提供該服務之賣家比例並不高，主要提供者爲專業出售高單價商品之賣家。

[290]面交耗時且不易掌握買家是否能準時赴約，故專職賣家大多不提供面交服務，但部分有店面之網拍賣家爲服務網友，漸漸衍生出「自取」選項替代面交。

表 1：2006-2007 年網友最常使用之網購付款方式

2007年網友最常使用之網購付款方式

付款方式(%)	2007	♂*所得高	♀*所得高	♂*所得低	♀*所得低
便利商店代收	39.1	24.7	**40.9**	30.4	**49.7**
線上信用卡全額支付	34.2	**54.7**	**53.3**	31.7	28.8
貨到付款	33.9	31.3	30.1	**37.1**	32.4
銀行實體ATM轉帳	31.8	23.4	29.9	31.9	**34.0**
線上ATM轉帳	20.3	21.7	18.7	23.0	18.4

資料來源：資策會MIC，2007年11月

2006-2007年網友網拍最常使用付款方式

付款方式	2006	2007
銀行實體ATM轉帳匯款	52.3%	**46.8%**
線上ATM轉帳	**26.3%**	**34.8%**
現金面交	23.2%	**23.7%**
貨到付款	21.9%	**24.2%**
便利商店代收款項	17.2%	20.3%
郵政無摺存款	17.1%	19.5%

資料來源：資策會MIC，2007年11月

註、資料來源

資策會 MIC，2007 年 11 月

整體來講，不論網友選擇何種付款方式，受詐騙之風險高低取決於受款方。B2C 交易，基於購物網站即爲受款人的特性，網友受詐騙機率幾近於零。但並不代表無任何而 C2C 交易的受款方，相形之下就顯得複雜難以掌握。再加上身分認證機制仍存在無法百分之百正確核對之問題，網拍交易風險明顯較高。雖「貨到付款」及「面交」付款方式可規避掉大部分之詐騙，但由於詐騙手法不斷翻新，目前也已發生多起利用貨到付款所進行的交叉詐欺[291]。面交也曾爆發過當面搶劫等人身安全問題。網友在進行網拍交易時，都應格外提高警覺。

三、 交易方式

快速方便簡單，是電子商務的特性。基於人民特定的需求，經過長期的慣性，逐漸成爲人們購物的習慣，且比例逐年增加當中。B2C 與 C2C 交易方式亦有所不同，下面就針對台灣目前幾個網購及拍賣網站分別說明其交易方式及流程：

(一) Yahoo！奇摩購物中心：

步驟 1：登入帳號，如首次使用該購物網站，須先註冊成爲會員才能使用網站購物。Yahoo！購物中心此頻道目前是由興奇科技所經營，透過技術上的結合，一般網友只要有 Yahoo 帳號，就可以使用同一帳號登入 Yahoo！奇摩購物中心。以 Yahoo 網站在台灣之到達率來看，確實大大降低了網友須註冊才可購物之門檻。

步驟 2：點選”我要購買”按鍵。(如無執行步驟 1，在步驟 2 後將會強制要求執行步驟 1)

步驟 3：選擇付款方式。提供 ATM 轉帳及信用卡付款。ATM 轉帳是採用

[291] 詐騙歹徒是用假信用卡去訂貨，然後直接請郵購公司將買家所訂貨品寄達，買家以爲已經收到貨，所以就貨款匯錢給詐騙者。http://sypp.tcpd.gov.tw/cgi-bin/SM_theme?page=47e89489(Last Visit：2009.6.30)

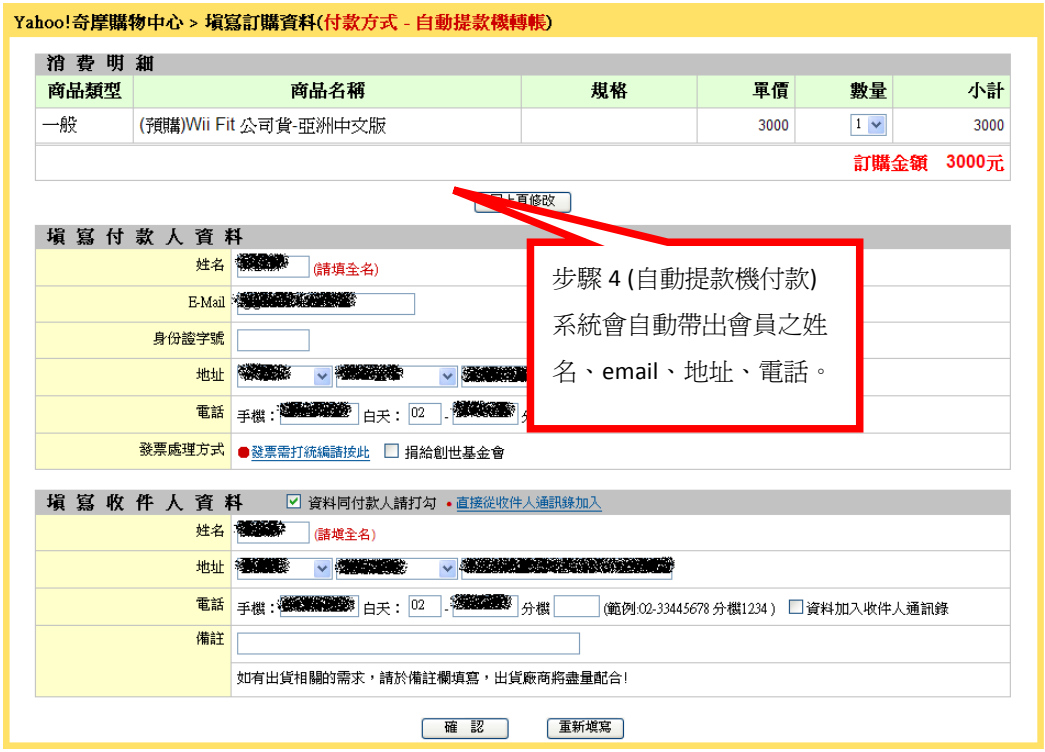
單筆訂單獨立產生一筆虛擬帳號，有繳費期限，如超過期限仍未完成付款，該筆訂單交易則自動取消。信用卡付款亦提供分期付款，一般商品皆可到 12 期零利率。消費者亦可選擇信用卡紅利折抵，但僅限刷卡一次付清。

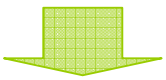
步驟 4：填寫收件資料。此步驟爲購物流程中，顯示及填寫最多個人資料的一個步驟。尤其是如選擇透過信用卡付款，尚須提供信用卡卡號、信用卡背後末三碼、信用卡到期月年等高層級資料。Yahoo!購物中心整段流程[292]皆採用 SSL 加密傳輸與網路銀行等級相同的 128bit 伺服器數位憑證，信用卡資料在傳輸途中被竊取之風險性相對低。惟經筆者實際測試，在提供錯誤之持卡人身份證字號及出生年月日，而僅輸入正確之信用卡卡號、信用卡背後末三碼及卡片有效年月之狀況下，該筆信用卡付款仍成功通過授權。表示網站業者並未限制**信用卡持卡人須與購買者同一人**。另外也未對信用卡持卡人資訊作進一步核對，僅針對信用卡之有效性進行授權。此漏洞易造成信用卡盜刷之情事發生，雖然持卡人事後可透過否認交易拒絕付款，但任何的盜刷案件，無疑皆在在打擊消費者對於網路購物安全度的信心。另外，由此處也不難發現，網站業者對於消費者購物方便性之重視程度遠遠超過網站潛在之損失[293]，唯有透過法令的規範，才能強制購物網站將業績擺在交易安全之後方。

[292] http://buy.yahoo.com.tw/help/helper.asp?p=safety (Last Visit：2009.6.30)

[293] 信用卡盜刷發生時，貨款因持卡人否認交易而無法收款，業者之損失爲貨物已寄出之損失。


步驟 1
YAHOO! 奇摩 購物中心
會員登入/登出
新使用者? 立即註冊
首頁 | 服務說明 | Yahoo! 奇摩
興奇科技
SONY BD片買2送1！
想暢玩魔獸！點卡快速到！
X360超猛低價$4980！
說中文了！Fit中文化登場
首頁 電腦資訊 消費電子 視聽家電 美妝 服裝 精品/手錶 鞋包配飾 居家生活 交通/美食 書籍DVD 超商取貨 品牌旗艦 快速到貨 送你機票
Game 搜尋 進階搜尋 熱門：公司貨 psp NDSL ps3 PS2
您的位置在：購物中心 > 消費電子 > Game > 任天堂Wii > Wii 遊戲軟體
我的帳戶 一起買 訂單查詢 客服中心
Game
任天堂Wii
激安！お買い得！
熱門新到貨
Wii 主機組合
Wii 原廠周邊
Wii 遊戲軟體
Wii 保護收納周邊
Wii 各式擬真套件
Wii 輸出入/電源
Wii各式實用周邊
GC遊戲/周邊
全站商品分類
本分類熱銷榜
(預購)Wii Fit 公司貨-亞洲中文版
看商品放大圖
（上一頁 瀏覽同分類商品 下一頁）
中文版登場!再送小禮物
(預購)Wii Fit 公司貨-亞洲中文版
◆送可愛吊飾+航海王NDSL專用包
◆WiiFit公司貨中文化終於登場
◆語音、文字完全中文化
◆提供了40種以上的健身訓練
賣場編號：1240161 ▶加入追蹤清單
廠商建議價 3000 元
轉帳價 3000 元(限ATM)
網路價 3000 元 (刷卡可用信用卡紅利折抵 接受19家銀行)
分期價
3期0利率 每期 1000 元 接受台新等 26家銀行
6期0利率 每期 500 元 接受花旗等 27家銀行
12期0利率 每期 250 元 接受國泰世華等 25家銀行
12期 每期 267 元 接受台北富邦等 1家銀行
24期 每期 137 元 接受聯邦等 15家銀行
本商品預計出貨日：2009-0
贈 品 08/12/31前-送手機吊
08/12/31前-送航
步驟 2
我要購買
放入一起買 (說明)
Yahoo!奇摩購物中心 > 選
步驟 3
選擇付款方式
刷玉山信用卡購物享分期優惠
訂購商品名稱
(預購)Wii Fit 公司貨-亞洲中文版
選擇付款方式
ATM價： 3000元
刷卡價： 3000元（一次付清）
3000元（使用信用卡紅利折抵）
分期價： 1000元x 3 期 0 利率 (接受台新等 26家銀行)
500元x 6 期 0 利率 (接受花旗等 27家銀行)
250元x12 期 0 利率 (接受國泰世華等 25家銀行)
267元x12 期 (接受台北富邦等 1家銀行)
137元x24 期 (接受聯邦等 15家銀行)
下一步
回上頁修改


Yahoo!奇摩購物中心 > 填寫訂購資料(付款方式 - 自動提款機轉帳)
消 費 明 細
商品類型
商品名稱
規格
單價
數量
小計
一般
(預購)Wii Fit 公司貨-亞洲中文版
3000
1
3000
訂購金額 3000元
填 寫 付 款 人 資 料
姓名
(請填全名)
E-Mail
身份證字號
地址
電話
手機：
白天：
發票處理方式
發票需打統編請按此
捐給創世基金會
填 寫 收 件 人 資 料
資料同付款人請打勾
直接從收件人通訊錄加入
姓名
(請填全名)
地址
電話
手機：
白天：
分機
(範例:02-33445678 分機1234)
資料加入收件人通訊錄
備註
如有出貨相關的需求，請於備註欄填寫，出貨廠商將盡量配合!
確 認
重新填寫
步驟 4 (自動提款機付款)
系統會自動帶出會員之姓名、email、地址、電話。



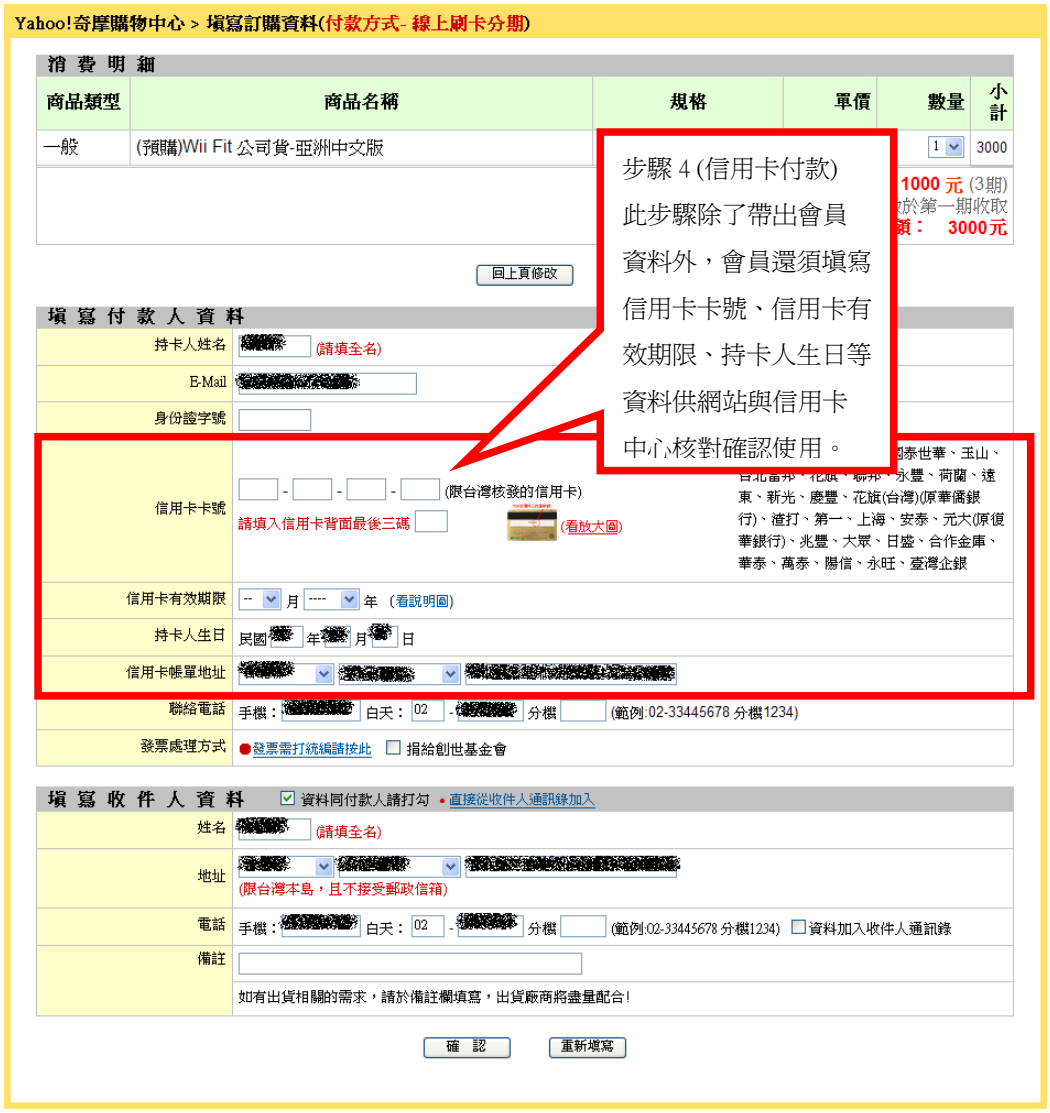


圖 3：YAHOO 奇摩購物中心網站購物流程

註、資料來源
YAHOO 奇摩購物中心網站

(二) PChome 24 小時購物：

步驟 1：登入帳號，只要有任一組 PChome 網站服務之帳號，就可使用該組帳號密碼登入 PChome 24 小時購物網站。首次使用者須註冊成爲會員。(如無執行步驟 1，在步驟 3 後將會強制要求執行步驟 1)

步驟 2：點選”立即訂購”選項。

步驟 3：結帳，確認購物清單。

步驟 4：填寫寄送資料及選擇付款方式。網站自動帶出之會員之姓名、地址、電話號碼。提供信用卡付款(零利率分期及紅利折抵)、SmartPay[294]、現金貨到付款等多種選項。

步驟 5：同意線上購物電子商務約定條款。

步驟 6：付款。與 Yahoo 購物中心比較，PChome 24 小時購物付款選項多了「貨到付款」的選擇，單筆訂單上限五萬元。信用卡付款方面也同 Yahoo 購物中心，皆未限制信用卡持卡人須與購買者同一人，也未對信用卡持卡人資訊作進一步核對，僅針對信用卡之有效性進行授權。

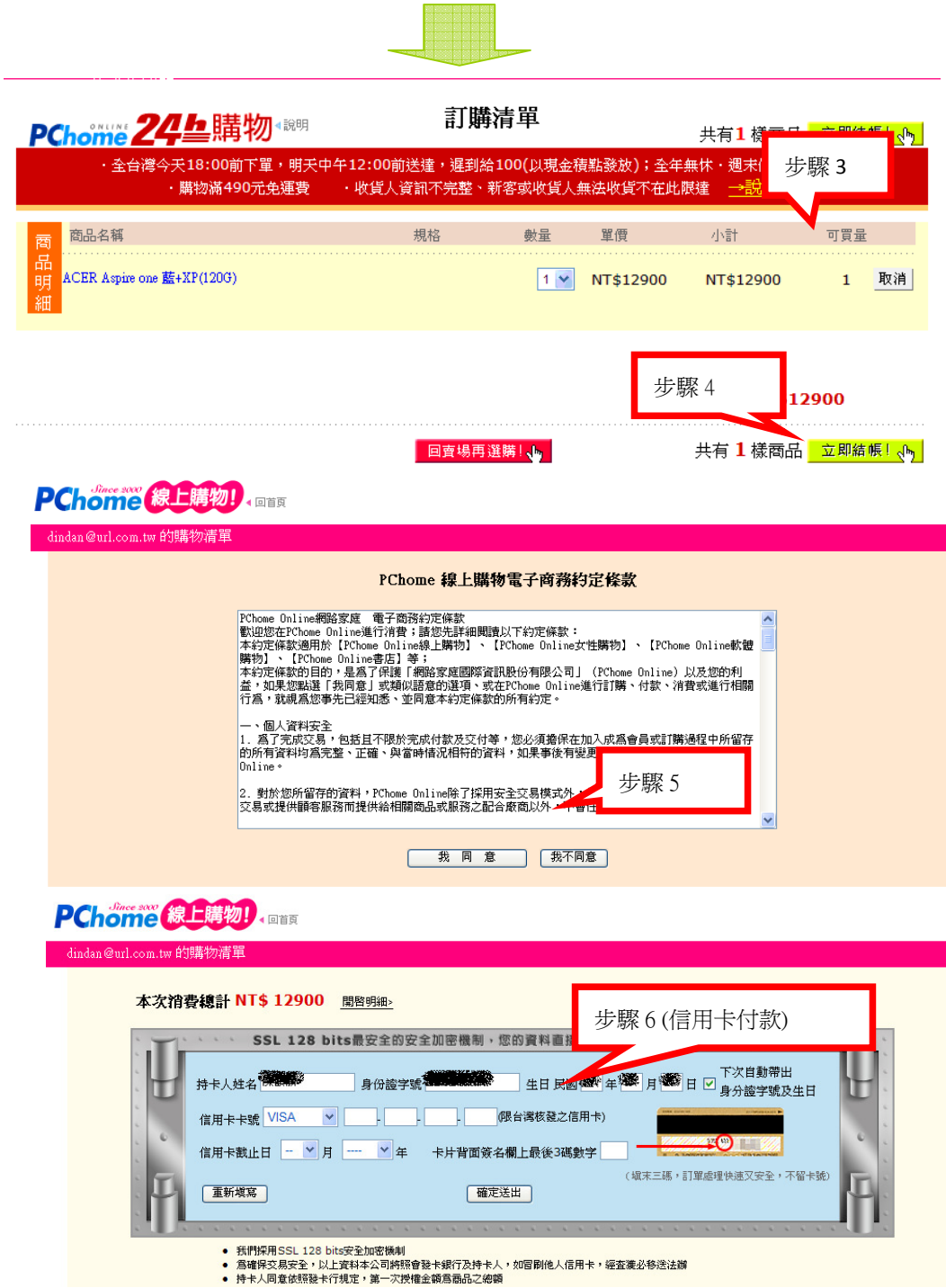

訂購清單
步驟 3
商品明細
商品名稱
規格
數量
單價
小計
可買量
ACER Aspire one 藍+XP(120G)
NT$12900
NT$12900
取消
步驟 4
12900
回賣場再選購!
共有 1 樣商品
立即結帳!
dindan@url.com.tw 的購物清單
PChome 線上購物電子商務約定條款
步驟 5
我 同 意
我不同意
dindan@url.com.tw 的購物清單
本次消費總計 NT$ 12900
步驟 6 (信用卡付款)
SSL 128 bits最安全的安全加密機制
持卡人姓名
身份證字號
生日
下次自動帶出
身分證字號及生日
信用卡卡號
VISA
信用卡截止日
卡片背面簽名欄上最後3碼數字
重新填寫
確定送出

圖 4：PCHOME 線上購物網站購物流程

註、資料來源

PCHOME 線上購物網站

(三) Yahoo 拍賣：

步驟 1：登入帳號，如首次使用則須註冊一個 Yahoo 會員帳號才可開始購物。(如無執行步驟 1，在步驟 2 後將會強制要求執行步驟 1)。登入這步驟

雖然簡單，但也存在著風險。近幾年來，各大網站飽受釣魚網站(Phishing)[295]之擾，造成大量會員帳號密碼被竊取及濫用，網站秩序瞬間大亂。Yahoo 當然也身受其害，於是推出了 2 項安全登入機制來保護 Yahoo 會員的帳號密碼安全。

1. 安全圖章：此圖章係提供會員以文字或圖片等方式，自行選擇或上傳圖形；而日後在登入前，便可在登入頁的右上方看見該圖章。這項功能是爲了讓使用者能更容易辨認是否進入假造的釣魚頁面，降低被竊取帳號及私人資料的風險。問題是：一般網路使用者，除了自用個人電腦外，亦常透過使用公用電腦上網。如網咖、辦公室等等。而公用電腦使用者眾，並無法透過安全圖章機制全面防制釣魚網站。

[295]網路釣魚(Phishing) 起源於英文字 Fishing(釣魚)，原意是釣(盜)取網路使用者的帳號密碼及個人資料，它是目前非法駭客竊取使用者帳號密碼的慣用手法之一。非法釣客(Phishers)或駭客會仿製知名網站的登錄頁面，然後利用垃圾郵件或即時通訊發送連結，誘使網友登入，直接騙取網友的帳號、密碼，甚至姓名、地址、電話及信用卡資料，再利用這些資料獲取不當利益。

圖 5：YAHOO 線上購物網站購物認證安全圖章

註、資料來源

YAHOO 線上購物網站

2. 帳號安心鎖：利用雙重認證機制保護網友的帳號安全，就像家裡上了二道大鎖，降低盜刊風險及被冒用帳號。第一重爲安全圖章機制，第二重即安心鎖。網友可以選擇透過內政部核發之自然人憑證或是 Hinet 的動態密碼鎖登入。此機制確實能有效保障帳號安全。就算因爲被誤植木馬程式或釣魚網站受騙而被竊取帳號密碼，只有網友選擇透過安心鎖登入之帳號，盜用者將無法單憑帳號密碼登入 Yahoo 帳號進而濫用帳號犯罪。雖然是個立意良好之機制，但就實際面來看，恐怕又是一個叫好不叫座之示範機制。

(1) 申請自然人憑證，網友須滿 18 歲之中華民國國民才可申請自然人憑證，且須支付 275 元工本費，再加上可使用的服務主要仍屬於政府服務，因此，截至 2008 年 12 月 29 日，累計發卡數僅爲 1520012[296]，發行量僅佔經常上網人口之 14.79%。

(2) HiNet 動態密碼鎖使用國際知名安全廠商(RSA)之產品。每 60 秒會隨機產生一組動態密碼，且每組密碼只能使用一次，使用過的動態密碼無法再次使用。使用須額外付費，動態密碼鎖首年年租費$599 元/個，第 2 年起每年$399 元/個。使用族群主要還是網拍大賣家及相對重視個人帳戶安全的使用者。

除了使用門檻相對高外，當會員身邊未攜帶自然人憑證或 HiNet 動態密碼鎖時，就無法登入 Yahoo 會員帳號，對於登入的便利性，難免有些影響，也間接將導致使用率遲遲無法提升。。

[296] http://moica.nat.gov.tw/html/apstatistic.CEXE(Last Visit：2009.6.30)

圖 6：YAHOO 線上購物網站購物認證帳號安心鎖

註、資料來源

YAHOO 線上購物網站

步驟 2：透過「競標」方式出價或是「直接購買價」立即買。**下標前的觀察與判斷，是決定此交易風險高低的主要原因之一**。

1. 棄標：拍賣平台中，大多數皆非屬專業賣家。每位賣方描述商品的重點不同，提供說明資料的完整豐富度當然也不盡相同。如果看過賣方提供的商品資訊，或對交貨、付款……仍有不清楚的地方，都可以使用「問與答」，進一步向賣家的詢問。因此在下標前，務必確認清楚，以免造成棄標[297]的情況發生。

2. 詐欺：詐欺常出現在幾種狀況下：

- 商品售價與市價相差過多。透過低售價讓買家產生搶便宜之心態因此下標購買。
- 賣方爲新註冊幾天內評價累積快速。透過多帳號的操作，做假評價分數以用來降低買家之警覺。

[297] http://help.cc.tw.yahoo.com/help_cp.html?product=2&catyname=%A5%E6%A9%F6%A7%B9%A6%A8%B6%B7%AA%BE&funclass=%B6R%AEa%B1%F3%BC%D0 (Last Visit：2009/6/30)

- 賣方近期評價大量出現中立或負分、出售與過去商品類型截然不同之商品或過去該帳號只使用於購買如今出售一堆商品。以上種種異常狀況，有可能賣家帳號已經被盜用。

- 問與答內容模稜兩可、含糊不清時，有可能賣家根本不瞭解商品本身，只是透過熱門商品來吸引買家眼球及詐騙。

- 面交地點偏僻或是面交前仍要求先支付部份款項。

3. 售後服務差：事先可先透過問與答試探賣家回答問題之態度及速度。或藉由賣家評價內容可過濾掉不負責任的賣家。

步驟 3：付款。一般網拍付款方式主要爲 ATM 轉帳、貨到付款及面交。Yahoo 近幾年來大力推行線上金流機制「輕鬆付」，所有的付款服務在 2008 年 4 月推出信用卡付款[298]趨於完整。將原本 B2C 付款優勢「信用卡付款」搬移到拍賣中，並提高買賣交易風險保障至 5 萬塊。業者表示「輕鬆付」爲網拍最安全的付款方式，加入防治財務竊取與洗錢之技術，能有效防制詐欺。其可能的最大風險爲輕鬆付使用者帳號被盜用[299]。平台業者如能加強帳號盜用機制，會員才能真正「輕鬆付」安心買。

[298] http://tw.memo.help.yahoo.com/c2c_read_announce.php?prop_id=2&mesg_id=71

[299] http://www.itis.tw/node/1154

圖 7：YAHOO 線上購物網站購物輕鬆付使用流程

註、資料來源

YAHOO 線上購物網站

(四) 露天拍賣：

步驟 1：登入帳號，須註冊成爲露天拍賣會員始可使用。有鑑於市面上之安全登入方式並無法達到真正的效益，且亦無法兼顧使用的便利性。露天拍賣並無推出其他額外之登入方式，僅透過登入頁面的安全提醒，加強會員帳戶安全的警覺度。

圖 8：露天拍賣網站登入頁面

註、資料來源

露天拍賣網站

步驟 2：透過「競標」方式出價或是「直接購買價」立即買。露天拍賣銜接 ebay 發展多年之交易安全 know-how，透過內部過濾系統(Filter)，有效過濾可疑詐欺、假出價、疑似帳號盜用等等違規行爲，提前一步幫會員把關，有效降低站上詐欺率至萬分之二。直逼 ebay 內部交易安全指數之高規。

步驟 3：付款。一般網拍付款方式主要爲 ATM 轉帳、貨到付款及面交。露天拍賣鑑於網拍交易大多透過 ATM 轉帳進行付款，付款前後所須進行之交涉流程繁複，爲降低這些既定流程，透過會員一次性的設定及露天系統與銀行間資訊的的串接，讓會員享受到快速付款的交易。另一方面，爲避免帳號盜用之情況造成付款快手功能被濫用及使用者個資外洩，露天拍賣特別加入第二層密碼把關，且強制要求不可與登入密碼雷同，以保障會員個資之安全。

圖 9：露天拍賣網站付款機制

註、資料來源

露天拍賣網站

第二項、 消費者資料蒐集、認證、使用、保存及退出

既然不論是 B2C 或是 C2C 網站，都要求使用者須先完成註冊動作，才可

使用網站。對於註冊時，網站又會要求哪些資料呢?而這些資料，網站又如何來使用及保護呢?

一、 蒐集範圍

註冊時：帳號、密碼，個人姓名、性別、email、手機、電話、身分證字號、地址等基本資料。

註冊後：連線設備的 IP 位址、使用時間、使用的瀏覽器、瀏覽及點選資料記錄。

交易後：付款資料、銀行帳號、送貨地址。

二、 認證方式

目前國內網站所採用的認證方式，大致上可歸納爲下面幾項：

(一) 手機認證：由系統傳送認證碼至會員所提供之手機門號，會員須於收到手機簡訊認證碼後，回網站填入認證碼，即完成認證。

(二) Email 認證：由系統傳送一封 email 至會員所提供之電子信箱中，會員須在收到確認後後點選信件中的認證連結即成功完成認證。

(三) 信用卡認證：透過線上「取得銀行授權交易 1 元」的方式，查證信用卡的有效性。

(四) 新式身分證認證：透過新式身分證之發證日期，與戶政單位開放之查詢系統[300]作確認，如資料無誤，即完成認證。

(五) 固定電話認證：在網頁的固定電話欄位填入想使用的固定電話，然後用該固定電話撥打認證電話，撥入後，根據系然指示完成動作即可。

(六) 自然人憑證：透過 API 與內政部憑證管理中心連線確認爲憑證本人之認證方式。

其實上述的方式，除自然人憑證認證外，其他方式均無法認證會員的真正身分。韓國政府有鑑於此[301]，於 2006 年年底國會通過了“促進利用信息通

[300] https://www.ris.gov.tw/uping_new.html(Last Visit：2009.6.30)

[301] http://news.sina.com/w/2008-06-18/164215770459.shtml(Last Visit：2009.6.30)

信網及個人信息保護有關法律”修正案，規定在平均每天點擊量超過 10 萬的入口網站和公共機關網站的留言欄上登載文章、照片、視訊等內容時，必須先以本人真實姓名加入會員。如果網站違反確認實名的做法，將會收到政府要求改善的命令。如果不遵守命令，將處以 3000 萬韓元以下罰款。具體來說，就是相關網站不安裝實名認証系統，最高可以罰款 1000 萬韓元。對於沒有安裝實名認証系統的網站，將給 3 天時間履行命令。3 天內仍然不改的，在必交的 500 萬韓元罰款的基礎上，每天追加征收 50 萬韓元。與此同時，如果違反《選舉法》第 82 條第 6 款：“網絡媒體留言板、聊天室等實名制”的規定，沒有刪除未標明真實姓名文章的話，將處以 300 萬韓元罰款。對於個人來說，惡意發文者最高可以判 7 年拘役，5000 萬韓元以下罰款。韓國的網絡實名制是否間接侵害了個人資料隱私權呢?其實不然，韓國實名制是一種變通的實名制。韓國信息通信部允許網友在通過身份驗証後，用代號等替代自己的真實姓名在網上發布訊息。也就是說韓國的網路實名制原則上是“後台實名”，即在註冊登錄時用真實身份訊息，但在前台發文時可用代號替代真實姓名。這樣既保護了隱私權，也在很大程度上保証發文人對自己的發言負責。韓國網路信息化建設起步較早，居民身份証等主要信息已實現電子化，門戶網站與居民身份証信息中心等機構聯網，可以對網民註冊時填入的身份証號碼等個人資料真僞進行驗証。一旦發生法律糾紛，警方可以很容易找到肇事者，進而節約社會成本，頗值得台灣借鏡。不過該實名認証系統的安全性及存取限制，又是另一資安考量。一旦被駭客入侵，嚴重性將無法想像。因此，政府如欲推行實名制，除了法令限制外，更應規劃一套完整的認證機制，在保護人民的個人資料安全下，有效解決網路無身分無責任的不安全交易環境。

三、 國內電子商務網站隱私權規範

一般合法使用的規範皆在各網站隱私權聲明載明，內容大致包含幾個以下要素：

(一) 隱私權保護政策的適用範圍

(二) 資料的蒐集與使用方式

(三) 資料之分享

(四) 供應商和其他服務供應商

(五) 子公司和合資公司

(六) 資料之保護

(七) 網站對外的相關連結

(八) Cookie 小餅乾之使用

(九) 個人帳號之保密

(一〇) 隱私權保護政策之修正

以露天拍賣[302]爲例：

隱私權保護政策的適用範圍

隱私權保護政策內容，包括本網站如何處理在您使用網站服務時收集到的個人識別資料。隱私權保護政策不適用於本網站以外的相關連結網站 ，也不適用於非本網站所委託或參與管理的人員。

資料的蒐集與使用方式

您在註冊帳號、瀏覽網頁、參加網站活動時，我們會收集你的個人識別資料。我們也可以從其他合作夥伴處取得個人資料。當你在註冊時，我們會問及你的姓名、身分證字號、出生日期、性別、電話、及電子郵件地址等資料。在註冊成功，並登入使用我們的服務後，我們就會認識你。於一般瀏覽時，伺服器會自行記錄相關行徑，包括您使用連線設備的 IP 位址、使用時間、使用的瀏覽器、瀏覽及點選資料記錄等。如果你選擇在露天拍賣上進行出價、購買或出售物品行爲，我們會蒐集你的出價、購買及出售物品行爲資料，同時在露天拍賣的個人信用中心也會蒐集其他會員對你的意見，做爲我們增進網站服務的參考依據，此記錄爲內部應用，絕不對外公布。

資料之分享

露天拍賣絕不會任意出售、交換、或出租任何您的個人資料給其他團體

[302] http://www.ruten.com.tw/system/server_center.htm?00060002(Last Visit：2009.6.30)

或個人。只有在下列情況除外：

在您同意分享資訊的情況下；

- 經確認爲拍賣結標後的買賣雙方，網站人員得以經任何一方之要求提供聯繫資料以供完成交易使用；
- 經您授權露天拍賣提供您所要求的產品或服務；（例如願意收到新品通知）
- 司法單位因公眾安全，要求露天拍賣提供特定個人會員資料時，露天拍賣將視司法單位合法正式的程序，以及對露天拍賣所有使用者安全考量下做可能必要的配合；
- 有違反任何露天拍賣政策、權利、智慧財產權或任何露天拍賣或其他會員安全時。

供應商和其他服務供應商

我們可能會與第三者「供應商和服務供應商」合作，來推動我們的服務。例如，我們可能會將我們網站的一個或多個方面的運作外包給其他「供應商」或「服務供應商」，讓他們根據我們的要求展開服務。在某些情況下，「服務供應商」會直接從你那裏收集資料〔例如，在我們要求「服務供應商」爲我們進行問券調查時〕。在這些情況下，我們會通知你將有「供應商」或「服務供應商」介入，而且對你所有資料的透露你都有權選擇是否接受。無論在任何情況下，我們都會限制這些「供應商」和「其他服務供應商」存取、使用及透露你資料的方式。通常，我們不允許這些「供應商」和其他「其他服務供應商」將你的資料出售給第三者。

子公司和合資公司

我們會與全世界經授權爲你的個人對個人交易需求提供服務的子公司及合資公司共用我們的大部份資料，其中包括你的個人辨認資料。就這些實體機構對你資料的存取而言，他們至少會像對待他們的其他會員提供的資料一樣對你的資料進行保護。我們通常要求我們的子公司與合資公司對所有會員提供的保護不得低於在此文件中規定的標準。

資料之保護

本網站主機均設有防火牆、防毒系統等相關的各項資訊安全設備及必要的安全防護措施，加以保護網站及您的個人資料。

網站對外的相關連結

本網站的網頁提供其他網站的網路連結，您也可經由本網站所提供的連結，點選進入其他網站。但該連結網站不適用本網站的隱私權保護政策，您必須參考該連結網站中的隱私權保護政策。

Cookie 小餅乾之使用

Cookies 是伺服端爲了區別使用者的不同喜好，經由瀏覽器寫入使用者硬碟的一些簡短資訊。您可以在 Netscape 的「功能設定」的「進階」或是 IE 的「Internet 選項」的「安全性」中選擇修改您瀏覽器對 Cookies 的接受程度，包括接受所有 Cookies、設定 Cookies 時得到通知、拒絕所有 Cookies 等三種。如果您選擇拒絕所有的 Cookies，您就可能無法使用部份露天拍賣上的個人化服務，或是參與部份的活動。依據以下目的及情況，露天拍賣會在本政策原則之下，在您瀏覽器中寫入並讀取 Cookies：

- 爲提供更好、更個人化的服務，以及方便您參與個人化的互動活動。Cookies 在您註冊或登入時建立，並在您登出時修改。
- 爲統計瀏覽人數及分析瀏覽模式，以了解網頁瀏覽的情況，做爲露天拍賣改善服務的參考。

個人帳號之保密

請妥善維護您的會員帳號、密碼或任何個人資料。 請您留意無論何時您透過網站討論區、電子郵件、或聊天室等公開區域所主動揭露的個人資料，均可能被其他第三人蒐集或使用，上網時請特別小心。

隱私權保護政策之修正

當您使用本網站所提供的服務時，露天拍賣將視同您已閱讀、且同意本

政策。本網站隱私權保護政策將因應需求隨時進行修正，修正後的條款將公告於網站上，請您隨時查詢最新公告內容。如果您不同意本政策，請立即停止使用本網站服務。

兒童隱私

未滿 12 歲之兒童非本站目標族群，本站將不會准許其註冊，也不會刻意蒐集兒童之個人資訊。且註冊過程之會員合約內容中也會有清楚的標示提醒。

各家購物網站及網拍註冊流程所要求之個人資料大同小異，但資料的要求的多寡，網站所須負擔之保護責任應隨之加重。

PChome 線上購物會員註冊頁面：

爲購物網站中要求之會員個資量最低的一個。註冊流程最爲簡單。網友只須提供 email 及設定密碼即可馬上使用。

圖 10：PChome 線上購物會員註冊頁面

註、資料來源

PChome 線上購物網站

Yahoo 購物中心拍賣會員註冊頁面：

Yahoo 購物中心及 Yahoo 拍賣皆透過 Yahoo 會員中心頁面來進行註冊流程。

- 在註冊的頁首，特別標示會員所填寫之個人資料並不會轉作其他用途使用，讓會員安心填寫。
- 系統已預設勾選會員訂閱電子報。

圖 11：Yahoo 購物中心拍賣會員註冊頁面

註、資料來源

Yahoo 購物中心網站

露天拍賣會員註冊頁面：

圖 12：露天拍賣會員註冊頁面

註、資料來源

露天拍賣網站

金石堂網路書店會員註冊頁面：

圖 13：金石堂網路書店會員註冊頁面

註、資料來源

金石堂網路書店網站

Payeasy 購物網站會員註冊頁面：

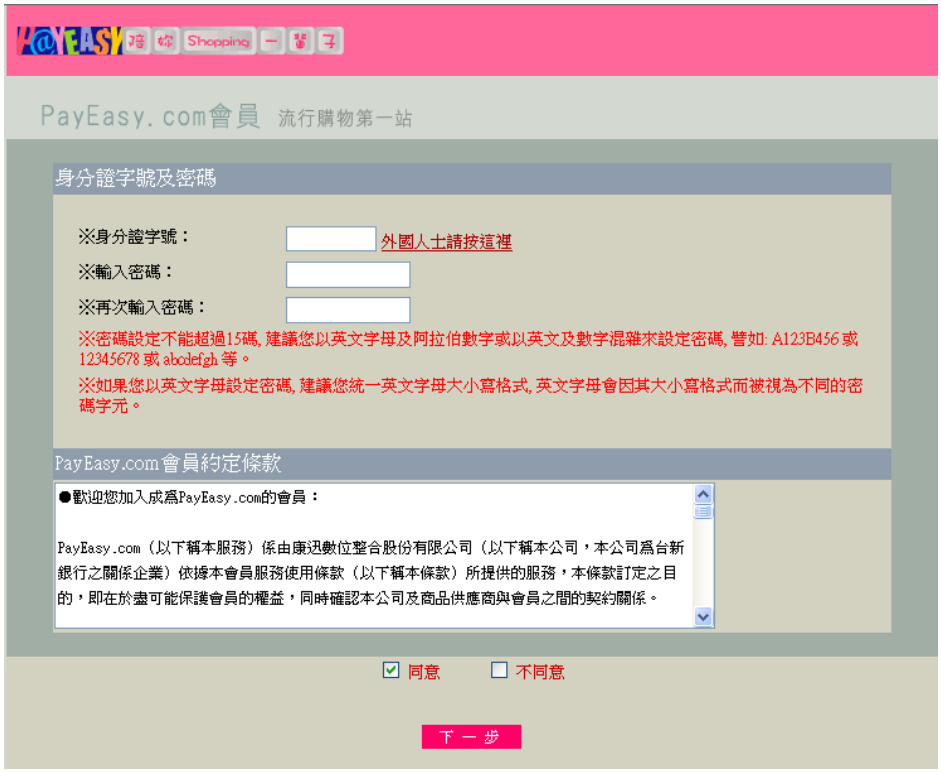


圖 14：Payeasy 購物網站註冊頁面

註、資料來源

Payeasy 購物網站

表 2：各家網站註冊網頁個資要求量比較表

個人資料	Yahoo購物中心\拍賣	Pchome線上購物	露天拍賣	金石堂網路書店	Payeasy
姓名	v		v	v	v
家用電話				v	v
手機	v		v	v	v
email	v	v	v	v	v
地址				v	v
身分證字號	v		v	v	v
出生年月日	v			v	v
性別	v			v	v

註、資料來源

筆者整理

個資要求量最少：PChome 線上購物

個資要求量最多：金石堂網路書店及 Payeasy

- 深究其註冊時個資要求目的，主要是一來方面後續購物物品配送所須之姓名、電話及地址。一來是發生惡意詐欺行爲時之後續法律追溯用。既然購物網站本身目前尚無有效的身分認證機制，會員註冊時所填資料之正確性，當然也只能根據後續交易的金流及物流來確認部分資料。

- 對於一般網友而言，自然會填寫正確無誤之資訊以確保後續物品能順利送達，但對於有心詐欺之份子而言，註冊時所填寫之資料，大多爲虛假，最後當然也無法用來追溯其法律責任。

- 再者，既然大多數使用者爲達線上購物能順利進行而填寫正確個資，當網站發生個資外洩時，受害最爲嚴重的，反而是這群忠實使用者，徒有人善反被欺之感。

- 身分證字號要求過度頻繁。不管是網站會員註冊的電子形式或是紡間問卷或入會資料等紙張形式，皆如同套好招般要求民眾填寫個人身分證字號，但卻不知其收集之目的爲何?民眾面對這如同制式般個資請求,在完全無警覺心及拒絕力的情況下，通常就自然而然的填寫給了出去。爲何購買商品須讓

對方得知自己的身份證字號，爲何加入會員也需提供個人身分證字號，這個問題值得深入探討，也許是亞洲區個資收集及流通如此順暢的原因之一。

整體來講，PChome 線上購物之低個資量的作法，不但降低網站本身對於過多個資保護的責任，也讓消費者以最快的速度完成註冊流程，馬上跳回購物環境中，不因註冊流程的停頓導致網友中斷購買慾望。

四、 保存及退出

每家電子商務業者，會針對個別的情況，在隱私權聲明中說明會員資料使用的範圍。此項公開的聲明，主要是爲了保護會員個資安全。但實際上，仍存在著幾個問題：

(一) 任何超出隱私權聲明使用範圍皆須**在會員同意分享資訊的情況下**，才允許發生，而這種情況卻往往發生在網友無警覺的情況下。原因在於一般會員對於個人資料保護的警覺度原本就低，尤其是面對抽獎或促銷活動時，往往不察情況下就同意了協力廠商(third party)存取自己的個人資料。網站應主動提醒會員，在同意協力廠商使用其個資的情況下，所收集的資料是否僅用於此次活動，並且於活動結束後將相關資料全部銷毀，哪些個人資料可能會被強制公開顯示等等提醒內容。例如抽獎活動，須透過民營郵局寄發獎品時，得獎人之姓名、電話、地址將會被強制公開印製在郵包標籤上等。

(二) **會員資料的保存應設期限**。由於台灣網站發展快速，大大小小如雨後春筍般產生。網友通常註冊了就使用，久不使用也就慢慢的忘記曾經註冊過該網站。因此各大網站會員資料庫必定存在著一群幽靈嚐鮮使用者資料。網站不該永久保存這些會員資料，應透過通知等方式，完整移除超過一定期限未使用網站服務之會員資料。

(三) 更正權的存在和條件。網站不可拒絕會員要求更正個人資料。但可透過簡易之身分認證，確認爲個人資料所有者後，協助其更正正確個人資料。

第三項、 個別存在之個資外洩問題

一、 國內案例

1. 台北市政府法規會，也就是主管消費者保護的機關網站，把民眾申請國賠的資料，全都開放提供檢索，不但個人身分資料全都查得到，就連就醫紀錄都被掛上網。法規會表示是外包資訊廠商，忘記把資料加密，才導致個資全都露，已經請廠商趕工補救(2008/11/17)[303]

探討：這個個資外洩問題來自於外包資訊廠商忘記把資料加密。公家機關作爲政府示範單位，更應做好人民個資保護。對於外包廠商，也應謹慎選擇。資料傳遞時應做進行加密，並限制專責人員控管資訊讀取權。專案完成後，對於個資作廢的處理流程也應做到盡善盡美，滴水不漏。

2. 博客來網站 96 年辦理金馬影展套票出售，但因作業疏失，導致會員的個人資料外流，上百人權益受影響，其中 17 人不願接受博客來的和解，要求賠償 169 萬元，台北地院判博客來賠償 13 萬 7900 元；仍可上訴。此外，法院也認定，博客來爲「無店面零售業」，並非電腦處理個人資料保護法規範的範圍，但法官認爲，博客來將客戶資料外洩，仍應負起賠償責任，但資料僅是洩給當時購買金馬影展套票的同好，並未向第三人公開，法官認爲博客來過失情節不重，被害人精神受損尚微，判每個被害人可獲賠 7000 元至 1 萬 7400 元不等。[304]

探討：個資外洩問題發生於程式端，雖然博客來宣稱個資僅是洩給當時購買金馬影展套票的同好，但在身分上仍屬第三人，且非經本人之同意。像博客來這樣已具規模的商務網站，每日交易量龐大。程式端作業人員應更加謹慎，所撰寫之網站程式，因爲這些程式決定了網站未來對於惡意攻擊的防禦能力。網購企業應加強此一方面工程師寫作觀念與技巧。

3. 離職員工導致資料外洩國內外案例 刑事警察局於今年（2008）3 月接獲企業報案，某企業離職員工自行成立一家與舊公司性質雷同的電子商務公

[303] http://times.hinet.net/times/article.do?newsid=1842697&isMediaArticle=true&cate=general (Last Visit：2009.6.30)

[304] http://www.isecutech.com.tw/ISTF2008/news_detail.aspx?aid=4694 (Last Visit：2009.6.30)

司，該離職員工盜用接任同仁的帳號、密碼，入侵公司資料庫，甚至取得舊公司國外競標的訂單，竊取資料值 5 百萬台幣。今年（2008）初某購物台離職經理將客戶資料存入個人硬碟中，並盜賣 14 萬筆個資取得不法獲利。[305]

探討：內部員工竊取個資其實是最難去防範的一個環節。也是造成資料外洩的最大威脅。外接式儲存裝置、Email 以及 IM(Instant Messenger)都是主要的資料外洩途徑。企業應提高資料外洩防護的預算，尋求專業技術來協助企業阻絕惡意入侵或外洩，結合網路端與主機端的防護，有效防止機密資料外流，改善商業流程，以及管理法規作業與風險，確實保護企業免於受到外洩的威脅。

4. 戰國策爆發客戶資料外洩事件[306]。知名主機代管商戰國策，爆發客戶資料外洩事件，包括代管主機的登入密碼與客戶的資料，都在搜尋引擎上找得到，目前多數搜尋引擎已經清除這些個資，建議使用者立即更換密碼。

探討：由於戰國策不願說明造成此事件的原因，目前也只能透過幾個方面猜測原因。一位不願透露姓名的主機代管廠商主管表示，如果有做到登入身分的控管，例如 IP 位址與登入帳號、密碼的比對等，Google 的網路蜘蛛程式不可能有辦法存取內部訂單系統的資訊。他說：「最有可能的是系統做了異動之後，忘記加上身分認證的功能，然後內部管理人員的瀏覽器安裝了類似 Google Toolbar 的工具軟體，使得 Google 的伺服器可以收集到內部系統的網址，網路蜘蛛才有辦法循線收集到這些網頁。」一般人可能沒有注意，Google 在隱私權條款中寫到，「當您造訪我們網站或使用我們的其他產品時，Google 伺服器會自動記錄資料，包括 URL、IP 地址、瀏覽器的類型和使用的語言以及造訪日期和時間。」
爲了防止網路蜘蛛程式搜尋資訊，多數網站會在網頁上放上宣告網路蜘蛛禁止存取範圍的「robots.txt」文件檔。

二、 國外案例

1. 英國政府被迫緊急下令暫時關閉「政府入口網站」，以保障數以百萬計民

[305] http://www.ithome.com.tw/plog/index.php?op=ViewArticle&articleId=21243&blogId=1252(Last Visit：2009.6.30)

[306] http://www.ithome.com.tw/itadm/article.php?c=53022(Last Visit：2009.6.30)

眾的個人資料安全，原因是有人在酒吧的停車場發現一個拇指碟，裡面存有這個網站的機密登入密碼，而這個網站涵蓋處理稅務等業務的上百個公務機關。[307]

探討：這個問題環節一樣也發生在內部人員對於資料保護不夠謹慎，且員工可透過隨身碟等外接型式複製取走個人資料。

2. 智利一名電腦駭客從政府及軍方的伺服器中，盜走六百萬人的機密資料，隨後將全部個資貼在一個科技論壇的部落格上。這些資料包括個人的身分證號碼、住址、電話號碼及學歷背景等。駭客還留話說，他這麼做的目的在於突顯智利當局對於機密資料的保護有多麼鬆懈、疏失。這些資料被 po 上部落格之後，沒多久有關當局就發現，隨即採取行動，刪除並報警。警方也已經展開調查。[308]

探討：駭客透過網站應用程式或資料庫的漏洞來進行資料竊取。企業本身唯有加強資料庫之安全層級及提升程式人員之安全寫作能力及觀念，才能避免駭客如入無人之境，恣意妄為。

3. 資料外洩讓全球企業一年損失 1 兆美元[309]。全球企業在 2008 總計有高達 46 億美元的 IP 價值損失，並花費約 6 億美元修補相關的資料外洩問題。換算下來，去年全球企業的資料外洩損失可能高達 1 兆美元。

探討：McAfee 發布最新報告引用普渡大學的一份研究結果指出，全球企業因資料外洩所造成的損失，去年估計高達 1 兆美元。

普渡大學的這項研究，是由資訊保險暨安全教育研究中心的研究員檢驗 800 位 CIO 的問卷，這些 CIO 來自美、英、德、日、中、印、巴西，及杜拜等國家。檢驗內容包括其重要資訊（如 IP 的原創）如何儲存，儲存在全球何處，以及資訊如何傳送與遺失等。

[307] http://www.itis.tw/node/2234 (Last Visit：2009.6.30)

[308] http://www.itis.tw/node/1761 (Last visit：2009.6.30)

[309] http://www.ithome.com.tw/itadm/article.php?c=53229(Last Visit：2009.6.30)

結果顯示，受訪的企業在 2008 年總計有高達 46 億美元的 IP 價值損失，並花費約 6 億美元修補相關的資料外洩問題。McAfee 以這個數字爲基礎做計算，認爲去年全球企業的資料外洩損失可能高達 1 兆美元。McAfee 並由其網路安全的專業委員會檢驗該結果。McAfee 總裁兼執行長 Dave DeWalt 表示，McAfee 利用這項研究結果，做保守的估計。

擔任 CERIAS 執行總監的普渡大學電腦科學教授 Eugene Spafford 指出，公司企業過於低估他們 IP 的損失與價值。「和黃金、鑽石，或原油一樣，IP 也是可做國際貿易的另一種形式流通貨幣，遭竊時也可能對經濟產生嚴重的影響。」

這份研究還發現，經濟不景氣也讓資料更加危險。39%受訪者認爲，在現有經濟景氣下重要資料也比過去更容易外洩。開發中國家也較英、美、德、日等國家更願意投入保護重要資料（如 IP）。74%的中國受訪者及 68%的印度受訪者表示，爲保有競爭優勢而願投入 IP 的保護。

三、 個資外洩之可能原因

1. **使用者電腦被植入木馬程式**：一般而言，木馬程式[310]是一種 Client/Server （用戶端 / 伺服端）架構，在受害者機器上的稱爲伺服端，遠端進行操控的稱爲用戶端。一旦受害者的電腦遭植入木馬程式後，駭客就可在用戶端利用公開網路（網際網路）遠端操控伺服端的電腦，其後果可能導致檔案遭刪除、帳號密碼被篡改、機密資料洩漏等，甚至利用受害者電腦發動攻擊 (或傳染) 其他的電腦設備造成更嚴重的損害。因木馬程式具有隱蔽、自動啓動、欺騙、自我恢復、破壞、傳輸資料的行爲特徵，一般使用者不容易察覺它的存在；但駭客要遂行其任務，首先必先將木馬程式透過各種管道植入受害者機器上，因此瞭解木馬程式的傳播方式，將有助於防範駭客的入侵。木馬程式的傳播方式主要有下列三種：

[310] http://cissnet.edu.tw/knowledge_02.aspx (Last visit：2009.6.30)

甲、　　將木馬程式以郵件內容或附件的形式夾帶在電子郵件中，收信人只要打開自動預覽功能或附件，電腦就會感染木馬程式。夾帶郵件內容之程式可能是 Java Applet 、 ActiveX 等，夾帶在郵件附件的檔案格式可能是可執行檔.exe、圖形檔.gif、壓縮檔.zip 等。

乙、　　以提供工具、檔案、圖片爲幌子，誘騙使用者下載，如僞裝的修補程式、 p2p 下載軟體、工具軟體，將木馬隨附在軟體安裝程式內，乘機植入木馬程式；或將木馬程式僞裝成合法的檔案或圖片，只要一下載，木馬程式就會自動安裝。

丙、　　將木馬程式以 Java Applet 、 ActiveX 等型式隱藏在網頁中，利用瀏覽器自動執行的漏洞入侵受害者的電腦，使用者只要瀏覽該網頁，稍微不慎即可能遭受入侵。

2. **資料拼圖(懶人密碼)**：所謂資料拼圖[311]，即是將不同來源取得的個人資料比對後，拼湊出完整的資料，再利用一般民眾喜歡用生日、電話號碼等特殊數字作爲密碼的習慣，直接上網「測試」各種可能的帳號密碼組合。一旦成功，即可以合法的身份登入使用者帳號，直接觀看使用者的個人資料與各種記錄，讓資料更完整。駭客在網路上利用資料拼圖手法最知名的案例，要算是去年底發生的 Payeasy 事件。去年 12 月 9 日晚間，Payeasy 突然有來自中國大陸 IP 的大量異常登入，在被登入的 3,9000 多個會員帳號中，有 14%遭測試成功，27%則是帳號正確、密碼錯誤。Payeasy 發現異常後，便緊急封鎖特定 IP，並通知會員更改密碼，事後雖未傳出用戶遭詐騙成功的案例，但確有用戶在事後接到詐騙電話。

3. **網站資料庫及程式安全漏洞**：簡單來說就是利用網頁程式設計者忽略檢查使用者從表格或瀏覽器輸入內容所造成的安全漏洞，目前只要是有資料存取需求的網頁大都使用 SQL 資料庫系統，讓管理者可以方便管理網站資料或讓使用者可以進行查詢與交易，如果程式設計者在寫程式時有所疏忽，那麼網路不法份子可能可以簡單的利用一些惡意的 SQL 指令去進行未被授權的不法行爲，例如竊取資料或者侵入系統或破壞資料，而且這也只是利用 SQL 指

[311] http://www.zdnet.com.tw/news/software/0,2000085678,20127775,00.htm (last visit:2009.6.30)

令本身的瑕疵來入侵的，所以只要是支援 SQL 指令的資料庫皆會受影響，使用者可以輕易的靠一行指令或得伺服器的最高權限帳號，取得最高管理權限，這樣就能自由的獲取所有的資料了，因爲是使用正常管道及一般的操作正常指令，那些防火牆及防毒軟體都無法事先偵測。目前各家資料庫也注意到此事件的嚴重性而作了許多安全上的更新，不過，最重要且基本的解決方式還是設計師在寫網站系統時能事先對這些指令作出一些規定和限制來防範，免得將來有類似的新漏洞問題又重複影響資料安全的問題。

4. **內部管理失當**：大部分企業用戶對資安的重視僅侷限於輸入端(Input)，但在輸出端(Output)防護卻相當薄弱。現在 USB 隨身碟或大姆哥使用相當普遍，員工或客戶可以很容易從 PC 端竊取重要企業研發或內部資料。應透過阻斷(Disable)USB 接口功能，斷絕資料被竊取之虞。設定內部安全等級(Security Level)，不同階層之內部員工，有限制性的進入、讀取、儲存、匯出權限限制且紀錄所有的 log 資料。

第四項、 電子商務網站對於會員資料保護流程個資安全之管理與技術防護

一、 外在防護

網站上個人資料的傳送，應全面透過 SSL 加密，甚至會員的密碼應轉碼爲非明碼。安裝防毒程式、防火牆、虛擬私人網路、入侵偵測系統等等。

二、 內部資訊安全

網站本身應制定完善的組織架構、清楚指引及工作流程。管制內部人員對於會員個人資料的輸入、使用、查閱、傳送、輸出等權限。身份識別機制、資訊存取管理、PKI 公鑰架構及加解密傳輸則可視爲城池內的各式關卡。甚至與員工簽署保密條款，和外包合作廠商也應一併簽立，以保障消費者權益。

三、 他山之石- eBay 如何做好個資安全管理與防護

根據隱私暨資訊安全研究機構 Ponemon Institute 及網路隱私權保護組織 TRUSTe 發表隱私保護最值得信賴（Most Trusted Company for Privacy）的排行榜調查結果：

表 3：隱私保護最值得信賴（Most Trusted Company for Privacy）的排行榜調查結果

2008 Ranking	2008 Ranking
1 American Express (remained number one)	12 Intuit (+7)
2 eBay (+6)	13 WebMD (-1)
3 IBM (no change)	14 Yahoo! (new to the top 20)
4 Amazon (+1)	15 Facebook (new to the top 20)
5 Johnson & Johnson (+1)	16 Disney (-1)
6 Hewlett Packard (+10)	16 AOL (-12)
6 U.S. Postal Service (+1)	17 Verizon (new to the top 20)
7 Procter & Gamble (+2)	18 FedEx (new to the top 20)
8 Apple (new to the top 20)	19 US Bank (-2)
9 Nationwide (remained the same)	20 Dell (-7)
10 Charles Schwab (-8)	20 eLoan (-9)
11 USAA (+4)	

註、資料來源

隱私暨資訊安全研究機構 Ponemon Institute 及網路隱私權保護組織 TRUSTe

EBay 以上升六個名次的姿態穩坐隱私保護最值得信賴排行榜第二名。爲何 eBay 得以獲得民眾的肯定，認定爲隱私保護最值得信賴的公司呢?。Ebay 做了些什麼呢?

(一) Ebay 網站經營拍賣至今，已投資極大的成本及人力於交易安全上，透過專責部門的核心運作，將交易安全防範成效納入獲利模式，轉而取代傳統的「費用部門」認定。例如：TnS 部門研發新式之高命中率(High Hit Rate)過濾機制，透過實際運作，在上線期間總共避免了近 500 萬之 GMV 交易損失。該機制爲網站所減緩之潛在損失即爲 500 萬。這 500 萬對 eBay 來講，即爲獲利。因爲 ebay 網站有提供購物安全保障，所有的會員只要是透過 ebay 所規範的安全付款方式付款，但卻沒有收到商品，即可向 ebay 申請購物安全補助。當這套新上線過濾機制，有效遏阻 500 萬交易量之高風險交易時，相對的，也降低了 ebay 購物安全保障所賠償給會員之損失。

(二) Ebay Security Center[312]：透過專屬頁面，從如何買的安全、如何賣家安全、如何保護帳號安全、如何防範釣魚網站等等所有安全議題，均完整且詳盡的專頁介紹，且掛附在網頁頁尾(footer)。

[312] http://pages.ebay.com/securitycenter/index.html?_trksid=m40 (Last Visit：2009.6.30)

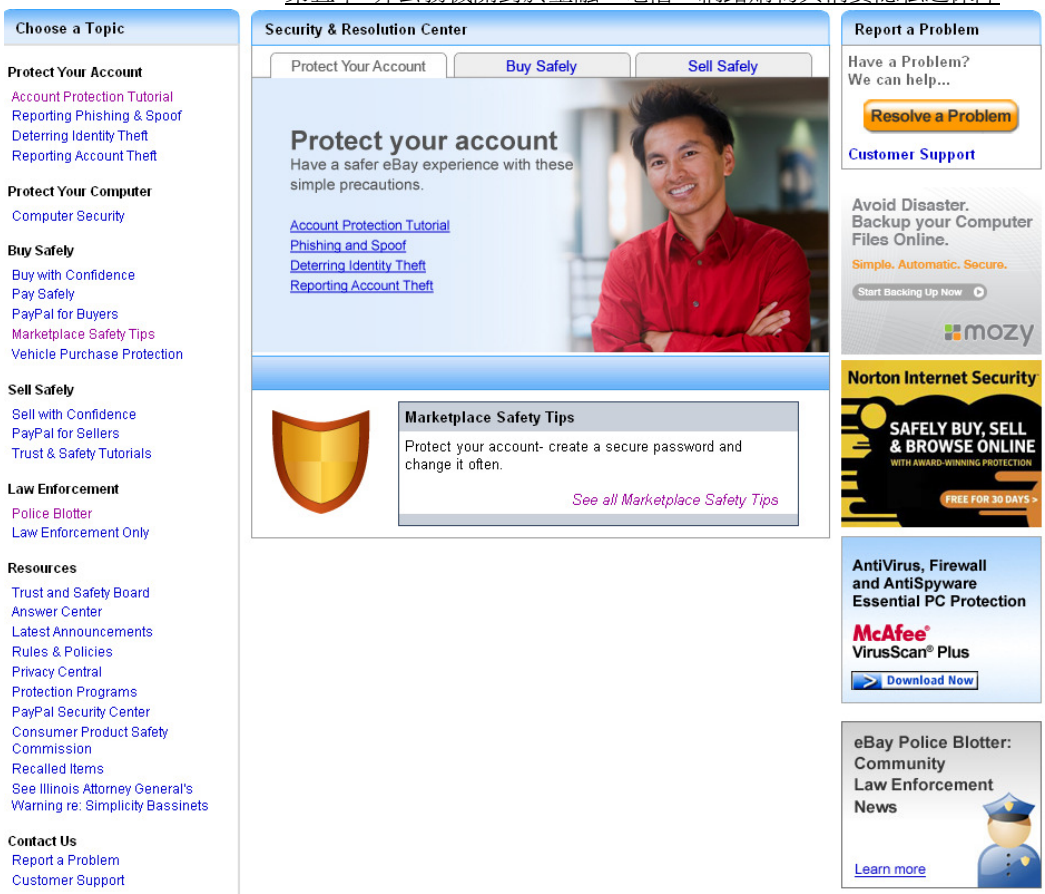


圖 15：Ebay Security Center

註、資料來源

Ebay 網站

(三) EBay 已取得 TRUSTe 隱私權方案的授權。TRUSTe 爲一個獨立的非營利機構，其任務在於推廣資訊揭露與取得同意等相關原則，以建立使用者在網際網路上的信任與信心。爲了證明對隱私權的重視，eBay 特地透過 www.ebay.com/ 來揭露資訊運用的相關措施，並將其的隱私權實務作法交由 TRUSTe 來審核。所有參與且取得隱私權方案的授權的網站，皆可在網頁上看到由 TRUSTe 所發出之審核標誌如下。

Your privacy is important to us

eBay does not rent or sell your personal information to third parties without your consent. To learn more, read our privacy policy.

Your address will be used for shipping your purchase or receiving payment from buyers.

TRUSTe CLICK TO VERIFY

TRUSTe

SIGN UP FOR A TRUSTE SEAL
SEARCH FOR SEALHOLDERS
CONTACT US

Seal Programs :: Privacy Education :: Watchdog Dispute Resolution Service

Verified

eBay Inc.
Validated Privacy Statement
For www.ebay.com
License Agreement Version MSA/1.0

eBay Inc. is a certified licensee of the TRUSTe® Privacy Seal Program. The privacy statement and practices of www.ebay.com have been reviewed by TRUSTe for compliance with our strict program requirements.

Make Informed Choices for Your Personal Information

About TRUSTe

TRUSTe Privacy Standards and Principles

The TRUSTe program is consistent with government and industry guidelines concerning the use of your personal information. These standards include the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Federal Trade Commission and Department of Commerce's Fair Information Practices, the California Online Privacy Protection Act, and the CAN-SPAM Act.

Make Privacy Your Choice

- **Visit TRUSTe's site** to see if other familiar companies are part of the program.
- **Get our quarterly email newsletter** with alerts, definitions and tips to be more confident online.
- Learn how to **protect your personal information.**
- **File a Watchdog complaint** if you feel eBay Inc. has violated its privacy agreement.

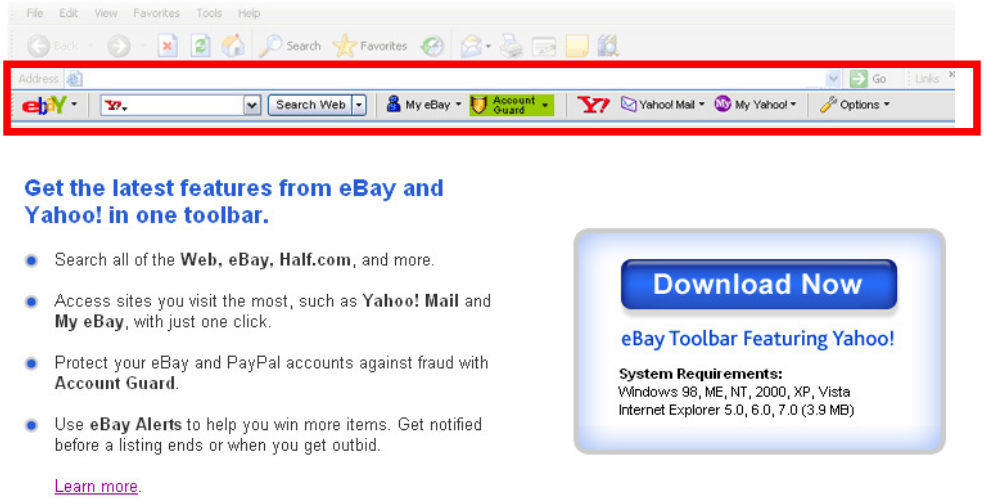


圖 16：TRUSTe 所發出之審核標誌

註、資料來源

Ebay 網站

(四) EBay toolbar：功能面與安全面防護兼具之實用工具。Ebay 會員可以透過已安裝於網頁之 toolbar 搜尋 ebay 商品、Yahoo 網頁資訊、Yahoo email 等等。當會員進入假冒的 ebay 網頁(釣魚網站)時，toolbar 會自動偵測出現提醒訊息，避免會員受騙登入了竊取帳號密碼的網站。

(五) eBay 內部權限控制網絡：ebay 內部員工從基層到高階，根據業務別細分每個人的帳號權限。以客戶支援部門來說明，不同的支援別又細分限制使用內部工具之權限。所以同是隸屬於客戶支援部之員工，會因其工作內容而被限制僅可使用相關聯之調查工具。所有的電腦登入(Login)密碼，強制在固定期限內必須變更。數據資料更是嚴謹，非屬分析師業務者，無法透過 DW 匯出供分析之資料。所有的報表資料，每一項目皆有專屬之縮寫代號代表，

就算不小心遺失報表或失竊，非 ebay 內部員工，也無法從報表中得知該數據所代表之意思。

(六)　GR 部門：eBay 爲了加強與警方間合作默契，在交易安全部門內增設 GR(政府關係管理部門)，透過全球參訪及演講，宣導 ebay 交易安全的成效，更積極與政府警方合作，調查跨國網拍犯罪事件，建立國際假冒網站之移除聯繫網絡。

四、　業界實際狀況及困難

並非所有的企業都能像 ebay 一樣，願意且有能力投入大量的資源及金錢。企業的經營，通常都是「先求有再求好」，基本獲利掌握住，才有可能將編列預算投入資安建設。另一個原因爲，大部分企業，皆不知該如何著手?因此，台灣電子商務網站廣泛存在著資安建設不足，主要的原因是-規模小。如政府能透過如同集約化經營之模式，從流程、控制、改善、人員教育訓練全面性的發展，輔導中小企業提升資安實務，如此一來，才能協助台灣企業升級，突破資安建設門檻。

第五項、　個資法對於電子商務之影響及衝擊

電腦處理個人資料保護法(簡稱個資法)，雖然尚未三讀通過，但因其修法重點第一是「擴大適用」，將原本只對「特定行業」適用，擴大爲所有公、民營事業均適用；其次是「加重刑度」，將意圖營利而竊取、洩漏個資等行爲，由最高可處兩年徒刑，提高爲五年。此修正草案一旦三讀通過，對整體社會個資外洩的情況，必施嚇阻之用。

一、　新法對於購物網站規範範疇

個資法尚未修改前，網站對於會員的資料採多多益善之態度，取得會員越多資料，網站業者就越能夠過這些資料分析會員客群，針對不同族群進行行銷規劃。個資法上路後，購物網站對於持有會員個資，所應負擔的責任也就相對沉重。購物網站將可能面臨以下問題：

(一) 因個資法是採推定過失責任，即企業必須證明其就會員個資的外洩無故意或過失，否則即應負擔賠償責任。困難就在於舉證。所謂舉證之所在，敗訴之所在。因此，企業應打從根本全面落實會員隱私權聲明及盡最大之努力保護會員個人資料。

(二) 團體訴訟[313]：透過團體訴訟，小蝦米也能對抗大鯨魚，企業被迫正視個資外洩問題。以 EBAY 韓國過去曾發生過個資外洩之情況，外洩個資量約 1000 萬筆。10 萬人參與訴訟，每人求償金額爲美金 3000 元。

(三) 個資法訂立法定賠償金額，每人每一事件新台幣二萬元以上十萬元以下，基於同一原因事實，賠償總金額合計以新台幣五千萬爲限。對於規模較小之網站，只要發生一次資料外洩意外，公司就可能無力支付這高額的賠償金而導致破產關門大吉。經過利弊分析評估後，顯示在投資報酬率(ROI)上，企業對於資安投資意願應該相對提升。但政府應輔導這些中小企業，在符合效益的原則下，進行資安防護。以免法令間接壓抑產業發展。

(四) 降低會員個人資料需求。若企業評估後，仍無法增加資安投資，最簡單的方法就是在可運作的範圍內，儘可能降低會員個資提供量。

(五) 企業面對個資法，除了既定之規範外，還須克服法令上的限制條件，蒐集個資須當事人「書面」同意。書面方式並非目前網站確認當事人同意使用個人資訊的方式，如愈符合法令規範採書面形式，將產生極大的作業困難。

二、 政府能做什麼?

先進國家如日本、歐美的政府和民眾，對於個人資料以及企業隱私權均十分重視，透過專業的個資保護處理，不僅讓企業建立好的形象，也能顯示一個國家消費友善環境進步的程度；我國政府應急起直追，加強落實個人資料保護，並負起教育大眾和企業經營者的責任。借鏡鄰近國日本，日本在 2003 年 5 月通過個人情報保護法，明訂只要擁有 5,000 筆以上個資的公、民營機構，就得做好資料外洩防範；2005 年施行 P Mark 制度，到今年初內閣指出，

[313] 增訂相關團體訴訟之規定，爰將章名修正爲「損害賠償及團體訴訟」。

只有 3 家企業，因違反 JPIPA 勸告後被罰。在在顯示，政府給予明確的執行方向，外加法令規範，其業者自律力量將能發揮到極致。我國個資法修正草案業已通過一讀，通過朝野協商，即可送交二、三讀完成立法。企業各界相當關切，但如何做好個資保護，卻毫無所從。APEC 將在 2010 年就貿易便捷化措施作總結，其中就包括隱私權標章認證制度。因此 P Mark 即將成爲國際隱私權保護的標準，我國該主動建制台灣的隱私權標章認證制度，以參與亞太國際貿易競爭。[314]

初步建議如下：

1. 政府補貼中小企業資安預算：資安設備與服務對於一般中小型網站，屬昂貴投資。舉例如網路安全監控設備個資料流網路服務監控設備來說，低階(可處理 20 萬個資料流)費用 21 萬，中階(可處理 100 萬個資料流)，費用 110 萬，高階(可處理 200 萬個資料流)，費用 140 萬。以一般中小網站會員個資量，至少都須花費 20-110 萬元。網站弱點掃描也由 40 幾萬到 80 多萬部等。而實務上，除了大型網站會採購進階設備或資安服務外(進階設備爲有無該設備，皆不影響網站運作。)，一般中小型網站，在網站尚可營運之狀況下，並不會特別編列針對保護會員隱私之高階設備。很不幸的是，一但發生資安事件，消費者個人資料將大批洩漏，特別是網路公司，且因數位化，難以追回。倘若政府可以透過輔導計畫，透過有效的輔導模式，採政策補助加廠商自籌款比例分是，補助網站資安升級，且透過輔導案，更能有效掌握及追蹤補助成效。經濟部商業司自 2005 年起，已因應 B2C 線上購物市場之需求，在營業登記項目上增設無店面零售業，讓 B2C 的市場經營模式有所明確定位，並積極建立計畫與機制進行相關輔導。未來在相關輔導作業上，亦可增加資安輔導之規劃。2009 年初，依行政院經濟建設委員會第 1352 次會議委員會會議記錄(98.02.10)[315]，提出「振興經濟擴大公共建設投資—智慧台灣」六項中

[314] http://www.ctjob.com.tw/EnterprisesNews/News.aspx?ArticleId=7545(Last visit：2009.6.30)

[315] 依會議結論，本項計畫針對(一)本計畫推動工商憑證普及化，強化工商資訊系統，提升零售業資通安全，輔導新開店商家導入 e 化應用，有助於國家競爭力之提升，原則同意。(二)爲確保工商憑證有效利用，憑證免費發放應與報稅、勞健保等電子化政府相關應用結合，以有需求之企業爲主要發放對象，並請經濟部加強工商憑證宣導推廣工作。參見 http://www.cepd.gov.tw/ml.aspx?sNo=0011546 (last visited 2009.6.30)。

長程計畫中的第四項計畫即爲「加速企業網路應用暨資安提升計畫」。惟該項計畫提報立法院預算審查時，遭立委質疑有關「零售業資安提升計畫」係以1.2億經費補助大型企業(如新光三越、衣蝶百貨、頂好超市、松青超市、7-11超商、全家超商、全虹通訊、神腦國際、家樂福、大潤發、夢時代、遠企、台茂購物中心、富邦、東森電視購物、中華電信 emome 行動購物等[316])，反之，真正需要積極提升資安效能之中小企業恐未能有效受惠。2009年八月底，經濟部商業司宣布委託中華民國資訊軟體協會推動「提升零售業資安品質計畫」，此次資安品質提升計畫，從認知推廣、教育訓練、檢測診斷，以及導入服務，提供完整的推廣方式，藉由中華民國資訊軟體協會召集 35 家具有豐富經驗的資安廠商，配合全省各地零售業者提出的需求，從防止電腦病毒、程式安全檢查、預防駭客入侵，以及企業內部如何建立資安管理制度，均提供零售業完全免費的服務。並於 9 月 14 日在台大醫院國際會議中心舉辦「2009 零售業資訊安全高峰論壇」，日後並將定期在北、中、南等地舉辦個資保護月及資安推廣研討會，協助業者打造消費者可信賴的購物環境[317]。

另一方面，在補助案量化下，政府更能協助輔導商爭取到最低之設備或服務價格。

表 4：網路安全監控設備契約價格預估表

項次	品名	契約單價
60.03	網路安全監控設備 20 萬個資料流網路服務監控設備	529,638
61.01	網路安全監控設備 100 萬個資料流網路服務監控設備	996,680
61.02	網路安全監控設備 100 萬個資料流網路服務監控設備	1,119,403
61.03	網路安全監控設備 100 萬個資料流網路服務監控設備	1,172,708
62.01	網路安全監控設備 200 萬個資料流網路服務監控設備	1,452,462

[316] 自由電子報—亂花錢 1.2 億補助大企業提升資安，2009.02.26 參見 http://www.libertytimes.com.tw/2009/new/feb/26/today-p12.htm(last visited 2009.6.30)。

[317] 提升零售業資安品質計畫 協助零售業提升資訊安全意識，經濟日報，2009.09.15,http://edn.gmg.tw/article/view.jsp?aid=185175&cid=10

62.02	網路安全監控設備 200 萬個資料流網路服務監控設備	1,705,757
62.03	網路安全監控設備 200 萬個資料流網路服務監控設備	1,812,367

項次	產品名稱	決標金額
71	DragonSoft 全中文安全弱點掃瞄軟體-專業版,50 U (授權壹台主機，Client 端 50U；授權書加光碟含壹年弱點更新與支援)	77,630
72	DragonSoft 全中文安全弱點掃瞄軟體-DVM 版(授權壹台主機，Client 端無限制；授權書加光碟含壹年弱點更新與支援)	853,000
73	DragonSoft 全中文安全弱點掃瞄軟體-全自動 Advance 版 (授權壹台主機，Client 端無限制；授權書加光碟含壹年弱點更新與支援)	440,379

註、資料來源
筆者自行整理

2. 鼓勵並補助自然人憑證之運用：自然人憑證發卡量，安全性與不可否認性，雅虎已率先使用於登入流程。如目前由於自然人憑證之使用範圍多存在於公家單位，因此人民對於自然人憑證之使用需求極低。建議政府應設立自然人憑證應用小組，專門發展自然人憑證的運用，免費申請自然人憑證，降低申請門檻。內政部亦透過活動抽獎，來增加及延續自然人憑證之使用率。

圖 17：自然人憑證展期抽獎活動

註、資料來源
內政部憑證管理中心

3. 將自然人憑證帶入網購流程中,甚至網站註冊流程中,將可漸漸發展成”不記名註冊”。減少註冊會員需填寫個人資料量，相對的也減緩網站個資外洩之內容量。從註冊、登入、購買皆可運用自然人憑證取代帳號密碼。透過程式端與內政部自然人憑證資料庫確認「特定人」身分(非個人資料)，完成內政部資料庫之實名認證。網站本身僅取得認證時的自然人憑證資料，並無法取得該認證人存在於內政部資料庫之個人隱私資料。自然無個資外洩之問題及風險存在。惟在自然人憑證推廣使用方面，未來如果擴大其使用範圍，使其應用相容於其他屬性憑證時(如衛生署之醫師人員憑證及公務員公文簽核之應用等)，宜注意電子簽章中的 CPS(Certification Policy Statement)範圍，並宜注意電子簽章法相關配套運作及應用。

4. 輔導中小企業建立個人資料保護措施：中小企業多半未經過資安認證，亦無正確觀念。如，資料庫權限分層控管，進出資料庫 log 資料異常警示、登入個資資料庫時禁止工程師使用任何傳訊軟體及隨身碟、密碼強制加密等等。政府可規範出一套標準作業程序，供企業遵循，如企業無法自行完成所

有資安作業程序，亦提供認證協力廠商，供企業選擇來完成資安認證。針對完成認證之廠商，給予認證標章或減稅補貼。

5. 獎勵創新注重個人隱私之資訊流、金流、物流流程：網路透物透過資訊流、金流、物流三端串接而成。因此各個階段作好個資保護，就能降低個資外洩之風險，也易追查問題點爲何。例如：如網友可使用悠遊卡序號在網站上購物，至選擇之取貨便利超商取貨，且於超商內確認貨物及使用悠遊卡付款。如圖示：全部流程皆無買家之個人身分資料，透過間接方式來確認「買方身分」(如條碼、悠遊卡序號、icash 卡)，只須買家所出示之取代傳統之確認「買方個人資料」，方便安全也快速。立法院通過電子票證發行管理條例一案，讓其他流通量大之儲值卡運用更爲廣泛，再者，儲值卡最高儲值金額 1 萬元之限制，已足以應付一般之網購品單價，也可避免一旦網購受騙民眾損失額度。以上述爲例，7-11 之 Icash 卡即可取代較有地域性流通之悠遊卡。

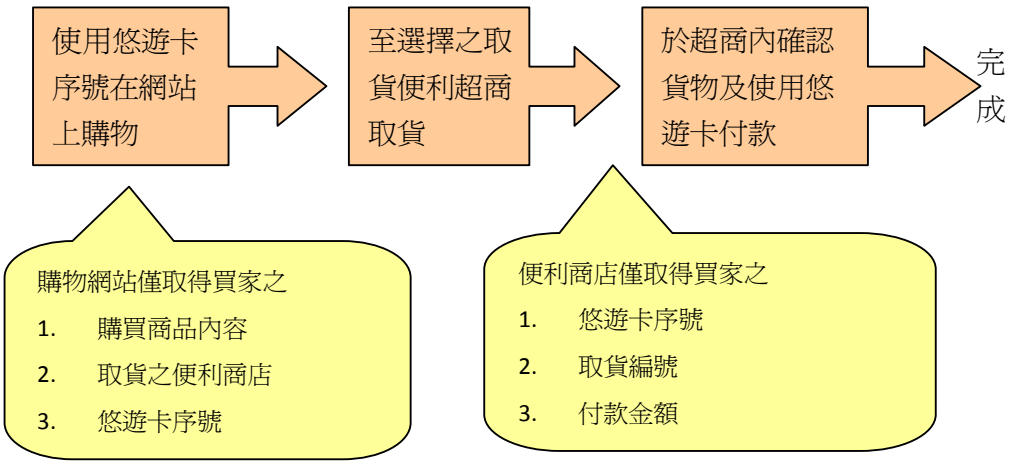


圖 18：悠遊卡購物、取貨及付款流程

註、資料來源

筆者整理

6. 政府應帶頭倡導帳號密碼安全觀念，甚至全面間接密碼化，透過 token 或簡訊密碼鎖等等形式，取代一般的帳號密碼形式。根據 ALS / NII 產業發展協進會最新完成的「2007 台灣網路安全信心調查」[318]，國人網路安全信心不足，僅 34.4%表示有信心，63.1%擔心個人資料外洩。整體而言，38.5%受訪民眾對網路安全沒有信心，比例高於有信心的 34.4%與持平的 25.2%。與先進國家相較，有信心的比例亦低於美國的 53%及德國 43%，突顯國人的網路安全信心不足。 就個別項目來看，最有信心的是『自己能安全使用網路』，佔 56.3%；其次爲『電腦防毒防護軟體可提升網路安全』的 52.7%；第三名爲『政府 e 化服務』的 35.7%，顯示民眾對於自己可掌控項目的信心度，遠高於政府與業者掌控項目。

而最沒信心的前三大項目依次爲『業者保護個人資料』(63.1%)、『政府保護個人資料』(45.2%)、『網路交易安全』(44.7%)，顯見民眾對個人資料保護與網路交易安全問題相當擔憂，不管是企業或是政府保護個資方面，若無法改善，將不利於網路服務的未來發展。因此，政府應先做起個資火車頭，由自身先效行個資安全保護，進而強制合作廠商也應遵照辦理，慢擴大到私企業。未來不再發生公部門個資外洩之新聞，以提升民眾對政府之信心。

第六項、 結論

MIC 調查數據顯示在金融業部份，僅有 7.1%選擇減少支出，有 31.8%都會在明年加碼資安投資，另外六成則打算持平。似乎多數業者仍在觀望此法案之後續發展。近幾年個資外洩事件頻傳，最後結果似乎皆無疾而終。嚴重傷害民眾財產損害，更打擊網友對於網購安全信任度。政府應盡快三讀通過個資法修正草案，讓所有資安事件有法可循。另一方面，行政機關應針對民眾加強宣導，保護個人資料安全之觀念，提供個人資料要謹慎，並了解個人資料之用途爲何?相信消費者與業者共同努力下，台灣資安環境才能全面提升。另一方面，在景氣寒冬中，政府如能協助中小企業，透過補助輔導企業

[318] http://www.als.org.tw/article/new_paper_sg.asp?id=168(Last visit：2009.6.30)

成長。台灣個人資料防護機制，必定能更進一步大幅降低資料外洩對人民經濟所成造成的損失。

第六章　德國個人資料保護標誌與日本 P-Mark 制度相關議題探討

第一節 德國個人資料保護標誌及個人資料保護審核制度[319]

近年來在歐陸方面的德國，透過聯邦個人資料保護法 (Bundesdatenschutzgesetz，BDSG) 及州政府個人資料保護法 (Landesdatenschutzgesetz，LDSG) 之授權，訂定了相關辦法及審核規定以實施個人資料保護標誌 (Datenschutzgutesiegel) 制度[320]，以強化個人資料之保護[321]。

爲確保個人資料保護得以落實，Schleswig-Holstein 州於 2000 年依該州個人資料保護法第 32 條設立該州的獨立個人資料保護中心 (Unabhangiges Landeszentrum fur Datenschutz Schleswig-Holstein，簡稱「ULD」)，其爲德國行政法上的公法營造物 (rechtsfahige Anstalt des offentlichen Rechts)，具有獨立行使職權的能力，負責公部門在法規上及技術上有關個人資料保護及個人資料安全的管理以及私部門相關議題之諮詢工作。ULD 自成立之後，便積極參與有關個人資料保護及個人資料安全的計畫 (如 Platform for Privacy Preferences，簡稱 P3P、Java Anon Proxy/JonDo，簡稱 JAP、歐盟的 Identiatsmanagement 計畫，簡稱 IdM、Datenschutzaudit、Datneschutz-Gutesiegel 及 European Privacy Seal

[319]德國個人資料保護標誌及個人資料保護審核制度簡介－以 Shleswig-Holstein 州爲例，葉亭巖撰，載於科技法律透析，2009 年 3 月，第 20～26 頁。

[320] LDSG 是在不違反 BDSG 之規範下所制訂的各州個人資料保護法，各州所規範內容不盡相同，但其所遵循的原則及方向是一致的，惟值得注意的是，有些州並未將個人資料之審核及個人資料保護標誌規範納入。

[321]爲保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損，進而造成個人隱私權之侵害，德國於 1990 年即制定「聯邦個人資料保護法」，後因歐盟於 1995 年制訂了個人資料保護指令，各會員相繼制訂或修改其國內法將指令轉換爲國內法律，德國聯邦個人資料保護法即據此修改相關規定，增加有關個人資料保護監督機構 (Beauftragter) 及個人資料保護審核之相關規定，以符合歐盟個人資料保護指令之要求。惟在德國各州有關個人資料保護審核及規定及個人資料保護標誌制度最爲完整的則爲德國北部的 Schleswig-Holstein 州，因此，接下來有關隱私權標誌制度之介紹將以該州爲主要討論之對象。

，簡稱 EuroPriSe 等)，推動個人資料保護在研究及實務上的發展，因而成爲歐洲個人資料保護審核(Datenschutzaudit) 及個人資料保護標誌(Datneschutzgutesiegel) 制度之先驅。而 ULD 自 2001 年起至今，已頒發 59 個個人資料保護標誌予 IT 產品及其相關服務，以及 24 個個人資料保護審核標誌予通過個人資料保護審核之機關單位。

爲提供民眾對於處理個人資料之企業、政府機關單位之信賴，以及刺激保護隱私相關之科技技術和服務之發展， Schleswig-Holstein 州的個人資料保護法第 4 條第 2 項及第 43 條第 2 項提供了個人資料保護標誌及個人資料保護審核制度之法源，藉此提供公開、公正的審查項目及程序以供遵循及參考。Schleswig-Holstein 對於個人資料之保護，係透過該州之個人資料保護法規範有關處理個人資料產品之認證制度，以及要求公務機關應採取個人資料安全之適當措施，並對公務機關個人資料保護之工作進行審核及認證，藉此提供民眾對於隱私權之信賴基礎、刺激與隱私相關之科技技術與服務發展，以落實個人資料保護之工作。以下將分別簡介個人資料保護標誌及個人資料保護審核相關規定：

圖 19：個人資料保護標誌圖

註、資料來源
ULD 網站

圖 20：個人資料保護審核標誌

註、資料來源

ULD 網站

一、個人資料保護標誌 (Datenschutzghtesiegel)

依據 Schleswig-Holstein 州的個人資料保護法第 3 條之規定，該法規之適用範圍爲該州之公務機關 (offenliche Stelle) 或受公務機關委託行使公權力的私部門，再依同法第 4 條第 2 項之規定，公務機關處理個人資料時，應優先使用符合個人資料保護及經確認符合一定資料安全程序規範之產品。因此，州政府於 2001 年 4 月制定有關頒發「個人資料保護標誌之審核程序規則」(Gutesigelverordnung nach § 4 Abs.2 LDSG - Landesverordnung uber ein Datenschutz, Datenschutzauditverordnung，簡稱「DSAVO」)，以規範審核產品程序等相關事項。

(1) IT 產品之認證

製造者或經營者得就其生產及銷售而爲公務機關所使用之硬體、軟體或自動處理程序交由 ULD 進行認證，視其是否符合個人資料保護以及個人資料安全之相關規範。若經由 ULD 認證其已符合相關規範，則可頒發具有認證編號及有效期限兩年之標誌，以示證明；但若 ULD 事後發現該 IT 產品已不具通過認證之要件時，則可撤銷所授予之認證標誌。

(2) 經 ULD 承認專家

ULD 可授予具有專業知識、且可信賴及能獨立審核之專家認證，並以適當之方式公開獲得認證專家之名單，以供查詢；此外，ULD 應審視專家是否具有相當資格得以適任，否則得撤銷其認證。

(3) 選定認證之專家及相關程序

申請者得委託經 ULD 承認之專家進行審核、認證程序，並由專家提出載明以下項目之書面資料，交由 ULD 就審核的邏輯方法及專家審核的角度再次審核後，始能獲得個人資料保護標誌，其中包括：a. 審核時間；b. IT 產品詳細的名稱；c. 使用之目的；d.IT 產品的特別功能，特別是具有避免及減少使用個人資料 (第 4 條第 1 項及第 11 條第 4、6 項 LDSG)、資料處理安全(第 5、6 條 LDSG)、保障資料主體權利(第 26-31 條 LDSG) 之功能；e. 特別功能之評斷 f. 綜合審核意見等。

(4) 認證費用 －ULD 可就其所被交付的認證工作依費用規則 (Gebuhrenordnung) 收取適當費用[6]。

二、個人資料保護審核制度 (Datenschutzaudit)

除了個人資料保護標誌之規定外，Schleswig-Holstein 州之個人資料保護法亦於第 43 條第 2 項規定，該州之公務機關得自發性地就其所提出之個人資料保護政策供 ULD 審核及評斷，以確保其符合個人資料保護相關法規之規範，並能獲得民眾之信賴，因而於 2001 年公布「ULD 執行個人資料保護審核規定」(Anwendungsbestimmungen des Unabhangigen Landeszentrums fur Datenschutz zur Durchfuhrung eines Datenschutzaudits nach § 43 Abs. 2 LDSG，簡稱「HDSA」) 規範其詳細之內容。

(1) 審查之對象及客體

該項審核之進行對象僅爲該州之公務機關及受委託行使公權力之私人企業，而審核之核心項目包括：個人資料保護及個人資料安全內部管理系統(Datenschutzmanagementsystem，其包含單一自動化程序及非自動化個人資料處理程序) 之說明、UDL 就被審核機構之過去個人資料保護成果審查及未來個人資料保護目標等項目，待審查通過後，ULD 將授予該公務機關認證。

(2) 審核認證之期限

審核認證之期限爲三年，期間內若有違反個人資料保護法規及資料安全規範等事項，ULD 則可將其審核通過之認證予以撤銷。

(3) 審核程序

公務機關申請個人資料保護之審核應與 ULD 有一書面之協議，其協議內容包含： a.審核之種類及範圍；b.個人資料保護審核之流程，其中包括：實施個人資料保護成果之審查、未來個人資料保護目標之確立、個人資料保護管理系統之建立、ULD 對該公務機關之審查鑑定及授予個人資料保護審核標誌；c.執行審核之時間及個別之步驟等．

(4) 重新取得審核認證

公務機關於三年之有效期間經過後，應更新其過去實施個人資料保護之成果、制訂適合的個人資料保護聲明，並獲得 ULD 之審查鑑定意見後，重新獲得 ULD 授予之認證。

三、小結

Schleswig-Holstein 自 2001 年推行個人資料保護標誌及個人資料保護審核制度至今，已頒發共 83 個認證通過之標誌予 IT 相關產品、服務及公務機關，且每年申請審核及認證的數目逐漸增多，重新取得審核認證的之產品及服務亦佔總數的 32% (相關數據請參見下表)，由此可見，該制度已獲得廠商及公務機關之信賴，藉此彰顯其對於個人資料保護之重視。雖然 Schleswig-Holstein 對於個人資料保護標誌及個人資料保護審核制度僅就公務機關實施，卻已有相當之成效，此外，制該度也獲得歐盟層級之重視，並參考該制度自 2007 年 7 月起試行歐盟隱私權標章 (European Privacy Seal，EuroPriSe)[322]。因此，未來若可擴大其實施對象自私部門，俾能將該制度發揮更大之效用，以利用市場機制將個人資料保護之推行至每個使用者。

[322] EuroPriSe 相關資訊請參考：https://www.european-privacy-seal.eu/ (最後到訪日：2009.6.30)

表 5:個人資料保護標誌及個人資料審核認證通過數量表(2002-2008/12/10)

	個人資料保護標誌數量	個人資料保護審核制度數量
2002	0	2
2003	4	5
2004	2	4
2005	9	0
2006	5	5
2007	20	7
2008	19	1
重新取得	18	1

註、資料來源
ULD 網站相關整理

若我國未來如參考德國 Schleswig-Holstein 州所推行之制度建立隱私權標章，或有以下幾點應予考量：

1、成立獨立機構，廣邀專家學者加入：隱私權標章制度影響民眾對於電子商務產業之信心，因此，建議應成立公正獨立之機構審核認證申請者提出之資料，並廣邀具有技術或法律專長的專家學者加入，參與審核及認證工作，以增加隱私權標章制度之可信任性。

2、非公務機關亦應納入審核認證之對象：隱私權標章制度受規範對象討論仍多侷限於電子商務業者，然而，德國 Schleswig-Holstein 州卻僅侷限於公務機關，因此，未來我國在設計該制度時，若能取長補短建立全面性的隱私權標章制度適用對象，則不僅可以促進電子商務產業發展，亦可兼顧我國公務機關個人資料保護工作。

3、審核項目及程序法規化：未來若推行隱私權標章推行後，是否取得隱私權標章將可能影響消費者與之交易之意願，亦或可能影響民眾使用電子化服務之意願，因此，對於其審核項目及審核程序之進行之瞭解，將能決定其是否準備完善而得以取得隱私權標章。有鑑於此，審核項目及程序應一併納入法規範，並公開予民眾，提供欲申請者得以事先瞭解審核之內容。

4、訂定有效期限，並可撤銷取得之標章：科技技術日新月異，對於個人資料保護之政策亦將隨著技術進步而有所改變，因此，隱私權標章應訂定有效期限，促使獲得者能持續關注個人資料保護之議題，更新其對於隱私權保護之政策。再者，若發現獲得標章之單位違反個人資料保護規範事項，亦應即時撤銷其標章，以取信於大眾。

5、建立申訴之管道，並教育民眾：認證乃短時間之決定，但使用者與獲得標章組織之接觸及互動時間較長且頻繁，再者，申請認證之組織欲通過審核認證，勢必會將最好之表現呈現於專家面前，因此，審核認證之機構應建立可申訴之管道，提供民眾檢舉違反規範之組織單位，並同時接受民眾之諮詢，適時教育民眾有關個人資料保護之觀念。

第二節 日本的 P-mark 制度

日本於 20 世紀 90 年代末期分別建立了「個人資料保護管理體系」（Personal Information Protection Management System, PMS）與「隱私標章」（Privacy Mark）制度。前者透過規劃並導入管理系統的作法，協助企業強化維護個人資料之能力；而後者則是以前開管理體系爲基礎，提供各界一個判斷企業資訊安全制度健全與否的公正指標。

爲回應 OECD 於 1980 年發布的八大原則，通商產業省曾於 1989 年制定「私部門電腦處理個人資料保護指針」（民間部門における電子計算機処理に係わる個人情報の保護について(指針)）。而當歐盟於 1995 年公布「個人資料保護指令」後，爲恐影響國際貿易市場，日本政府不得不正視「私部門」個人資料保護的問題，從而於 1997 年再度制定「私部門電腦處理個人資料保護準則」（民間部門における電子計算機処理に係る個人情報の保護に関する

ガイドライン）[323]，以期在正式立法前，迎合歐盟指令之要求[324]。

爲強化企業保護個人資料的能力，使日本成爲歐盟指令所稱具有「適當」（adequate）保護機制的國家，日本情報處理開發協會（Japan Information Processing Development Corporation，以下簡稱 JIPDEC）基於前開準則，依據日本「工業標準化法」規定，於 1999 年 3 月訂定了「個人資料保護實踐計畫之要求事項」（個人情報保護に関するコンプライアンス・プログラムの要求事項），而 JIS Q 15001 即爲其編號。除前述已提及的 JIS 外，Q 是指「日本工業規格」分類中「標準物質/管理體系」（標準物質/管理システム）項目之代碼，15001 則是代表大分類「1」及中分類「5」下的 001 號規格。

JIPDEC 制定 JIS Q 15001 的用意，如同其全稱般，在於揭示企業導入個人資料保護實踐計畫時所應採納的事項。由於相關規定事實上僅爲最低限度之要求，因此無論企業產業別爲何，抑或規模之大小，均可配合其自身的特性，依據 JIS Q 15001 設計專爲其量身打造的個人資料保護管理體系。而隨著日本政府於 2005 年全面施行規範私部門的「個人資料保護法」，JIPDEC 也依循「個人資料保護法」及根據該法第 7 條制定的「個人資料保護法基本方針」（個人情報の保護に関する基本方針）[325]，於 2006 年修正原有 JIS Q 15001 之內容。故在日本實務上，一般亦往往以 JIS Q 15001：1999 及 JIS Q 15001：2006，區別版本之差異[326]。

除 JIS Q 15001：2006 外，在日本另有「資訊隱私管理體系」（Information Security Management System, ISMS）工業規格 JIS Q 27001:2006[327]；惟此

[323] 平成 9 年(1997 年)3 月 4 日通商產業省告示第 98 號。

[324] 參 JIPDEC 隱私標章促進中心(財団法人日本情報処理開発協会プライバシーマーク推進センター)編，個人資料保護管理體系實施指針(個人情報保護マネジメントシステム実施のためのガイドライン)，日本規格協會發行，第 1 版第 5 刷，頁 8，2008 年 4 月。

[325] 平成 16 年(2004 年)4 月 2 日閣議決定。

[326] 參 JIPDEC 隱私標章促進中心，前揭書，註 14，頁 9。

[327] 日本通商產業省曾於 1981 年發布「資訊系統安全對策實施事業所認定制度」（情報システム安全対策実施事業所認定制度），成爲現行日本資訊隱私管理體系的前身。而當經濟產業省於 2001 年廢除前開認定制度後，JIPDEC 緊接於 2002 年 4 月開始推動「資訊隱私管理體系妥適性評價制度」（情報セキュリティマネジメントシステム適合性評価制度），當 ISO/IEC 於 2005 年 10 月發布 ISO/IEC 27001：2005（Information technology - Security techniques - Information security management systems - Requirements），日本亦於 2006 年將其轉化爲內國工業規格，成爲現今的資訊隱私管理體系 JIS Q 27001:2006。參岡村 久道，情報セキュリティの法律，商事法務，初版 1 刷，頁 254，2007 年 7 月。

一管理機制是針對所有可能產生隱私風險的「資訊資產」進行制定，其範圍涵蓋個人資料，但並不以「個人資料」爲限[328]。而就現行日本個人資料保護管理體系 JIS Q 15001：2006 而言，包括了：1、適用範圍；2、用語及定義；及 3、要求事項等三個部分；其中，又以第三部分「要求事項」最爲重要。

爲有效落實個人資料保護工作，JIS Q 15001：2006 採行 ISO Guide 72：2001（Guidelines for the justification and development of management system standards）有關「管理系統」建立的標準，並具體導入了由戴明（Edwards Deming）博士提出的 PDCA 循環（PDCA Cycle）概念。所謂的 PDCA，分別指 Plan（計畫）、Do（執行）、Check（查核）及 Act（改善）等四者，而 JIS Q 15001：2006「要求事項」即以 PDCA 爲基礎進行設計，透過不斷地進行「計畫→執行→查核→改善」此一循環，期使導入之企業得以持續精進其個人資料保護管理體系[329]。

表 6：PDCA 循環下的 JIS Q 15001：2006 要求事項

項號	內容	項號	內容
Plan（計畫）		3.4.3	適當管理
3.1	一般要求事項	3.4.4	資料本人之權利
3.2	個人資料保護方針	3.4.5	教育
3.3	計畫	3.5	個人資料保護管理體系文件
3.3.1	特定個人資料之範疇	3.5.1	文件之範圍
3.3.2	法令、準則及其他相關之規範	3.5.2	文件管理
3.3.3	對於風險之認識、分析及對	3.5.3	紀錄管理

[328] 參淵邊 善彥、五十嵐 敦編，前揭書，註 8，頁 188。

[329] 參 JIPDEC 隱私標章促進中心，前揭書，註 14，頁 17。

	策		
3.3.4	資源、職掌、責任與權限	3.6	申訴及諮商之因應
3.3.5	內部規則	Check（查核）	
3.3.6	計畫書	3.7	查核
3.3.7	緊急情事之應變	3.7.1	運用之確認
Do（實施）		3.7.2	監督
3.4	實施與應用	3.8	改正處置及預防處置
3.4.1	運用程序	Act（改善）	
3.4.2	蒐集、利用及提供之原則	3.9	事業代表人之改善

註、資料來源

JIPDEC 隱私標章促進中心「個人資料保護管理體系實施指針」；筆者整理製表

除納入 PDCA 循環概念外，JIS Q 15001：2006 的另一項特色，則在於管理體系本身與日本現行個人資料保護法制緊密關聯的程度。當日本於 2005 年全面實施「個人資料保護法」並於制定「個人資料保護法基本方針」後，JIPDEC 即將前述兩者有關事業於個人資料蒐集、處理與利用上所應遵守的事項及所負之義務，具體落實於 JIS Q 15001：2006 內容中。故可知導入「個人資料保護管理體系」的企業，即代表該業者確實依循現行個人資料保護規範，妥善維護並具體執行個人資料保護工作。

第一項　隱私標章（Privacy Mark）制度之設計

日本政府爲迎合歐盟指令的要求，雖於 1997 年發布了「私部門電腦處理個人資料保護準則」，然而個人資料外洩事件卻仍層出不窮。爲有效落實前開準則的要求，JIPDEC 在通商產業省的指導下，於 1998 年 4 月推動了「隱私標章」（プライバシーマーク）制度，並以 1997 年發布的保護準則爲審查標準；凡依據準則內容妥善落實個人資料保護工作且通過審查的民間企業，即可於其轄下的實體店家、網站、職員名片及相關出版品上使用「隱私標章」。透過公正第三機構的審查，使得取得「隱私標章」的企業，除象徵具備維

護用戶個人資料的適切能力外，亦可藉由參與「隱私標章」制度，獲取民眾對於企業之信賴[330]。

另一方面，由於「隱私標章」制度推動不到一年的時間，JIPDEC 旋即制定了 JIS Q 15001，從而 JIPDEC 也立即改以 JIS Q 15001 作爲企業能否取得「隱私標章」的先決條件，期使「隱私標章」制度更昭公信。而隨著 JIPDEC 於 2006 年依據日本「個人資料保護法」及其基本方針修正 JIS Q 15001 規範後，JIS Q 15001：2006 也取代原有的 JIS Q 15001：1999，成爲現階段民間企業能否取得「隱私標章」之審查指標。

第二項　制度推動架構

就隱私標章制度的推動架構而言，分爲兩大部分：其一係由 JIPDEC 本身擔任的「授證機構」(付与機関)，其二則是由其他組織提出申請，並經 JIPDEC 指定而來的「調查機構」(指定機関)[331]。

一、授證機構

「授證機構」可說是整個隱私標章制度的靈魂，而此一重要角色，正是由制度原始推動者 JIPDEC 親自擔綱，負責調查機構的指定、制度管理規範之研擬，以及隱私標章發放等重要工作。爲遂行前述事項，隱私標章制度尚設置了兩個內部單位：

(1)、隱私標章制度委員會（プライバシーマーク制度委員会）：由學者、專家、企業代表、消費者代表及法界人士共同組成的隱私標章制度委員會，專責右揭事項之審議工作：1、制度相關基準、規程之制定與修正；2、調查機構的指定及指定資格之取消；3、隱私標章使用資格之取消；及 4、整體制度之運作狀況。針對第 1 項工作，「隱私標章制度委員會」則訂有「隱私標章制度設置及營運規約」(プライバシーマーク制度設置及び運営要領)[332]，成爲整體制度之規範重心。

[330] 參淵邊 善彥、五十嵐 敦編，前揭書，註 8，頁 156、157。

[331] 前揭註書，頁 157、158。

[332] (最新版本)平成 20 年(2008 年)8 月 8 日施行，全文可自右揭網址下載：http://privacymark.jp/reference/pdf/pmark_guide080808/pmark_guide080808.pdf (last visited Oct. 18, 2008).

(2)、消費者申訴窗口（消費者相談窓口）：消費者申訴窗口的設置，目的在於提供消費者有關個人資料保護事宜的諮商服務，同時接受消費者對於隱私標章制度之申訴。以期透過諮商及申訴內容的分析檢討，研擬防範事件再度發生之措施。

二、調查機構

受到「隱私標章制度委員會」指定的調查機構，則實際負責接受民間企業提出的申請，並於接受申請案件後，就申請人是否符合申請條件進行實質審查，最終作出是否給予申請人隱私標章之決定。若調查機構審查後，認定申請者符合隱私標章使用資格，則應將此一決定向 JIPDEC 進行報告，由 JIPDEC 發給隱私標章。

針對調查機構的指定，「隱私標章制度委員會」訂有「隱私標章授證審查調查機構指定基準」（プライバシーマーク付与認定指定機関指定基準）[333]，凡符合相關條件者，即可向 JIPDEC 申請擔任調查機構。截止 2008 年 10 月為止，受指定的調查機構已達 16 個單位或組織[334]；而其所得接受隱私標章申請的範疇，則可分為三大類：

(1)、以「組織成員」為主：例如「資訊服務產業協會」（情報サービス産業協会）及「電腦軟體協會」（コンピュータソフトウェア協会），僅接受會員之申請。

(2)、以「產業別」為主：例如「醫療資訊系統開發中心」（医療情報システム開発センター），接受醫療、保健及照顧產業之申請。

(3)、以「地域」為主：例如「北海道 IT 促進協會」（北海道ＩＴ推進協会），則僅接受本公司所在地位於北海道之企業所提出的申請案件。

[333] 指定基準全文，可自右揭網址下載：http://privacymark.jp/reference/pdf/pmark_guide080808/Shiteikikan_Kijun.pdf (last visited 2009.6.30).

[334] 指定調查機構詳細名單與資料，可參閱右揭網址：http://privacymark.jp/agency/member_list.html (last visited 2009.6.30).

第三項　隱私標章之申請、審查與發放

凡有意獲取「隱私標章」的民間企業，只消符合下列申請條件，即可向經 JIPDEC 指定的相關調查機構，提出「隱私標章」之使用申請[335]：

1、申請者須於日本當地設有營業據點。

2、依據 JIS Q 15001：2006 揭櫫的要求事項，建立符合企業需求的「個人資料保護管理體系」，並完備得妥善實施該等管理體系之組織架構。

3、申請者不得存有消極條件（欠格事由），並應於申請書中宣誓並無該等事項：

(1)、提出申請之日前三個月內，申請人即曾提出「隱私標章」申請或復審申請，從而遭到否准者。

(2)、提出申請之日前一年內，申請人曾遭取消隱私標章使用資格或解除隱私標章使用契約。

(3)、申請人曾發生個人資料外洩事件，依據 JIPDEC「隱私標章制度設置及營運規約」規定，「禁止申請期間」尚未經過者。

(4)、公司董事（非法人團體之代表人或管理人亦同）曾被處以有期徒期以上之刑，自執行終了或已無須受刑之執行之日起尚未逾兩年者；或曾因違反個人資料保護法而遭處刑罰，自執行終了或已無須受刑之執行之日起尚未逾兩年者。

企業提交申請書並通過「形式審查」後，調查機構將派員至申請人的營業處所，就書面審查階段產生的疑問，以及企業依 JIS Q 15001：2006 導入之「個人資料保護管理體系」進行「實質審查」；而在審查的過程中，調查機構亦得要求申請企業，針對調查人員指摘的缺失事項進行改善。待完成審查程序後，調查機構將依據審查結果作出合格與否之決定，並將其決定通知 JIPDEC。截至 2008 年 10 月為止，全日本共有 9,781 家業者，取得隱私標章之使用資格[336]。

[335] 參淵邊 善彥、五十嵐 敦編，前揭書，註 8，頁 158、159。

[336] 現階段已取得日本「隱私標章」企業之詳細資料，可參閱右揭網址：http://privacymark.jp/

針對調查機構審查合核的企業，JIPDEC 將於其簽訂「隱私標章授與契約」(付与契約)，並將契約書及「隱私標章使用證可證書」(使用許諾証) 交付予申請人。「隱私標章授與契約」的有效期限爲 2 年，企業得於期間屆至前申請延長 2 年；此後則應每 2 年重新提出申請並再次接受審查。凡未申請展延或更新審查的企業，即自動喪失其隱私標章使用資格。

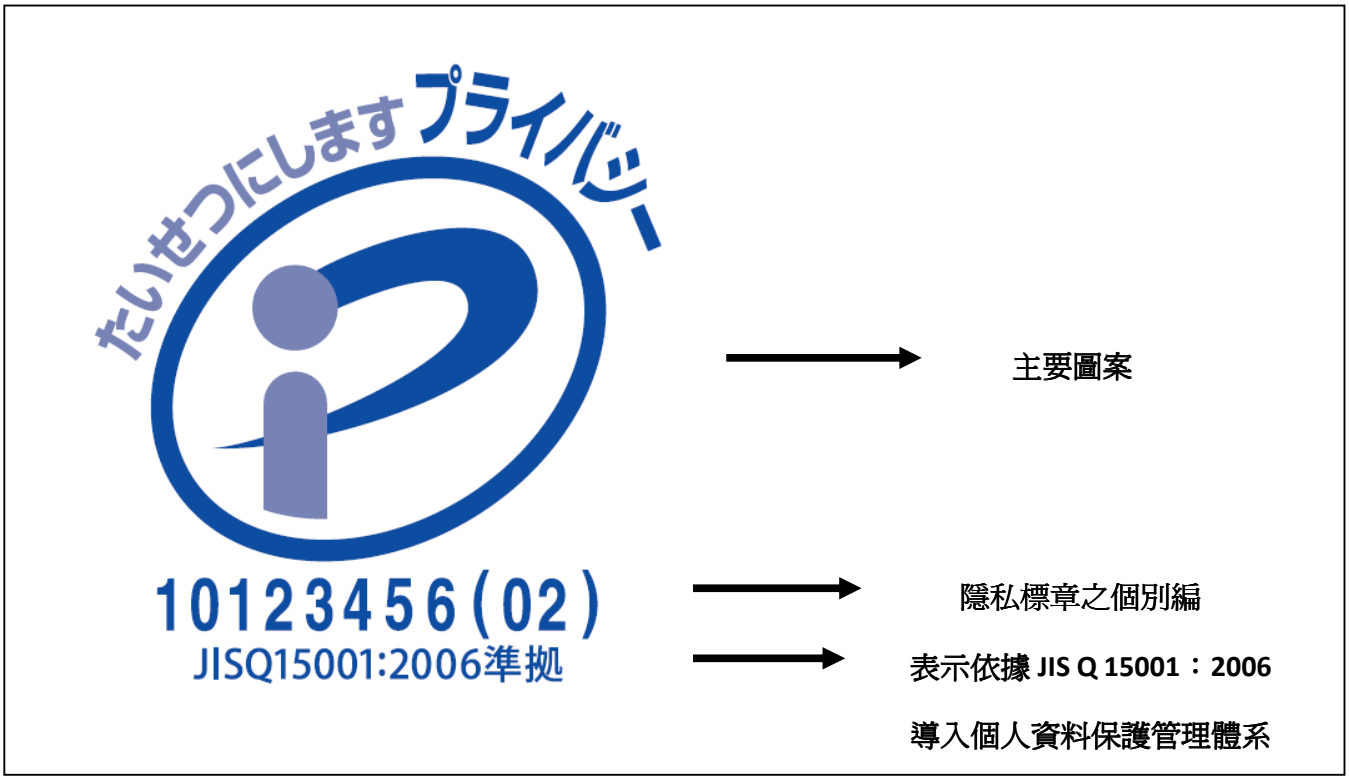


圖 21：日本「隱私標章」樣式及組成部分說明

註、資料來源

JIPDEC；文字部分：研究整理

certification_info/list/clist.html (last visited 2009.6.30).

四、國際合作之推動

資訊科技的快速演進，使得跨國貿易成爲輕易之事，但在打破藩籬的同時，如何確保交易對象的可靠與安全性，往往成爲雙方能否順利達成交易或進行合作的關鍵因素。有鑑於「企業資訊安全」識別的高度需求，除 JIPDEC 所推動的「隱私標章制度」外，事實上各國並不乏相似之機制；然因各國所發放的隱私標章，往往侷限於特定地區或單一國家，若欲使其效力橫跨疆域或國境，則惟有透過跨國合作一途。

爲促進國際貿易的發展，JIPDEC 歷來持續與其他國家隱私保護推動組織洽商合作事宜。2001 年 JIPDEC 首先與美國的 BBBOnLine 共同推動了「相互承認計畫」（Mutual Recognition Program），使得 JIPDEC「隱私標章」與 BBBOnLine 發行的「隱私標誌」（Privacy Seal），於符合特定條件時，彼此將具有對等之地位[337]。繼 BBBOnLine 後，JIPDEC 亦於 2002 年 9 月與韓國「資通訊協會」（Korea Association of Information & Telecommunication, KAIT）達成協議，除各自發行的「隱私標章」及「電子隱私標章」（ePrivacy Mark）外，同時推出「相互承認標章」（參圖二）。此外，中國大陸的大連市爲爭取日方軟體委外（Outsourcing）業務，「大連市軟體產業協會」亦於 2008 年 6 月與 JIPDEC 進行合作，凡通過審查並取得該協會「PIPA 標誌」[338]（參圖三）的軟體業者，亦得申請使用等同於 JIPDEC 隱私標章的「PIPA—P-Mark 互認標誌」（參圖四），藉以獲得日方投資者之信賴。

[337] JIPDEC 與 BBBOnLine 的相互承認計畫，已於 2008 年 6 月 30 日結束。

[338] PIPA 全稱爲 Personal information protection assessment。

圖 22：日韓相互承認標章

註、資料來源

KAIT

圖 23：大連市軟體產業協會「PIPA 標誌」

註、資料來源

大連市軟體產業協會

圖 24：大連市軟體產業協會「PIPA—P-Mark 互認標誌」

註、資料來源

大連市軟體產業協會

第七章　結論與建議

第一節　資訊安全法制之建立

各國關於資訊安全的規範，有概括方式加以規定者，也有在個別領域特別加以立法者(主要爲通訊、金融、醫療等領域)。在不區分領域的立法方式中，一般是針對與資訊安全有關的行爲，作概括性規定，例如 1998 年澳洲通過的隱私權法案(Privacy Act)中確立的的國家隱私原則(National Privacy Principals, NPP)，是於第四條規定任何組織應採取適當步驟，以保護其所持有之個人資訊免於遭誤用、漏失、或未經授權之存取、修改、或揭露；而在個別領域中立法的方式，則是根據產業特性，對於保護步驟有更細緻的規定。在針對個別領域加以立法的情形中，所訂定的法規對於資訊安全，除要求採取技術上的安全措施，並有要求在流程、組織架構上進一步就資訊安全事項加以管理的特色。例如歐盟針對電子通訊業，是於「電子通訊個人資料處理暨隱私權保護指令」（Directive on Privacy and Electronic Communications, Directive 2002/58/EC）第四條要求公共電子通訊服務提供者(public communications service provider)必須提供適當的組織上與技術上措施，以確保服務安全性，並於必要時與通訊網路提供者(communications provider)共同維護網路安全。又因爲上述安全措施是在考量風險與成本後的平衡，因此在採取適當措施後，仍會造成用戶一定風險時，公共電子通訊服務提供者尚必須告知用戶所承擔的風險、如何採取保護措施與上述措施所需成本。

其他國外立法例包括，美國針對金融服務提供者的資訊安全需求，根據「金融服務現代化法案」(Gramm-Leach-Bliley Act)，有制定「客戶資料安全與機密保護標準」。該標準著重於員工管理、資訊系統與系統錯誤管理，所要求建立的安全計畫包括各金融機構需指定專人負責資訊安全、應對於客戶資訊安全進行風險評估、設計、實施與定時監管相對應安全措施、於客觀環境、包括營業內容、改變時應調整安全措施、及與適當服務提供者合作並

發展安全措施。另外美國在「醫療保險可攜性與可責性法」(Health Insurance Portability and Accountability Act）也針對關於醫療資訊隱私的資訊安全保護加以規定。該法關於資訊安全的規範重點在於資料取得之控制、員工的背景調查、資料傳送與儲存過程中的加密、資料處理之政策與步驟、偶發事件反應與災難回復計畫等流程上的管理步驟。[339] 另OECD在「資訊系統及網路安全指導方針」(The 2002 OECD Guidelines on the Security of Information Systems and Networks）(以下簡稱爲安全指導方針)[340]中所指出的，政府應率先建構資訊安全體系，所以政府在資訊安全環境的建構上，有其指標性與重要性。OECD安全指導方針的目標是要求所有與會國共同建立安全文化（culture of security），以確保數位經濟及資訊社會發展過程安全穩定。該方針是以1.認識 (awareness)、2.責任 (responsibility) 、3.反應 (response)、4.道德規範 (ethics) 、5.民主 (democracy)、6.風險評估(risk assessment)、7.安全設計與實施 (security design and implementation)、8.安全管理 (safe management)、9.再評估 (reassessment)九個原則，建立資訊安全管理體系[341]。該指導方針已成爲OECD各會員國建構資訊安全管理系統的重要參考，例如，英國即於1993年根據該原則頒佈「資訊安全管理實務準則」，並於1995年訂定BS 7799part1作爲「資訊安全管理實務準則」之國家標準，作爲資訊安全管理的基礎；BS7799與ISO/IEC 17799牽涉的層面包括：資訊安全政策、組織安全、資產分類、人員安全、實體及環境的安全、通信與操作原則、存取控制、系統開發與維護、業務持續營運及符合法令規範。[342]

---

[339] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 81-82。

[340] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002), *at* http://www.oecd.org/dataoecd/16/22/15582260.pdf. (last visited on 2009.6.30)

[341] See *id.*, at 9-13.

[342] 目前英國的 BS7799 更已被國際標準組織（ISO）採用，於 2000 年時正式公告成爲 ISO/IEC1779。我國經濟部標準檢驗局也採納上述標準之精神，依據 ISO/IEC1779 制定了 CNS 17799 資訊技術-資訊安全管理之作業要點、以及依據 BS7799:PART2:2002 制定了 CNS 17800 資訊技術-資訊安全管理系統規範。制定上述標準的重要性在於，因爲 BS7799 與 ISO/IEC1779 設計的目的在發展可以適用於各種產業與組織的資訊安全管理體系，所以要建立個資法修正草案中所要求的個人資料檔案安全維護計畫，此種包括組織與技術方面要求的資訊安全管理體系，參考 CNS17799/17800 即會是一個適當的選擇。參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 87-88。

在此方面，我國政府是以納入 ISO17799 內涵的「行政院所屬各機關資訊安全管理要點」、依循 BS 7799 爲範本的「行政院所屬機關資訊安全管理規範」以及「行政機關資訊安全管理作業原則」與「行政機關資訊安全管理作業原則」等行政規則建立政府內部資訊安全的基本規範。上述行政規則中，關於個人資料保護部分，於「行政院及所屬各機關資訊安全管理規範」內特別有如下之規定

一、 應依據電腦處理個人資料保護法等相關規定，審慎處理個人資訊；

二、 應建立個人資料控制及管理機制，並視需要指定負責個人資料保護之人員，以便協調管理人員、使用者及系統服務提供者，促使相關人員瞭解各部門應負的個人資料保護責任，以及應遵守之作業程式。[343]

至於在資訊安全管理的整體架構上，我國在政策面是以「建立我國通資訊基礎建設安全機制計畫」[344]作爲政策綱領，並在政府單位中建立「國家資通安全會報」統籌各政府單位管理資訊安全工作。該計畫自 2001 年開始執行以來，已建立第一階段國家資通安全基本防護能力，目前第二階段之目標在建立國家資通安全整體防護體系。在此體系下，我國資訊安全的法制面架構與個人資料保護相關部分可區分爲資訊安全法制與資訊安全標準兩方面，分述如下。[345]

在資訊安全法制上，可分爲犯罪預防與資料隱私保護兩方面加以敘述。在關於犯罪預防的方面，我國於 2003 年 6 月於刑法中，針對干擾電腦運作、電磁紀錄的行爲，增訂「妨害電腦使用罪」章加以處罰。針對資料內容隱私保護，則是於第三百一十五條增列以「開拆以外之方式窺視其內容」的文字，規範以破解密碼方式，窺視他人電子訊息的行爲；並加入第三百一十八條之一和三百一十八之二之條文，規範利用電腦或網路，洩漏他人祕密的行爲。

在關於個人資料隱私保護方面，我國是以電腦處理個人資料保護法作爲

[343] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 82-83。

[344] 全文可參考行政院國家資通安全會報，http://www.nicst.nat.gov.tw。

[345] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 83。

保護個人資料的基礎。現行個資法中關於資訊安全方面，是以要求登記以及建立個人資料檔案安全維護計畫方式爲之。但個資法第二十條第五項也僅規定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，對於個人資料檔案安全維護計畫如何建立仍付之闕如，所以尚須參考個別法令或其他規定。

與上述個人資料檔案安全維護計畫以及標準有關的規定，在通訊傳播業中，包括規範電信業的電信業電腦處理個人資料管理辦法，[346]電信業電腦處理個人資料管理辦法是概括式的就當事人查詢個人資料的程式、個人資料檔案安全維護標準加以規定，並於第十二條中，就個人資料檔案安全維護標準區分爲資料安全、資料稽核、設備管理與其他其他安全維護等事項加以規定，其作法或可提供其他產業之借鏡參考，包括：

一、 資料安全方面：

(一)、 個人資料檔案建置在資料庫者，應釐定使用範圍及使用權限，並設置使用者代碼、識別密碼，識別密碼應保留，不得與他人共用，並應製作使用紀錄。

(二)、 個人資料檔案建置在個人電腦者，應將資料儲存於軟式磁碟片上，並定期拷貝。

(三)、 非經允准不得刺探或使用個人資料檔案。

(四)、 個人資料檔案使用完畢，不得留在電腦終端機上。

二、 資料稽核方面：

(一)、 以電腦處理個人資料時，應核對個人資料之輸入、輸出、編輯或更正是否與原件相符。

(二)、 個人資料提供利用時，應核對與檔案資料是否相符，如有疑義，應調閱原檔案查核。

(三)、 設備管理方面：

[346] 參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 84。

1、 建置個人資料之有關電腦設備，應定期保養。

2、 更新設備時，應注意資料之安全。

(四)、 其他安全維護事項：

1、 以電腦處理個人資料檔案之人員，其職務有異動時， 應將所保管之儲存媒體及有關資料列冊移交。電信業應另行核給密碼，以利管理。

2、 遵守一般電腦安全維護之有關規定。

除了上述標準，個人資料檔案安全維護計畫，尚可以參考我國已建立的其他資訊安全國家標準，例如多數政府機關已通過 ISO27001(ISO 27001 認證是規範、實施、操作、監督、審查與改善資訊安全管理系統)及其 11 個構面進行系統化檢視，以確保機關對重要資訊資產之保護。例如在關於資通安全技術標準，我國除已建立關於資通安全檢測技術、資通安全驗證方法、資通安全認證程式、資通安全管理標準、資訊產品安全標準、資訊產品安全準則等相關標準外，並已修訂資訊技術設備安全通則(CNS 14336)定資訊技術安全評估準則(CNS 15408)、資訊安全管理系統驗證/登陸機構之認證指引(CNS 14731)[347]。根據「行政院資通安全會報」規定，資安等級 B 級以上之政府單位，皆須於 2008 年之前建置完成資安管理系統（Information Security Management Systems，ISMS），並取得第三方認證通過。除了政府帶動外，民間企業也紛紛體認到 ISMS 的重要性，許多大型的電信業、金融業、資訊服務業等，都陸續以通過 ISO27001 爲努力的方向，通過 ISO27001 認證已成爲組織及企業永續經營之必要工作。目前國內已有許多政府部門或是民間企業取得 ISO 27001 的認證，隨之而來的挑戰是「如何讓 IT 能在符合安全系統的要求下提升效率與效能，降低因爲安全控制措施所帶來的不便，並展現資訊部門的價值」。

[347] 上述國家標準可以在國家標準（CNS）檢索系統中查詢，網址爲 http://www.cnsonline.com.tw/index.html。參考：服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心，頁 88。

綜上所述，個人資料保護管理程序的主要範圍及目標包含如下：

(1)建立、實作、維護與改進個人資料保護管理系統；

(2)確認組織的個人資料保護管理系統與本標準一致；

(3)請求外部組織或個人確認個人資料保護管理系統與本標準一致；

(4)請求外部組織驗證/註冊此個人資料保護管理系統。

在此範圍及目標下，區分爲規劃階段、執行階段、檢查階段及改善階段四個循環階段來進行個人資料保護相關作業。

一、規劃階段

公務機關或非公務機關進行規劃時，必須先要瞭解個人資料的定義，以現行個資法中定義的個人資料，指自然人之姓名、出生年月日、身份證統一編號、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。這部分的規範範圍或嫌不足，目前修法中已經再加以擴充。規劃階段應該制訂單位內的個人資料保護政策，確定內部執行個人資料保護的方向及目標，規劃階段的步驟應包括

(1)個人資料之確認;

(2) 法律、指導綱要與其他法令;

(3)風險識別、分析與對策;

(4)資源、角色、責任與權責;

(5)內部規章;

(6)規劃文件;

(7)緊急狀況之準備等。

因此規劃階段確認內部所處理之個人資料後，必須瞭解相關的法律，進行相關的風險識別及分析，而後規劃內部的角色與權責，訂定內部規章，最

重要的是要有緊急狀況處理之準備。

二、執行階段

執行階段爲實際執行的行爲，所以重點在於制訂作業上的運作程序，並且依據此程序執行個人資料保護作業，執行事項主要爲個人資料的蒐集、處理及利用。執行階段的工作項目應包括：

(1)運作程序;

(2)獲取、利用與提供原則;

(3)特定目的之確認;

(4)適當的獲取;

(5)特種個人資料蒐集、處理或利用之限制;

(6)直接向當事人蒐集個人資料之告知措施;

(7)蒐集非由當事人提供個人資料之告知措施;

(8)利用之措施等。

執行階段蒐集、處理及利用時的告知措施非常重要，另外對於特種個人資料的蒐集利用的限制必須確實瞭解，利用個人資料時一定要合乎法律、政策及程序的要求。

三、檢查階段

檢查階段非常重要，也就是運作過程中是否可以符合法律及規劃階段政策的要求，因此各單位必須建立稽核的制度。檢查階段應包括：

(1)準確度之安全;

(2)安全控制措施;

(3)員工的監督;

(4)受託人的監督;

(5)運作確認;

(6)稽核等。

此階段要稽核個人資料在蒐集、處理及利用過程的安全控制措施，並確認運作程序過程中是否有缺失。稽核人員的培養及訓練非常重要，有合格的隱私權顧問師可以確保稽核制度的順利進行及發揮應有的功效。

四、改善階段

改善階段主要針對檢查階段的缺失進行改善作業，單位內應建立、實作與維護程序，以決定責任及權責，確保矯正與預防措施的實作，此程序應包含下列事項：(1)確認不符合的內容；

(2)確定不符合的原因，提出矯正與預防措施；

(3)決定期限，實施所提出的措施；

(4)記錄實作矯正與預防措施的結果；

(5)審查實作矯正與預防措施的有效性;

(6)組織管理階層的審查。

另要防止資料外洩，須從改善資料的可見度和對資料的控制力開始，即使已被改變的資料，也要在外洩前就加以阻止。可以透過以下資料保護技術來實現，諸如：

1. 監控各種通信與傳輸管道：控制使用者透過各種方式，如電子郵件、Webmail、P2P 應用程式、IM、Skype、HTTP、HTTPS、 FTP、Wi-Fi、USB、CD、DVD、印表機、傳真與移除式儲存裝置，在網路上傳送、存取、列印與儲存機密資料。阻止會竊取員工憑證的木馬程式、蠕蟲、檔案分享應用程式，避免機密資料遺失，即使資料已修改、複製、張貼、壓縮或加密，仍可保護所有的資料，且不會中斷正當的日常作業。強制選項應有： (1)監控 – 允許資料傳輸 (2) 防止 – 阻止資料傳輸 (3) 警示 – 通知管理人員與使用者 (4)加密 – 確保資料在加密後才能夠傳輸 (5) 隔離 – 等待驗證。
2. 全面加密防護：自動加密整個裝置（如硬碟），而不需要使用者介入或受過訓練，或是影響系統資源，可有效防止裝置失竊或遺失時，確

保該裝置的機密資料受到加密，不致外流。檔案與資料夾加密，透過自動新增會與被保護的檔案一起傳輸的檔案標題，確保檔案不使用時仍能永遠保持加密，無論檔案與資料夾儲存於何處，是在本機硬碟、檔案伺服器、移除式裝置，甚至是電子郵件附件中，檔案與資料夾都能受到嚴密的加密保護，未經授權的人無法存取該檔案。

3．企業級管理及稽核回報

使用強大的中央管理平台，能根據詳細的內容來指定對未經授權存取機密資料的篩選、監控和封鎖行爲：(1)管理全磁碟、檔案和資料夾加密功能，控制政策和管理修補程式，復原遺失的金鑰，呈現有無遵循政策。(2) 使用 Active Directory、Novell NDS、PKI 等來同步安全政策。(3) 透過廣大的稽核功能來確認裝置已加密。(4) 記錄資料交易，記錄如寄件者、收件者、時間戳記、資料證明、上次成功登入日期與時間、上次收到更新的日期與時間，以及加密是否成功等資訊。

小結

我國目前在個別保護法制上面，雖已具相當之發展，然「國家資通安全會報」本身之法源依據卻付之闕如，建議在整體法制規劃上，應考慮對國家資訊安全建立一部法律，做爲基礎。

資訊安全的議題，並不是「技術」，而是一種「管理」，不論資訊安全的軟硬體如何周全，因爲參雜了「人」這個最不確定[348]，但也最重要的因素，顯然完善的管理制度，才能降低資訊安全風險。目前依我國「國家資通安

[348]警政署從近來收集到的資料發現，中國網軍開始透過搜尋引擎找尋政府高層的私人 E-mail，並以攻擊這些私人信箱爲主。警政署資訊室主任李相臣指出，私人信箱的防護較差，而政府高層仍有人習慣透過私人信箱處理公務，導致私人信箱一旦被入侵，機密資料也隨之外洩。臺灣因爲經常遭到中國網軍的針對式攻擊（Target Attack），許多政府高層的公務帳號經常會收到惡意郵件的攻擊。李相臣表示，隨著政府近年來提高對公務電子郵件的防護，中國網軍也改弦易轍，將攻擊對象轉向政府高層防護較弱的私人信箱。警政署巡官叢培侃表示，從今年 3 月～8 月，中國網軍將臺灣某受害主機當作跳板，發動一波惡意郵件的攻擊。他透過搜尋引擎隨機查詢這些寄送清單後發現，許多都是在機敏單位工作或政府高層的私人信箱。他更進一步發現，某個研究單位的通訊錄可以透過搜尋引擎找到，其中包含許多機敏機關和政府高層的私人聯絡 E-mail。他清查這份通訊錄發現，有 40%曾遭到惡意郵件攻擊，其中更有近半數收到超過 10 封以上的惡意郵件。參見 2008-11-18, iTHome Online: 中國網軍盯上政府高層私人 E-Mail。http://www.ithome.com.tw/itadm/article.php?c=51942

全會報通報與應變作業流程」[349]規定分成各級政府機關(構)責任區、主管機關責任區、國家資通安全會報(通報應變組)責任區及協助支援單位責任區四大區塊[350]。前述之通報機制，僅適用於行政院所屬機關，經機關發覺、查知有資訊安全事項後，依循體制通報、處理。但資訊安全事件如爲跨國、或涉及私人公司或個人，並無主管或應負責通報之行政機關，此時即由 FIRST 組織[351]內各會員，依循相互通報機制，向各國境內之協調中心（ Coordination Center ）發出通報。目前我國接受通報之機關爲官方成立之 TWNCERT[352]。

由上述我國通報機制及作業流程可以看出，在私領域的反應協調方面，欠缺有效的聯繫機制，如能從上位的法律建構建立公領域與私領域聯繫的法源基礎，並輔以本研究所建議之標章制度推動，當更有效維護資訊安全。另外資安專業人員的不足，卻也爲政府機關維護資訊安全的隱憂之一。因爲網路無國界，現今的資訊駭客等已非區域性的攻擊;另外政府資訊安全設備之建置及考量常委外作業(就學資訊之考生資料外洩即爲一例)，亦可能造成資訊安全及隱私的漏洞，不可不慎。本研究之所以鎖定公務機關之教育單位以及常遭資安隱私外洩的非公務機關的電信、金融及購物，乃依據法務部調查局於 2007 年的網路趨勢報告顯示：2006 與 2007 年的網路威脅趨勢顯示，從 1999

[349] 參 http://www.junglicity.gov.tw/.../國家資通安全會報通報與應變作業流程.ppt

[350]註：

1. 各級政府機關（構）及主管機關以現行政府組織體系運作。

2. 各單位發生資安事件時，須於廿四小時內通報國家資通安全會報及循內部程序上報行政體系督導長官。

3.主管機關業管資通安全業務首長責任：

（1）掌握資安事件狀況。

（2）及時督導資安事件之處理。

（3）提出檢討，並視情況向高層長官、民意機　關報告或向媒體、社會大眾說明。

4. A、B 級事件須由部會副首長協助督導。

[351] FIRST（Forum of Incident Response and Security Teams）譯爲「電腦及資訊安全緊急應變小組論壇」，或有稱之爲「電腦安全事件應變小組論壇」、「資安事件應變小組論壇」，於 1990 年成立，是全球最早成立、在電腦安全事件的應變上被認定具有領導地位的國際性資訊安全非官方組織 。

[352] TWNCERT（Taiwan National Computer Emergency Response Team）財團法人資訊工業策進會於 2003 年成立，其人員則由國家資通安全會報技術服務中心（技服中心）人員兼任，已加入 FIRST。

年 11 月開始，藉由台灣 Domain Name 而發生的駭客攻擊，多達 12,324 次，其中包含企業網站（com.tw）6,513 次、學校網站（edu.tw）3,013 次，以及政府網站 （gov.tw）705 次。一般而言，雖然教育單位網站被駭客入侵所產生的金錢損失較不顯著，但駭客可透過學校網站作爲跳板，再行連結至企業及政府相關網站後端，盜取資料，其嚴重性不容忽視[353]。

第二節　個資法中公務機關監督機制之加強

基於國家機器之巨大及資源之豐富，如未對於公務機關取得個人資料、其後對於該資料之利用、保存，以及公務機關間對於取得之個人資訊能否交換流通等事項加以限制規範，則個人隱私將可能面臨極大侵害風險，個人形象可以透過鉅細靡遺的政府資料庫重新形塑，亦可能發生違反當初蒐集目的之個人資料使用。參酌國外立法例，即便有法律明文規定、執行法定職務所必要、當事人已公開或其他以合法公開資料，以及出於研究目的且已處理無從辨識當事人等例外情況，仍應取得當事人之同意，使得爲資料之蒐集、處理及利用；否則僅因法律規定、法定職務或有研究需要，即不需取得當事人同意，無異將當事人之資訊自決權架空，保障資訊自決權即形同具文。依個資法草案第 15 條規定，公務機關只要符合「執行法定職務必要範圍內」、「經當事人書面同意」、「對當事人權益無侵害」三種情形之一種，即可進行個資的蒐集或處理，同樣地，依草案第 16 條規定，公務機關只要符合「法律明文規定」、「爲維護國家安全或增進公共利益」、「爲免除當事人之生命、身體、自由或財產上之危險」、「爲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爲統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從辨識特定當事人」、「有利於當事人權益」或「經當事人書面同意」等七種情形之一種，即可在原始蒐集之特定目的外利用已蒐集之個人資料。此等設計過於寬鬆，民眾之個資保障可能不足。

草案中亦允許以其他限制性允許條件替代當事人同意的制度設計，不但

353 從數字看資安：2007 年 3 月全球網路整備度，台灣退居第 13，http://www.i-security.tw/learn/sub_200703_TippingPoint.asp

嚴重壓縮當事人同意的作用空間，也顯違背當事人的資訊自決權，因此若欲真正保障資訊自決權則必須將當事人同意置於所有限制性允許之上，將之視爲所有資訊作爲的必要前提條件。然，當事人同意並非在所有情形皆實際可行。當同意事實上不可行（impractable）時，原則上雖即不應允許個資之蒐集處理與利用，但例外在所涉及（資訊自決以外）權益之侵害極微小且告知或同意將妨礙重大利益時，應考量利益衡平而設定免除同意之正當理由[354]。

綜上所述，論者[355]有建議修正條文如下：

第十五條（公務機關資料蒐集處理之原則）

公務機關對個人資料之蒐集或處理，應有法定執掌所授權之特定目的，並經當事人書面同意，於必要範圍內爲之。

公務機關對敏感性個人資料之蒐集或處理，除應符合前項之規定外，非有下列情形之一，非經公務機關內資訊保護官(類似機制）之審查，不得爲之：

一、爲免除當事人之生命、身體、自由或財產上之危險所必要。

二、爲進行與當事人有關之訴訟或其他民事、刑事或行政紛爭解決程序所必要。

三、爲公共衛生、犯罪預防或科學知識之目的，進行調查、統計或學術研究而有必要。

四、法律明文規定。

有下列情形之一者，得經公務機關內資訊保護官(類似機制）之審查，免除前二項之書面同意：

[354] 法務部針對本研究報告之意見及建議回應認爲，查個資法第 1 條明文規定，個資法之立法目的除避免人格權受侵害外，「並」有促進個人資料之「合理」利用之功能，當私益與公益有所衝突時，於合乎憲法比例原則之考量下，立法者認爲不必獲得當事人書面同意，即可於法律明文規定或公務機關基於執行法定職務之必要，蒐集或利用當事人之個人資料，此係爲平衡「私益」與「公益」而設，如所有例外情況均須得當事人同意，可能影響公共任務或公權力之行有害於公益。

[355] 邱文聰，從資訊自決與資訊隱私的概念區分—評「電腦處理個人資料法修正草案」的結構性問題，月旦法學雜誌 168 期，2009.05.

一、依法律規定得不經當事人同意者。

二、當事人自行公開或其他已合法公開之個人資料。

三、爲免除當事人或他人生命、身體、自由或財產上之危難所必要。但涉及敏感性個人資料時，尚須當事人事實上或法律上無行爲能力，或情況緊急不及取得當事人書面同意者。

四、個人資料之蒐集、處理或利用對當事人權益僅造成極微小之影響，而取得當事人同意程序將嚴重妨礙合法目的之達成，且以依其他適當方式保護當事人權益者。

第十六條(公務機關資料供特定目的外利用)

公務機關對個人資料之利用，應於執行法定職務必要範圍內爲之，並與蒐集之特定目的相符。但有下列情形之一者，公務機關得經機關內資訊保護官(類似機制）之審查，將合法蒐集之個人資料爲特定目的外之利用：

一、經當事人書面再同意，且用於公務時，其利用目的不違背利用機關之法定執掌者。

二、公務機關爲維護國家安全所必要，且取得當事人再同意程序將嚴重妨礙此目的之達成者。

三、爲免除當事人或他人之生命、身體、自由或財產上之危難所必要。但涉及敏感性個人資料之特定目的外利用時，尚須當事人事實上或法律上無行爲能力，或情況緊急不及取得當事人書面再同意者。

四、特定目的外利用對當事人權益僅造成極微小之影響，且以依其他適當方式保護當事人權益者。

五、依個人資料提供利用之方式已經永久去連結而無從識別特定當事人，且當事人對特定外利用未爲反對之表示者。

六、明顯有利於當事人權益。

七、法律明文規定。

公務機關將合法蒐集之敏感性個人資料供爲特定目的外之利用時，公務利用目的並應符合第十五條第二項之規定，非公務利用目的並應符合第十九條第二項之規定。

第十九條 （非公務機關資料蒐集處理之原則）

非公務機關對個人資料之蒐集或處理，除當事人自行公開或其他已合法公開之個人資料外，應有下列特定目的之一，並經當事人書面同意，於必要範圍內爲之：

一、 履行與當事人間契約或類似契約關係之義務。

二、 履行法定義務。

三、 爲科學知識之目的，進行調查、統計或學術研究。

四、 爲新聞報導之目的。

五、 其他法定或經當事人同意之目的。

非公務機關對敏感性個人資料之蒐集或處理，非有下列情形之一，並經當事人書面同意，不得爲之：

一、 法律明文規定。

二、 履行法定義務所必要。

三、 爲免除當事人或他人生命、身體、自由或財產上之危難所必要。

四、 學術研究機構爲科學知識之目的，進行調查、統計或學術研究而有必要。

五、 爲正當報導與公益有關事務所必要。

六、 爲進行與當事人有關之訴訟或其他民事、刑事或行政紛爭解決程序所必要。

七、 爲當事人之醫療診治或疾病預防目的，而由專業醫事人員所進

行之必要行爲。

有下列情形之一者，得免除前二項之書面同意：

一、 依法律規定得不經當事人同意者。

二、 當事人自行公開或其他已合法公開之個人資料。

三、 爲免除當事人或他人生命、身體、自由或財產上之危難所必要。但涉及敏感性個人資料時，尚須當事人事實上或法律上無行爲能力，或情況緊急不及取得當事人書面同意者。

四、 個人資料之蒐集、處理或利用對當事人權益僅造成極微小之影響，而取得當事人同意程序將嚴重妨礙合法目的之達成，且已依其他適當方式保護當事人權益者。

第二項之蒐集或處理及前項同意之免除，於依法應設置資訊保護官(類似機制）之非公務機關，應經資訊保護官(類似機制）之事前審查。

第二十條（非公務機關資料供特定目的外利用)

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爲之。但有下列情形之一者，非公務機關得將合法蒐集之個人資料供爲特定目的外之利用：

一、 經當事人同意再同意，且用於公務時，其利用目的不違背利用機關之法定執掌者。

二、 爲免除當事人或他人生命、身體、自由或財產上之危難所必要。但涉及敏感性個人資料時，尚須當事人事實上或法律上無行爲能力，或情況緊急不及取得當事人書面再同意者。

三、 特定目的外利用對當事人權益僅造成極微小之影響，且已依其他適當方式保護當事人權益者。

四、 依個人資料提供利用之方式已經永久去連結而無從識別特定當

事人，且當事人對特定目的外利用未為反對之表示者。

五、 明顯有利於當事人權益者。

六、 法律明文規定。

前項特定目的外之利用，於依法應設置資訊保護官(類似機制）之非公務機關，應經資訊保護官(類似機制）之事前審查。

非公務機關將合法蒐集之敏感性個人資料供為特定目的外之利用時，公務利用目的並應符合第十五條二像之規定，非公務利用目的並應符合第十九條第二項及第四項之規定。

非公務機關依第一項規定利用個人資料行銷時，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。非公務機關應於首次行銷時，免費提供當事人表示拒絕之方式。

針對上述建議中有關「資訊保護官(類似機制）」之設置一節，實涉及政府單位中的組織人力配置，雖於目前階段有所困難，但於未來政府進行組織改造時，或可從行政院整體角度考量，於組織上適當配置資訊長(或法務長、主計長)之職務[356]。另公務機關該等工作執掌範圍，必須特別注意各公部門間，有關「資料拼圖[357]」的隱私疑慮防堵，即藉由各機關間相互個人資料之利

[356]關於建議參考歐盟資訊保護官(類似機制）的設立，涉及政府改造。原先法務部希望設立一獨立機關。上一波政府改造原先在行政院下設四個長官（法務長、主計長、人事長、資訊長），其中資訊長的角色或當時設定的定位較類似本研究所稱之資訊保護官(類似機制），因此在組織的變革上可採取這樣的建議。參考期末座談會，陳美伶委員發言記錄。

[357] 自 2007 年中起，國內發生多起購物網站會員資料外洩並遭詐騙集團利用的事件，從經營雅虎奇摩購物中心的興奇科技、東森購物、Payeasy，以及金石堂、博客來與誠品網路書店等知名業者，皆傳出類似事件。但警方調查除東森購物有相關企業主管涉嫌盜賣個人資料外，其他業者都未查出內部資料外洩異常。警方認為，在個人一般資料氾濫的情況下，透過比對使用者個人資料，並藉以猜測帳號密碼的「資料拼圖」手法，恐怕已成為詐騙集團的最愛。所謂資料拼圖，刑事局偵九隊表示，即是將不同來源取得的個人資料比對後，拼湊出完整的資料，再利用一般民眾喜歡用生日、電話號碼等特殊數字作為密碼的習慣，直接上網「測試」各種可能的帳號密碼組合。一旦成功，即可以合法的身份登入使用者帳號，直接觀看使用者的個人資料與各種記錄，讓資料更完整。駭客在網路上利用資料拼圖手法最知名的案例，要算是 2007 年底發生的 Payeasy 事件。2007 年 12 月 9 日晚間，Payeasy 突然有來自中國大陸 IP 的大量異常登入，在被登入的 3,9000 多個會員帳號中，有 14%遭測試成功，27%則是帳號正確、密碼錯誤。Payeasy 發現異常後，便緊急封鎖特定 IP，並通知會員更改密碼，事後雖未傳出用戶遭詐騙成功的案例，但確有用戶在事後接到詐騙電話。參見 ZDNet Taiwan,「資料拼圖」成帳號竊取主要手法，2008.02.05, http://www.zdnet.com.tw/news/

用就可以較完整拼湊出個人基本資料的細節(包括稅務財產總歸戶、交通監理等)。另外在公務機關有關就學資料保護方面，教育主管單位宜加強學校內資安專責人員配置及資安預算之編列，目前各級學校的資安防護是政府部門間較爲迫切需要注意的[358]。

另對於公務機關之監督機制，草案中則未有規定，僅提示個資當事人得提起行政訴訟、請求國家賠償；惟個人資訊權受到侵害之態樣之形式特殊，受侵害之當事人的個人資訊常係在不自覺的情況下被違法蒐集、處理、利用，從而當事人對於侵害之發生更係難以察覺；此際，國家對於公權力侵害個人資訊權非不僅自我節制，自我監督檢查之機制亦爲闕如，反要求人民以自力救濟之方式對抗國家無形之侵害，實屬立法缺漏，宜改進之。在前述討論中，建議增設「資訊保護官(類似機制)」設計，即用以進一步進行監督審查，防堵「非執掌範圍」內之個資外洩。資訊保護官(類似機制）之執掌，除進行機關內相關資安教育宣導之規劃外，另對於各機關間有關個人資料之相互蒐集、處理及利用，應嚴加審核把關，以維個人隱私之尊重。在個案審查標準上，可以本研究有關歐盟對於電信資料互通的八大基準做爲參考，即「目的特定」、「接觸限制」、「資料最低調閱」、「資料探勘禁止」、「有權接觸機關之司法或獨立檢驗」、「業者保留資料之目的」、「系統分離」、「安全維護」。另外，資訊保護官(類似機制）對外方面，必須依照內部之偵測及回應，對外與各單位依通報機制建立回應管道，未來結合隱私標章制度時，更應主動檢視標章使用的各項細節規定，以免標章失其效力。

再者，有關德國對於公務機關的隱私標章認證審核制度介紹一節，我國可參考推動之，對公務機關個人資料保護之工作進行審核及認證，藉此提供民眾對於隱私權之信賴基礎、刺激與隱私相關之科技技術與服務發展，以落實個人資料保護之工作。也唯有公務機關對隱私保護的審核項目及程序建立法規化的基礎後，始可續就非公務機關就相關制度推廣之。除積極規劃各公

software/0,2000085678,20127775,00.htm

[358]教育單位常因學校規模及經費來源不足之情況，並未能如中央及地方其他機關一般得以建置資安設備或有資安專業人員之配置，然各級政府應加強教育網路之控管，避免學校機關(構)成爲跳板攻擊之跳板，間接造成其他公務機關與企業網站之損失。

務機關必須就資安預算爲詳實編列以因應未來認證審核機制外，在審核項目及程序方面，應特別重視隱私標章的有效期限之審核檢視與建立申訴管道，避免類似我國電子簽章法立法時之疏漏[359]。

第三節　個資法中非公務機關之部分宜盡量透過市場機制及自律輔導解決

產業自律規範的形態包括下列四種類型：

一、 自行規範(self-regulation)：產業自訂行爲規範準則，而政府僅提供相關意見。

二、 擬制規範(quasi-regulation)：在政府指導或影響下產業自訂行爲規範準則，或機關作成之行政指導(如規範說明、警示意見等)。

三、 共同規範(co-regulation)：政府法定規範作爲產業自訂規範的補充規定。若產業未訂，依政府規定。產業自訂規範爲要件規定，政府法定規範作爲效果規定。例如空氣污染防制法第 32 條規定，公私場所之固定污染源因突發事故，大量排放空氣污染物時，負責人應立即採取緊急應變措施，並於一小時內通知當地主管機關。前項情形，主管機關除命其採取必要措施外，並得命其停止該固定污染源之操作。違反 32 條第 2 項者，依同法第 49 條規定，可「處一年以下有期徒刑、拘役或科或併科新臺幣二十萬元以上一百萬元以下罰金。其中之「緊急應變措施」即爲自行規範，主管機關命採取之必要措施則爲補充規定。

四、 違反自律之法定規範(explicit government regulation)：政府擬於法律規範中明訂產業行爲準則及效果。例如，依律師法第

[359] 電子簽章法在制訂過程中有關政府公告排除事項一節，由於未如美國立法訂定「定期檢視期」，造成政府機關一旦公告排除特定事項可以適用電子簽章法後，將無法與時俱進地檢視更新，造成電子簽章法被排除適用的情況反較可以適用的情況爲多。

39 條第 3 款之規定，律師有違背律師倫理規範或律師公會章程之行為，情節重大者，應付懲戒。其中是否屬違背律師倫理規範或律師公會章程之情節重大行為？由律師公會團體自行規範＆，如認確屬違反，則可移送懲戒。刑法 193 條規定，承攬工程人或監工人於營造或拆卸建築物時，違背建築術成規，致生公共危險者，處三年以下有期徒刑、拘役或三千元以下罰金。其中「違背建築術成規」為要件規定，包括建築業之規範。

以目前政府部門積極推動的 ISO27001 驗證為例，可謂擬制規範或是共同規範，而德國、日本推行的隱私標章制度，亦可謂綜合擬制規範及共同規範，在日本企業推行的標章制度，由於有管制監理的成分在內，亦屬於一種具違反自律的法定規範意涵。

一、政府宜透過補助或輔導方式協助中小企業建制資訊安全防護體系

資安設備與服務對於一般中小型網站，屬昂貴投資，一般中小型網站，在網站尚可營運之狀況下，並不會特別編列針對保護會員隱私之高階設備。倘若政府可以透過輔導計畫，以有效輔導模式，採政策補助加廠商自籌款比例方式，補助網站資安升級，且透過輔導案，更能有效掌握及追蹤補助成效。

二、持續鼓勵並輔導推廣自然人憑證及工商憑證之利用；並應帶頭倡導帳號密碼安全觀念，甚至全面間接密碼化，透過 token 或簡訊密碼鎖等等形式，取代一般的帳號密碼形式。

我國政府對於公開金鑰基礎建設（Public Key Infrastructure, PKI）之建置已施行多年，並在公部門與私部門聯繫間分別成立自然人憑證及工商憑證兩項重要基礎網路建設，該等建置在資訊安全的防護上已有一套機制及成效，本研究之建議應加強該兩套憑證機制之運用面，並以此做為主要身份認證機制。至於其他非公務機關相關之運用，則可考慮運用間接密碼化，透過 token 或簡訊密碼鎖等形式，取代一般的帳號密碼形式。而對既有之工商憑證及自然人憑證之資安防護，除技術面外，應加強前述之人員管控與稽核，全面降低因人為因素造成資安外洩之缺失可能性，此部分除可利用資安法制建立加強外，電子簽章法及未來公行為(公務機關)之數位簽章立法均可透

過相關主管機關的施行細則或管理辦法中加強之。

三、政府應輔導資安認證機制或仿德、日本隱私認證標章方式，獎勵創新注重個人隱私之資訊流、金流、物流流程

認證標章機制之推動必須透過政府之積極輔導始能產生一定之效用，本研究建議宜仿德國、日本近來推行之隱私認證與 P-Mark 制度，由政府對於個別產業施以標章制度之輔導，結合上述之技術、人員與管理層面之檢視，強化個人隱私保障的資訊流、金流及物流鏈結之整合，並視產業發展需求，積極建立區域性及國際性之交流、推動與合作．另針對已經隱私標章認證之企業，亦可考慮在個資洩漏的不幸事件中，適度調整舉證責任之認定及法院對於企業責任認定之裁量。

第四節　整體建議部分

綜上所述，可知我國政府機關針對強化個人資料保護雖已卓具成效，但部分法制及行政配套措施及執行面仍未臻完備，本研究提供如下建議，謹供未來相關施政之參考。

一、立法部分

(一)短程建議

1、 對於個資法修正之進一步建議

個資法修正草案歷經多個會期未能順利通過三讀，雖對於個人資料保護面向有所遺憾，但反由補強充實面觀之，卻是對於法律完備度的潛在契機。建議新法案送交立院審議時能就本研究提出之問題，進一步釐清增訂：

(1) 特殊敏感性個人資料的定義範圍(草案第 6 條)之再釐清。條文中之醫療、基因及健康檢查三者間之關係，建議於立法說明中，詳析其區別實益，以杜未來適用疑慮。

(2) 草案第 15 條有關公務機關得依特定目的，爲個人資料之蒐集與

處理一節，明訂三種例外情況。建議應尊重當事人之資訊自決權，對於「於執行法定職務之必要範圍內」及「對當事人權益無侵害時」的兩種情況，仍應考慮須經當事人書面同意之告知，而不可直接對個人資料予以蒐集或處理。

(3) 草案第 16 條有關公務機關得爲特定目的外之個人資料之利用的七種例外情況，有待進一步檢視其是否過於寬鬆，並設計監督機制或參歐盟八大準則，以避免對個人資料利用之浮濫。

(4) 對於草案第 19 條及第 20 條有關非公務機關對於個人資料之蒐集、處理及利用之例外規定，亦建議一併予以配合調整檢視。

（主辦單位：法務部; 協辦單位：行政院衛生署）

(二）中、長程建議

1. 對於資訊安全法制位階調整化之建議宜將其法源提升至法律的法位階層次。如本章第一節所述，我國目前有關資訊安全之法制，多均以行政規則定之。建議(資通安全會報)宜將其法源提升至法律的法位階層次，並建議參考 OECD 指導原則等外國立法例，以提高資訊安全的重視程度。而一旦有了法律位階的設計後，未來該法律之主管機關爲何(國家通訊傳播委員會？)，亦須審慎評估。或待隱私認證標章制度建立後，一併配合考量制訂「資訊安全基本法」，以同時管理公務機關以及協調回應非公務機關有關資安事件之處理。

（主辦單位：行政院資通安全會報　協辦單位：國家通訊傳播委員會）

2. 對於個別產業管理相關法制建議

個資法草案已將非公務機關的適用行業(「八大行業」)別予以打破，進而全面適用於所有行業，但爲因應現行個資法之規定，原「八大行業」多有細部規定有關個人資料保護之處理原則(如電信業電腦處理個人資料管理辦法)，未來個資法全面適用各非公務機關之行業時，現行相關處理原則及管理辦法勢必要重行檢視及調整，另針對特殊產業，是否仍有必要(如就醫資訊相關產業)，另行訂定新的處

理原則，亦爲個資法通過施行時之一大考驗，建議主管機關(法務部)即早透過公聽方式，獲致共識，以爲因應。

（主辦單位：法務部; 協辦單位：行政院衛生署、國家通訊傳播委員會、行政院金融監督管理委員會、教育部）

3. 電子簽章法之配合檢視

本研究建議未來爲有效管控個人資料之保護、杜絕不當個資外洩，宜採用憑證安全機制。然現行自然人憑證之推廣應用面如將擴及其他應用，勢必牽涉原自然人憑證之憑證作業基準或憑證互通應用，建議於電子簽章法修法(經濟部商業司)時，與自然人憑證之主管機關內政部共同因應配套評估考量。

（主辦單位：經濟部商業司、內政部; 協辦單位：經濟部工業局）

二、行政部分

(一)短程建議

1. 輔導獎勵之建議

本研究中引用德國及日本有關隱私標章認證制度之推行，建議相關單位(研考會、經濟部、內政部、財政部、金管會、法務部等)，審慎評估。在非公務機關標章制度推廣方面，經濟部或可藉由商業登記之便進行，在公務機關部分，內政部主管業務(如戶政、警政等資料)繁雜，事涉個人資料保護強化者較多，另有關金融隱私部分亦建議金管會研議，故建議由個資法中央主管機關之法務部會同上述部會共同研商規劃。

（主辦單位：法務部 協辦單位：行政院研究發展考核委員會、經濟部、內政部、行政院金融監督管理委員會）

2. 監督機制之建議

無論前述之隱私標章認證制度是否在我國順利推展，個資法草案通過，全面適用於所有行業後，對於較易造成個資外洩之電信業或無

店面零售業、金融業等，相關主管機關均有必要對於其管理及監督機制及法規進行調整。對於違反隱私保障之所轄公務及非公務機關，應嚴加管理並就其違反處以罰則。
(主辦單位：經濟部、國家通訊傳播委員會、行政院金融監督管理委員會; 協辦單位：行政院消費者保護委員會）

（二）中、長程建議

1. 組織建置之建議

本章第二節有關公務機關部分建議時，所提出之「資訊保護官(類似機制)」設置，建議由行政院做整體及各級機關組織調整時之參考。以目前就學資訊個人資料外洩事件頻繁爲例，或全非資訊安全設備建置之問題，反多爲人爲因素所致。而此問題之發生，在於整個資訊安全「規劃、執行、檢查、改善」流程中，對於「檢查」及「改善」階段中，欠缺有效監督機制所致。以各級學校或相關學術單位爲例，主管機關(教育部)確依規劃階段要求所屬各級學校完成一定資安標準認證，然實際操作時由於人員配置及經費受限，導致監督檢查機制之可能疏漏，造成學校內徒有認證之名，而無資安保護之實，並可能淪爲駭客入侵跳板攻擊之跳板。故，本研究建議，除依現行規定要求各級機關行政副首長爲資安負責人外，更應積極從中央及地方各級機關規劃類似「資訊保護官(類似機制)」之相關人員妥適配置及預算經費籌撥，以收監督實效。

（主辦單位：行政院人事行政局; 協辦單位：行政院研究發展考核委員會、教育部、交通部、行政院行政院金融監督管理委員會、行政院衛生署）

2. 預算補助之建議

承上所述，監督檢查人力之編制，涉及人事預算之編列。另對於非公務機關之中小企業，是否考慮資安強化建置之補助(行政院經建會)，有待進一步檢討規劃。所謂「徒法不足以自行」，個人資料之保護雖有相關法律做爲後盾，然在數位匯流的時代中，降低個人資

料外洩，仍有賴設備及技術面之偵測、預警及防堵。另在各級機關設備經費預算編列上，有否考量設計一定比例之資安預算，以維設備採購及維護之基本預算。

（主辦單位：行政院經濟建設委員會；協辦單位：經濟部、教育部、行政院衛生署）

附件一　參考文獻

一、書籍

中文書籍

1、 林子儀，基因資訊與基因隱私權－從保障隱私權的觀點論基因資訊的利用與法的規制，收錄於當代公法新論（中）翁岳生教授七秩誕辰祝壽論文集，2002 年。

2、 法治斌，政府行政作爲與隱私權之探討，行政院研究發展考核委員會委託研究計畫，2000 年。

3、 林子儀， 93 年。

4、 許宗力，民主法治國家的情報活動－重建情報法治的若干建議，收錄於法「資訊取得法」立法政策與法制之研究，收錄於權力分立與憲政發展，19 與國家權力，1996 年。

5、 王澤鑑，侵權行爲法（1）2002 年版。

6、 法治斌，董保城，憲法新論，2004 年 10 月，台北：元照。

7、 李震山，基因科技發展與基本權利保障，收錄於多元、寬容與人權保障——以憲法未列舉權之保障爲重心，2005 年

8、 吳庚，行政法之理論與實用，2005 年 10 月。

9、 余啓民，經建會法協中心委託研究案，電子金融服務與付款機制電子化管理規範研究。

10、 服務業科技應用之個人隱私權保護相關法制之研究—以通訊傳播爲中心

英文書籍

1、 J. THOMAS MCCARTHY, T*he Rights of Publicity and Privacy 1*（1st ed. 1987）

2、 THOMAS M. COOLEY, *The Law of Torts 29* （1888）.

3、 SAMUEL D. WARREN & LOUIS D. BRANDEIS, *The Right to Privacy*, 4 HARV. L. REV. 193 （1890）.

4、 WILLIAM L. PROSSER, *Privacy*, 48 CAL. L. REV. 3 （1960）.

5、 JEFFREY ROTHFEDER, Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret（1992）.

日文書籍

1、 邊 善彥、五十嵐 敦編，個人情報管理ハンドブック，商事法務出版，第 2 版第 1 刷，頁 5，2008 年 4 月。

2、 (財団法人日本情報処理開発協会プライバシーマーク推進センター)編，個人資料保護管理體系實施指針(個人情報保護マネジメントシステム実施のためのガイドライン)，日本規格協會發行，第 1 版第 5 刷，頁 8，2008 年 4 月。

3、 岡村 久道，情報セキュリティの法律，商事法務，初版 1 刷，頁 254，2007 年 7 月。

二、期刊論文

中文期刊

1、 劉靜怡，網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河，資訊管理研究，第四卷，頁 144-145，2002 年。

2、 周慧蓮，英國個人資料保護最新案例發展及其對我國法制之啓示，資策會科技法律中心科技法律透析，民國 94 年 1 月。

3、 周慧蓮，資訊隱私保護爭議之國際化，月旦法學雜誌第 99 期，民國 93 年 1 月。

4、 台灣新竹地方法院不起訴書，科技法律透析，民國 88 年 7 月。

5、 李震山，電腦處理個人資料法之回顧與前瞻，中正法學集刊第 14 期，頁

6。

6、 蔡明誠等著，基因檢測受試者同意書相關研究與討論，生物科技與法律研究通訊第 17/18 期，2003 年，頁 34。

7、 李崇僖，基因資訊隱私保護法理與規範，台灣本土法學雜誌第 91 期，2007 年，頁 75。

8、 張冠群，二ＯＯ九年一月金融控股公司法關於共同行銷及關係人交易與風險集中揭露之修正條文評析，月旦法學雜誌 (No. 168) 2009.5 頁 200。

9、 [1]林育廷，「淺談我國網路金融法治相關問題之研究」，科技法律透析，2001 年 2 月，頁 56。

10、 張冠群，二ＯＯ九年一月金融控股公司法關於共同行銷及關係人交易與風險集中揭露之修正條文評析，月旦法學雜誌 (No. 168) 2009.5 頁 204-205。

11、 宏裕，位置定位服務深入探討（上），網路通訊，116 期，頁 114，2001 年 3 月。

12、 宏裕，位置定位服務深入探討（中），網路通訊，117 期，頁 110，2001 年 4 月。

13、 宏裕，同前，頁 117-8。

14、 葉亭巖，德國個人資料保護標誌及個人資料保護審核制度簡介－以 Shleswig-Holstein 州爲例，載於科技法律透析，2009 年 3 月，第 20～26 頁。

日文期刊

1、 参堀部 政男，個人情報保護に関する国際動向と日本の対応，法とコンピュータ，第 26 期，頁 5，2008 年 7 月。

2、 顧客情報の取扱いに関する諸問題―個人情報保護法案を踏まえて―，金融法務事情 No.1642，2002.5.5。

學位論文

1、詹文凱，《隱私權之研究》，台灣大學法律學研究所博士論文，1998 年 6 月。

2、林建中，《隱私權概念之再思考— 關於概念範圍、定義及權利形成方法》，台灣大學法律學研究所碩士論文，1999 年 1 月。

3、藍培青，《隱私權在美國演進歷程之研究》，淡江大學美國研究所博士論文，1997 年 5 月。

4、莊郁沁，論醫療隱私權之保障，國立台灣大學國家發展研究所碩士論文，2002 年。

5、吳昊，由醫療資訊隱私權之觀點論全民健保 IC 卡政策，國立台灣大學法律學研究所碩士論文，2001 年。

6、邱文聰，由醫療資訊談國家醫療權力的管制，國立台灣大學法律學系研究所碩士論文，1998 年。

7、楊宗杰，醫療資訊隱私權侵害之研究－以健保 IC 卡政策爲例，南華大學公共行政政策研究所碩士論文，2006 年。

8、陳彥碩，論商業應用下基因檢測所涉法律議題，國立清華大學科技法律研究所碩士論文，2007 年。

9、熊愛卿，網際網路個人資料保護之研究，國立台灣大學法律學研究所碩士論文，2000 年。

10、 曾令嫻，論電子病歷流通與個人資料保護之研究-以告知後同意爲中心，國立中正大學法律學研究所碩士論文，2006 年，頁 185。

11、 賴靜儀，從資訊自決權論學生資料保護，94 年國立臺灣師範大學公民教育與活動領導學系碩士論文，頁 128-138。

12、 施峰達，「我國『金融檢查』與『財務隱私權』法制關連性之探討-以銀行業之監理爲中心」，中原大學財經法律學系碩士論文，91 年 1 月，

頁 81~84。

三、網站

1、 The 2007 International Privacy Ranking
http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597

2、 莊庭瑞，從健保 IC 卡談個人資料保護，自由時報 91.08.06 自由廣場，
http://www.tahr.org.tw/site/PDPA/Juang.htm

3、 健保 IC 卡可設密碼保護就診隱私，
http://discuz.club1069.com/redirect.php?tid=187148&goto=lastpost

4、 人類免疫缺乏病毒傳染防治及感染者權益保障條例，法源法律網，
http://db.lawbank.com.tw/FLAW/FLAWDAT01.asp?lsid=FL013990

5、 簡榮宗，網路上資訊隱私權保障問題之研究，
http://www.cyberlawyer.com.tw/alan4-08_3-4.html

6、 立法院網站各國法律發展，
http://npl.ly.gov.tw/do/www/billIntroductionContent?id=19 1.資料保護法(德文版)：http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg03.htm 2.資料保護法(英文版)：
http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg01_eng.htm

7、 Data Protection Act 1998 Legal Guidance, available at <
http://www.dataprotection.gov.uk >

8、 行政機関等個人情報保護４法案の概要，日本總務省行政管理局，
http://www.soumu.go.jp/gyoukan/kanri/kenkyu_f.htm。

9、 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html 。

10、 OECD 網站：

(1) http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html 。

(2) http://www.oecd.org/document/1/0,3343,en_2649_34255_28863233_1_1_1_1,00.html 。

(3) http://www.oecd.org/document/50/0,3343,en_2649_34267_2514994_1_1_1_1,00.html 下載 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders http://www.oecd.org/dataoecd/24/33/2956464.pdf。

11、 網站 http://www.pmc.gov.au/privacy/apec/meetings.cfm 有 2007 First Data Privacy Meeting 相關資料。

12、 歐盟最新(2008-08-30) JOC_2008_224_R_0050_01 請參 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:224:0050:0056:EN:PDF

13、 See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 全文置於 http://www2.echo.lu/legal/en/dataprot/counceur/conv.html

14、 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, Official Journal of the European Communities of 23 November 1995 No. L. 281, p. 31. http://www2.echo.lu/legal/en/dataprot/ directiv/directiv.html

15、 自由電子報，開放肺結核個資，網搜曝光，2007.11.07 http://www.libertytimes.com.tw/2007/new/nov/17/today-life1.htm

16、 US to outlaw corporate prejudice based on genes http://www.newscientist.com/article.ns?id=dn11787&feedId=online-news_rss20.

17、 中央健康保險局網站
http://www.nhi.gov.tw/webdata/webdata.asp?menu=9&menu_id=175&webdata_id=917&WD_ID=196.

18、 台灣社會需要什麼樣的個人資料保護？–個資相關法案座談會
http://www.tahr.org.tw/index.php/article/2008/08/29/608/.

19、 聯合報，《基測個資外洩案 竄改三推甄生成績 交換個資》，2008 年 6 月 26 日。資料來源：
http://mag.udn.com/mag/campus/storypage.jsp?f_ART_ID=133171.

20、 http://www.epochtimes.com/b5/8/8/29/n2244755.htm FCRA 的全文與簡介，請參見聯邦貿易委員會(FTC)網站，網址：
HTTP://WWW.FTC.GOV/PRIVACY/PRIVACYINITIATIVES/CREDIT.。

21、 防制資料外洩評估實務 3 步驟
http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=4766 (2009.01.13)

22、 U.S. DEPT. OF COMMERCE, NAT'L TELECOMM. AND INFO. ADM., PRIVACY AND THE NII：SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995), *available at* <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.>（last visited on 2008/10/22）.

23、 S 1164, Location Privacy Protection Act.
http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp

24、 Personal Information Protection Law in Japan
http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=2920

25、 交通部電信總局相關網址
http://www.dgt.gov.tw/Chinese/Regulations/5.3/5.3.2/Query-user.shtml。

26、 電信事業用戶查詢通信紀錄作業辦法。

http://www.dgt.gov.tw/Chinese/News-press/94/press-dgtnews-940624.shtml
。

27、 Directive on privacy and electronic communications, DIRECTIVE 2002/58/CE, Article 9 and Article 6, 2002.07.31, p44-45, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

28、 資策會:台灣經常上網人口 1014 萬 普及率 44%【中央社】 http://www.fbb.org.tw/modules/news2/article.php?storyid=181

29、 資策會資訊市場情報中心（MIC）發表 2008 台灣網路購物市場報告。 http://incubator.sce.pccu.edu.tw/frontpage/front/bin/partprint.phtml?Part=news567&Category=&Style=3

30、 PChome 24h 購物 獲 97 年經濟部產業製程/流程創新獎 http://event.pchome.com.tw/ipo/invent/2008/in2008_1119.htm

31、 AC 尼爾森 2005 年全球消費者線上調查：
全球有十分之一的人口在網上消費 德英爲網路購物最大消費族群

http://tw.cn.acnielsen.com/news/20051101.shtml

32、 Yahoo!奇摩購物中心服務說明 http://buy.yahoo.com.tw/help/helper.asp?p=safety

33、晶片金融卡 Smart Pay 交易說明 http://shopping.pchome.com.tw/?m=index&f=activity&ac=AC00013604

34、 內政部自然人憑證發卡 2009/11/30 縣市統計資料 http://moica.nat.gov.tw/html/apstatistic.CEXE

35、 買家棄標熱門問題 http://help.cc.tw.yahoo.com/help_cp.html?product=2&catyname=%A5%E6%A9%F6%A7%B9%A6%A8%B6%B7%AA%BE&funclass=%B6R%AEa%B1%F3%BC%D0

36、 登入 Yahoo!奇摩

http://tw.memo.help.yahoo.com/c2c_read_announce.php?prop_id=2&mesg_id=71

37、 YAHOO 輕鬆付遭破解 駭客盜用帳號詐騙被逮
http://www.itis.tw/node/1154

38、 國民身分證領補換資料查詢 https://www.ris.gov.tw/uping_new.html

39、 韓國在爭議中推行網路實名制
http://news.sina.com/w/2008-06-18/164215770459.shtml

40、 露天拍賣隱私權保護政策
http://www.ruten.com.tw/system/server_center.htm?00060002

41、 http://times.hinet.net/times/article.do?newsid=1842697&isMediaArticle=true&cate=general

42、 iThome online
http://www.ithome.com.tw/plog/index.php?op=ViewArticle&articleId=21243&blogId=1252

43、 戰國策爆發客戶資料外洩事件

http://www.ithome.com.tw/itadm/article.php?c=53022

44、 英政府網站資安出岔　千萬民眾個資恐遭竊 http://www.itis.tw/node/2234

45、 智利電腦駭客盜走六百萬個資 po 上部落格 http://www.itis.tw/node/1761

46、 McAfee：資料外洩讓全球企業一年損失 1 兆美元
http://www.ithome.com.tw/itadm/article.php?c=53229

47、 木馬程式簡介 http://cissnet.edu.tw/knowledge_02.aspx

48、 「資料拼圖」成帳號竊取主要手法

http://www.zdnet.com.tw/news/software/0,2000085678,20127775,00.htm

49、 Security & Resolution Center

http://pages.ebay.com/securitycenter/index.html?_trksid=m40

50、中時健康
http://www.ctjob.com.tw/EnterprisesNews/News.aspx?ArticleId=7545

51、行政院經濟建設委員會第 1352 次委員會議紀錄
http://www.cepd.gov.tw/m1.aspx?sNo=0011546 。

52、自由電子報—亂花錢 1.2 億補助大企業提升資安，2009.02.26 參見
http://www.libertytimes.com.tw/2009/new/feb/26/today-p12.htm。

53、2007 網路安全信心調查：國人信心不足，最憂個資外洩，最盼嚴懲不法
http://www.als.org.tw/article/new_paper_sg.asp?id=168

54、EuroPriSe 相關資訊請參考：https://www.european-privacy-seal.eu/

55、プライバシーマーク制度設置及び運営要領
http://privacymark.jp/reference/pdf/pmark_guide080808/pmark_guide080808.pdf

56、指定基準全文，可自右揭網址下載：
http://privacymark.jp/reference/pdf/pmark_guide080808/Shiteikikan_Kijun.pdf .

57、指定調查機構詳細名單與資料，
http://privacymark.jp/agency/member_list.html .

58、現階段已取得日本「隱私標章」企業之詳細資料，
http://privacymark.jp/certification_info/list/clist.html .

59、OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002), *at* http://www.oecd.org/dataoecd/16/22/15582260.pdf.

60、行政院國家資通安全會報，http://www.nicst.nat.gov.tw。

61、國家標準（CNS）檢索系統，http://www.cnsonline.com.tw/index.html。

[1]

附件二　行政院研究發展考核委員會對「政府機關強化個人資料保護措施之研究」期中報告審查意見及回應

98 年 3 月 18 日

一、 實務上，司法院大法官解釋雖先後於該院釋字第 585 號及第 603 號等 2 號解釋中明文表示隱私權屬憲法第 22 條保障範圍;惟該院釋字第 535 號解釋似僅敘及隱私權爲憲法保障之權利，並未認定隱私權屬憲法第 22 條保障範圍。是研究報告第 1 頁所稱「…釋字五三五號解釋文再次明確使用隱私權，並確認隱私權爲憲法二二條概括基本權所保障。」建議能於本案期末報告初稿相關處能有更明確之說明；另按「後天免疫缺乏症候群防治條例」業於 96 年 7 月 11 日修正爲「人類免疫缺乏病毒傳染防治及感染者權益保障條例」，故研究報告第 2 頁（5）引該條例舊名稱卻於其註 4 列上開修正時間，建議能於本案期末報告初稿中修正。

研究團隊回應：經確認 585 號解釋爲隱私權之確立，603 號解釋爲確立資訊隱私權．另有關「後天免疫缺乏症候群防治條例」一節，已依建議修訂．

二、 本研究第二章就美國、德國、英國、日本、經濟暨合作發展組織（OECD）及亞太經濟合作會議（APEC）等國家或組織之隱私權相關法制進行介紹，惟對於國外之最新理論見解與規範趨勢之整理分析仍有不足，建議進一步瞭解各國政府在落實個人資料保護相關法規方面採取哪些具體的措施？我國法令執行狀況相較之下何以不足？方符比較法制研究之方法與目的。

研究團隊回應：已依建議於結論章中敘明並比較參酌之．

三、 針對我國個人資料保護與資訊安全法制分析，有關「個人資料保護法」修法的各種爭議，尤其是諸多民間團體對於官方修法版本和立法委員修法意見所提出的建議和質疑，其內容應能反映出我國現行「電腦處理個人資料保護法」及當前政府機關個人資料保護措施不足之處，請就此一面向進行補強及深入分析。

研究團隊回應：針對立委修正建議多爲個資法草案賠償機制與罰則問

題，另有關個資法草案學者建議部分，已參考近期法學論著補充（如針對公務機關例外處理、利用個資之評析及資訊保護官(類似機制）設置等建議）。

四、 第四章有關民眾就醫資訊之探討，有些特定的個人資訊保護問題，可能涉及其他法制如醫療法和人體試驗相關法制等，本研究論及是類問題，應做較深入之分析。另第二節係以醫學系實習生強制篩檢愛滋案爲案例，建議增列大考中心資料外洩、指考及基測學生資料遭補習班不當利用等案例，作爲就學個人資料外洩所引發侵害民眾隱私疑慮之探討議題。另本節研究內容建議參照第一節架構進行論述。

研究團隊回應：建議增列大考中心資料外洩、指考及基測學生資料遭補習班不當利用等案例，作爲就學個人資料外洩所引發侵害民眾隱私疑慮之探討議題已補充進入期末報告。有關人體試驗相關法制一節，本研究已點出並建議法務部重新針對「敏感性個人資料」之相關文字重新釐清。

五、 第五章對於非公務機關網路購物、金融、電信與消費隱私之保障等文獻資料相當完整，惟對於違法洩露個人隱私之非公務機關的罰則問題等並未著墨，應加強整體性的歸類和分析；另第三節研究內容建議參照第一節架構進行論述。

研究團隊回應：本研究並未涉及罰則之建議乃由於前述回應提及，罰則爭議是行政機關授權立法後，，與代表民意之立法機關協商下之產物，此爲國內立法之現實生態。本研究之結論，係從建議法務部及洩漏個資頻繁的非公務機關之主管機關角度層面出發，建議重新、全面將監管相關法制配合個資法修訂，作一檢討並期盼提升法位階層次。

六、 第六章主要介紹日本等國家之「隱私權標章制度」，卻缺乏系統性的分析或結論可供我國參採之處，體例上不免突兀，請研究團隊再檢討其必要性並加以調整。

研究團隊回應：已依建議於結論章中適度表述。

七、 第七章之研究結論尚未就前面章節所發現之問題癥結提出改善建議或

可執行之配套措施；此外，內容過於強調資訊安全及相關法制建立之問題，對於個人資料保護法制的修正方向，似乎著墨過少。至於政府內部應該建立哪些制度〔例如個人資訊保護官(類似機制)〕，以及中央和地方機關應該如何分工，才足以落實資訊安全和資訊保護法規，應於期末報告補強。

研究團隊回應：已依建議於結論章中適度表述。

八、 本研究內容稍嫌零散，建議針對我國各行政機關所屬主管事項，在個人資料保護措施方面有哪些不足之處，進行更全面性、系統性的檢索、歸類和分析，方能展現本研究的實務貢獻。

研究團隊回應：已依建議於結論章中適度表述。

九、 本研究原排定於 97 年 7 月-10 月間就主要議題進行學者專家座談，惟迄今尚未辦理，請加速趕辦並將座談會紀錄列入附錄。

研究團隊回應：已改進並詳附會議記錄。

十、 研究報告內容未見參考文獻附錄，單就附註內容來判斷參考資料來源、範圍及正確度，仍嫌不足，請將參考文獻增列入附錄。

研究團隊回應：已改進。

十一、期末報告請依照本會報告格式處理。

研究團隊回應：已改進。

附件三　期末報告修正說明

（一）陳教授美伶（文化大學法律學系）：

1、研究方法：本項研究較偏重文獻與資料之分析論述，尚乏實證的對照。既以「強化」爲主軸並以「政府機關」爲對象，宜加強現況之調查與分析，始符合目標之設定。

研究團隊回應：現況調查分析係依據彙整相關新聞摘錄案例爲之，有呈現在前面各章節中。

2、研究資料：研究蒐整資料充實且多元，尚符合研究案設定之目標。

3、研究結論：結論稍嫌零散且未能扣合主題，是否可成爲政策建議之立論基礎宜再斟酌。

研究團隊回應：已改正

4、研究建議是否可具體可行：建議分短、中及長程，內容堪稱具體明確，惟偏向法制化之建議，行政部分較無創見。另行政部分之建議缺少強化政府資通安全組織之論述，以及運用資訊科技保護個人資料等技術層面之具體作法，建議補充相關內容。

研究團隊回應:已依委員建議加強,並江委員發言記錄列於註釋中(參見第七章「結論與建議」第二節）

5、建議本研究應（可）修訂部分：各章內容具獨立性，惟與研究主題欠缺聯結，建議研究發現部分重新調整，強化整體性的論述，有系統的將各章的重要研究發現與結論具體呈現。

研究團隊回應：已依研考會意見做章節調整

（二）劉教授靜怡（台灣大學國家發展研究所教授）

1、研究方法：請強化個人資料保護措施的實證研究。

研究團隊回應：本研究案各議題均以新聞事件做爲實證研究基礎，且電子商務部分亦利用各網站功能進行實證評比分析。保護措施之「實證」研究，似非本計畫題目所強調。委員建議將於結論章節中改進。

2、研究資料：有關美國文獻部分應請更新資料內容。

研究團隊回應：委員所指之部份文獻，已盡量補充

3、研究結論：第 221 頁至第 222 頁（註 354）的研究建議應註明出處。

研究團隊回應：已補正註明出處

4、研究建議是否可具體可行：請依「就醫」等 5 個個人資料類型，進一步提出類型化之建議。**研究團隊回應：將於結論建議章節中加強說明**

5、建議本研究應（可）修訂部分：

（1）第七章結論與建議欠缺系統性的論述，建議重新歸納整合。

研究團隊回應：已依委員建議調整。

（2）民眾之個人資料係由各目的事業主管機關本於權責加以監督管理，例如「人體生物資料庫管理條例草案」由衛生署主管，因此，除個資法提供整體性的規範外，宜由各主管機關審視其主管法規在個人資料保護措施上是否完備。

研究團隊回應：此部分已呈現於結論建議中，但會將委員針對具體主關機關業務執掌予以進一步描述

（3）設置「資訊保護官(類似機制)」之建議涉及政府單位之組織結構及人力配置，宜由行政院做整體考量；至於非公務機關如擬透過市場機制及自律輔導來強化個人資料保護，若缺乏誘因或獎懲機制，將難以落實，請研究團隊強化相關論述。

研究團隊回應：已依建議予以補強自律機制部分於結論建議章節中

（三）黃教授明達（淡江大學資訊管理學系）

1、研究方法：研究範圍較廣泛，宜有特定研究對象較佳，如探討「電信資訊」之個人資料保護措施時，可考慮針對某電信公司進行個案分析。

2、研究資料：蒐集 OECD、APEC、歐盟、美國、日本等組織或國家的相關資料，尚屬完備。

3、建議本研究應（可）修訂部分：研究建議宜與研究過程所蒐集的內容及研究發現互相佐證。

研究團隊回應：已依多數委員建議予以補充修訂

（四）胡副教授毓忠（政治大學資訊科學系）

1、研究建議是否可具體可行：各項短、中、長程建議在技術與實務面該如何落實與執行，需再加強相關論述。

研究團隊回應：已於結論建議章節中加強

2、建議本研究應（可）修訂部分

（1）如何落實並執行資料分享和流通使用，並且符合個人資料保護法規的電腦規範，以達成個人資料保護的目標，需要再強化和討論。

研究團隊回應：已於電信小結中建議採用八大準則，供政府參考

（2）公務及非公務機關運用個人資料時，如何落實個人資料保護監督工作，並避免落入違反人權及個人資料保護法之情況，似宜再進一步論述

研究團隊回應：在資料運用及行政協助部分已有論述，請參相關篇幅

（3）宜就屬於電腦化和非電腦化之個人資料保護措施加以區隔論述。

研究團隊回應：委員建議似與個資法修訂分類及宗旨有差，未進一步區隔

（4）建議運用個案情境的描述和分析，以驗證結論與建議的可行性和必要性。

研究團隊回應：本報告均於摘錄之新聞報導後，做實際法律面之分析

（五）蘇副主任俊榮（財政部財稅資料中心）

1、多數政府機關已通過 ISO27001 驗證，透過 ISO27001 之 11 個構面作系統化檢視，確保機關對重要資訊資產之保護。惟第 216 頁提出電信業管理方法僅就「資料安全方面」、「資料稽核方面」…等 4 構面規範，其作法卻可作爲其他產業之借鏡參考，請再補充說明。

研究團隊回應：電信討論章節中參考之八大準則，將適度納入結論中一體建議適用

2、建議就現行資訊安全管理系統（ISMS）之 ISO27001 認證有關資料保護部分及隱私標章認證進行比較，說明二種規範重疊部分，避免未來政府機關制度設計疊床架屋，另亦請補充建議政府機關應加強防護之部分。

研究團隊回應：已依建議增列 ISO 標準做爲補充說明

3、本研究對於現行資料防護方式及技術說明篇幅過少，可新增一節討論下列問題：**研究團隊回應：已依建議增列 ISO 標準做爲補充說明**

（1）本研究僅以 1 頁（第 220 頁）說明資料保護方式之建議，應就管理面及技術面，提供管控方式之具體規範，以及補充目前政府機關「資料防護方式及技術」相關作法。（可擇一重要機關說明）
（2）可就各政府機關「資料防護方式及技術」現行作法與個資法（草案）或隱私標章認證不足部分再補充說明。
（3）補充說明未來政府機關資料保護管控方式及技術應加強之方向。
（4）建議就各項防護方式或技術所增加成本部分提出說明，例如系統效率降低、預算成本增加。

4、附件 4 建議修正部分

第 256 頁：「500 萬筆財稅個資外洩」建議修正爲「網路申報財稅個資疑似外洩」。

研究團隊回應：已依建議微幅修改文字，免生疑慮。

（六）徐科長振邦（教育部）

1、研究結論第 226 頁敘明「目前就學資料的資安防護是政府部門間較為迫切需要注意的」，似乎指涉強調推動資安政策不力，不知如何推論？

研究團隊回應：已依建議微幅修改文字，免生疑慮。

2、針對本研究將國中基測考生個資外洩案列為個案加以分析，本部體認到其新聞事件所引起外界重視的程度，已積極規劃成立基測專責單位，並自本(98)年起，委請國立臺灣師範大學協助辦理試務電腦作業，加強保護考生個資。

研究團隊回應：已依建議改正

3、有關研究結論建議於各級學校設置「資訊保護官(類似機制)」一節，除涉及人員編制增列及經費籌措外，因國民教育階段之人事屬地方自治事項，另有許多國中小班級及學生數不多，設置專人辦理，是否符合成本效益？請再酌。**研究團隊回應：已用適度文字表述貴部主管業務困難及立場**

4、本研究結論與建議宜徵詢相關部會意見再行定案。**研究團隊回應：已採納**

（七）熊研究員正佩（經濟部商業司）

1、電子簽章法之配合檢視部分（第 228 至 231 頁之建議）：

經濟部商業司係主管電子簽章法之修訂與解釋，依該法第 11 條規定，憑證機構應製作憑證實務作業基準應載明之事項送本司核定。內政部憑證管理中心憑證實務作業基準係內政部主管，醫事憑證中心憑證實務作業基準為行政院衛生署主管，政府憑證總管理中心憑證實務作業基準、政府憑證管理中心憑證實務作業基準、組織及團體憑證管理中心憑證實務作業基準，均係行政院研考會主管。文中所提自然人憑證之核發與推廣應用為內政部主管，與電子簽章法修訂內容無涉。**研究團隊回應：報告中並未混淆**

2、監督機制之建議：

若個資法修正通過，各行各業將全面適用，文中論及個資外洩之電信業，其目的事業主管機關爲國家通訊傳播委員會。**研究團隊回應：報告中並未混淆**

（八）楊科長秀蓮（行政院金管會銀行局）

1、 第五章所引「金融服務業現代化法案」（第 87 頁）、「金融消費者資訊隱私權法」（第 89 頁）及「財務隱私權法」（第 94 頁）與第七章第四節整體建議部分二、行政部分建議本會應對「隱私標章認證制度之推行」審慎評估與建議研議金融隱私部分（第 230 頁），均涉及整體金融業之規範，應由本會主政爲宜。**研究團隊回應：考慮在結論建議中敘明貴會立場**

2、第五章第一節第一項所提及網路銀行監理一節(第 82 頁)，建議結語改爲「故我國網路銀行業務開展可視爲乃以傳統銀行經營業務的另一型態，主管機關業納原先實體金融業高度管制的規範體系管理之」。

研究團隊回應：已依建議改正。

3、第五章第一節第二項(第 82 頁至 86 頁)金融業對個人資料的蒐集、處理、利用及保全，僅述及金控公司與其子公司及各子公司間之規範，至非屬金控公司及其子公司之規範與其他通則性規範並未敘明，建議補充之。

研究團隊回應：座談會中已表達立場，本研究計畫並非專爲金融立法做比較，限於篇幅時間，有待於其他研究計畫加強研究。但已有利用註釋部分，略述之。

4、第五章第一節第二、三項(第 82 頁至 96 頁)分別簡介台、美金融業對個人資料之蒐集、處理、利用及保全規定，並於報告第 94 頁以文字簡要說明我國規定與美國之「金融服務業現代化法案(GLBA)」及「金融消費者資訊隱私權法(Regulation P)」間之差異，建議就兩國之重要規範及立法意旨以表列方式提供異同比較。

研究團隊回應：座談會中已表達立場，本研究計畫並非專爲金融立法做比較，限於篇幅時間，請於其他研究計畫加強研究。

5、第五章第一節第三項（第 94 頁）所述有關金控公司子公司取得客戶資料之「事前書面同意」及「嗣後選擇退出」之機制，恐不經濟而與經營綜效目標有悖乙節，按金融控股公司子公司依金融控股公司法第 43 條之規定，交互運用客戶資料，而有關客戶資料之取得過程及事後之維護控管，自必附隨衍生相關成本，與經營綜效無涉，並與報告第 92 頁有關美國金融服務現代化法案中有關金融機構必須滿足「告知」及提供消費者選擇終止機會之立場不符。

研究團隊回應：已依建議將部分文字刪除，免生疑慮。

6、第五章第一節第三項另提及美國之財務隱私權法及公平信用評等法案(第 94 頁至~96 頁)，惟並未說明該二立法是否可作爲我國未來立法之參考，建議可補充之。

研究團隊回應：已於小結前言部分加強說明外國法令直的參考部分。

7、第五章第一節第四項（第 97 頁）提及我國現行法令架構具二大缺失，建議具體說明並提出建議，以爲本會日後修訂相關法令之參考。

研究團隊回應:已利用註釋部分予以舉例說明,以降低主管機關之不便。

8、第五章第一節第五項提供國內外近來與資料外洩或資料保護相關之案例(第 97 頁至 102 頁)，建議可增列一總結意見，就各案例之因應措施、改善建議及所獲啓示彙整說明，並可作爲第六項各建議之部分立論基礎。另四、遏止網路釣魚，金管會提供金融業網站資料（第 101 頁），本會網站於 98.8.24 改版首頁相關單位內容以重新區分爲「金融資訊網站」、「本國公(協)會」、「外國相關網站」、「其他政府網站及相關活動專區」、「合法金融業網站連結」、「上市（櫃）、發行公司網站連結」、「金融發展研究基金專屬網頁」等七類。

研究團隊回應：已依建議予以修訂

9、第五章第一節第六項「小結」(第 102 頁至 103 頁)係就金融機構委外實務

提出建議，惟其內容似亦可適用於非委外業務，若是，則該項之序言或可略作修正(即不侷限於委外業務)。另因第五章第一至四項均在論述資料保護之相關規定，然建議事項卻未對我國現行法令提出任何建議，可再補充之。

研究團隊回應：已依建議將委外字眼予以擴大。並於小結前言部分加強說明外國法令直的參考部分。

10、第七章第四節二、行政部分（一）短程建議 1.（第 230 頁）金融隱私部分亦建議財政部與金管會共同研議，關於「金融隱私」部分應如何加強與改進方向，建議可具體說明並補充之。

（九）法務部法律事務司書面意見

1、本研究報告之主題爲「『政府機關』強化個人資料保護措施之研究（初稿）」，然其中第五章則係在探討「『非公務機關』對於金融、電信、網路購物與消費隱私之保障」，似乎與本報告之主題不盡相符，建議第五章之討論重心應予調整，例如可探討目前銀行業之主管機關（行政院金融監督管理委員會銀行局）對銀行業強化個人資料保護措施有何督導作爲等是，另在第五章舉出國內外近來發生案例，其中一例爲 2500 萬筆財稅個資外洩（本報告第 100 至 101 頁），又提及可能是公務機關之「財政部」外洩之賠償責任等語，亦與本章係在探討「非公務機關」之主題不符，亦併請調整。另本報告著重在法制度層面之論述，在強化個人資料保護措施之建議上，仍嫌不足，建請加強實際操作層面之論述，以豐富本報告之研究成果，並可供政府機關採納操作。

研究團隊回應：報告係全文引用新聞報導文字做爲實務分析，對於部分新聞用語之準度，已依建議予以改正

2、電腦處理個人資料保護法（以下簡稱個資法）歷經多年修法，版本多元，目前最新進度係於立法院完成一讀程序，研究報告第 X 頁、第 228 頁「…建議新法案送交立院審議時…」、第 29 頁「增訂敏感性資料蒐集之限制：有關犯罪前科、健康、醫療及基因等四類個人資料（目前草案總共應爲 5 類）」、第 30 頁「非公務機關蒐集兒童資料之限制（目前草案無之）」、第 32 頁「行政院在立法理由中即建議，於新法中增列機關首長核准制度，以強化檢查程序…（目前草案無之）」等，經查均

與目前草案之進度及內容不符，建請修正。另報告第 26 頁：「目前經指定納入個資法第 3 條第 7 款第 3 目的團體計有：…」查截至今年為止，已有 10 個事業團體經指定納入適用個資法之範圍，本報告之資料應予更新（最新資料可在本部網站法律事務司之個資保護項下查詢）。

研究團隊回應：已依建議改正

3、依個資法第 27 條第 1 項規定，公務機關係負無過失之損害賠償責任（除非機關能證明損害係因天災、事變或其他不可抗力所致，始可免責），另依個資法第 28 條規定，非公務機關係採推定過失主義，需由非公務機關舉證證明自己無故意過失，始可免責，研究報告內第 54 頁有關侵權行為主觀要件需由當事人舉證之說明，似與法條規定不符，建請修正。

研究團隊回應：查

故意責任：要故意行為才處罰，像毀損罪，過失毀損不會罰

過失責任：過失行為也會處罰，像侵權行為，過失也罰

事變責任：無過失也會處罰 事變責任又分二種：

不可抗力責任：如天災造成，也要負責

通常事變責任：指即使債務人已盡其應盡注意義務，但而仍不免發生

已依法務部建議，適度於文字說明。

4、本報告多處提及，個資法草案第 6 條、第 15 條、第 16 條有關（特種）個人資料例外允許可以蒐集或利用之情形過多（例外規定過於寬鬆），有些情形基於公益理由，不必經當事人同意即可為蒐集或為特定目的外之利用，恐對當事人保障不足，保障資訊自決權恐將形同具文（例如本報告第 X 頁之 1.對於個資法修正之進一步建議、第 49 頁之（三）、第 50 頁之（四）、報告第 76 頁、第 221 頁等），查個資法第 1 條明文規定，個資法之立法目的除避免人格權受侵害外，「並」有促進個人資料之「合理」利用之功能，當私益與公益有所衝突時，於合乎憲法比例原則之考量下，立法者認為不必獲得當事人書面同意，即可本於法律明文規定或公務機關基於執行法定職務之必要，蒐集或利用當事人之個人資料，此係為平衡「私益」與「公益」而設，如所有例外情形

均須得當事人同意，可能影響公共任務或公權力之行使，有害於公益（例如行政執行機關蒐集公法債務人之財產資料，係本於法定職掌之作為，如需先得債務人本人同意，豈非通知該債務人事先脫產？）是以，個人之資訊自決權於此範圍內應受限制。

研究團隊回應：已將法務部之意見利用註釋方式呈現於…「有論者」以為…之條文建議下方，充分反應法務部之立場。

5、本報告提及，個資法對公務機關侵害個人資訊權之自我監督檢查機制付之闕如，建議設計監督機制，以避免對個人資料利用之浮濫（報告第 X 頁、第 51 頁之（六）、第 226 頁）一節，查行政機關之行政行為本應受憲法及行政法上一般原理原則之拘束，無待明文，如本研究報告之法評價上，認為公務機關侵害個人資訊權應比其他限制或剝奪人民權利之行政作為更須建立公務機關之自我監督機制，建請提供相關條文之修法建議，並提供相關立法例，明確建議公務機關應採何種自我監督措施，以同時兼顧個人資訊權與公益及行政效率之要求，本部將審慎評估納供修法之參考。

研究團隊回應：監督機制部分已透過「資訊保護官(類似機制)」之建議提出

6、本報告提及基測個資外洩案中，博暐公司受教育部委託處理考生個人資料，如考生資料外洩，可依國家賠償法向博暐公司及教育部請求損害賠償一節，惟依個資法第 5 條及其施行細則第 11 條第 2 項規定，博暐公司視同委託機關（按應為國立桃園高中）之人，當事人行使個資法之權利，仍應向國立桃園高中為之。

研究團隊回應：已改正

7、目前我國並無個人資料保護之專責機構，故個資法之規範設計係採分散式管理模式，由各目的事業主管機關就所管事業（團體、個人）加以監督管理，本報告第 130 頁提及「在未來，應鼓勵不同行政機關，就其個別行政任務之特殊性，制訂出符合該法領域之資料保護規範」，本部至為贊同，是以，本報告提出對個別產業管理相關法制建議部分：「…另針對特殊產業，是否仍有必要（如就醫資訊相關產業），另行訂定新的處理原則，亦為個資法通過施行時之一大考驗，建議主管機關

（法務部）及早透過公聽方式，獲致共識，以為因應」等語（報告第ＸⅠ頁、第 229 頁），基於權責分工以及部會互相尊重之立場，仍宜由各目的事業主管機關本於權責審酌是否就各該行業增訂相關法制，而不宜由本部主導，惟如各該部會認有增訂法規之需要，本部仍將適時協助提供法制作業之相關意見（另本報告第ＸⅠ頁至第ＸⅡ頁、第 230 頁提及輔導獎勵之規劃研議部分，因個別產業情形不同，同理亦須由各目的事業主管機關本於權責主動規劃輔導獎勵措施）

研究團隊回應：毋須改正

（十）衛生署疾病管制局書面意見

1、P55(註記 112)「人類免疫缺乏病毒傳染防治及感染者權益保障條例第 8.,10,18 條，人類免疫缺乏病毒傳染防治及感染者權益保障條例施行細則第 3,5-7 條・…署授疾字第 0930000341 號」因法規名稱已依 96 年 7 月新修訂內容，惟條文內容為舊法之條次，且該次修正業將施行細則刪除，惟其授權訂定之補償辦法尚未完成法制作業程序，原施行細則尚未完成廢止程序，故援引之施行細則不宜使用新條例名稱，建議修正為「人類免疫缺乏病毒傳染防治及感染者權益保障條例第 15.,16,23 條・後天免疫缺乏症候群防治條例施行細則第 3,5-7 條・…署授疾字第 0970000016 號」。

研究團隊回應：已改正

2、P56「根據人類免疫缺乏病毒傳染防治及感染者權益保障條例(之前稱為「後天免疫缺乏症候群防治條例」)第 8 條第 1 項規定，當衛生單位接獲報告或發現感染、或疑似感染愛滋，及與感染愛滋病毒者共同生活或有性接觸者，應通知篩檢，逾期未受檢則強制篩檢。疾管局曾以行政院衛生署 93 年 4 月 16 日署授疾 0930000341 號函公告，基於感染風險、…包括性工作者、嫖客、性病感染者、吸毒者、賣毒者、男性間有性行為者」一節，配合條文修正，第 8 條改為第 15 條；刪除共同生活或及男性間有性行為者等字語；93 年 4 月 16 日署授疾 0930000341 號函修正為 97 年 1 月 18 日署授疾字第 0970000016 號公告。

研究團隊回應：已改正

3、75 頁第二行配合條文修正刪除「實習機構基於感染風險及國內防疫等目的，必須取得實習生之愛滋病歷資料，勘稱正當…」等文字。

研究團隊回應：已改正

（十一）研考會意見：

1、研究發現欠缺系統性的論述，請重新歸納綜整。如第七章第一節提出「資訊安全法制之建立」,由於資訊安全法制相關探討未於前述各章節出現，即導入研究發現，略顯突兀。

2、本研究提出建立資訊安全法制、個資法修正條文等政府機關強化個人資料保護措施之建議，惟均著重整體法制面，欠缺對於「就醫資訊」等 5 個議題之個別建議與配套措施，請補充相關內容。

3、本研究建議透過修正個資法相關條文來強化公務機關蒐集、處理及運用個人資料之監督機制，雖有參考價值，惟在立法完成前，政府機關如何避免公務人員利用職務不當蒐集、處理及運用個人資料，侵犯及損害民眾權益，建議研究團隊補充如何強化政府機關內部之監督考核機制。

4、本研究重點及預期成果之一係檢討各相關主管機關對非公務機關蒐集、處理及運用個人資料之監督機制。本研究對於上開監督機制之建議採「市場機制」及「自律輔導」之方式解決，惟未提出相關配套措施或具體作法，建請補充相關內容。

研究團隊回應：自律機制部分已於結論章節前言部分加強敘明

5、章節安排及內容：

（1）各章內容係依專長分工撰擬，論述架構與體例不一，例如第四章與第五章雖同屬案例類型化分析，但二者論述方式明顯不同，尚需調整修正。

研究團隊回應：已於小結部分適度調修改正

（2）第一章第二節「現有相關法制發展部分」與第二章第三節「相關組織對於隱私權保障發展方面」內容與議題相同，建議整併至第二章。

研究團隊回應：已改正

（3）第七章第二節係針個資法中公務機關監督機制之強化提出修正條文建議，與第四節對於個資法修正之建議內容相同，請予整併；第三節「個資法中非公務機關之部分宜透過市場機制及自律輔導解決」所列政府宜透過補助或輔導方式協助中小企業等三項建議皆爲政府提高電子商務安全之措施建議，顯與前開標題內容不符。

研究團隊回應：已於結論章中之前言部分略加強說明相關連處

（4）對於個別領域之法制分析、背景及名詞定義等內容著墨過多，如第五章引用「金融控股公司及其子公司自律規範」、「美國電信法」、「歐盟電子通訊個人資料處理暨隱私權保護指令」等，多將條文直接貼入本文，缺少相關解析說明，建議酌予精簡或改列爲附錄以提高可讀性。

研究團隊回應：已改正

（5）本研究漏（冗）字、錯字仍請研究團隊謹慎檢視後修正（如 p1、p2、p56、p59、p 196、p228、p216）；另內容格式請依本會作業規定修正。

研究團隊回應：已改正

八、研究小組說明：

有關資料修訂部分，研究團隊將依據與會學者及委託單位所提供建議進行修正；另錯漏字亦一併更正。針對部分委員意見已於座談會中予以回應

附件四　期末報告初稿學者專家座談會會議紀錄

「政府機關強化個人資料保護措施之研究」計畫案學者專家座談會記錄

時間：2009 年 5 月 12 日上午十點

地點：東吳大學法學院 1704 研討室

參與人員：

(1)研究團隊：余啓民老師、葉奇鑫律師、陳芊諭助理、劉蓉菁助理

(2)與會專家：司法院資訊處郭瑞蘭處長、台北地檢署張紹斌主任檢察官、金管會資訊處薛大勇副處長、警政署資訊室李相臣主任、資策會科技法律中心戴豪君主任、遊戲橘子李永欽法務長

(3)研考會承辦人：戴純眉小姐

一、余啓民老師簡報

（一）針對公務機關個人資料保護之建議。

（二）對於個資法草案條文之看法。

（三）對於非公務機關有關身份認證機制採代碼(token)方式爲之，輔以自然人憑證之推動的看法。

（四）對於隱私保護標章制度及審核程序之看法，例如我國應否積極推動隱私保護標章。

（五）資安法制及程序之建議。

（六）其他建議事項。

二、專家座談會提問

（一）研究題目與內容是否配合？

郭瑞蘭處長：

內文與題目有不搭配之疑慮，即內容比題目涵蓋的範圍廣。若委託單位設定之研究目標也有包含非公務機關之個人資料保護之研究，建議設法

使研究題目同時涵蓋公務關與非公務機關。

余啓民老師：
公務機關針對就醫與就學，其他如警政戶政等公務機關資料交換、調閱及交叉運用資料等情況。

戴純眉小姐：
題目主要爲研究公務機關蒐集與處裡個人資料現況之問題，教育部及衛生署做案例化及類型化之研究；至於非公務機關的部分，由於有網路購物等，公務機關如何去監督非公務機關，例如現行個資法是否訂有條文關於罰則、如何預防非公務機關繼續洩漏個資，以及賠償補救機制。研究團隊可能是三個負責撰寫的人，因此內容比較分散，希冀透過座談會給予研究團隊如何限縮內容之建議、鎖定焦點，以達成預期目標，提供公務機關政策上之具體建議。

張紹斌主任：
撰寫內容看起來似乎是以個資法作爲分類，超出題目範圍之非政府機關的部分，建議加副標題-以個資法爲中心。其中網路購物的露天拍賣是最沒有紛爭的，但是與公務機關沒有太大關係。

（二）簡報第九頁針對政府補貼資安預算部份作討論。並請專家對收尾建議內容提出己見。

李相臣主任：
政府機關內部資料控管與保護措施；政府機關如何監督非政府機關之資料流通，最多侵害案例出現於此。內容以第五章爲重點，第六章隱私權標章，是否需要刪除？

戴純眉小姐：
建議過大，需要具體可行的措施。例如列舉幾個主管機關以及主管機關

之權責。鼓勵自然人憑證之運用，應如何施行？

戴豪君主任：
研究團隊切入點以行業別分類討論頗值贊同。
針對計畫結論部分的具體建議：

1. 首先有關政府補貼資安預算：在去年全國科技會議後，經濟部已對某些例如輔導零售業、無店面建立計畫與機制去輔導。政府如何去輔導企業或是自己建立資安機制是比較需要討論的。
2. 其次在自然人憑證的應用上。舉例而言，最近行政院在推行公務員識別證欲結合自然人憑證，自然人憑證只要是中華民國國民都可以申請，而屬性憑證一定要有專業證照或某組織團體，國內應用屬性憑證最成功的是衛生署的醫師人員憑證（HCA）。現在公務員的屬性憑證欲將公務員的自然人憑證與屬性憑證合而為一，可能需要審慎考量。政府政策上已經決定這樣做，在經濟上效益是有，但是全面推廣自然人憑證應考慮到兩個問題：一是自然人憑證是否有逾越 CPS 的使用範圍，應進一步確認 CPS 載明的範圍，如果超過該範圍，是否可行？第二是否可以限縮公部門 G2B 的運用？對此應注意我國電子簽章法中規定當事人自主原則，當事人包括自然人，電子簽章、電子文件均應得當事人之同意，公部門不得強制要求。
3. 幾個提供給政府建議的大方向：
   (1)　關於資訊保護官(類似機制）及公務機關自我監督--
   未來配合組織改造（資訊長 法務長 主計長）從院的層級來看，應把業務放在哪一個長？法務部過去曾經要設隱私署但未達成。另外公務機關的自我審查是要做，應特別注意「資料拼圖」的問題。稅捐機關有財產總歸戶，公部門間（例如稅捐機關與間機關）互相的資料流通可參考歐盟相關指令。
   (2)　參考國外立法例，相信未來個資法不會是唯一的法律，尤其是醫療、電信、金融三個行業應要有特別專精立法。個資法過去是規定八大行業，現在把八大行業取消，變成普遍應用，更加確定個資法成為一個基本法，亦即成為一最低標準。但此最低標準在某些行業沒有適用，例如前述醫療、電信、金融行業或許有更高的隱私標準，因此除未來個資法的修法通過後，要求各目的事業主管機關訂定行政規範，例如敏感性資料以衛生署為最大宗。

(3) 公部門的個人資料除了重視如何保護外，也應注意如何利用這些個人資料，例如因應 SARS 的危機，有時公務機關要有積極的機會利用。

李永欽法務長：

非公務機關而言，蒐集愈多的個人資料，法律上的義務似乎就愈多？對於線上遊戲或網路購物業者來說，不論是業者或消費者都希望這些環境越安全越好，以減少實體和虛擬財產的損害。但現階段非公務機關在個人資料的蒐集上，蒐集的越多，風險就越大，現在非公務機關都傾向於「個人資料最少蒐集化」。

另天堂遊戲開始後，台北縣刑警隊便建議本公司導入自然人憑證並應用到遊戲內。三、四年前在相關技術成熟後本公司導用了自行開發的憑證技術到遊戲中，相關憑證的發卡量超過三十萬張，但實際使用的人大概只有一半而已，研究原因發現，用了憑證後對於現金交易道具者和外掛使用者會不方便。所以技術和方便性必須取得一個平衡點，使用者才會多。

其次對於非公務機關而言，雖然在法制面各界期待導入德國與日本的標章制度，但企業法務長重視的是降低企業風險、控制損失的範圍，因應新的個資法草案的團體訴訟制度，如果一企業使用了標章制度，花了大成本加強了該制度所要求的資安防護並取得了標章，若還是不幸發生了個資洩漏事件，在訴訟上法官對企業責任的的裁量標準會降低嗎？企業的損害賠償責任因取得標章就可以減少？如果不會的話，爲何企業要花這些錢去做這些事情，因爲企業增加再多的資安成本仍沒有十足的把握保證可以防止駭客的入侵，在現階段法令並未有相關的想法前，企業有沒有可能期待一個更符合這些社會價值判斷的法令產生？例如大陸和韓國都有對於使用外掛式者的處罰及對於企業責任的降低等立法以加強防護。如我國也能如此，或許企業或公部門（例如警方）也就再也不用耗費那麼多的資源處理資安的案件。

李相臣主任：

目前研究報告與預期目標、結論脫節。

第二頁上半部（檢視公務機關、檢視非公務機關、檢討相關政府機關對

非政府機關的監督、提出建議），與第九頁上面（鼓勵政府機關輔導民間企業，本來沒事結果建議找事，與主題不符）完全是錯的答案。

第二頁上面第二點建議淡化，因爲第三點已經達到第二點的目標，主題應該是檢討公務機關對非公務機關處理個人資料的監督機制，而第九頁上半部其實都可以拿掉，因爲研考會要的不是這個，這個是經濟部(補助一節)的事情。研究內容裡面其實都有答案，只是結論下錯方向。

我的建議是，

(1) 政府機關應如何導入標章？例如警政署應該哪部份應該處理，哪些部份不要處理，應通過怎樣的審核機制？

(2) 有關資訊官的設置，現在沒有資訊的主管機關，學校更慘，學校沒有資訊人員的編制。所以可以討論，政府是否設置資訊長之外，各機關是否應有專責人員？

(3) 針對非公務機關進行審核，目的事業主管機關應明確化，例如雅虎，誰是目的事業主管機關？經濟部只是發執照。

(4) 賠償制度的建立，民眾如何知道政府保存的資料是錯誤的（例如出入境紀錄）？賠償機制的建立，如何要求政府及非政府機關，尤其是非政府機關。因爲買一本書兩百，但是我必須要輸入我的身份證號碼、姓名、出生年月日、手機號碼等等，此時政府應該跳出來要求非政府機關不能這樣做，主要的目的只是要辨認購書人，應該以出生年月日與身份證後四碼便可以確認其身份，存那麼多資料與目的不符。而錄影帶資料的調閱對資安的影響亦大。結論的補貼建議似乎不可行。

薛大勇副處長：

1. 針對金融部份，某家銀行個資嚴重外洩，行政院特函金管會要求有積極作爲。經過多次的會議結果，決議由金管會檢查局於例行檢查時，就受檢銀行個資保護的措施作評鑑。但因涉及資訊專業及工作負荷等因素，僅能部分實施。針對類似情形，公務部門時有所聞，因此建議能透過立法或行政程序給予規範。也就是立法與行政妥善配置，使立法支援行政作爲。

2. 不贊成採用補助，不患寡而患不均，標章制度的建立。個人認爲應該著重如何強化資安的環境與立法，引導業者往此方向去走，有了良好的環境與法律規範，自然水到渠成。
3. 金管會曾經討論自然人憑證作線上簽核，在尚未正式推動前，即有部分單位反應不適宜，提出類似離職員工如何處理自然人憑證及私人憑證爲何用於公務？又如自然人憑證作線上簽核的安全機制是否足夠？因此建議本報告應從建制環境與機制出發，而不是往補助的方向走。

張紹斌主任：

1. 建議作爲：
   (1) 針對特定行業，其目的事業主管機關要制訂更詳盡的保護規範，但不一定是網路業或電子環境，購物台不一定是網路。實例上購物網站過半小時候就有電話，源源不絕的資料外洩。
   (2) 補貼等同於丟錢到水池裡。因此建議主管機關建立比較嚴格的作業流程(SOP)，違反者即予處罰。如果沒有特定目的事業主管機關，請研考會研究指定主管機關。
   (3) 針對特定行業的資料大量外洩，給予目的事業主管機關有警告的權限或內部通報制度，或各資安委員會作跨部會協調，以免資源分配不均。

郭瑞蘭處長：

1. 參酌外國立法例，以後個資法應該是一基本法，再就個別行業屬性或特性做個別化的處理。本報告在法制面就個資法修正的建議，蒐集、處理原則上應有當事人書面同意，利用需要再同意，其可操作性值得研究。公共利益大於個人隱私利益時應如何權衡？
2. 蒐集、利用原係分別規定，現在把利用的法條合併到蒐集中，蒐集的「對緊急度不如利用時的緊急，操作的面向不同。另第 15 條修正條文當事人權益僅造成極微小的影響」，屬於不確定的法律概念，建議

再考量。

3. 針對錯別字請更正，例如職掌（V）執掌（X）P.170 錯字（已）
4. 對於第三章，第七章結論的前面建議要融入第三章。
5. 第四章第二節第一項二、建議將「本案所涉及之爭點」修正爲「基測個資外洩案」；同節第四項將「本案評析」修爲「案例分析」。

戴純眉小姐：請老師先對專家意見作回應。

余啓民老師：

針對補助的部份，以建制環境爲優先，部份在經濟部範圍內提出建議。

自然人憑證的提出，並提出可能的問題，供長官參考。葉律師的本來應思考的是帳號代碼 token，可避免查驗的東西。

郭瑞蘭處長：資訊保護官(類似機制）設在機關內部的實效性有多大？

余啓民老師：機關與機關間資料互通，可能會踰越原使用目的。

戴豪君主任：可參考政府資訊公開法，政府資訊「得公開」的範圍與裁量基準。

葉奇鑫律師：TOKEN 與自然人憑證的問題均有。

附件五　法源資訊網站裁判新聞彙整（以領域分）

一、金融

1.呆帳大戶 5 千萬現形 銀行法初審草案通過[360]

去年間發生某集團負責人潛逃美國，留下在台灣一大筆爛帳，民眾批評銀行保護呆帳大戶的隱私權毫無理由，金管會在輿論壓力下，開始每半年公佈呆帳超過一億元以上的名單。立法院則於昨（二十四）日初審通過銀行法修正草案，規定銀行可公佈呆帳超過五千萬元，或是貸款半年內發生逾期轉帳呆帳超過三千萬元的客戶資料。

此修正案如果通過，呆帳門檻也將從現行的一億元，降爲五千萬元；據了解，去年發生該集團掏空事件之後，就有輿論強烈建議應修正銀行法第４８條規定，主張要公佈三千萬元以上的呆帳大戶名單。當時金管會引用該條第２項規定，銀行對於顧客之存款、放款或匯款等有關資料，「除其他法律或中央主管機關另有規定者外」，應保守秘密；要求銀行揭露呆帳大戶。

金管會表示，依行政院金融監督管理委員會９６年３月３日金管銀（一）字第０９６１０００８６０號釋示，各銀行對每一客戶轉銷呆帳金額達新台幣一億元以上之呆帳資料，不在該法第４８條第２項保密義務之範圍，並應依同法第４９條第２項規定揭露；金管會進一步指出，在經過研擬之後，決定門檻降爲五千萬元。此外，在昨日的初審也通過銀行資本適足率或淨值占資產總額比率低於百分之二，在限期內未改善，必須退出市場，由主管機關派人接管。

但根據媒體的報導，由於部分立委本身就是呆帳大戶，因此有金融業者表示，在三讀以前到底會不會變化，銀行界也在觀察。參考金管會先前公佈的資料，近十多年來累積上一億元以上的呆帳至少有將近五百筆，尤其以房地產界爲大宗。在公佈了資料之後，不少呆帳大戶如今避居海外，或是重新掛招牌等等。

[360] 銀行法第 48-49 條・提供不良債權資料涉及銀行法第四十八條之保密問題第 1-3 條 ・釋 字第 293 號 ・96 年 重上 字第 417 號 ・96 年 重上 字第 428 號・金管銀（一）字第 09610000860 號 ・農金 字第 0965070566 號 ・首波呆帳大戶名單公布 26 銀行初估逾千億法源編輯室 / 2008-11-25

2.500 萬筆財稅個資疑似外洩 財部：個人 P2P 所致[361]

又到了報稅旺季，但根據媒體報導，最近卻驚傳五百萬筆納稅義務人的資料可以透過點對點分享軟體輕鬆瀏覽，今（五）日在立法院財政委員會引起軒然大波。

立委上午在財委會針對個資外洩與網路報稅安全進行質詢，財政部表示，造成個資外洩的問題，全因民眾使用點對點分享軟體，並非從財稅資料中心外洩出去。立委要求財政部三天到七天日內，必須針對未使用點對點分享軟體報稅民眾資料是否外洩，做出專案報告。

依照綜合所得稅電子結算申報作業要點第２點規定，納稅義務人利用網際網路辦理綜合所得稅結算申報及個人所得基本稅額申報，其通行碼有三種。內政部核發之自然人憑證、納稅義務人之「身分證統一編號」加上所得年度十二月三十一日戶口名簿上所載之「戶號」、其他經財政部審核通過之電子憑證。

財政部為了簡化納稅人申報所得稅流程，近年致力推動網路報稅。財政部指出，從五月報稅至今，已有十一萬件使用網路報稅，民眾在使用網路申報前，依上開規定，可申請自然人憑證或是金融機構憑證，若無憑證則可利用簡易網路申報，也就是用身分證統一編號加戶口名簿號碼，其中民眾若使用簡易網路申報，與網路點對點分享軟體時，財稅個資就極容易因為分享而外洩出去，全屬於個人行為所造成，非政府資料外露。

根據電腦處理個人資料保護法第１７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。如果真是財政部的資安機制出現問題導致個人資料外洩，依同法第２７條第１項規定，公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。即使被害人並非財產上的損害，依同條第２項規定，也可以請求慰撫金。

[361] 電腦處理個人資料保護法第 17,27 條 ・電腦處理個人資料保護法之特定目的及個人資料之類別第 1,2 條 ・綜合所得稅電子結算申報作業要點第 1-3 條 ・各類所得資料網際網路申報作業要點第 1-3,5 條 ・稽徵機關於結算申報期間辦理綜合所得稅納稅義務人查詢課稅年度所得資料作業要點第 6,7 條 ・釋 字第 631 號 ・財北國稅資 字第 0950210222 號 ・法律決 字第 0940009245 號 ・法律 字第 0910024855 號 ・個資外洩事件 消保會將與法務部攜手防堵法源編輯室 / 2008-05-05

3.債協無法取得債務人資料 司法院緊急協商[362]

消債條例在兩周就要上路實施，司法院卻接獲銀行公會反映，在前置協商作業中，除財稅資料中心同意銀行查詢個別債務人財產資料外，其他包括聯徵中心、勞健保局、集保公司、郵政總局等與個人所得與資產有關的單位，都不同意銀行可以直接函詢債務人個人資料。

司法院對此相當震驚。司法院表示，將儘快與行政院取得聯繫，促請行政院近期內召開跨部會協調會議。依消費者債務清理條例第１５１條第２項規定，債務人向最大債權銀行請求進行協商債務清償方案時，視同債務人同意或授權銀行，得向財稅等其他機關或團體查詢財產、薪資等個人資料。不過，由於債務前置協商是銀行與債務人間的協議，尚未進入法院的程序，無法適用強制執行法第１９條第２項規定，由法院發函給包括財稅等行政機關調閱個人財產等資料。因此，包括金管會、財政部及勞委會等單位，如果沒有一致的作法，銀行與債務人的協商制度根本無法推動起來。

另參考財政部金融局８５年１０月２２日台融局（一）字第８５２９８５５３號函釋意旨，雖曾有建議放寬銀行法第４８條第２項規定，准許「訴訟中」之債權人得向有關機關查詢債務人之財產，以利求償，但財政部金融局表示訴訟中之債權是否成立並未確定，爲保障相對人之利益，不宜同意其債權人得向有關機關查詢相對人之財產，金融局認爲還是必須等到債權人取得執行名義後，依強制執行法第１９條第２項規定，請求執行法院爲必要之查詢。

司法院表示，對於消債條例施行所需配合的共通事項，行政機關應採取一致的作法，以便銀行在與債務人協商時能夠快速取得債務人個人相關資產、薪資、存款、勞健保及股票等資料，作爲銀行研判是否與債務人達成協商成立的參考依據，避免產生道德風險。因此司法院將緊急與行政院協調促請各相關單位協同辦理，以免債務人與銀行的前置協商作業停擺。

[362] 銀行法第 48,61.1 條 ・消費者債務清理條例第 19,20 條 ・消費者債務清理條例第 151-153 條 ・金管銀（一） 字第 09510002020 號 ・台財融（一）字第 0918010593 號 ・台融局（一）字第 85298553 號 ・臺灣高等法院暨所屬法院 95 年法律座談會民執類提案第 5 號 ・卡債族與銀行進行協商 需提出債權人清冊法源編輯室 / 2008-03-28

4.財產申報司法官被跟蹤 法部：個資已遮蓋[363]

標　　題：有關公職人員財產申報資料查閱相關新聞澄清說明
新聞出處：法務部

有關本（９７）年１月１３日媒體報導司法官疑似被不名人士跟蹤，且其財產申報資料曾有不同民眾查閱乙節，經本部政風司清查結果，各政風單位目前均未曾接獲反映司法人員遭跟蹤之情事，另依現行公職人員財產申報資料審核及查閱辦法第１２條規定，各受理申報單位於接受民眾申請查閱公職人員財產申報資料時，得不提供申報人之年籍、土地地號、房屋建號等個人資料。故目前本部所屬各政風單位於受理民眾查閱時，均已將申報人之身分證字號、門牌號碼、車牌號碼，予以遮蓋，避免影響申報人之個人隱私及人身安全。

[363] 政府資訊公開法第 7,8,18 條 ・公職人員財產申報法第 2,5-7 條 ・公職人員財產申報資料審核及查閱辦法第 2,12 條 ・法務部公職人員財產申報案件處罰鍰額度基準第 1,2 條 ・法政 字第 0950046988 號 ・金管銀（一） 字第 09510002020 號 ・公職人員財產申報法遲未施行 法務部說明/ 2008-01-17

5.現金卡個資外洩詐欺集團？ 銀行老總喊冤[364]

內政部警政署刑事警察局宣布偵破，銀行客戶現金卡申請書資料外洩，遭詐騙集團冒辦信用卡盜刷案。而被媒體以頭版頭條方式，點名洩漏個人資料的銀行，總經理特別澄清表示，是代辦公司出問題，卻要銀行背黑鍋，相當不公平。

翁姓男子原本在銀行委託的代辦公司任職，涉嫌趁職務之便，影印民眾申辦現金卡的個人資料，再以電子郵件轉賣給大陸詐騙集團，進行網路盜刷。由於申請表格上姓名、身分證字號、電話、職業等資料相當詳盡，還附上有申請人身分證正反面影本，以及附給銀行的財力證明、薪資扣繳憑單，讓詐騙集團很輕易地就能冒名向十多家銀行申辦信用卡。刑事局偵九隊前（二十）日將翁某逮捕。

法界人士表示，姓名、出生年月日、身分證統一編號等個人資料，依據電腦處理個人資料保護法第２３條本文規定，非公務機關利用時，應於蒐集的特定目的必要範圍內爲之。若因違反規定，致當事人權益受有損害，依同法第２８條第１項本文規定應負損害賠償責任。依同條第２項適用同法第２７條第３項規定，每人每一事件最高可獲賠新台幣十萬元。

此外，根據銀行法第４５條之１第１項規定，各銀行均應建立適當有效的內部控制制度。參照金融機構辦理現金卡業務應注意事項第２１點第１項規定，若金融機構辦理行銷涉及個人資料外洩等非法行爲，經查證屬實者，主管機關得視情節輕重，依相關規定予以處罰，必要時，得暫停或停止辦理現金卡業務。

[364] 銀行法第 45.1,48,61.1,129 條 ・電腦處理個人資料保護法第 2,3,23,27,28 條 ・銀行內部控制及稽核制度實施辦法第 17,30,31 條 ・金融機構辦理現金卡業務應注意事項第 4,19-21 條 ・電腦處理個人資料保護法之特定目的及個人資料之類別第 1,2 條 ・臺灣高等法院暨所屬法院八十六年法律座談會民事類提案第二十四號 ・銀行現金卡個資外洩詐欺集團 刑事局破獲

6.銀行現金卡個資外洩詐欺集團 刑事局破獲[365]

標　　題：偵破某大銀行客戶現金卡申請書資料外洩，遭詐欺集團冒辦信用卡盜刷案

新聞出處：內政部警政署刑事警察局

（一）刑事警察局偵九隊於網路巡邏時發現使用雅虎奇摩帳號 my68my78 者，在「光華螞蟻市場」網站刊登大量訊息「高收課本。紅綠本買賣～預付卡買賣～轉接～來信留聯絡方式 my68my78@yahoo.com.tw」、「出售奇摩拍賣帳號～要什麼評價的都有！可長期配合！！請來信 my68my78@yahoo.com.tw」，另以帳號 my68my78 於網路上清查後發現，該帳號使用人並於「跳蚤市場」網站有「高收課本紅綠本買賣，電話卡買賣，轉接來信留聯絡方式 my68my78@yahoo.com.tw」等訊息，研判該帳號使用者乃是詐騙集團份子，於網路上張貼上述訊息收購人頭金融帳戶後再使用於犯罪行爲上以逃避警方追緝，影響社會治安甚鉅，刑事警察局偵九隊獲線後，即向局長黃茂穗報告，黃局長獲報後極爲重視，指示偵九隊全力偵辦，刑事警察真九隊即與台北市政府警察局信義分局偵查隊共組專案小組積極偵辦。

（二）經專案小組追查相關資料，清查出涉案人乃居住於汐止市伯爵山莊內之翁〇欽涉有重嫌，經向臺灣士林地方法院聲請搜索票，前往該嫌出入之特定地點，查扣信用卡卡號資料、民眾現金卡申請人資料、各家銀行信用貸款民眾申請資料等乙批、作案用手機等相關贓證物，其中現金卡申請人資料除了申請表格填有申請人基本姓名、身分證字號、本身持有電話、職業、公司資料外並有申請人聯絡人電話，更誇張的連申請人身分證正、反面影本，及附給該家銀行申請人爲證明財力持有的它家銀行信用卡正、反面影本資料及薪資扣繳憑單也一併被翁嫌以電子郵件寄給藏匿在大陸的信用卡盜刷集團因而外洩，經刑事警察局偵九隊向聯合信用卡中心查詢後，初步得知已有被害人資料被冒用申請別家銀行信用卡因而被盜刷成功；另從翁嫌電腦中清查出來的信用卡資料，發卡銀行分別有中信銀、花旗、荷蘭、國泰世華、玉山、慶豐、遠東、

[365] 銀行法第 48,61.1 條 ・中華民國刑法第 210,216,317.318.1.339 條 ・電腦處理個人資料保護法第 28,34 條 ・釋 字第 293 號 ・金管銀 (一) 字第 0938011278 號 ・台財融 (四) 字第 0924001326 號 ・法律 字第 0910044369 號 ・洩漏第一家庭無限卡資料 銀行挨罰 200 萬/ 2007-11-21

兆豐、台北富邦、聯邦、萬泰、新光、匯豐、華南、台灣銀行、中華、土銀、上海等１０幾家銀行，其中已有數十張卡有被盜刷紀錄，全案依詐欺、僞造文書、電腦及處理個人資料保護法、妨害秘密等罪嫌移送臺灣士林地方法院檢察署偵辦。

（三）專案小組正清查該家銀行內部控管機制是否出現問題及相關業務承辦人員，有無勾結信用卡盜刷集團，導致客戶資料被委外的現金卡代辦公司外洩販賣給在大陸之信用卡盜刷集團，使客戶權利嚴重受損。爲杜絕個人資料外洩、人頭戶氾濫警方請大家不要隨便填寫個人資料調查表給他人；另特別呼籲銀行及信用卡中心應嚴格控管個人原始申請基本資料，因該申請資料有申請人詳細申請資料，一經外洩遭詐欺集團利用可能造成民眾重大損失。

7.遏止網路釣魚 金管會提供金融業網站資料[366]

標　　題：金管會提供我國所有金融事業網站網址資料
新聞出處：行政院金融監督管理委員會

鑒於金融網路運用日益蓬勃發展，各金融服務事業所提供之商品及服務透過網際網路提供者愈形普及，為便於社會大眾瀏覽金融相關網站，同時為遏阻「網路釣魚」或「虛設網站」誘騙民眾誤上假網站，騙取個人資料或誤信假消息，增加金融網路業務風險，行政院金融監督管理委員會已於本（９６）年１１月９日大幅增列及調整該會全球資訊網站首頁週邊單位內容，將週邊單位區分為「相關政府機關」、「銀行」、「證券期貨」、「保險」、「檢查」、「外國相關監理單位及交易所」及「國際組織」等７大類，並呼籲民眾直接點選金管會網站（ｈｔｔｐ：／／ｗｗｗ．ｆｓｃｅｙ．ｇｏｖ．ｔｗ／），以連結各類金融機構網址，俾確保相關金融業者網址之正確性及安全性，期望各界善加利用。

[366] 網際網路等電子式交易型態交易資料保存規範第 1-2 條 ‧證券商採網際網路等電子式交易型態交易所使用之交易主機應具備之相關受託買賣有價證券檢查點控制項目第 1 條 ‧財政部國有財產局個人電腦及網路管理規範第 2,4,5,6,7,9 條 ‧防範歹徒猜中網路銀行客戶密碼之安全控管措施第 2-5 條 ‧台證交 字第 0930026521 號 ‧全新買空賣空詐騙手法 盜奇摩帳號五百個/ 2007-11-19

8.網路銀行帳戶遭盜領 140 萬 銀行拒絕賠付[367]

網路金融詐騙猖獗，一位林姓男子二月間開啓網路銀行帳戶，出國幾天卻遭盜轉新台幣一百四十萬餘元。不過，銀行認爲沒疏失，拒絕理賠。警方指出，歹徒的手法日新月異，從「懶人密碼」到植入「木馬程式」不斷演變，民眾使用網銀更要小心謹慎。

受害的林先生說，他開設的網路帳戶，於二月十六日到十九日出國期間，歹徒利用ＯＴＰ非約定轉帳機制，四天內盜轉十六筆共一百四十萬三千八百元；他認爲銀行疏失，血汗錢平白無故受損。但該家銀行表示，網路銀行帳戶需三道認證機制，交易時也需要進一步確認，設計上沒有問題，由於此案件已進入司法程序，不認爲有必要先理賠給消費者。

面對這種情況，行政院金融監督管理委員會銀行局官員指出，根據個人網路銀行業務服務定型化契約範本第１３條第３項規定，除非銀行證實客戶故意或過失，否則應先賠付，再報請檢調和警察單位調查處理，釐清責任。不過，銀行表示，如果可以確定林先生的損失是因爲機制錯誤，或被植入木馬程式而遭盜領，他們會負起責任，但也有可能是客戶沒盡到保守帳號、密碼等資料的責任，則不在賠償之列。

刑事警察局科技犯罪防治中心表示，最近共有四十多位受害者報案，遭盜取金額逾千萬元，根據調查，確實有駭客組成犯罪集團破解網路帳戶機制，但嫌犯是在大陸遙控犯案，除非他們回台灣，否則很難逮捕。警方提醒民眾，使用網路銀行要謹慎小心，除了要常更換密碼，上網時也應注意不明「釣魚」網站，當心洩漏個人資料，或被植入木馬程式，若有疑慮，可以上刑事局網站下載最新的防堵軟體。

爲防範民眾的網路銀行密碼被歹徒猜中，致權益受損，參照防範歹徒猜中網路銀行客戶密碼之安全控管措施第４點第１款規定，網路銀行「用戶代號」不得少於六位，若以身分證字號或帳號作爲識別，則應另行增設「使用者代號」以資識別；至於網銀「密碼」，依同點第２款規定，建議採英數字混合使用，宜包含大小寫英文字母或符號，不得訂爲相同的英數字或連號，且不得少於六位（若搭配交易密碼使用則不應少於四位）。

[367] 銀行法第 42.1,125.3 條 ・防杜人頭帳戶範本第 1,2 條 ・個人網路銀行業務服務定型化契約範本第 1 條 ・防範歹徒猜中網路銀行客戶密碼之安全控管措施第 3,4 條 ・台財融（一）字第 0911000105 號 ・台融局（一）字第 0090723995 號 ・電話語音、網路銀行約定轉帳 隔日才生效法源編輯室 / 2007-04-30

9.1500 戶逾億元呆帳大戶 金管會：3/15 公布[368]

基於社會公益考量，行政院金融監督管理委員會將依銀行法第４８條第２項授權規定以及銀行法第４９條規定，對於轉銷呆帳客戶資料予以適度公開。金管會表示，將採歸戶方式，公布門檻爲新台幣一億元以上轉銷呆帳名單，約有一千五百戶符合公布條件。爲即時揭露資料，銀行應在今年三月十五日前，先在銀行網站專區揭露截至二○○六年六月底的呆帳轉銷資料。

金管會說，銀行對客戶資料保密是銀行客戶基本權利，銀行就客戶各種業務往來關係所知悉或持有一切資料，均屬客戶隱私權範圍，銀行如隨意公開客戶資料，不但將失去客戶信賴，且將影響其業務經營，進而不利整體金融市場穩定與發展。

不過，因偶有特殊政商關係及企業集團進行利益輸送，導致銀行授信產生呆帳之情形，甚至動用國家大量資金處理該等授信呆帳，鑒於該等案件社會公益及社會成本已經大於客戶隱私權保護之考量下，有重新考慮請各銀行適度公開轉銷呆帳客戶資料之必要。

金管會並針對財政部８２年１２月３１日台財融字第８２１１６３１４號函釋提出說明，金管會指出，該函釋之意旨係銀行得提供呆帳客戶資料予依法有調查權之機關，但該查詢機關仍負有保密義務，故其僅爲保密責任之移轉，並非解除銀行之呆帳資料保密義務。該函並未明確表達上開意旨，且亦未就呆帳資料解密後銀行應如何處理予以規範，故確須重新調整並進一步規劃解密後呆帳資料的完整揭露程序。

至於揭露作法方面，金管會表示，參酌立法院財政委員會通過之銀行法第４８條修正條文草案將轉銷呆帳之解密門檻訂爲三千萬元，惟基於修法前僅能以法律授權規定發布，應採較高門檻，且將採歸戶方式爲計算基準，故提高公布門檻爲一億元以上，並依據銀行法第４９條規定，各該銀行須在每年四月底前將截至前一年底之上開資料在其網站專區揭露，揭露內容包括借戶戶名、隱藏後四碼之身分證字號或統一編號及呆帳轉銷餘額。

[368] 銀行法第 48,49,125.2,125.3,127.1 條 ・銀行業辦理外匯業務管理辦法第 5 條 ・釋字第 293 號 ・台財融 字第 82116314 號 ・台融局（六）字第 89498141 號 ・金融機構已轉銷呆帳戶之資料是否爲銀行法第四十八條第二項保密義務之範圍 ・「銀行法」第 48 條條文修正草案・金融史上首例 接管銀行呆帳大戶名單公布法源編輯室 / 2007-03-02

10.力霸風暴 政院著手修法公布呆帳大戶名單[369]

力霸風暴引發連串金融危機，陳水扁總統昨（十）日隔海指示修法，公布「呆帳大戶」。行政院金融監督管理委員會表示，依據總統指示，政院將檢討修正銀行法，在不侵犯隱私權原則下，針對那些呆帳過高，或可能故意搬運金錢者，若達到一定金額以上者，公布其名單。

總統率團訪問尼加拉瓜，在與隨行媒體茶敘時針對力霸重整引發中華銀擠兌風暴發表談話指出，台灣發生這種銀行掏空、呆帳問題，到最後好像都沒事，好像都是政府在負責，人民在埋單，所以，他一直要求應該要公布這些掏空、呆帳的銀行大戶名單，但行政部門一直以所謂法律規定指絕對不可以公布這些呆帳大戶名單，希望能由民進黨立法院黨團提案修法，讓法律沒有障礙。

金管會表示，依銀行法第４８條第２項規定，銀行不能把存款人與客戶往來匯款資料公布，應保守秘密，對於是否要公布一般正常銀行呆帳大戶名單，立法院曾有不同意見、修法與建議；審查中的銀行法第４８條條文修正案確有適度調整必要，在不侵犯隱私權情況下，對貸放金額壞帳過高，有不法的貸放，或內部人交易搬運金錢的貸款，應可訂出一定金額以上可以公告。至於已被接管的銀行，依行政院金融重建基金設置及管理條例第１１條第１項規定，在中央存保介入清理過程中，例如花企、東企，或中華銀行，若有呆帳逾新台幣一百萬元，名單均會公布。

立委表示，已就銀行法第４８條第２項規定兩度提出修正草案，要求公布金融機構轉銷呆帳金額達一千萬元以上的大戶名單，朝野協商後確定將公布的門檻提高爲轉銷呆帳三千萬元以上，以及自貸放後一年內即轉爲呆帳且金額在一千萬元以上的惡性呆帳戶。由於該案已可逕付二讀，希望能讓該案排在這幾天的院會討論案前幾案趕快過關。

[369] 銀行法第 48,49 條 ・行政院金融重建基金設置及管理條例第 10,11 條 ・行政院金融重建基金處理經營不善金融機構作業辦法第 5,6 條 ・銀行資產評估損失準備提列及逾期放款催收款呆帳處理辦法第 7,9,11 條 ・「銀行法」第 48 條條文修正草案・保密條款翻修 惡意呆帳銀行將可公佈姓名・上市公司重整風波 金管會決議重罰 240 萬法源編輯室 / 2007-01-11

二、電信

1.行動電話個人資料安全 消保會將嚴格把關[370]

標　　題：個人資料安全 免驚～～行動電信門號申辦嚴格把關！
新聞出處：行政院消費者保護委員會

行政院消費者保護委員會（以下簡稱行政院消保會）日前接獲民眾申訴其身分資料遭冒用申辦行動電信預付卡門號，甚至因此被警方列爲犯罪嫌疑人，建議加強對電信業門號申辦者身分資料查證及把關責任云云。行政院消保會遂於９６年１２月４日上午邀集主管機關國家通訊傳播委員會（以下簡稱通傳會）、內政部警政署（以下簡稱警政署）、中華電信公司等九家電信業者及全虹、震旦等電信通路業者召開會議，除確認各電信業者因應可攜式門號規劃之「來電答鈴」識別語音均已建置完成外，並請各電信業者對消費者因常接到舊用戶親友來電造成困擾之情形，免費更換其他門號之服務。對冒用身分資料申辦行動電信門號部分，則請業者對所屬經銷商（加盟店）應定期及不定期查察是否落實申辦者須以本人雙證件正本辦理行動電話門號之申裝業務，如發現未依規定辦理者，應立即終止合約。

隨著行動電話攜碼服務用戶日益增加，手機門號網內網外告知機制，對消費者的權益已愈形重要。行政院消保會於本（９６）年８月間與主管機關國家通訊傳播委員會（以下簡稱通傳會）及中華電信公司等電信業者召開之會議，除請各電信業者應落實手機簡碼「５７０１６」（網內門號查詢語音服務專線）專線服務功能，即消費者只要撥打「５７０１６」輸入欲查詢之門號，即可獲知屬於何家電信業之門號外，並促請各電信業者應就可攜式門號規劃以「來電答鈴」語音提供識別之機制，以保障發話端（付費者）權益。是項答鈴告知機制各電信業者均表示已建置完成，日後除搭配優惠方案提供攜碼服務之新用戶免費試用一個月，協助其發話端（付費者）親友辨識所撥號碼爲網內或網外；消費者亦可視個別需求選擇是否繼續租用。

有關行動電信門號申辦作業規定，各電信業者表示對所屬合約經銷商（加盟店）之門市均會進行經常性定期及不定期之查察，或委託外聘公司進行私下查訪，了解有無落實申辦者證件審核工作，行政院消保會已要求渠等將本（９６）年度１至１１月份查核資料送該會以作爲督導考核之參考。另有關消費

[370] 中華民國刑法第 210,212,216,217 條 ・行動通信業務管理規則第 35,72-74 條 ・行動通信業務管理規則第 76,77 條 ・行動電話業務營業規章範本第 1 條 ・院解 字第 3915 號 ・70 年 台上 字第 1107 號 ・95 年 訴 字第 1490 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 4 號 ・個人資料外洩引發詐騙 法務部：修法重懲/ 2007-12-18

者反映因手機門號經常接到舊用戶親友之來電者，各電信業者亦允諾提供免費更換其他門號之服務，以協助消費者解除困擾。
至於冒用身分申裝行動電信門號之把關，行政院消保會除促請通傳會與警政署持續辦理有關僞冒或變造身分證件之辨識技巧與教育訓練外，並以中華電信公司提供之案例：「所屬某直營門市業務人員發現冒用身分資料之申辦人時，除當場拒絕其申辦作業外，並即時通報公司，經由內部通報機制轉知所屬各地門市，而成功阻擋該名人士轉至其他門市據點申辦，並報警逮捕在案。」，請各電信業者對落實審核資料及驗證工作，從而阻卻不法情事之有功同仁，予以適當之獎勵。
另爲期許各電信業者之查獲資料能資源共享，發揮更大功效，行政院消保會並促請通傳會積極研議建立整合各電信業者查獲冒用申裝資料之通報查詢系統的可行性。

三、就醫

1.稽查診所未事先通知 衛生局要賠醫師 39 萬[371]

台北市政府衛生局三年前無預警，跑到血管外科醫師的診所稽查病歷，引起該醫師不滿，認爲衛生局侵害他的名譽、隱私權，流失病患，訴請國家賠償一百八十餘萬元。臺北地方法院審理後認爲，北市衛生局違反程序，稽查前未依法先通知診所，判決須賠償該醫師的的精神和營業損失共三十九萬元。該醫師所開立的診所，因未在一名曾姓病患的病歷上簽章，北市衛生局在民國九十四年六月八日作成行政處分，要求同年月二十日前改善完畢。北市府衛生局爲了稽查該醫師有否改善，就在處分書上限定完成改善的隔日，指派稽查員前往稽查。該醫師認爲稽查員沒有出具有權檢查的公函，以及執行職務的證明文件，顯然稽查不當，造成營業損失和名譽侵害，請求衛生局國家賠償一百八十七萬多元。

衛生局則主張，稽查員至診所稽查時，是進行「制裁證據調查」，不必事先通知，查核時只要出示身分證明文件即可。不過，法官認爲依照醫療法第２６條規定，醫療機構應依法令規定或「依主管機關的通知」，提出報告，並接受主管機關對其診療紀錄等的檢查及資料蒐集。所以，衛生局稽查前要先行通知，而衛生局無法證明有事先通知。且醫療法施行細則第１４條規定，主管機關依醫療法第２６條規定執行檢查及資料蒐集時，其檢查及資料蒐集人員，應出示有關執行職務的證明文件或顯示足資辨別之標誌。

而且行政檢查侵害受檢人權利，和檢警的搜索、臨檢相當，應遵守比例原則，衛生局主張稽查無須事先通知，只要稽查員出示身分證明即可的說法，不足採信，最後認定稽查員未事先通知已超過必要程度，對於該醫師看診造成干擾，其職業權尊嚴受損，可獲賠償三十萬元。至於登報道歉部份，法官認爲無此必要，駁回該醫師的請求。

[371] 醫師法第 12,29 條 ・醫療法第 26,67,68,102 條 ・醫療法施行細則第 14,49,53 條 ・96 年 簡 字第 135 號 ・衛署醫 字第 0960046106 號 ・衛署醫 字第 0930220492 號 ・衛署醫 字第 85000844 號 ・看婦科卻皮膚潰爛 病患控知名醫師賠百萬・臺灣臺北地方法院有關「稽查診所未事先通知 衛生局要賠醫師 39 萬」民事判決一則 法源編輯室 / 2008-06-24

2.捐血試驗是否感染愛滋 衛署：已觸犯刑責[372]

標　　題：有危險行爲者，捐血觸法
新聞出處：行政院衛生署疾病管制局

於１２月２７日完成愛滋病毒基因序列比對，證實發現今（９６）年第一起捐血者輸血感染愛滋病毒案例。該局再次鄭重呼籲民眾，目前全台灣有十家匿名篩檢醫院提供免費服務，愛滋病毒感染初期，約有６－１２週的空窗期，故切勿以捐血方式檢驗自身是否感染愛滋病毒，以免造成於愛滋病毒感染之空窗期捐血因而危害受血者感染之憾事。

該局追蹤上述感染愛滋病毒之捐血者，僅於９６年１１月由捐血中心通報，經疫調發現其感染的危險因子爲男性間行爲，該名患者共有６次捐血行爲，近期內捐血日期分別爲：９６年１１月（發現感染愛滋病毒）血品已棄未使用、９６年7月、９６年３月，衛生局人員已回溯追蹤當時之受血者，其中９６年７月之受血者，計３名，１名於１２月初因疾病死亡，２名存活者確定感染愛滋病毒，且經過病毒基因序列比對，已證實確由輸用該名感染者９６年７月所捐之空窗期血液導致感染；另９６年３月之２名受血者均因病死亡，依愛滋病毒空窗期推估，個案９１年更早期捐血之血品應無感染之虞。累積至今國內發生輸血感染愛滋病毒之個案共１８例。

依據台灣血液基金會現行捐血作業程序上對於捐血民眾均有提醒感染愛滋病、感染性病、或曾有危險性行爲、靜脈注射藥癮者、曾有吸毒、慢性酒精中毒者、同性戀或雙性戀者等請勿捐血，並由捐血民眾簽名具結。該名感染愛滋病毒捐血者明知自己符合不宜捐血的條件仍逕行簽名且進行捐血，將涉及違反人類免疫缺乏病毒傳染防治及感染者權益保障條例第二十一條「明知自己爲感染者…而供血或以器官、組織、體液或細胞提供移植或他人使用，致傳染於人者，處五年以上十二年以下有期徒刑…未遂犯罰之」之嫌，此外，造成受血人感染，捐血者必須自負相關民事損害賠償及刑事傷害罪之責任。

台灣血液基金會爲對因輸血感染案例提供道義救濟，８３年即通過輸血感染愛滋病毒道義救濟要點，當有因輸血感染愛滋病毒之確定案例時，則提供新台幣２００萬元之救濟金，衛生署疾病管制局將協助本案受血感染者向台灣血液基金會申請相關道義救濟事宜。

---

[372] 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 11,12,23 條 ・血液製劑條例第 3,5,7,10,16 條 ・血液製劑條例施行細則第 2,5,8 條 ・捐血者健康標準（95.03.15 訂定）第 2-5 條 ・95 年 上易 字第 1012 號 ・署授疾 字第 0950000230 號・衛署防 字第 88027849 號
・越南妹賣春 雲林愛滋患倍增？衛生局澄清/ 2007-12-28

爲減少上述案例一再發生，衛生署疾病管制局均不定期實地前往各捐血站進行查訪，期整個捐血程序能充分提供諮商與告知之機會，盡全力預防有危險行爲者捐血，該局再次沈痛且鄭重呼籲民眾，誠實面對自己，如有不安全性行爲、感染性病、或是有靜脈注射藥癮，可能正處於感染愛滋病毒之空窗期者，均不宜捐血，以免危害用血人安全；也千萬不要利用捐血做愛滋病毒之篩檢，而危及用血者的安全。另外該局委託１０家醫院（如附件）接受免費匿名篩檢服務，這些醫院及單位均會提供正確快速的檢驗且顧及個人隱私，並提供必要之諮詢與服務，民眾切勿利用捐血來達成檢驗目的，卻遺禍他人。目前提供免費匿名篩檢及諮商服務的醫院有台大醫院、台北榮總、台北市立聯合醫院疾病管制區、衛生署桃園醫院、台中榮總、中國醫藥大學附設醫院、成大醫院、高雄榮總、高醫附設中和紀念醫院、慈濟醫院等１０家醫院，民眾可就近利用，其他縣市民眾亦可赴當地衛生局所接受篩檢，或利用全省免付費的諮詢專線１９２２查詢相關資訊。此外，如果捐血者對於自身血液安全有疑慮，不希望影響他人健康，也可以利用「良心回電」方式，即時告知捐血中心，以避免不幸的事件再度發生。

3.人體受試爲藥害事前預防研究 與建檔無涉[373]

標　　題：推動藥害事前預防相關研究，絕非媒體報導與全民基因檢測建檔有關

新聞出處：行政院衛生署

衛生署爲促進國人健康，提昇用藥安全，將我國執行成果完善的藥害救濟制度，進一步藉由藥害基因研究相關計畫之推動，將藥害救濟由事後的救濟，脫胎換骨，邁向「事前預防」，可使我國成爲全世界第一個進行藥害預防的國家，同時開啓我國個人化醫療的先端。此類研究係針對台灣好發藥害之藥物使用對象，探討相關基因與藥物使用導致藥害，及藥物不良反應發生之風險性評估，絕非與所謂建立全民基因檢測建檔有關。

我國的藥害救濟制度自８８年施行以來，共完成６２３件藥害救濟申請案之審議，其中給予救濟之案例數共２６６件。統計顯示以因使用抗痙攣類藥物（如：carbamazepine、phenytoin）、降尿酸類藥物（如：allopurinol）及抗結核類藥物（如：rifampin、isoniazid 及 pyrazinamide）等導致不良反應者爲最多，所發生之嚴重不良反應則以皮膚及皮下組織病變（如：史蒂文生氏- 強生症候群；ＳＪＳ、毒性表皮壞死溶解症及多型性紅斑；ＴＥＮ）爲最多。臨床上因ＳＪＳ／ＴＥＮ可導致大範圍的皮膚脫落及更高的死亡率而被視爲極嚴重的藥物不良反應。近年來世界各國研究陸續發現藥害與藥物不良反應的產生應與族群及其特定基因序列具有相關性。且根據已發表於國際學術研究期刊「自然」，對於臺灣地區病患服用 carbamazepine 引發ＳＪＳ／ＴＥＮ的回溯性研究結果，顯示當病患帶有ＨＬＡ- Ｂ＊１５０２特定基因時，服用 carbamazepine 引發ＳＪＳ／ＴＥＮ之嚴重藥物不良反應之風險較未帶有此特定基因之病患爲高。衛生署業於９６年９月１９日公告含 carbamazepine 成份藥品仿單須加刊「從回溯性研究報告得知，臺灣病患使用 carbamazepine 引起ＳＪＳ／ＴＥＮ之嚴重藥物不良反應與具ＨＬＡ- Ｂ＊１５０２基因型在統計學上有高度相關性（Ｏｄｄｓ Ｒａｔｉｏ：１３５７；９５％ Ｃ．Ｉ．：１９３- ８８３８）」研究結果顯示帶有ＨＬＡ- Ｂ＊１５０２基因的病人，服用 carbamazepine 發生 SJS/TEN 的風險較未帶有此基因的病人至少高出１９３倍，而臺灣約有５％的民眾帶有ＨＬＡ- Ｂ＊１５０２基因」等注意事項，以提供臨床醫師爲病患處方該藥品時之參考。

[373] 藥害救濟法第 1,3-5,9,12 條 ・藥害救濟申請辦法第 1-4 條 ・藥害救濟給付標準第 3-5 條 ・96 年 判 字第 894 號 ・94 年 訴 字第 1296 號 ・衛署藥 字第 89037926 號 ・衛署藥 字第 0910054159 號 ・衛生署擬課業者國民營養捐 實質變相加稅/ 2007-12-03

衛生署侯署長認爲我國應進行個人化醫療之研究，並讓藥害救濟由事後救濟邁向事前預防，因此衛生署提出「藥害防制計畫」進行藥害基因之前瞻性研究，來評估基因型鑑定的臨床預測效能，是否能有效降低藥害的發生率。藉由此計畫之推動，將使我國藥害救濟體制，由事後的救濟，『脫胎換骨』邁向事前預防，同時開啓我國個人化醫療的先端。此類研究係針對台灣好發藥害之藥物使用對象，且該研究執行前應通過人體試驗倫理委員會（ＩＲＢ）審查，並取得病人之受試者同意書，受試者的人數是有限的，研究之執行亦需符合藥品優良臨床試驗準則（ＧＣＰ），充分保障病人之權益及隱私，並不是進行或與所謂全民基因檢測建檔有關。

4.結核病人資料外漏 疾管局已進行緊急處理[374]

疾病管制局在今日晚間八時五分接獲某報記者通知，可在網路上查詢到該局結核病患名單。
疾管局獲知後立即依據行政院資訊安全相關規定，成立緊急因應小組，迅速查明原因，進行危機處理，管制損害。
經查，本次事件共有９５３名結核病患姓名、居住縣市等個人資料外漏，判斷外漏時間約從１１月９日起迄今一週。出境管制名單可從Ｇｏｏｇｌｅ搜尋引擎，透過已知結核管制病患姓名搜尋，所幸必須已知結核病患姓名，否則無法搜尋到資料，判斷資料尚未廣泛流傳。
經初步了解，係因系統設計出現瑕疵，致具系統權限者於使用查詢功能時，遭Ｇｏｏｇｌｅ擷取造成。是否有駭客或植入木馬程式所造成，仍待查明。
該局晚間八時四十五分已緊急將該份名單自網路移除，並立即聯繫Ｇｏｏｇｌｅ移除庫存頁面，關閉伺服器進行檢修，尋找外漏的原因。
該局表示：
一、對於部分名單的外漏，向當事人慎重道歉，若有當事人因此權益受損，該局將負起責任。
二、本案屬資安事件，該局已依資安全管理程序，陳報國家資通安全會報通報應變組，目前暫停系統服務，並立即修改程式弱點，將經過完整嚴密測試後才會再度上線。
三、呼籲從此次管道獲得個人資料的任何民眾，都應遵守傳染病防治法及個人隱私保護法之相關規定，不得洩露。

[374] 中華民國刑法第 318,318.1 條 ・傳染病防治法第 10,64 條 ・電腦處理個人資料保護法第 3,7,8,18,23,33,34 條 ・釋 字第 631 號 ・94 年 上訴 字第 2203 號 ・94 年 上易 字第 1237 號
・臺灣高等法院暨所屬法院因應新修正刑法施行座談會提案 第 26 號 ・台財融 字第 86620894 號 ・國防機密花 40 元買到？碎紙再賣 軍機外露/ 2007-11-19

5.衛署生醫資訊整合案 消基會：病患無隱私[375]

行政院衛生署明（三）日將開標一項計畫，計畫名稱爲「生醫資訊整合資料中心規劃案」，該計畫案一旦通過，屆時全台消費者的癌症登記資料庫、戶籍資料庫、健保資料庫及死因檔等，都將彙集整合於資料中心，作爲資料比對之用。中華民國消費者文教基金會表示，衛生署政策明顯涉及消費者的「個人資料隱私權」及「資訊自主控制權」，在未廣泛徵求社會各界意見前，逕行公告規劃方向，簡直是黑箱作業，嚴重損及消費者權益。

消基會表示，以全民健保資料爲例，依中央健康保險局對外提供資料作業要點第５點規定，該等個人資料的蒐集，是爲了健保給付及醫療費用支付之目的，也應僅限於該目的範圍內加以使用，衛生署不應超出該目的範圍以外，提供給研究者或產業界另外加以利用。尤其，全民健保制度之下，民眾給付保費給健保局，全國民眾都是保險契約的消費者；而且由於全民健保是「強制保險」，使得民眾甚至連選擇不投保的機會都沒有。衛生署的政策形同讓民眾在「沒有選擇餘地的情況下」、非志願的將自己的病歷資料全都露且提供給研究者使用，嚴重影響消費者隱私及權益。

消基會指出，不僅是這個「未來」的生醫資訊整合資料中心，可能會侵害民眾的隱私權及個人資訊自主權，事實上衛生署「目前」便已經透過國家衛生研究院，對外提供全民健保資料給各界研究者使用，但是這樣的作法從來沒有經過消費者的同意，更沒有經過任何公聽會或公開討論的程序。依消費者保護法第３０條規定「政府對於消費者保護之立法或行政措施，應徵詢消費者保護團體、相關行業、學者專家之意見。」。

另外，目前國家衛生研究院相關的資訊安全機制，缺乏任何消費者團體或民間團體加以監督，亦沒有經過任何外界的資訊安全專家加以評估，只是由衛生署和國家衛生研究院自認爲「安全」，就逕行將消費者健保資料對外提供使用，其作法極爲不妥，有違反電腦處理個人資料保護法第８條、第１７條之虞。消基會表示，若消費者就醫等隱密資料不幸外洩，簡直是將消費者推向承受詐騙、恐嚇集團騷擾、威脅之際；病患的病歷資料和個人基本資料是個人隱私權中非常重要的一環，有許多的疾病，消費者是不願意讓外界知悉

[375] 電腦處理個人資料保護法第 7,8,17 條 ・國家賠償法第 2,4,10,11 條 ・消費者保護法第 30 條
・中央健康保險局對外提供資料作業要點第 4,5,6,17,27,28 條 ・中央健康保險局提供電腦處理個人資料作業要點第 3,4,5,12 條 ・全民健康保險家庭醫師整合性照護計畫第 5 條 ・法律 字第 0910038370 號 ・病歷電子化推動成效佳 隱私保護倍受重視法源編輯室 / 2007-07-02

的，若因資料外洩，產生對消費者個人、家庭、事業或人際關係上的傷害或損失，責任誰負。

衛生署於「生醫資訊整合資料中心規劃案」的招標說明當中甚至表示，不旦要將民眾的健保資料、戶籍資料、死因檔、癌症登記資料互相連結比對，甚至還要進一步跟目前建置中的「全民電子病歷資料」互相連結比對，令人相當吃驚。消基會認爲，衛生署不旦應停止七月三日招標的「生醫資訊整合資料中心」案，更應該立即停止並檢討現行由國衛院對外逕行提中民眾健保資料的作法，以保障消費者個人隱私權及個人資訊自主權。若衛生署執意通過此案，未來一旦發生資料外洩損及消費者權益，消基會將依電腦處理個人資料保護法第２７條及國家賠償法第２條向衛生署求償。

6.醫學系實習生強制篩檢愛滋 衛生署不同意[376]

日前發生醫學系實習生因感染愛滋遭醫學中心拒絕實習，全國公私立醫學校院院長會議上週行文衛生署疾病管制局，詢問可否針對實習醫師強制篩檢？疾管局開會後實習醫師不是高危險群，強制篩檢恐將違法。另，爲避免拒絕篩檢的實習醫師被貼標籤，也不建議以「知情同意」方式篩檢。
針對實習生或實習醫師強制篩檢的提議，由於涉及敏感人權爭議，及學生受教權保障，疾管局日前邀集專家學者、愛滋防治團體進行討論，最後決議不得要求強制篩檢，也不得要求提出檢驗證明。疾管局建議醫院、醫學院，以委員會或專案小組方式，發現學生、實習醫師感染者時，保護其隱私權，並提供就學權益保障、病情追蹤、病患風險評估等協助，保障醫病權益。
疾管局官員表示,近年來不只一位醫學生因感染愛滋病而在實習之前遇到「困擾」，也曾聽說醫學生被實習醫院拒絕的傳言。據了解，所涉及院校均保密處理，評估實習生的權益與臨床接觸病患的風險後，適度調整課程（如侵入性治療課程僅觀摩不動手等）。官員坦言，的確有部分醫院要求醫學系實習生應提供體檢證明或篩檢報告，但這已違法，不論學校或實習醫院，依法都不得要求進行愛滋篩檢或要學生提出相關檢驗證明。
疾管局強調，根據後天免疫缺乏症候群防治條例第８條第１項規定，當衛生單位接獲報告或發現感染、或疑似感染愛滋，及與感染愛滋病毒者共同生活或有性接觸者，應通知篩檢，逾期未受檢則強制篩檢。疾管局曾以行政院衛生署９３年４月１６日署授疾字第０９３０００３４１號函公告，基於感染風險、國內防疫與國防需要，「應」接受強制愛滋病毒檢查九大類對象，包括性工作者、嫖客、性病感染者、吸毒者、賣毒者、男性間有性行爲者、矯正機關收容人、外籍勞工、現役軍及義務役役男等族群，但不包括醫事人員，「連醫生也沒有全面篩檢」。
官員指出，除被公告須強制篩檢愛滋病毒的對象外，衛生機關不能對一般人強制篩檢。官員強調，台灣醫護人員高達數十萬人，歷年感染者僅三十七人，就比例而言，絕非高危險群，且一旦發現感染愛滋後，可調整爲非侵入性治療的職務，包括放射科、病理解剖及檢查、衛教行政工作，減少感染機率。
此外，與會專家認爲，可預期國內從事醫學相關職業的愛滋感染者「會越來

[376] 中華民國憲法第 8,22,23 條 ・人類免疫缺乏病毒傳染防治及感染者權益保障條例第 8,10,18 條 ・桃園縣管理娼妓自治條例第 6,19,22 條 ・後天免疫缺乏症候群防治條例施行細則第 3,5-7 條 ・各級學校防治後天免疫缺乏症候群處理要點第 4-7 條 ・署授疾 字第 0930000341 號 ・不准「愛滋生」上學？ 教部：校園禁歧視法源編輯室 / 2007-05-18

越多」，建議應比照國外做法，醫院、校合作成立諮詢委員會，協助已知感染的醫學生或醫師，協調出能維護醫病雙方權益的具體臨床操作準則。

7.防亂倫！人工生殖子女結婚前 可先查親等[377]

人工生殖寶寶會不會在不知情的情況，與自己有血緣關係的人結婚？爲避免「近親結婚」等倫理爭議發生，行政院衛生署擬定相關辦法，未來人工生殖寶寶打算結婚時，可以向衛生署國民健康局查證，與結婚對象是否有親屬關係，但不會透露實際父母資料。

人工生殖法於今（九十六）年三月公布實施，國健局根據母法，進一步訂定「人工生殖子女親屬關係查詢辦法」、「精卵捐贈親屬之關係查證辦法」等相關辦法，預計行政院最快可在六月底通過。據統計，從民國八十七年迄今，台灣地區已有二萬多名人工生殖寶寶，專家推估，其中約有一到二成是藉助他人捐贈精、卵孕育的人工生殖子女。爲避免人工生殖子女長大後，面臨民法第９８３條第１項、第１０７３條之１結婚、收養等近親倫理爭議，因此衛生署擬定精卵捐贈、人工生殖子女的關係查詢機制。

國健局表示，需要他人捐贈精卵的不孕夫妻，未來可憑醫院證明，向戶政單位申請自家四等親內戶籍謄本，並交醫療機構核對，避免因近親結合產下先天基因缺陷寶寶。此外，人工生殖子女在結婚前，也可向國健局申請人工生殖子女證明，再向戶政事務所查詢結婚對象是否在六等親內；欲收養人工生殖子女，可先確認是否在八等親內，避免人工生殖子女在不知情狀況下，發生人倫悲劇。

戶政單位會把查好的資料寄給國健局，由國健局比對，再告知申請人，「未」或「有」在親屬表列上發現相符姓名。人工生殖子女不會知道捐精或捐卵者的身分。由於捐贈精卵者資料必須保密，官員強調，若有人刻意要探查特定捐贈者資料，可依電腦處理個人資料保護法、刑法洩密罪等，依法查辦。

至於捐精捐卵的營養費，也有初步共識。儘管人工生殖法第８條第１項第３款明訂屬於無償方式，但衛生署也訂出給予精、卵捐贈者營養、交通與工時損失補助費用上下限。其中，捐精者可以取得一次新台幣四千元至八千元營養費；捐卵過程較爲複雜，需打排卵針且需開刀，因此，捐卵營養費者較高，約有五萬元至十萬元。而爲了杜絕「精牛」出現，國健局將嚴格把關，醫療院所在接理之後，必須立刻上網通報，依同條項第４款規定，一人只能捐贈一次，一旦有活產，依同法第１０條及第２１條第１項第１款規定，剩餘的精子就必須銷毀。

[377] 民法第 968,970,983,1073.1 條 ・人工生殖法第 8-10,21,24 條 ・中華民國刑法第 132,316,318.1 條 ・電腦處理個人資料保護法第 17,34 條 ・人工生殖技術倫理指導綱領第 1,2 條 ・施行人工協助生殖技術醫療機構評核要點第 3,5,6 條 ・人工生殖限不孕夫妻 衛署：有助健全家庭法源編輯室 / 2007-05-11

8.尊重基因產權 馬偕銷毀噶瑪蘭族唾液檢體[378]

馬偕醫院今年一月採集廿九名噶瑪蘭族人的唾液進行族群研究，但事後噶瑪蘭族人認爲違反原住民族基本法第２１條第１項，提出異議。經協商後，馬偕昨天當著族人的面，公開銷毀檢體。這是國內第一起因受試者異議，研究者尊重基因產權放棄檢體，並公開銷毀事件。過去部分研究者常以義診或其他名義，未經同意取得其基因資訊，尤其原住民更是許多研究者眼中寶庫。馬偕事前雖已要求受試者填同意書，但昨天非常低調，表示尊重噶瑪蘭族決定，並允諾今後沒有徵得全族族人同意下，不會再做類似人體採樣實驗。該計畫由馬偕輸血醫學研究室主持人負責，其有「台灣血液之母」之稱，不僅是國際輸血界重要人物，長期從事族群基因、血緣研究，希望了解噶瑪蘭族與阿美族等各原住民族間的關係與起源。

今年一月十一日晚上，噶瑪蘭族頭目召集卅餘名族人開會，宣布隔天馬偕醫院要爲族人採集唾液。十二、十三日連著兩天清晨，新社村鄰長要大家到村子裡的噶瑪蘭風味餐廳接受唾液檢驗，馬偕派四人到場作業，餐廳負責人也接受唾液採集，她說，醫院人員有拿同意書要大家簽名。採集唾液的消息傳開，有人認爲馬偕未完整告知研究目的，被採集者應享權利，被採集者簽下的同意書也被收走，違背研究倫理的公平原則。

有異議的噶瑪蘭族人認爲，馬偕醫院違反原住民族基本法第２１條第１項「政府或私人於原住民族土地內從事學術研究，應諮詢並取得原住民族同意或參與」。向馬偕醫院提出異議之後，雖然表示「我也不曉得怎麼會發生這種事」，但同意立即停止使用，並在族人面前銷毀唾液檢體。

近來基因醫學衍生的隱私問題迭有爭議，去年中研院設置台灣基因體資料庫，引起原民團體關注；最近國科會行文屏東縣牡丹鄉，希望補齊八年前抽血時蒐集資料，但被拒絕，對方要求研究者說明八年前爲何要抽血。未來相關倫理爭議勢必一再出現，研究者應更加審慎行事。

[378] 原住民族基本法第 21 條 ・基因治療人體試驗申請與操作規範第 4 條 ・體細胞治療人體試驗申請與操作規範第 2 條 ・衛署醫 字第 0940218247 號 ・歧視有理？美國管制商業健康保險使用基因資訊之研究・原民第 13 族正名 原民會：民族自治的開始法源編輯室 / 2007-04-02

9.四千筆個資外洩 刑事局逮捕七嫌擴大追查[379]

坊間一些不肖征信社對外廣告宣稱無所不能，警方一直懷疑幕後有個人資料外洩管道。刑事局偵七隊三組會同花蓮縣警方追查，循線在全台各地逮捕七名嫌犯到案。初步清查，這個犯罪集團一年多來非法獲利近億元，包括戶政、勞健保、電話通聯等至少四千多筆個人資料外洩。
花蓮縣警察局於去年六月偵辦電話詐騙集團，循線追查時發覺有不明人士打電話至中華電信公司花蓮營運處南區服務中心，向該服務中心騙取十餘名客戶之姓名、年籍等基本資料，涉嫌提供詐騙集團或國內多家知名徵信社使用，對無辜社會大眾造成巨大危害，由於案情不單純、犯嫌人數眾多、且跨越多縣市，花蓮縣警察局刑警大隊遂與刑事局偵七隊三組共組專案，並報請花蓮地檢署檢察官指揮偵辦。
專案小組深入調查發現，一名綽號「張小姐」的女子係專門接受犯嫌等人之委託，透過管道向相關政府機構人員取得欲查詢之個人電話、戶政、地政、健勞保、醫師名冊、學籍、電腦網路ＩＰ等相關基本資料，並以每筆新臺幣二千五百元至八千元、電話雙向通聯紀錄每月份新臺幣二萬五千元至三萬元不等之代價，售予犯嫌。
從九十四年底至今，已有四千餘筆個人資料遭外洩，初步估計此一犯罪集團已獲利近一億元。犯罪集團中的一名成員覬覦綽號「張小姐」以此方式獲取龐大利益，亦招攬手下等人自組犯罪集團，並勾結任職某電信公司主管人員，將民眾申請電話之個人基本資料，牟利販售給需要之不法歹徒。
本案受害民眾遍及台北、嘉義、屏東等地，警方在鎖定嫌犯行蹤後，在昨（七）日兵分多路前往台北市、台中市、板橋市、嘉義市、屏東縣等地逮獲七名嫌犯，全案於訊後依詐欺、妨害秘密以及違反電腦處理個人資料保護法等罪嫌移送花蓮地檢署偵辦。
根據刑法第３１５條之１規定，無故以電磁紀錄竊錄他人非公開之活動、言論、談話者，處三年以下有期徒刑、拘役或三萬元以下罰金。此外，電腦處理個人資料保護法第３３條規定，意圖營利違反第１８條、第１９條第１項規定，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；另依同法第３５條規定，公務員假借職務上之權力、機會或方法，觸犯本罪者，加重其刑至二分之一。

[379] 中華民國刑法第 315.1,315.2,339 條 ・電腦處理個人資料保護法第 18,19,33,35 條・電信業電腦處理個人資料管理辦法第 1,3,5,8,9,10,11,12,14 條 ・94 年 上易 字第 1237 號 ・台財融 字第 86620894 號 ・應用與相關法制的問題研析－個人資料在商業應用上的界限 ・教召員個人資料全都露 國防部：明年改善法源編輯室 / 2007-03-08

四、就學

1.按指紋管理出缺勤？ 老師：教部侵犯人權[380]

台北縣某所私立國中近日傳出要老師以採納指紋的方式，來取代傳統的簽到簿，好管理老師的出缺勤狀況，校內部分老師拒絕這項計畫並且向媒體投訴，認爲校方這樣的方式不尊重人權也侵犯了隱私權。不過，教育部人事局確拿出了法務部９０年３月２０日（９０）法律字第００５７３４號函釋，認爲學校以指紋管理出缺勤，並沒有違法。

根據該校老師的說法，早在本（十）月初開始，就有老師被拉進學校辦公室內按指紋，且一次要採兩枚指紋，引起老師的反抗，甚至揚言如果要指紋，就去警察局找。而校方也因爲沒有事前說明，就向各老師採納指紋，亦讓老師覺得不被尊重，但因爲部分老師敢怒不敢言，讓上週五爲止，全校上百名老師，已有近二十多位老師配合。

校方則是解釋，用指紋方式做出缺勤管理，純粹是因爲方便，強調這不是侵犯人權，並指出已經和廠商簽約，因此非做不可。而教育部中部辦公室在聽到這樣的消息後，表示會請督學到學校了解狀況，強調一切將依法辦理；學校方面，在昨（二十一）日上午改口，表示可能會等時機成熟後再執行。

不過教育部人事局還是堅持這樣的行爲並沒有違法，甚至指出中央某些部會也是採取這樣的方式管理出缺勤；對於教育部說法，教師會感到憤怒，指出依據司法院大法官釋字第６０３號解釋指出，指紋乃重要之個人資訊，個人對其指紋資訊之自主控制，受資訊隱私權之保障，國家基於特定重大公益之目的而有大規模蒐集、錄存人民指紋、並有建立資料庫儲存之必要者，則應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。

其強調重點在非有必要不得要求人民「按指紋」，此無非爲保障人民資訊隱私權而解釋。採按指紋以爲簽到退登記，是否有違上開解釋意旨，應考慮「按指紋以爲簽到／退登記」是否基於特定重大公益之目的？之手段、方法與欲達成之目的（管理簽到退）是否合乎比例原則？有無其他方式亦可以達成簽到退之管理？又對所蒐集之指紋檔案，有無採取組織上與程序上必要之防護措施？請貴處本於主管機關之權責卓裁，以符憲法保障人民資訊隱私權之本旨。

[380] 中華民國憲法第 22-23 條 ・電腦處理個人資料保護法第 7-11 條 ・釋 字第 603 號 ・釋 字第 599 號 ・(90) 法律 字第 005734 號 ・法律 字第 0920047242 號 ・(無) 字第 （無） 號 ・私採學生指紋辦案？ 校方：單純機會教育法源編輯室 / 2008-10-22

2.教室偷錄音補教老闆涉妨害秘密 檢方起訴[381]

媒體報導，台北縣某補習班負責人涉嫌在教室內裝錄音機，被班上張姓老師搜到後報警，檢方認定補習班教室屬非公開場所，將負責人依妨害秘密罪嫌起訴。

該負責人主張，補教界在教室內裝設監視錄影器非常普遍，礙於經費，她只能不定時在教室內裝錄音機。此舉是爲了保護老師與學生，以免發生突發狀況，事先也已告知張姓老師，沒想到竟然被起訴，真的很冤枉。張姓老師則認爲該負責人是想利用竊錄蒐集對她不利的證據，趁機開除他以節省資遣費。檢察官則認爲教室屬張姓老師專用教室，該名負責人的行爲已經構成妨害秘密，將他起訴。

依照刑法第３１５條之１第２款規定，無故以錄音、照相、錄影或電磁紀錄等竊錄他人非公開之活動、言論、談話或身體隱私部位者，處三年以下有期徒刑、拘役或三萬元以下罰金。本罪最重要的構成要件在於「無故」及「非公開」如果行爲人是爲了保護某一法益如：夫妻一方爲取得他方通姦證據，而侵犯他方隱私時（如竊聽或竊錄私人秘密通訊），依臺灣高等法院花蓮分院８９年上易字第２１３號刑事判決認爲，應認是夫妻一方爲維護婚姻純潔所作出之必要努力，而非屬「無故」妨害他人秘密之行爲。

至於「非公開」的要件，法條固然已明文規定，但依照法務部９０年３月９日法九十檢字第０４６０６６號函之見解，有關他人公開活動時，利用工具窺視或偷拍隱私部位，如果個人客觀上顯然無公開隱私活動，且有合理期待時，對於侵害隱私權行爲，分別得依刑法或社會秩序維護法等相關規定處罰。

[381] 中華民國刑法第 315.1-315.3 條 ‧96 年 易 字第 2878 號 ‧91 年 聲判 字第 7 號 ‧89 年 上易 字第 213 號 ‧法九十檢 字第 046066 號 ‧法務部 (89) 法字第 000805 號 ‧臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 19 號 ‧竊聽捉姦 侵犯隱私非「無故」檢方不起訴法源編輯室 / 2008-10-01

3.私採學生指紋辦案？ 校方：單純機會教育[382]

南部某一所國中的家長向媒體指稱，校園內二年級的某班因爲常常發生學生物品失竊狀況，該班的老師竟然採取學生指紋，這樣不尊重人權的行爲，發生在校園，令他感到相當錯愕及憤怒。而校方則回應，表示老師是藉此機會向學生解釋警察的辦案手法，認爲這是一個很好的機會教育，且學生按捺的指紋也沒有被收走。

根據校方的說法，認爲這起事件純粹是個誤會，承認老師的教導方式確實容易讓人誤會，但強調只是一個比較另類的教導方式；但家長質疑，因爲當天有學生掉東西，下午訓導處就要全班同學按指紋，豈不是太巧合。校方解釋，當天是讓學生按下指紋後，相互觀察每個人的指紋，藉此學習，並沒有真的拿指紋要比對或是另有所用，對於這樣的教學方式讓家長誤會感到抱歉。

法界人士表示，依據教育基本法第８條第２項規定，學生的學習權、受教育權、身體自主權及人格發展權，國家應予保障，並使學生不受任何體罰，造成身心之侵害。法界人士同時表示，老師依據教師法第１７條第１項第８款規定，非依法律規定不得洩漏學生個人或其家庭資料。如果學生的權益受到損害，依據教育基本法第１５條規定，政府應依法令提供當事人或其法定代理人有效及公平救濟之管道。

而指紋乃重要之個人資訊，個人對其指紋資訊之自主控制，受資訊隱私權之保障，參照司法院大法官釋字第６０３號解釋指出，個人自主控制個人資料之資訊隱私權，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使用有知悉與控制權及資料記載錯誤之更正權。憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第２３規定意旨之範圍內，以法律明確規定對之予以適當之限制。

[382] 中華民國憲法第 22-23 條・教育基本法第 8,15 條 ・教師法第 16-17 條 ・釋 字第 603 號
・95 年 國 字第 10 號 ・94 年 國 字第 4 號 ・院臺訴 字第 0970086563 號 ・檢查學生書包侵犯隱私？ 法官：阻卻違法法源編輯室 / 2008-10-06

4.檢查學生書包侵犯隱私？ 法官：阻卻違法[383]

台北市一名女學生在升旗時被老師檢查書包，其學生家長因不滿老師此等行為是違反了民法１９５條第１項的侵害隱私權，因此提出了告訴，要求老師賠償一百萬元。台北地院審理認為，老師是為了校園秩序，該行為是行使教師「生活指導權」裁量範圍。

法官認為，隱私權的保障並非漫無邊際，而且老師僅是查看書包內物品，有無攜帶違禁品，並未查閱學生日記、手機等內容的隱私，加上原告無法主張何項隱私被侵害，最後才判老師不必賠償。不過，台北市教育局表示，不主張老師搜書包行為，這個判決只是單一個案。

家長得知判決後表示，一切交由司法處理。但是老師卻表示，日前家長在網路上散佈不實的消息，有損名譽，因此已經以刑法第３１０條誹謗罪對該名家長提出告訴。對此，學生家長則不回應。

人本教育基金會大呼這項判決太離譜，全國家長團體聯盟也認為不可思議，認為基於教育人權，各級老師是絕對不可以隨意對學生搜書包，而就算是有相當理由及證據，也必須只能限定在特定對象的學生，絕不可以全面搜索所有學生的書包。再者，我國教育基本法第８條第２項規定學生身體自主權及人格發展權，國家應予保障，不受身心之侵害。

學者指出，台灣法官遇到未成年人的個案，其人權保護等級往往自動降級，總是以「出於好意或管教」等種種理由加以限制，顯示法官對未成年者人權意識單薄，跟不上國際的水準；並且呼籲，若學生在受教、學習或人格權上有受侵害，可依同法第１５條尋求救濟之道。

[383] 教育基本法第 1-3,8,15 條 ・民法第 18-19,195 條 ・中華民國刑法第 310,315 條 ・教師法第 16-17 條 ・84 年 台上 字第 2934 號 ・95 年 上易 字第 202 號 ・56 年 台上 字第 1016 號 ・台訓 (一) 字第 0920151620 號 ・台訓 (一) 字第 0920074060 號 ・大學教師口出穢言 學生集體抗議要求解雇/ 2007-12-18

5.數位「學生證」侵害隱私 學權會發動拒刷[384]

台北市政府教育局推動「數位學生證」，以學生證結合悠遊卡，並要求學生上、下學刷卡，被外界質疑爲「電子監控」，侵害學生隱私，並有資料外洩疑慮。中學生學生權利促進會昨（十四）日在西門町發起拒刷行動，希望學生以實際行動捍衛自己的人權。

學權會昨在捷運西門站六號出口發送自製「僞數位學生證」，搞笑諷刺政策不當，同時提供「反侵害人權封條」貼紙，鼓勵學生貼在學校的讀卡機上。學權會代表表示，數位學生證的記名功能和強迫使用政策，讓學生何時出入學校、借了什麼書、買了什麼東西，通通被記錄，等於全方位監控，與犯人、寵物無異。學權會質疑，全民指紋建檔政策因違反人權被司法院大法官釋字第６０３號解釋認定違憲，爲什麼以數位學生證全面記錄學生作息就合法？甫從高中畢業的學生反應，校內刷卡機數量不夠，爲了排隊刷卡反而耽誤時間，趕時間的同學直接拿包包過刷卡機，機具卻無法分辨學生證、健保卡或悠遊卡，「ＫＴＶ的威力卡，它也嗶嗶叫」；明明人已經到教室，忘了刷卡或感應不靈，卻被視同遲到或曠課，必須去教官室補簽到，變得更麻煩。且有很多學生每天只有一百元，想買東西，得先排隊儲值，再拿著電子錢包排隊購物，下課時間都花在排隊，還不如單純以零錢購物便利。

而刷卡機制卻約束不了翻牆蹺課的人，有心逃課者可以請同學代刷，但學生安全問題多半發生在上學前、放學後的校外，這套監控系統名義上是爲學生安全而設，卻無法預防或處理校外安全問題。學權會認爲，教育局應盡速檢討，擬定資料保護的配套措施，數位學生證不應強制使用，也不可結合點名，更不可未經學生同意，就將資料賣給廠商或研究單位，嚴重違反電腦處理個人資料保護法第８條第９款規定。學權會未來不排除針對幾所特定學校，發動大型的抗議拒刷活動。

教育局則表示，數位學生卡是爲確保學生安全在校的善意措施，教育局會行文學校不得處罰忘刷卡學生，改以輔導取代，若學校仍處罰學生，學生可依教育基本法第１５條及高級中學法第２５條規定向教育局申訴；而在學校完成宣導、系統配套措施完備前，學生刷卡與點名制度應雙軌進行，不得因學生未刷卡而當作曠課處理。至於目前刷卡機設置是以每一百五十名學生配備

[384] 教育基本法第 8,15 條 ・高級中學法第 25 條 ・國民教育法第 2,3,6 條 ・電腦處理個人資料保護法第 7,8,10,11 條 ・臺北市國民中學學生學籍管理辦法第 5,6,11 條 ・臺北市高級中等學校學生申訴案件處理辦法第 3,4,9 條 ・臺北市○○區○○國民小學學生申訴處理要點參考範例第 2,3,5,6 條 ・釋 字第 603 號 ・釋 字第 599 號 ・大學員生合作社先辦證才能消費 學生不滿法源編輯室 / 2007-10-15

一台，應該不會有排隊過久的問題，若刷卡機不夠，校方可向教育局提出要求。

五、網路購物

1.知名網路書店會員個資外流 法院判賠 13 萬[385]

知名線上購物網站九十六年辦理金馬影展套票出售，但因作業疏失，導致會員的個人資料外流，上百人權益受影響，其中十七人不願接受該購物網站的和解，要求賠償新台幣一百六十九萬元，台北地方法院昨判該購物網站應賠償十三萬七千九百元。全案仍可上訴。

依照電腦處理個人資料保護法第３條第７款規定，非公務機關指依法行使公權力之中央或地方機關外，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。參考法務部９３年１２月０１日法律字第０９３０７００５４６號函，登記資本額爲新臺幣一千萬元以上之股份有限公司之組織型態，且有採會員制爲行銷方式之百貨公司業及零售式量販業爲非公務機關。法院認定，該店面爲「無店面零售業」，並非電腦處理個人資料保護法第３條第７款規定，所規範的非公務機關，但法官認爲，該網站將客戶資料外洩，仍應負起賠償責任，但資料僅是洩給當時購買金馬影展套票的同好，並未向第三人公開，法官認爲該網站過失情節不嚴重，被害人精神受損尚微，判每個被害人可獲賠七千元至一萬七千四百元不等。

[385] 電腦處理個人資料保護法第 3,18,28-30 條 ‧96 年 重上 字第 428 號 ‧95 年 訴 字第 12632 號 ‧92 年 簡 字第 337 號 ‧法律 字第 0940039602 號 ‧北市法二 字第 09431537500 號 ‧法律 字第 0930700546 號 ‧KTV 業者洩露個人資料 法部：將修法規範法源編輯室 / 2008-11-20

2.個資外洩事件 消保會將與法務部攜手防堵[386]

標　　題：消保會與法務部攜手保護個資外洩消費者權益
新聞出處：行政院消費者保護委員會

由於消費者購物致個資外洩被詐財事件日欲嚴重，受害人數不斷攀昇，引發各界對此問題的高度重視，而登上「２００７年十大消費新聞排行榜」第一名，因此如何在最短期間內偵破此案堵住外洩管道，已是政府相關機關迫在眉睫的重大客題。爲此，行政院消費者保護委員會（以下簡稱消保會）特地由楊美鈴秘書長偕本會消保官並會同台北縣、市政府消保官專程拜會法務部朱楠次長，就如何保護因購物致個資外洩消費者權益議題進行討論。
有關此次拜會獲至以下共識：１．法務部將促請檢方加快偵辦此類案件的進度。２．雙方同意以舉辦研討會方式，增進行政調查工作的質量。３．雙方同意成立窗口，建立資訊快速交流管道。４． 法務部將儘速推動修法將電視購物頻道及網路購物等業者列爲電腦處理個人資料保護法之適用範圍，並就加重罰責、賠償總金額須考量業者利得及減輕被害人舉證等方面進行研議。５．促請各目的事業主管機關就其主管行業推動資安認證工作。
有關電視購物頻道或網路購物業者增列爲「電腦處理個人資料保護法」之適用範圍，如果無法在立法院本會期完成修法工作，則法務部將與目的事業主管機關以指定方式將上開業者列爲「電腦處理個人資料保護法」之適用範圍。
另行政院消保會認爲所有因購物致個資外洩被害消費者（不論是東森購物、富邦ｍｏｍｏ購物或博客來網路書店客戶…），因可能造成財產上或非財產上（侵害隱私權）之損害，故可依消保法第７條、民法第１８４條及第１９５條等規定要求業者負損害賠償責任。
行政院消保會認爲建構安全的消費環境，不能僅靠政府機關的偵查作爲，因最根本的解決之道，仍需靠企業經營者內部嚴謹的管控作爲，否則危機四伏的消費環境，不但讓消費者受害怯步，業者亦終將吞下失去市場的苦果。

[386] 民法第 184,185 條 ・消費者保護法第 7,7.1 條 ・電腦處理個人資料保護法第 3,28,33,36 條
・信用卡詐欺犯罪防制中心作業要點第 1,4-8 條 ・釋 字第 631 號 ・臺灣高等法院暨所屬法院八十六年法律座談會民事類提案第二十四號 ・銀行現金卡個資外洩詐欺集團 刑事局破獲/ 2007-12-25

3.電視購物台外洩客戶個資 法部擬加重刑度[387]

詐騙案件愈來愈多，連國內知名購物頻道、網路書店近日相繼傳出，疑似客戶個人資料外洩引發的詐騙案。對此，法務部表示，將會推動修正電腦處理個人資料保護法，讓適法範圍推及所有行業，並加重刑度，取消告訴乃論，希望能夠有效遏止個資外洩氾濫的情形。

一位退休女老師向知名電視購物台刷卡購買新台幣數千元的電器，不久，即接到顯示是〇八〇〇免付費電話的來電，對方自稱是購物台人員，，並清楚說出女老師身分證字號及訂購品，表示未收到刷卡款項；女老師二度刷卡後，對方稱信用卡失效，仍未收到款項，向她騙取信用卡卡號及末三碼密碼。其後，又相繼接到銀行人員、金管會人員來電，指她的信用卡被盜用，戶頭被列警示帳戶，存款須轉入安全帳號，將女老師存款盜領一空。

法務部指出，今（九十六）年九月至十一月，該家購物台客戶，因個資外洩遭詐騙，即有八百三十多人，損失金額達六千多萬元，受害人分布各縣市。內政部警政署反詐騙一六五專線統計資料也指出，每週接獲網路或購物詐騙案量約三百五十件，而與購物台相關的詐騙案就占三成，購物台已成爲個資外洩最嚴重的公司。

現行電腦處理個人資料保護法於民國八十四年八月十一日制定公布，適用對象依該條例第３條第７款規定，非公務機關只限於徵信業、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業等八大行業，以及少數指定團體。至於電視購物、網路商場則不在適用範圍之內，因此，法務部希望能推及到所有行業，已於九十四年完成修正草案，並更名爲「個人資料保護法」，但迄未未完成立法。

官員指出，業者既然要蒐集消費者個人資料，就應該盡到保護消費者的責任，草案第８條第１項第２款、第４款明定，業者在蒐集消費者個資前，有責任告知消費者目的和用途，讓消費者有時間進行防範措施；如果個資外洩，消費者就可以根據同法第２９條請求損害賠償。另，對於意圖營利而竊取、洩漏個資等行爲之最高刑度，也將由現行法第３３條規定之二年以下有期徒刑，提高爲五年以下；同時，刪除同法第３６條告訴乃論之規定，改爲公訴罪，即不需當事人檢舉，就可由檢警主動偵辦。

[387] 電腦處理個人資料保護法第 3,28,33,36 條 ・查緝電話詐欺恐嚇犯罪實施要點第 1-4 條 ・信用卡詐欺犯罪防制中心作業要點第 1,4-8 條 ・釋 字第 631 號 ・臺灣高等法院暨所屬法院八十六年法律座談會民事類提案第二十四號 ・「個人資料保護法」草案 (原名稱：「電腦處理個人資料保護法」)・現金卡個資外洩詐欺集團？ 銀行老總喊冤法源編輯室 / 2007-12-10

4.網拍膠囊、錠狀食品 消基會：逾九成違規[388]

網路拍賣已成爲民眾買賣商品的管道之一，但若自行販售未經衛生署發證進口的膠囊錠狀食品，皆屬違法。消基會針對國內網路拍賣第一平台，蒐集十七件膠囊和錠狀食品，調查發現有十六件商品賣方的個人資料不完整高達百分之九十四，另外有十五件商品賣家同時出售其他膠囊和錠狀食品。
此次調查發現，十七件商品中有八件未刊登有效日期，另外有七件商品有減肥豐胸的暗示。消基會指出，這次調查的十七件商品中，僅有一件因爲係企業經營者所販售，所以賣方的公開資訊最爲完整，其餘十六件商品賣方的個人資料皆不完整。
消基會指出，國內第二大網路拍賣平台，自今年六月中已展開自律行爲，將膠囊和錠狀食品下架，消基會呼籲第一平台也應跟進，負起網路拍賣平台把關責任，不要爲了利益，讓虛擬賣家販售違規食品，危害民眾健康。
消基會表示，依電子商務消費者保護綱領第５點有關「線上資訊揭露」之規定，當拍賣賣方爲企業經營者，應主動提供完整的賣方資訊；若拍賣賣方爲業餘人士，也應提供完整賣方資訊，讓消費者在掌握賣方資訊後可安心購買產品。但此次調查結果顯示，消費者能知悉賣方的完整資訊者顯爲少數，主管單位不應任由業者或是賣方「主動提供」完整資訊，而讓消費大眾的權益受損。
消基會表示，雖依據食品衛生管理法第１９條第１項規定，食品廣告誇大不實，依同法第３２條第１項規定，可處新台幣三萬到十五萬元罰金；誇稱療效可處二十萬元到一百萬元罰金。但因網拍賣家常以不實資料登錄，法令無法落實，網拍膠囊、錠狀食品已成爲民眾健康隱憂。

[388] 食品衛生管理法第 19,28,29,32 條 ・電子商務消費者保護綱領第 5 條 ・95 年 台上字第 216 號 ・府訴 字第 09670142200 號 ・衛署食 字第 0960400245 號 ・網拍平台收取 3% 手續費 公平會：不違法法源編輯室 / 2007-08-14

5.新春購物不吃虧 消保會提供民眾教戰手則[389]

隨著網際網路的普及，電子商務的發展也成了必然的趨勢，新春期間的長假，消費者除出外拜年旅遊外，勢必花比平常更多之時間在家上網瀏覽商品及購物，但因網路上也充斥者眾多陷阱，爲保護消費者權益，消保會歸納出幾項網路購物自保原則，提供消費者上網購物時參考。

消保會提醒民眾，在下單購物前應先查證業者身分，並充分瞭解所欲購買的商品或服務的規格及品質等各項資訊，同時應詳讀定型化契約條款及業者的隱私權保護措施，還有注意業者是否有快速、有效、公平之消費爭議處理機制。付款時，最好選擇定型化契約條款中的安全付款方式，例如：貨到付款。

消保會說，網路交易賣方在訂定型化契約時應注意是否符合網路交易定型化契約應記載及不得記載事項指導原則。依據消費者保護法第１１條之１第１項規定，業者與消費者訂立定型化契約前，應有三十日以內之合理期間，供消費者審閱全部條款內容。另依消費者保護法第１２條第１項規定，定型化契約中之條款違反誠信原則，對消費者顯失公平者，該契約無效。

民眾於交易完成後別忘了保存各項交易資料，此外，爲避免受騙，有幾點情形要特別注意：交易條件太好；在交易完成前要求你提供個人或財務的資訊；高額誘人的抽獎或贈品活動；須先寄送金錢以換取特別贈品的交易；高報酬率之投資機會；誇大功效的醫療或保健產品。

最後，行政院消保會呼籲消費者倘有任何消費爭議，或有消費相關問題要諮詢或申訴，均可依消費者保護法第４３條「消費者與企業經營者因商品或服務發生消費爭議時，消費者得向企業經營者、消費者保護團體或消費者服務中心或其分中心申訴。」之規定，撥打「一九五〇」全國性消費者服務專線電話轉接各縣市消費者服務中心，或直接向各縣市政府消費者保護官請求協助。

[389] 消費者保護法第 11-16,18-21,43 條 ・網路交易定型化契約應記載及不得記載事項指導原則第 1 條 ・電子商務消費者保護綱領第 1,5 條 ・民法第 88,89,91,114,153,154 條 ・93 年 判 字第 1221 號 ・公處 字第 094093 號 ・防旅遊網站詐騙 觀光局：認明網消會認證法源編輯室 / 2007-02-14

六、其他

1.座車被偷裝 GPS 檢：無法竊視竊錄不違法[390]

媒體報導，某電信大亨的趙姓情人，因不滿電信大亨的郭姓司機，在其座車底下安裝全球衛星定位系統（ＧＰＳ），控告郭某涉嫌妨害秘密，郭某聲稱是受該電信大亨之命行事，電信大亨則表示，是因因擔心女友安全才安裝追蹤器。由於追蹤器並沒有錄音、錄影功能，檢察官下不起訴處分。

按刑法第３１５條之１規定，無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者；或無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者，處三年以下有期徒刑、拘役或三萬元以下罰金。

另參考法務部９０年３月９日法九十檢字第０４６０６６號函之意旨，有關他人公開活動時，利用工具窺視或偷拍隱私部位，是否涉及刑事責任，應個案認定，凡是個人客觀上顯然無欲公開隱私活動，且有合理期待時，對侵害隱私權行爲，分別得依刑法或社會秩序維護法等相關規定處罰之。

據悉，該電信大亨買了一台車給其女友代步，不料，兩人感情生變，趙女指控電信大亨的郭姓司機在其座車底部安裝追蹤器，藉以掌握趙女行蹤。郭某聲稱一切都是聽命行事。電信大亨坦承，追蹤器確實是其授意安裝，因爲擔心趙女女友安危，也怕車子被偷，才安裝ＧＰＳ，以了解女友行蹤，另由於業者證稱，吸底盤式的ＧＰＳ，車輛移動時雖可發出信號，但只能得知該車位置，而不能窺視、竊錄，不構成妨害秘密罪，檢方於是對郭某不起訴處分。

[390] 中華民國刑法第 315.1,315.3,319 條 ・97 年 台上 字第 4546 號 ・96 年 易 字第 2878 號 ・94 年 上更（一） 字第 592 號 ・法九十檢 字第 046066 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 19 號 ・偷窺女性更衣獲不起訴？ 淫穢情書卻觸法法源編輯室 / 2008-12-04

2.偷窺女性更衣獲不起訴？ 淫穢情書卻觸法[391]

台北縣廖姓男子因發現劉姓女鄰居在換衣服時都不拉窗簾，自己觀看了兩年之外，還拉軍中同袍陳姓男子一起共賞，甚至寄給劉姓女子一本日本ＡＶ女優所出版的書籍。而前（二十五）日台灣板橋地檢署偵查終結，認爲廖姓男子偷窺女鄰居更衣並沒有觸法，因此全案處分不起訴，引起了不少爭議。
根據檢方說法，雖然廖姓男子長期偷窺女鄰居更衣，但是因爲沒有使用任何攝錄影工具，且女鄰居也表示沒有看到有人使用攝影機偷拍，因此不符合刑法第３１５條之１構成要件，最後檢方只好以「確有踰矩，亦有道德上可議之處」，但並未構成違法要件，予以不起訴處分。
不過，在今（九十七）年的西洋情人節時，因爲廖姓男子偷拆女鄰居的信用卡帳單，並且在信函當中加註淫穢字語，檢方表示，偷拆他人書信，還在上面書寫情色文字，這部份就構成了刑法第３１５條妨害書信秘密罪，因此在前日將廖姓男子起訴。根據媒體的報導，劉姓女子表示雖然偷窺部份不起訴，但還好最後還是以妨害書信秘密罪將他繩之以法。
參照臺灣臺北地方法院９６年易字第２８７８號刑事判決意旨，刑法第３１５條之１第２款之構成要件乃「無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或是身體隱私部位」，倘屬公開而非隱私之身體部位，顯非妨害秘密罪所欲保護之法益，自與該條構成要件不合。

[391] 7 年偷拍裙底慣犯 創下和解金額百萬紀錄・中華民國刑法第 315-315.1 條 ・院解 字第 3461 號 ・90 年 基簡 字第 334 號 ・95 年 上訴 字第 2856 號・96 年 易 字第 2878 號・法九十檢 字第 046066 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 19 號 法源編輯室 / 2008-11-27

3.苗栗監聽核准率居冠 法官：陳報率待改進[392]

監聽核准權由檢方移轉法院將近一年，苗栗地方法院核准率高達九成，冠居全國，也遠高於各地方法院平均核准率的七成五，較花蓮地院的四成、連江地院爲零，更相差懸殊。不過，警憲調與海巡等單位多數未依規定在監聽結束後十二天內，報由檢察官向法院陳報監聽結果，按時回報率僅五成八。
根據通訊保障及監察法第５條第１項規定，有事實足認被告或犯罪嫌疑人有該條項各款罪嫌之一，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。
該通訊監察書，依同條第２項規定，偵查中由檢察官依司法警察機關聲請或依職權以書面記載同法第１１條的事項，並敘明理由、檢附相關文件，聲請該管法院核發；檢察官受理申請案件，應於二小時內核復。如案情複雜，得經檢察長同意延長二小時。法院於接獲檢察官核轉受理申請案件，應於二十四小時內核復。審判中由法官依職權核發。法官並得於通訊監察書上對執行人員爲適當之指示。
苗栗地方法院庭長表示，法院支持偵查機關打擊犯罪，所以較少駁回監聽票的聲請，但監聽後不能石沉大海，才能落實追蹤考核與對人權的保障。該庭長指出，監聽票的時效一般核發一個月，依通訊保障及監察法施行細則第２７條規定，監聽結束後，執行機關應於通訊監察結束後，於七日報由檢察官於收文後五日內陳報法院審查，但真正依規定陳報者並不多。法院呼籲，監聽涉及隱私，攸關人民權益，偵查機關因辦案需要聲請監聽，對於監聽結果必須清楚交代，以落實人權保障。

[392] 通訊保障及監察法第 2,5,11,15 條 ・通訊保障及監察法施行細則第 27-29 條 ・法院辦理通訊監察案件應行注意事項第 24-26 條・院台廳刑一 字第 0960025264 號 ・(89)法檢 字第 001043 號 ・臺灣高等法院暨所屬法院 96 年法律座談會刑事類提案 第 44 號 ・海外軍官、記者遭監聽 美國國會展開調查法源編輯室 / 2008-11-24

4.唱國歌不起立被列黑名單？ 日教師：違憲[393]

根據媒體的報導，日本神奈川縣某所公立高中職員，因爲不滿縣教育委員指示校長，並且製作一連串聽到國歌不起立的教職員黑名單，而告上法院；教職員指出，這樣的行爲已經嚴重違反保護個人資訊的相關案例，更侵犯了憲法保障個人的思想自由。

據了解，該所公立高中有十八名教職員，昨（十七）日向橫濱地方法院提起告訴，除了要求教育委員會刪除他們的個人資料之外，還要賠償每個人一百萬日圓的慰問金。起訴狀中指出，教育委員會要求公立高中校長報告聽到國歌不起立的教職員名單，並且要蒐集紀錄每個人的資訊。

教職員曾根據個人資訊保護條例要求刪除資訊，當初縣審查會也做出蒐集資訊不恰當的回覆，不料隔年又繼續編列黑名單。據了解，東京地方法院以及最高法院曾經在去(九十六)年做出教育委員會規定「唱國歌應以鋼琴伴奏」、「教師唱國歌應起立」屬於違憲的判例。因此日本不少專家認爲該縣教育委員的作爲應屬違法。

比照國內亦有類似規定，例如中華民國國徽國旗法第１１條規定升降國旗必須要全體肅立、唱國歌等；另依據刑法第１６０條規定，意圖侮辱中華民國，而公然損壞、除去或污辱中華民國之國徽、國旗者，處一年以下有期徒刑、拘役或三百元以下罰金；意圖侮辱創立中華民國之孫先生，而公然損壞、除去或污辱其遺像者亦同，似乎有異曲同工之處。但實務上因此被提起公訴的案例倒是少之又少。

[393] 中華民國刑法第 118,160 條 ‧中華民國國徽國旗法第 11-12 條 ‧84 年 上易 字第 5037 號
‧台內民 字第 79062 號 ‧（74）台內民 字第 347655 號 ‧（74）台內民 字第 360470 號
‧國慶典禮缺席要記過 教部：學生可提申訴法源編輯室 / 2008-11-18

5.內政部力推上網登記結婚 法務部表示反對[394]

我國的結婚制度，自今（九十七）年五月二十三日開始，就已經採取登記制度，但依據民法第９８２條規定，結婚應以書面爲之，有二人以上證人之簽名，並應由雙方當事人向戶政機關爲結婚之登記；內政部表示，爲了讓民眾更方便，將推動以自然人憑證的方式上網登記結婚，如此一來，想要什麼時候結婚，只要上網登記即可。

內政部長表示，爲了讓結婚容易化，且降低離婚率，今後會致力增訂兩願離婚的相關規定，好讓離婚不再那麼方便。針對這項離婚的提案，有學者提出不同的看法，認爲離婚並不是不好的事，重點應該是要協助離婚後的雙方分別再婚，提高結婚率，以及如何教育單親家庭的幼童等問題。而對於上網登記結婚，民眾也普遍抱持反對意見，認爲網路結婚一點真實感也沒有，也怕個人資料外洩。

但也有民眾持贊成意見，認爲這樣的方式節省許多時間，對於工作忙碌的族群，或許是個不錯的方法；戶政人員則表示，雖然上網辦理是很方便，但是現在網路的安全卻是個問題，如果出現駭客侵入，有什麼糾紛的話，又該如何解決？而主管民法的法務部也認爲，雖然提案的立意良好，但婚姻涉及身分的變動和後續財產的分配，對於人民權利的影響極大，因此不應該採取草率的方式。

法務部指出，上網登記結婚，有辨識身分的困難度且沒有辦法確認結婚的真意，因結婚的要件之一便是雙方有結婚的真意，目前則是由戶政機關人員依據戶籍法第９條辦理結婚登記時，當面探求雙方真意，且會尋問是否有民法第９８３條是直系血親等等關係或是其他不能結婚的事由，法務部認爲，這些都是網路結婚無法做到的，因此不應該貿然的施行。

[394] 97 年 婚 字第 170 號 ・法律決 字第 0970700202 號 ・廳民三 字第 0970000772 號 ・法律決 字第 0970700201 號 ・(76) 廳民一字第 1998 號 ・結婚登記制 23 日實施 證人須在證書上簽名・民法第 982-985,988 條 ・戶籍法第 4,9,27,33 條 ・95 年 婚 字第 172 號法源編輯室 / 2008-09-01

6.上海新規定 不守交通規則將登上電視報紙[395]

在台灣，如果不遵守道路交通標誌、標線、號誌之指示，都是依據道路交通管理處罰條例第６０條第２項規定，處新臺幣九百元以上一千八百元以下罰鍰；不過如果是在上海，可就沒那麼輕鬆了。上海的交通部門最近有項新的交通規定，只要是行人或是駕駛者違規，全部都會用拍照或是錄影存證，而且還會登上電視或是報紙的版面。

根據上海交通部門的說法，上海人非常愛面子，如果登上媒體就會讓大家都知道自己違規，因此正可利用這個弱點，矯正行人和駕駛者。不過，有不少市民表示，這樣的方式根本就是侵犯人民的隱私權，但官方卻回應，如果沒有違規，也就不會有處罰，畢竟每年在馬上虎口失去生命的人不計其數，交通規則就是用來保護行人和駕駛者的生命。

且在台灣，道路交通管理的稽查和違規紀錄，由交通勤務警察，或依法令執行交通稽查任務人員執行；不過，對於違反交通規則行爲，依據同處罰條例第７條之１規定，民眾也可以敘明違規事實或檢具違規證據資料，向公路主管或警察機關檢舉，經查證屬實者，應即舉發。另參照道路交通案件處理辦法第３條規定，交通案件之處罰，除違反道路交通管理處罰條例或社會秩序維護法及其他法律，應依該條例或社會秩序維護法及其他法律處罰外，其刑事責任部分，仍適用刑事法律有關規定處理之。

對於行人規範，參照司法院大法官釋字第４１７號解釋意旨，國家爲加強交通管理、維持交通秩序及確保交通安全，乃制定道路交通管理處罰條例，俾車輛及行人共同遵行。如有違反，則予處罰，以維護人車通行之安全，進而保障人民之生命、身體及財產。該條例第７８條第３款規定：行人在道路上不依規定，擅自穿越車道者，處一百二十元罰鍰，或施一至二小時之道路交通安全講習。其對人民違反行政法上義務之行爲予以處罰，係爲維持社會秩序及增進公共利益所必需，核與憲法第２３條以法律限制人民自由權利之意旨尚無牴觸。

[395] 中華民國憲法第 7-8,16,23,24 條 ・道路交通管理處罰條例第 7-7.3,60,78 條 ・道路交通案件處理辦法第 2-4,12,27,33 條 ・釋 字第 417 號 ・94 年 交抗 字第 484 號 ・95 年 交上易 字第 2 號 ・(86)交路 字第 010606 號 ・(87)交路 字第 015559 號 ・南市機慢車紅燈右轉僅勸導不罰 全國首推法源編輯室 / 2008-08-29

7.總統個資一筆 300 元 史上最駭集團遭破獲[396]

刑事局日前偵破一起堪稱歷來規模最大的個人資料外洩案！該駭客集團不僅入侵郵局，盜領民眾存款，還入侵健保局、購物台、電信業者等電腦主機，竊取包括前總統、現任總統、名模等五千萬筆個資，並以每筆三百元的價格出售。

警方表示，集團首腦陳嫌一干人等，與大陸駭客聯手，透過台灣多所大學主機做跳板，入侵國內各公、私機構電腦主機，竊取超過五千萬筆個資，內容從家庭狀況到就醫紀錄都有，國內政商名流無一倖免。警方訊後將六嫌送辦。由於從多處管道入侵盜取個資，同一人的個資被重複盜取，因此累計達五千萬筆，警方依妨害電腦使用罪、詐欺、洗錢等罪嫌送辦。

參照臺灣板橋地方法院９３年簡字第１５９２號刑事簡易判決，無故入侵他人電腦取得他人電腦之電磁紀錄，則刑法第３５８條、第３５９條兩罪間有方法結果之牽連關係，應依同法第５５條之規定，從一重處斷。

依本案而言，該駭客集團入侵公務機關、民間企業的電腦以竊取個資，依上開判決意旨，具牽連關係，應從一重之無故取得他人電腦之電磁紀錄罪處斷，但刑法修正後，廢除牽連犯規定，故兩罪間應數罪併罰。此外，由於嫌犯是對於公務機關的電腦或其相關設備犯前開規定之罪，依同法第３６１條規定，加重其刑至二分之一，且爲非告訴乃論罪。

[396] 中華民國刑法第 55,339,358-363 條 ・警察機關資訊安全實施規定第 2,3,5-7,11,14 條 ・96 年 簡上 字第 39 號 ・93 年 簡 字第 1592 號 ・法檢字第 0950804053 號 ・法檢字第 0950801421 號 ・94 年少年法院（庭）庭長法官業務研討會法律問題提案 第 20 號 ・小心防範網路之網頁掛馬攻擊 調查局呼籲 法源編輯室 / 2008-08-27

8.竊聽捉姦 侵犯隱私非「無故」檢方不起訴[397]

桃園縣某賴姓男子與徐姓情婦通姦生子遭判刑，卻持續交往，妻子委託徵信社在丈夫車上裝設ＧＰＳ與竊聽器，逮到丈夫與徐女通姦，賴某反控妻子妨害秘密，檢察官調查認為，妻子並非「無故」侵害賴某隱私，昨日下不起訴處分。

根據刑法第３１５條之１規定，無故利用工具或設備窺視、竊聽或以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者，處三年以下有期徒刑、拘役或三萬元以下罰金。本條妨害秘密罪之構成，以「無故」竊錄他人隱私為要件，檢察官認為妻子欲保護者為婚姻與家庭，而在與隱私權的法益衝突中，家庭與婚姻，在比例原則上應優於丈夫的隱私權，侵害隱私的蒐證行為並非「無故」，因此認定不構成妨害秘密罪嫌。

參照臺灣高等法院花蓮分院８９年上易字第２１３號刑事判決同此意旨，認為夫妻婚姻關係中，夫妻雙方為維持圓滿婚姻生活所應盡之純潔保持義務，不僅出於道德上之期許，其婚外性行為更受到刑事法律規定之明文禁止。因此，任何違反婚姻純潔義務之行為，依一般經驗法則，其行為均採取秘密之方式為之，其證據之取得，極為困難。

如果夫妻一方之行為，在客觀上，已經足以導致他方對婚姻之純潔產生合理之懷疑時，不論他方是基於「去除婚姻純潔之疑慮」或「證實他方有違反婚姻純潔義務事實」的動機，而對對方私人領域有所侵犯時（例如以竊聽或竊錄其私人秘密通訊），應認為是他方為維護婚姻純潔所作出的必要努力，而非屬刑法第３１５條之１之「無故」妨害他人秘密之行為。

[397] 中華民國刑法第 315.1,315.3,318.2,319 條 ・通訊保障及監察法第 24,29,30 條 ・96 年 易 字第 2878 號 ・95 年 上訴 字第 2856 號 ・89 年 上易 字第 213 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 19 號 ・法務部 (89) 法字第 000805 號 ・地鐵擁吻被放上網 受害者認已侵犯隱私權法源編輯室 / 2008-08-14

9.KTV 業者洩露個人資料 法部：將修法規範[398]

部分ＫＴＶ視聽歌唱業者，留存消費者的個人相片、身分證號碼等個人資料，以便向消費者催收帳款。這類的個人資料，法務部表示，不受電腦處理個人資料保護法的約束，但若有侵害他人人格權或隱私權時，仍受民法相關規定的規範，若涉及侵權，即有損害賠償的責任。

台北縣政府經濟發展局向法院部查詢，部分ＫＴＶ視聽歌唱業者，私自留存消費者的個人資料，包括消費者個人照片、身分證號碼、手機、住家地址及電話等資料，如果涉及個資外洩，是否適用電腦處理個人資料保護法的規範。法務部表示，現行電腦處理個人資料保護法主要是規範公務機關及非公務機關。但所謂「非公務機關」，依同法第３條第７款規定是指：１、徵信業及以蒐集或電腦處理個資爲主要業務的個人或團體。２、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。３、其他經法務部會同中央目的事業主管機關指定的事業、個人或團體（包括，期貨業、產物及人壽保險公會、不動產仲介經紀業、利用電腦網路開放個人資料登錄的就業服務業、登記資本額爲一千萬元以上的股份有限公司，且有採會員制爲行銷的百貨業、零售式量販業等）。

所以，ＫＴＶ視聽歌唱業者並不受電腦處理個人資料保護法的約束，若涉及侵權行權，個人僅得依民法相關規範求償。但有鑑於該法已未能有效保護個人資料，電腦處理個人資料保護法第２條的修正草案中已刪除非公務機關行業別的限制，法務部表示，一旦將來修正草案通過後，任何自然人、法人或其他團體，除爲單純個人或家庭活動的目的而蒐集、處理或利用個人資料外，皆受到該法的規範。

[398] 電腦處理個人資料保護法第 3,5,7,8,18,19,27,28 條 ・電腦處理個人資料保護法施行細則第 2,7,8,37 條 ・96 年 重訴 字第 193 號 ・95 年 訴 字第 12632 號 ・法律決 字第 0950026402 號 ・法律決 字第 0940001159 號 ・「個人資料保護法」草案 (原名稱：「電腦處理個人資料保護法」)・利用個人資料行銷 修正案：消費者可拒絕法源編輯室 / 2008-06-17

10.結婚登記制 23 日實施 證人須在證書上簽名[399]

五月二十三日起儀式婚將改爲登記婚，新人結婚必須到戶政事務所完成登記才生效，公開儀式不再是婚姻生效的要件。戶政事務所官員表示，內政部已通過民眾假日辦理結婚登記，但基於戶政人力不足，需於三天前向戶政事務所預約，再依據戶政所安排的時間前往辦理，且登記日即結婚日，不可辦理追溯。

官員指出，依新修正民法第９８２條規定，民眾結婚需完成登記才生效，日後公證結婚或縣市政府辦理集團結婚將不再具有法律效力，而新人多選擇在假日結婚，當天雙方皆十分忙碌，可能無暇親自到戶政所登記，官員建議，民眾可利用婚前籌辦婚禮的空檔提前到戶政所辦理登記。

但新制度引發困擾的不僅於此，以往舉行婚禮，許多人喜歡找地方首長、民意代表或是名人證婚，但同條規定，結婚應以書面爲之，有二人以上證人的「簽名」，公證法施行細則第６０條第１項規定，結婚書面的公證，結婚的男女當事人應偕同證人攜帶身分證明文件親自到場，並在結婚書面上簽名。同條第３項規定，公證人還必須告知結婚當事人未向戶政機關辦妥結婚登記前，其結婚尚未生效力，並於公證書上註記。

所以依照新制，未來兩名證婚人需在戶政所提供的結婚證明書上填具身分證字號及戶籍地址，由於近來詐騙集團猖獗，可能讓許多職業證婚人卻步。就有民意代表坦言，以前常當證婚人，覺得也算是沾喜氣，但如果要寫出這麼多個人資料，的確會有疑慮。但戶政事務所指出，以往證婚人其實只是儀式婚的證人，一般民眾到戶政所登記時多以父母爲證婚人，新法實施後應不致受影響，至於舊式結婚證書則可作爲紀念用。

[399] 民法第 982,988 條 ‧戶籍法第 12,17.1,35 條 ‧公證法施行細則第 60,62,63 條 ‧院 字第 1434 號 ‧31 年 上 字第 135 號 ‧20 年 上 字第 452 號 ‧臺灣高等法院暨所屬法院 93 年法律座談會民事類提案 第 4 號 ‧擾民？登記才算結婚日 宜蘭縣籲收回成命 法源編輯室 / 2008-05-21

11.利用個人資料行銷 修正案：消費者可拒絕[400]

立法院昨（十九）日初審通過電腦處理個人資料保護法修正案，除了擴大保護對象的範圍之外，還明訂從事商品行銷的業者，應該要提供消費者拒絕個人資料作爲行銷工具的反應管道，如果消費者拒絕業者的行銷，業者應立即停止。不過對於有關刑事責任以及相關賠償總額、如何簡化民眾舉證責任，以及立委使用個人資料是否免責等問題，因爲立委意見甚多，將保留到朝野協商再處理。

依據電腦處理個人資料保護法第３條第７款之規定，現行條文對於電腦處理個人資料保護法的保護範圍，僅適用於徵信業等八種行業，一般行業以及個人都不適用。不過修正條文將擴大到除單純個人、或是家庭活動目的蒐集處理或利用個人資料之外，任何自然人、法人或其他團體，都在適用的範圍之內。且不經電腦處理的個人資料，亦在保護之列。

而同法第１８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，並符合當事人書面同意者或爲學術研究而有必要且無害於當事人之重大利益者等，不得爲之；參照法務部８７年１２月１４日（８７）法律字第０４５４５６號函規定，電腦處理個人資料保護法第１８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，並符合該條所定情形者，不得爲之。如意圖營利違反上開規定，致生損害於他人者，依同法第３３條之規定，應科以刑事責任。

則修正案另規定，從事商品行銷的業者，要在首次行銷時就免費提供消費者拒絕的管道，而且一旦表明拒絕行銷，業者應立即停止使用個資行銷。此外，同法第１３條第１項規定，公務機關應維護個人資料之正確，並應依職權或當事人之請求適時更正或補充之，參照電腦處理個人資料保護法施行細則第２５條說明，當事人應提出足資釋明之證據。修正案則是規定，非公務機關對於保有的個人資料，亦有更正、補充及通知的義務，如果違法蒐集、處理或利用個人資料都應刪除、停止蒐集該個人資料。

[400] 電腦處理個人資料保護法第 3-6,13,18,23-24,33 條 ・電腦處理個人資料保護法施行細則第 2-7,23-25 條 ・95 年 訴 字第 4098 號 ・93 年 上易 字第 1896 號 ・(87) 法律字第 045456 號 ・台財融 字第 85254083 號 ・台財保 字第 861777545 號 ・個資外洩事件 消保會將與法務部攜手防堵法源編輯室 / 2008-05-20

12.洩露個資最高賠 10 億 朝野有共識下週送審[401]

我國民眾的個人資料時常遭到外洩、且外洩的個人資料被犯罪集團利用於詐欺的犯行相當嚴重，近日朝野達成重大共識，立法、司法與行政部門決聯手祭出天文數字的重罰加以遏止，目前立法院審議中的電腦處理個人資料保護法草案內容，個資外洩賠償上限從現行法二千萬元提高到十億元。

根據現行電腦處理個人資料保護法第２７條第４項、第２８條第２項規定，如果民眾的個人資料外洩，不論洩漏者是公務機關或非公務機關，索賠的最高總額以新臺幣二千萬元爲限。而行政院版草案提高到五千萬元，國民黨立委的版本則無賠償上限。但司法院指出，現今個資外洩情形嚴重，限額五千萬元太低，大企業可能認爲無關痛癢，但無限賠償又可能導致企業倒閉，衍生出社會問題，因此建議將上限訂爲十億元，法務部評估後認爲民眾應可接受。

此外，草案第２９條也規定，受害民眾索賠時，不須負舉證責任，非公務機關要證明已窮盡一切方法，仍無法防止駭客竊取資料才能免責，公務機關只有在天災、地震等不可抗力才能免責，否則須負無過失責任；草案第２２條同時賦予縣市政府有「行政檢查權」，不須透過法院審查程序，即可查扣企業非法所有的個人資料。至於草案規範對象，不限現行法第３條第６款第７款規定的公務機關和徵信、醫院、電信等業，只要使用電腦或書面處理個資，統統在保護範圍。

全案目前不僅獲朝野立委同意，法務部也表支持，上述機關一致認爲，公務和非公務機關使用民眾個人資料情形普遍，應加重賠償責任，才能保護民眾隱私權；由於全案已有共識，下週一立院司法委員會將開始逐條討論。

[401] 腦處理個人資料保護法第 3,22,27-29 條 ・電腦處理個人資料保護法施行細則第 2,6,7,42 條 ・96 年 重上 字第 428 號 ・96 年 重訴 字第 193 號 ・衛署醫 字第 0960046106 號
・法律決 字第 0950041999 號 ・法律決 字第 0940041370 號 ・民國 86 年 11 月 00 日臺灣高等法院暨所屬法院 ・個人資料外洩引發詐騙 法務部：修法重懲法源編輯室 / 2008-05-16

13.MP3 密錄不能當證據！ 法官：因侵犯隱私[402]

某立委被控賄選案，臺中地方法院今（一）日一審宣判，合議庭認爲，證人以ＭＰ３錄下的對話，爲非法蒐證，不具證據能力，單憑錄影畫面無法證明該五萬元現金究竟是政治獻金或賄款，將涉案立委等五人均判無罪。
該立委遭控前往一陳姓男子住處，交付五萬元椿腳費給陳某，嗣後，該立委再度前往陳家，陳某欲退還該五萬元，該立委仍要他「到摳人」，但因陳堅持不收，該立委才取回現金。由於第二次退錢的畫面被陳家監視器拍下，對話則被另一名在場的秘密證人以ＭＰ３錄音，成爲檢方起訴該立委賄選並求刑五年的兩大關鍵證物。
依刑事訴訟法第１６５條之１第２項規定，錄音、錄影、電磁紀錄或其他相類之證物「可爲證據」者，審判長應以適當之設備，顯示聲音、影像、符號或資料，使當事人、代理人、辯護人或輔佐人辨認或告以要旨。同法第１５５條第２項規定，無證據能力、未經合法調查之證據，不得作爲判斷之依據。合議庭認爲，監視器畫面的證據能力固然沒有問題，但錄音的部分，合議庭表示，秘密證人錄音時並未經過陳某及該名立委的同意，目的也非爲了舉發賄選，已侵害到該立委憲法保障的秘密通訊自由，這部分的證據是以非法的方式取得，沒有證據能力。
依照同法第１５８條之４規定，除法律另有規定外，實施刑事訴訟程序之公務員因違背法定程序取得之證據，其有無證據能力之認定，應審酌人權保障及公共利益之均衡維護。所以，如果是公務員違法監聽取得的證據，依照本條規定，法官權衡以後，還是有可能「敗部復活」。
但私人違法取證的效力爲何，法無明文規定，有論者以爲，應以憲法第２３條的比例原則審查，參照臺灣高等法院臺中分院９６年度選上字第６號民事判決意旨，在賄選的案子，賄賂行爲，常以隱秘方式進行，被害人舉證極度不易。在此前提下，如果以侵害隱私權的方式而取得的證據，不法行爲人的隱私權與被害人的訴訟權就發生衝突，則被害人取得的證據能否引用，就必須視其是否符合比例原則而定。但本案爲刑事案件，證據法則當然比民事訴訟更嚴格，且必須進行更嚴謹的論證才行。

[402] 賄選？賭博？選舉賭盤監聽 院、檢不同調・中華民國憲法第 16,22,23 條 ・刑事訴訟法第 155,158.4,165.1,168.169 條 ・97 年 台上 字第 1069 號 ・97 年 台上 字第 561 號 ・96 年 選上 字第 6 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 33 號 ・「 92 年公訴檢察官實務研討會」法律問題提案 第 14 號 法源編輯室 / 2008-05-01

14.課員給錯戶籍資料 無辜男子 23 件官司纏身[403]

一名律師助理爲了幫人打官司，前往某戶政事務所，查詢一名謝姓男子資料，課員卻誤提供另一同名的謝姓男子資料，讓無辜的謝某莫名其妙背了二十三件刑、民事官司。檢察官調查後，依洩密罪將該課員起訴。

根據刑法第１３２條第１項規定，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。同條第２項規定，因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。

所謂「關於中華民國國防以外應秘密之文書、圖畫、消息或物品」，依臺灣高等法院９６年度上易字第９８１號刑事判決意旨認爲，指國防上應秘密之事項以外而與「國家」政務或事務上具有利害關係而應保護之秘密者而言。本罪既然爲保護國家法益之犯罪，個人之基本資訊能否當然即謂係本罪保護之客體，實非無疑。所以依照此判決意旨，如果洩漏的個人資訊與國家利益無涉，就不是本罪所要保護的對象。

該課員應訊時表示，自己是爲了便民，才直接用姓名查詢，並非故意。但檢察官指出，律師助理申請時，已註明欲查明的謝姓男子的地址，但該課員卻給了住在不同街的謝某資料，顯示他沒有詳加審核，由於公務員有保守個人資料的義務，因此依刑法洩漏國防以外祕密罪起訴。但如果依照上述的判決意旨，該課員洩漏的資料是個人資訊，能否論以洩漏國防以外祕密罪，可能就會產生爭議。

至於該課員被控妨害秘密（同法第３１８條規定參照）及違反電腦處理個人資料保護法第３４條兩罪，因爲不處罰過失行爲，檢察官另將該課員不起訴處分。儘管對方已被起訴，謝某仍氣憤表示，雖然先前請求國家賠償十萬元已敗訴，但他會堅持上訴捍衛權益。

[403] 中華民國刑法第 132,134,318 條 ・電腦處理個人資料保護法第 7-17,27,34,36 條 ・96 年 上易 字第 981 號 ・95 年 上訴 字第 1456 號 ・93 年 台上 字第 6220 號 ・(88) 法律 字第 036750 號 ・法務部 (76) 法檢(二)字第 1130 號 ・個人資料外洩引發詐騙 法務部：修法重懲法源編輯室 / 2008-04-30

15.小心防範網路之網頁掛馬攻擊 調查局呼籲[404]

標　　題：調查局呼籲民眾防範網路犯罪集團之「網頁掛馬」攻擊
新聞出處：法務部調查局

調查局表示，香港影星陳冠希與其他女星私密照片，遭不明犯罪集團刻意於網路散布，引發民眾瀏覽之熱潮。網路犯罪集團也利用這個熱潮，藉由設置相關網站或部落格，內藏惡意連結，或攻擊一般正常網站，插入隱藏性惡意連結，致使不知情之民眾電腦遭受入侵，政府機關、民間機構及個人之重要機敏資料，有遭受竊取之風險。

調查局調查發現，近來網路上出現許多以提供陳冠希與其他女星私密照片之網站及部落格，該等網站及部落格是以提供相關相片之名義，吸引民眾前往瀏覽，當民眾連上該網站及部落格時，會在民眾不知情的情況下，下載惡意木馬程式至電腦系統中，達到控制民眾電腦系統，並進而竊取機密資料或達到進行其他犯罪行為之目的。

經調查局與坊間科技公司合作，並經實機驗證後發現，多達１６１個網頁隱藏惡意程式，迄今仍有逾６０個網頁持續危害。由於惡意程式除能避開部分防毒軟體之偵查，致使受害者難以察覺。經驗證某特定惡意程式，目前仍有高達３７．５％的防毒軟體無法偵測。（此種攻擊模式又稱之為「網頁掛馬」，請參閱後列名詞解釋：網頁掛馬）

相關網址例示如下（以下網址請勿任意點選）：

http://72.167.132.171/chen_photo.html

http://se.97ai.com/html/42/62969.shtml

http://ww2.spooots.com/index.html

知名搜尋引擎亦有針對部分惡意網站提出警告，在搜尋結果的網址名稱下，加註「這個網站可能會損害您的電腦」之警語。

惡意網站之攻擊目的：

該等惡意程式以蒐集受害者資料及機密檔案為主要目標，常見之機密檔案資料，包括網路銀行、線上購物、個人信箱之帳號密碼、電腦系統中之文件與照片、鍵盤側錄、隨身碟內之檔案資料。

其餘尚有下列惡意攻擊行為：

[404] 中華民國刑法第 210,212,220,235,358,359,362 條 ・釋 字第 617 號 ・95 年 易 字第 121 號
・95 年 易 字第 152 號 ・94 年 訴 字第 1514 號 ・法檢字第 0950804053 號 ・94 年少年法院（庭）庭長法官業務研討會法律問題提案 第 20 號 ・香港藝人裸照風波未平 張貼轉寄皆為觸法/ 2008-02-19

１．關閉常見的掃毒程式與偵測軟體，或利用Ｐａｃｋｅｒ軟體變形技術，躲避掃毒軟體偵測。
２．利用ＩＥ漏洞，植入惡意連結，大量散布，或影響對外連線。
３．竊取個人資料，如線上聊天軟體ＭＳＮ、ＱＱ之聊天對談紀錄及密碼等資料。
４．植入廣告軟體。
５．植入Ｒｏｏｔｋｉｔ或掛載ＡＰＩ　Ｈｏｏｋｅｒ程式，達到控制系統目的。

「網頁掛馬」又稱之爲網頁隱藏式惡意連結。簡單來說，其攻擊模式分成四個步驟：
１．駭客攻擊企業組織或政府機關的網站，網頁遭到竄改，植入一段惡意連結，或者是設立惡意網站，透過各種宣傳手法，吸引民眾到站瀏覽
２．網站的使用者連上該網站。
３．使用者看不到這個連結，也不必點選這個連結，只要連上網站，就會轉引自駭客預先設計好的陷阱。
４．在不知情的情況下，使用者被植入木馬程式。

網頁掛馬與釣魚網站（Ｐｈｉｓｈｉｎｇ）不同之處，釣魚網站通常是設置一個以假亂真的網站，來欺騙網路瀏覽者上當；網頁掛馬則是攻擊一個正常的網站，利用網路瀏覽者對於正常網站的信任感，讓使用者在不知不覺中被植入木馬程式，或者是駭客自行設立一個網站或虛設部落格，以各種方式吸引民眾瀏覽，再送出惡意程式。

相關法令

一、散布猥褻物品罪

散布陳冠希與其他女星私密照片，無論是以架設網站，或傳送電子郵件等方式，可能觸犯刑法第２３５條散布猥褻物品罪。

刑法第２３５條散布猥褻物品罪

散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處二年以下有期徒刑、拘役或科或併科三萬元以下罰金。

意圖散布、播送、販賣而製造、持有前項文字、圖畫、聲音、影像及其附著物或其他物品者，亦同。

二、妨害電腦使用罪

藉由網頁掛馬或其他攻擊方式，入侵他人之電腦系統或設備者，成立下列罪刑：

（一）刑法第３５８條無故入侵電腦系統設備罪

無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦 系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

（二）刑法第３５９條無故取得刪除變更他人電磁紀錄罪

無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

（三）刑法第３６２條製作專供犯妨害電腦使用之電腦程式罪

製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

（四）其它法令

視具體個案，成立刑法僞造文書罪，或違反著作權、商標權等規範。

16.地鐵擁吻被放上網 受害者認已侵犯隱私權[405]

上海一對情侶在地鐵擁抱親吻，不料地鐵的站務人員用監視器監看到畫面，最後甚至把這段影片放在網路上供大家觀看。此舉引發這對情侶強烈的不滿，認爲嚴重的侵犯了他們的隱私權，打算對這家地鐵公司提出告訴。上海地鐵公司則表示會調查這件事情，若員工有違法的行爲，一定會嚴肅處理。
不法侵害他人之隱私，雖不一定會造成被害人財產上的損失，但依據我國民法第１９５條第１項規定，被害人雖非財產上之損害，亦得請求賠償相當之金額。此外，上開行爲亦觸及刑法３１５之１條第１款，利用工具或設備窺視、竊聽他人非公開之活動、言論談話者，可處三年以下有期徒刑、拘役或三萬元以下罰金。
而根據電腦處理個人資料保護法第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，不得爲之；若有違反至他人受損害者，將依同法第３３條，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（非公務機關：參照同法第３條第７款說明）。

[405] 中華民國刑法第 315.1,315.3,319 條 ・民法第 18,184,195 條 ・電腦處理個人資料保護法第 1-3,18,28,33-34 條 ・96 年 易 字第 2878 號 ・95 年 簡 字第 790 號 ・95 年 訴 字第 110 號
・法律決 字第 0950026402 號 ・府警保 字第 09605000232 號 ・檢查學生書包侵犯隱私？ 法官：阻卻違法法源編輯室 / 2008-01-24

17.核發監察書法院將嚴格把關 確保人民隱私[406]

標　　題：通訊監察改制屆滿一月 法院核准率百分之六一點五八
新聞出處：司法院

修正通訊保障及監察法自９６年１２月１１日起施行，偵查中案件，改由法官核發通訊監察書；綜理國家情報機關首長爲國家安全對在境內設有戶籍者核發通訊監察書，改由高等法院專責法官決定是否同意。司法院爲落實通訊保障及監察法修正精神及司法院釋字第６３１號解釋意旨，確保人民隱私之合理期待，並兼顧刑事訴追及國家安全維護之正當需求，已函頒「法院辦理通訊監察案件應行注意事項」，提示法官審核通訊監察案件，應在監察目的必要限度內，本於侵害最少之原則，妥速辦理各類通訊監察案件；並建置法院通訊監察管理及查核系統，監督有無違法監察情事。

鑒於通訊監察侵害人民基本權之程度強烈，司法院所屬各法院自通訊保障及監察法修正規定施行後，均秉持憲法保障祕密通訊自由之基本原則，妥適審查每一聲請通訊監察案件，其符合法律規範者，均迅速核發通訊監察書；認爲不符法律規範者，則迅速批復不予准許，自通訊保障及監察法修正規定於９６年１２月１１日施行起迄９７年１月１０日（１２時）止之一個月間，各法院共受理聲請通訊監察案件１２３２件，全部核准者共６５１件，部分核准（部分駁回）者共１９２件，全部駁回者共３７０件，核准率爲百分之６１．５８。尚未准駁之案件，法院將在法定時限內妥善處理之。

聲請通訊監察之案件，最多者爲毒品危害防制條例案件，及違反公職人員選舉罷免法案件，由於法律對得監察之罪名係採列舉規定，故各法院對於以法律未列舉之罪嫌聲請通訊監察之案件（例如施用毒品），均不予准許。

各法院就駁回聲請案件，均一併通知駁回之理由要旨，法官據以駁回之理由，最多者爲「欠缺就監察犯罪曾經嘗試其他蒐證方法而無效果之具體事實；或不能或難以其他方法蒐集或調查證據之具體理由」，其次爲「無可信其通訊與聲請監察犯罪有關連性之具體事證」及「無事實足認有通訊保障及監察法第５條或第６條所定罪名之嫌疑」。

司法院所屬各法院爲保障人民之祕密通訊基本權，於通訊監察結束後，將確實依據通訊保障及監察法第１５條暨通訊保障及監察法施行細則第２７條規

[406] 通訊保障及監察法第 5,6,15 條 ・通訊保障及監察法施行細則第 27,28 條 ・法院辦理通訊監察案件應行注意事項第 1-3,9,25 條 ・釋 字第 631 號 ・95 年 台上 字第 6903 號 ・93 年 台上 字第 2949 號 ・臺灣高等法院暨所屬法院 96 年法律座談會刑事類提案 第 40 號 ・臺灣高等法院暨所屬法院 96 年法律座談會刑事類提案 第 42 號 ・院台廳刑一 字第 0960025264 號
・沿街搜郵筒查恐嚇扁疑犯 警方：一切合法/ 2008-01-16

定，通知受監察人，通知之內容將包含「有無獲得監察目的通訊資料」，以落實保障人權。

18.沿街搜郵筒查恐嚇扁疑犯 警方：一切合法[407]

標　　題：刑大回應９６年１月３日蘋果日報Ａ６版，「目擊警監看郵筒；私閱民眾明信
　　片」聲明新聞資料
新聞出處：內政部警政署

蘋果日報自９６年１２月７日起陸續接獲恐總統家屬及其他政治人物明信片，案經蘋果日報報社分別向刑事警察局及本局刑事警察大隊報案後，由刑事警察局、本局刑事警察大隊、台北縣政府警察局中和分局等有關單位共同成立聯合專案小組，並於１２月１３日起多次舉行專案會議，積極展開分工偵查。

因該明信片投遞地區計有中和、永和、台北郵件處理中心（含中正區、萬華區、大同區、大安區、信義區、松山區、中山區等７個行政區）等地，總計有８３１個郵筒（台北市地區７１１個、中和地區１１２個、永和地區７８個郵筒）。此無論於數量及幅員上，單靠郵務人員於收件時執行過濾清查工作，所需人力與資源勢必是一大難題，於是認爲派警力主動配合郵務單位清查，以期及早發現追查。

經聯合專案小組請示檢察官有關適法問題，並經臺灣郵政公司（政風室）內部協商同意認爲可行後，始由警方派員於９６年１２月２４日至２６日止及９６年１２月３１日、９７年1月2日（共5日），配合郵務士收取信件之時段及作業程序派員隨同，先由郵務士過濾類似恐嚇明信片，再由執勤員警採以複式觀察，期能於第一時間掌握該等類似爲「恐嚇明信片」筆跡可疑明信片之投遞郵筒位置，並予記錄，以能遂行後續偵查作爲。員警於執勤過程中，並未有查扣、搜索甚至開拆任何郵件情形。

另有關本案實施請求郵政機關協助配合檢視明信片查處恐嚇案有無違法說明：

（一）按無故開拆他人之封緘信函者處拘役或三千元以下罰金，刑法第３１５條定有明文。惟本案事例並無開拆之情事，且警察基於偵辦恐嚇罪而取得郵政機關之同意下之偵查作爲，尚無採強制處分，於法尚非無據。

（二）另有無涉及通訊保障及監察法 1 節，明信片之內容尚非係屬有隱私或秘密之合理期待之範疇（參照該法第３條第２項），亦無該法之適用。

[407] 中華民國刑法第 151,305,315,346 條・通訊保障及監察法第 2-3,13-14 條 ・通訊保障及監察法施行細則第 2-6 條 ・釋 字第 631 號 ・65 年 台上 字第 1212 號 ・94 年 選訴 字第 994 號 ・院台廳刑一 字第 0960025264 號 ・電視台二記者 製黑道嗆聲案依恐嚇罪判刑/ 2008-01-04

附件五　法源資訊網站裁判新聞彙整（以領域分）

19.讓黑心產品都銷聲匿跡 消保會新年新希望[408]

標　　題：「２００７年十大消費新聞排行榜」揭曉－個資外洩、黑心產品及預付型交易衍生
問題均入選行政院消保會宣示「創造安心消費環境」！
新聞出處：行政院消費者保護委員會

您知道今（９６）年度最重大的消費新聞議題是什麼嗎？答案揭曉！不但包括「網路及電視購物產生之消費者資料外洩」、「黑心產品問題」，還有近日最令人震撼的亞力山大事件所代表的「預付型交易因業者倒閉所產生之爭議」議題也名列其中！爲解決民眾心中的擔憂，行政院消費者保護委員會１２月１８日特別宣示明（９７）年度將以「創造安心消費環境」爲主要施政目標，不但要讓黑心產品及服務漸次消聲匿跡，更要讓消費者在沒有安全顧慮的環境下快樂、安心、自在的消費！ 爲了解本年度最重大的消費新聞議題，作爲明年度優先重點工作之參考，行政院消保會日前特別邀集產、官、學及民間消保團體等各界的專業人士舉辦座談會，評選出「２００７年十大消費新聞排行榜」，並於１２月１８日假行政院新聞中心舉辦的年終記者會上揭曉。

記者會當天首先由１０位表演者用角色扮演的方式，搭配相關的主題道具，以動態的肢體動作呈現出今年的十大消費新聞，表演者以生動活潑的演出爲記者會拉開序幕，並同時展示行政院消保會的「十大消保對應措施」，逐項說明政府相關部門所建立的因應機制,提醒消費者如何維護自身的消費權益。

行政院消保會秘書長楊美鈴致詞時表示，從剛出爐的十大消費新聞中，可以看出本年度最重大的消費議題主要是消費者的個人資料保護問題，在電視購物頻道或網站交易時造成個人資料外洩;再者,就是產品及服務的安全問題，如豬肉含磺胺劑、大陸毒牙膏、油品違法添加甲醇等事件；第三則是預付型交易的風險問題，例如最近最令人感到震驚的亞力山大倒閉事件；另外，今年度名人代言廣告的問題仍持續發燒，如謝老師減肥藥事件；最後，通訊產品的消費資訊問題也是大家關注的焦點，例如可攜式門號網內或網外互打的問題、互動簡訊之資費問題等，而這些消費過程中隱含的變數，在在導致消費者無法放心、安心地消費。

[408] 消費者保護法第 11.1,12,36,58 條 ・零售業等商品（服務）禮券定型化契約應記載及不得記載事項第 1 條 ・健身中心定型化契約範本第 1 條・健身中心定型化契約應記載及不得記載事項第 1,2 條 ・臺北市政府處理違反消費者保護法及臺北市消費者保護自治條例事件統一裁罰基準第 2,3 條 ・經商 字第 09602420380 號 ・經商 字第 09602405691 號 ・汽油摻水及禮券遭拒案 消保會將加強查核・知名百貨驚傳跳票 民眾要求兌換禮卷遭拒/2007-12-19

爲解決消費者的憂慮，符合廣大消費民眾的期待，楊秘書長指出，來年行政院消保會將以「創造安心消費環境」爲施政目標，並以「完備個資保護機制」、「持續黑心產品之管控」、「強化弱勢族群之教育宣導」、「健全消費者保護法制」、「加速定型化契約之研修與查核」以及「加強公安查核」等６大重點作爲該會未來具體工作項目，與消費者站在一起並肩打造最舒適、安心的消費環境。

其中，值得一提的是，對於本年度最重大、並造成廣大消費者恐慌的消費問題－購物頻道及網路書店之個資外洩事件，行政院消保會除第一時間協調業者儘速研擬改進措施，主管機關加強查核措施外，並請法務部儘速推動電腦處理個人資料保護法的修正，包括擴大行業適用範圍、指定電視購物頻道及網路購物等業者爲電腦處理個人資料保護法之適用範圍、加重罰責以及減輕被害人的舉證責任等。行政院消保會強調，未來將特別致力於完備個資保護機制，持續促請其他相關單位建立完善之個資保護機制，讓消費者安心購物。

另就黑心產品問題，爲解決消費者對於市面上進口產品品質的疑慮，行政院特別在今年底邀集相關部會，成立「進口產品安全跨部會專案小組」，並架設「不安全進口產品資訊網」，由行政院消保會主責，促請各主管機關於邊境管制或市場抽驗時發現或接獲國外通報的瑕疵商品訊息時，立即公佈於網站，讓消費者迅速掌握到相關訊息，以便在消費時作出正確的決定。目前已有超過４８２則瑕疵產品訊息登載於網站上供參。另外，１９５０全國消費者服務專線，亦提供民眾電話查詢的服務，讓無法上網的消費者，也能方便查詢。

行政院消保會說，該會未來除繼續強化該專屬網站的檢索功能外，對於管控密度不足的黑心商品、食品及中藥材等，也將持續積極協調主管機關強化及落實突發事件之應變及執行橫向聯繫機制、流向追蹤管理及標章認證等管制措施，務求讓黑心產品及服務漸次消聲匿跡。

至於近來亞力山大倒閉事件則是使預付型交易及假分期真貸款的相關問題再度受到關注，對此，行政院消保會除於第一時間與相關單位協商保障消費者權益之因應措施，協助消費者解決問題外，未來並將朝健全消保法制的方向努力，例如促請主管機關下修健身中心定型化契約應記載及不得記載事項內有關履約保證的金額及時間等，以提供消費者更多的保障。

※「２００７年十大熱門消費新聞排行榜」如下：

（一）網路及電視購物產生之消費者資料外洩如東森購物、博客來等事件。

（二）農漁水產品之藥物殘留，如豬肉（磺胺劑）、白蝦及大閘蟹（硝基？喃）。

（三）黑心產品問題，如大陸毒牙膏、湯瑪士小火車玩具、層積材等。

（四）預付型交易及假分期真貸款，因業者倒閉所產生之爭議，如亞力山大、中興百貨倒閉等。
（五）油品違法添加甲醇。
（六）禮券定型化契約應記載及不得記載事項，全面實施。
（七）遊覽車旅遊之公安意外。
（八）旅行社陸續無預警倒閉事件，如喜洋洋、辰欣事件。
（九）名人代言之商品瑕疵或疑廣告不實，例如「謝老師」事件。
（十）通訊資訊不充足，如可攜式門號網內或網外互打的問題、手機簡訊和來電答鈴之資費問題。

20.全球電子郵件 美國調查：95%是垃圾郵件[409]

美國加州一家網路安全公司，將每天從全球各地約五萬名客戶所收到的十億多封郵件加以分析，十三日公布結果指出，今（二○○七）年全球電子郵件中，有將近百分之九十五是「垃圾郵件」。雖然美國已自二○○四年施行垃圾郵件管制法，嚴懲垃圾郵件的寄件者，不過，垃圾郵件的數量每年依然持續暴增。

在台灣，國家通訊傳播委員會（ＮＣＣ）昨（十三）日首度針對國內二十家網際網路業者所提報的資料進行調查，結果發現，國人也飽受垃圾郵件攻擊之苦。據資料統計顯示，網友今年十月、十一月份各收到約九十五億、九十七億封電子郵件，其中超過八成是垃圾郵件，而且還不包括沒被網路業者攔截的色情郵件。而垃圾郵件之中，有高達百分之九十五，是來自國外的。

參照行政院會通過之濫發商業電子郵件管理條例草案第９條第１項規定，垃圾郵件的受害者，可委由財團法人或公益社團法人提起訴訟，且損害賠償總額，依該條例第７條第３項規定，以每人每封商業電子郵件新台幣五百元以上二千元以下計算，但如果能證明受有更高損害者，則不在此限。ＮＣＣ官員表示，該項草案雖已於民國九十四年送交立法院，不過，至今仍不見天日，希望能夠加速立法。

ＮＣＣ官員指出，處罰垃圾郵件發信者，可能會有侵害憲法第１２條賦予的「通訊自由」，不過，垃圾郵件涉及多方法律關係，與收件者隱私權、資訊不外露權利相關，二者孰高孰低，可參照司法院大法官釋字第５７７號、第４１４號有關禁止菸商廣告與藥物廣告的解釋，且商業電子郵件只是代第三人轉送郵件，在社會上評價本來就比藝術等表達爲低，更何況大量寄送垃圾郵件所造成的損害，已遠大於其所表達言論的利益，二相權衡之下，立法規範垃圾郵件應該沒有憲法上的爭議。

[409] 中華民國憲法第 11,12,23 條 ・電腦處理個人資料保護法第 24,28,30,33 條 ・電子商務消費者保護綱領第 2,3,5 條 ・釋 字第 577 號 ・釋 字第 414 號 ・「濫發商業電子郵件管理條例」草案・垃圾郵件氾濫 NCC 擬設專責單位受理檢舉法源編輯室 / 2007-12-14

21.個人資料外洩引發詐騙 法務部：修法重懲[410]

標　　題：發揮個人資料保護法的功能，捍衛人民的隱私權益
新聞出處：法務部

近日來社會上發生許多重大的個人資料外洩事件，不論是銀行業者、電視購物頻道、網路書局大量的個人資料均遭不法份子竊取或轉售給詐欺集團利用，致使許多民眾受害，因此要求政府加強重視個人資料保護的聲音，逐漸高漲，亦呼籲要追究業者未盡個人資料保護的法律責任。法務部早在９０年間就已注意個人資料保護問題，並積極著手修正現行之「電腦處理個人資料保護法」，並於９４年完成該法修正正草案並送請立法院審議，惟至今仍未完成立法程序，未能充分發揮保護個人資料的立法意旨。有鑑於此，法務部將積極與立法院朝野黨團繼續協商，期能儘速完成個人資料保護法修正草案的審議公布施行，對目前個人資料滿天飛，詐騙集團隨手即可蒐集個人隱私的狀況，必可發揮立竿見影的效果。

爲貫徹個人資料保護法保護個人隱私權益的立法意旨，次此修法針對現在社會上洩漏個人資料的問題做了大幅度的增修，對民中隱私權益保護的重要規定有下列幾項：

１．取消僅部分非公務機關適用該法的限制，任何民間公司、團體或個人均適用個資法，將不再發生電視購物公司、網路書局外洩客戶資料，受害人卻不能依本法追究該公司責任的不合理現象。

２．增訂業者的搜集告知義務，及若發生資料外洩事件時業者有義務適時通知當事人的規定，讓民眾能得知誰在蒐集他的個人資料，資料外洩時也能及時被通知而採取必要的防範措施。

３．個人資料保護客體不再限於經電腦處理之個人資料，亦即人工處理資料亦納入保護範圍。

４．對於買賣個人資料的違法行爲，提高爲５年以下有期徒刑的刑事責任，並取消現行法須告訴乃論的規定，期使檢警能主動偵辦，追出洩露個人資料的黑手。

在面臨資訊化社會的今天，個人資料保護已成爲一個非常重要的議題，各國際組織如ＯＥＣＤ、ＡＰＥＣ亦制定了有關個人資料保護綱領或原則。我國是一個資訊業大國，更應重視個人資料的保護工作與國際社會接軌。現行之

[410] 電腦處理個人資料保護法第 1-3,23,33-36,38 條 ・94 年 上易 字第 1237 號 ・法律決 字第 0950026402 號 ・(90) 法檢決 字第 000716 號 ・台財融 字第 86620894 號 ・「個人資料保護法」草案 (原名稱:「電腦處理個人資料保護法」)・電視購物台外洩客戶個資 法部擬加重刑度/ 2007-12-12

「電腦處理個人資料保護法」是在８４年間制定完成，現時的社會環境、網路科技與昔時大不相同，現行法難以遏阻日益猖獗的個人資料外洩事件，對民眾隱私權益之保護確有疏漏。法務部誠摯希望立法院朝野黨團能重視此一問題，及早完成個人資料保護法的修法程序公布施行，徹底打擊詐騙集團並讓民眾免於資料被任意揭露的恐懼，並符合國際社會保護個人資料之要求。

22.維護當事人隱私 司法院：一律皆平等對待[411]

標　　題：關於９６年１２月１０日平面媒體，刊登「維護當事人隱私　不該有特權」一文之
　　澄清稿
新聞出處：司法院

關於９６年１２月１０日平面媒體，刊登「維護當事人隱私　不該有特權」１文，與本院業務有關者，特予澄清如后：

一、本院網站法學資料檢索系統之裁判書查詢，有關臺灣高等法院９６年度矚上重訴字第１７號證券交易法案，無法以「趙玉柱」、「趙建銘」爲全文檢索語詞查得，卻得以「蔡清文」爲語詞檢索查得的原因如下，絕無所謂「差別待遇」情事，特此澄清。

（一）依本院於９５年１１月２８日召開「研議裁判書公開兼顧個人隱私政策方案」會議結論，自９６年７月１日起儘量隱匿個人資料，包括當事人及訴訟關係人之姓名。則自９６年７月１日以後無法以「趙玉柱」、「趙建銘」爲全文檢索語詞，查得臺灣高等法院９６年度矚上重訴字第１７號證券交易法案，自屬必然。

（二）至於以「蔡清文」爲語詞檢索，卻可查得前揭案件，係因「蔡清文」一詞，曾出現於表格欄內，而囿於技術，表格內的姓名換行，尚無法隱匿所致。

二、上文指前揭案件本來沒有上網，是媒體反應後才在９６年７月１０日上網及其他內線交易案的判決書中也有「公平性交易」字眼，依然查得判決等情，經查本院爲避免性侵害相關資訊不慎被公開，故以程式將判決書內容有「性交」字詞者列爲不公開，惟爲補救與性侵害無關的判決書被程式誤刪，因而於不公開之個案案號下方告知民眾：「該案經程式自動判定爲不得公開案件，民眾若認係程式誤刪，可利用本院信箱反應，由本院相關業務廳判斷補正」。經本院以「公平性交易」及「擬制性交易」爲檢索語詞，確可查得本台開案的一、二審判決書，其原因即是本院依民眾的反應，事後補正者。

[411] 刑事訴訟法第 50,51,308-310.1 條 ・最高法院辦理民、刑事訴訟案件注意事項第 4,5 條・刑事訴訟簡化判決書製作方式暨簡易程序案件判決格式第 1 條 ・79 年 台上 字第 3543 號
・73 年 台上 字第 5222 號 ・臺灣高等法院暨所屬法院 55 年度法律座談會 刑事類第 5 5 號
・(48) 台令刑 (五) 字第 5177 號 ・電視購物台外洩客戶個資 法部擬加重刑度/ 2007-12-11

三、以「趙玉柱」、「趙建銘」爲全文檢索語詞，於本院網站首頁的「司法院新聞」，即可查得臺灣高等法院９６年度矚上重訴字第１７號證券交易法案趙玉柱、趙建銘判決結果等相關新聞，所謂「爲特權把關」遮掩云云，顯有誤會。

23.警察勤務區家戶訪查辦法 內政部依法通過[412]

標　　題：內政部部務會報通過「警察勤務區家戶訪查辦法」
新聞出處：內政部發言人室

一、警察勤務條例（以下簡稱本條例）第１１條第１款修正案，業奉 總統於本（９６）年７月４日令公布生效。依修正內容，本部應賡續訂定家戶訪查辦法，以符規定。

二、按修正前本條例第１１條第１款規定略以：「警察勤務方式如左：一、勤區查察：於警勤區內，由警勤區警員執行之，以戶口查察爲主，並擔任社會治安調查等任務。…（第二款以下略）」，業經修正爲：「警察勤務方式如左：一、勤區查察：於警勤區內，由警勤區員警執行之，以家戶訪查方式，擔任犯罪預防、爲民服務及社會治安調查等任務；其家戶訪查辦法由內政部定之。…（第二款以下略）」，合先敘明。

三、本條例第１１條條文修正後，在臺灣地區實施逾六十年之久的警察機關戶口查察制度，須全面變革，「戶口查察」名稱實已正式走入歷史。修正公布後之條文，保留「勤區查察」勤務名稱，並授權內政部訂定家戶訪查辦法法規命令。本條例刪除「勤區查察以戶口查察爲主」等文字後，未來警勤區員警將改以「家戶訪查」方式取而代之，來達成「犯罪預防」、「爲民服務」及「社會治安調查」等任務，工作重點明確，不再以「查戶口」爲勤務重點。

四、爲符民主法治潮流，積極保障人權，本辦法納入行政法諸多重要原理原則規範，融入社區警政精神，積極爲民服務，兼顧達成維護社會治安目的與民眾隱私權之保障，闡明資料蒐集、保護與資訊公開之規定與限制，使警勤區經營工作透明化、公開化與多樣化，細心傾聽民眾感受，真正關心社區民眾之所需，乃係警察勤區查察勤務方式之重大政策變革。

[412] 警察法第 9 條 ‧警察勤務條例第 11,12 條 ‧戶警聯繫作業要點第 2-4,6 條 ‧釋 字第 535 號 ‧92 年 上易 字第 1790 號 ‧89 年 訴 字第 159 號 ‧總統令修正「警察勤務條例」‧警察家戶訪查帶槍？ 警署：沒規定要帶槍/ 2007-11-23

24.罰單洩漏個資嚴重 交通部成詐騙集團打手[413]

交通部郵寄罰單，驚爆個人資料在過程中「一洩千里」！據統計，全台每年有數萬件的違反汽機車投保強制險罰單、催繳汽、燃料稅罰單都以列印表單直接寄發，包括身分證字號等個人資料「赤裸裸」地公布在上頭，成了治安大漏洞。

台北縣民謝先生指出，因漏繳機車強制險，依強制汽車責任保險法第４９條第１項第１款規定，收到交通部台北監理所寄來的罰單，該張罰單是以電腦報表用紙列印，再直接表單對折寄出，一面是他的名字和地址，一面是載明他身分證字號、姓名、車號、地址與違規事實的罰單內容，全都揭露在信上。他曾質問監理所此舉是「剝奪人民的隱私權」，但官員卻指「規定就是這樣做」，置之不理。

負責郵寄的台灣郵政證實有此漏洞，郵務處官員指依道路安全交通安全規則第７條及道路交通管理處罰條例第９條前段規定，一般違反交通規則都會開寄發道路交通管理事件通知單，並以透明式信封郵寄，但他們卻發現部分罰單直接用電腦表單寄發，個人資料沒有密封，也沒有塗銷部份數字，郵局曾建議監理單位改進，對方卻回答成本太高。

消基會直指太離譜，交通部這種做法已明顯違反電腦處理個人資料保護法第６條、第８條本文「公務機關對個人資料之利用，應於法令職掌必要範圍內爲之，並與蒐集之特定目的相符」之規定，他呼籲受害人應檢具相關資料，一旦發現個資因此被盜用或受害，可依同法第２７條第１項、第２項規定，向交通部請求財產上及非財產上之損害賠償。

謝先生不滿的說，他的身分證曾被盜用，被拿去做非法用途，所以有切身之痛，政府機關非但沒盡到保護人民與便民的責任，還把民眾個資露光光，交通部公路總局乾脆改名「露透社」。公路總局指出，通常是民眾開車或騎車在路上被攔檢，或交通違規被抓到，警察連線到監理單位發現車主有未繳款項，才會由監理單位將罰單或催繳單以列印報表寄發，這類罰單一年數以萬計，公路總局將要求未來寄發必須塗去部份個人資料。

[413] 電腦處理個人資料保護法第 3,6,7-17,27 條 ・強制汽車責任保險法第 49-51 條 ・道路交通管理處罰條例第 8,9 條 ・道路交通安全規則第 1,2,7 條 ・法律 字第 0940046975 號 ・法律 字第 0940017828 號 ・交路 字第 0930034993 號 ・四千筆個資外洩 刑事局逮捕七嫌擴大追查法源編輯室 / 2007-11-05

25.使用者變站長 批踢踢實業坊驚傳個資外洩[414]

國內最大網路討論區批踢踢實業坊（ＰＴＴ）今（二十二）日凌晨驚傳大烏龍，所有使用者突然擁有站長權限，導致部份知名網友資料外洩，稍晚站方緊急關站，公告下午五點會重新開站。

ＰＴＴ系統權限在凌晨一點三十五分突然出現不明原因錯誤，使得所有使用者全都擁有站長權限，每個使用者均能任意觀看、搜尋、新增、修改或刪除全站數十萬筆個人資料和權限，甚至可以發送虛擬的ＰＴＴ貨幣。ＰＴＴ站方直到一點五十五分才關站，已傳出部分知名網友的隱私權被侵犯，部分網友甚至在看板上公佈他人隱私資料；部分看板也傳出災情，看板功能設定遭更改，文章被大量刪除或標記，如知名的八卦版則被解除靜態功能，ｉｎ２版部份資料傳出外洩等。

批踢踢（ＰＴＴ）是以學術性質爲目的，提供各專業學生實習的平台，創立於一九九五年九月十四日，採電子佈告欄系統（俗稱ＢＢＳ），提供網路快速、即時、平等、免費，開放且自由的言論空間，二○○○年成立ＰＴＴ２，以提供個人或團體等私人性質爲主看板，二○○四年又成立ＰＴＴ３，主要提供海外學生專用。由於ＰＴＴ廣受網友愛戴，除原本ＢＢＳ功能外，也提供個人ｗｉｋｉ服務。

法界人士表示，警察機關因偵辦刑案需要，可否逕向電子佈告欄站主蒐集個人資料，法務部８７年６月２９日（８７）法律字第０２１３７５號曾作出釋示，按警察機關因偵辦刑案需要而依刑事訴訟法第２２９條或第２３０條規定，向公務機關或受電腦處理個人資料保護法規範的非公務機關請求提供相關個人資料，該受請求提供的公務機關或非公務機關即可分別援引電腦處理個人資料保護法第８條第１款、第２３條第１款規定提供。惟如非屬電腦處理個人資料保護法規範的行業，似尚難援引該法請求提供。

[414] 電腦處理個人資料保護法第 3,8,23,33,34,35 條 ・刑事訴訟法第 229,230 條 ・政府網際服務網管理規範第 5 條 ・教育部網路學習環境及內容建置補助要點第 1,2 條 ・(87) 法律 字第 021375 號 ・部落格發言如可受公評 應受言論自由保障法源編輯室 / 2007-08-22

26.董監酬勞將適度揭露 金管會：擬強制列名[415]

個別董監事的董監酬勞將適度解密，金管會研擬年底前修改法規，擴大包括獨董在內的董事酬勞揭露範圍，仿照新加坡及香港作法，在董監酬勞金額八個級距中，強制列出個別董監事的姓名，不再像現在只列出人數沒有公布姓名。

證券交易法第１４條之２第１項修正後的獨立董事制度，今年開始實施，對於獨董的薪酬及能否領取董監酬勞，相關法令並無規範，只有上市上櫃公司治理實務守則第２６條第２項規定，有原則性規定獨董要有合理報酬，不少學者專家建議，獨董的薪酬應該揭露。行政院金融監督管理委員會官員表示，現行董監酬勞只揭露到每一個級距的人數，金管會正檢討，要把人數的揭露改爲姓名，屆時每一位董監事，包括獨董在內，領取的董監酬勞屬於哪個級距，都可清楚看出。

早期董監酬勞是個別董監事逐一揭露，後來因工商界反映可能有遭綁架及隱私權等問題，主管機關修正爲「彙整揭露」，不強制公布每位董監名單，後來再把揭露的級距從五級改爲八級，但因只有人數，沒有姓名，外界仍認爲，上市櫃公司董監酬勞是依績效發放，應攤在陽光下接受檢驗。

官員表示，金管會將在下半年修改年報編制準則等相關法規，強制要求揭露每一級距的姓名，屆時獨董也不會被排除，一樣會揭露。目前董監酬勞，從二百萬元到一億元共分八級，以二百萬元到五百萬元級距爲例，目前只揭露適用的人數，未來將列出姓名，如位於二百萬到五百萬元的有張三等人，外界可以知道張三的董監酬勞位於這個級距，但仍無法確知是二百多萬元，還是四百多萬元。

至於個別獨董的董監酬勞是否要逐一公布？官員表示，獨董跟一般董事應適用相同規範，如果要公布個別獨董的董監酬勞，如張三金額是多少、李四是多少等，是否適當，可能需要更嚴謹的研究。此外，對於獨董應不應該領董監酬勞，官員表示，獨董也是董事，法律責任跟一般董事一樣，不能刻意剝奪獨董享有盈餘分配的權利，責任跟報酬應衡平。這屬公司自治事項，由公司自行決定，實際上，獨董如果只有固定薪資，沒有董監酬勞，收入相對會比一般董事少。

[415] 證券交易法第 14.2,178,181.2,183 條 ・上市上櫃公司治理實務守則第 26 條 ・公開發行公司年報應行記載事項準則第 11 條 ・經商 字第 09602414750 號 ・經商 字第 09402199670 號
・經商 字第 09400586770 號 ・金融機構首例 產險公司未設獨立董事遭罰法源編輯室 / 2007-08-20

27.偵查中 檢察官可核發監聽票 釋 631：違憲[416]

針對偵查中案件，可由檢察官核發監聽票。司法院大法官今（二十）日舉行第一三〇九次會議作成釋字第６３１號解釋認爲，民國八十八年七月十四日制定公布之通訊保障及監察法第５條第２項規定，與憲法第１２條保障人民秘密通訊自由意旨不符，至遲於十二月十一日新法施行前失效。
一名警局資訊室警員，於九十年間接獲Ａ女子用行動電話撥打他的手機，要求協助查詢另一高姓女子個人資料，該名警員因此使用他的電腦連線內政部警政署，並將相關資料告知Ａ女子。此舉經檢察官核發監聽票，監聽警員的行動電話而被查獲。台灣高等法院以監聽譯文爲證據，認定該名警員構成刑法第１３２條第１項洩密罪，駁回他的上訴。
該名警員認爲，監聽票應一律由法官核發，通訊保障及監察法第５條第２項有關「通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權核發」的規定已違憲。且檢察官當初是以槍砲等重罪名義核發監聽票，但法院卻將不屬同條第１項各款所列重罪而取得的監聽譯文，作爲認定他有罪的證據，有牴觸憲法疑義，聲請解釋。
大法官釋字第６３１號解釋也認爲，民國八十八年七月十四日制定公布之通訊保障及監察法第５條第２項規定，沒有要求監聽票原則上應由客觀、獨立行使職權的法官核發，卻讓職司犯罪偵查的檢察官與司法警察機關同時負責監聽票之聲請與核發，難謂爲合理、正當的程序規範，與憲法第１２條保障人民秘密通訊自由之意旨不符，應自解釋公布之日起，至遲於九十六年七月十一日修正公布之新法施行之日失其效力。

[416] 中華民國憲法第 12,22 條 ・中華民國刑法第 132 條 ・通訊保障及監察法第 1,2,5,7 條
・釋 字第 603 號 ・司法院大法官解釋第 631 號 ・12 月起「監聽」須報請法官核准 總統公布法源編輯室 / 2007-07-20

28.爆料少了保護傘 立委擋修個資法告知條款[417]

法務部研修「個人資料保護法草案」，增訂間接取得之個人資料，於處理或利用前應向當事人告知資料來源，否則應負行政及刑事責任。但此一新增條文因爭議頗大，立委擔心會影響爆料的訊息來源，上會期就卡在立法院，未能順利完成二、三讀。

民國九十四年二月間行政院院會討論通過草案第９條規定，除非有「有前條第二項所列各款情形之一」、「當事人自行公開或其他已合法公開之個人資料」、「學術研究機構基於公共利益爲統計或學術研究之目的而有必要，且資料經處理後或依其揭露方式無從識別特定當事人」、「不能向當事人或其法定代理人爲告知」、「大眾傳播業者基於新聞報導之目的而蒐集個人資料」各款得免爲告知外，公務機關或非公務機關依第１５條或第１９條規定蒐集非由當事人提供的個人資料，應於處理或利用前，向當事人告知個人資料來源及第８條第１項第１款至第５款所列事項。

據了解，這項修法受阻主要是因部分立委認爲，此舉不利於立委接受爆料，因此建議將國會議員除外，不受上述規範。官員指出，以「爆料天王」爲例，其經常揭發第一家庭成員及特定政治人物的弊案，其中有真、有假，若依新增的告知規定，其在使用個人資料前，應先告知當事人，就沒搞頭了。

法務部指出，此項新增規定，是爲避免個人資料遭不法濫用而有損權益，因此規定凡不是向當事人直接蒐集，而係向第三人蒐集的個人資料，需告知當事人資料來源，使其了解其個人資料被蒐集的情形，並得以判斷供該資料來源是否合法，及早採取救濟措施。個人隱私具有普世價值，法務部認爲向第三人取得的個人資料，內容是否正確，不無問題，如隨便使用，勢必會影響個人名譽。

主張將國會議員排除適用的立委表示，立委「揭弊」是行使職權，難免有來自各方的訊息，但消息來源都不能透露，如果法律條文明定必須說明來源，必將使提供訊息者卻步，不利揭弊。至於，立委揭弊是否行使職權，在立法院職權行使法中並沒有明確規範，法務部認爲，若立委不受規範，應在職權行使法中訂定規定，而非訂在個資法中，因此反對將國會議員排除於個資法「告知」的適用規定。

[417] 中華民國憲法第 73 條 ・電腦處理個人資料保護法第 7,8,11,18,34 條 ・釋 字第 435 號
・釋 字第 401 號 ・95 年 台上 字第 2365 號 ・「個人資料保護法」草案 (原名稱：「電腦處理個人資料保護法」)・洩漏第一家庭無限卡資料 銀行挨罰 200 萬法源編輯室 / 2007-07-10

29.Google「街景服務」 在美爆發隱私權爭議[418]

網路搜尋引擎 Google 與美國軟體巨擘微軟公司再度爲了爭取線上客戶開戰，二十九日同一天推出網路地圖服務新功能，包括逼真的美國大城街頭實景。

Google 的「地圖與地球」網頁（網址 http://maps.google.com ）二十九日首度推出「街景」服務，提供美國各大城市的景觀，包括舊金山、紐約、拉斯維加斯、丹佛、邁阿密，以及知名的科技重鎮加州北部矽谷。只要輸入地址，就可以有如置身當地，看到街頭實景，不像過去只有鳥瞰圖。 Google 表示，街景服務「很快將擴及其他都會地區」，街景的使用者幾乎可以行遍城市的大街小巷，抵達前先在餐廳訂位，甚至將焦點推近至巴士站牌與路標，以擬定旅行計劃。

不過，街景服務也引來侵犯隱私的問題。例如，Google 製作街景服務的方式，是派出配備攝影機和全球定位系統的卡車到街上，獲取數量龐大的畫面資料再組合起來，讓使用戶可看到一個地點的全景。然而，當時在當地活動的人、停在路邊的車子甚至房子裡的居民，有的在不知情之下被拍攝存進 Google 的資料庫，如此做法是否合宜已在美國引發討論。

在台灣，實務上曾發生一個案例，某一家房訊公司單純僱請工讀生拍攝房屋外觀等相片資料提供查詢服務，產生了是否構成侵害他人隱私的疑義。對此，法務部９２年７月４日法律字第０９２００２６１９２號函示，如其並未與自然人之姓名等相結合，尚不足以識別該個人者，則該資料即非電腦處理個人資料保護法第３條第１款規定所稱的個人資料。

然，該案在臺灣高等法院９３年度上易字第１８９６號刑事判決中，提出相左見解，認爲這些照片雖不足以識別各房屋之歸屬對象，惟該公司嗣將房屋相片與法拍屋債務人之資料相互結合，架設於網路上供會員查詢，其呈現之內容涵括個人之識別資料、財產狀況、住家及設施情形，將使得「個人資料」身份明確化，自應受電腦處理個人資料保護法第１８、３３條的規範。

[418] 電腦處理個人資料保護法第 3,18,33 條 ・電腦處理個人資料保護法施行細則第 30,31,32,40 條 ・電腦處理個人資料保護法之特定目的及個人資料之類別第 1 條 ・93 年 上易字第 1896 號 ・臺灣高等法院檢察署暨所屬各級法院檢察署 86 年刑事法律問題座談 ・法律 字第 0920026192 號 ・法拍網輸地址看相片檢察官十查八中函辦法源編輯室 / 2007-06-01

20.員警勾串徵信業者違法監聽 名人隱私不保[419]

臺灣板橋地方法院檢察署與刑事局、台北市刑警大隊共同破獲一個暴力討債集團。該集團透過徵信社，向電信業者員工以及松山分局的員警，以一筆新台幣二千元的代價購買個人資料。檢方昨（十七）日晚間一口氣偵訊十四名嫌犯，其中彭姓員警以十萬元交保，五名徵信業者則遭到聲押。

板橋地檢署日前接獲線報，指稱蔡姓男子及其手下涉嫌接受國內各大徵信業者委託，佯裝成中華電信員工，謊稱要修理電話，進入徵信社業者所提供的電話裝機地點，破壞電信箱後，夾線竊錄，每線收費四千五百元，錄滿每卷再收六百元，從去（九十五）年迄今，不法所得高達三百五十五萬五千元，而違法監聽的對象還包括部分藝人和名人。

檢警監控過程中，發現松山分局有員警與徵信業者有所聯繫，進而查出勾串不法。由於時值「靖紀專案」期間，刑事局在掌握有員警涉案後，即展開監控，並於昨日會同北市刑大偵五隊共同行動。板檢指出，台北市政府警察局松山分局彭姓偵查隊員與在遠傳電信上班的鄭姓員工，涉嫌違背職務販售民眾戶籍、車籍、出入境或電信基本資料給徵信業者，謀取不法利益。台北市警察局指出，去年十二月就發現彭姓員警涉案事實，因此，主動將線索提供給檢方，在彭姓員警交保後，已經先將他調到警備隊，等待後續偵辦，再做懲處。

檢警發動搜索同時，赫然發現竟有某一媒體記者正和業者「泡茶」，檢警也不排除有媒體與徵信業者掛勾，取得藝人、名人資料作爲跟蹤偷拍爆料依據。板檢強調，這次搜索共帶回二十二人偵訊，由於全案涉及違反電信法第５６條之１、通訊保障及監察法第２４條第１項及第３項、電腦處理個人資料保護法第３３條及刑法第１３２條第１項洩漏國防以外秘密等罪嫌，情節重大，檢方將深入追查，擴大偵辦。

[419] 電信法第 6,7,56.1 條 ・中華民國刑法第 132,133,315.1,318.1 條 ・通訊保障及監察法第 2,24 條 ・電腦處理個人資料保護法第 7,8,18,23,33,35 條 ・法務部 (84) 檢 (二) 字第 0552 號
・臺灣高等法院暨所屬法院 84 年度法律座談會 刑事類第 8 號 ・臺灣高等法院暨所屬法院 90 年法律座談會刑事類提案 第 19 號 ・電話竊聽、盜打真方便？ 電信箱輕易打開法源編輯室 / 2007-05-18

21.刷卡存根聯未隱藏卡號 消基會：恐遭盜刷[420]

信用卡詐騙手法日新月異，消費者對於個人隱私資料保護，也愈加注重。消基會特別針對大台北地區賣場、百貨公司和超市的信用卡簽單和發票的卡號資料「全都露」調查，結果發現新光三越百貨任一分店的刷卡存根聯，皆完整揭露消費者卡號，消基會表示，此舉容易造成被盜刷或製造僞卡的危險，將要求新光三越三月底前全面改善。

消基會表示，爲解決信用卡帳單的卡號資料外洩問題，主管機關曾發布財政部金融局９２年０７月０７日台財融（四）字第０９２４０００９０８號函明示：「各發卡機構（貴行（社））自九十二年十一月十五日起，寄發之信用卡帳單及繳款聯上，不得完整列示客戶信用卡卡號或身分證統一編號，並應於九十二年十月底前完成系統更新。」。但消費者又發現刷卡仍存發票和簽帳單有資料外洩之虞，主管機關因而進一步要求，自九十五年一月一日起，新安裝之刷卡端末機必須完成隱藏卡號的功能，至九十六年四月一日後，各信用卡業務機構必須完成所有刷卡機隱藏卡號的功能。

換句話說，消費者在今（九十六）年四月一日前，最好將刷卡存根聯保存好，否則的話，很有可能淪爲詐騙集團盜刷的工具！消基會指出，如果網路、電視店家能多一層過濾，要求出具身份證字號或是信用卡末三碼，想要依信用卡卡號進行盜刷者，比較不容易得逞。但問題就出在每個店家是否都有這麼仔細？因此消費者的卡號隨著存根聯流落在外的風險仍在。

依據消費者保護法第７條第１項規定：「商品或服務具有危害消費者財產之可能者，應於明顯處爲警告標示。」。此次調查發現，將消費者卡號全揭露於存根聯上的新光三越，未於存根聯上善盡提醒消費者之責。消基會呼籲新光三越應立即改善信用卡存根聯完整印出消費者卡號的缺失。新光三越表示，此案涉及系統設定問題，但會在三月底前依照金管會要求全面改善。

消基會提醒消費者，應養成妥善處理信用卡帳單、簽單與發票的習慣，切勿任意棄置，以免遭有心人士僞造卡片或冒用。消基會建議，消費者如欲丟棄以上物件，可利用碎紙機處理或將其撕毀成小碎片，方可保萬無一失。此外，若遇到任何刷卡存根聯未做到隱藏卡號情況，請向消基會檢舉，消基會將立即要求業者改善，以防盜刷情況發生。

[420] 消費者保護法第 7,10,10.1 條 ・特約商店徵信及管理作業準則第 3 條 ・疑似僞卡側錄點（CPP） 之通報調查作業程序及要點第 1 條 ・93 年 台非 字第 190 號 ・台財融（四）字第 0924000908 號 ・台財稅 字第 0920453416 號 ・台財融（四）字第 0924000644 號 ・從『國外僞卡科技植入台灣』談信用卡詐欺犯罪防制問題之研究 ・超市離職員工竊簽單 上網盜刷購買奢侈品 法源編輯室 / 2007-01-16

22.偷拍藝人別墅外露天派對 週刊總編遭判刑[421]

一家週刊五年前以封面報導，指多名女藝人、撞球國手等人舉辦露天派對，因在別墅外偷拍，臺灣臺北地方法院昨（十）日依妨害秘密罪判處總編輯四月徒刑，得易科罰金。這也是該家週刊來台創刊之後，首次被依妨害秘密罪判刑。

民國九十年八月四日晚間，週刊跟拍多名年輕女藝人及撞球國手等人到北投地區的別墅，該刊人員在別墅外的工地上，偷拍該等人在別墅戶外游泳池畔的派對活動，並於八月九日出刊的雜誌中，以「露天搖頭性愛派對」爲封面標題宣稱是獨家直擊，一度引發演藝圈不小的轟動。該期雜誌大賣，多名藝人廣告代言遭到撤銷，藝人認爲形象嚴重受損，陸續提出刑事和民事告訴。

週刊辯稱，別墅外的游泳池公開可見，任何人從四周高處都可輕易看見游泳池畔情形，並不具隱密性，且因相關人士當晚行爲異常，合理懷疑有嗑搖頭丸，才會跟拍。合議庭雖同意相關公眾人物是否吸用毒品及其言行與公共利益有關，但也指出，該別墅設有大門，有圍牆與外界隔離，游泳池的位置在大門入口後數十階梯下方，一般人難以經圍牆或大門看見游泳池。此外，游泳池畔有濃密的樹木遮擋鄰房視線，場地、活動均非其他人可任意進入或觀看，別墅的大門、圍牆及樹木，均足以達到防止路人窺視效果。

法官認爲，一般人在別墅外無從目睹圍牆內活動，當事人在別墅內的行爲主觀上便認定是非公開活動。判決指出，如以公眾人物言行恐遭社會大眾模仿，遽認其言行與公共利益有關，允許媒體因此侵入公眾人物住宅、開拆公眾人物封緘信函，不啻以廣泛的公共利益，剝奪公眾人物的居住安全、隱私等憲法保障之人權。因此，依據刑法第３１５條之２第３項及第３１５條之１第２款妨害秘密罪，判處週刊總編輯四個月有期徒刑，依刑法第４１條第１項前段規定，得易科罰金新台幣一萬八千元。

依刑法第３１５條之１第２款規定，無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者，處三年以下有期徒刑、拘役或三萬元以下罰金。如果對此一竊錄內容加以製造、散布、播送或販賣者，依同法第３１５條之２第３項規定，處五年以下有期徒刑、拘役或科或併科五萬元以下罰金。該竊錄內容之附著物及物品，不問屬於犯人與否，依同法第３１５條之３規定，均沒收之。

[421] 中華民國憲法第 10,12,22 條 ・中華民國刑法第 41,315.1-315.3 條 ・通訊保障及監察法第 24,29,30 條 ・91 年 易 字第 24 號 ・90 年 基簡 字第 334 號 ・88 年 易 字第 679 號
・狗仔偷拍更衣越演越烈 港特首擬著手立法法源編輯室 / 2007-01-11

23.教召員個人資料全都露 國防部：明年改善[422]

立法委員今（九）日指出，國防部後備司令部教育召集令設計不良，在寄發教召令時將個人姓名、戶籍地址、身分證字號等個人資料全部揭露，涉嫌違法。國防部後備司令部動員管理處表示，已就教召令郵寄信封設計不良部分改進，明（九十七）年起就可改善。

立委上午召開「國防部二十萬退役軍人個資全都露」記者會，在記者會上出示一份教召令，信封上有大塊透明膠膜，透過膠膜可清楚看到教召員的名、身分證字號、出生年月日、戶籍地址、軍職專長等資料。立委表示，去年八月接獲民眾陳情，從收到教召令後就陸續受到詐騙集團騷擾恐嚇，教召令赤裸裸讓教召人員個人保密資料，透過郵寄方式，寄到後備軍人家裡，呈現給詐騙集團。

立委說，每年都有教召令未送達被教召人的情形，但教召令對電腦個人資料的保密程度比信用卡帳單還不如，除已違反電腦處理個人資料保護法規定，還可能落入詐騙集團手中而不自知，他主張國防部應即刻改善，這三年來收到教召令的後備軍人，如果個人資料因此被不法集團運用，也可依該法第２７條規定向國防部求償。

後令部動員管理處表示，教召令信封設計是爲了避免被誤當成廣告信件，不過，因被教召人及立委反映有洩露個資之虞，後令部已檢討，並完成新式信封送國防部核准，並承諾全面銷毀舊信封，明年起寄發教召令將全面換發僅露出姓名、郵寄地址的信封，保證不會再發生被教召人個人資料外洩情形。

根據兵役法第３７條第３款及召集規則第２２條第３款規定，後備軍人及補充兵應教育召集，由國防部依軍事需要按年度計畫實施，召集令及有關準備事宜由縣市後備指揮部依地區後備指揮部所定年度教育召集實施計畫完成，並副知轄區內直轄市、縣（市）政府及警察分局。依召集規則第２３條第１項第２款規定，警察分局接到召集令及召集名冊，詳予核對後，分送所屬分駐所、派出所，並督導其將召集令於召集日前十日交付完畢。

[422] 民法第 184,195 條 ・兵役法第 37,39,43 條 ・國家賠償法第 6,7,12 條 ・妨害兵役治罪條例第 2,6,12 條 ・電腦處理個人資料保護法第 3,6,27,30 條 ・召集規則第 22-25 條 ・不識字又跑錯地方 錯過「教召」被送法辦法源編輯室 / 2007-01-09

附件六　資安人網站法律新聞彙整

資安人

全方位防制資料外洩

法律新聞

Last visited on 2009-01-18

[就醫]

[就學]

2008/12/15 Sony 歌迷網站洩兒童個資 開罰 1,000 萬美元
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4722

2008/11/24 補助弱勢 稻、江政大學生個資竟外洩
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4697

2008/09/30 大陸北大、清大校園遭入侵
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4617

2008/06/26 高市國中校務系統遭駭 教育局嚴加防範
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4476

[網路購物]

2009/01/12 戰國策 4,270 筆資料外洩 Google 全都露
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4758

2009/01/06 韓國三星數位相框 藏有惡意病毒
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=474

7
2008/12/18 網友個人資料 Yahoo!奇摩僅保留 3 個月
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4729
2008/11/21 博客來會員個資外流 判賠 13 萬
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4694
2008/09/22 網購電腦 英國銀行客戶資料全都露
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4602
2008/08/25 雅虎奇摩假釣魚網站 上百帳號密碼遭盜
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4547

[金融]
2009/01/06 英國銀行電腦故障 千億英鎊遭透支
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4748
2008/11/17 IMF 遭入侵 疑中國駭客所為
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4691
2008/11/03 日本保險公司資料外洩 兩千女大學生資料全都露
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4664
2008/09/22 網購電腦 英國銀行客戶資料全都露
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4602
2008/09/08 釣魚郵件猖獗 目標鎖定銀行業者
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=458

2
2008/07/29 美國金融網站 7 成 6 有安全漏洞
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=451
4
2008/07/07 匯豐洩個資 2.5 萬段對話記錄遺失
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=448
3
2008/07/04 花旗客戶 PIN 碼遭竊 後端伺服器被入侵
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=448
2

[電信]

2008/12/29 注意小細節 避免掉下電子郵件陷阱
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=474
2
2008/12/18 惡意郵件量增 5 倍 美伺服器最大宗
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=472
8
2008/12/15 奈及利亞電郵 小心受騙上當
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=472
4
2008/12/01 發送垃圾郵件 Facebook 判獲 8.73 億美元
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=470
1
2008/12/01 歐巴馬手機資料 美國電信業者駭走
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=470
4
2008/11/03 Messenger 連線不穩 小心駭客機器人大舉入侵
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=466

5
2008/10/24 網路、整合通訊、安全、服務 塑造企業動態概念
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4650
2008/10/06 中國 Skype 遭監控 百萬用戶資料無所遁形
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4624
2008/08/25 駭客入侵 FEMA 語音信箱被塞爆
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4550
2008/07/29 iPhone 安全漏洞 成網釣攻擊對象
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4515
2008/07/21 多功能智慧型手機 將成駭客新目標
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4504

[其他]

2009/01/12 移民署電腦當機 8 人非法入境
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4755
2009/01/10 Babyhome 網站遭 DDoS 攻擊 暫封鎖國外 IP
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4753
2008/12/22 Google 實景搜尋服務 日民眾要求關閉
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4735
2008/12/18 英婦女上網求職 60 萬遭盜
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=473

0
2008/12/18 2009 年犯罪趨勢 利用就業網站傳送電腦病毒
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4731
2008/11/21 申請國賠洩個資 台北市府網站安全堪憂
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4693
2008/11/10 115 位應徵者資料公開 Google 地圖使用不當惹禍
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4673
2008/11/03 Google 未使用新套件 Android 平台存漏洞
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4668
2008/10/27 共享使用權限 恐產生安全漏洞
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4658
2008/10/27 微軟系統嚴重漏洞 發佈緊急更新
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4661
2008/10/27 微軟黑屏 網路恐怖主義現形
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4660
2008/10/25 Check Point 新推出多款資安防護產品
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4651
2008/10/20 「毒」電腦 企業一年中毒達 86 次
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4644
2008/10/20 無名小站禁用 Javascript 防範惡意程式
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=464

5
2008/10/20 資料庫弱點掃瞄支援 30 種資料庫 強調遵循法規
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4648
2008/10/15 浩網科技協助全國「地政電子謄本」硬體設備整合建置暨營運專案 獲得肯定表揚
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4639
2008/10/09 「有名小站」漏洞全都露
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4630
2008/09/26 僞造證件又一樁 假發票真詐騙
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4614
2008/09/25 「毒」人小布 網路搜尋 No.1
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4606
2008/09/22 台灣雨傘代工總經理監守自盜 竊取公司機密
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4601
2008/09/15 花蓮教育局網站遭攻陷 漏點淫照刊上網
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4593
2008/09/10 Openfind OES 2.5 打造企業安全搜尋新標竿，推出去量資料庫搜尋
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4591
2008/09/08 韓國 1100 萬名個資遭竊 政府官員涉入其中
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4581

2008/09/08 Internet 安全漏洞 使用 BGP 監視資料流
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4585
2008/09/01 兩岸犯罪集團入侵多家機構 建立五千萬筆個資資料庫
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4553
2008/08/11 台北市銷毀 75 萬市民指紋資料
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4529
2008/07/29 英國遭木馬病毒 Asprox 攻陷
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4516
2008/07/24 聯達科技宣布代理美國 AceNet FlowWALL 產品
http://www.informationsecurity.com.tw/DLP/news_detail.aspx?aid=4511

附件七　聯合知識庫網站法律新聞彙整

聯合知識庫

法律新聞

您以 個人資料外洩+日期>=20070119+日期<=20090118+報別=聯合報|經濟日報|聯合晚報|Upaper 共搜尋到 85 筆資料

[網路購物]

1. 被騙扣款有問題男子失財近 60 萬[423]

中壢市高姓男子 8 日夜晚接到冒名某銀行客服小姐電話，告訴他曾透過電視購物頻道買商品，且銀行扣款有問題，要求立刻去自動提款機「解除購物條碼設定」，他因此被騙走近 60 萬元。

中壢警分局長陳金陵呼籲，「購物個人資料外洩詐騙」已成爲歹徒主要的詐騙手法。歹徒會故意製造緊張情況，告訴被害人存款會遭盜領，讓被害人越來越慌亂，加上來電顯示爲銀行電話，讓被害人對假銀行人員深信不疑，才會被騙錢財。民眾若有疑慮均可撥電話「165」向警方查證，或中壢分局偵查隊報案電話 4222032。

2. 道一尺 魔一丈
攔電郵 植木馬 你的個資拼出來[424]

網路詐騙層出不窮，大型電子商務網站安全防護網也愈架愈高，但道高一尺、魔高一丈，網購業者說，反詐騙大作戰需要消費者配合，才能遏止網路個資外洩與詐騙案繼續蔓延。

國內電子商務龍頭雅虎奇摩近年來加強建構安全交易環境，先提供買賣家賠償方案，接著推出結帳通，買賣雙方結標後可直接在系統平台進行聯繫，不需以電子郵件溝通，杜絕劫標信干擾，隨後又有輕鬆付平台，監控所有金流交易流程，將詐騙的風險降到最低。

雅虎奇摩電子商務服務事業部事業總監李芃君說，歹徒犯案的手法大都是攔截電子郵件，在賣家電腦中植入木馬，入侵業者平台，竊取資料，或是從不

[423] 2008-12-12/聯合報/C2 版/桃園綜合新聞

[424] 2008-06-22/聯合報/A3 版/焦點

同的管道「拼」出個資，恐怖的是，犯罪集團資料庫完整，對消費者購物喜好、付款習慣一清二楚，警覺性不高的消費者很容易被騙。
另一大拍賣網站露天拍賣則設置個人雙重密碼機制，使用者須設定兩組密碼，歹徒無法輕易入侵；此外，公司還有一組交易安全人員，全天候檢驗每個登入 IP，只要發現來源有異，立即封鎖；知名的女性購物網站 PayEasy 也備有安全檢測團隊。
不過，網購業者費盡心思織出防護罩，卻往往百密一疏。露天拍賣公關古嘉惠說，防範詐騙光靠業者沒有用，消費者警覺心也很重要，目前最新犯罪手法稱爲「資料拼圖」，百貨公司抽獎名單、大賣場促銷活動參加者資料都是歹徒覬覦目標，消費者在日常生活不知不覺把個人資料外洩出去。
網購業者補充，詐騙集團「土法煉鋼」從各種管道蒐集資料，慢慢拼湊出個人資訊，由於不少人帳號、密碼從個資中皆有脈絡可循，甚至一組密碼「打通關」，一不小心就被歹徒入侵成功。

3. 個資外洩只要一指 65%詐騙案 在家購物著了道[425]

上網拍賣（購物）或電視購物日益普遍，消費者不出門也可以享受瞎拼樂趣，不過一六五反詐欺專線統計資料顯示，便利快速的「無店鋪購物」型態，已成爲消費者個人資料外洩主要管道！
詐騙案件 網購最大宗
一六五反詐欺專線統計，今年從三月到六月中旬爲止，全國詐騙報案件數高達一萬兩千多件，其中約八千件屬於無店鋪購物詐騙，占報案總數的六成五以上，估算被騙金額超過兩億元。
換句話說，平均每天有九十件詐騙案正在發生，至少被騙走一百五十萬元，而這些只是反詐騙專線統計，估計實際詐騙數字遠超過官方數據，「美麗之島」台灣成了「詐騙天堂」。
統計也指出，知名的購物網站、電視購物頻道與大型企業附設的購物網站幾無一倖免，都有因客戶個資外洩而被詐騙的紀錄。
雅虎東森 受害者最多
其中，拍賣網站「一哥」雅虎奇摩拍賣網，平均每周被騙件數超過兩百件，排名第一；電視購物龍頭東森購物，每周被騙件數平均高達百件以上，排名第二。雅虎與東森旗下客戶被詐騙案例最多，個資外洩始終無法有效改善，令人質疑兩大購物平台的資訊安全，是否在哪個環節出了問題。

[425] 2008-06-22/聯合報/A3 版/焦點

另外博客來網路書店、PayEasy、誠品網路書局、日系化妝品 DHC、年代購物網、PC HOME 等購物平台統統都曾經「中獎」發生客戶個資外洩事件。
警方調查，歹徒取得個資後，最常見的詐騙方式有兩種，一是拿著盜取的信用卡號嘗試在其他網站登錄，冒刷購物換現金；二是僞裝成網路或電視購物台的服務人員打電話告訴消費者，付款方式勾選錯誤，例如「一次付清」變成「多次分期扣款」或「定時定額付款」，要求消費者到提款機更改設定，乘機入侵帳戶。
個資正確 消費者不察
由於歹徒對消費者購買時間、金額、送貨地址、聯絡電話等統統正確無誤，許多消費者接到詐騙電話誤以爲真，往往依照歹徒指示到 ATM 轉帳。
網站或電視購物台個資外洩詐騙事件頻傳，卻很少主動通知或提醒會員「資料外洩，不要被騙」，消費者總是在警方或銀行找上門後，才驚覺自己的資料被人竊取，或者信用卡被盜刷了！
歹徒狂刷 報復購物網
更令人擔心的是，詐騙集團行徑囂張，PayEasy 盜刷千萬事件轟動一時，刑事警察局警務正常金蘭說，四月十二日至十三日兩天內，PayEasy 新註冊的十二名「新會員」各拿出百餘張信用卡集中、瘋狂刷卡購物，由於冒刷手法太明顯，研判歹徒動機不是盜刷而是報復，企圖癱瘓 PayEasy 作業系統。
常金蘭說，去年底 PayEasy 發現會員資料外洩後，刊登大幅廣告提醒會員「不要被騙」反制詐騙集團，事隔不久，歹徒即侵門踏戶 PayEasy 網站狂刷，警告意味濃厚。
常金蘭說，PayEasy 攔截到冒刷的信用卡都屬有效卡，也就是卡號、有效月年、背面驗證號碼等所有欄位都對，推測歹徒不僅掌握完整正確資料，而且還有極大量的有效卡在手中。
填個問卷 也危機重重
常金蘭說，網路與電視購物平台雖可能是個資外洩主要管道，不過辦手機、填寫問卷調查表，甚至辦一張超市會員卡也可能不小心就洩漏自己隱私，個資外洩每分每秒都在發生，詐騙集團更是無孔不入，消費者自保最重要的是，不管電話那端如何正確說出你個人資料，「絕不聽從陌生人指示操作 ATM」。

4. 固定密碼資料容易外洩… 信用卡動態密碼 安心付款[426]

[426] 2008-06-05/經濟日報/C2 版/致富寶典

網路購物屢見駭客入侵，很多消費者都擔心資料外洩。台塑網科技、法德科技、萬事達卡國際發卡組織與新光銀行最近合作，未來信用卡登入認證時，每次都會產生新的一次性密碼，取代原先慣用的固定密碼，讓消費者不必擔心木馬程式或駭客截取帳號密碼，阻絕駭客或個人資料外洩等問題。
台塑網是長期經營全國最大 B2B 的電子交易，每年交易金額超過 2,000 億元，為了嚴格要求資訊控管，與科技業者共同研發「信用卡動態密碼認證及動態安全付款系統」，建立身分認證平台，讓付款更安全。
台塑網表示，過去網路購物使用信用卡時，除了必須要通過網站登入帳號密碼認證，在網路結帳付款時，還要輸入一連串的數字，如信用卡號、到期年月、姓名或卡片後面三碼與身分證字號等資料；使用一次性密碼，只要透過攜帶式讀卡機產生一次性密碼，經由銀行端系統演算，就能確認持卡人的身分，完成付款授權。
簡單來說，持卡人每次登入網站交易，都會產生新的一次性密碼，取代原先的固定式密碼，消費者不必擔心木馬程式或駭客截取帳號密碼等資料，購物網站也無法得知信用卡的詳細個人資料，以阻絕駭客或個人資料外洩的問題。

5. 假冒購物台詐騙水上連傳數起[427]

水上警分局最近受理多件詐騙案，詐騙集團利用購物台名號向被害人佯稱網站有問題或簽收單簽錯，騙取被害人帳戶的金額，從 2 萬到 5 萬元不等，警方呼籲民眾上網或電視購物時，千萬不要隨意將個人資料外洩。
警方表示，45 歲江姓男子接到陌生女子來電聲稱是購物台員工，指他簽收單上簽到每月扣款項目是錯誤的，要他查詢帳戶有沒有被扣款，他查完後表示並無扣款，在雙方交談中，他把帳號等資訊透露給該女子，並按照指示操作匯款，被轉走 2 萬 8000 元。
37 歲楊姓男子同樣接到自稱是購物台員工的電話，表示當天是結帳日，網站簽收有問題，要他打電話到銀行確認，他按照指示號碼打電話，假的銀行員說「如果今天不處理，電腦會自動將帳戶扣款」，他情急之下照著詐騙集團方式操作 ATM，將帳戶內 4 萬多元全都轉出去了。

6. 常上的網站 2 成躲著木馬[428]

[427] 2008-04-30/聯合報/C2 版/嘉義縣市新聞

[428] 2008-03-26/聯合晚報/A9 版/焦點

網路詐騙猖獗，東森購物、奇摩拍賣、誠品網路書店陸續傳出個人資料外洩，「資安人雜誌」表示，初步也發現，民眾常上的 3000 多個網頁中，大約有 20%都會下載惡意程式，可能導致個人資料外洩，被不法人士取得、盜用。網路個資外洩越來越普遍，除了東森購物等，最近上海書店的網路購書服務，也傳出有讀者接到詐騙電話，對方能清楚掌握姓名、在哪裡拿書取貨等訊息。資安專家邱銘彰表示，越是知名網站，越容易受到駭客攻擊，惡意連結，初步發現，一般人常上的新聞等 3000 多個網站中，20%都會同時下載惡意程式，但網友並不自覺電腦已經被「作了手腳」，而且防毒軟體也沒辦法百分之百過濾。

今天他也示範在電腦中虛擬，當上網瀏覽網頁時，駭客利用瀏覽器弱點，已在電腦中植入惡意程式，趁機竊取資料或造成中毒，儘管網站的網管發現、修復，駭客還是會一直找機會下手。

邱銘彰說，個人資料一轉手可賣得十幾萬元，對一些「閒閒沒事作」的駭客是不小誘惑，而獲得資料的詐騙集團，「很容易回本」，因此詐騙集團常與駭客勾結。

上海書店則表示，基本上網路書店購書都是到店取貨付款，但詐騙集團聲稱店員弄錯了繳款方式，誤改成分期付款，要求消費者到提款機前操作，假借查詢餘額，實則趁機混淆消費者轉帳，匯出款項，而且常挑在假日進行，讓焦慮的消費者很難查證。

同時，詐騙手法也翻新，來電顯示會跟書店原本的服務電話一致，重撥無人接聽，但若直接回撥，會有人應答，詐騙集團還會聲稱，是會計假日加班才發現錯誤，若不相信還會由扮演主管的人來說服。

另外，最近流行手法，還有請消費者到提款機時，改由進入英文介面操作，藉由一般消費者不熟悉英文指令，假借是「查帳」，實則一步步要消費者照著跨行轉帳、按帳號、匯出金額。

7. 葉奇鑫(露天拍賣營運長)
多照顧小網站業者[429]

因先前工作經歷的因素，是由政府機關的角度看民間，現在是從民間看政府。了解企業知名度建立不易，只要發生一次資安事件就可能把辛苦成果毀於一旦，不得不小心。

我向來認爲資安和個資保護是企業很重要的一環，特別是網路企業，只要資安出現漏洞導致會員個人資料外洩。但坦白說，每個公司由於資本額的關係，

[429] 2008-03-18/經濟日報/A15 版/座談會

在資安領域處理能量是不同的，這不是應不應該的問題，而是成本上很實際的問題。
但我還是要呼籲，網站資安問題要越早重視越好，等到網站流量大了，架構複雜後，成本反而更高。此外，一個網站的主事者是否重視這個問題，也是因素之一。以我本身而言，每個星期二中午就是露天的資安會議，我親自主持討論網站的穩定和安全性。老闆重視，員工才會重視，才不至於讓資安或個人資料保護流爲空洞的企業口號。
我覺得個資法推動上應有三方面循序漸進，一是立法、二是教育宣導、三是輔導，而且要多照顧小型網站的業者，讓他們有更大的生存空間，否則整個創意市場的產值會減少，例如先前沒有修定的罰則（民事賠償以 2 萬爲下限）是很不合理的，但經過修正，就是好的開始，且要有罰則上限，以保障企業端。此外，政府應在法律通過後，訂立各種輔導方案，讓企業有範本可依循，例如可能要修改原有的會員合約，如果有標準範本依循，可大幅降低企業適應新法的時間和成本。
此外，我建議業界和社會大眾應嘉獎企業勇於面對個資危機的案例，例如先前的 PayEasy 事件，他們主動運用媒體力量，告知會員網站已受到詐騙集團鎖定，並且讓會員可以免於受到詐騙，企業精神值得贊許。但是反應出來的是 PayEasy 業績立即受到影響，甚至事實被部份輿論扭曲，對企業是一大打擊。基於以上案例，現在露天的作法是，會員進入網站需通過二道密碼後，才能查看個人資料並進行修改，這是全國首創的做法，雖然會造成些許麻煩，但會員還是能夠體諒配合。
個資法真的很重要，若部份執法單位或是主管機關都搞不清楚權責，或根本不懂法案，只會造成民眾誤會和企業損失，所以我支持要有專職機構負責，而且要提高層級，讓企業知道要去找那一個單位，而非把問題推來推去，不然法律定出來後，才是問題的開始。

8. 網拍名店 「東京著衣」個資外洩[430]

雅虎奇摩上最大衣物拍賣商家「東京著衣」的消費者，最近頻頻接到電話，要求重新操作櫃員機轉帳，買家懷疑是個人資料外洩，遭到詐騙集團利用。「東京著衣」有十萬多筆網友肯定評價，是銷售量與評價都最高的賣場，顧客廣及美、日、香港、新加坡市場，甚至有來自沙烏地阿拉伯的華人買家上網訂購。

[430] 2008-03-10/聯合報/A8 版/生活

一名黃姓消費者表示，她在本月一日下午接到自稱是賣家客服人員來電，表示她在 7-11 取貨付款時，因爲門市人員拿錯單子，她被設定成分期付款，未來還會持續從銀行扣款，請她到銀行作個取消的動作；由於對方知道她的身分資料與購買物品、金額，電話確是賣家之前所打來的號碼，一開始她完全相信對方。

她說，對方還向她保證絕對不是詐騙集團，只是要協助她取消扣款；在詢問過程中，得知她使用郵局帳號，接著就表示會把資料傳真給郵局，請郵局派人來說明協助，隔約五分鐘，她果然接到電話，而且手機上顯示號碼就是郵局後方的免付費客服號碼。

後來她想到當天是周六下午，郵局怎麼可能上班，且對方一直要她提供帳號，她才警覺應該是詐騙集團所爲。許多消費者都有類似的經驗，在知名台大 PTT「e-shopping」版也引起熱烈討論。

東京著衣周姓負責人表示，由於有許多合作廠商，仍不清楚資料從那個管道流漏出去，也有可能是消費者電腦中毒，在網路上被駭客側錄下資料；公司在三月四日已向嘉義市警局第二分局公園派出所報案，也在網站上加強公告提醒買家小心被詐騙，並花廿多萬元持續不斷寄簡訊提醒消費者。

雅虎奇摩拍賣公關主任許卉妃說，奇摩不清楚詐騙集團如何取得「東京著衣」的消費者資料，但會配合警方辦案，並持續加強宣導防治，不讓買家受騙。她提醒網友，櫃員機並沒有設定或解除分期付款的功能，切勿依電話指示操作櫃員機。

9. 東京著衣怪電話頻頻 買家疑個資外洩[431]

雅虎奇摩上最大衣物拍賣商家「東京著衣」的消費者，最近頻頻接到電話，要求重新操作 ATM 轉帳，買家懷疑是個人資料外洩，遭到詐騙集團利用。

東京著衣周姓負責人表示，目前不清楚資料從哪流出去；已在 4 日向嘉義市警局所報案，並花 20 多萬元寄簡訊提醒消費者注意。

Yahoo!奇摩拍賣公關主任許卉妃表示，不清楚詐騙集團如何取得「東京著衣」的資料，會配合警方辦案。

「東京著衣」是奇摩網路上最大的衣物拍賣商家，網友肯定評價高達 10 萬多筆，一名黃姓消費者表示，她在 1 日下午，接到自稱是賣家客服人員來電，表示她在 7-11 取貨付款時，因爲門市人員拿錯單子，她被設定成分期付款，請她到銀行取消；由於對方知道她的身分資料與購買物品、金額，電話確是賣家之前所打來的號碼，一開始她完全相信對方。

[431] 2008-03-10/Upaper/2 版/焦點

黃姓消費者表示，對方還知道她使用郵局帳號，宣稱由郵局人員接手，顯示號碼還真的是郵局的免付費客服號碼。只是當天是周六，對方一直要她提供帳號，她才警覺應該是詐騙集團。

10. 假網拍：繳清變分期 詐 2 女大學生

表明願幫忙連絡銀行 受害人唸出免付費電話 即接獲顯示該號碼來電 警方懷疑網路個資外洩[432]

又傳網路購物詐騙，屏東地區兩名大學生最近在網路購物後，有歹徒自稱購物網站人員，佯稱操作出問題，兩人先後被騙近 4 萬元，警方懷疑是網路個人資料外洩，呼籲經常使用網路的民眾提高警覺。

一名 24 歲的女大學生上個月 29 日在拍賣網站上刷卡購物後，本月 24 日接獲自稱是拍賣網站工作人員的電話，指稱當天電腦操作失當，把一次繳清的刷卡金額誤爲分期付款，這名工作人員還很好心地向客戶索取信用卡的免付費電話，表明願意幫忙與信用卡銀行連絡，取消錯誤的帳單。

女大學生不疑有他，立刻把寫在信用卡背後的免付費電話唸給歹徒，隔了不久，女大學生就接獲銀行的電話，而且顯現的來電號碼就是信用卡的免付費電話，女學生當時還覺得「怎麼效率那麼好」？結果電話那頭的「銀行人員」說，必須由本人到提款機操作，才能取消交易，她信以爲真，不一會兒功夫，戶頭裡的 29000 多元就不翼而飛。

此時這名女大學生驚覺被騙，當天晚上立刻向里港警分局新圍派出所報案，警方發現，本月 13 日也有一名女學生在網路購物後，被以相同的手法騙走 1 萬 8 千多元，兩名女大學生都是因爲看到來電顯示是銀行的免付費電話號碼，不疑有他，才會上當受騙。

目前警方已調查是否有個資外洩的情形發生，同時提醒民眾在接獲不明電話時，「一定要遠離提款機」，凡事一定要再做查證，才不會上了歹徒的當。

11.「面交取款」59 人被騙上億元

假檢警謊稱身分遭冒用、個資外洩 以安全帳戶或車手當面簽收現款 6 人被訴[433]

政府大力宣導詐欺集團以自動櫃員機轉帳方式騙錢後，領款車手越來越大膽，竟改採面對面取款方式騙光民眾積蓄，高雄檢警偵辦黃致仁爲首的詐欺

[432] 2007-12-27/聯合報/C2 版/屏東縣新聞

[433] 2007-12-24/聯合報/C1 版/高屏澎東・教育

案發現，一名被騙了 2 千萬元的婦人，最後一筆 6 百萬元是當面交付的，籲請民眾提防。
該集團從今年 4 月至 8 月，共騙了 59 人、1 億 3 千萬元，他們利用民眾擔心多年積蓄被列爲犯罪所得而被凍結或沒入的心態，「假好心」幫忙，動輒騙款上千萬元。高雄地檢署檢察官李怡增日前依詐欺罪起訴黃致仁（24 歲）、李原慶（25 歲）、黃柏仁（25 歲）、鄭子瑜（女，34 歲）、曾偉傑（31 歲）、張譯心（女，46 歲）等 6 人。
高雄市刑大指出，公家機關不會聯繫民眾將錢轉到所謂的安全監管帳戶，更別相信所謂「千萬不能告訴別人、銀行行員或警方都和詐欺集團勾結…。」等說法，遇有可疑狀況，請立即掛掉電話，重播 165 反詐騙電話查詢。
檢警指出，黃致仁集團從今年 4 月起以亂槍打鳥方式撥民眾的電話，謊稱電話費未繳或身分遭冒用、個人資料外洩等，再派人假冒檢察官、警察、金管局人員與民眾連繫，甚至派車手當面簽收民眾的現款。
其中，桃園縣張姓婦人接到「金管局林科長」電話，表示她的身分遭冒用辦理行動電話，除積欠電話費，存款帳戶也被用於犯案，將被凍結，再經一連串的電話誘騙，建議她把存款匯入檢察官的官安全帳戶，她便在兩週內匯款 775 萬元，詐騙集團甚至要她辦房貸以免房屋遭查封，所幸她及時驚醒，保住房子。
另一新竹縣黃姓婦人今年 6 月接到詐騙集團假冒監理所人員的電話，指稱她的轎車超速違規，罰單未繳，她稱未到過彰化，詐騙集團改口稱可能是個人資料外洩，身分遭冒用，要她報案，不久有員警來電話，指她牽扯很大詐騙金額，須趕緊申請金融安全帳戶保護系統，並要他到法院公證，因時間已接近銀行休息時間，騙徒主動表示替她申請監察委員公證，她在 6 月 15 日及 20 日兩天匯了 10 筆共一千一百多萬元給假冒的監委。
另外，台北鄭姓婦人在 5 月 10 日至 6 月 15 日間，陸續匯多筆 2、3 百萬到所謂的「安全帳戶」，她匯了將近 1400 萬元後起疑，詐欺集團爲取信於她，出面再收取她 6 百萬元。

12．個資外洩？東森得易購承諾補償[434]

在台北市消保官強力要求下，東森得易購公司上午承諾將與「無店舖協會」成員如 momo 台、博客來網路書店等業者共同建立「補償金」制度，未來只要消費者能證明因個人資料被網路購物業者外洩，導致遭詐騙集團詐騙而蒙受損失者，皆可以檢具相關資料，獲取補償。

[434] 2007-12-14/聯合晚報/6 版/焦點

台北市消保官陳柏菁表示，「補償金制度」就是由電視購物等無店舖業者，共同集資建立專戶，類似聯保制度，只要消費者能證明在電視或網路購物時，因個資外洩遭詐騙集團利用，使消費者被詐騙蒙受損失時，即可由專戶補償。該項構想上午經東森得易購公司承諾，將和其他業者共同成立，但對於該制度成立時間、資金規模及如何補償方式、如何認定等還要再商議。
【記者楊美玲/台北報導】
爲防止無店舖交易過程中，造成資料外洩，東森得易購將邀富邦 MOMO、博客來或 YAHOO 等網路與電視購物者，共同成立補償金制度，富邦 MOMO 與 YAHOO 皆表示，目前尚未收到東森得易購的邀約，所以無法表達任何看法。YAHOO 則表示，內部於 2004 年即開始實施買家賣家保障專案。
YAHOO 奇摩公關經理吳苑如表示，網友若透過 YAHOO 平台進行買賣，一旦遭到詐騙，都可以憑交易紀錄與報案三聯單，向 YAHOO 提出求償，最高賠償金額爲一萬元，但若是透過金流制度系統輕鬆付的虛擬戶頭交易，最高可求償 3 萬元。

13. 冒博客來名行騙 至少 20 人受害[435]

詐騙集團冒名博客來網站行騙越發囂張，歹徒連上回金馬影展畫位個人資料外洩案也拿來當藉口，說電腦因此受損，需要重新更正資料。再加上歹徒熟知顧客何時購買何物，連用何種方式取貨都能掌握，據悉目前至少廿餘人受害。
博客來公關經理薛希翎表示，他們從十二日起就接到大批客訴電話，經過系統檢查，確定不是系統安全問題，有可能是顧客的 e-mail 資料遭集團盜用，近來如 Yahoo!奇摩拍賣等網站也遭詐騙集團以同樣手法行騙，博客來並非個案。
博客來日前曾發生金馬影展畫位個資外洩事件，但博客來表示，最近的詐騙案與上回完全無關，上次是工程師對特定的四百多名網友發信時出的問題，這次則是廣泛的網友資料遭詐騙集團盜用。
薛希翎表示，博客來獲悉民眾遭到詐騙後，立即在網站掛公告，表明博客來絕不會以電話等方式，告知客戶因設定錯誤，須至ＡＴＭ操作修正或提供信用卡資料，希望客戶遇狀況快打一六五反詐騙專線，他們都有發簡訊提醒顧客小心。
不過，博客來顧客黃先生表示，並未收到簡訊。眾多網友也爭相披露接到詐騙電話的經過，還有人說：「想想，去我家對面的書店買書也不錯。」

[435] 2007-11-23/聯合報/A3 版/焦點

另外，上回的個資外洩事件，博客來除對想退票的觀眾全額現金退票，還送一份限量版的「二〇〇七台北金馬影展特刊」。

【記者張錦弘／台北報導】張姓讀者昨天向本報投訴，有人謊稱博客來網路書店客服人員，藉口把她誤爲分期付款客戶，以阻止扣款爲由，向她詐財，但被她識破，歹徒竟知道她買過哪些書，她懷疑個資外洩，已中止博客來會員身份。

張小姐說，她曾打一六五防詐騙專線，警方告訴她，已有別人投訴同樣案例。她再向博客來反映，客服人員說，也有別的客戶反映，目前已在處理。張小姐懷疑，若非博客來內部人員把客戶資料外洩，就是網站已遭駭客入侵，她覺得很不保險，已中止博客來的會員身分。

14. 博客來洩個資 挨轟

金馬影展劃位者 賠500元e coupon[436]

博客來網站驚傳個人資料外洩，四百多名在博客來登記金馬影展劃位的網友，收到的註冊成功通知信中，都包含其他網友的姓名、手機、住家住址等，一堆人上網怒罵博客來。博客來回應強調，這是系統「個案」疏失，將賠償每位網友五百元的e coupon。

昨晚近六時起，金馬影展官方部落格開始湧入網友留言，抱怨從博客來收到的通知信中，不但有自己的資料，還有一堆別人的資料，有網友表示自己曾打電話給客服中心，但對方只是迭聲說「對不起」，沒說要怎麼補救。

網友群情激憤，怒罵博客來沒做好控管，要求賠償，但「別想用e coupon打發」。晚間七時，有網友怒道「事情已經發生這麼久，怎麼還不見博客來處理」，直到近七時五十分，金馬影展才留言表示已和博客來洽談解決之道。

晚間十時許，博客來行銷部經理薛希翎出面表示，由於博客來這次爭取金馬影展線上劃位，因此網友在前天起在誠品買好套票後，必須到博客來網站登記劃位，但因有人反映未收到註冊確認信，因此工程師針對未收到信函的四百多位網友重發確認信，「系統就是在這批補發信中出問題」。

薛希翎強調，此案並非博客來整體系統問題，而是工程師針對這批補發信時「略作調整」時出的問題，「絕對是個案」。目前博客來已研擬內部懲處，針對此次受害網友，將每人發放一組一百元、總共五組的e coupon，使用期限至明年一月止，但每組都須單獨使用。

[436] 2007-11-06/聯合報/A10版/生活

至於爲何不直接發放現金，薛希翎說是因爲網友分散各地，怕聯絡不及，另外也有現金帳戶轉帳不便等問題。若仍有網友不滿，薛希翎說也只能交給公司法務部處理。
【記者蘇詠智／台北報導】針對購買金馬影展套票消費者的資料被博客來網路書店外洩一事，金馬影展主辦單位指資料外流是博客來的疏失，影友可直接詢問博客來處理狀況。

[就醫]

1. 透過健保卡消費 個資恐外洩[437]

經建會計劃對全台 670 萬戶家庭發放消費券，政府擬透過健保卡作爲發放消費券的電子錢包成爲一個選項，衛生署中央健保局副總經理李丞華昨（16）日表示，利用健保卡兼用電子錢包難度不大，不過若放寬到一般商家，因加密功能非短期可達，將有個人資料外洩的問題要考慮。李丞華表示，透過健保卡充做電子錢包，作爲消費券發放，法令及實務上並不困難，困難之處是安全把關，涉及的認證門檻高，將增添諸多困難。

2. 擴大 DNA 採樣 ‘理由說清楚’

立院擬修法 人權團體反彈 正當性及必要性不足 主張限縮採樣犯罪類型[438]

對於立法院擬修法擴大 DNA 採樣的建檔範圍，相關法案本會期可能三讀通過，人權團體上午提出強烈抨擊，質疑政府蒐集及建立這樣一個龐大的國民「敏感性個人資料」的正當性與必要性，不但可能造成政府濫權，一旦此類高度私密的資料外洩，人民權益將遭嚴重侵犯。
警政署在本屆立法院會期積極推動修法，將 DNA 採集除現有性侵害及重大暴力犯罪外，還擴及到傷害、公共危險、毒品危害、竊盜罪等犯罪嫌疑人。包括台灣人權促進會、民間司法改革基金會、北市律師公會等數個人權社團上午舉行記者會，表達高度懷疑及強力反對立場。
台權會會長劉靜怡質疑，警政單位有何證據支持擴大犯罪嫌疑人的 DNA 採集，能達到防範犯罪及維持社會治安的功效？個人 DNA、財務、性傾向等屬

[437] 2008-11-17/經濟日報/A2 版/財經要聞

[438] 2008-07-11/聯合晚報/A11 版/社會

於敏感性個人資料，不同於一般個資，修法視同空白授權，難以掌握警政單位在後端如何使用這些資料。
劉靜怡表示，無限上綱的擴大採樣，很可能轉變成爲一種變相的全民 DNA 大採樣，將全民都視爲潛在的罪犯。且警政署在擴大採樣之後，要如何作好資料庫的保存保護，都未曾對國民作公開的說明，讓人質疑難保不會因爲內控機制的失靈，讓這些高度私密的個人資料外洩給其它人做不當利用。
人權團體主張，DNA 擴大採樣有違憲侵害人民權益之虞，對採樣的犯罪類型應加以限縮，且應確保採樣程序啓動的獨立審查機制，避免執行單位任意濫權，而除了偵察犯罪強制採樣外，其餘的 DNA 樣本的使用，必須取得被採樣人同意並通知樣本使用記錄。

3. 施部長講法

隨意公告他人姓名 小心觸法[439]

前陣子，有人收到交通違規罰單，發現單子寫得太清楚，讓他的個人資料外洩，就有民意代表出面指責主管單位沒有顧慮民眾個人隱私。過去也有愛滋病患、肺結核病患的資料被揭露在網站上，讓他人搜尋到。有些醫院對病患的資料不夠注意，讓人上網便一覽無疑。這些事件讓當事人隱私外露，幾乎變成透明人。
重大逃漏稅可對外公告
其實很多法律都允許公布姓名，有些是好事，比如每年財稅單位都會定期公開表揚納稅大戶，因爲依稅法規定，只要得到同意，可以對外公告他們的姓名或公司名稱。
相對地，對於有重大欠稅或重大逃漏稅的人，主管機關也可以對外公告。另外，有些公務員依法必須申報財產，如果漏報或短報，監察院可以公布他們的姓名。
一般來說，被主管機關公布姓名，多不是好事；比如，檢調公布的十大通緝要犯、十大經濟要犯等；曾經也有一審法官爲了防範某外國人出境，就把他的姓名和大頭照送到各港口、機場，不讓他脫逃。
與少年相關的法令，類似的規定很多。其一，養不教，父母之過；少年犯的父母如果忽略教養，致使少年犯罪，主管單位可以要求接受親子教育輔導，如果拒不接受，經過三次以上處罰，就可以公布父母的姓名。
縱兒女犯罪姓名可公布

[439] 2007-11-27/經濟日報/A13 版/稅務法務

其二，如果父母允許少年或兒童去做危害身心健康的服務性質工作，被罰錢之外也會被公告姓名，而像酒家、茶室、電玩場所等，如果容許少年出入，主管機關可以公告這些店家的負責人姓名。
其三，法律規定，若和未滿 16 歲的人從事性交易，或引誘、容留、媒介未滿 18 歲的人從事性交易，或者強迫、控制甚至用以買賣、質押，做這些事的人經判決確定的話，可公布姓名。
另外，像兒童福利法規定，虐待、遺棄或利用兒童去做不正當的事，也會被公開姓名。藥事處理法也有規定，違規藥物的廣告負責人，衛生署要公告姓名和藥物名稱。
當然，不能隨便公告別人的姓名，必須依法公告，因爲個人的姓名和違法情節被公開，涉及名譽，應有法律根據，不然可能構成妨害祕密罪或洩密罪，若違反的是「電腦處理個人資料保護法」，可要求賠償，嚴重的話也構成刑責。
舉例說，對於檢調人員未依「證人保護法」規定，把應受身分保密保護的證人資料交付出去或洩了密，即構成犯罪；換成媒體記者或律師，因爲職務或業務上而知道、持有應受保護的證人資料，隨意交付或洩密，也有刑責。就有民眾看到報紙寫他爲某案作證，姓名和照片都登出來了，氣得找記者理論。
被害人曝光媒體要受罰
目前，社會注重男女平權，性騷擾防治法或性侵害防治法都規定，廣告物、出版品、廣播、電視和網路，不得報導或記載被害人的身分、姓名或其他可以被辨識的資訊，違反的話要處以罰鍰。
現在，媒體在使用少年的相片或姓名時，也特別小心了，因爲依少年事件處理法規定，少年犯的相關資訊不能在媒體或透過資訊公示的方式讓別人知道。
（本專欄由法務部長施茂林口述，記者徐谷楨採訪整理，每周二刊登）

4. 冒充捐血中心 歹徒詐個資

民眾投訴：對方電話提出正確身分資料後要求補充 恐中心資訊外洩 中心清查後否認[440]

花蓮捐血中心昨天接獲捐血人投訴，指有詐騙集團冒充捐血中心人員名義騙取他的個人資料，捐血中心澄清沒有類似查詢動作，籲請民眾切勿受騙，另經清查保存的捐血人資料，並未外洩。
捐血中心主任王雲龍說，捐血人如接到類似詐騙電話，請立即向捐血中心查證，以免受騙，捐血中心電話：8560990。

[440] 2008-04-30/聯合報/C2 版/花蓮縣新聞

王雲龍表示，數年前曾發生詐騙集團冒用花蓮捐血中心名義，假借抽中大獎要預繳稅金爲由，企圖向民眾詐財。他說，最近個人資料外洩事件頻傳，但傳出冒用該中心名義詐取個人資料的手法是首見，民眾務必要小心提防。
該捐血人投訴說，他定期到花蓮捐血中心捐血，日前接獲一位年輕小姐電話，對方自稱是捐血中心人員，主動告知他正確的身分資料後，要求再提供一些資料，他不疑有詐提供後，愈想愈不對，於是打電話向捐血中心查證，發現對方電話號碼並非捐血中心所有，因擔心個人資料已外洩，讓他惴惴不安。
投訴人懷疑花蓮捐血中心保存的捐血人資料可能已外洩，經捐血中心啓動自我檢查系統，確認資料未外洩。
捐血中心秘書曾慶熹說，中心保存的捐血人個人資料都附有保密作業流程，電腦本身有各項防範侵入措施，機房也安裝兩道精密鎖，員工在處理相關作業上，都很小心。
曾慶熹表示，相關文件報廢時如有捐血者個人資料，員工都以碎紙機銷毀。外出作業時手提電腦也會加裝防窺片。
郵寄的檢驗報告信函如遭退件，只會電話確認捐血者通訊地址，方便再一次投郵，不會再向捐血人詢問其他個人資料。

[就學]

1．學校公告洩個資 教部：不應該[441]

教育部大專院校弱勢學生助學計畫審查結果最近出爐，各大專院校陸續通知學生審查結果，卻有部分大學將學生身分證字號及家庭年收入狀況公布在校內網站，供學生點閱，引發資料外洩疑慮，經學生反映後，學校已撤除改進。
發生這種情形的學校，北部、南部、國立和私立學校都有，學校都是在校內網頁公開學生身分證字號，以及家庭年收入審核結果，學生都可點閱。
不過這種公布身分證字號和家庭年收入的作法，引發個人資料外洩疑慮，相關學校經學生反映後，紛紛上網撤除資料，並且改以保密作法。
例如有的學校現在網頁上只公告大專院校弱勢學生助學計畫審查結果出爐，但學生要以密碼才能看到獲通過的名單，且只公布學生的學號，並沒有姓名和系所。有的學校以電子郵件通知學生，並給學生一個密碼，也有學校改以電話通知未審核通過的學生等。

[441] 2008-11-22/聯合報/C3 版/教育

有大學表示，爲顧及學生的隱私，不想在網頁上公告學生的名字和系所，希望替學生保密，避免被他人知道，才會公布身分證字號，加上今年教育部新增排富查核，公布學生的家庭年收入，希望完整資訊能整讓學生有申訴的機會。

教育部高教司四科指出，學校不應公開學生的資料，就算公告相關事項與資訊時，也應該要注意資料的保密，更重要的是，一定要顧及學生的感受，如果學生覺得不妥，學校應該注意調整。

高教司也說，雖然學校不公布學生姓名和系所，然而，身分證字號和年收入等資料，都屬學生個人資料，尤其是身分證字號，有可能會遭有心人士利用，應該要保密，公布在網路上非常不適合。

2. 基測個資外洩 監院：教部失責

博暐販賣個資 違法圖利 教部：考生資料將交由政府專責單位 不再委由民間處理[442]

教育部委託博暐圖書網路公司辦理 97 年國中基測電腦處理作業，但博暐違法販售考生個資及成績，侵害考生權益，監察院昨天通過糾正，指出教育部疏於監督，明顯怠忽職責。

教育部主任秘書潘文忠對此表示，教育部尊重並接受建議，也會檢討改進。

監察院調查發現，博暐公司趁取得考生個人基本資料及成績機會，將 97 年第一次國中基測考生個資及成績外洩，販賣給中南部 10 多家補教業者，並提供給 7 所私立高中作爲招生之用。

監察院指出，全案經高雄地檢署及台中地檢署分別偵查起訴，但高雄地檢署偵查又發現，博暐公司在承包 96 年國中基測電腦作業時，就曾經協助學生僞造假成績單。

此外，93 年國中基測時，電腦作業承包廠商大正資訊網路公司也發生運用考生個資，寄發升學特輯給考生，顯示教育部辦理國中基測有很多疏失不當。

監察院糾正案文指出，教育部未能預見國中基測試務繁雜且專業，每年由不同學校輪流主辦，易爲承包廠商壟斷，且未善盡監督電腦採購作業職責，又

[442] 2008-11-14/聯合報/C3 版/教育

未能以 93 年考生個人資料外洩爲鑑，積極檢討改進，加強保密措施，以致於 97 年弊端擴大，教育部疏於監督，明顯怠忽職責。

潘文忠昨晚指出，當初教育部發現博暐有違法情事，即主動移送檢調調查，希望依法快速處理；在教育部內部也舉辦多次檢討會議，檢討流程及討論未來是否設專責機構處理等，以便進一步做好防護工作。

教育部中教司司長蘇德祥則表示，教育部在事後已有積極改善作爲，明年考生的個人資料將送交政府專責單位，不再委由民間處理，不會有外洩問題。

3. 賣考生個資 大正、博暐多人到案[443]

高雄地檢署偵辦國中基測考生個人資料外洩案，檢察官劉河山昨天指揮檢警到台中市帶回大正與博暐公司負責人林正杰與他的女友許慧珠等人偵訊，初步發現兩家公司涉嫌轉賣數十萬筆考生資料，獲利至少四百三十萬元。

根據雄檢掌握的線索，大正資訊與博暐圖書實爲同一家公司，大正資訊標到今年國中基測相關業務後，利用承辦的機會，取得全國基測考生名單等資料，將考生資料以一百萬元至一百八十萬元不等的金額，販售給十多家補教業者。

雄檢表示，被告除涉妨害秘密罪，大正受政府委託承包基測業務，卻洩漏考生資料，還涉背信，依電腦處理個人資料保護法規定，可加重其刑二分之一。

針對國中基測考生資料外洩案，雄檢昨天指揮電信警察隊、高雄市警局及檢察事務官分別到台北、台中、高雄等地搜索，扣得基測考生資料、電腦等物，傳喚廿餘人到案。

檢警除傳喚大正資訊負責人林正杰、博暐圖書網路公司負責人許慧珠，還有一名吳姓男子。吳姓男子涉嫌將嬰幼兒的基本資料賣給彌月蛋糕及幼教圖書業者，檢方正追查取得資料的管道。

4. 基測個資外洩 檢方大搜索 2 人聲押[444]

偵辦國中基測考生個人資料外洩案，高雄地檢署檢察官劉河山昨天指揮檢警人員兵分 20 路展開搜索，帶回大正與博暐公司負責人林正杰與許慧珠等人偵訊後，因認爲兩人涉犯妨害秘密等罪嫌重大，今天上午將兩人聲請羈押，另有補教業者數人被以 100 萬元不等交保。

---

[443] 2008-06-15/聯合報/A9 版/社會

[444] 2008-06-15/聯合晚報/A4 版/話題

雄檢指出，林正杰疑因公司財務吃緊，才藉由販賣考生資料給補教業者籌措資金，北、中、南各地都有補教業者向他購買，有的二、三家集資合購，金額從 100 萬到 180 萬元不等。已有部分補教業者承認購買考生資料。
檢察官劉河山去年 11 月間偵辦另案時，發現有一以吳姓涉嫌人爲首的販售個人資料集團，向相關業者四處兜售，即指揮電信警察第三中隊組成專案小組進行蒐證。蒐證發現，涉案的除了前述集團，還有博暐圖書網路公司。
經查博暐與標得今年全國國中基本學力測驗的電腦閱卷、計分等事務的大正資訊公司實爲同一家公司，大正利用承辦國中基測試務的機會，取得全國國中考生名單及學測答案卡等，將參加國中基本學力測驗的考生資料及成績，販售給有意取得這些資料作爲招生使用的北、中、南部的的補教業者共十餘家。
電信警察隊、高雄市警察局少年隊及地檢署檢察事務官等共 77 人，兵分 20 餘路，分別到台北、台中、高雄等地的涉嫌人住居所及公司等進行搜索，扣得基測考生資料、電磁記錄等，傳喚 20 餘人到案。
雄檢強調，專案小組對販售資料集團持續監控期間，原本打算在蒐證成熟且不影響基測作業的情形下發動偵查，後來因有補教業者不滿大正公司提高價碼，對外爆料，專案小組唯恐證據滅失，提前發動偵查，並知會台中地檢署及在該署協助，對博暐等公司及相關購買基測考生資料的補教業者進行搜索。

5. 數位學生證 監控「犯人」？

學權會等團體喊停辦 教局：再討論[445]

台北市教育局從今年 3 月起，在北市各高中職、國中小學全面推動數位學生證，因結合悠遊卡、學生證和校園門禁管理等功能，引發有監控學生及個人資料外洩之虞，而且還加重校園行政工作；部分教師和學生團體昨天要求教育局應立即停辦。
台北市教育局資訊室主任韓長澤指出，新「卡」上路，難免會有陣痛期，教育局會在 9 月前改善系統問題，並縮短補卡換證的時間；至於存廢問題，教育局將在 7 月召開檢討會議，邀集學生、教師和專家學者等一同檢討。
台北市教師會、中學生學生權利促進會、台灣人權促進會等團體，昨天舉行記者會，針對數位學生證提出多項質疑。中學生學生權利促進會發言人許仁碩指出，教育局要求學生刷卡進出校園，根本是以數位化之名，行監控學生之實，「簡直是把學生當成寵物跟犯人來管」！

[445] 2007-06-16/聯合報/C1 版/北市・教育

許仁碩指出，學權會針對台北市約 40 所國高中職、約 650 名學生進行問卷調查，目前多數學校仍以人工點名制度爲主，超過 5 成學生認爲刷卡無法取代人工點名，還有部分學校因爲學生沒帶卡或忘記刷卡，而罰以愛校服務或視同遲到、曠課。

教師會代表郭文瑛說，教育局希望藉由數位學生證取代人工點名制度，減輕老師壓力，實際上卻更加重老師的工作負擔，因爲刷卡機可能會出錯、漏刷，況且不論學生有無刷卡，老師還是要在班上再次確認學生的出席狀況，教育局應檢討刷卡的必要性。

政大法律系助理教授廖元豪表示，市府推動數位學生證的決策過程有明顯瑕疵，不但事先沒有徵詢各方意見，而且也應該尊重不願意使用的學生，徵詢學生同意，再發卡給願意使用的學生。

6. 老鼠會收購帳戶 計畫找學生…

電話費沒繳 數月詐近億 上百人受害 緊急收網逮 7 人[446]

詐騙集團以電話費沒繳、身分遭冒用等亂槍打鳥方式詐騙，再傳真自己發明的「個人資料外洩授權止付聲明書」騙民眾將積蓄匯入「國家安全帳戶監管」，高雄市多位民眾被騙了數十萬元至 299 萬元，刑事局等單位昨天逮捕「領款車手」及「簿子頭」共 7 人。

警方發現簿子頭集團每月收購 300 本人頭帳戶，領款車手用完就丟，而車手集團每天提領數百萬元，估計該集團短短數月詐欺金額近億元，有上百人受害，循線擴大偵辦中。

落網 7 人分別是刊登廣告收購帳戶的王進杉（36 歲）、鍾侑埕（37 歲）及其擔任護士的女友陳俞君（31 歲）、蔣元彥（32 歲）及專責提領詐騙款項的陳泓甫（33 歲）、王郁文（30 歲）及郭信宏（25 歲）。

警方說，王進杉與鍾侑埕近來爲了更容易收購人頭帳戶，計畫吸收在學學生以老鼠會方式大量收購人頭帳戶，高雄地檢署檢察官彭斐虹，指揮刑事局偵八隊三組、台南市警局、高雄港警局等單位在昨天緊急收網，分別在台南縣及嘉義縣市逮捕七人。

[金融]

1. 工會爆料：彰銀股東個資外洩[447]

[446] 2007-06-01/聯合報/C2 版/高市澎縣新聞

[447] 2008-11-04/聯合報/B2 版/錢線焦點

彰化銀行預定本月 21 日召開股東大會，改選董監事。但彰銀工會昨天爆料，近日彰化銀行股東個人資料外洩，甚至有自稱受委託收購委託書的相關機構假冒財政部和彰銀工會名義，向股東收購委託書。
財政部國庫署長蘇樂明昨天表示，冒名徵求委託書是有刑責的，至少涉及詐欺罪，財政部已進行了解，如果確有其事，一定依法處理。
蘇樂明說，他日前聽到相關訊息，第一時間聯絡台新金控總經理林克孝和彰化銀行總經理陳淮舟，但他們兩人完全不知道有這樣的事，已允諾會去了解。
彰銀工會指出，已向財政部提出檢舉。財政部表示，將請金管會調查。
彰銀本月底的董監改選牽涉董監席次分配，主要股東台新金、財政部都出面徵求委託書，彰銀工會也插一腳。市場人士指出，台新和財政部已對席次分配達成默契，在 9 席董事中台新 5 席、財政部 4 席；財政部的 4 席包括 2 席獨立董事。
彰銀工會呼籲，股東若發現自己是被相關機構以假冒財政部和工會名義收購委託書，可以向大華證券查詢，並撤銷委託。

2. 固定密碼資料容易外洩…
信用卡動態密碼 安心付款[448]

網路購物屢見駭客入侵，很多消費者都擔心資料外洩。台塑網科技、法德科技、萬事達卡國際發卡組織與新光銀行最近合作，未來信用卡登入認證時，每次都會產生新的一次性密碼，取代原先慣用的固定密碼，讓消費者不必擔心木馬程式或駭客截取帳號密碼，阻絕駭客或個人資料外洩等問題。
台塑網是長期經營全國最大 B2B 的電子交易，每年交易金額超過 2,000 億元，爲了嚴格要求資訊控管，與科技業者共同研發「信用卡動態密碼認證及動態安全付款系統」，建立身分認證平台，讓付款更安全。
台塑網表示，過去網路購物使用信用卡時，除了必須要通過網站登入帳號密碼認證，在網路結帳付款時，還要輸入一連串的數字，如信用卡號、到期年月、姓名或卡片後面三碼與身分證字號等資料；使用一次性密碼，只要透過攜帶式讀卡機產生一次性密碼，經由銀行端系統演算，就能確認持卡人的身分，完成付款授權。
簡單來說，持卡人每次登入網站交易，都會產生新的一次性密碼，取代原先的固定式密碼，消費者不必擔心木馬程式或駭客截取帳號密碼等資料，購物網站也無法得知信用卡的詳細個人資料，以阻絕駭客或個人資料外洩的問題。

[448] 2008-06-05/經濟日報/C2 版/致富寶典

3. 網路報稅 當心駭到你[449]

上網報稅已經成爲國人報稅的重要管道之一，但不論在家或在公司利用網路報稅，都要小心駭客隨時都在網路中。網路資安公司賽門鐵克表示，除了木馬程式外，更要注意 USB 病毒，這些往往都在使用中無意將個人資料外洩。賽門鐵克表示，一般來說，網路報稅會洩漏個人資料，最容易出錯的還是人爲因素，最常出現情形是報稅民眾網路安全知識不足，誤擊電子郵件中的釣魚網站，進而導致木馬程式入侵。

以賽門鐵克三月份的垃圾郵件的資料指出，網路報稅盛行的美國，駭客往往藉著報稅季的熱潮，寄送假冒國家稅務單位的釣魚郵件，誘騙收信者下載病毒或惡意報稅軟體，企圖竊取個資與信用卡資料。

因此在家中或公司報稅，使用的電腦最好不要有 P2P 軟體，即使用外掛的程式，同時要有安全軟體包括是否有入侵偵測，及還原備份等功能，其次報稅上傳成功後，最好備份於其他行動硬碟，刪除原來連網的資料。

此外，避免進入釣魚網站，最好以手動鍵入 URL 網址，或是從「我的最愛」中進入網站。每年要利用網路報稅時，最好都前往財政部電子繳稅服務網站，下載最新版網路報稅程式。網址爲 http://tax.nat.gov.tw/index.html。

賽門鐵克個人消費性產品事業部系統工程師王世煜表示，報稅季節一向是駭客活動高峰時節，僅依賴安全網路報稅系統還不夠，報稅者還需要建立正確使用習慣，才得以防止個人資料外洩的可能性。

4. 申報點上網報稅 個資不會外洩[450]

桃園市盧小姐來電：到國稅局輔導申報服務地點做網路申報，是否會有個人資料外洩的情形？

北區國稅局桃園縣分局答覆：前些日子發生報稅時資料外洩，是因納稅義務人個人電腦安裝分享軟體，該分局 96 年度所得稅申報期間所設置的申報輔導教室使用的電腦並無安裝分享軟體，在協助民眾報完稅後，會將資料另存磁片由民眾自行帶回，並不會存在硬碟內。另外，每天均有資訊人員做資訊安全的確認，請各位鄉親安心使用申報。

5. 擔心個資外洩網路報稅減少[451]

---

[449] 2008-05-22/聯合晚報/A14 版/社會

[450] 2008-05-22/經濟日報/A17 版/稅務法務

[451] 2008-05-13/聯合報/C2 版/台南市新聞

96 年度綜合所得稅開始申報多日，財政部國稅局鼓勵納稅人善用網路報稅，日前卻傳出網路報稅導致個人資料外洩，讓許多想用網路報稅的人心生膽怯，改用現場辦理。南區國稅局表示，受資料外洩影響，影響納稅人網路報稅，網路報稅人數也比往年少。

據財政部財稅資料中心查證，部分納稅人家中電腦裝有 P2P 分享軟體，如 FOXY 等傳輸軟體，容易被人擷取上傳網路的資料。「保險起見，寧願到國稅局排隊。」多名上班族利用上班空檔專程到國稅局申報所得稅，大多都是擔心個人資料被盜取，乾脆親自現場申報以求心安。

南區國稅局服務科長鄭月嬌表示，即日起納稅人在啓用報稅軟體前、後皆會顯示警語，建議上傳報稅資料期間，關閉或移除分享軟體。完成報稅後將資料檔儲存於隨身碟，並將硬碟內的資料刪除，避免遭不肖者竊取。

鄭月嬌說，只要避免使用分享軟體，網路報稅仍是非常隱密、安全且快速。申報期間以金融或自然人憑證報稅還可參加抽獎，獎品有機車、摺疊式腳踏車與百貨公司提貨券等，洽詢電話 2298007。

6. 自然人憑證 下月起中午可辦[452]

報稅季節又到，新黨台北市議會黨團昨天指北市申請自然人憑證的比率仍不到一成，爲方便市民辦理網路報稅，要求市府延長戶政事務所申辦自然人憑證的時間，讓上班族也能撥空辦理。

民政局指出，各區戶政事務所因應 5 月申報綜合所得稅，5 月 1 日起中午均可受理民眾申辦自然人憑證；5 月 26 日至 30 日止，除中午彈性上班，夜間也延長上班至晚間七點。

新黨市議員侯冠群、王鴻薇、潘懷宗等昨天舉行記者會指出，具有網路身分證功能的自然人憑證，舉凡報稅、申辦電子戶籍謄本、查詢車籍、查詢違規罰鍰、健保個人資料等，提供 841 項網路服務，有了自然人憑證，在家上網就可輕鬆享受政府 E 化服務，也降低個人資料外洩的危險。

王鴻薇表示，自然人憑證已開辦 5 年，但北市至今只有 19 萬 8000 人申辦，申辦比率不到一成，與很多上班族要請假申辦的因素有關，市府應考慮便民，讓上班族可以抽空申辦。

民政局表示，申請自然人憑證十分簡單，只要年滿 18 歲，備妥國民身分證正本及規費 275 元，就可到任一戶政事務所辦理，並可當天領卡。

相關問題可就近向戶所查詢，或向民政局便民專線 23450258 洽詢。

[452] 2008-04-24/聯合報/C2 版/北市要聞

7. 電子錢 Smart Pay[453]

想在網路上買東西，又擔心個人資料外洩？銀行公會宣布發行「無記名」小額晶片儲值卡「電子錢 Smart Pay」，防止資料外洩，父母也可以用這張卡控制孩子的零用錢，不必擔心卡債問題。

去年底台銀、合庫銀、新光及元大銀行等 4 家銀行已與台北縣政府合作發行「電子錢 Smart Pay」旅遊認同卡。農曆春節後，各銀行將正式對外發售「電子錢 Smart Pay」，可在實體商店及線上購物、繳費、繳稅，餘額並可贖回。

8. 跨售搶客戶 消費者保護不周全[454]

星期五下午，在科技公司上班的志雄（化名）趁著休假，想到銀行辦外幣存款、約定轉帳，順便再買基金，走進銀行營業大廳，抽了號碼牌第 96 號，等候人數多達 25 人。

志雄利用時間先去找理專辦基金申購，理專一邊處理基金，一邊幫志雄處理其他的臨櫃業務，志雄省去排隊，理專一口氣幫忙搞定。

一站購足 有利有弊

金控成立以來，標榜 one-stop-shopping（一站購足），金管會主委胡勝正說，「我信任你，我就跟你買，不必再去找其他金融機構，非常方便。」

金控時代掀起的跨業行銷風潮，不僅金控子公司內部互相跨售，即使是沒有加入金控的金融機構，也流行起異業策略聯盟。例如保誠集團入股玉山金，獲得銀行保險的好處，全球人壽也與台新金合作，同樣著眼於銀行保險。

金控跨售搶客戶，提供客戶很多好處。舉例來說，很多銀行推出「購買理財商品，存款加碼」的活動。只要客戶購買基金、保單、連動債券等，存款利率就可加倍。

消費者可以在一家金融機構，購買不同金融產業的商品，還可以獲得優惠或折扣，雖然不能說這是金控成立帶來的好處，但金控成立帶動市場競爭，的確讓消費者購買各類金融商品更方便。

「金控提供便利的金融服務，但商品項目不一定很精專。」實踐大學風管與保險系主任彭金隆說，金控的商品委員會評估那個產品獲利高，決定上架的多半是標準化商品，不見得滿足所有消費者的需求。

金鼎投顧董事長魏哲楨說：「有些消費者就不一定喜歡一次購足的金融商品，反而比較喜歡從不同專業領域的金融機構，提供金融服務。」

這種說法是否成立，從以下營業員與投資人的一段對話窺知一二。

---

[453] 2008-01-24/聯合報/B2 版/錢線焦點

[454] 2007-12-26/經濟日報/A4 版/金融新聞

一位在金控旗下券商任職的營業員小陳（化名），在上層長官的業績壓力下，前幾天打電話給中實戶老王，希望能拓展股票以外的基金、保險等商品。
「王先生，我們金控現在買基金、保險有優惠折扣喔！你要不要參考看看。」小陳說。老王回道：「不需要啦！股票才是我的興趣，我老婆已經跟銀行理專買基金，另外，我小姨子就在拉保險了。」
小陳認爲，專業領域的商品，須由專業人員來銷售較占有優勢。舉例來說，營業員可能對上千檔的上市櫃股票如數家珍，但對國內基金、海外基金，甚至壽險、產險等的專業知識，就不如銀行理專或保險員了，無法進一步提供更精細的商品，供不同消費者選擇，也會大幅降低交叉行銷的成功率。
個資外洩 最受詬病
金控時代下的消費者，另一個困擾是，不想要 one-stop-shopping 的人，可能常感受到被騷擾。
金控成立前幾年，不少民眾會接到金控主動推銷的電話，或接到金控子公司寄發的垃圾郵件，讓消費者感覺煩不勝煩。
「每一個消費者對金融產品的感覺不一樣，有人喜歡聽別人推薦，但有人不喜歡」。長期關注消費者保護議題的金管會銀行局主秘蕭長瑞說。
胡勝正表示，金管會嚴格要求銀行落實個人資料保護措施，沒有顧客的同意，不能把客戶名單交給其他子公司。
行政院消保會公布的 2007 年十大熱門消費新聞排行榜，消費者最在意的就是，個人資料外洩問題。
金控跨售行銷不能說是個人資料外洩的禍源，但一位外資券商主管說，這段期間資訊保護問題嚴重，業者爲了競爭，殺價、搶資料、搶客戶，消費者權益的維護，的確需要再加強。
尤其是，金控時代銷售的商品，從單一走向多元結構，風險係數複雜，業者行銷時有無充分告知，都攸關消費者權益。
彭金隆還點出另一個金控時代下值得消費者思考的問題，他說，金控追求綜效的成果，理論上是業者跟消費者共享，但這六年來，金控市值大增，大股東創造更多的財富，卻未明顯看到消費者享受到價格下降的好處。
一位資深金融界人士說，金控業者無法在價格上明確回饋消費者，可能也跟金控的 cost saving（節省成本）成效不彰有關。
他表示，金控應該對消費者做好顧客關係管理（CRM），進一步提供消費者更好的服務。對於消費糾紛處理，最好要有一套標準化流程，總之，金控時代下的消費者議題，金控需要加強的地方還很多。（系列三）

9. 靜止戶條款與消費權益[455]

日前在消基會調查之七家銀行中，有六家銀行已規定有「靜止戶條款」。所謂「靜止戶條款」，亦即銀行表明如消費者帳戶內之餘額未達一定門檻，且於半年至二年之期間內，消費者並無存款與提款記錄者，即會被列爲靜止戶，而不再有孳息。惟此攸關存戶權益之訊息，各銀行並未明確告知消費者。

據消基會調查指出，上述六家銀行中，竟有四家銀行並未於契約中載明被列爲靜止戶之確切餘額爲何。而四家銀行中之三家銀行，則以「貴行得隨時調整之（指最低存款餘額）」作爲約定內容。然而，銀行雖於契約中事先加以記載，但依消費者保護法施行細則第 12 條規定「定型化契約條款因字體、印刷或其他情事，致難以注意其存在或辨識者，該條款不構成契約之內容...」。因此，依財政部 89 年之行政命令：「金融機構應於存款契約中載明有關靜止戶之規定內容，並以粗黑字體標示，以提醒消費者注意，善盡告知義務；對於轉入靜止戶之存款戶，應刪除收取手續費（服務費）之約定。」換言之，業者如未以加大、加粗或以其他顏色的字體揭示上述訊息，即係違反規定。

實務上，近年來由於銀行業者對於客戶的個人資料保護太過鬆散，並未盡到嚴加保護之責，讓歹徒有可趁之機。有些思慮比較單純或對銀行業務未甚瞭解的客戶，因爲不知其銀行帳戶、電話、地址等重要資訊業已外洩，在全無防範之心的情況下被歹徒詐騙，以致一生積蓄被騙一空的事件，屢有所聞。因此，金管會遂於 94 年間要求，金融機構辦理客戶臨櫃匯款時，或以存款機存入款項時，如發現有異常疑似受騙等情形者，應協助提醒或勸阻客戶，必要時通知警察機關協助處理。可惜，銀行業者大多言者諄諄，聽者藐藐，「把關」的效果仍相當有限。而個人資料外洩之情事，對客戶而言非同小可，某些單位卻仍草率行之，實令人對消費者之權益，深覺不平與不安。

晚近銀行業者業務競爭激烈，生存不易，金融機構爲救亡圖存，本應從如何加強對客戶的服務，提高顧客的往來意願等著手。惜許多單位捨此之途，反而在如何占消費者便宜上錙銖計較。據消基會調查指出，目前銀行業者除「靜止戶」不計息之資訊模糊不明外，其他不利消費者之條款，尚包括：「起息點不明」「錯帳要消費者自行舉證」「抵銷或喪失期限利益條件太嚴苛」「金融卡掛失處理不合理」「變更約定，銀行說了算」及「除外責任，全由銀行自己訂」等。在自由競爭市場之我國，這些不合理的現象居然也能大行其道，倒是令人有時空錯亂之感，亦足見我國消費者對消費權益之自覺，仍有待提昇。

[455] 2007-08-21/經濟日報/A12 版/觀點

基於保護消費者權益之立場，我們期待銀行業者至少要盡到善良管理人的注意義務。例如銀行客戶中，如有所謂「靜止戶」，應儘速清查，利用各種資訊管道，以盡到通知客戶的義務，而不應動輒以「靜止戶」之名，達到「謀取利益」之實。此外，針對前述對消費者不利之某些措施，金融業者應以誠信爲本，適時予以檢討，並主動爲必要之修正，因爲惟有業者積極維護其正面之形象，才能取得消費者更大的信賴，而消費者真心的信賴，才是維持商譽和長期營業利潤的最佳利器。「靜止戶條款」如此，其他政策之推動，亦復如此，金融主管機關和各銀行，萬萬不可在保護消費者權益的前提下，有所疏忽。

（作者是消費者文教基金會董事兼財務長、台北大學法學系教授）

10. 恐嚇個資外洩 一天詐 200 萬

詐騙集團「亂槍打鳥」 哄騙轉匯「安全帳戶」 女保險員上當 52 萬泡湯[456]

警方發現最近「假資料外洩」的詐騙案件增多，不少被害人誤將存款轉匯到「安全帳戶」，積蓄被騙一空，有女保險業務員上當匯出 52 萬多元，還是她父母發現不對勁，昨天陪她報警。

基隆市警局刑警大隊偵四隊調查發現，成立詐欺專責組 3 年多來，爲防範詐騙犯罪不遺於力，本市被騙發生數也由 94 年每周 8.84 件，降到 95 年的 6.96 件，今年統計到上周，平均每周 5.24 件，雖有下降，但詐騙集團「亂槍打鳥」仍會命中。

偵四隊最近發現假籍各機關名義，通知民眾「個人資料外洩」的被騙案件增加，騙民眾不懂法律，恐嚇涉及洗錢或詐欺會被凍結名下財產，使民眾陷入圈套，提出存款匯入「安全帳戶」，進而提領一空，本月 11 日一天內就接獲 4 件，被騙近 200 萬元。

昨天上午又有人被騙，一年輕女保險業務員由父母陪同報案，偵四隊長黃垂郎指著牆壁上張貼的報紙剪報，提醒他們詐騙的類型，她父母說她平時工作忙，無暇看報，不知有這麼多詐騙技倆；她接獲詐騙電話父親就在身旁，但騙徒警告她不能告訴別人，她才沒找父親商量。

她說，前天上午她手機接到刑事偵查科警察的電話，說她賣帳戶涉嫌洗錢，她說不可能，對方就說她個人資料外洩，被人冒用開戶，問她有哪幾家銀行戶頭，她據實以報，對方就說相信她的清白會和檢察官說明白，後來就有書記官打來，叫她把錢領出來存入安全帳戶。

[456] 2007-05-19/聯合報/C2 版/基隆要聞

她擔心對方所說，若未趕在中午 12 時前處理好就會被起訴，趕緊把 28 萬元匯給對方，又將一筆定存解約，將 24 萬 9000 元再轉匯出去。由於還有 8 萬多元的存款由母親保管，她轉向母親要錢，她父母一問，才知女兒上當。

11. 大陸駭客入侵

So-net 上千客戶資料外洩

信用卡遭盜刷 銀行指業者負擔 警方擔心會員資料將成詐騙工具[457]

台灣索尼通訊網路 So-net 網站日前傳出被駭客入侵，會員網友個人資料外洩、信用卡被盜刷，被盜刷的信用卡張數約一千八百四十張，國內幾乎所有發卡銀行都中獎。

So-net 網站是由中國信託商銀收單，由於 So-net 網站可能未盡到保護客戶資料職責，銀行認爲，目前初步清查發現約有五百多萬元的信用卡盜刷損失，應該由業者（即 So-net）負擔。

警方表示，此次駭客入侵 So-net 網站，雖然損失金額有限，但警方擔心，這些駭客除了盜刷客戶信用卡資料外，還同時擷取客戶的姓名、身分證字號、住家公司電話、手機、親屬聯絡人等資料，這些資料可能成爲詐騙集團的行騙工具。

台灣索尼通訊 So-net 網站是台灣前三大提供 IP 位址網站，該網站還有線上購物、影音加值及遊戲中心，相當受網友歡迎。但卻傳出會員資料外洩案，刑事警察局清查發現，So-net 公司內，有六成以上電腦都被植入木馬程式，疑似遭大陸駭客入侵，導致 So-net 上千名會員個人資料遭側錄外洩，信用卡被盜刷或做預借現金。

辦案人員說，這些駭客可能來自中國大陸，以俗稱「釣魚網站」的假網頁，或郵寄電子郵件、圖檔等方式夾帶木馬程式入侵，So-net 員工甚至高層幹部都不知自己的電腦已中毒。事發後，So-net 內部已緊急加強系統防火牆，確保會員資料不再外洩。

警方調查，大陸駭客藉假網頁入侵 So-net 後，以遠端搖控及側錄鍵盤動作的惡意程式，藏伏在 So-net 公司員工及幹部電腦，並搜尋擷取 So-net 會員信用卡資料，包括地址、消費額、卡號、有效年月及信用卡背面檢核碼等，拿到資料後，就到其他網站盜刷購物並向發卡銀行預借現金。

台灣各大發卡行上月發現 So-net 網站出現資料外洩案，報警清查發現，幾乎所有的發卡銀行都中獎。最大發卡行、中國信託商銀近廿筆，平均每卡損失

[457] 2007-02-23/聯合報/A4 版/綜合

從數百元到數千元不等。

[電信]

1. 竄改來電顯示 婦人被騙 58 萬[458]

詐騙集團常利用網路電話或節費器等通訊器材更改來電顯示號碼，取信詐騙對象，嘉義市周姓婦人為此信以為真，被騙 58 萬元，市警局昨天強調，請民眾詳查及立刻報警最重要。

周姓婦人報案說，前天接到自稱台中市民權郵局人員電話，聲稱 1 名男子到郵局要提領她帳戶存款，由於她未在民權郵局開戶，而且也不認識領款的男子，儘管「郵局人員」口氣急迫，一再提醒，但她不予理會。

她才掛斷電話，又有自稱「陳宏源」警官來電，指她的帳戶涉及洗錢，警方已移由檢察官偵辦，接著再接到自稱法務部行政執行署書記官「陳玫玲」電話，要求她配合偵辦，同時不能任意讓旁人知道；她見電話沒有「來電顯示」，表示懷疑。

「陳玫玲」要周姓婦人打 105 查詢執行署電話，對方還傳真「個人資料外洩授權止付聲明書」及「法務部執行假扣押處分令」給她後，再來電時電話顯示與周姓婦人查詢的號碼相同，她不疑就依對方指示陸續將存款匯到指定帳戶，輾轉之間被騙 58 萬元。

市警局查證後強調，詐騙手法不斷翻新，詐騙集團知道透過網路電話或節費器等設備，更改來電顯示號碼，如果被害人未再深入查證，很容易就落入詐騙集團的陷阱。

2. 投機怕外洩
私密沒刪光 小心變冠希[459]

消費者過去汰換舊手機，最常見的兩種處理方式，一是擺在家裡抽屜中，一是拿到市面的通信行回收，但這兩種方式都不環保，後者甚至可能有個人資料外洩的風險。

仔細看每支手機的構造，多少都含有可再利用金屬的成分，不少通信行會以每支五十元到一百元的價格回收廢棄手機，即使如此仍有很多民眾不知道有此管道，隨意把舊手機丟在家中，更不環保的就隨垃圾一起丟棄。

---

[458] 2008-06-19/聯合報/C2 版/嘉義縣市新聞

[459] 2008-04-01/聯合報/A9 版/生活

環保專家指出，這些被淘汰的手機若當成一般垃圾掩埋或焚化處理，裡面的有害物質就會進入大氣、土壤和水源，間接或直接危害人類健康。手機除了多種有價金屬外，也含有鉛、汞、鎘、鈹、含氯塑料（ＰＶＣ）與溴化阻燃劑（BFRs）等有害物質，例如電池裡的重金屬鎘會嚴重汙染水源和土壤，充電器及配件的線材若含有ＰＶＣ，焚化會產生世紀之毒戴奧辛，手機機板的元件使用鉛焊接，鉛會對中樞神經系統造成嚴重傷害。

較有環保意識的消費者，拿到通信行回收或變賣，仍有個資外洩與未達真正環保的疑慮。許多通信行願意拿錢收購廢棄手機，一部分是爲了拆下可用的零件用來維修其他手機，也有的是轉手賣到第三世界國家處理，仍會造成當地的環境汙染。

過去曾有名人手機中的私密照片外流，可能是因爲消費者未清除廢棄手機上的個人資料，就拿到一般通信行回收。專家建議，民眾回收手機前除了應將電池取出分開外，不要忘了先刪除或格式化（format）手機內的個人資料。

3. 誤信門號推銷個資外洩涉詐欺[460]

申辦電話門號要注意！台北縣刑大今年 8 月偵破一個虛擬的溫泉度假村詐騙案，循歹徒使用的人頭帳戶追查，日前約談台中縣一名王姓女子到案說明，她懷疑是在申辦行動電話門號時造成個人資料外洩，無端捲涉詐欺案被移送，讓她不斷喊冤。

由於過去也有人頭帳戶申請人質疑被電信業者冒用身分申請帳戶，警方呼籲民眾申請電話門號，最好直接到門市申辦，不要輕信來路不明的電話推銷。王女說 4 月接獲自稱某電信業者客服人員電話推銷，對方還派人專程將門號及贈品送到她公司，她將身分證影本交給電信公司委託的快遞人員，沒想到會被歹徒用來冒名申辦人頭帳戶。

4. 手機來電顯示 又騙走 320 萬

詐騙集團冒充警方取得存款銀行電話 篡改顯示要求轉帳 誤信銀行打來 退休公務員破財[461]

宜蘭縣又見手機顯示爲金融機構電話的詐騙案；一名楊姓退休公務人員，見手機顯示的號碼爲其存款的銀行，誤信詐騙集團的謊言，以爲他的資料外洩，擔心存款被查封，而騙走 320 萬元。宜蘭縣警察局刑警大隊已著手偵辦。

---

[460] 2007-12-08/聯合報/C2 版/北縣要聞

[461] 2007-09-26/聯合報/C1 版/宜蘭・教育

「金融機構不會於晚上用電話與當事人聯繫！」刑警大隊反詐欺專組組長田獻廷說，科技日益發達，歹徒的詐騙手法也更加狡詐，篡改手機來電顯示，已經不稀奇，因此民眾不要盡信手機的來電顯示；一般來說，金融機構與公家單位晚上不上班，當手機顯示的電話碼是金融機構或公家單位時，民眾就應有所警覺；最好方式是自己主動撥回去查詢。

五結鄉一名退休的楊姓公務人員，前幾天接到一通電話，對方聲稱是台中警方人員，楊因個人資料外洩，存款遭歹徒冒用，台中地檢署偵辦後，將查扣楊的存款，對方還表示願替楊向楊的存款銀行說明，要楊先告知存款銀行的電話號碼；楊不疑有他，當下告知存款銀行的電話。

沒多久，楊的手機顯示存款銀行的電話，楊誤信是銀行打來，加上對方聲稱得知楊的帳戶遭歹徒冒用情事，更讓楊信以為真；因而聽信對方謊言，到自動櫃員機轉帳，先被騙了 9 萬元；翌日上午對方再來電，楊將存款全數轉出，一共被騙了 320 萬元。

田獻廷說，電話詐騙集團幾乎都是兩岸不法分子聯手犯案，他們透過「雙模機」不僅可以篡改手機的來電顯示，也及時阻斷手機的電話通聯，讓警方無法繼續追查下去，偵辦的難度相當高；不過，電話詐騙集團必須抓住民眾的貪、怕、急等心理弱點，才有得手之機；民眾一旦接獲可疑的電話，哪怕手機的來電顯示是自己熟悉的電話號碼，只要冷靜下來查詢，則可避免上當失財。

5. 少年駭客再犯 竊個資千萬筆

高中時 入侵總統府網站 畢業後 入侵大考中心網站 事隔兩年遭黑道吸收[462]

曾經入侵總統府網站，宣布愚人節放假一天的駭客蘇柏榕又再度犯案，這次他和林姓高中生分別入侵中華電信等各大網站主機，竊取內部資料販售，警方估計已有上千萬筆個人資料外洩。

初步統計，曾犯妨害電腦使用罪的蘇柏榕（二十二歲）入侵網站，還有台大批踢踢、無名小站、PChome、雅虎、Google、十九所桃園地區國中、EZpeer、台灣深藍網站、艾噹洛學院、卡提諾論壇等。

警方表示，當年蘇柏榕就讀建中時，以高超的駭客手法入侵總統府網站，宣布愚人節放假一天；高中畢業後，又入侵大考中心網站盜竊考生資料引起全國震驚。

[462] 2007-09-22/聯合報/A16 版/社會

當時刑事局偵九隊隊長李相臣逮捕他時，因珍惜他的天才電腦能力，怕他遭黑道利用，還要他天天到刑事局報到，親自輔導他考上大學；想不到事隔兩年，蘇柏榕仍遭黑道吸收，盜取各大網站個資。目前擔任刑事局科技犯罪防制中心主任的李相臣昨天再度逮捕他時，難掩失望。

警方指出，現就讀聯合大學、網路暱稱爲 CB 的蘇柏榕，和就讀高中的林姓少年（十六歲），兩人因爲傑出的電腦入侵能力，遭有黑道背景的駭客盯上，吸收入侵各大知名網站後，盜取資料轉賣給補習班、詐騙集團等團體，牟取數十萬元的利潤。

刑事局表示，他們日前接獲由建中、北一女學生組成的台灣深藍網站報案，指出網站遭人入侵，經過追查後，發現蘇柏榕涉嫌。

警方連日追查，發現駭客集團利用一名不知情的交通大學數學系學生，透過他在學校宿舍的伺服器，連上交通大學網路主機，以交大網路當跳板，開始入侵中華電信及台大批踢踢。林姓少年則在家中入侵其他網站。

令警方震驚的是，兩人入侵網站如入無人之境，林姓少年甚至取得雅虎的網站運作程式，商業機密可能外洩。警方驚覺事態嚴重，昨天在蘇、林兩人住處、交通大學展開搜索，並將兩人帶回警局偵辦。

警方發現，兩名駭客除以各種手法入侵網站，還利用免費的學術網路，將竊取資料存放國外主機，躲避警方追緝。

6. 透視台灣 e 競爭力數位台灣系列報導之一 數位台灣 e 化生活有成[463]

我國從 2002 年推動數位台灣計畫以來，已爲民眾生活帶來許多好處。行政院決定五年 556 億元將台灣建設成爲優質網路社會 (Ubiquitous Network Society,UNS)。

行政院政務委員林逢慶指出，台灣網路使用人口已超過 1400 萬人，個人連網普及率超過 6 成，光是今年有超過 240 萬民眾使用網路報稅，初步估算就節省 45 億元社會成本。

寬頻網路是數位台灣最重要的基礎建設，交通部郵電司長鄧添來指出，數位台灣計畫從 2002 年啓動時，就設定 6 年 600 萬寬頻到家，打造台灣成爲亞洲最 e 化的國家，到 2007 年第一季統計，已達 552 萬戶，超過了預定進度，年底可達成 600 萬寬頻用戶目標。

[463] 2007-11-01/經濟日報/E2 版/數位商機

鄧添來認爲，未來要邁向優質網路社會，一方面要繼續推動寬頻網路建設，無論是 ADSL、3G 上網，爲了達到無縫隙的寬頻服務，WiMAX 無線技術可以解決偏遠及有線寬頻無法到達的地區。
政府將建置高速寬頻有線暨無線網路，鼓勵發展食、醫、住、行、育、樂等與民眾生活相關的應用，持續推動電子化政府創新服務，創造公平數位機會，創新科技化服務產業，將台灣建設成優質網路社會。
在數位台灣計畫中，政府與學術研究機構已做了先導型研究計畫，針對 32 位元 IPv4 網址編碼不敷使用，已提前著手規劃 128 位元 IPv6 網址編碼，未來每個人的生活空間中，不再只是一台電腦上網，而是所有居家物品都有網址，都可以上網，更容易自動化控制。
針對網路社會興起，內政部與相關單位在數位台灣計畫實施期間，已大力推動「網路身分證，一卡在手更便利」，政府服務 24 小時不打烊，民眾只要向內政部憑證管理中心申請「自然人憑證」，不必再跑政府機關，只要在辦公室或家裡上網就可享受 e 化服務，降低個人資料外洩的危險，自然人憑證就像「網路身分證」一樣。
數位台灣計畫項下之（e 化生活分項），分爲數位學習、數位典藏、數位娛樂、網路文化建設、故宮文物數位博物館、不動產資訊、網路健康服務、e 化交通、關懷 e 起來、交通安全、智慧型都市交通控制、安心住家、社會安全保障，是由內政部次長簡太郎召集相關單位，建設網路化社會。
內政部資訊中心主任沈金祥指出，數位台灣應該以民眾謀福祉爲目標，經濟部著重居家用品感測化，內政部建置優質社區安全防護，交通部有移動車機生活服務，國科會推動情境式學習服務，農委會輔導業者建立生產履歷商品，衛生署希望從健康角度推動緊急醫療網，讓民眾生命健康獲得及時的保障。
政府並未忽略網路文化建設，文建會資訊小組組長王揮雄表示，除了將文化資產、古老照片、民間信仰予以數位化典藏，同時也提出活化台灣數位文化內涵的新觀念，新作法，讓民眾可以透過寬頻網路瀏覽典藏文物。

[其他]

1. 個資法立法 保護民眾權益[464]

與會者：
行政院研考會資管處處長何全德

[464] 2008-05-12/經濟日報/A15 版/座談會

中華民國資訊軟體協會秘書長張國鴻
中華無店面協會理事林坤正
主持人：經濟日報副主任王花順
記錄：陳家詡
攝影：毛洪霖

近來個人資料外洩事件不斷發生，在沒有完善的法律約束管制下，有些不良企業鑽法律漏洞，民眾求助無門。有鑑於此，中華民國資訊軟體協會舉辦第二場個資法座談會，透過各界專家的意見，期許政府能夠快速通過個資法，不僅民眾權益受到保護，企業也可依循，在良好的互動機制內開創更多商機。本次座談會邀請到行政院研考會資管處處長何全德，談政府機關如何保護民眾的個人資料不外洩、以及未來強化對基層機關人員教育訓練；中華民國資訊軟體協會秘書長張國鴻，談軟體產業如何協助企業做好資訊安全、證據保全及教育訓練等，並建議對企業進行資安分級認證；中華無店面協會理事、康迅（Payeasy）總經理林坤正，談先前 Payeasy 個資外洩後，其危機處理做法提供業界參考，並從企業面來看待個資法。

行政院研考會資管處處長何全德
立法保護 迫在眉睫

何全德：就政府的角度來看，政府本身建置有 2,300 萬筆重要個人資料(例如戶政資訊)，所以政府本身應以身作則，好好保護這些資料，特別是在高度資訊化的社會，不小心洩漏可能就是一筆龐大資料，相對而言，個資法立法及施行可說相當迫切。

所以行政部門希望立法院能夠趕快通過個資法，因政府本來就有責任保護民眾個人的資料，在新政府上任後，期望再次檢視個資法內容。例如，個資法已不是只保護個人資料，也要對於未來數位網路時代的需求，建立資訊人權的廣義概念，即是建立公民權，爲未來網路社會建立穩定的經濟秩序，激發新的商機及創新的經濟模式。

雖然研考會本身不是個資法的主管機關，但研考會推動整個政府 e 化，在新的個資法尚未完成立法前，研考會訂有相關行政命令及規範作爲各機關處理這議題的依據，以充分保護個人的資料，例如現在的行政規範規定如果有涉及到個人的資料就不能上網公開，不能把個人的基本資料隨便擺上網路讓大眾瀏覽。如果真的有上網的必要，就要符合一定的安全規範，例如個人資料的加密處理或電子認證，像網路報稅爲了便利民眾，民眾就必須要透過一些安全技術的程序處理。

當然這樣還不夠，研考會還會進一步推動相關措施，以加強保護個人資料，例如，訂定資安相關規範，推動資安及隱私保護訓練、國家資訊安全防護中

心致力於重要機關的資安保護工作。其實最有效的方法就是從基層訓練做起，例如教育公務人員、機關首長，把個人資訊保護工作當作是責任。此外，可以參考國外有第三者認證機制，由獨立客觀的第三者來幫公私組織認證，通過認證再給予證書，可有效客觀的落實個資保護。

但不可否認的是有時過度的保護會影響正常商業活動，所以如何在此議題取得平衡點也非常重要的，總括而言，希望立法院能夠快速通過個資法，以保障所民眾的個人資料和安全。

中華民國資訊軟體協會秘書長張國鴻

配套方案 盡速建立

張國鴻：修正後的個資法草案，對廣大的中小企業衝擊最大，因此在個資法通過前後建議政府應廣泛的徵詢各方意見，同時積極教育大眾、政府機關、民間團體，建立相關配套方案，所有軟協業者也願意全力配合企業界，制定更完善的資安制度，建構嚴密個資保護網。

個資法是現代資訊化保護隱私的進步立法，但是影響到企業的經營非常廣泛，企業不論大小都必須倚賴大量的個人資訊，如何在消費者隱私權保護與企業經營的效率與成本方面，求得合理的平衡，是行政院與立法院必須慎重考慮的。由於企業掌握的個人資料，都已經透過電腦處理與網路傳遞，使得問題的複雜度更爲增加，尤其是網路上日新月異的駭客手法，顛覆傳統法律上的舉證責任與損失的認定。

許多已經發生的案例中，被指控洩露個人資料的企業本身，其實自身也是備受駭客侵擾的受害者，但是在個資法是否得以免責或減輕責任，都是尚未釐清的問題，還有攸關賠償責任追究的舉證問題，和涉及的電腦鑑識專業知識，也少有專業領域人員。

個資法的通過與執行已箭在弦上，我建議行政院必須責成所屬部會，就其所主管的企業在個資法施行後可能遭遇的問題，與業界共同研究有效對策，此外，建議主管全國上市公司的金管會，應考慮如何有效稽核上市公司在資訊安全上的投入是否適當？假如上市公司從現在開始更重視各種資訊安全的防護，相信個資法未來施行後所可能發生的問題就少了一半。

尤其可以參考日本個資保護認證制度，透過具備公信力的認證制度，取得消費者對企業保護個人隱私的信任，另外對中小企業要加強宣導，提供各種有關法律、制度與技術方面輔導，才能將個資法實施後所產生的衝擊降到最低。軟體協會所屬的資訊安全促進會，會中的數十家資安廠商，可以說是「已經準備好了」，未來將組織一個資訊安全顧問服務團和政府攜手合作，共同推廣資訊安全的認知與各種技術方面的諮詢。

中華無店面協會理事林坤正

恐讓中小企業生存更困難

林坤正：其實目前台灣每天都在發生詐騙事件，可知台灣的個人資料已經遭竊十分嚴重。此外，據 Payeasy 先前被詐騙集團鎖定攻擊後，以及警方查證的結果，有許多詐騙攻擊來自對岸，業界相信台灣人民資料已被大量竊取，而對於個資法的訂立，似乎有點太慢。

但我們不能不重視個資法的訂定，建議應多由企業和相關單位討論出更具體、合宜的法案，以供未來遵循，而不是漠視一些正在發生的問題草率訂定法案，否則個資法通過後，會造成企業界另一棘手的問題，並致使中小企業生存更困難。

另一個要討論的問題是，目前有兩種個資竊取的方式，一是資料拼圖(Data Merge)，這種資料搜集的犯罪手法在早期郵購的時代就已經存在，郵購業者透過其他管道來取得個人資料，例如政府機關、大型組織機構等，並且會將每個人的資料連結起來，所以當歹徒詐騙時，可以很詳細的告訴受害者，讓人無從懷疑。此外，資料遭竊的程度，可能詳細到消費者何時刷過卡購物，然後誘騙受害者刷卡有誤，並到 ATM 轉帳，就成爲詐騙集團的獵物。

另一種常見的資料竊取的方式爲 SQL Injection，犯罪者會在大型網站或者大型企業資訊系統植入木馬程式，利用這些程式把用戶的資料盜走，企業、政府機關或物流廠商，如果採用較不專業精密的資料庫系統，就很容易資料遭竊，而所有的個人資料其實都是環環相扣，往往防不勝防，也很難釐清遭竊的源頭。SQL Injection 是目前歹徒竊取資料庫資料最常見的手法。

經過上次被詐騙集團鎖定的經驗，我建議企業未來如果遇到被鎖定竊取資料，最有效的作法是「正面迎戰、誠實爲上」，並且和歹徒搶時間保護自己的會員。例如 Payesay 先前在各大平面媒體主動發佈消息，同時在第一時間主動致電告知會員可能被詐騙的手法，雖然衝擊到業績，但卻可確實做到零詐騙，結果獲得更多會員再度肯定。現在 Payeasy 的業績不減反增，以上希望可以提供給大家參考。

2. 店員兼車手 超商內洗錢[465]

綽號「瘋狗」陳弘德爲首詐騙集團，涉嫌免費提供毒品，讓吸毒者四處收購人頭帳戶，再雇用超商店員擔任領錢「車手」，利用深夜在超商內設提款機洗錢。前後不到一年集團買到 300 多本人頭帳戶，得手千餘萬。

桃園縣近來發生多起假冒公務機關名義行騙案，警方雖然鎖定詐騙集團所使用特殊帳號，但怪異的是就是追不到負責領錢「車手」。

[465] 2008-06-19/聯合報/C2 版/桃園縣新聞

直到日前破獲一起搶奪案意外發現，該集團在台幕後首腦爲 37 歲、有毒品前科綽號「瘋狗」陳弘德，檢察官葉益發前天深夜指揮縣警局刑警大隊等單位兵分十路，將陳弘德等 8 人一舉成擒，並起出 300 多本人頭帳戶與成員私下聯絡專用「教戰守則」。
刑大偵三隊隊長侯振裕說，該集團與大陸綽號「順董」多人共組兩岸詐欺集團，再假藉公署或知名公司名義，打電話給被害人佯稱「網路購物」、「個人資料外洩」、「健保退費」、「假援交」等手段詐財；桃園縣政府教育處、工務處等單位最近遭詐騙集團以「公署名義」冒名詐財案，也是該集團所爲。
侯振裕說，全案中最特殊的是，大陸「順董」擔心陳弘德在台灣「搞怪」，還聘請有詐欺前科的吳智裕擔任在台「督導」，每天緊盯陳弘德行騙「進度」。
在台行騙首腦陳弘德爲了收購人頭帳戶，不惜以「供應毒品」手法，教唆吸毒者四處蒐購，人頭帳戶不乏有不知情的大學生、軍人和工程師身分。
不僅如此，陳弘德擔心警方追蹤，還特別雇用在超商工作有詐欺前科員工邱建庭擔任領錢「車手」，再利用邱建庭深夜值班機會，就在超商內設提款機「洗錢」。警方調查後依洗錢防制法罪嫌將 8 人移送。

3. 個資外洩案 傳藝人作證[466]

檢調偵辦個人資料外洩案，近日將約談被害藝人作證，詢問是否對買個資者提出告訴；另將有第二波約談涉嫌賣出個人資料的公務員行動。
檢調將陸續以證人身分約談個人資料外洩的藝人、名人，並出示個人資料給被害人看，再詢問是否提出告訴。檢方指出，違反個人資料保護法屬告訴乃論，必須有被害人提告，涉嫌下單買個人資料、非法蒐集買賣個人資料的業者如壹週刊等單位或個人才構成犯罪。
目前已知名模隋棠、歌手王心凌及劉文正、製作人詹仁雄、演員徐華鳳及前中姐張淑娟、前中華棒球隊總教練郭泰源、星光二班賴銘偉以及台啤球員何守正等都是被害人。檢調表示，該約談的都會約談。
據指出，檢調偵辦本案監聽近兩年，下一波將約談中南部警界、戶政、監理站人員。健保局台中分局職員陳芷瑜日前被檢調約談到案，她是負責保費業務的聘雇人員，權限只能看到繳費資料，但被洩漏的資料卻有多筆醫療紀錄，不排除另有人洩漏醫療紀錄給她再轉賣給個資集團。
檢調查出，涉及買賣個人資料的到案業者熊世芬，與其他業者幾乎都來自台中市，中部數縣市警界等公務員，將是下波偵辦個資外洩的重點對象。

[466] 2008-04-29/聯合報/A11 版/社會

4. 打檢察官名號詐騙 3 人起訴[467]

楊姓男子疑因個人資料外洩，致詐騙集團打著最高檢察署特偵組檢察官周士榆名義，誘騙他領出 510 萬元交付保管，警方逮捕取款的曾壽山、范姜群杰、彭晟烜。檢方將 3 人起訴，並求刑 2 年 6 月以上徒刑及強制工作。

檢方查出，今年 3 月 7 日下午 1 時許，曾壽山（32 歲）、范姜群杰（21 歲）、彭晟烜（22 歲）先在台北縣林口鄉會合，范姜、彭將曾的照片貼在僞造的台北地檢署監管科員識別章上。

同日，新店市楊姓市民接獲自稱台北市健保局潘姓女職員電話，告知他健保卡遺失，疑遭詐騙集團拿去設人頭帳戶，正由台中地檢署調查中。隨後，楊妻就接到自稱台中市警局警官電話，告知檢察官周士榆已發出 3 張拘票要逮楊。

不久，楊妻又接到「台北地檢署監管科科員江信哲」電話，佯稱有一筆詐騙集團非法詐騙的 510 萬元匯到楊的聯邦銀行帳戶，要她提領交由地檢署監管科代保管，以免其他帳戶的存款被拖累凍結。對方詳細說出楊的其他銀行帳戶取信楊妻，雙方約定交款地點。

楊姓男子與妻子趕到銀行領錢，途中擔心遭騙，打電話向健保局詢問，確認沒有潘姓女職員，轉而向警方報案。警員埋伏交款地點，逮獲曾壽山等 3 人。

台北地檢署偵辦時，范姜群杰供稱，看報紙廣告應徵收款員，綽號「阿峰」男子給他一支行動電話，要他等候通知收款，每收 100 萬元可分得 4 萬元；曾壽山供稱是看廣告應徵收款員；彭晟烜則說范姜臨時拜託他開車載到台北辦事，未參與犯案。

5. 防止資料外洩
檔案加密&確實刪除 保障安全[468]

網際網路及科技日漸普及，消費者的生活愈來愈離不開電腦，但「水能載舟、亦能覆舟」，在享受科技所帶來的便利之際，一個不小心，自己也會成爲受害者。

戰國策技術支援課主任胡邦元提醒，不管是視窗作業系統或是蘋果公司的 MAC 作業系統，只要讓有心人碰到硬碟，網路上隨處下載的回復軟體都可以找回已刪除的檔案。

---

[467] 2008-04-28/聯合報/C2 版/北基要聞

[468] 2008-02-24/經濟日報/A5 版/熱點

胡邦元說，一般使用者要清除檔案，通常是丟到資源回收筒裡，由於存取檔案的磁區未受到破壞，所以檔案仍然存在。胡邦元形容，假如電腦是一本百科全書，一般的刪除動作就像是拿掉目錄，但內頁不受影響。

不肖的工程師如果別有居心，可以透過維修電腦的機會，不管有沒有刪除，都可以竊取到重要檔案。雷米科技表示，免費回復軟體如 Undelete Plus、Finaldata 等，也有付費軟體 R-Studio。MAC 電腦也有專屬的回復軟體，例如付費的 Data Rescue Ⅱ。

莊正豪提醒，如果檔案不小心刪除，應該馬上停止任何電腦動作，馬上下載回復軟體進行資料救援。因爲電腦會主動暫存資料，新檔案如果不小心與刪除檔案覆寫在相同位置上，就無力回天了。

除了透過接觸硬碟偷竊電腦資料，網路也是一個漏洞。最近經常發生網路交易平台會員個人資料外洩，淪爲詐騙集團行騙工具的案件。胡邦元表示，部分駭客透過網路散布木馬病毒，如果民眾不小心點選，木馬病毒立即入侵電腦，使用者所有新增的鍵入資料都會以傳送副本的方式流出。也有另一類型的木馬病毒，會竊取系統控制權，讓有心人士可以任意進出你的電腦，自由盜取想要的資料。

電腦專家提醒：「檔案加密與確實刪除是保護資料的不二法門。」

例如 MAC 電腦使用者可以使用蘋果內建的加密檔案 File Vault，把重要的檔案轉成影像檔，透過密碼才能打開檔案夾。

如果要送修或賣出舊電腦，應該要將重要資料徹底銷毀。關於資料的確實刪除，胡邦元建議，使用者先對欲刪除的資料進行加密，如此一來即使有心人想回復資料，也需要進行繁複的解碼程序。接著，在資料刪除之後，最好進行磁碟重組，讓資料重新搬移、歸納。

電腦專家也推薦可以到網路下載點搜尋免費的刪除軟體，可以針對特定磁碟，進行刪除資料的「毀屍滅跡」。也有透過將整個硬碟覆寫方式，清除任何硬碟上的程式、文件與作業系統，所以使用前，務必確定需要的資料是否已經進行備份。

戰國策總經理林尚能說：「不管科技再怎麼防，但人心難防。」對電腦資訊維護公司來說，工程師因爲會經手公司與個人的機密資料，操守很重要。

林尚能表示，一般維修公司爲了維護資訊安全，除了對硬體、軟體建立「防火牆」，更會建立「防水牆」，進行內部人員控管。以戰國策爲例，面試工程師時，如果覺得有疑慮，公司會打電話到原任職公司探聽員工人品，並進行法律宣導，建立員工營業秘密保護意識。

目前電腦維修公司眾多，有個人工作室、也有學生兼差，品質參差不齊。林尚能建議，如果要維修電腦，盡量找具有商譽的資訊公司。這些公司通常愛惜羽毛，較不可能做出違背信譽的事情。

6. 微軟兩點不漏計畫 全面防盜[469]

市面上出現「幾可亂真」的 Windows 仿冒軟體，使消費者花錢卻當冤大頭。台灣微軟公司日前與燦坤及多家大型通路商合作推出「兩點不漏」軟體辨識計畫，協助消費者避免買到仿冒軟體。

第一點是建議消費者前往貼有象徵合法通路商標誌「安心採購店貼」的通路購買，第二點是透過 WGA 驗證，消費者便可確保購得正版軟體。

微軟法務長施立成表示，曾接獲消費者購買到仿冒軟體客訴案例。許多人在一安裝軟體後即「中毒」，一套軟體最高紀錄內含 20 個病毒。也有人因盜版軟體中暗藏木馬程式或間諜軟體而受害。除了容易產生系統執行失誤外，更可能使個人資料外洩，造成難以想像的損失。

施立成說，爲了協助消費者購買到正版軟體，台灣微軟提供「真品辨識四步驟」採購祕訣：(1)消費者在選購時需注意軟體是否向商譽卓著的經銷商購買？(2) 檢查產品內是否包含真品保證書 (COA)？(3)是否有全像圖 CD/DVD 或復原媒介物？(4) 產品包裝及元件是否爲高品質專業製造？消費者在購買軟體時，只要透過真品辨識四步驟，便可以初步確認購買到的是正版軟體。

7. 隱私評比墊底 個資法別拖了[470]

在英國的「隱私國際」與美國的「電子隱私資訊中心」新近公布二〇〇七年國際隱私權評比，第一次被納入評比的台灣，在全部四十七國中成績墊底，被列爲「監控盛行」的社會之一。

雖然這個評比依據的資料並非完全正確，例如報告中提到台灣設有全民指紋資料庫，即與大法官釋字六〇三號解釋宣告強制捺指紋規定違憲的結果有所出入。不過報告的其他部分卻點出了幾項台灣隱私保障的問題。

該報告提及台灣嚴重的個人資料外洩與詐騙情況，相信國人都有相同感受。尤其去年下半年從政府機關到網路、電視購物公司，一再傳出將個人資料在網路上「全都露」或是購物後隨即接到詐騙電話的案例，顯示台灣公私兩部門對於個人資料保護輕忽的態度。台灣在隱私權保障執法的成效也得到最差評價。

---

[469] 2008-01-31/經濟日報/A12 版/企業商機

[470] 2008-01-19/聯合報/A19 版/民意論壇

其實，最該讓政府感到慚愧的是，台灣早在十多年前就已公佈施行「電腦處理個人資料保護法」，不過該法僅適用於少數行業（網路購物、電視購物公司尚未在適用範圍之內），而且有關該法執行、監理、處罰的權責又分散在各部會（各部會根本沒有足夠人力、經費辦理資料保護業務），以致該法的「宣示」意義遠大於實際應有的功效。

當然，政府部門也意識到問題的嚴重性。行政院在立法院上會期即提出「個人資料保護法」草案，希望將個資保護的規定全面延伸到各個行業。不過由於立委們忙於改選，該案終究沒能通過。

在這次選舉中取得絕對多數的國民黨，爲了展現照顧民生、發展經濟的決心，公布了七大優先法案的清單。不過清單中卻不見「個人資料保護法」草案。衷心盼望一再宣示要優先通過「福國利民法案」的政黨，以及所有新任的立委們，能在新國會新會期中討論通過「個人資料保護法」，除洗刷台灣在國際隱私評比墊底的惡名，並讓全體民眾能夠免於個資外洩、詐騙的恐懼。更重要的，唯有民眾資訊隱私確保，相關產業才能更蓬勃發展。

8. 催生個資法 人民福祉優先[471]

與談人：中央研究院資訊科學研究
所副所長 莊庭瑞
法務部法律事務司專門委員
劉佐國
台灣隱私權顧問協會常務監事
邱月香
主持人：黃嘉裕
記錄：陳家詡
攝影：毛洪霖

前言：個人資料保護法，是一個對人民而言十分重要的法案，但事實上，真的能夠有效執行嗎？並符合人民的需求嗎？而國外對於這方面的進步和重視究竟如何呢？以下邀請到三位專家共同與會一同探討。

莊：民眾不懂法律 無法爭取己身權益

莊庭瑞：從十年前開始，民間團體對個人資料保護的議題持續關注，但到目前爲止，在法律上的保障還是不夠，所訂立「電腦處理個人資料保護法」並沒有隨著時代進步，執行面上也未達理想。一般民眾對於個資法也未充分了解，更沒有能力去爭取自我權益。

[471] 2007-12-13/經濟日報/A19 版/座談會

回顧以往，個資法一開始是政府爲了加入 WTO 而設立的法案，但隨著時代變遷，法律需要更貼近民眾生活，而有修法的必要。但有時修法壓力的來源反而是相關產業要發展或是想解套，與民眾實質需要沒有關係。

現在是網路無遠弗界的傳輸環境，資訊流通已經是十分快速，但個資法並沒有跟上腳步。例如在跨國傳輸個人資料的規範上，需要非常注意，但無論是舊法或新法草案，政府都採取寬鬆的看法。例如中國政府調閱 Yahoo 香港分公司所持有的使用者個人資料，以起訴異議分子的情形，值得我們警惕。許多資訊服務業的亞太總部，可能設在香港或是他國，卻可能蒐集處理國人的個人資料。

▲母子公司個資 應受法律規範

還有一個議題是，台灣企業界常有母公司以下有子公司，但各公司經營不同性質的事業，例如一個子公司經營醫療事業、另一個子公司經營保險事業。但母、子公司間是否交換使用對方所蒐集處理的個人資料，但這些事情其實受到個資法的規範。

未來，政府可以要求各公務機關必須依據個資法的規定和最低度需求的原則，只做依法必須做的個人資料的蒐集與處理，而對各機關已掌有的個人資料庫的使用，尤其在相關人員在資料的取用權線上，必須訂有嚴密的作業流程，並確實做到授權、認證、以及稽核。(及所謂 Au-thorization、Authentication、and Auditing；AAA)管控。

更重要的是參考國外進步案例，例如瑞士有獨的個人資料保護的部門主動進行監督、檢查的工作，也作教育訓練的推動，但反觀台灣卻沒有。我認爲台灣也應該設置獨立的個人資料保護委員會，進行教育宣傳、投訴處理、及主動監督的工作，以落實個人資料保護。

在企業方面，成功的企業相當著重於個人資料保護的強化和專業，一家公司只要對顧客的隱私充分保障，與競爭對手比較起來，相對的就受到消費者更多的認同和信賴，就有無限的商機，此爲相輔相成的道理。

劉：政府應加強個人資料保護

劉佐國：個資法於 84 年公佈實行，但當時只限定於八大行業，例如學校、醫院、銀行、電信業者等，主要原因是爲避免造成產業太大衝擊，但隨著社會進步，例如購物台、網路購物興起，反都不在個資法規範中，但其交易的金額和客戶人數卻一直上升，再單看近期的媒體報導，就可知資訊外洩和便賣的嚴重程序，所造成民眾和企業界的重大損失，無法估計。

在修正的個資法 28 條已加強八大行業以外產業，希望該法能夠快通過，讓民眾得到更好的保障，但推究主因，政府機關和民眾不熟悉，例如銀行資料外

洩後無法可管，其主因是金管會督到不週，都已造成企業和民眾無法挽回的損失。

總而言之，政府擁有最多的資料，但往往洩漏的資料也最多，有鑑於此，目前依個資法第九條規定，公務機關或非公務機關非由當事人提供資料，應於使用前向當事人告知資料來源，這可以有效掌管源頭，讓真正的不法分子可以依法辦理，而不再是無法可循。

法務部是法務執法機關，雖適用於各主管機關，但我覺得台灣應可以設立一個專門資料管理部門，例如以前境管局發現員工將資料賣給旅行社，後來有特設立一個專門管理的部門充分掌握資料，讓類似案件不再發生，這就是一個很好的改革典範。

▲可仿效國外 設個人隱私獨立機構

也可以參考國外都有獨立的機構，譬如香港、澳洲，例如澳洲政府自 1998 年通過隱私條例後，成立專責的聯邦個人隱私專員公署，澳洲的個人隱私委員會由市政府單位直接控管；香港於 1996 年制定個人資料 (隱私)條例後，設立個人資料私隱專員公署；再看看中國大陸明年開始，也開始要實施隱私權，雖然中國一開始相當排斥，但現在進度已超越台灣。

還有在歐洲地區，自歐盟個人資料保護指令於 1995 年通過以來，歐盟各國皆必須配合訂定較以往更嚴謹的個人資料使用條例，這都是台灣可以借鏡的，更期望給合民間協會力量，往往民間資訊才是政府應重視的，並同時輔導和教育民眾，雙管其下，台灣才能接軌國際，放眼未來。

對私人企業而言，政府應當鼓勵，例如國外企業都會有個隱私長，他們會不定期的舉辦全球的資訊安全會議交流，未來期望台灣的購物台或網站業者都可以有隱私長的設立。也希望採取國外已有的標章制，也會和經濟部、金管局設立一個正式標誌，如果得到認證的企業即可獲得此標章，讓消費者能夠安心和企業交易，企業也能夠善盡保護客戶之責。

法務部也會在法案通過之後，聯合行政院、各企業界、工會等，推動各式議題的座談會，並結合民間協會共同推動，有效抑制不當資訊行銷的氾濫。

邱：應加強民眾

對於隱私權基本認知

邱月香：在美國居住 15 年的時間裡，發現美國政府和人民很重視隱私權的國家，其實這個觀念在先進國家都是受到相當的重視，再舉日本爲例，除了政府也十分重視外，民間隱私權協會也不於餘力的配合推動，才有今天的成果。但反觀台灣，近期報章雜誌所報導的個人資料外洩新聞屢見不鮮，已造成許多民眾的精神或金錢上的損失，所付出的社會成本相當高，社會不重視、修正法案遲遲不能通過的情形下，個人隱私權問題不但無法可管，若再加上民

眾也不了解自己的權益，可說是雪上加霜，但這也就是台灣隱私權顧問協會成立所要解決的問題以及背負的艱困責任。

▲期待三讀立法 免於個資外洩

其實台灣應該效法國外，把推動隱私權視爲尊重人權的基本要求之一，並同步教育民眾隱私權的基本認知，積極促進國際交流和及與國外保持良好的運作機制，以彌補台灣的不足，最重要的是，期待個資法修法的三讀能夠趕快通過，政府理應保護人民免於處在恐懼的資料外洩事件當中，人民福祉應是政府考量第一優先。

日前由台灣隱私權顧問協會舉辦的國際個人資料保護研討會，就邀請到日本隱私權顧問協會會長來台交流，國內產官學界都共襄盛舉，造成熱烈迴響。協會是結合一群產、學界的熱心人士組成，經過努力，終於在 96 年 8 月 3 日正式成立，第一屆理事長由陳振楠博士擔任，他不僅推動資安產業不遺餘力，也十分重視個人資料保護，大家都努力要提升台灣對外競爭力，建立起台灣重視隱私權的形象，期許在修正法案三讀過後，有更多企業能夠共襄盛舉參與，讓協會理念能夠有更多人知道，並一同爲台灣成長而努力。

我也要再次呼籲，隱私是人民的基本權利，希望政府能夠積極落實相關法令推動，應該把人民的福利放在前端，才能有效降低無謂的損失，讓民眾生活安康也能讓經濟更爲活絡。

9. 2500 萬筆！ 英搞丟半數國民個資

兩張光碟郵寄遺失 包括個人身分、保險號碼及銀行帳戶 首相布朗一家也是苦主 全國人心惶惶[472]

英國發生有史以來最嚴重的個人資料外洩烏龍，儲存近兩千五百萬筆英國民眾個資的兩張光碟，竟然在郵寄過程中遺失，英國首相布朗爲此代表政府在國會向全民道歉。此事影響到英國六千萬人中將近半數人口，擔心自己的銀行資料可能外洩且遭到盜用盜領。

英國稅務及海關總署一名低階公務員上月十八日將這兩張光碟寄給審計單位，卻忘了依照規範以掛號寄出，導致光碟下落不明。經過多日尋找未果，財政大臣達林廿日才向國會坦承此事。

光碟中有英國家庭申請十六歲以下兒童福利補助的資料，包括國民姓名、地址、出生年月日、社會保險號碼和銀行帳戶資料，據信也包括布朗首相一家。在英國，凡是家有十六歲以下兒童的家庭都可以申請福利補助，每月可領取免稅津貼，目前申請補助的家庭約有七百廿五萬個。

[472] 2007-11-22/聯合報/A15 版/國際

這個尷尬的大烏龍也創了世界紀錄，從來沒有任何一國政府能夠一次讓如此多的國民資料面臨外洩危機。消息曝光後英國民眾大為恐慌，媒體報導，近日內可能有數百萬英國人向銀行查閱帳戶資料或更改提款密碼，以策安全。布朗在與下議院議員的每周例行「首相午餐會報」中表示：「我對於可能造成申請兒童福利補助的家庭不便，表達深深的遺憾與歉意。」他並向英國人民保證，政府會盡一切努力保護人民的資料不外洩或被盜用。
布朗已要求資訊安全專家進駐政府單位，檢查各部會作業流程。財政大臣達林也下令警方搜尋光碟的下落，他表示目前尚無任何證據顯示光碟落入罪犯手中，也未出現資料遭盜用的跡象。
達林近來才為了主要房貸商北岩銀行（Northern Rock）的擠兌風暴傷腦筋，甚至被批評危機處理能力不足。現在又出了如此大的紕漏，達林的政治前途已岌岌可危。
資訊委員湯瑪斯表示，這個錯誤令人震驚。「這已經不光是法律問題，而是人民對政府失去了信任。試想人民將如此重要的個人資料交到政府手中，結果卻出了這種紕漏。」

10. 微笑署長退休 苦瓜首相挨罵[473]

英國發生有史以來最嚴重的個人資料外洩烏龍，搞丟資料的稅務海關總署，署長葛雷雖宣布辭職，仍可領到豐厚退休金（右上圖）。首相布朗則在國會遭反對黨痛批，面色凝重。

11. 舊戶口名簿外流 隱私劫

全從西區戶政所流出 未經碎紙處理 還有完整版 議員批恐成詐騙集團犯罪工具[474]

嘉義市議員蔡文旭昨天在議會拿出一疊從西區戶政事務所外流的舊戶口名簿，這些舊戶口名簿大部分是被撕掉的，部分則是完整無缺。蔡文旭痛批戶政單位沒有依照正常程序將舊戶口名簿碎紙處理，許多民眾的基本資料可能已外洩，成為詐騙集團犯罪工具。民政局長陳敏權表示，將徹查戶口名簿外流的原因並追究責任。
蔡文旭昨天拿著一疊舊的戶口名簿詢問陳敏權，戶政事務所對於民眾換發新戶口名簿後，舊的戶口名簿是如何處理？陳敏權說，戶政事務所會將當天收到的舊戶口名簿集中起來，再做碎紙處理，避免民眾的個人資料外洩。

---

[473] 2007-11-22/聯合報/A15 版/國際

[474] 2007-11-09/聯合報/C1 版/嘉義．教育

蔡文旭說，既然如此，爲何他手裡會有未經碎紙處理的舊戶口名簿，而且其有中 2 份連撕都沒撕，保留得很完整，這些舊戶口名簿都由西區戶政事務所外流，約在 5 個月前他就已經拿到資料，他希望民政局、戶政事務所趕快「補破網」，不要讓民眾的基本資料繼續外流，成爲詐騙集團犯罪工具。
不過，對於舊的戶口名簿究竟是誰提供，蔡文旭並不願透露，只說「來自西區戶政事務所」。
當時在議會旁聽的戶政課長李枝容、西區戶政事務所主任陳建良，看到蔡文旭手中的資料後非常訝異，立即根據戶口名簿的資料展開調查，確定這批舊戶口名簿是從西區戶政事務所外流的。
陳建良說，依照該所作業流程，戶政人員收集的舊戶口名簿，全部都要經過碎紙處理，如今卻有舊戶口名簿外流，應該是戶政人員一時疏忽，直接將舊戶口名簿丟進垃圾桶，導致資料外洩，戶政事務所會盡速調查外流原因再追究責任。

12. 購 600 人頭逃稅 小老鼠露餡[475]

花蓮戶政事務所最近受理大量「自然人憑證」申請時，發現不少申請書填載的電子郵件信箱雷同，或將其中的@寫成國字「小老鼠」，檢調據以破獲保險代理人公司負責人周淑貞涉嫌購買六百多名人頭虛設十家保險代理人公司，開立發票金額十一億元，協助華南、泰安、富邦等產險公司逃稅。
案由調查局東機組、北機組、台北縣調查站共同偵辦，昨將周淑貞等人依涉嫌違反商業會計法、稅捐稽徵法移送台北地檢署法辦。這是利用蒐購自然人憑證從事不法的首例。
「自然人憑證」是由內政部憑證管理中心所簽發，民眾辦理自然人憑證以後，只要在家上網就可以經由網路享受政府 e 化服務，降低了個人資料外洩的危險。簡單地說，自然人憑證就像是「網路身分證」。
檢調指出，周淑貞擔心有欠稅或所得偏高的無效人頭，才代爲申請自然人憑證，進而向政府網站查詢，以排除無效人頭。
檢調指出，依保險法規，未具保險代理人或經紀人資格者不得招攬業務，產險公司也不得支付佣金，但有些產險公司雇用不合資格者拉保險。公司須支付他們佣金，但不能以此報帳。
涉案的產險公司，向周淑貞虛設的十餘家保險代理人公司購買發票報帳，價格爲發票的百分之十五至十七。周淑貞收下價金後，涉嫌大量收購薪資人頭及製造不實費用逃避稅捐。

[475] 2007-11-01/聯合報/A10 版/社會

東機組今年八月間接獲情資，指花蓮地區有原住民大量申領自然人憑證ＩＣ卡異常，有人在填寫電子郵件信箱的「@」時，竟以國字直接填寫「小老鼠」，研判有不法集團在幕後操控。
調查發現，周淑貞涉嫌自民國八十九年起，在台北、花蓮等地虛設十家保險代理人公司，為申報幽靈員工的薪資和股東股利，以一張自然人憑證一萬元的代價向原住民蒐購人頭，每年申辦六百多張自然人憑證報稅，製造營業假象。
檢調昨天搜索華南、泰安、富邦等三家產物保險公司總公司及分公司等四個據點，帶回五人調查。周淑貞供稱，購買人頭以沖銷高額佣金，她也為保險公司仲介人頭逃漏稅捐。

13. 因應措施

戶政所防詐騙專線受理查詢[476]

詐騙集團以身分證更換被冒領、作業有誤等藉口，打電話趁機詐財，讓戶政單位同時段查詢電話接不完。
北區戶政事務決定派登記股，由專線電話受理查詢，遇大批人潮前來查證，還提供專人諮詢服務。
北區戶政事務所主任林玉釵說，詐騙集團常以換發身分證作業等理由，藉機套騙被害民眾個人資料，除派員加強宣導，換發身分證作業嚴謹，不可能變造或個人資料外洩，碰到詐騙電話旺季，戶政事務所另有一套因應措施。
舉例說，詐騙集團會誆稱，有疑問可問某戶政單位幾號櫃台。
林玉釵表示，上個月詐騙集團指稱可問北區戶政所幾號櫃檯，因查詢電話多，就暫時把這個編號的櫃檯取消，有人到戶政所一看，根本沒這個櫃檯，就知是詐騙電話。

14. 賽門鐵克：線上遊戲 駭客的天堂

天堂、魔獸世界最常被鎖定 台北釣魚網站數量冠亞太[477]
線上遊戲成為駭客的新寵，賽門鐵克昨（20）日公布全球網路安全威脅研究報告，發現遊戲橘子代理的線上遊戲「天堂」，與智冠代理的「魔獸世界」為最常被鎖定的目標；另外，台北是亞太暨日本地區擁有最多釣魚網站的城市。

[476] 2007-10-06/聯合報/C2 版/台中市新聞
[477] 2007-09-21/經濟日報/C6 版/產業新聞

賽門鐵克表示，根據調查，線上遊戲已是惡意程式碼攻擊的主要目標，前 50 大惡意程式碼排名中，有 5%鎖定線上遊戲；而天堂和魔獸世界爲最常成爲被鎖定目標的兩個遊戲。在亞太暨日本地區，排名第一的惡意程式碼就是竊取線上遊戲帳號的 Gamepass.Trojan 木馬程式，台灣是回報這隻木馬程式頻率第二多的國家，僅次於大陸。

台灣寬頻網路建置日漸完善，上網人口提升，根據統計，台北是亞太暨日本區擁有最多釣魚網站的城市。所謂釣魚網站是指，駭客設立一個與真實網站相當類似的網頁，例如網路銀行，可能透過在搜尋網站登廣告，吸引網友點選，或是發送電子郵件，「釣」網友點選，藉此竊取帳號及密碼，盜取使用者在網路銀行的錢財。由人口密度來看，台灣爲本區惡意活動排名第三位的國家。

趨勢昨天也公布 8 月的資安威脅報告，針對線上遊戲玩家的惡意程式日漸活絡，除造成個人資料外洩，線上遊戲破解程式也隱藏被間諜程式入侵的危險。例如 TSPY_LINEAGE.FZK 病毒，就是用來盜用「天堂」線上遊戲帳戶相關資訊的程式，能讓駭客竊取並盜用受感染使用者的合法線上遊戲帳戶。

另外有一隻以垃圾郵件爲散播媒介的惡意程式 WORM_ZHELATI.MAB，利用影音分享平台 YouTube 的高人氣，網友會收到一個標示內含有 YouTube 影片的連結，但這個連結與任何影片無關，而是將網友引導至僞冒的 YouTube 網站，引誘網友下載蠕蟲程式。

趨勢科技資深技術顧問簡勝財建議，網友應定期更新修正程式，不要開啓不明來歷的連結或檔案，以免誤上含有惡意程式的網頁。

15. 出租帳戶涉罪 女子貪小虧大[478]

台北縣一名李姓女子 8 月底接到自稱「戶政課」男子電話，以她的個人資料外洩被當人頭冒用，遭詐騙集團詐騙高達 1720 萬元，龜山警方前天查獲台北縣陳姓女子將帳戶以 3000 元出租，詐騙集團在該帳戶得手 120 萬元，警方昨天將她依詐欺罪嫌函送桃園地檢署偵辦，陳女後悔不及。

警方調查，李姓女子（59 歲）家境富有，她在 8 月 28 日至 30 日三天內，至富邦、華銀分行共匯出 5 筆現金，分別匯至聯邦、一銀、中國商銀 4 家分行的帳戶，總共被詐騙 1720 萬元。

已移民美國的李女指出，她偶爾才回台灣，8 月 27 日下午，她接到一名戶政課男子來電，對方說她的身分證遭人冒用詐騙，她的銀行戶頭已被監管。對方留下地檢署人員電話，她打電話求證，一名自稱地檢署的男子說她的個人

[478] 2007-09-16/聯合報/C2 版/桃竹苗宜花新聞

資料外洩，遭人冒用當人頭詐騙，要她把帳戶的錢匯到安全處監管，她一時相信，陸續匯款 5 次，被騙 1720 萬元。她直到本月 3 日向戶政單位查證，發現受騙報案。
其中李女在 8 月 28 日第 1 筆匯款 120 萬元，匯入聯邦銀行迴龍分行的陳姓女子（26 歲）的帳戶，警方將陳女約談到案，陳女供稱，她因要繳交保險費，身上缺錢，看到報紙刊登借「簿」3 萬元的小廣告，在 8 月 23 日，她打電話詢問，自稱張姓的男子表示借用存簿帳戶每 10 天租金 3000 元，10 次 3 萬元，當天她在住家巷口，將存簿、印章和金融卡交給一名年輕男子，對方交付 3000 元租金。
陳女指稱，10 天後，她再打廣告所留電話向「張姓男子」查詢和索取租金，對方卻已不接電話，她再到銀行欲結清該帳戶，未料帳戶已被列爲警示戶，才知道被騙了。

16. 補發退休金 勞保局被批擾民

金額千餘元 申請程序麻煩 不少民眾直接放棄 建議應到公所直接發放[479]

勞保局最近發函通知民眾補領新制勞工退休金，金額大多是 1000 餘元，卻要民眾繳交影印身分証、存摺等資料，掛號郵寄，民眾抱怨還要到郵局寄掛號信，實在擾民，建議勞保局直接派員到鄉鎮公所發現金才便民。
勞退新制 94 年 7 月實施，已結算舊制退休金的民眾，經核算有些人可還可領取雇主提撥退休金與新制之間的差額，雙溪鄉不少年滿 60 歲民眾，近日陸續接到勞工保險局勞工退休業務處核發科寄送的書函，通知領取新制退休金的差額，但金額都不多，雙溪鄉連先生可領 1989 元，張先生只有 928 元可領。民眾擔心是詐騙集團新伎倆，不敢貿然打書函上的聯絡電話，還先向查號台確定勞保局電話，才證實確有其事，不過領個千百元的退休金，還要填寫、影印一堆文件，被批爲擾民。
雙溪鄉民代表簡華祥說，既然是必須發給民眾的退休金，金額又那麼少，應直接派員到鄉鎮公所發放，當場核對身分資料後，發給現金即可，還要填密密麻麻的申請表，不識字的基層勞工批評麻煩、乾脆放棄領取。
簡華祥說，雙溪地處偏遠又沒有公車，民眾「上街」影印，光是搭計程車就要花 200、300 元，寫申請表、影印、郵寄又要花 50、60 元，民眾批評領到的錢光辦手續就花掉大半，還要擔心個人資料外洩，勞保局應該下鄉發放才對。

[479] 2007-09-04/聯合報/C1 版/北縣・教育

勞保局公關科長張德蓉表示，勞退新制 94 年 7 月上路，發放新制勞工退休金的通知書，全國估算有 1、2 萬件，只是要民眾提出申請，等核發後就匯入申請者帳戶，沒想到造成偏遠地區退休勞工不便，會檢討有無其他便民措施。

17. PTT 道歉 清查紀錄 錯誤 20 分鐘 127 筆資料遭修改[480]

PTT 公關站長高嘉瑜昨天對於因程式更新發生錯誤，可能導致部分網友資料外洩一事表示歉意，也強調會檢討改進。

高嘉瑜表示，目前沒有會員反映資料外洩，但如果有，PTT 會協助找到散布者，也會負起應有的法律責任。

高嘉瑜說，PTT 每兩周都要更新系統程式，昨天更新後於凌晨一時卅分重新上線，因系統中有錯誤，導致上網登錄者都有站長權限，可任意觀看、搜尋、新增、修改全站一百萬會員的個人資料，並發送虛擬的 PTT 貨幣。相關人員發現錯誤後，凌晨一時五十分關站，直到昨天下午一時四十五分重新開站。

高嘉瑜指出，清查後發現系統錯誤的廿分鐘，有一萬人登錄，紀錄顯示有一百廿七筆修改權限，多數是會員發送虛擬貨幣給自己，五筆則是更改使用者密碼；部分看板功能設定則遭更改，文章被大量刪除或標記，這些更動都已恢復。

不過，有站長權限即可查詢會員資料，這廿分鐘有多少會員個人資料被看過、下載甚至外洩，高嘉瑜說，這部分完全無法清查。

高嘉瑜表示，會員登錄時留下的資料包括姓名、地址、生日及電子信箱，但沒有身分證字號，相信多數都是假資料。

高嘉瑜說，經過這次教訓後，未來測試系統時，會另開網站測試，確保無誤後，才會正式上線。

消基會：PTT 非營利難求償

【記者顏甫珉／台北報導】由於ＰＴＴ屬於非營利機構，且沒有收費行爲，消基會董事長程仁宏坦言，即使個人資料外洩，實際求償有相對困難。

程仁宏指出，ＰＴＴ屬於非營利機構，站在提供服務的角度，仍必須做好安全防護。經過這次事件後，ＰＴＴ應該明確說明這個免費的服務有可能遭受駭客攻擊，或有任何缺失的可能性讓使用者知悉。

另外網友則表示，ＰＴＴ對於真實身分認證相當嚴格，如今卻又指稱網友大多數用假資料登錄，對於遵守規定的網友來說，真是情何以堪。

[480] 2007-08-23/聯合報/A8 版/生活

網友 JeffyLiaw 就要求ＰＴＴ站台如果不能有效保護網友隱私，就不能要求填寫正確的個人資料。
消基會提醒，盜看他人個人資料的網友，只要有任何的騷擾行動，就會違反電腦處理個人資料保護法第三十四條，可處三年以下有期徒刑。

18. 收購關鍵字 變形詐騙

網路陷阱 植入惡意網站 再以木馬程式竊取民眾財稅資料[481]

上網以「關鍵字」搜尋網站或資訊，已成了網友生活、工作上不可獲缺的一部分，不過，網友可能不知道，由於部分熱門的「關鍵字」已遭詐騙集團向入口網站購買，因此，遇此情形，當網友以「關鍵字」在入口網站查尋時，排在第一筆的網站往往是詐騙集團所設的惡意網站，網友點選後，簡直是羊入虎口，不但個人隱私、帳戶資料可能遭搜刮，還可能被詐騙，這是許多網友做夢都想不到的網路陷阱。
例如在 5 月的報稅季節，刑事局就很擔心「報稅」、「國稅局」等關鍵字，恐遭歹徒收購後，植入惡意網站，當不知情的民眾點選後，再以木馬程式竊取民眾財稅資料，因此，前一陣子，刑事警察局科技犯罪防制中心除了加強與入口網路業者聯繫外，並加強網路巡邏，所幸未發現可疑的「假網站」。
釣魚手法騙走上億
刑事警察局科技犯罪防制中心主任李相臣指出，自去年底起，網路犯罪以「網路釣魚」和「關鍵字」兩大新興犯罪手法入侵國內 20 餘家銀行、最大拍賣網站和各大航空公司網站，造成全台上千萬筆民眾個人資料外洩，損失金額直逼上億元，而且後續損失可能持續增加，因爲「國內百分之十是惡意網站」，李相臣鄭重發出警訊。
利用英文相似字造假
他指出，這兩大新興的網路犯罪手法，「連警察也得承認會上當」，網路安全防範難上加難；其一是以假網站誘騙消費者填資料，即利用英文字如ｉ與ｌ、ｎ與ｈ的相似度，虛造網站，竊取民眾資料，例如「taiwanbank.com」與「taiwanbahk.com」這兩個網站，「你能分辨得出後者是釣魚網站嗎？ 」
李相臣同時指出，這種網路釣魚（fish-ing）三年前在全球就達高峰，現在手法更精密，利用相似度極高的網址、網頁，或向國內最大入口網站購買關鍵字的假網站，誘騙使用者輸入帳號、密碼等資訊，致使民眾在入口網站上打入「銀行」、「機票」」等關鍵字，點選搜尋結果前，根本不會懷疑網站的真實性。

[481] 2007-07-07/聯合晚報/4 版/焦點

台股、大考熱門關鍵字
還有暑假旅遊旺季時，「旅行社」、「機票」，還有近來持續漲勢的「陸股」、「台股」以及基測時的「大考」、「重考」和「補習班」等，都是熱門的關鍵字，而其共同特點就是它吻合時事。
據了解，國內各大入口網站標售關鍵字的價格，以其熱門程度而有所差異，例如當今熱門的「投資理財」關鍵字，「少說一、二個月就要 50 萬元。」
連警方也承認很難防
歹徒「以小搏大」在截獲民眾的個人資料，上網盜刷購買精品、機票…等，甚至在網路銀行盜領轉帳存款，「釣魚、關鍵字假網頁的手法已非防火牆可防堵」李相臣不諱言地指出，連他自己都很難防，也因此初估影響範圍難以估計。

19. 網頁攻擊病毒來勢兇 趨勢示警[482]

趨勢科技昨（20）日表示，16 日在義大利造成超過 4.4 萬台電腦被入侵的惡意程式攻擊發出警訊，此惡意攻擊已在歐洲及美國漫延，亞洲則有日本及大陸遭受波及，預估將向其他亞洲國家快速散播，趨勢科技籲請台灣網友千萬提高警覺。
趨勢表示，這個惡意程式，主要是駭客隨機挑選安全防護較不完整的網站做爲跳板，在此類網站中植入惡意連結程式 HTML_iFrame.CU，一旦網友點選此網站，電腦即會被連結另一個 IP 位址，並植入名爲 JS_DLOADER.NTJ 的惡意程式，再利用微軟瀏覽器 IE 中的程式弱點入侵電腦，以植入更多可竊取個人機密資料的木馬程式。除了個人資料外洩，也會成爲駭客散播惡意程式的工具。
趨勢科技資深技術顧問簡勝財表示，此類型病毒攻擊手法爲多層次攻擊，不僅在第一層遭植入惡意程式的網站並無特殊的畫面或現象，在個人電腦被轉接至其它網址下載惡意程式後再植入其它惡意程式的掩護下，而受感染的個人電腦不會有如當機或電腦速度變慢的中毒症狀，所以網友較難察覺是否遭攻擊。

20. 兼差模特兒 個資全都露

電子信箱遭入侵 還接到簡訊 查到電腦老師[483]

[482] 2007-06-21/經濟日報/C7 版/科技產業

[483] 2007-04-05/聯合報/C4 版/中部雲嘉綜合新聞

嘉義縣林姓女大學生兼差當模特兒，她的奇摩電子郵件信箱遭駭客入侵，清涼沙龍照等私密個人資料外洩，駭客還傳手機簡訊給她「天蠍美女不要記恨」，她嚇得報警，警方懷疑駭客可能看到被害人照片而暗戀，昨天傳喚涉案的電腦老師李姓男子到案，他否認犯行。
林姓女大學生（22 歲）就讀大學心理諮商系 3 年級，高中時就兼職當模特兒，去年 12 月 10 日發現自己電子郵件信箱遭盜用，幾天後又收到「天蠍美女不要記恨」的手機簡訊。
林女說，本來以為只是單純駭客入侵遭植入程式致電腦中毒，但這名駭客竟然知道她是天蠍座，研判是電子信箱裡的郵局帳號、住址等私密資料外洩，心駭客找上門而報警。
嘉義縣警方根據伺服器等資料，昨天傳喚 29 歲的李姓男子，他自稱曾是職訓局電腦老師，是電腦高手，不可能笨到當電腦駭客還留下紀錄讓警方查到，但仍被警方函送法辦。

21. 高市長選舉驗票

影印選舉名冊 中選會：侵犯隱私[484]

高雄市長選舉官司進入驗冊階段，高雄地院同意陳菊、黃俊英兩造影印選舉人名冊，中選會認為形同「選舉名冊外流」，將衍生侵犯個人隱私及其他嚴重問題，昨天要求高雄市選委會緊急向高雄地院提出異議。
中選會官員說，選舉官司經法院裁定雖可驗選舉人名冊，但只限在法院監督下進行閱覽、記錄，從不曾影印，只有二〇〇四年總統大選官司，當時法院為求時效，將選舉名冊影印，但僅供兩造在指定地點閱覽，並非交由雙方帶回。這次高雄地院同意雙方帶走選舉名冊影本，是「破天荒第一遭」。
官員說，選舉名冊、選票在選後都須封存，僅法院或檢察官才能開封，如今將名冊影印交給兩造，已形同選舉人名冊外流。雖然影本保留地址，但每頁都有投開票所編號、第幾鄰、每戶多少人、有無投票等等資料，「有心人」要對照出哪一戶的投票情形，非常容易，若有椿腳據此向選民「選後算帳」，或造成選民不滿個人資料外洩而抗議求償，後果都很嚴重。即使法院事後要求兩造交回影本，難保被有心人私下另印副本留存。
中選會估計，高雄市全部的選舉名冊約有三分之一，已被陳、黃兩造影印帶走，「名冊外流」嚴重，因此要求高雄市選委會緊急向高雄地院提出異議，立即停止兩造帶走其他選舉名冊影本，並速謀補救。

[484] 2007-03-24/聯合報/A13 版/綜合

22.「自然人憑證」申辦有優惠[485]

中西區戶政所鼓勵民眾申辦「自然人憑證」，即日起舉辦「5 人同行，1 人免費」及「個人來辦，摸彩打折」優惠活動。

自然人憑證內含「數位簽章」跟「公開金鑰」，由內政部憑證管理中心簽發。申請後，民眾可透過網路享受政府 E 化服務，不必再親自到政府機關，而且憑證附有加密功能，防止個人資料外洩。

已申請憑證的謝姓市民說，透過網路就能申請電表、水表與報稅，甚至可在交通部與財政部的網站，查詢個人相關資料，方便又節省時間。

中西區戶政事務所主任江學通表示，自然人憑證服務項目已達 800 多項，未來將增加至 1500 項，如提供民眾申請電子戶籍謄本等服務。

江學通說，申請費每人 275 元，若集體申辦，每 5 人即有 1 人免費；個人申請也有抽獎與打折的優惠，最高可打 85 折。

凡設有戶籍的年滿 18 歲以上國民，持國民身分證正本，即可至戶政事務所辦理，也可跨縣市辦理。

江學通表示，隨到隨辦，辦理時間爲每周一至周五，另增周六上午照常服務，集體申辦請事先打電話預約。戶政所也提供「到府收件」，有需要的民眾可洽電 2232609 葉先生。

[485] 2007-02-06/聯合報/C2 版/台南市新聞