

個人資料保護在台灣：誰的事務？*

莊庭瑞

中央研究院 資訊科學研究所

台灣 台北市 南港區 115 研究院路二段 128 號

E-mail: trc@iis.sinica.edu.tw

2003 年 3 月 17 日

(修改) 2003 年 4 月 18 日

摘要

本文嘗試對個人資料保護在台灣의 現狀作一簡要描述。我們認為 1995 年 8 月通過的《電腦處理個人資料保護法》，並未能達到實質保護個人資料的目的，並分析其原因。我們尤其在意公務機關在蒐集、處理、利用個人資料上，是否已逾越必要目的，以及是否善盡其安全維護的責任。我們以多項案例說明目前《電腦處理個人資料保護法》的缺失，以及修法的必要。我們並認為應該設置獨立的「個人資料保護委員會」，進行教育宣導、投訴處理、及主動督察的工作，以落實個人資料保護。

關鍵詞： 隱私、個人資料保護、身分識別、身分證、

* 原文刊於《國家政策季刊》(ISSN 1684-7784)，第 2 卷第 1 期 (2003 年 3 月)，第 53 至 70 頁。
《國家政策季刊》由行政院研究發展考核委員會出版發行。

Personal Data Protection in Taiwan: Whose Business? *

Tyng-Ruey Chuang

Institute of Information Science, Academia Sinica

128 Yen-Jiou-Yuan Road, Section 2, Nangang 115, Taipei City, Taiwan

E-mail: trc@iis.sinica.edu.tw

March 17, 2003

(revised) April 18, 2003

Abstract

This paper attempts to outline the current landscape of personal data protection in Taiwan. After an analysis of the 1995 *Act of Computer Processing of Personal Data and Its Protection*, we conclude that the Act is full of loopholes, hence not helpful in protecting people's privacy. We are particularly critical of various governmental offices and state enterprises about their liberty in collecting citizens' personal data and their mishandling of the collected personal databases. Many incidents involving leakage of personal data from governmental civil databases are used to support the proposal of a remedial amendment to the 1995 Act, so that personal privacy can be better protected. We also advocate the idea of establishing an independent Personal Data Protection Commission in Taiwan. .

Keyword: Privacy, Personal Data Protection, Personal Identification, National ID.

* Appeared in *National Policy Quarterly* (ISSN 1684-7784), vol. 2, no. 1 (March 2003), pp. 53-70. *National Policy Quarterly* is a publication of Research, Development, and Evaluation Commission of the Executive Yuan, Taiwan.

壹、隱私與個人資料保護

隱私 (Privacy) 是現代社會中重要的概念。它的意涵與範疇，卻又難以明確定義。一般認為，隱私意指一個人對個人空間 (personal space) 的私密性主張，亦即其不為他人所侵犯 (intrude) 的權利。此個人空間並不單指物理上的實體空間，如個人的身體、居所庭園；它也泛指如日記、書信往來等個人思想、活動與記錄的空間。隱私，此一「獨處之自由」¹，也被認為是個人主體性的表示，是我群之間的分界、社會生活的一環。同時，隱私也和個人所在的社會或團體的特質息息相關，而有相對上的差異²；此外，個人隱私與公眾利益，也常有不相容之處，其間如何界分，更是引發許多討論。

資訊社會裏人際之間的往來，多使用數位資訊技術以媒介進行 (如電話、電子郵件等)，個人在社會裡的活動，更常是自願或不自願地參與各類資訊系統的運作 (如使用自動提款機提款、被攝影監視器錄影等)。隱私裡個人空間的概念，可以說已是與個人相關的資訊空間的概念；而個人對隱私的權利主張，很大部分也等同對個人資料 (personal data)³ 的權利主張。而隱私保護的議題，也就是個人資料保護的議題：個人資料若非自主地被揭露於外界，如同個人隱私遭受侵犯一般，將對當事人形成困擾而造成負擔，故需加以保護。

而資訊技術的進展，更是衝擊眾人對隱私概念的認知。數位化的資訊技術的特質在於可對資料做無失真的複製，以及快速與大量的儲存、傳輸與處理。技術與商業的進展，讓資訊處理工具日益廉價化及普及化，也可能導致眾人對個人隱私的合理期待 (reasonable expectation)，日益降低。舉例來說，個人於公眾場所的日常活動，在該場所未裝設錄影監視器之前，享有一定的匿名性的。因為同時活動於該場所的眾人，若不借助攝影器材，無人可以精確記憶他人的容貌，並於日後重述複製。這種匿名性，某種程度允許個人更能「享受生活」(如情侶間的親暱行為)。公眾場所一旦裝設攝影監視器後，個人的舉止便可以被無失真的紀錄、儲存、複製；必要時，並可於日後取出調閱或與其他資料相互檢索。而且，對於已被錄製的個人影像，當事人也難以主張處置的權利 (如果使用的是隱藏式

¹ 即所稱 “the right to be left alone” (Samuel and Brandies, 1890)。Samuel 和 Brandies 於 1890 年於 Harvard Law Review 發表 *The Right to Privacy* 一文。一般認為，這是將隱私視為個人權利，並應以法律保護的濫觴。該文認為，隱私若不受保護，對個人將產生干擾，造成當事人的負擔，使其無法「享受生活」(“enjoy life”)。同時，有關個人的資訊，如肖像，是個人的財產 (property)，不可隨意利用 (如不經當事人同意，刊於媒體或作其他商業使用)。

² 例如：未成年子女，相對於成年子女，對父母來說，其可保有的隱私範圍顯然不同。又如，個人在工作場所與在「匿名戒酒團體」(Alcoholics Anonymous) 兩個環境中，所願透露的個人資訊，可能有非常大的差異。

³ 個人資料，意指「足資為個人識別」(personal identifiable) 之資料。見《電腦處理個人資料保護法》(1995 年訂立)，第三條：「個人資料：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」。

攝影監視器，當事人甚至不知已被錄製的事實)。個人若因為無法避免被公眾場所的監視錄影機攝影(或不能確定有無隱藏式監視錄影機的存在)，結果可能是自我約束在公眾場所的舉止，或減少在公眾場所的活動。

資訊社會與隱私的議題，從資訊科技如何「制約」(regulate)個人行為的角度來討論，是一種方式。Lessig (1999)進一步以科技架構(architecture)、法律約束(law)、市場機制(market)、社會常規(social norm)四個角度，討論隱私的概念，以及其對個人行為的制約。值得說明的是，資訊技術對個人隱私維護，未必全然是負面的；例如，密碼技術可以增強個人通訊的私密性，有助於隱私維護。重點是資訊技術的進展，(正面或負面地)影響了眾人對隱私的看法以及自身的行為。同理，相關法律的訂立或訴訟的案例，也都會影響眾人對個人隱私的認知與期待。市場機制(如大眾媒體為了新聞價值，日夜跟蹤知名人士)與社會常規(如「不言人是非」或「言人是非」等人情事理上的約束或縱容)，也同樣制約了眾人對個人隱私的態度。在下一節，我們約略以這四個角度，對個人資料保護在台灣的現況，作一整理與分析。

貳、個人資料保護在台灣的現況

隱私為我國《民法》所保障之個人權利；個人隱私若受不法侵害，被害人雖非財產上之損害，亦得請求賠償⁴。《電腦處理個人資料保護法》更對公務與非公務機關蒐集、處理、與利用個人資料的情形，明文規範。然而，個人隱私或資料遭受侵害的情形，卻日益增多且類型繁複。除了新聞媒體對相關案例的報導(如眾多金融卡或信用卡遭盜錄、複製、冒用的事件⁵)，許多民間社團也已經以會訊或專刊的方式，對個人資料保護的問題，進行分析與探討⁶。可見社會大眾對隱私及個人資料保護這個議題的重視。

我國《電腦處理個人資料保護法》的立法目的，在於規範電腦處理個人資料，「以避免人格權受侵害」，同時「促進個人資料之合理利用」(第一條)。該法對於個人資料，固然採取保護的原則，如第六條：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍」。然而，由於許多法條的制訂非常寬鬆，該法並未達到實質保護個人資料的目的。《電腦處理個人資料保護法》的缺陷，可分三方面分析。

⁴ 《民法》(2000年修正)第195條：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額」。

⁵ 參見(謝明俊，2003)等的報導。

⁶ 參見《2001年台灣人權報告》、《人權雜誌》2002年春季號、以及《中華民國愛滋感染者權益促進會會刊》第13期(2003年1月)等的報導。

- 一、無主管機關且罰則輕。法務部僅為該法之「協調連繫」機關（第四十二條）。這與《消費者保護法》第四十條明訂：「行政院為研擬及審議消費者保護基本政策與監督其實施，設消費者保護委員會」的情形，成為對比。此外，《電腦處理個人資料保護法》罰則太輕，例如：「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」（第二十七條）；這對大規模、制度性的侵害（如電信公司員工盜賣數百萬戶客戶資料的情形），難起嚇阻作用⁷。
- 二、位階低。「個人資料之保護，依本法之規定。但其他法律另有規定者，依其規定」（第二條）；尤其「醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業」（第三條第七款第二目），可依「有關之法規及其他法律有特別規定者」，逕行個人資料之蒐集或電腦處理，不需當事人事先同意（第十八條）。
- 三、公務機關權力大。該法雖限制：「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」（第六條）。可是，「對當事人權益無侵害之虞」如何認定，顯然較有利於公務機關。此外，為達「特定目的」所蒐集處理之個人資料，是否為「最低度需求」（minimum necessary），也並未規範⁸。另外，該法容許以寬鬆的條件，允許公務機關對已蒐集處理之個人資料，做特定目的外之利用（第八條）⁹。

台灣目前個人資料遭受盜用、誤用或其他不法侵害的情形，非常普遍。主要即是《電腦處理個人資料保護法》立法寬鬆，未能有效阻止公務與非公務機關不

⁷ 參見（蔡再本，2003）。

⁸ 也就是說，是否非蒐集、處理該項個人資料，該公務機關即無法進行其法定職責？「最低度需求」的用意在於限制公務機關，即使在特定目的下，依然不可蒐集、處理不必要的個人資料。例如，舊有戶籍登記（與身分證）上的職業、本籍、學歷三項個人資料，已超出戶籍管理此特定目的之所需之「最低度需求」個人資料，而目前的確也已經不予登載。

⁹ 見《電腦處理個人資料保護法》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」。

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

當蒐集處理個人資料的情形。而蒐集而成的個人資料庫，因其管理輕忽，而常有被盜用或誤用的例子。因個人資料遭受侵害，導致個人權益受損時，當事人在舉證和訴訟求償上，反而非常困難，處於非常不利的地位。個人資料從何機關、經由何人流出，以個人之力，查證上非常困難。而且個人資料一旦不當流出，即可被任意複製傳送，個人無從控制。此外，個人資料從外洩到被不法使用，到當事人察覺其權益受損，其中可能經過一段不短時間，此種潛伏效應（latent effect），使得案件的追查，更加不易。

目前檢調單位偵查個人資料遭受侵害的情形，多著重於知名人士案例（如大眾週刊不法取得政治或影藝人士的車籍資料，以跟蹤其車輛和行蹤），或是大規模受侵害的案例（如財金資訊公司人員整批洩漏委辦銀行的信用卡客戶資料）。固然這些案例所牽涉的個人資料，事關名人的隱私及眾人的財產，有較高的市場與新聞價值，而成爲受重視的指標性案件。但是一般大眾個別受害的情形，卻不應受到忽視。例如，竊車集團常有以不法流出的個人車籍資料，向受害者聯絡勒索的情形，但這些個人資料如何不法流出，可能並非檢調單位最優先偵查的方向，而檢調單位起訴的對象，通常也止於車輛和資料的竊盜者，而不是一併起訴未妥善保管個人資料的單位¹⁰。

以上的情形，其實說明了一項癥結：蒐集處理個人資料的一方，通常並不是資料外洩後權益受損的一方；受損的是個人，而個人很難追究個人資料蒐集處理者的責任。也因此，蒐集與處理個人資料的一方，其實並沒有很強的動機，依《電腦處理個人資料保護法》第十七條的規定，「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」，因爲被依第二十七條，「致當事人權益受損害者，應負損害賠償責任」，而被起訴的情形並不常見。即使被訴，最後的賠償金額也不大。我國目前《電腦處理個人資料保護法》的立法方式與執法情形，與個人資料受侵害的環境與市場的形成，其間的關連，值得進一步探究。

在另一方面，一般大眾對自身個人資料的重要性，以及保護的方法，往往欠缺認識。常見的情形包括：參加問卷抽獎等商業活動時，依對方的要求，留下不必要的個人資料（如身分證字號）；將身分證、其它身分證明文件或其影本隨意交給他人代辦手續；簽署自己並不充分瞭解的授權書，同意對方調閱自己的個人資料（如授權保險公司調閱個人於中央健保局的歷年就診資料）；以及對他人（尤

¹⁰ 相關報導參見（黃啓洞，2002）。公務機關的責任見《電腦處理個人資料保護法》第十七條：「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」。同法第二十七條：「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」。

其假冒為可信任機關之人員)探詢自己的個人資料時，沒有應有的警覺。一般大眾也不熟悉《電腦處理個人資料保護法》裡對個人的基本保障。

對他人抱持著基本信任，不去侵犯別人的隱私，或許是我們的社會價值與常規；但對於個人資料在資訊社會裡的商業價值，以及如何防制商業機構或公務機關對個人隱私的漸進式侵蝕，許多台灣民眾還未能充分解瞭，也缺少自我防禦的能力，以致個人隱私容易遭受制度性的侵害¹¹。正要走出威權體制遺風的台灣社會裡，許多民眾對行政機關的各式規定與要求，在個人資料的蒐集或處理方面是否合法合理，仍有少作思考、全然接受的傾向。而公務機關也常勇於嘗試新的資訊技術於個人資料處理(如健保 IC 卡計畫)，或為了行政便利，對既有的個人資料庫作新的連結處理(如財產總歸戶計畫)。這些計畫中的個人資料保護議題，卻往往被執行機關簡化為資訊安全議題；對這些計畫在《電腦處理個人資料保護法》與相關法律上的適法性，如個人資料庫間的連結處理，是否已構成特定目的外之利用等議題，少有探討。

目前台灣在個人資料保護的大眾教育，以及對公務機關與商業團體的監督，大部分的工作是落在關心的民間團體與立法委員身上。1998 年的「反國民卡行動聯盟」¹²，以及 2002 年 7 月發起的「全民個人資料保護聯盟」¹³，都是例子。這些聯盟的發起，起因通常是對特定政府計畫在個人資料保護上的疑慮。而聯盟的組成則包括民權與弱勢團體、學者專家以及個人。除了以一般的記者會或活動劇來喚起大眾對議題的注意外，聯盟尚以出席立法院的公聽會、參加立法委員的記者會、對個別黨團與立法委員的簡報與遊說、致函行政首長、到監察院陳情、以及舉行研討會或專題演講等多種方式，以深化議題的討論，進而影響或中止這些有疑慮的政府計畫的進行。

台灣的民間組織成功的透過運動(campaign)，得到不少具體結果，例如：1998 年底「國民卡計畫」在輿論壓力之下，行政院與廠商議約失敗，負責規劃的行政院研考會並遭監察院糾正；促成行政院於 2001 年底提戶籍法第八條條文修正案於立法院，請求刪除「請領國民身分證，應捺指紋並錄存」的規定，並獲內政委員會初審通過；以及 2002 年中起至今，對健保 IC 卡計畫中涉及個人隱私保護的問題，成功地喚起社會大眾的關注與討論。相較於國外諸如「美國民權聯盟」(American Civil Liberties Union; ACLU)¹⁴、「電子隱私資訊中心」(Electronic

¹¹ 例如，「不做虧心事，不怕半夜鬼敲門」以及「各人自掃門前雪，莫管他人瓦上霜」等民間諺語，所傳達的是自我在隱私上的自律與道德訴求，而不是他人行為侵犯到自我隱私，導致個人不便和負擔時，個人在公義與法律的伸張。

¹² 參見網址 <<http://gptaiwan.org.tw/~nonid/>>。

¹³ 參見網址 <<http://www.tahr.org.tw/PDPA/>>。

¹⁴ 參見網址 <<http://www.aclu.org>>。

Privacy Information Center; EPIC)¹⁵、或「隱私國際聯盟」(Privacy International; PI)¹⁶等民權團體的成果，並不遜色。不過，ACLU、EPIC、以及PI等民權團體，以其常態性組織的性質，以專職人員進行研究、出版、宣傳、與遊說¹⁷，其持續運作的能力，與所發揮的效果，就不是我國「反國民卡行動聯盟」或「全民個人資料保護聯盟」等民間臨時組織可以相比。

另一方面，資訊科技快速地被引進、並廣泛地被社會大眾使用，固然彰顯台灣為一高度「網路就緒」(network ready)的社會¹⁸，但同時也帶來多項個人資料保護的議題。新興的資訊技術和服務，多與個人生活相關，但在商業推廣或是個人採用的過程裡，對於這些新興資訊技術的侷限性或延伸性，以及在個人隱私上的意涵，一般並不受到特別注意。一些使用者，在與資訊技術服務的提供者、或是惡意的使用者互動時，因為對所使用的資訊服務不甚瞭解，也就特別容易受到侵害。台灣社會或許已是「網路就緒」，但未必所有使用者皆是「網路通」(network savvy)，而這也牽涉到「數位落差」(digital divide)的議題¹⁹。也就是說，因為對個人資料保護議題不熟悉，以致容易遭受侵害的，可能也是資訊能力較弱的群體。而公務機關或商業機構在設計資訊服務系統時，也未能充分考量資訊弱勢群體的能力，以及他們傾向於對制度或系統上的信任，以致於讓惡意的第三者可以藉此引導加害(如以退稅退款為名，進行轉帳詐騙的例子)²⁰。而有些行政機關，

¹⁵ 參見網址 <<http://www.epic.org>>。

¹⁶ 參見網址 <<http://www.privacyinternational.org>>。

¹⁷ 例如，為因應美國於2001年9月11日遭受恐怖份子攻擊後，美國政府可能以國家安全的理由，對人民權力日漸設限的情形，ACLU即以“Keep American Safe and Free”策劃專題網頁(網址 <<http://www.aclu.org/safeandfree/>>)，亦參見其「隱私與技術」專題網頁(網址 <<http://www.aclu.org/Privacy/PrivacyMain.cfm>>)以及其所出版的教育宣導小冊(Stanley and Steinhardt, 2003)。同樣的，EPIC與PI自1998年起，每年皆出版*Privacy and Human Rights: An International Survey of Privacy Laws and Practice*系列報告一冊，對世界各國(當然包括台灣)的個人隱私保護情形，作持續的整理分析(網址: <<http://www.privacyinternational.org/survey/>>)。

¹⁸ 據「世界經濟論壇」(World Economic Forum)最新一期*Global Information Technology Report*的報導，台灣於2002-03年度的「網路就緒指標」(Network Readiness Index)為全球第9名(在亞洲僅次於新加坡的3名，另外南韓為第14名、香港第18名、日本第20名)。台灣在2001-02年度的排名為全球第15名。

¹⁹ 我國數位落差之情況與檢討(約當2001年時)，可參見《數位落差與資訊社會研討會彙編》(2001年12月)。

²⁰ 參見(張啓凱，2003)等之報導。「退稅為名，轉帳詐騙」的事例，說明了個人資料保護的諸多議題與面象。一方面，歹徒設立的入帳人頭帳戶，涉及「身分盜用」(identity thief)；亦即人頭並不知情，其個人身分已被使用來開立用以詐財的帳戶。而受騙匯入款項的個人，其電話號碼、姓名等個人資料又是經由何種管道流出，而可被歹徒作為聯繫與取得信任的依據？另外，國內金融帳戶間的轉帳，設計為「內訂為可轉到任何非約定帳戶」(即所謂的 default opt-in)，而非「內訂為只可轉到事先已申請的帳戶」(即所謂的 default opt-out)，這其實是科技架構上的缺失。國稅局健保局等公務機關，或其他可被信任的組織，頻頻成為歹徒行騙過程中取信於人的道具，固然是其法人身分被盜用，但其結果是稀釋了這些機構的公信力。這些情形，說明了「信任」(Trust)，其實是網路化社會中關鍵的一環。

也利用一般大眾欠缺相關資訊技術的評估能力，推行並無必要的計畫（如指紋辨識系統的建置等），並以誇大效益或贈品抽獎的方式，以蒐集公民的個人資料²¹。

討論台灣的個人資料保護，不能不觸及台灣的戶籍與身分證制度。目前我國的身分證統一編號，是一個只憑號碼就可以辨別身分不同的方法，並可以依此號碼到多項個人資料庫索引，查詢並組合出公民的個人相關背景資料（所謂 *personal profile*）。此種一人一號的制度是否合理，已是引人討論的議題²²。再加上強制性質的身分證制度與戶籍管理資訊系統（基本上即為一個集中性的全國公民個人基本資料庫），固然是政府在行政管理上的利器，但同時也成為公民隱私與個人資料保護上的一大癥結。政府的許多計畫，打算以戶政資訊系統為基底，就個人資料作新的連結處理，或是以非肉眼可視的新式資訊載具（如 IC 卡等）製作身分證。這些計畫牽扯到許多個人資料保護的議題，也引發許多爭議²³。

況且，這些有關個人身分識別的政府計畫，有些在規劃之初即非以行政作業之必要或效率性為單一考量，而是被賦予帶動相關資訊產業、或是配合相關資訊政策的任務²⁴。其著眼點常是法令上的強制性規定，藉以達到特定身分識別資訊技術的普遍採用，以及其所延伸的相關應用。例如，以身分證制度的強制性，以及《戶籍法》第八條「請領國民身分證，應捺指紋並錄存」的規定，而達到全民指紋建檔與指紋辨識系統建制的目的，以及其在戶籍管理此特定目的外的利用（如用於犯罪偵察等）。

參、政府的角色

²¹ 例如，台北市政府民政局為了推廣其「指紋暨臉型建檔」計畫，於 2002 年散發的「輕鬆按一下、便利跟著來」宣傳海報，在「建置好處」部分，即宣稱「未來將增加申辦項目擴展至老人年金、健保卡補發、護照申辦、機場通關…等」。為說服民眾自願加入計畫，並說「建置完成隨即送贈品一份，送完為止；另可參加全市悠遊卡及機票抽獎」。

²² 參見（黃文雄，1998）。

²³ 當中議題，參見參考書目中本人多篇短論，以及出席相關機關會議之書面資料，不在此一一重述。

²⁴ 例如，「行政院資推小組 IC 卡規劃及推行小組」於 1997 年 7 月 21 日召開第一次委員會議，討論「識別證卡合一 IC 卡」時，即已有「產業協調」的分組（詳見會議記錄，網址：<http://www.rdec.gov.tw/mis/gsnnet/eng/iccard/mrecord1.htm>）。與會的產業代表，對於晶片記憶空間之分配（是否政府民間各用一半），以及對於該計畫的明確商機所在和民間進行投資方式，皆表達高度興趣。《電腦處理個人資料保護法》雖已於 1995 年 8 月 11 日公布，據記錄與會人士並無就個人資料之法律保障議題，進行討論；《電腦處理個人資料保護法》之法定協調聯繫機關法務部，也無代表與會。此外，此「識別證卡合一 IC 卡」計畫（詳見《「國民身分證健保合一智慧卡（簡稱國民卡）」專案徵求建議書文件》，網址：<http://www.rdec.gov.tw/mis/gsnnet/eng/iccard/rfp0610.html>），規劃以整體委外方式進行，應是配合當時政策；隨後行政院並於 1998 年 4 月 8 日核定通過《行政院所屬各機關資訊業務整體委外作業實施辦法》。行政院另於 2002 年 11 月 1 日核定通過《行政院所屬各機關資訊業務委外服務作業參考原則》，新的參考原則對於政府資訊業務委外之原則及策略，有較清晰之規範，在委外範疇方面，並排除「相關法令另有規定，或屬政府核心資訊業務者」。

高度資訊化的社會裡，除了商業機構蒐集處理大量的個人資料，各政府機關因其職務所需，也建立許多個人資料庫。依我國《電腦處理個人資料保護法》，公務機關需有「特定目的」，且必須在「法令規定職掌必要範圍內」、「經當事人書面同意」、或「對當事人權益無侵害之虞」時，始可進行「個人資料之蒐集或電腦處理」(第六條)。而且，「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」(第八條，但亦見同條允許之九種例外情形)。這些限制，在於避免政府無理由、無限制地蒐集處理公民的各類個人資料，並作不當使用。例如以血緣、出生地、黨籍等資料為依據，制度性地歧視某些群體，或是秘密地蒐集特定個人的資料，甚至不法監視其活動。

依法已蒐集於各政府機關的個人資料庫，其安全維護，顯然是重要的議題。一般機關，似乎傾向把這議題，認為是資訊系統或網路安全的議題，重視的是定時備份、防火牆的設置、或是防止外人經由系統漏洞入侵等「外患」問題。對於這些資訊系統的管理，尤其在作業流程上，以及在資料經手人員的訓練管控上，是否訂有嚴謹的作業準則以及稽核方式，以防止「內賊」竄改盜用其中的資料，則較少注意。而眾多的案例的確也指出，不少政府機關因管理不善，以致所保管的民眾個人資料遭內部人員盜賣，讓民眾蒙受重大的精神及財產損失²⁵。

所以，在行政作業方面，政府最少可以要求各公務機關，必須依據《電腦處理個人資料保護法》的規定和「最低度需求」的原則，只作依法必須作的個人資料的蒐集與處理。而對於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限上，必須訂有嚴密的作業流程，並確實做到在「授權、認證、以及稽核」(及所謂 Authorization, Authentication, and Auditing; AAA) 上的管控。

對於既有的身分證制度與其使用方式，應立法限制其使用。身分證之用途應

²⁵ 這裡僅摘錄數件 2002-03 年的案例，以說明情形之嚴重。(黃哲民，2002) 報導：「被盜取資料者的身分不拘，…除了多名女立委、政商名流、總統家人，還有兩位黨主席與一名甫離職的部長名列其中」。而檢調單位的大動作，「據了解，導火線正是因為壹週刊報導部分立委時，當事人驚覺個人資料離奇外流，轉而要求檢警調查」。其中涉案的警員、戶政人員等，「利用公務之便取得民眾的入出境、車籍、前科、口卡甚至不動產坐落、行動電話、銀行帳戶與存款數額等資料，簡直無所不包」。另外，財政部為大股東的「財金資訊股份公司」，也爆發員工因個人私利，整批盜賣顧客的信用卡密碼，詳見(宋伯東，2002)的報導。交通部為大股東的「中華電信股份公司」，則發生員工以顧客的行動電話號碼反查其登記住址，並洩漏給他人，以致顧客被「駕車跟監，作勢衝撞以為警告，更在其住處外擲石騷擾，讓被害人精神受到莫大威脅」，詳見(張致和，2003)的報導。就連一般大眾最注視的健康資料，也發生保險公司「勾串中央健保局人員，以低價購買個人就醫資料」。檢調單位並發現，「外洩健保單位從北到南都有」，「健保局內部電腦資料控管鬆散，幾乎任何有密碼的人，都可查詢資料，但事後查不出由何人何時調閱、列印資料」，詳見(牟玉佩、陳于嫻，2003)的報導。

該只是公民至政府機關辦理個人權利義務事項時，用以證明身分而已；不應強制要求公民隨身攜帶，成為個人行動的必備證件²⁶。身分證現在更被廣泛的作為商業用途（如銀行開戶、申請電話等）或個人之間的身分證明用途，不受任何限制，如成為機關或大廈出入管制的依據（即俗稱的「押證件」）。這些作法，不僅讓商業機構規避其本應進行的客戶身分確認的工作與成本，更迫使個人揭露不必要的個人資料（如配偶與雙親的姓名與自身的身分證統一編號等）。目前一些使用身分證影本以表示本人授權，或是將身分證交付他人以委託行使權利的作法，並不是合適的作法，應以立法限制；也就是說，身分證應由當事人出示，方有身分識別之效用，且應於識別後立即收回，不能留置（包括影本）。此外，身分證統一編號因其可作為區別我國國民的單一號碼²⁷，可據此相互索引該個人於其他資料庫中的個人資料，故身分證統一編號的浮用，對不熟諳個人資料保護的民眾尤其不利，更需立法限制其使用²⁸。

此外，政府不可以涉入商業活動所需的身分認證的機制或運作²⁹。不同的商業行為，所需要的身分認證的程度與方法不同：購買電話卡與辦理信用卡或進行房屋買賣時，其中身分證明需求不同；各種線上購物與面對面交易，身分確認的方式也有極大的差異。政府如果以現行的身分證制度為基底，介入數位身分證的市場，以身分證的強制性質，以及其公權力意涵，政府的採用方式與系統，勢必成為資訊技術取舍或商業環境經營上，重大的非市場因素。此數位身分證系統的技術提供廠商（無論是否以資訊服務委外方式承作，或是完全由政府規劃執行），恐也將因此取得市場上的支配性地位。整體而言，這並不有利於商業環境的多樣發展。政府所應該作的，反而是嚴格限制身分證的使用（只限公民與公務機關之間往來時使用）。同理，政府也不應進行無特定目的的指紋建檔工作（無論是強制或自願性質），甚至以其作商業上身分證的用途。

政府應該作的，是讓社會大眾瞭解個人資料保護的重要性，並對不尊重當事人權益、不依誠實及信用方法、或逾越特定目的以蒐集處理個人資料的情形，積極調查，並對違法者確實加以懲處，以保護民眾的權益³⁰。這些教育宣導、投訴處理、以及主動督察的工作，依目前《電腦處理個人資料保護法》不訂主管機關

²⁶ 然而，依現行《戶籍法施行細則》，第二十條：「國民身分證之效用及於全國。國民身分證應隨身攜帶，非依法律不得扣留」。國民身分證成為國人自由行動的必要證件。亦參見該細則關於戶口清查的諸項規定。戶籍與身分證的制度，實為威權執政者控管公民居住行動之方式。

²⁷ 依筆者瞭解，只有在原有編號重複、錯誤，或個人性別變更時，國人的身分證統一編號才可能更換。

²⁸ 身分證統一編號浮用之情形，亦見於美國社會保險號碼（Social Security Number; SSN）逐漸成為通用的身分識別號碼（如被要求使用為駕照號碼等），參見（Garfinkel, 2000; pp. 20-25, 32-35）。這種因眼前的行政便利，而將原本為特定目的之用的個人資料或系統，轉作他用的情形（所謂 mission creep），對行政機關是很大的誘惑，故需立法加以限制。

²⁹ 然而，目前政府似乎常往相反的方向規劃，參見（李宗佑，2002）。

³⁰ 《電腦處理個人資料保護法》第六條：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍」。

的情形，並不能有效展開。許多國家皆以設置個人資料保護委員會（Personal Data Protection Commission）的方式，甚至設立個人資料保護官的職務，由專職機關專人負責，將保障個人資料的重要訊息，主動推廣至社會各階層，並接受各界的查詢和投訴³¹。

肆、誰的事務？

在高度資訊化的社會裡，商業機構和政府機關，或甚至許多個人，在資訊處理技能上，超出一般社會大眾甚多。這種資訊技能上的差距，加上商業機構與政府機關在資源與制度上的優勢，使他們在個人資料的蒐集與處理上，具有極大的能力與諸多可能，非一般大眾可以分別抗衡。因為個人資料的私密性質，尤其經由眾多與個人相關的異動資料，可組合而成爲對個人活動的監視，如何保障個人資料，使個人權益不受侵害，便成爲眾人關注的事務。

經由法律程序、訴訟判例，或是「個人資料保護委員會」政府專職機關的宣導與監督，北美與西歐國家在個人資料保護的事務上，已有一定的程序及機制，而一般大眾對於隱私與個人資料保護的議題，也不陌生³²。相較之下，我國在個人資料保護的相關事務上，雖有《電腦處理個人資料保護法》的立法，但在執行上，卻不能顯著的達到保護的目的。尤其公務機關在個人資料的蒐集處理，常有逾越必要目的情形，或對於其所掌有的個人資料庫的安全維護，怠惰以對。對於眾多商業機構在個人資料處理或保護上，有無遵守《電腦處理個人資料保護法》的規定，也沒有制度性的督察。民權團體或組織，限於經費與人力，通常僅能關注特定的隱私議題或政府計畫。總結以上情形，導致一般大眾的個人資料易遭受侵害、個人權益受損時，並且於發現受害之時，並無可遵循的諮詢或救濟管道。個人資料保護，雖是眾人的事務，在我國目前實際上幾乎是無人關注的事務。

³¹ 例如，澳洲政府自 1998 年通過《隱私條例》（*Privacy Act*）後，成立了獨立、專責的「聯邦個人隱私專員公署」（The Office of the Federal Privacy Commissioner，網址：<http://www.privacy.gov.au>），該個人隱私保護專員本身且是澳洲「人權及平等機會委員會」成員之一。以臨近的中華人民共和國香港特別行政區爲例，其自 1996 年制定《個人資料（隱私）條例》後，已依該條例設立「個人資料私隱專員公署」（網址：<http://www.pco.org.hk>），負責該條例的執行工作和各界推廣。澳洲與香港設立這些保護機構的情形並非特例。事實上，自歐盟《個人資料保護指令》（*Directive 95/46/EC*）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，其中即包括獨立的個人資料保護機構的設立。據香港「個人資料私隱專員公署」之統計，全球至少已有 30 個國家設有獨立性質之個人資料保護公署（全表參見網址：<http://www.pco.org.hk/textonly/english/infocentre/relatedwebsite.html>）。

³² 關於以訴訟方式達到個人隱私在美國受到實質保護的情形，可參見（Alderman and Kennedy, 1995）。歐盟關於個人資料保護之法律，可參考《歐洲議會與歐盟議會 1995 年 10 月 24 日通過之 95/46/EC 指令：關於個人資料處理以及此類資料自由流動的個人保護》（*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*，網址：http://europa.eu.int/comm/internal_market/en/dataprot/law/）。

爲了落實個人資料保護，政府應積極籌設「個人資料保護委員會」，主動進行個人資料保護的教育宣導、投訴處理、以及監督調查工作，對違法者加以懲處，以保護民眾權益。對於《電腦處理個人資料保護法》罰則過輕、位階太低的情形，應以修法，以阻止目前商業機構在處理個人資料時，常有逾越必要目的，或是不以誠信方法進行的情形。對於公務機關權力過大的情形，尤其當其認爲「對當事人權益無侵害之虞」，即可進行個人資料之蒐集處理規定（且不論其所蒐集的資料是否爲達特定目的之最低度需求），應修法緊縮其權力；同法第八條允許公務機關在寬鬆的條件下，對已蒐集處理之個人資料，逕行作做特定目的外之利用的情形，亦應同時檢討。

伍、結語

數位化的台灣社會，會是一個怎樣的社會？或許她不應該只是一個會使用資訊技術於生活的社會，而更應該是一個能探索資訊技術對生活影響，並能爲之因應的社會。隱私與個人資料保護的議題，隨著生活的數位化，其重要性將逐漸顯著。數位台灣的社會大眾，是否清楚其中的議題？對於由政府、商業、社會、與技術四方而來，在個體自身上的這一場隱私拉鋸戰，是否都已經做好準備？

數位台灣，妳是否已做好準備？

參考書目

- 立法院，《消費者保護法》，1994年1月11日公告。
- 立法院，《電腦處理個人資料保護法》，1995年8月11日公告。
- 立法院，《戶籍法》，1997年5月21日公告。
- 立法院，《民法》，2000年4月26日公告。
- 立法院，《全民健康保險法》，2002年7月17日公告。
- 行政院，《戶籍法施行細則》，1998年3月4日公布。
- 行政院，《行政院所屬各機關資訊業務整體委外作業實施辦法》，1998年4月8日核定。
- 行政院，《行政院所屬各機關資訊業務委外服務作業參考原則》，2002年11月1日核定。
- 行政院資訊發展推動小組「IC卡規劃及推行小組」，《「國民身分健保合一智慧卡（簡稱國民卡）」專案徵求建議書文件（含補充說明及詢答紀錄彙訂本）》，1998年6月10日。
- 中央研究院資訊科學研究所，《國民卡相關技術與社會影響研討會》彙編，1998年11月4日。
- 中央健康保險局，〈健保IC卡卡片存放內容〉，《衛生署公報》，第32卷第1號（2002年8月23日）。
- 中央健康保險局，〈健保IC卡管理須知〉，《衛生署公報》，第32卷第6號（2002年11月4日）。
- 中華民國愛滋感染者權益促進會，〈哪些政策侵犯我的權益？〉專題企畫，《中華民國愛滋感染者權益促進會會刊》，第13期（2003年1月1日）。
- 台灣人權促進會策劃，李茂生主編，《2001年台灣人權報告》。前衛出版社，2002。

台灣人權促進會，〈誰在看我？我要隱私權〉專題，《人權雜誌》，2002 年春季號。

李宗祐，〈電子身分證，六年將發三百萬張〉，《中國時報》，2002 年 11 月 20 日。

宋伯東，〈財金公司員工涉勾結偽卡集團〉，《聯合報》，2002 年 9 月 17 日。

牟玉佩、陳于嬌，〈賣民眾就醫資料，健保局 2 人送辦〉，《聯合報》，2003 年 1 月 14 日。

何建明、王大為、黃世昆、莊庭瑞、劉靜怡、陳正然，〈國民卡：資訊社會最大的夢魘〉，《中國時報》，1998 年 8 月 18 日。

黃文雄，〈一人一號系統，衍生資訊安全問題〉，《中國時報》，1998 年 9 月 23 日。

黃哲民，〈總統家人黨主席，隱私也被賣了〉，《中報晚報》，2002 年 4 月 19 日。

黃啓洞，〈員警勾結擄車集團，提供失竊車籍資料遭羈押〉，《東森新聞網》，2002 年 1 月 10 日。

莊庭瑞，〈資訊、社會與個人：再談「國民卡」風暴〉，《自由時報》，1998 年 10 月 18 日。

莊庭瑞，《出席內政部研商「國民身分證健保合一 IC 卡規劃方向」方案會議書面資料》，1999 年 4 月 20 日。

莊庭瑞，《出席中央健保局「健保 IC 卡第一次專家會議」書面補充意見》，2000 年 2 月 24 日。

莊庭瑞，〈從健保 IC 卡談台灣的個人資料保護〉，《自由時報》，2002 年 8 月 6 日。

莊庭瑞，《出席立法院衛生環境及社會福利委員「健保 IC 卡」公聽會書面意見》，2002 年 10 月 23 日。

莊庭瑞、黃文雄，〈指紋全民建檔，擾民傷財〉，《中國時報》，2001 年 7 月 19 日。

莊庭瑞、何建明，〈全民指紋建檔的源由與分析 — 兼談我國行政與立法部門對個人隱私保護的認識〉，《人權雜誌》2002 年春季號。

莊庭瑞、陳佳君、童素琴（編），《數位落差與資訊社會研討會彙編》，中央研究院、行政院研究發展考核委員會、財團法人資訊工業策進會共同出版，2001 年 12 月。

張致和，〈用戶資料外洩，中華電信遭人檢舉想私了〉，《中國時報》，2003 年 3 月 14 日。

張啓凱，〈電告轉帳退稅，歹徒設的局〉，《中國時報》，2003 年 3 月 7 日。

蔡再本，〈洩漏消費者個人資料，業者僅賠每人 4 元？！ — 過輕的罰則不足以業者濫用個人資料〉，《消費者報導》，第 261 期（2003 年 1 月）。

劉靜怡、王大為、莊庭瑞、黃世昆、張藝鴻、蕭奕弘、曾志超，《戶籍資料運用、個人資料保護與身分識別之研究：戶政資訊系統與相關制度建置之研究》，台北市政府民政局委託研究計畫期末報告，2001 年 2 月 1 日。

謝明俊，〈起獲偽造金融卡，全是世華銀〉，《中國時報》，2003 年 2 月 7 日。

Ellen Alderman and Caroline Kennedy, *The Right to Privacy*. DIANE Publishing Co., July 1995.

The Economist, "Printing Error – A judge has ruled that fingerprint evidence is scientifically unreliable." January 17, 2002.

Oscar H. Gandy, Jr., *The Panoptic Sort*. Westview Press, 1993.

Simons Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly & Associates, 2000.

Jerry Kang, "Information privacy in cyberspace transaction." *Stanford Law Review*, 50(April 1998): 1193-1294.

Mark Landler. "Hong Kong plans digital ID." *New York Times*, February 18, 2002.

Lawrence Lessig, *Code and Other Laws of Cyberspace*. Basic Books, 1999.

Simon London, "Radio ID tags spread waves of anger among privacy activists." *Financial Times*, Weekend March 1-2, 2003.

David Manasian, "Digital dilemmas: a survey of internet society." *The Economist*, 366:8308(January 25-31, 2003).

National Research Council, *Trust in Cyberspace*. National Academy Press, 1999.

Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.

Jay Stanley and Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*. American Civil Liberties Union, January 2003.

Peter P. Swire, "Financial privacy and the theory of high-tech government surveillance." *Washington University Law Quarterly*, 77(Summer 1999):461-513.

Samuel D. Warren and Louis D. Brandeis, "The right to privacy." *Harvard Law Review*, 14:5(December 15, 1890):213.