第一章　緒論

第一節 研究背景

維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。司法院釋字第 603 號解釋理由書：「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，其中包含個人自主控制其個人資料之資訊隱私權，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。」即係明確宣示隱私權是人類的基本人權，具有普世價值，是以人們就其私領域應享有一定的控制權，私人資訊應依法受到保護，不被他人非法侵擾、窺探、蒐集、利用和公開[1]。

再者，隨著新興科技引領人們步入全新的資訊時代，人們習於以數位方式記錄生活，而在數位匯流及資料探勘等相關技術普及應用下，他人私密資料之蒐集與分析成爲輕而易舉之事，進而加深了個人資料遭到不當利用之風險[2]，有關隱私權之爭議，而鬧上公堂的案例，不僅數量上日漸增多，在類型上也日益複雜而多元。事實上，個人資料在資訊科技發達的推波助瀾下，「隨時」可能因爲人爲因素，或者單純的技術性原因，而流入網際空間爲他人所讀取、進而加以利用。此外，由於網路的傳輸性，不僅快速，而且無遠弗屆，使得個人的資料一旦遭披露於公開場域，就不可能予以回收。換言之，個人資料日漸透明，且一旦流入網際空間，就會瞬息千里，舉世皆知，任何人皆能取得、掌握並流通，後果難以收拾。

---

[1] 宋榛穎、林怡臻。〈媒體侵犯隱私權之判決研究：臺灣與美國之比較〉，《傳播與管理研究》，11 卷 1 期，2011 年 7 月，頁 4。

[2] 郭戎晉。〈論數位環境下個人資料保護法制之發展與難題--以「數位足跡」之評價爲核心〉，《科技法律透析》，24 卷 4 期，2012 年 4 月，頁 18。

爲因應資訊科技以及網路技術的日新月異，先進國家政府早已立法規範，確保個人資料受到適當保護與運用，我國甚早即關注隱私保護問題，於 1995 年實施電腦處理個人資料保護法，並鑒於該法之缺失，立法院於 2010 年 4 月 27 日三讀修正通過，並於 5 月 26 日公布個人資料保護法，於該法中進一步擴大適用主體之範圍，增加搜集、處理或利用個資之義務，提高罰則，並增訂團體訴訟制度與訴訟專屬管轄之規定。法務部嗣於 2011 年 10 月 27 日公告施行細則草案，預計新版個人資料保護法最快在 2012 年 6 月實施。

時值國內個人資料保護法制邁入新紀元之際，如何預防附隨社群網路之發達與數位資訊科技之進步而導致個人資料可能遭受濫用的惡害，檢討我國法制是否妥當，有無造成過重負擔或保護不足之問題，即是眼前刻不容緩的工作。

第二節 研究目的

本研究之主要目的，係針對我國新版個人資料保護法的規範基礎，探討台北市政府各機關該如何落實個人資料保護法執行方案；同時針對個人資料保護法施行後，對各行政領域之法制以及行政流程可能產生的衝擊影響進行評估，檢討法規範可能潛藏之各項疑義，並藉由國外相關法制及實務案例之經驗，就本法的解釋、適用以及相關的法制配套提出建議，提供思考保障個人資料隱私、自主之新方向，以調和人民「知的權利」與個人資料保護之衝突，期有助未來實務應用及相關法制的進一步發展。

第三節 研究架構

爲達成上述研究目的，本計畫的研究內容將循以下三大架構順次開展：

壹、 個人資料保護之法理分析

個人資料保護法第一條明定：爲規範個人資料之蒐集、處理及利用，以「避免人格權受損害」，並「促進個人資料之合理利用」，特制定本法。據此，本法之立法目的在於保護個人之人格發展，及促進個人資料之合理利用，因而立法規範個人資料之蒐集、處理及利用之程序與限制，以平衡個人資料的合理利用與資料當事人的人格發展，明確個人資料保護之射程範圍。

由是觀之，個人資料保護法的規範，乃環繞在個人隱私保障的核心理念而爲建構。是以，本研究有必要先從比較法的觀點，探求美國法上「資訊隱私權」（Information Privacy）之淵源發展，包括最初概念的提出、學者的討論、在美國侵權行爲法上的肯認，立法上的創設，到被提升至憲法權利的經過。另外考慮我國法制深受歐陸法系，特別是德國法的影響，針對德國聯邦憲法法院所提出的「資訊自決權」（Informationelle Selbstbestimmung）的發展，亦有介紹的必要。最後再以歷史分析法佐以規範分析法，從憲法及大法官會議解釋爲立論基礎，彙整我國之相關法源，基於前述研究方法所獲致之結果，對隱私之內涵、範圍、定義予以探究及釐清，以作爲後續討論個人資料保護法制的基礎。

貳、 個人資料保護之實證規範架構

在抽象的基礎理論分析之後，接下來即有必要針對個人資料保護的實證規範架構進行研究。此一單元的論述安排，首先，台灣作爲繼受法的國家，自不能免於外國法的影響，因此首先將從比較法的觀點，針對個人資料保護法制的運用，略予闡明，俾收他山之石可攻錯之效。接下來，再以上述的分析爲基礎，闡釋我國個人資料保護法制的架構及並指出適用上可能存在的問題點。

（一）個人資料保護法制規範之範圍、方式、類型與發展趨勢——比較法的觀察

二次大戰後，個人資訊隱私權漸獲重視，惟發展緩慢，一些國際組織（如聯合國、經濟合作暨開發組織、歐洲理事會、歐洲聯盟、亞太經合會）陸續通過個

人資料保護規範，企圖影響會員國法制的建立及走向。事實上，全球各國際組織或國家對於資訊隱私的態度大相逕庭，可分爲三種類型：（一）全方位或全面適用式（comprehensive）的個人資料保護法制（如歐盟會員國、澳洲、加拿大、日本、2010 年 4 月 27 日「個人資料保護法」修正案生效後的台灣）；（二）僅適用於少數特定產業的部門式（sectoral）個人資料保護法制（如美國、2010 年 4 月 27 日「個人資料保護法」修正案生效前的台灣）；（三）完全欠缺個人資料保護法制（如中國大陸、印尼及菲律賓）[3]。現估計，全球超過六十個國家[4]擁有某種形式的個人資料保護法律。

其中，對於建立全球一致性的個人資料保護標準頗有影響的歐洲聯盟，爲保護會員國國民的隱私基本人權及促進會員國間個人資料的自由流通，於 1995 年制定「資料保護指令」（Data Protection Directive），並於 1998 年 10 月生效。而歐盟資料保護指令與 OECD 及 APEC 等國際組織規範不同者，歐盟資料保護指令對於會員國具有強制拘束力。然而，如同歐盟一般指令，資料保護指令並不具「自動執行」（self-executing）效果，不能直接適用於會員國人民，仍賴會員國按指令所要求的最低標準制定內國個人資料保護法規，但各國立法並非完全一致，仍容許因地制宜（如各國關於行政程序與違反效果的規定不盡然相同）的存在[5]。類似於我國 2010 年 4 月 27 日新修正的「個人資料保護法」，歐盟資料保護指令全方位地適用於自然人、法人及政府部門對於個人資料的蒐集、利用或分享等行爲[6]，以期解決個人資料流通所衍生的弊端。

亞太經合會則於2004年11月制定亞太經合會隱私綱領（The APEC Privacy

[3]See Jody R. Westby, American Bar Association, International Guide to Privacy 6 (2004).關於個人資料保護法規的世界地圖（A map of Data Protection Laws Around the World），http://www.guardianedge.com/resources/data-protection.php (last visited May 25, 2012)。

[4] Karin Retzer, Cynthia Rich, Morrison & Foerster LLP, GLOBAL SOLUTION FOR CROSS-BORDER DATA TRANSFERS: MAKING THE CASE FOR CORPORATE PRIVACY RULES, 38 Geo. J. Int'l L. 449 (Spring, 2007).

[5]Westby, supra note 8, at 89-91.

[6] EU Data Protection Directive, arts. 2 and 4, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited May 25, 2012).

Framework[7]），揭櫫個人資料蒐集、利用、處理及分享的九大原則（預防損害【Preventing Harm】、通知【Notice】、蒐集限制【Collection Limitation】、個人資料之利用【Uses of Personal information】、選擇【Choice】、個人資料完整性【Integrity of Personal Information】、安全維護【Security Safeguards】、接近與更正【Access and Correction】及責任【Accountability】）。雖然，亞太經合會隱私綱領對於會員經濟體（Member Economies）並無強制拘束力，但可協助會員經濟體制定足以衡平隱私保護與個人資料跨國流通的隱私法規。事實上，這九大原則乃參考全球許多隱私相關法律體制（如OECD「有關隱私權保護及個人資料跨國流通之準則」【The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data】）發展而來。

相較於歐盟或我國 2010 年 4 月 27 日新修正的「個人資料保護法」採用「政府管制」爲主、「市場機制」爲輔的全方位或全面適用式（comprehensive）個人資料保護模式，美國則採「市場機制」爲主、「政府管制」爲輔的部門式（sectoral）個人資料保護模式。美國模式係將個人資料的蒐集、使用或分享問題，委由當事人個人與資料蒐集者雙方自行透過自由市場的機制協商，政府並不積極介入管制，必要時才輔以產業界自訂的自律規範。然而，在某些特定的產業，濫用消費者個人資料的問題嚴重，形成隱私權保護的危機，政府乃特別制定僅適用該特定「部門」的法令，以求市場失靈之解決。在所謂「部門式」的立法中，對於個人資料的蒐集、利用及分享，美國政府部門因「1974 年隱私法」而受到面向較廣的拘束，但私人部門則欠缺如「歐盟資料保護指令」的全方位式保護個人資料的規範[8]。自 1970 年代起，美國國會陸續通過不少僅適用於特定產業部門的隱私法律，如公平信用報告法（Fair Credit Reporting Act）、家庭教育權利及隱私法（Family Educational Rights and Privacy Act）、金融隱私權法（Right to Financial Privacy Act）、隱私保護法（Privacy Protection Act）、有線通信政策法（Cable

[7] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (last visited May 25, 2012).

[8] *See* Westby, *supra* note 3.

Communications Policy Act）、錄影隱私保護法（Video Privacy Protection Act）、電話消費者保護法（Telephone Consumer Protection Act）、駕駛人隱私保護法（Driver's Privacy Protection Act）、健康保險可攜性與責任法（Health Insurance Portability and Accountability Act）、兒童線上隱私保護法（Children's Online Privacy Protection Act, COPPA）、金融服務現代化法案（Gramm-Leach-Bliley Act, GLBA）、未經邀請而主動推介色情與市場銷售之侵犯管制法（Controlling the Assault of Non-Solicited Pornography and Marketing Act, Can-Spam Act）、銀行秘密法（Bank Secrecy Act）、美國愛國法（The USA-Patriot Act）等[9]，對於個人資料之蒐集、使用或分享加以規範。

因此，本部分將針對目前美國、歐盟以及亞太經合會的相關規範，就其法制有關個人資料保護之範圍、方式、類型及管理機制進行探究，以一窺該法的優劣。最後並就上開國際組織及國家相關規範與實務案例，歸納國際上因應資訊社會之變遷，個人隱私之保護有何發展趨勢，檢視我國關於個人資料保護立法之良窳，所以他山之石可以攻錯，瞭解外國法制的經驗及發展，有助於我國個人資料保護規範法制的解釋、運用、探尋與確定。

（二）我國個人資料保護法制的規範模式與重點

觀察新修訂之個人資料保護法，其修正重點包括：一、擴大保護客體：不再以經電腦處理的個人資料爲限，更擴及於人工處理者或其他非實體個人資料，特別加強對醫療、基因等高敏感性特種個人資料之保護。二、適用主體之全面化：將原適用電腦處理個人資料保護法之非公務機關僅限定於法律及主管機關[10]所

[9] 周慧蓮，資訊隱私保護爭議之國際化，月旦法學雜誌，104 期，頁 115，2004 年 1 月； DANIEL J. SOLOVE AND MARC ROTENBERG, INFORMATION PRIVACY LAW 23-24 (2003); *also* Westby, *supra* note 3, at 15-63.

[10]按「電腦處理個人資料保護法」第 3 條第 7 款之非公務機關，除法律明文規定之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、保險業及大眾傳播業外，另按法務部之公告包括「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

規定的十餘種特定行業部門之規範廢除，全面性擴及公務機關以外之自然人、法人及其他團體。三、義務之增訂：新法中增訂對公務機關或非公務機關蒐集個人資料時，應告知當事人之義務；間接蒐集時告知資料來源義務；個人資料被竊取、洩漏等事件發生時之通知義務；及非公務機關利用個資行銷時當事人得選擇退出（opt-out，意即當事人得於自己資料被蒐集、處理或利用後，要求停止再利用之權利）之制度。四、提高罰則及加強中央目的事業主管機關或直轄市或縣、市政府爲檢查等處分之權責，加強行政監督。五、增訂團體訴訟制度與訴訟專屬管轄制度[11]。

究其根本，此次修正主要係爲彌補舊法以往實證之缺失，並切合資訊時代之需求，朝向加強保護當事人資料之方向而爲立法。探究本法適用的要義，在於確保個人資料私密性不受侵害，並爲避免不當適用本法反造成今後社會生活維繫、政府資訊公開乃至於產業經濟活動之損害。[12]上述規範意旨在實務上是否能夠獲得徹底的實現，吾人對於個人資料保護法之法例體系、適用範圍、規制手法以及程序是否已充分且正確地掌握，至爲關鍵。

從而，本節將先從規範的觀點，就我國個人資料保護與資訊安全之立法予以詳盡的分析探討，解析我國個人資料保護的規範架構與特色，並對適用上易發生爭議的法律要件進行釋義研析

參、 未來新法施行對台北市現行法規可能產生的衝擊暨其因應之道

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。」可參見網路資料庫 http://www.moj.gov.tw/public/Attachment/21111658463.pdf，2012 年 5 月 25 日。

[11] 范姜真媺。〈個人資料自主權之保護與個人資料之合理利用〉，《法學叢刊》，57 卷 1 期， 2012 年 1 月，頁 71。

[12] 關於個人資訊隱私保護作爲資訊公開的界限，我國資訊公開法第十八條第六、七兩款即著有明文。比較法上，以美國爲例，亦將資訊隱私保護列爲豁免公開的原因之一。參 湯德宗，政府資訊公開法修正芻議，收於「政治思潮與國家法學——吳庚教授七秩華誕祝壽論文集」，頁 268-270（2010）。

個人資料保護法的正式施行，強化了個人資訊隱私保障的結果，無疑將會對公務部門、資料主體當事人、企業及委外廠商間關於個人資料的往來與使用，造成深遠的影響。站在行政機關的立場，未來在個人資料保護管理策略上，不論是內部業務管理程序、委外處理機制的實務作爲，都必須時時以維護個人資料安全爲念，是以針對個別行政領域的法規與實務運作流程，從個人資料保護的視點進行通盤檢討，自爲本研究計畫的核心任務。

由於個人資料保護所涵蓋的範圍甚廣，涉及個人、企業或法人組織及國家機構，重要性不言可喻，因此，本計畫將依據前述各章節的研究發現，基於本計畫之研究目的，對個人資料保護相關之法律議題予以彙整後，就制度面與實務面提出興革建議；此外，在研究過程中，並將選定台北市政府警察局、衛生局，社會局、民政局與教育局等五個機關，就其所主管的自治法規，擇一與該局負責人員訪談，期能更具體掌握實務上所面臨的實際問題，進而針對其資訊安全法制的強化與個資保護法制之配套等方面進行論述，提出具體的規範及建議內容，裨作爲行政機關因應個人資料保護法施行之參考。

第四節、 研究過程與方法

爲瞭解個人資料保護法通過後，對於現行台北市的法制與行政實務，將造成何種衝擊，以及法制上應如何適切回應此一衝擊，本研究將採取「文本分析」（text analysis）與制度的「比較研究」（comparative study）來進行相關資料的整理與分析，希冀透過一手及二手資料的蒐集、分析與比較，指出各國（或地區）關於個人資料保護法制的規範特色，以作爲檢討台灣現行法制的認知基礎。詳言之：

1. 運用資料之範圍與種類

以我國與美國、歐盟與亞太經合會，關於個人資料保護及政府資訊公開的相關法規、學說及實務文獻爲主。

2. 蒐集資料之程序與方法

自行蒐集或購買本國及外國相關文獻資料。挑選、整理具有法理的創見以及實務判決見解。

3. 資料分析方法

針對美國、歐盟以及亞太經合會與個人資料保護的有關指針，進行實證條文之規範分析與文獻資料比較分析、尤其是各國（區域）間對隱私權規範密度差異之解析。此外，就觀察所得之結論，再與我國關於個人資料保護之司法案例爲對照分析。

第五節 預期研究結果

本研究計畫以我國現行的電腦處理個人資料保護法及已通過尚未全面施行的個人資料保護法爲基礎，比較分析現代主要國家關於個人資料保護之規定、個人資料外洩的通知措施及因應科技發展對隱私保護的未來發展趨勢。是以本研究計畫的執行，將有助於對於我國及現代主要國家個人資料保護法制之瞭解，研究成果並得以供中央或台北市將來相關立法或政策制訂之參考，亦可裨益於法院未來適當處理有關個資外洩及隱私保護之爭議。

第二章　個人資料保護的法理基礎

──隱私權概念的發展與我國法的繼受

第一節 個人資料保護與隱私權

個人資料保護法（下稱新法）之前身係電腦處理個人資料保護法（下稱舊法），其修正草案是 2004 年送至國會，並先後經二次的屆期不續審後三度送至立法院，嗣在「大眾傳播媒體處理或利用個人資料前應否告知當事人」的爭議中，罕見的經院內的復議後，始落錘定音[1]，其過程可謂一波三折。然而，新法雖於 2010 年 4 月 27 日完成三讀程序，並於同年 5 月 26 日經總統公布，但迄今尚未施行。

相對於舊法是參考 OEDC 所揭示之隱私保護暨個人資料國際傳遞指導綱領的八項原則（限制蒐集原則、資訊內容完整正確原則、目的明確化原則、限至利用原則、安全保護原則、公開原則、個人參加原則及責任原則）而制定，新法之立法原則係參考 1995 年歐盟資料保護指令所提出之九項要求（資料品質原則、資料處理合法原則、敏感資料之處理、告知當事人、當事人之權利、當事人的反對權與自動化的個別決定、資料保密與安全、向國家主管機關登記與處理作業公開以及國際資料傳遞原則）而修訂[2]。雖然如此，新法的規範仍係環繞著個人資料與隱私保護爲核心而建構的理念，卻始終不變。

德儒耶林（Rudolf von Jhering）的名言：「目的是法律的創造者」，既然一般咸認個人資料保護法的立法目的在於隱私保護，是以本章即擬先針對隱私權——

[1] 呂丁旺，修正《個人資料保護法》的釋義與實踐（上），國會月刊，第 38 卷第 11 期，頁 20。

[2] JODY R. WESTBY, AMERICAN BAR ASSOCIATION, INTERNATIONAL GUIDE TO PRIVACY 84-85 (2004). 本計畫第三章對於各該原則的實證並有詳細的介紹。關於此一原則相關的中文文獻，可參黃荷婷，個人資料保護法之政策與執行措施─建構安全信賴的政府，人事月刊，第 52 卷第 7 期，頁 7-10。

特別是「資訊隱私權」——的概念生成以及保護內涵進行探討，其間並借鏡、比較法（美國、德國）的經驗，論述隱私權概念在我國的概念建構、規範內涵與實證基礎等，期能透過對於隱私權意涵的釐清，有助於吾人對於個人資料保護法中相關條文的立法意旨以及規範功能的侷限有所認識，以作爲本研究計畫後續各章開展的基礎。

壹、 個人資料保護法的法理基礎概觀

（一） 以「資訊隱私權」作爲核心的個人資料保護

按個人資料保護法第 1 條明定：「爲規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」據此，新法之立法目的乃在衡平個人人格法益之保障與個人資料之合理運用，其保護範圍應及於個人資料之蒐集、處理與利用。

參照 2005 年 9 月 28 日司法院大法官所作出的釋字第 603 號解釋文第一段：「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。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，而受憲法第二十二條所保障（本院釋字第五八五號解釋參照）。其中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。惟憲法對資訊隱私權之保障並非絕對，國家得於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。」據此，學界乃將前述新法所欲避免之個人法益侵害，指向前述解釋文中所揭示之具基本權地位的隱私權，或者，由於新法所規範之客體係「已外部化的個人資料」來看，更確切地說，應是「資訊

隱私權」。[3]

（二）「第三人對個人資訊隱私權之侵害」立法規制上的質疑

在「個人資料之合理運用」的立法目的部份，針對國家機關的立法限制乃基本權傳統防衛面向之常理，尚無疑慮；有疑問的是在針對第三人侵害個人資訊隱私權的立法妥當性上。

許宗力與曾有田兩位大法官在釋字第 603 號解釋所共同提出的協同意見書中指出：「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。」，同時，參照司法院大法官於 2011 年 7 月 29 日，針對「新聞採訪者之跟追行爲受到社會秩序維護法第 89 條第 2 款規定限制是否違憲」一案，所作成之釋字第 689 號解釋的解釋理由書中指出的：「個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大爲增加，個人之私人活動及隱私受保護之需要，亦隨之提升。」等語，則大法官前述之立論，看似有意無意地參酌了德國聯邦憲法法院在 1983 年「人口普查判決（Volkszählungsurteil）」中針對資訊自決權的相關論述，並由此似乎可推論出，國家除應避免公權力機關侵害個人資訊隱私權外，並應有義務針對來自第三人之侵害採取適當的保護措施。據此，新法遂在其第三章中，針對「『非公務機關』對個人資料之蒐集、處理及利用（個人資料保護法第 19-27 條）」設有專章之規定。

[3] 參 劉靜怡，隱私權的哲學基礎、憲法保障及其相關辯論，月旦法學教室第 46 期，第 45 頁（2006.08）。

然則，姑且不論「爲避免第三人對個人資訊隱私權之侵害」是否即得當然導出國家有於現行已有之法制下另行立法保護之義務[4]，但將本質上應劃歸民事侵權領域的私人間衝突，與對抗公權力侵害的基本權保護事項，同時規範於同一法律之中是否合適，實有值得檢討之處。此外，以新法有限之九個條文的專章規定，是否即可涵括並率爾適用於所有的第三人對個人資訊隱私權之侵害之領域，恐亦不無疑問。

貳、 隱私權作爲基本權概念的引進

（一）我國早期實務上所呈現之紛亂的隱私權概念

「隱私」概念的探討在我國之歷來文化與社會生活中並不發達；近代以來「隱私權」的概念多由國外傳入。[5]然而，我國實務很早即對「隱私權」之議題做出過解釋，如法務部在民國 71 年（1982 年）7 月 26 日法律字第 9168 號函釋，即曾出現「隱私權」之用語，將隱私（權）等同秘密（權），認屬於民法上之人格權。[6]其後，在我國民國 88 年（1999 年）的民法修正中，並明文將「隱私」與身體、健康、名譽、自由、信用與貞操等人格權並列，以作爲得請求非財產上損害賠償之權利類型。然而，此種並列究係欲將之限縮於身體、健康、名譽、自由、信用與貞操之外的人格法益，抑或採取當時學說之意見，將「隱私利益」認爲是一「綜合性之人格權」，係集合生命、身體、健康、貞操、肖像、信用、名譽、

[4] 蘇永欽大法官在其所提之釋字第 689 號解釋（2011 年 7 月 29 日）的協同意見書中，對「社會秩序維護法第 89 條第 2 款規定，使新聞採訪者之跟追行爲受到限制是否違憲」乙事，就認爲當第三人侵害只屬傳統私權衝突領域時，並不是基本權間的直接衝突，故非國家保護義務之典型適例。

[5] 廖緯民，以個資法做爲公設街頭監視系統的法律規範基礎─一個比較法上的觀點─，台灣本土法學，第 87 期，頁 126（2006.10）。

[6] 王澤鑑，侵權行爲法（一）─基本理論，頁 149-150（1998.09）。另外，司法院第一廳所編即的民是法律專題研究（一）之第 225-226 頁，在民國 71 年司法院第一期司法業務研究會中，針對一件偷錄他人幽會並於其後予以騷擾之侵權事件，亦也相同之見解。

財產各該權利之一部（即各該權利之秘密部份）而形成[7]，在法釋義學上其實是留有解釋空間的。

相對於前述法律層次的隱私權討論，司法院大法官於 1992 年 3 月 13 日所作成的釋字第 293 號解釋表示：「銀行法第四十八條第二項規定『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』，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」，則早已明白肯認隱私權在我國憲法具基本權之地位，但卻始終未對隱私權之概念和憲法依據加以說明。此一立場，並爲司法院大法官於 2000 年 7 月 7 日所作之釋字第 509 號解釋所承繼。

此外，在法院判決先例上，作爲我國民法修正條文正式引入隱私權保護規定前，實務針對隱私權最明確之見解的臺灣高等法院 87 年（1998 年）上字第 76 號判決，其表示：「所謂隱私權，乃係不讓他人無端地干預其個人私的領域的權利，此種人格權，乃是在維護個人尊嚴、保障追求幸福所必要而不可或缺者。人的尊嚴是憲法體系的核心，人格權爲憲法的基石，是一種基本權利。憲法第二十二條明定『凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障』，隱私權係憲法所保障之基本人權，是被肯定爲值得保障之法的利益。又所謂不法侵害他人之自由，即係強制個人之身體或意思自由，此與無端干預個人事務，侵害個人不欲人知之隱私權利，二者除被害人於行爲當時知悉與否外，就違反個人意志之重要特徵上，及立法所欲保障個人意思決定之自由而言，並無二致」，則爲隱私權在我國憲法上找到了實證基礎，惟其論理上並使用了日本法上才有的「追求幸福的權利」，卻不免令人錯愕。其後，在最高行政法院 87 年判字第 2576 號判決中，法院實務表示：「人於睡眠狀態中具有極致之隱私權，不容他人侵害，他人亦無從限制其睡眠狀態中之姿勢動作」，則明確地闡明了隱私權概

[7] 翁岳生等著，資訊立法之研究，頁 38（1987）。

念應涵括「身體的自主決定權」的想法，對隱私權的保護領域作較爲廣義的詮釋，似有將我國法上隱私權朝向美國法的方向理解的痕跡。[8]

（二）我國釋憲實務對隱私權作爲憲法上基本權利的確立

在憲法未設明文規定的情況下，隱私權之所以得以確立成爲我國憲法上的一項基本人權，大法官解釋的實證，無疑是最大的推手。

例如，大法官在前已提及的釋字第 293 號解釋、釋字第 509 號解釋及其後於 2001 年 12 月 14 日作成之釋字第 535 號解釋中，皆肯認隱私權應受保障，然美中不足者，大法官卻始終未指出隱私權保障在我國的實證法源所在及權利體系上之定位爲何。同時，其在釋字第 509 號解釋中將個人名譽及公共利益與隱私並列，在釋字第 535 號解釋中將人民行動自由及財產權與隱私權同列，則不無造成基本權利體系上混淆的疑慮。

前述疑問，大法官直到於 2004 年 12 月 15 日針對三一九槍擊事件真相調查特別委員會所作成之釋字第 585 號解釋的「解釋理由書」「五、真調會行使調查權之方法、程序與強制手段」下的第一段中，方予以表明；其謂：「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，並爲保障個人生活秘密空間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（本院釋字第五○九號、第五三五號解釋參照）」。不過，由於前述大法官之論述係出現在解釋理由書中，而國內通說將大法官之解釋類比於法院之判決，故直至前述文字出現在釋字第 603 號解釋的解釋文中，隱私權在我國應作爲基本權利而受保障，方真正被確立。

[8] 所謂「美國法上的隱私權概念的理解」，可參本章第二節第一目針對美國法上隱私權的論述。又司法實務上對隱私權的此種「美國化」的理解，引發學者有違我國（較傾向德國模式的）基本權建構體系的質疑，參 張國清，隱私權保護概念的比較探討，全國律師，第 5 卷第 6 期，頁 16-17（2001.06）。

不過，縱使大法官已作出釋字第 603 號解釋，國內學界對於隱私權之實證基礎、概念內涵乃至保護範圍，卻仍是眾說紛紜。此亦更彰顯在掌握隱私權之概念核心上，有必要從比較法之觀點，理解隱私作爲一種權利的型塑過程，以期能對吾人構思本土化的隱私權概念，有所裨益。

（三） 小結：隱私議題的文化相對論

從比較法的角度觀察，隱私權的概念內涵，在不同的國家、法系間，有著相當高的差異性。例如法國學者孟德斯鳩在闡明自由權時，曾將自由區分爲憲法關係的自由權，以及市民關係的自由權，前者在斯時係指排除「國家公權力之行使」，對個人私生活領域之侵害的消極自由權；而後者則係處於市民生活間，本諸於實證法、習慣或當事人間之約定，而得爲排除「由之於國家之外之其他團體或個人之侵害」的消極自由權。[9] 這樣的說法，在採取德國基本權保障模式，將傳統自由權之防禦面向限縮於對抗國家並基於公私法之區分而異其法律適用的我國，自然顯得頗有些格格不入；然而，相對於未採行嚴格公私法區分的美國，卻可以作爲幫助我們理解，何以隱私權概念在該國實務的發展脈絡，得以如此輕易地由私法上的侵權行爲法領域轉入憲法層次的探討。

我國學者王郁琦先生，引用 Alan Westin 教授 1976 年在其名著《Privacy and Freedom》中，針對隱私問題所發表的看法：「每個社會必須以其本身之方式進行研究，敏銳的專注於社會習慣，進而探就是否有以其他措詞爲名的隱私規範，並以交叉文化比對的方式去識別其中所有的爭議」，提出隱私問題在文化上的重要意義便在於其相應不同社會所表現出的相對性，並進而在此一基礎上左右了法律和政策上的選擇。[10] 因此，作爲隱私權概念繼受國的我國進行法比較的觀察的最終目的，並非在撿擇應採取何國立法例上的隱私權概念，毋寧係藉由不同文化間隱私規範間的比較，去演繹出合於我國國情與法制體系的隱私權概念。

[9] 轉引自朱柏松，個人資料保護之研究─近代隱私權概念之形式及發展─（上），法學叢刊，第 29:2＝114 期，頁 78（1984.04）。

[10] 王郁琦，資訊時代隱私權理論基礎初探，世新法學，第 1 期，頁 284（2004 年 5 月）。

第二節 隱私權概念的發展

誠如之前所言的，隱私權是一個會因應不同社會、文化與法制而變動的概念，因此，在不同國家會形成不同的面貌。再者，雖然隱私權概念至今在其原生發展國之美國亦仍屬發展中之概念，並隨其實務或有所變動[11]，但藉助對彼國歷史和規範的觀察與分析，仍將有助於掌握隱私權在我國之發展脈絡，並進而爲本文提供研究之參考。另外，德國法上的資訊自決權，在個人資料保護法的研究上，亦常爲學者所引述，故本研究計畫在此，亦對此一概念作簡單的整理介紹，並嘗試比較兩者的一同即其對個人資料保護法制之影響。

壹、 美國法上的隱私權

〈一〉隱私權用語的提出

「隱私權」之用語，早在 1881 年 De May v. Roberts 一案便見諸於美國實務判決之上，惟當時並未將之當作一個獨立概念加以探討。[12]其後，Samuel D. Warren 因不滿其家居生活與女兒婚禮被媒體詳細報導，於是與 Louise D. Brandeis（後曾出任美國聯邦最高法院法官）共同在哈佛法學評論（Harvard Law Review）上發表「隱私權（The Right to Privacy）」一文，[13]渠等認爲傳統的名譽毀損法制保護並不充分[14]，而將「個人私生活」的本身稱作隱私這個概念，並且認爲隱私應該受到法律上之保護，該文中並援引了普通法之案例及 Thomas Cooley 法官所稱「不受他人干擾的獨處權利（the right to let alone）」的「生活的權利（right to

[11] 美國法上隱私權的概念明顯受同時期大法官─尤其是首席大法官─個人價值觀的影響。對此之相關論述。可參見：王俊文，我國憲法上隱私權相關問題的釐清，東吳法研論集，第 2 期，頁 221-222（2006.04）。

[12] 王俊文，同上註，頁 196。

[13] Samuel D. Warren & Louise D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[14] 當時侵權行爲法保障的範圍只及於受他人使用不實資訊之侵害，對於真實且隱密之資訊則不受保護。請參見：田育菁，社群網站於我國隱私權保障之研究，國立東華大學財經法律研究所碩士論文，頁 17（2011）。除此之外，當時對於隱私的概念認爲不屬於個人之財產，因此無法以財產法之規範作出主張。

life）」，企圖在侵權行爲法領域中提出新的權利類型。[15]

該文雖著重強調了隱私權侵害之構成，並非在關注公開事實之真實與否，而是在「防止私生活被侵犯」以及「個人對其自身事務公開揭露的決定權利」，並以此連結「個人的思想、情緒和感受（thoughts, emotions, and sensations）」，以保障「不受侵犯之人格（inviolate personality）」。然而，該文並未對「個人私生活」加以釐清與界定，其雖提出「惡意無法當作隱私侵犯的抗辯事由，因惡意不是隱私侵犯的責任成立要件」;「公開不實內容傷害到個人形象爲名譽權侵害所要保障之內容，但相對於名譽權，隱私權侵害之構成，並非在關注公開事實之真實與否，而是在防止私生活被侵犯或描述(即隱私著重在保護個人私生活的完整性）」;「隱私權並非在禁止全面之私人事務被公開，私人事務之內容具有一般（如日常間的耳語私話，該文中並提出，此一排除事由，除社會一般性之理由外，同時亦係基於對於言論自由之尊重而來）或公共利益（如出席法庭作證義務的履行）之事務性質時允許揭露」等觀點，但其仍非提供了一個全面的隱私概念，而僅係在普通法下探究隱私權之根源與應有之發展。[16]

〈二〉傳統的隱私權概念

1. Samuel D. Warren 和 Louise D. Brandeis 的奠基

雖然 Samuel D. Warren 和 Louise D. Brandeis 所發表的隱私權一文並未對隱私權權概念加以界定，但其將隱私的保障應包括「避免私生活領域之無故受侵擾」與「個人對其自身事務公開揭露與否決定（第一次揭露）的權利」，二者共同構

[15] 關於該經典論文的中文介紹，可參 詹文凱，隱私權之研究，國立台灣大學法律研究所博士論文，頁 18-19（1998）。附帶說明，在此之前，美國實務多係將隱私權侵害之案件，透過契約之違反、信賴之違反、不法侵害、預謀侵害、詐欺等侵權行爲理論來加以處理。請參見張國清，前揭註 8 文，頁 6。

[16] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1102; 中文介紹，可參 田育菁，前揭註 14 文，頁 17-18。

成「個人私生活的完整性」，並透過精神層面與人格權作連結，使其具有「不受侵犯之人格（inviolate personality）」的特質，並提出「惡意不是隱私侵犯的責任成立要件」、「藉由『保障個人私生活的完整性概念』與『不實侵害個人形象』的名譽權加以區分」以及「隱私侵犯得透過事務性質涉及公共利益（下稱公益性排除事由）或言論具社會一般性（下稱一般性排除事由）之理由加以排除」等的觀點，卻爲之後美國的實務與學說發展奠下了相當的基礎。

2. 隱私權一文對學說理論的影響

在 Samuel D. Warren 和 Louise D. Brandeis 所發表的隱私權一文之後，引發學界熱烈的討論，學者多方嘗試對隱私權本質進行探討，致使隱私權的理論呈現出多樣花的樣貌。例如，有在隱私權一文的基礎上，將個人私生活的完整性與不受他人干擾的獨處權利（the right to let alone）作結合所提出的「獨處權理論」者；另有論者提出「親密關係自治理論」，則在隱私權一文的基礎上，提出透過社群的概念，去建構一個高度屬人之私人事務所構成的親密關係（intimacy），將之劃歸「私領域（private sphere）」，並賦予個人對親密關係之自治權限，來與「公領域（public sphere）」作劃分；「一般人格權理論」是在隱私權一文的基礎上，推論出「一般人格權」即是隱私權在憲法層次之上位基本權利，並將其目的指向保持個人人格之完整性；「資料保留權理論」，則進一步將「個人對其自身事務公開揭露與否決定（第一次揭露）的權利」限縮在「未文字化」或者「保密而不與人知」的個人「自己」之資訊。[17]

3. 實務判決先例的承認

事實上，自 Samuel D. Warren 和 Louise D. Brandeis 建構隱私權此一權利後，美國實務直到 1931 年才由加州最高法院於 Melvin v. Reid[18]一案之判決內容中揭示了以下的意見：「一、雖然過去案例曾對隱私權加以摸索，然該權利確係自普

[17] 張國清，前揭註 8 文，頁 10。
[18] Melvin v. Reid, 112 Cal.App. 285 .

通法以來未曾存在。二、隱私權爲存在於人（格）之權利，不屬於財產上之權利。三、由於其存在於人格上之權利，因此其權利隨著權利人之死亡而消滅，無法永遠存續。四、凡經權利人自身或經其同意加以公開者，隱私利益即喪失。[19]五、身爲社會知名人士如政治家、企業家等，在某種程度上，可認爲投身於公眾（dedicated his life to the public）之中，就此部分可視爲捨棄隱私權之主張。六、就新聞或新聞事件的傳播，以及公眾對於知悉某特定人生活的資訊存有正當利益（rightful interest），例如競選公職的候選人，並不存在著侵犯隱私的問題。七、光憑隱私權口頭的言詞，並不足以造成隱私的侵害，而必須有圖片、文字等具有永久或重製性的作爲始足當之。八、 若加害人以侵害他人隱私作爲獲取利益的手段，則被害人的權利主張的正當性亦隨之增加。[20]

此一判決，不但肯認了隱私權之存在，並將之導向「憲法層次的基本權保障」；另外，其明白地將隱私權與個人之人格作結合，使之「與個人人格具有不可分離之關係」，因而「否定了其作爲財產權之性質」，並認爲「關於隱私的公開，權利人僅具一次性的利益」；針對隱私權侵害的一般性排除事由，「將一般性界定爲限於非營利性質」，爲言論自由與隱私權的衝突劃下一道界線；最後，其認爲針對「『自願性』成爲『公眾人物』之人，對於其『參與公眾事務之部份』可認爲放棄隱私權之主張[21]」，將以上的看法與 Samuel D. Warren 和 Louise D. Brandeis 所建構隱私權和前述學說見解相結合後，基本上便是了美國傳統上檢討的隱私權案例的基礎。由是，此一判決也成爲美國實務上針對隱私權的重要判決先例。

---

[19] 換言之，隱私權僅針對第一次資訊揭露加以保障。

[20] 國內有學者認爲，對於隱私權侵害所爲之請求，訴因（Cause of Action）應僅限於他人以營利爲目的之商業利用行爲，由此所受到之侵害始得該當（將私人事務的「一般性」排除事由，限於非營利）。參 朱柏松，隱私權概念之衍變及其損害防止立法之動向，法學叢刊，第 134 期，頁 91-92（1989.04）。

[21] 事實上，加州最高法院在 1953 年 Gill v. Hearst Pub. Co. (40 Cal.2d 224) 一案，更進一步的認爲「縱使當事人不是公眾人物」，只其係「自願」進入公眾場所，而其在該當場所的行爲表現亦係出於「自願」，則該當行爲便不具隱私內涵；此之立場，其後形成了實務常被提出之「隱私二元論」的判斷標準，亦即縱使是非公眾人物，「在公共場合也沒有隱私可言；唯有在私人處所之行爲才有可能被認爲是隱私」。然而，此一立場，縱使是同爲 Gill v. Hearst Pub. Co.一案的審判法官，亦有不同意見：如果贊同此一說法，將意味著我們對公眾場合中之任何拍攝行爲都給予無限之豁免權。相關說明，請參見：田育菁，前揭註 14 文，頁 22。

4. 傳統實務的總結與實證化

1960 年，著名的侵權行爲法學者 William L. Prosser 發表 Privacy 一文，將當時實務上有關隱私權之相關案例從事類型化分析整理，從而，把隱私權之侵害分成四種型態[22]：一、入侵（intrusion），亦即以「物理性之方式」對「個人私生活領域」進行之具「高度冒犯性（highly offensive）[23]」的侵擾；二、私人事務的公眾揭露（public disclosure of privacy facts），亦即將個人「未決定公開揭露」而「與大眾無關」的自身事務予以公開，該公開並具有「高度冒犯性」；三、誤導（false light），亦即行爲人明知或魯莽置其「所公開揭露事項係虛僞不實」而不顧，以「不實侵害個人形象」的加害方式，使被害人受到公眾錯誤之理解，該加害行爲具有「高度冒犯性」；四、盜用（appropriation），亦即對他人之姓名、肖像或照片等「具個人特徵（identifier）之隱私利益」，在「未得允許」之下供作自己使用或商業利用以獲取利益。Prosserr 教授認爲隱私權並非單一之概念可以涵括；這四種類型即實務上通常被作爲隱私權侵犯而提起侵權行爲訴訟之理由。[24] 其後，Prosserr 教授針對這四種隱私權侵害類型之看法，更成爲侵權行爲法第二次整編 Restatement (Second) of Torts 之內容，而成爲美國的實證法制。[25]

〈二〉傳統隱私權概念的檢討

（1） Samuel D. Warren 和 Louise D. Brandeis 雖未對隱私權權概念加以明確界定，但其將隱私的保護範圍包含「避免私生活領域之無故受侵擾」

[22] 張國清，前揭註 8 文，頁 7-8。
[23] 是否具有高度冒犯性，是由社會一般性之觀點認定，在此係依一般理性人之角度作判斷。相關論述，可參見：田育菁，前揭註 14 文，頁 19-20，23；周逸濱，行政機關個人資料保護法制之研究─以日本法爲比較中心，國立臺北大學法律學系一般生組碩士論文，頁 12（2008）。另外，對於前述判斷標準，我國學者有將之稱爲「社會習慣法則（mores test）」者。請參見：林建中，隱私權概念初探－從美國法之觀點切入，憲政時代，第 23 卷第 1 期，頁 58（1997.07）。
[24] 周逸濱，前揭註 23 文，頁 11。
[25] 田育菁，前揭註 14 文，頁 19-23。

與「個人對其自身事務公開揭露與否決定（第一次揭露）的權利」，並由二者共同構成「個人私生活的完整性」，透過精神層面與人格權作連結，使其具有「不受侵犯之人格（inviolate personality）」的特質，卻普遍爲人所接受。其實，在 Melvin v. Reid 一案後，隱私權爲美國憲法上所保障之基本權利的觀點，也漸被接受而形成共識。不過，Prosserr 教授與 Restatement (Second) of Torts 實證法制的內容，卻著重於對判斷隱私權侵害之要件與「事後請求救濟」之保障方式，似「無法於發生損害前請求排除危險」，在今日資訊時代之眼光來看，此一保障實仍不完全充足[26]。

（2） 隱私侵犯得透過事務性質涉及公共利益（下稱公益性排除事由）或言論具社會一般性（下稱一般性排除事由）之理由加以限制。[27] 自 Melvin v. Reid 一案後，針對隱私權侵害的一般性排除事由之「一般性」被限定於非營利性質，亦已形成相當之共識。因此，將「姓名、肖像或照片等具個人特徵（identifier）之隱私利益」被「盜用」，另行歸於一類是否有必要，其實不無疑慮，蓋其完全似乎可由「私人事務的公眾揭露」來涵括。另外，有學者提出「未得允許而使用他人姓名或肖像以營利的『盜用』」與「公開之事務使原告形象扭曲（不論好壞）的『誤導』」兩種類別並無區別之實益存在，蓋其認爲兩者侵害之客體均是個人人格，不同的僅是侵害之方式而已。[28] 因此，亦有 Prosserr 教授所提出的後兩種分類根本不必要的意見存在。

（3） 自 Samuel D. Warren 和 Louise D. Brandeis 提出隱私權一文以來，「藉由『保障個人私生活的完整性概念』與『不實侵害個人形象』的名譽

[26] 田育菁，前揭註 14 文，頁 20。
[27] 或應提醒的是，此時，由於科技尚未如今日之發達與普及，故有關來自公益性排除事由的侵害尚非明顯，因此，討論著重的多是一般性排除事由。
[28] 係 Edward J. Bloustein 對 Prosser 隱私侵權四種類型提出的批判之一，可參見：田育菁，前揭註 14 文，頁 24。

權加以區分」已逐漸形成共識，但 Prosserr 教授所提出的「誤導」卻使得二者界線又趨於模糊；其中，行爲人「明知或魯莽」的描述，以使人對惡意是否爲隱私侵犯的責任成立要件，亦不由令人產生質疑。

（4） 隱私權與個人人格具有不可分離之關係，其目的在保護個人「不受侵犯之人格」，並不具財產權之性質。然而，對姓名、肖像或照片等個人特徵（identifier）的侵權行爲，雖可能同時侵犯「與人格密不可分的隱私權」，與「透過社會活動的參與（主要應是工作或營業），使其個人之姓名、肖像或照片成爲具備經濟價值的財產權」，但 Prosserr 教授將對姓名、肖像或照片的侵害直接歸於隱私權侵犯的描述方式，實有造成隱私權具有財產性質的誤會的風險[29]；其在此所強調的「供作自己使用或商業利用以獲取利益」之獲利（營利）期許，透過對實務在 Melvin v. Reid 一案之針對「一般性」的反面解釋來看，二者之立場其實是一致的，但 Prosserr 教授在此針對營利的強調描述，卻恐有過於「商業化」而貶抑了背後所隱含之人格或人性尊嚴之嫌[30]。

（5） 關於隱私的公開，權利人僅具一次性的利益，其實是自 Samuel D. Warren 和 Louise D. Brandeis 提出隱私權以來，傳統見解的共識。然則，若考量資訊流出的「不可回復性」及其後的科技發展與普及所帶來的影響[31]，則此種保護見解顯有保護不足之虞。因此，縱使在是採隱私權之核心思想爲「人格之不可侵犯性」的想法下，學者亦有認爲，應「源自於對人格尊嚴之尊重」，而肯認「個人對其資料之揭露不僅須了解，且得充分參與個人資料使用之每個階段」。[32] 此外，亦有學者提

[29] 同上註。
[30] 周逸濱，前揭註 23 文，頁 13。
[31] 有關科技發展與普及如何帶來隱私危機，可參閱：劉靜怡，雲端運算趨勢與個人資訊隱私保護，全國律師，第 14 卷第 2 期，頁 39-44。
[32] 此爲美國喬治華盛頓（George Washington）大學法學院 Solove 教授所主張。*See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy,* 53 STAN. L. REV. 1393, 1461-62 ，惟 Solove 教授在文中更強調當事人對於資訊流程的參與，必須

出，爲解決前述對於隱私公開之保障的問題，宜對「已公開而爲第三人持有之資訊」採取類似人格權保障之方式（A moral right-like approach），使當事人可以突破契約關係，對抗契約關係以外之第三人。[33]

（6） 傳統見解中，對「『自願性』成爲『公眾人物』之人，對於其『參與公眾事務之部份』可認爲放棄隱私權之主張」的想法，一直沒有被其後之實務發展所完全推翻，但爲因應人權保障的發展，美國法院實務上基於 1953 年 Gill v. Hearst Pub. Co.一案所開展的「在公共場合也沒有隱私可言；唯有在私人處所之行爲才有可能被認爲是隱私」的想法，已被揚棄。蓋公共場合並非沒有隱私，只是在社會一般性的衡量下，通常其隱私之期待可能較低而已。[34]

5. 小結

經由上面的討論，我們可以發現，美國法上隱私權的保障應包含「避免私生活領域之無故受侵擾」與「個人對其自身事務公開揭露與否決定（第一次揭露）的權利」，並由二者共同構成「個人私生活（隱私）的完整性」的想法並未被動搖。傳統隱私權概念最大的缺失，是在「個人對其自身事務公開揭露上的保護不足」，此亦何以其後學說和實務的開展皆環繞於「資訊隱私權」爲中心的緣由；有認爲 Prosser 將隱私侵權行爲類型及法制化阻礙該行爲之發展，無法適應現今社會中產生之問題，認爲 Prosser 至少必須承擔隱私權侵權行爲法無法適時的發揮作用的某些責任，且唯有超越 Prosser 所提的隱私權概念才得以使得隱私權侵權行爲適應時代變遷產生之問題[35]。

是「有意義的」（meaningful participation）始可。又，類似此等「個人有權控制個人資訊的使用與流向」的主張，亦頗多見於國內學者的論述，參 劉靜怡，前揭著 3 文，頁 42。

[33] Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1145 .

[34] 關於公共場所中的隱私權保障，特別是關於國家公權力機器所爲的資訊蒐集的合憲性問題，請參閱 蔡達智，開放空間中的隱私權保障，月旦法學雜誌第 145 期，頁 127-146（2007.06）。

[35] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1889-91 (2010) .

由於「資訊隱私權」仍係以前述傳統隱私權概念爲基礎而開展，其「與個人人格具有不可分離之關係，其目的在保護「不受侵犯之人格（inviolate personality）」，不具財產權之性質以及隱私侵犯得透過事務性質涉及公共利益（下稱公益性排除事由）或言論具社會一般性（下稱一般性排除事由）之理由加以限制」等特質仍將被保留下來。然而，也正因爲係以「保持個人人格之完整性」作爲「資訊隱私權」之正當性基礎，因而，傳統隱私概念中與資訊相關的自身事務皆被「資訊隱私權」的保護範圍所涵括，因此，今日我們談論隱私權時，當我們提到的是「生活領域」時，所強調的是往往是「有形的支配空間」之「不受侵擾」的防衛面向；當提及的是「資訊隱私」時，則是更積極地意指「個人人格發展」之「由內至外的全程參與控制」。

此外，「資訊隱私權」既係爲「保持個人人格之完整性」而存在，其與個人人格具有不可分離之關係，不具財產權之特性，自然不變。基此，「資訊隱私權」乃具備人格權特質之不可拋棄、不能轉讓的一身專屬性。[36] 然則，這並不意味著，資訊隱私權保護範圍內的生活利益，不會因爲社會生活的進行而產生財產價值，並進而得作爲財產權；應強調的是，縱使資訊隱私權保護範圍內的生活利益得爲財產權，但其亦僅在該當財產價值產生原因之範圍內，得作爲財產處分之客體，且仍不得因此破壞個人受保障之「個人人格之完整性」，亦即仍應考量是否存有「合理之隱私期待」（reasonable expectation of privacy）[37] 來作價值衡量。[38]

是否存在「合理的隱私期待」之判斷，分爲兩個要件，首先，必須是當事人自己主觀上要有隱私的期待，意即當事人對於某一事項係屬個人隱私必須要有自

[36] Andrew L. Shapiro 著，劉靜怡譯，控制權革命－新興科技對我們的最大衝擊，頁 251（2001）。該文中略謂：「正因爲我們不容許個人出賣選票與身體器官，或者將自己賣爲奴隸，或許我們也不應該允許個人出賣隱私。」

[37] 「合理的隱私期待」概念係源自於美國聯邦最高法院 Harlen 大法官的一份協同意見，Katz v. United States, 389 U.S. 347, 359-61 (1967) (Harlan, J., concurring). 有關美國司法實務上對「合理隱私期待」詮釋的現狀介紹，可參閱：劉靜怡，雲端運算趨勢與個人資訊隱私保護，全國律師，第 14 卷第 2 期，頁 44-50（2010.02）。

[38] 有關資訊隱私權得否作爲財產權之客體的相關討論，可參閱：王郁琦，前揭註 10 文，頁 283-305。

我的認知；第二，前述當事人主觀上的期待，從客觀面的社會通念判斷，可認爲屬於合理者。符合上述兩項要件，即可承認該事項屬於隱私的範疇，縱使處於公共的場合，仍受隱私權之保障。而從我國司法院大法官釋字第 689 號解釋所揭示的：「個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者。」文字觀之，可認爲「合理隱私期待」此一概念已被我國釋憲實務所接受。

合理的隱私期待概念的提出，擴充了隱私權的機能，使得隱私權的保障範圍，跨出了其原初所設定的「家宅」的範疇而進入了公共領域，惟不可諱言，如此一來，國家在公共空間的行政管制措施的合法性，也因爲必須納入隱私權的思考而顯得更爲複雜，例如國家在公共場所設置監視器的問題，即爲一例。[39] 就此，本研究計畫將特別在後述實務研究的部分以專節探討。

〈三〉資訊隱私權（Information Privacy）

1. 概說

承繼前述關於隱私權與資訊隱私權的討論，有關「資訊隱私權」的具體內涵，可析述如下：

（1）「資訊隱私權之本質」爲人格權之保障，與個人人格具有不可分離之關係，具備人格權特質之不可拋棄、不能轉讓的一身專屬性，其目的應指向「個人人格完整性之保障」，而不限於「不受侵犯之人格」面向上的防禦。由是，資訊隱私權本身並非財產權之客體，但不應

[39] *See e.g.*, DANIEL J. SOLOVE, NOTHING TO HIDE——THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 174-82 (2011).

因此認爲「資訊隱私權保護範圍內的生活利益」不得財產化，而具財產權之性質。

（2） 爲達成「個人人格完整性之保障」的目的，「資訊隱私權之保護範圍」應及於「由內至外的全程參與控制」；只要「會造成對個人人格之自由發展之影響」的個人資訊，由內在的決定保護，到外部化的全程參與控制，都在保護範圍之內。由是，傳統隱私權概念中的「避免私生活領域之無故受侵擾」似乎將被限縮在「有形的支配空間」：小至個人的身體，大至個人生活空間；然應注意的是，縱使在公共空間內，個人仍有形成私領域的可能，例如，在旅館租用的個人房間，使用中的封閉式公共廁所。但亦有認爲應將「與個人人格發展有關」而「尚未形成資訊」的「個人決定權」，應由資訊隱私之保護範圍抽離之見解存在。

（3） 由於隱私權並非美國憲法下明文承認之基本權利，儘管早在 1931 年加州最高法院便藉由 Melvin v. Reid 一案承認隱私權在美國憲法上的合法地位，但其並未具體指稱「隱私權之實證基礎」之所在，此問題並因而延續到「資訊隱私權的實證基礎」之上。由於，美國是判例法國家，是故，此問題之答案主要便只能求諸於實務的累積與形成。

2. 資訊隱私權的實證基礎：

美國最高法院對於隱私權之實證基礎最著名的判決先例，便是 1965 年 Griswold v. Connecticut[40]一案由 Douglas 大法官主筆所提出的「半影理論（penumbra）」。

[40] 381 U.S. 479 (1965).

Douglas 大法官認爲，在美國憲法的實踐上，本即非僅有憲法明文者始得被視爲憲法位階的權利而受保障，因此，透過聯邦憲法增補條款第 14 條之正當程序條款（Due Process Clause），以及憲法增補條款第 1 條、第 3 條、第 4 條、第 5 條及第 9 條所保護的權利，放射所形成的「半影」，即可爲隱私權的憲法基礎；例如，憲法增修條文第 1 條言論自由的「半影」可認爲包括教育方式的選擇權。以此方法可推知，憲法增補條款第 3 條禁止軍人在和平時期未經所有人同意住宿民房乃（住家）隱私的另一種表現，憲法憲法增補條款第 4 條明白肯認人民免於身體、住家、文件及財產受不合理之搜索和扣押，憲法增補條款第 5 條之「自證己罪條款（Self-Incrimination Clause）」使人民得創造「隱私地帶（zone of privacy）」對抗政府的強迫認罪，憲法增補條款第 9 條補遺權的規定：「特定權利經憲法明文列舉者不應解釋爲否認或抑制人民保有其他權利」。上述憲法權利章典（Bill of Rights）的條文所放射形成之「半影」，其所共同保護之利益，即爲隱私，甚且隱私可被認爲係先於權利章典而存在之人民基本權利。[41]

而後隨著美國司法實務對於隱私權保護領域的擴大詮釋，讓隱私與個人自治（personal autonomy）的概念連結地更加緊密；[42] 在此同時，個人基於自主尊嚴（dignity）與認同（identity）的維護，隱私權的保障應賦予人民擁有控制自我資訊的法律實力（即資訊隱私）的想法，亦日益爲學界與實務所接受，是以，資訊隱私的憲法實證基礎，可上溯自 Griswald 一案的「半影」的憲法論理，自無疑義。

3. 資訊隱私權的保護範圍

（1）人的保護範圍

[41] *Id.* at 485-86.

[42] 承認婦女有限度的墮胎自由的劃時代判決 Roe v. Wade (410 U.S. 113 (1973)) 中，主筆的 Blackmun 大法官將婦女墮胎的決定，也納入隱私權的保障中，即爲最有名的事例。當然，反對此等擴張解釋路徑者也不在少數，相關整理，*See* LOUIS FISHER & NEAL DEVINS, POLITICAL DYNAMICS OF CONSTITUTIONAL LAW 182-91（2001）.

關於資訊隱私權人的保護範圍的爭議，主要出現法人是否得爲權利主體上。其中，近年來最著名的案例，莫過於美國聯邦通訊傳播委員會（Federal Communication Commission）與電信業者 AT＆T，就其市場競爭者產業聯盟 ComTel 依政府資訊公開法（Freedom of Information Act）申請提供其協助調查所取得之相關文件與通信內容，AT＆T 得否基於個人隱私（personal privacy）權利之保護，主張適用政府資訊公開法之例外規定所發生的爭議。[43]

美國聯邦通訊傳播委員會認爲法人並非隱私權保護之主體，而不採 AT＆T 之主張。但聯邦第三巡迴上訴法院（the Count of Appeals for the Third Count）認爲政府資訊公開法中，雖未界定何謂個人的（personal）隱私，但卻明確的人（person）界定爲「個人、合夥、公司、協會和政府機關以外的公司組織」，從而認定 personal 一詞，應包涵公司法人在內，因此判決 AT＆T 勝訴。案經美國聯邦通訊傳播委員會上訴到聯邦最高法院後，本案主筆的首席大法官 John Roberts 在判決中，直接指陳公司法人（corporations）不得適用政府資訊公開法中有關個人隱私豁免的規定。新任大法官 Elena Kagan 對本案嗣後曾表明其贊同 John Roberts 意見的看法，氏認爲：美國實務 30 多年來針對個人隱私的詮釋，多將其限制在「個人（individuals）」而不及於其他；再者，若採聯邦第三巡迴上訴法院之見解，則不只公司法人得爲個人隱私之主張，很可能導致連州政府、地方政府甚至外國政府，都得主張之不合理結果。

由是，現今美國針對個人隱私之保護應不及於法人。此亦合乎傳統隱私權係一種精神層面的權利，與人格保障緊密連結的論述。

（2）事務領域上的保護範圍：

[43] 以下關於本案的概略介紹，係整理自 劉靜怡，誰應該受到資訊隱私權的保護？，台灣法學雜誌，第 175 期，頁 103-108（2011.05）。

美國實務承認個人有「使用避孕器材之權利（use of contraceptive）」、「墮胎權（abortion right）」、「同性戀性行爲（homosexual behavior）」、「資訊隱私（informational privacy）」、「（尚有爭議之」死亡權（right to die）」[44]，乃至於個人對「婚姻生活內容、生活計畫、個性偏好、外觀表現、職業選擇與教育內容」[45]等事務的決定，都在隱私權保護範圍的射程之內。

若以本文針對美國法上「資訊隱私權」之目的係爲保障「個人人格之完整性」，而將其保護範圍及於與人格形成有關之「由內至外的全程參與控制」來看，前述案例未嘗不可認定爲將涉及資訊隱私權的保護範疇。

貳、 德國法上的「資訊自決權」（Informationelle Selbstbestimmung）」

〈一〉「資訊自決權」的提出

作爲歐陸法系代表的德國，在基本權保障上，主要係採區分不同生活領域，以成文法之方式來建構其基本權圖譜，以求形成一個無漏洞的基本權保障。

然而，在面對 1983 年所制定的人口普查法，並以此法作爲全國性人口資料普查之依據而引發的憲法訴願中，德國聯邦憲法法院卻不得不針對個人資訊創設一個新的基本權概念，以填補可能產生的保護漏洞。蓋戶口普查所涉及的個人資料可能觸碰之領域理論區分下的個人生活領域甚多，而依照不同保護領域下的基本權保障去處理，未必能有效而全面的針對個人資料加以保障，且亦欠缺一個具一致性的操作基準。由是，德國聯邦憲法法院乃嘗試建構「資訊自決權的概念，

[44] 王俊文，前揭註 11 文，頁 205-215。
[45] 張國清，前揭註 8 文，頁 15。

來單獨處理有關個人資訊的問題，並作爲個人資料保護之憲法依據。學說上亦有稱之爲「資訊自主決定權」、「資訊自我決定權」、「資訊自決定權」者[46]。

1. 人口普查判決的內容簡介[47]：

〈1〉憲法秩序之核心，爲人之尊嚴與價值，其保障之範疇應包含使個人能在自由的社會中自主做決定。而此乃透過基本法第 2 條第 1 項（一般人格權）結合第 1 條第 1 項（人性尊嚴）所保障之一般人格權來加以確保。基於這種自主決定之思想，個人有權得以原則上自主決定，何時以及在何種限度內，公開個人的生活狀態。

〈2〉在今日與未來自動化資料處理條件下，此項權利需特別加以保護。特別是今日個人資料之處理不再如同以往必須求助於人力整理的資料卡或卷宗，而毋寧只要藉助自動化資料處理，於技術上將可毫無限制地加以儲存，且隨時不論距離之遠近可在秒速下加以提取個人資訊。

〈3〉更進一步地，透過完整之資料庫系統及彼此間的連結可能性，將導致個人無法知悉何人在何時及何種機會中知悉其何事，此乃違背其人格之自由發展，使其成爲單純之資訊客體（Informationsobjekt），且會對其形成心理壓力，影響其公共事務之參與，與憲法所保障之人性尊嚴不相符合。

〈4〉在現代資料處理（Datenverarbeitung）之條件下，應保護每個人之個人資料（persönliche Daten），免遭無限制之蒐集、儲存、運用、傳遞，此係屬基本法第 2 條第 1 項及基本法第 1 條第 1 項保護範圍。該基本人權保障每個人，原則上有權自行決定其個人資料之交付與使用。且個人資訊自決權之限制，僅得於有關重大公眾利益時（überwiegende Allgemeininteresse），方得爲之。

---

[46] 程明修，基本權各論基礎講座（3） ——資訊自決權：遺傳基因訊息，法學講座，第 19 期，頁 2（2003.07）。

[47] 周逸濱，前揭註 23 文，頁 26-27。該判決之中文譯本，請參見：蕭文生，關於「1983 年人口普查法」之判決，收錄於司法院編，西德聯邦憲法法院裁判選輯(一)，司法周刊雜誌社，頁 288 以下（1995）。

〈二〉德國法上「資訊自決權」與美國法上「資訊隱私權」之比較

在前述理解之下的「資訊自決權」，乃是相較於其他領域基本權與作爲「更具一般性的自我決定權（Selbstentscheidungsbefugnis）」的一種特殊型態；該特殊性在於，其保護範圍及於「所有」個人相關資訊，而突破了領域理論區分個人生活領域作出不同程度之保障的操作模式，同時將自我決定之對象指向個人相關資訊，而從一般人格權中獨立出來；其雖係由一般人格權所推導而出，但個人資訊對個人人格具有何種意義，並非其關切之點。[48]

基此而論，「資訊自決權」作爲基本權的保障，實際上是一種行爲自由的保障，其關注的重點，並非是「全程參與式的控制」，而是在其自主控制可能遭受侵害時（不論是在被蒐集、處理或利用之任何階段），保障其有權自行決定是否將其個人資料交付與提供利用的處分權。故而，其與美國法上的「資訊隱私權」在個案中的處理結果縱有可能相同，但兩者仍存在內在結構上的重大差異；因爲美國法上的「資訊隱私權」著重於個人人格的內在關聯，因此，個人外在行爲自由未受限制並不代表資訊隱私權即受保護，相對而言，蒐集有形塑人格形象作用之個人資訊涉及資訊隱私權之保護，但若所涉資料無礙個人人格發展，則不受資訊隱私權之保護，但其仍爲資訊自決權之保障客體，爲免侵害受資訊自決保障之當事人的自決權，其蒐集行爲仍應得其授權。這便是學者 Ronald Dworkin 之所以認爲，「資訊自決權是種授權式之自由（liberty as license）屬於個人外在行爲自由之表現，而資訊隱私權則是人格獨立性之自由（liberty as independence）」的原因。[49]

[48] 邱文聰，從資訊自覺與資訊隱私的概念區分─評「電腦處理個人資料保護法修正草案」的結構性問題，月旦法學雜誌，第 168 期，頁 174（2009.05）。

[49] 此爲學者邱文聰的評釋，本文亦從之。參 邱文聰，同上註文，頁 176。

第三節　隱私權概念在我國的繼受與個人資料保護法規範目的的探求

壹、　學說開展

〈一〉隱私權之實證基礎

由於並無憲法之明文規定，我國學者對隱私權之憲法依據缺乏一致性之見解，就此，有認隱私權之憲法依據係憲法第 22 條者[50]，有認除憲法第 22 條之外，亦不排除憲法第 10 條（居住自由）或第 15 條（財產權）者[51]，有認除憲法第 22 條之外，還可能有其他選擇，憲法第 12 條（秘密通訊自由）即是其一者[52]，有採美國法上之「半影（penumbra）理論」，由憲法第 10 條（居住自由）、第 11 條（表達自由）、第 12 條（秘密通訊自由）、第 13 條（信仰自由）、第 14 條（集會結社自由）、第 15 條（生存權）及第 22 條（概括規定）來建構我國隱私權之憲法依據者[53]。惟不論採何者，都避免不了藉助憲法第二十二條作爲承認此一新興基本權的（主要）橋樑，應無疑義。[54]

〈二〉隱私權的保護範圍

國內學者有從最原始的「獨處權」意涵出發，將隱私權保護範圍限定於「個人事務與身體的不受侵擾」者[55]；有參考美國法上之「隱私權」概念，將隱私權定義爲「對個人領域事務的控制權」，並將個人領域定性爲「涉己的（非涉他的）」且「私人的（非公共的）」者[56]；有參酌美國法上之「隱私權」與「資訊隱私權」

---

[50] 李惠宗，憲法要義，頁 325-343（2002 年）；許志雄（合著），現代憲法論，頁 238（2002 年）。

[51] 吳庚，憲法的解釋與適用，頁 305（2003）。

[52] 此係蘇永欽教授課堂上所表示之意見，引自：王俊文，前揭註 11 文，頁 223（註 96）。

[53] 詹文凱，前揭註 15 文，頁 44。

[54] 以憲法二十二條作爲規範基礎，承擔的風險就是（根據部分學者的主張），在面臨基本權衝突的衡量時，會較列舉基本權爲弱勢。關於憲法二十二條的規範功能，參 李震山，論資訊自決權，收於「現代國家與憲法——李鴻禧教授六秩華誕祝壽論文集」，頁 742（1997）。

[55] 林世宗，隱私權，全國律師，第 5 卷第 4 期，頁 35（2001.04）。

[56] 詹文凱，前揭註 15 文，頁 137-152。

概念，將隱私分爲廣義與狹義，前者指「對個人私密空間的自我掌握」，後者爲「資訊保密權」者[57]；有將隱私定義爲「隱私權是一種保障個人對於其個人資訊的控制、滿足個人的獨立自主、提昇個人自我表現及形成社會關係之能力的權利」者[58]；有將隱私權之保障等同德國法上之「資訊自決權」者[59]；有由社會學之觀點切入，將隱私定義爲「對自我向他人封閉或開放程度之狀態的控制權」者[60]；亦有直接放棄正面定義者[61]。

貳、 實務見解

自釋字第 603 號解釋後，釋憲實務已將憲法第 22 條當作是隱私權之實證基礎，並將其保護範圍界定爲「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」，若純就此一保護範圍之界定而言，其與美國法上之隱私權概念之描述極爲類似，似乎應以「人格權」作爲其權利本質。然而事實上，我國基本權的體系基本上係採德國之保護模式，而在此一基礎上，並不必然會導出前述保護範圍之界定，必然會產生係採美國法上見解的結論。蓋縱使在德國對「個人資料之自主控制」採「資訊自主權」之看法下，針對隱私權保護範圍的界定，亦非不得採釋字第 603 號解釋之看法。由是，關於「隱私權」乃至「解釋文中之隱私資訊權」的權利本質爲何，在學說上並非沒有討論之空間。

參、 小結

---

[57] 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，國立臺灣大學法律研究所碩士論文，頁 61（1999）。

[58] 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語法的規制，當代公法新論（中），頁 703（2002）。

[59] 林明昕，資訊公開 VS. 秘密保護─論「政府資訊公開法」之建立─，法政學報，第 16 期，頁 37（2003）。

[60] 陳仲嶙，隱私權概念的理解與填充，台灣憲法之縱剖橫切，頁 642-649（2002）。

[61] 王俊文，前揭註 11 文，頁 195。

基於前述隱私議題文化相對論之立場，本文認爲，縱使我國在隱私權概念係爲繼受國之一方，亦非不得發展屬於我國之隱私權概念，只要此之發展不會違背體系正義之要求，則在法釋義學上當有循此開展之空間。

基此，本文針對作爲個人資料保護法理基礎的隱私權，乃有以下之看法：

〈一〉隱私權之保護範圍：

由於作爲我國之有權解釋機關的司法院大法官，針對隱私權的保護範圍已於解釋文部分表明，故此，應予尊重。爰參酌釋字第 603 號解釋將其界定爲「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』」。

〈二〉隱私權之實證基礎：

1. 大法官之論理

〈1〉 維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。

〈2〉 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。

〈3〉 本文之補充

依照前述釋字第 603 號解釋對隱私權保護範圍之描述，憲法第 10 條（居住自由）和第 12 條（秘密通訊自由）亦應著落在隱私權保護範圍之內，因此，考量我國基本權之保護體系係採德國領域理論而建構，縱使肯認憲法第 22 條係隱私權之實證基礎，但不妨將之看作是「特殊基本權（指已明文劃出生活領域做爲其保護範圍之基本權）之補充規定」；即當所涉及的生活領域之隱私利益已受特殊基本權之保障時，則毋須援

引憲法第 22 條作爲隱私權保障的憲法依據，僅須逕依特殊基本權之規定處理即可；只有在找不到特殊基本權時，方有援引憲法第 22 條作爲隱私權保障的憲法依據之必要。

〈三〉個資法立法目的再釐清：兼涵「資訊隱私權」與「資訊自決權」之保障

本文以爲，有鑑於「資訊隱私權」與「資訊自決權」的內涵各有不同的旨趣，前者注重資訊與個人內在人格形成的關連；後者則可與人格抽離觀察，著重於外在行爲的自主決定，儘管在實踐上兩者有大量的重疊之處，但畢竟一方的內涵仍有他方所不及之處，基於「有疑義時應爲有利於人民自由之推定」的解釋法則，應將個人資料保護法的規範目的，解爲同時追求人民「資訊隱私」與「資訊自決」的保障。此等立場，並可從下列規範基礎獲得支持：

1. 大法官在釋字第 603 號解釋解釋文中，明白使用「個人自主控制個人資料之『資訊隱私權』」一詞，加上大法官將資訊隱私的保障求諸於「基於人性尊嚴與個人主體性之維護及人格發展之完整」，可認爲大法官已揭櫫——與人格發展息息相關的——「資訊隱私權」乃我國實證法秩序所保障。然進一步觀之，大法官對於「資訊隱私權」的闡釋：「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。」其用語明顯傾向德國式的「資訊自決權」的論述模式，是以在我國實證法秩序下，「資訊隱私」與「資訊自決」保障的交錯，並非不可想像之事。

2. 再者，就釋字第 603 號解釋所提出之資訊隱私權乃在「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。」來看，其所揭示的保障內容，不僅限於消極在受侵害或受侵害可能時的防衛性權利，亦包含了積極的「持續控制的權利」的特質。

3. 個人資料保護法中，設有許多以當事人的「告知同意」作爲蒐集處理與利用個人資料的限制性允許條件之規定，[62] 可被視爲係體現「資訊自決權」的設計。

4. 個人資料保護法第 1 條[63]，明白宣示本法之制定目的在避免「人格權」受侵害，由此可知，立法者係有意採取美國法上「資訊隱私權」的看法。再由個人資料保護法第 3 條[64]對於當事人對於個人資料之權利不得預先拋棄或以特約限制之規定，亦可窺知立法者企圖建構的是一個讓當事人「全程參與控制」的個人資料保護法制。最後，個人資料保護法第 51 條[65]第 1 項的兩款排除事由，明顯是美國法上針對隱私的一般性排除事由的明文化，而此種排除之考量並未見於資訊自決權中。

〈四〉規範目的的辨明實益

---

[62] 例如個人資料保護法第 15 條第 2 款（公務機關對個人資料之蒐集與處理，應經當事人書面同意）、第 16 條第 7 款（經當事人書面同意公務機關即可作原特定目的以外的運用）。針對非公務機關的個資處理，第 19 條第 1 項第 5 款、第 20 條第 1 項第 6 款也皆有類似的規定。

[63] 個人資料保護法第 1 條：「爲規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」

[64] 個人資料保護法第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」

[65] 個人資料保護法第 51 條：「有下列情形之一者，不適用本法規定：一、自然人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。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料（第 1 項）。公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐、處理或利用者，亦適用本法（第 2 項）。」

之所以不憚辭費，闡明個人資料保護法的規範目的，可能包含資訊自決與資訊隱私的保護此兩個不同的面向，在於此一規範目的的釐清，或有助於部分個資法適用上疑難的澄清。例如：

1. 有助於規範適用進一步的類型化

例如，透過規範目的與體系的考察，未來實務上或可將個人資料分爲以下兩類予以觀察：

（1）單純資訊自決權之保護：

與人格可抽離的資料，例如：監理站保有的車主車輛是否接受定檢的資料），解釋上即不存在資訊隱私之問題。對此類資訊，在個人資料保護法的適用上，可認爲：

A. 個人的同意可作爲機關處理利用個人資料，絕對的免責事由（個資法第 15 條第 2 項可完全適用）

B. 基於權利的相對化，即便在無個人同意的情況下，亦可透過公益與行政目的的利益衡量正當化個人資料的處理與利用。（個資法第 15 條第 1、3 項可完全適用）

（2）同時涉及資訊自決權與資訊隱私權保護之資料：

該個人資料的存在本身即意含著人格權的彰顯，此類資訊又可根據與人格權實現的重要性高低，分爲：① 高度關連：即所謂「敏感性資料」（個資法第六條參照）；② 一般關連：非敏感性的、可識別的個人資訊，例如個人的學經歷、財務資力、日常生活型態等資料。針對此類資訊，在個人資料保護法的適用上，可認爲：

A. 僅僅獲得個人的同意，不得當然成爲蒐集與處理個人資料的正當化事由（所以應對個資法第 15 條第 2 項作目的性限縮，不可逕自完全適用），而必須進一步有執行職務必要，在合乎行政目的的範圍內始得蒐集使用之。

B. 承上，非敏感性的個人資料，其蒐集、處理與利用，應該要以公益

與行政目的作爲主要的正當化根據，獲得個人同意僅僅意味著行政目的這一面衡量的份量可以強化而已（蓋據此可推定當事人認同機關蒐集處理資訊乃爲執行職務所必要的主張）。

C. 敏感性的資料，解釋上需受到最高程度的保護，此時的個人自主決定與人格權的實現聯結緊密，因此一定要以獲得當事人的同意，作爲容許機關蒐集、處理與利用的法律必要條件「之一」；此外，並須符合其他列舉的公益要件（個資法第 6 條第 1 項但書各款參照）始得爲之。且主管機關與法院，對於各該要件，必須從嚴解釋。

2. 澄清「資訊隱私權」的內涵，有助於確認本法所要保障的法律主體，係「自然人」而非「法人」。

個資法的保障主體，從資訊隱私權的觀點，基於資訊隱私權與人格的不可分離之特質，可認爲應僅限於「現生存之自然人」[66]，故實務常見之問題：主管機關於網站公告違法業者名稱，是否有違行政罰法與個人資料保護法？ 循此理路，即不生違反個資法之問題。

3. 個人資訊自決權的觀點強化「對當事人告知」的意義

一旦確立個人資訊自決是個資法保障的基礎內涵，那麼行政機關的告知，便成爲人民能否妥善行使資訊自決權的重要關鍵。在個人資料保護法通過後，學者間屢有批評現行法設有諸多以「當事人同意」作爲蒐集、處理個人資料的許可條件的的規定，但卻又多將其列爲「擇一」而非「必要」條件的規範模式，吾人若從資訊自決權的角度，自得批判此等規範模式架空了個資法對於個人外部行爲（即處分資訊）自由的本旨。

[66] 關於「現生存之自然人」的結論，相同見解，請參見：劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外─以監視錄影爲例（上），月旦法學教室，第 115 期，頁 43-45（2012.05）。

[67] 此外，對於個資法中免除行政機關告知義務的規定，亦有從嚴檢視之必要。[68]

[67] 類似批判，參 劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月但法學雜誌第 183 期，頁 152（2010.08）。

[68] 例如個資法第 8 條第 2 項第 2 款前段將「行政機關執行法定職務之必要」列爲豁免告知的事由，應屬明顯的立法錯誤，各行政機關應透過限縮解釋排除該款規定的適用。（並參本研究計畫第四章機關訪談的分析報告）

第三章　我國個人資料保護法之規範內容

二次大戰後，個人資訊隱私權漸獲重視，惟發展緩慢，一些國際組織（如經濟合作暨開發組織、歐洲理事會、歐洲聯盟、亞太經合會）陸續通過個人資料保護規範，意圖影響會員國法制的建立及走向。事實上，全球各國際組織或國家對於資訊隱私的態度大相逕庭，可分爲三種類型：（一）全方位或全面適用式(comprehensive)的個人資料保護法制（如歐盟會員國、澳洲、加拿大、日本、2010年4月27日「個人資料保護法」修正案生效後的台灣）；（二）僅適用於少數特定產業的部門式(sectoral)個人資料保護法制（如美國、2010年4月27日「個人資料保護法」修正案生效前的台灣）；（三）完全欠缺個人資料保護法制（如中國大陸、印尼及菲律賓）[1]。現估計，全球超過六十個國家[2]擁有某種形式的個人資料保護法律。

由於我國個人資料保護法制深受國際發展趨勢的影響，因此，爲提供我國關於個人資料保護立法之借鏡，本章第一部分將針對目前美國、歐盟以及亞太經合會的相關規範內容爲基本介紹，第二部分則爲我國個人資料保護法主要規範內容之探討。

第一節　主要國際組織及美國的個人資料保護規範

壹、經濟合作暨開發組織

經濟合作暨發展組織(The Organization for Economic Cooperation and

[1] See Jody R. Westby, American Bar Association, International Guide to Privacy 6 (2004).關於個人資料保護法規的世界地圖（A map of Data Protection Laws Around the World），http://www.guardianedge.com/resources/data-protection.php (last visited July 25, 2012)。翁清坤，論個人資料保護標準之全球化，頁 11-12，東吳法律學報，2010 年 7 月。

[2] Karin Retzer, Cynthia Rich, Morrison & Foerster LLP, GLOBAL SOLUTION FOR CROSS-BORDER DATA TRANSFERS: MAKING THE CASE FOR CORPORATE PRIVACY RULES, 38 Geo. J. Int'l L. 449 (Spring, 2007).

Development, OECD)堪稱個人資料保護領域的先驅，對於全球相關法律架構的發展頗有助益[3]。OECD於1980年通過「有關隱私權保護及個人資料跨國流通之準則」(The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)[4]揭櫫關於個人資料保護的八大原則:（一）限制蒐集原則(Collection Limitation Principle)，即個人資料的蒐集應合法、公正、並取得當事人同意或通知當事人；（二）資料品質原則(Data Quality Principle)，即個人資料於特定目的之利用範圍內，應力求正確、完整及更新之狀態；（三）目的明確化原則(Purpose Specification Principle)，即個人資料於蒐集時，目的應明確化，其後之利用亦不得牴觸最初蒐集之目的，目的變更者亦應加以明確化；（四）利用限制原則(Use Limitation Principle)，即個人資料不得爲特定目的以外的利用；（五）安全防護原則(Security Safeguards principle)，即個人資料爲防止遺失、未經授權的接近、毀損、利用、變更或揭露之風險，應採取合理之安全保護措施；（六）公開原則(Openness Principle)，即個人資料的蒐集、處理及相關政策的制定，應對一般人公開之。（七）個人參與原則(Individual Participation Principle)，即個人資料當事人對於他人持有自己的資料，得行使一定程序的控制；（八）責任原則(Accountability Principle)，即個人資料管理人(controller)應負遵守上開原則之責任[5]。

貳、歐洲理事會

歐洲理事會或歐洲委員會(The Council of Europe, CoE)於1981年制定「有關個人資料自動化處理保護個人公約」(the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)，其內容與OECD

[3] Jody R. Westby, American Bar Association, International Guide to Privacy 82 (2004).

[4] Available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited August 31, 2012).

[5]許文義，「個人資料保護法論」，頁 40，台北，三民書局，2001 年 1 月；Jody R. Westby, American Bar Association, International Guide to Privacy 82 (2004); Available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited August 31, 2012).

「有關隱私權保護及個人資料跨國流通之準則」雷同，並於1999、2001年加以修訂。該公約要求，個人資料的蒐集及處理應合法、公正、並符合原始目的；個人資料持有人應更新資料並維持其正確性，當蒐集目的消失時，應刪除相關個人資料；應採取適當的安全措施，以防止個人資料遺失、未經授權的接觸、毀損、利用、變更或揭露之風險；個人資料當事人對於他人持有自己的資料，亦得進行一定的控制。

參、歐洲聯盟

爲保護會員國國民的隱私基本人權及促進會員國間個人資料的自由流通，歐洲聯盟於1995年制定「資料保護指令」，並於1998年10月生效。與前揭UN、OECD、CoE及後述APEC等國際組織規範不同者，歐盟資料保護指令對於會員國具有強制拘束力。然而，如同歐盟一般指令，資料保護指令並不具「自動執行」(self-executing)效果，不能直接適用於會員國人民，仍賴會員國按指令所要求的最低標準制定內國個人資料保護法規，但各國立法並非完全一致，仍容許因地制宜（如各國關於行政程序與違反效果的規定不盡然相同）的存在[6]。歐盟資料保護指令全方位地適用於自然人、法人及政府部門對於個人資料的蒐集、利用或分享等行爲[7]，以期解決個人資料流通所衍生的弊端。

如同其他隱私規範，歐盟資料保護指令的主要內容由國際間廣泛接受隱私保護的重要原則所構成[8]，茲簡述如下：

（一）通知(Notice)原則：應向個人資料所指涉的當事人提供以下之通知(1)資料蒐集者之身分；(2)蒐集資料之目的；(3)關於資料之蒐集或揭露，如何行使可能之選擇；(4)個人資料將傳遞至何處與何人；以及(5)如何接近其所被蒐集之個人

[6] Jody R. Westby, American Bar Association, International Guide to Privacy 89-91 (2004).

[7] EU Data Protection Directive, arts. 2 and 4, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited August 5, 2012).

[8] Jody R. Westby, American Bar Association, International Guide to Privacy 91-92 (2004); Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation 63-108 (2007).

資料[9]。

（二）同意(consent)原則：處理個人資料前，應先取得當事人的「明確同意」(unambiguous consent) [10]；另當個人資料供直接行銷之用時，應賦予當事人選擇退出(opt-out)權[11]。

（三）一致性(consistence)原則：資料蒐集者對於個人資料的利用應符合(i)曾提供予當事人通知內容；及(ii)當事人已擇定之內容[12]。

（四）接近(access)原則：資料蒐集者應提供當事人得接近其個人資料並允許當事人得加以更正[13]。

（五）安全(security)原則：資料蒐集者應採取足夠措施，以確保個人資料的完整與秘密[14]。

（六）進一步傳遞(onward transfer)原則：倘將個人資料進一步傳遞予第三人，該第三人應以契約方式同意受下列的拘束(i)曾提供予當事人通知內容；(ii)當事人曾擇定之內容；及(iii)相關法令[15]。

（七）執行(enforcement)原則：當事人得對違法的資料蒐集者求償；會員國並應設置「資料保護主管機關」(the Data Protection Authority)調查、監督或介入個人資料之相關案件[16]。

肆、亞太經合會

亞太經合會於2004年11月制定亞太經合會隱私綱領(The APEC Privacy Framework)，揭櫫個人資料蒐集、利用、處理及分享的九大原則，雖對於會員經濟體(Member Economies)並無強制拘束力，但可協助會員經濟體制定足以衡平隱私保護與個人資料跨國流通的隱私法規。事實上，這九大原則乃參考全球許

[9] EU Data Protection Directive, art.10.
[10] EU Data Protection Directive, art.7.
[11] EU Data Protection Directive, art.14.
[12] EU Data Protection Directive, art.6.
[13] EU Data Protection Directive, art.12.
[14] EU Data Protection Directive, art.17.
[15] EU Data Protection Directive, art. 6, 7, 17, and 26.
[16] EU Data Protection Directive, art.29.

多隱私相關法律體制（如OECD「有關隱私權保護及個人資料跨國流通之準則」）發展而來，茲簡述如下：

（一）預防損害(Preventing Harm)：個人資料保護制度的設計應用以防止個人資料遭濫用而受到損害，倘個人資料之蒐集、利用與傳遞有損害發生時，應有適當的損害補償機制[17]。

（二）通知(Notice)：個人資料管理者應向當事人通知(i)個人資料已遭蒐集的事實聲明；(ii)蒐集個人資料之目的；(iii)向何人揭露個人資料；(iv)個人資料管理者的身份及所在；(v)當事人得接近、更正其個人資料與限制利用、揭露其個人資料的選擇和方法[18]。

（三）蒐集限制(Collection Limitation)：個人資料之蒐集應限於與蒐集目的相關者，依合法與公平方法爲之，於適當時應通知當事人或取得同意[19]。

（四）個人資料之利用(Uses of Personal information)：個人資料之利用僅限於與蒐集目的相符合者，但有下列情形之一者，不在此限：(i)取得當事人同意者；(ii)爲提供當事人所要求之產品或服務所必要者；或(iii) 經法律授權者[20]。

（五）選擇(Choice)：個人資料管理者於適當時，應提供當事人得就其個人資料之蒐集、利用和揭露行使選擇的機制。所蒐集者爲可公開取得之個人資料，則不在此限[21]。

（六）個人資料完整性(Integrity of Personal Information)：爲符合利用目的所需，個人資料應維持正確、完整並加以更新[22]。

---

17 APEC Privacy Framework, para. 14, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

18 APEC Privacy Framework, para. 15, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

19 APEC Privacy Framework, para. 18, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

20 APEC Privacy Framework, para. 19, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

21 APEC Privacy Framework, para. 20, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

（七）安全維護(Security Safeguards): 個人資料管理者應妥善地維護個人資料，防止未經授權接近、毀損、利用、修改或揭露個人資料[23]。

（八）接近與更正(Access and Correction)：當事人應被賦予得合理接近（查詢）被持有個人資料的機會並加以更正、補充、修正或刪除[24]。

（九）責任(Accountability)：個人資料管理人應負遵守上開原則之責任。個人資料傳遞至國內或國外第三人時，個人資料管理者應取得當事人個人的同意、或應善盡注意義務並藉由適當措施以確保資料接收者將以符合上開原則方式保護個人資料[25]。本項「責任」原則可爲個人資料跨國流通的規範基礎[26]。

伍、美國

相較於歐盟或我國2010年4月27日新修正的「個人資料保護法」採用「政府管制」爲主、「市場機制」爲輔的全方位或全面適用式(comprehensive)個人資料保護模式，美國則採「市場機制」爲主、「政府管制」爲輔的部門式(sectoral)個人資料保護模式。美國模式係將個人資料的蒐集、使用或分享問題，委由當事人個人與資料蒐集者雙方自行透過自由市場的機制協商，政府並不積極介入管制，必要時才輔以產業界自訂的自律規範。然而，在某些特定的產業，濫用消費者個人資料的問題嚴重，形成隱私權保護的危機，政府乃特別制定僅適用該特定「部門」的法令，以求市場失靈之解決。在所謂「部門式」的立法中，

---

[22] APEC Privacy Framework, para. 21, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

[23] APEC Privacy Framework, para. 22, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

[24] APEC Privacy Framework, para. 26, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

[25] APEC Privacy Framework, para. 26, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited August 14, 2012).

[26] Martin Abrahms, Eighth Annual Institute on Privacy and Security Law: Pathways to Compliance in a Global Regulatory Maze (2007--THE YEAR ON STEROIDS), 903 PLI/Pat 385, 395 (June-July, 2007).

對於個人資料的蒐集、利用及分享，美國政府部門因「1974年隱私法」而受到面向較廣的拘束，但私人部門則欠缺如「歐盟資料保護指令」的全方位式保護個人資料的規範[27]。自1970年代起，美國國會陸續通過不少僅適用於特定產業部門的隱私法律，如公平信用報告法(Fair Credit Reporting Act)、家庭教育權利及隱私法(Family Educational Rights and Privacy Act)、金融隱私權法(Right to Financial Privacy Act)、隱私保護法(Privacy Protection Act)、有線通信政策法(Cable Communications Policy Act)、影帶隱私保護法(Video Privacy Protection Act)、電話消費者保護法(Telephone Consumer Protection Act)、駕駛人隱私保護法(Driver's Privacy Protection Act)、健康保險可攜性與責任法(Health Insurance Portability and Accountability Act)、兒童線上隱私保護法(Children's Online Privacy Protection Act, COPPA)、金融服務現代化法案(Gramm-Leach-Bliley Act, GLBA)、未經邀請而主動推介色情與市場銷售之侵犯管制法(Controlling the Assault of Non-Solicited Pornography and Marketing Act, Can-Spam Act)、銀行秘密法(Bank Secrecy Act)、美國愛國法(The USA-Patriot Act)等[28]，對於個人資料之蒐集、使用或分享加以規範。

第二節　我國的個人資料保護規範

在台灣，相對於散落各產業領域的隱私相關法規（如金融控股公司法第四十二條第一項[29]、銀行法第四十八條第二項[30]、電信法第六條[31]及稅捐稽徵法第

[27] Jody R. Westby, American Bar Association, International Guide to Privacy ×× (2004).

[28] 周慧蓮，資訊隱私保護爭議之國際化，月旦法學雜誌，104期，頁115，2004年1月； Daniel J. Solove and Marc Rotenberg, Information Privacy Law 23-24 (2003); and Jody R. Westby, American Bar Association, International Guide to Privacy 15-63 (2004).

[29] 按金融控股公司法第四十二條第一項：「金融控股公司及其子公司對於客戶個人資料、往來交易資料及其他相關資料，除其他法律或主管機關另有規定者外，應保守秘密。」

[30] 按銀行法第四十八條第二項：「銀行對於客戶之存款、放款或匯款等有關資料，除有下列情形之一者外，應保守秘密：一、法律另有規定。二、對同一客戶逾期債權已轉銷呆帳者，累計轉銷呆帳金額超過新臺幣五千萬元，或貸放後半年內發生逾期累計轉銷呆帳金額達新臺幣三千萬元以上，其轉銷呆帳資料。三、依第一百二十五條之二、第一百二十五條之三或第一百二十

三十三條[32]），1995年制定的「電腦處理個人資料保護法」無疑係適用範圍最廣者，涵蓋公務及非公務機關對於個人資料的蒐集、處理或利用行爲。

惟電腦處理個人資料保護法所適用的客體，限於經電腦處理[33]的個人資料；且適用的主體於非公務機關部分，亦侷限於法律及主管機關[34]所規定的十餘種特定行業部門，故亦被歸類爲「部門式」立法[35]，而形成個人資料保護規範上的重大漏洞。由於該漏洞，造成該十餘種特定行業以外的各式各樣的非公務機關（或自然人）或非以電腦方式從事個人資料的蒐集、使用與分享，除非觸犯其他法律（如民法、刑法）外，完全不受電腦處理個人資料保護法之拘束，形同自由放任的個人資料交易市場，濫用情形乃屢見不鮮。有鑑於此，不乏要求制定更嚴格、「全方位」適用的個人資料保護規範之呼籲，乃有電腦處理個人資料保護

七條之一規定，經檢察官提起公訴之案件，與其有關之逾期放款或催收款資料。四、其他經主管機關規定之情形。」

[31] 按電信法第六條：「電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。電信事業應採適當並必要之措施，以保障其處理通信之秘密。」

[32] 按稅捐稽徵法第三十三條規定：「稅捐稽徵人員對於納稅義務人之財產、所得、營業及納稅等資料，除對下列人員及機關外，應絕對保守秘密，違者應予處分；觸犯刑法者，並應移送法院論罪：一、納稅義務人本人或其繼承人。二、納稅義務人授權代理人或辯護人。三、稅捐稽徵機關。四、監察機關。五、受理有關稅務訴願、訴訟機關。六、依法從事調查稅務案件之機關。七、經財政部核定之機關與人員。八、債權人已取得民事確定判決或其他執行名義者。」

[33]按「電腦處理個人資料保護法」第三條第一項第三款規定：「電腦處理：指使用電腦或自動化機器爲資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理。」

[34]按「電腦處理個人資料保護法」第 3 條第 7 款之非公務機關，除法律明文規定之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、保險業及大眾傳播業外，另按法務部之公告包括「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。」可參見網路資料庫 http://www.moj.gov.tw/public/Attachment/8826847477.doc，2009 年 8 月 15 日。

[35] Karin Retzer, Cynthia Rich, Morrison & Foerster LLP, GLOBAL SOLUTION FOR CROSS-BORDER DATA TRANSFERS: MAKING THE CASE FOR CORPORATE PRIVACY RULES, 38 Geo. J. Int'l L. 449, 456 (Spring, 2007).

法「修正草案」[36]之問世，歷經數年的周折，立法院終於2010年4月27日完成三讀修法，將「電腦處理個人資料保護法」名稱修正爲「個人資料保護法」，並將保護客體予以擴大，不再以經電腦處理之個人資料爲限[37]，且刪除非公務機關行業別之限制，使得任何自然人、法人或其他團體蒐集、處理或利用個人資料，皆受拘束38，以填補法律漏洞，符合國際隱私保護標準。

然而，新修正之個人資料保護法，因某些條文內容之可行性引起諸多爭議，面臨受規範產業界的反彈，因此，行政院遲至2012年9月21日才發布除第六、五十四條條文外，其餘條文定自2012年10月1日施行，並立即提出第六條、第四十一條、第四十五條、第五十四條之修正草案，在我國立法史上，實屬罕見。

觀察新修正之個人資料保護法，其修正重點包括：一、擴大保護客體：不再以經電腦處理的個人資料爲限，更擴及於人工處理者或其他非實體個人資料，特別加強對醫療、基因等高敏感性特種個人資料之保護。二、適用主體之全面化：將原適用電腦處理個人資料保護法之非公務機關僅限定於法律及主管機關所規定的十餘種特定行業部門之規範廢除，全面性擴及公務機關以外之自然人、法人及其他團體。三、義務之增訂：新法中增訂對公務機關或非公務機關蒐集個人資料時，應告知當事人之義務；間接蒐集時告知資料來源義務；個人資料被竊取、洩漏等事件發生時之通知義務；及非公務機關利用個資行銷時當事人得選擇退出(opt-out，意即當事人得於自己資料被蒐集、處理或利用後，要求停止再利用之權利)之制度。四、提高罰則及加強中央目的事業主管機關或直轄市或縣、市政府爲檢查等處分之權責，加強行政監督。五、增訂團體訴訟制度與訴訟專屬管轄制度。[39]

由於「個人資料保護法」（原名「電腦處理個人資料保護法」）的制定，

[36]電腦處理個人資料保護法修正草案總說明及條文對照表（行政院），可參見網路資料庫 http://www.acp.moj.gov.tw/public/Attachment/62228524321.pdf，2009 年 10 月 5 日。

[37] 個人資料保護法第一條、第二條第一項第二款及第四款。

[38] 個人資料保護法第二條第八款。

[39] 范姜真媺。〈個人資料自主權之保護與個人資料之合理利用〉，《法學叢刊》，57 卷 1 期， 2012 年 1 月，頁 71。

深受OECD「有關隱私權保護及個人資料跨國流通之準則」影響，故首先亦從其所揭櫫八大原則[40]來探討個人資料保護法之主要內容，然後，再探討其他重要內容：

壹、蒐集限制原則(Collection Limitation Principle)：

意指個人資料的蒐集應合法、公正、並取得當事人同意。

一、「同意」之要求—應經當事人同意而蒐集、處理或利用個人資料之情形：

按我國新修正的個人資料保護法第15條1項2款規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：二、經當事人書面同意。」第16條1項7款規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用： 七、經當事人書面同意。」第19條1項5款規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：五、經當事人書面同意。」第20條1項6款規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：六、經當事人書面同意。」可知，資料蒐集者(不論公務機關或非公務機關)對於個人資料的蒐集、處理或利用，除有其他法定原因外，應經當事人書面同意。

如上揭，按我國個人資料保護法第15、16、19及20條規定，除有其他法定理由外，個人資料的蒐集、處理或利用應經當事人書面同意。惟同意之構成要件應爲何？我國個人資料保護法並未進一步闡述，惟仍可參考國外立法例。按歐盟資料保護指令第2(h)條規定:「當事人的同意係任何出於自由意志、目的特定及基於告知後所表示之期望，藉以指出其同意個人資料被處理。」又按歐盟

[40] Jody R. Westby, American Bar Association, International Guide to Privacy 84-85 (2004).

資料保護指令第7(a)條規定，欲處理個人資料者，應經當事人毫不含糊、明確地同意。對此，按歐盟資料保護指令第29條所成立的工作小組指出，同意必須符合下列四項標準才會在法律上生效：（一）同意必須清楚且明確地指出其意願；（二）同意必須出於自由意志；（三）同意目的必須特定；（四）同意必須基於告知後所為。再者，同意是否應以書面為之，各國有不同規定，惟我國則明文要求應以書面為之。此外，欲使同意有效，則必須經告知才可，而所提供之隱私權政策通知應清楚及明確地指出何種個人資料將被蒐集、如何被利用、與誰分享，且不得有欺罔、誤導或錯誤之情事，否則，同意將會無效。

事實上，「告知後同意」(informed consent)乃個人資料蒐集、利用或分享的前提要件，蓋因資訊社會，包括個人資料在內的各種資訊乃決策所不可或缺，資料蒐集者或資料使用者無疑地將有強烈動機蒐集個人資料。惟針對是否同意個人資料被蒐集、利用或分享，當事人與資料蒐集者之間存在「資訊不對稱」或「知識落差」而造成市場失靈。按實證經驗，資料蒐集者有強烈動機使用煙幕戰術(smokescreen tactics)，故意不提供清楚的資訊。實際上，資訊不對稱未必阻礙當事人與資料蒐集者之間關於個人資料之交易。相反地，資訊不對稱之存在，反而使得個人資料之交易更加容易。由於當事人並不完全了解所屬個人資料將如何被利用，因而低估個人資料遭濫用之可能性，使得其不明就裡，便輕易授權資料蒐集者得利用或揭露其個人資料予第三人。據此，當個人不知何種資料被蒐集、如何被利用或分享、與因此將造成何種傷害時，當事人將輕忽保持個人資料的私密性是何等的重要，極易導致同意謬誤（consent fallacy）或同意陷阱（consent trap）之現象[41]。因此，關於個人資料的蒐集、利用或分享，亦應有「告知後同意」原則之適用，當事人的決策或同意權的行使應以「被告知」與「自願的」為前提，否則，個人資料的交易實無自由選擇的空間。告知後同意之首要，即在於使資料蒐集者蒐集、利用或分享個人資料之實際狀況得以「透

[41] Edward J. Jange & Paul M. Schwartz, Modern Studies in Privacy Law: Notice, Autonomy and Enforcement of Data Privacy Legislation: The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules, 86 Minn. L. Rev.1219, 1231 (June, 2002).

明化」，以利當事人同意權之行使。而「告知後同意」原則主要包含「揭露」及「同意」二個面向爲主，資料蒐集者應以合理努力而指出爲何蒐集個人資料，使得當事人得以了解其個人資料將如何被蒐集、利用或分享；而同意應以當事人對於其與資料蒐集者間之意思表示一致有所瞭解爲前提。

對於隱私權政策的通知義務，我國個人資料保護法之舊法（即「電腦處理個人資料保護法」）並未明文要求，惟新修正的個人資料保護法第8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。」[42]或1個人資料保護法第9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蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。有下列情形之一者，得免爲前項之告知：一、有前條第二項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人爲告知。四、基於公共利益爲統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者爲限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。第一項之告知，得於首次對當事人爲利用時併同爲之。」

[42]個人資料保護法第 8 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。」

可知，我國新修正的個人資料保護法即明文規定，不論是直接或間接蒐集資料，除符合得免告知情形者外，公務機關或非公務機關均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項，以利當事人爲「告知後同意」。

另按新修正的個人資料保護法第7條規定：「第十五條第二款及第十九條第五款所稱書面同意，指當事人經蒐集者告知本法所定應告知事項後，所爲允許之書面意思表示。第十六條第七款、第二十條第一項第六款所稱書面同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所爲之書面意思表示。」可知，立法者有意藉由所謂「告知後同意」或「告知後選擇」之原則，進一步落實對個人資料所指涉當事人之保護。

二、「同意」適用之排除—得不經當事人同意而蒐集、處理或利用個人資料之情形：

如前揭，各國際組織或國家制定法律（如個人資料保護法），要求資料蒐集者（如「產業」）蒐集、處理、利用或分享個人資料必須經過當事人同意。換言之，「同意」之要求即將是否同意個人資料被蒐集、處理、利用或分享之控制及決定權交到消費者個人之手。個人資料及資訊隱私的保護，對於現代社會高品質生活的追求，實屬不可或缺。

由於資訊隱私權將對於社會某些權利或利益造成限制，而有利益權衡之必要，故對於資訊隱私權的保障應非絕對的。如同我國司法院大法官第六○三號解釋：「惟憲法對資訊隱私權之保障並非絕對，國家得於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。」再者，「同意」雖是資訊隱私權及個人資料保護的重要基石，但其適用範圍亦並非絕對的，縱有些國家賦予「同意」特殊的地位，惟「取得當事人的同意」亦僅是得合法蒐集、

利用或分享個人資料的理由之一[43]。因此，針對蒐集、利用或分享個人資料之同意的取得，各個國家或國際組織的法制均有除外之規定。歐盟資料保護指令第7條[44]規定，有下情形之一者，縱未經當事人同意，仍得處理個人資料：（一）與當事人有契約，爲履行契約所必須者，或締約前根據當事人要求而採取的措施者；（二）資料控制者爲遵守法律義務所必須者；（三）爲保護當事人重大利益所必須者；（四）爲實踐公共利益或執行賦予資料控制者或接收個人資料的第三人之公權力所必須者；或（五）爲資料控制者或接收個人資料的第三人追求正當利益之目的所必須者，但當事人的基本權利及自由顯有更值得保護之重大利益者，則不在此限。

類似地，我國亦有「同意」適用範圍的除外規定，按新修正的個人資料保護法規定，有下列情形之一者，縱未經當事人書面同意，仍得蒐集、處理或利用個人資料，例如，按第15條第一項第一、三款規定:「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。三、對當事人權益無侵害。」第16條第一項第一至六款規定:「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露

[43] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent (WP187, 13 July 2011) 7, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (last visited July 31, 2012).

[44] 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, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited July 3, 2012).

方式無從識別特定之當事人。六、有利於當事人權益。」第19條第一項第一、二、三、四、六、七款規定:「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益爲統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」第20條第1項第一至五款規定:規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：一、法律明文規定。二、爲增進公共利益。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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。」綜上可知，無論係公務機關或非公務機關的資料蒐集者除非有上開情事者外[45]，仍應經當事人同意，才可蒐集、處理或利用個人資料。

惟「同意」的機制在公、私部門所扮演的角色顯不同，當事人（消費者）的同意在私部門規範體制係居於核心地位，賦予當事人較大空間協商個人資料的保護，但公部門規範體制較少依賴當事人（公民）同意的取得，而較多依賴立法機關賦予公務機關得不經當事人同意而仍蒐集、處理或利用個人資料之例外性強制規定46。例如，個人資料保護法第16條第一項第一款規定，法律明文

[45] 學者認爲，由於將「經當事人同意」僅列爲公務或非公務機關得合法蒐集、處理或利用個人資料的條件之一，因此，此種立法方式已實質架空個人資訊自主之最高精神。孫迺翊，社會給付請求權、當事人協力義務與隱私權保護，收錄於司法院大法官一百年度學術研討會「憲法解釋與隱私權之保障」(下冊)，頁93，2011年12月；劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，第183期，頁147-164，2010年8月。

[46] Ian Kerr, Carole Lucock & Valerie Steeves, Lessons from the Identity Trail—Anonymity, Privacy and Identity in a Networked Society 42 (2009).

規定時，公務機關對個人資料，得爲特定目的外之利用。而稅捐稽徵法第 33 條第1項即明文規定：「稅捐稽徵人員對於納稅義務人之財產、所得、營業及納稅等資料，除對下列人員及機關外，應絕對保守秘密，違者應予處分；觸犯刑法者，並應移送法院論罪：一、納稅義務人本人或其繼承人。二、納稅義務人授權代理人或辯護人。三、稅捐稽徵機關。四、監察機關。五、受理有關稅務訴願、訴訟機關。六、依法從事調查稅務案件之機關。七、經財政部核定之機關與人員。八、債權人已取得民事確定判決或其他執行名義者。」因此，倘有上開例外情形之一者，稅務資料毋庸取得當事人（納稅義務人）之同意，亦得提供他人爲特定目的外之利用。

貳、資料品質原則（Data Quality Principle）

爲確保個人資料的正確性，明定在個人資料作業程序上應適時更正或補充之，以期達成個人資料檔案內容之正確。[47]因此，個人資料保護法第十一條乃規定：「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。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。違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。因可歸責於公務機關或非公務機關之事由，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。」

事實上，不正確之個人資料將對當事人權益有嚴重影響，而個人資料因未更正或補充致使不正確時，如係可歸責於該蒐集機關之事由，自應課以該蒐集機關於更正或補充個人資料後，通知曾提供利用該資料之對象，以使該不正確

[47] 許文義，「個人資料保護法論」，頁 181，台北，三民書局，2001 年 1 月。

之資料能即時更新，避免當事人權益受損。[48]

參、目的明確原則(Purpose Specification Principle)：

綜合個人資料保護法第十五及十九條規定的規範意旨，可得知個人資料蒐集或處理之特定目的應加以明確化。

按個人資料保護法第十五規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人書面同意。三、對當事人權益無侵害。」又按個人資料保護法十九條第一項規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。五、經當事人書面同意。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」再者，按個人資料保護法第五十三規定：「本法所定特定目的及個人資料類別，由法務部會同中央目的事業主管機關指定之。」[49]可知，個人資料蒐集或處理之特定目的應加以明確化，且符合主管機關

[48]個人資料保護法第十一條之修正說明。

[49]有關電腦處理個人資料保護法第19條第1 項「目的事業主管機關」、同條第3 項之「中央目的事業主管機關」各係何單位疑義乙案，法務部認為，本法第19 條第1 項所稱「目的事業主管機關」，原則上係指管理本法第3 條第7 款所稱「非公務機關」之各級目的事業主管機關。惟根據本法第19 條第3 項規定：「前二項之登記程序、許可要件及收費標準，由中央目的事業主管機關定之」，準此，有關本法所稱之目的事業主管機關為何，尚須視該非公務機關目的事業所由成立之專業法規之管轄權規定而定。例如：私立學校法第4 條規定：「本法所稱主管教育行政機關：私立高級中等以上學校為教育部；其他私立學校，為所在地之直轄市政府或縣（市）政府。但私立高級中等學校，在直轄市為直轄市政府。」故「私立學校及學術研究機構電腦處理個人資料管理辦法」第3 條規定：「本辦法主管機關如下：一、國民中小學：直轄市政府教育局或縣（市）政府。二、高級中等學校：教

所指定之特定目的範圍內。

按歐盟資料保護指令第29條所成立的工作小組公佈的「同意定義之意見」中指出，同意必須特定，方能有效。換言之，未能指出處理之確切目的之「空白同意」(blanket consent)係不足以爲合法授權之基礎。資料控制者或資料蒐集者處理個人資料所依賴的同意愈空泛，則愈會被質疑同意之存在或有效性。[50]因此，爲了使同意符合特定的要件，同意必須清楚及精確地指出係針對特定個人資料處理的範圍及後續應用而爲之，而同意不得針對不設限、開放性(open-ended)的個人資料處理活動而爲之。其實，同意必須針對明確指出個人資料處理的不同面向(aspects)而爲之，其中，包括爲了何種目的而處理何種個人資料，而關於同意內涵的詮釋必須根據個人資料所指涉當事人及資料蒐集者雙方的合理期待(reasonable expectations)而爲之。因此，同意的特定化本質上即與同意必須係被告知的(informed)相通的。同意不得根據資料控制者單方處理個人資料的需求而輕率地解釋爲涵蓋各種目的，相反地，同意所針對的個人資料的處理應與達成特定目的具有合理及必需性關聯者爲限。此外，倘符合當事人的合理期待時，資料蒐集者雖爲供不同營運，仍可僅取得當事人一次的同意。倘資料控制者爲不同目的而處理個人資料或移轉個人資料予第三人時，則必須另外再取得當事人的同意。事實上，取得當事人同意的需要性，必須根據目的及資料接收對象之身分而就不同個案(case-by-case)加以判斷。例如，個人資料的處理乃爲履行

育部或直轄市政府教育局。三、專科以上學校及學術研究機構：教育部。」又電信法第3 條規定：「電信事業之主管機關爲交通部（第1 項）。交通部爲監督、輔導電信事業並辦理電信監理，設電信總局；其組織另以法律定之（第2 項）。」，故「電信業電腦處理個人資料管理辦法」第3 條規定：「凡於中華民國境內從事電信業，而爲個人資料之蒐集、電腦處理或國際傳遞及利用，應依本辦法向交通部電信總局辦理登記並取得執照。」。三、 目前金融監督管理委員會係金融業、証券業、保險業的中央目的事業主管機關；行政院衛生署係醫院的中央目的事業主管機關；教育部係學校的中央目的事業主管機關；交通部係電信業的中央目的事業主管機關；行政院新聞局係大眾傳播業的中央目的事業主管機關；經濟部係徵信業的中央目的事業主管機關。參見法務部94 年3 月9 日法律決字第0940001159 號函。

[50] Catherine Baker, New Data Protection: Act!, Ent. L.R. 2000, 11(8), 193, 193 (2000).

契約關係所必需(如爲運送買受物而需取得買方之地址)，已經其他法律授權，則毋庸得到當事人同意，但倘個人資料的處理超出契約履行所需(如爲評估買方付款能力而從事信用調查)，則應另外取得特定的同意。[51]

再者，按加拿大個人資料保護暨電子文件法(Personal Information Protection and Electronic Documents Act, PIPEDA52)第5(3)條之規定，資料蒐集者得正當地蒐集、利用或揭露個人資料之目的，應限於一個理性(reasonable)之人在同樣情況下認爲係適當(appropriate)之目的[53]。又按加拿大亞伯特省「個人資料保護法」(Personal Information Protection Act)[54]第7(2)條規定，資料蒐集者不得要求當事人同意蒐集、利用或揭露逾越產品或服務的提供所必要的個人資料而做爲提供產品或服務的前提。此外，我國個人資料保護法第5條亦有類似限制：「個人資料之蒐集、處理或利用，……，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。」易言之，同意之客體範圍之解釋亦必須考慮當事人個人的合理期待(the reasonable expectations of the individuals)。例如，於訂購雜誌時，當事人將合理期待雜誌社（即資料蒐集者）除爲了寄送雜誌及收費而使用其姓名及地址外，也會爲了招攬當事人續訂該雜誌而使用其個人資料。因此，對於雜誌社而言，其可以假設當事人之雜誌訂購行爲將構成其同意雜誌社得利用其個人資料而爲續訂之招攬行爲[55]。相反地，倘缺乏當事人之同意，則雜誌社不得將訂戶個人資料提供予保險公司，以供招攬保險之用，否則，將有違當事

---

[51] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent (WP187, 13 July 2011) 17-18, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (last visited July 25, 2012).

[52] Available at http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf (last visited August 31, 2012).

[53] Ian Kerr, Carole Lucock & Valerie Steeves, Lessons from the Identity Trail—Anonymity, Privacy and Identity in a Networked Society 35 (2009).

[54] Available at http://www.qp.alberta.ca/574.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779748938 (last visited July 3, 2012).

[55] Juliana M. Spaeth, Mark J. Plotkin & Sandra C. Sheets, The Impact of Canada's Personal Information Protection and Electronic Documents Act on Transnational Business, 4 Vand. J. Ent. L. & Prac. 28, 35 (Winter, 2002)

人之合理期待。此乃因將訂購雜誌所提供之個人資料轉爲保險公司招攬保險之用，已超出原始蒐集目的，應另取得當事人同意。可知，爲不同目的而利用或分享個人資料，應另外取得同意，否則，將被視爲違法，例如，Google告知Gmail用戶其個人資料僅供email目的使用，卻未事前取得當事人同意，即將其轉用於Google Buzz社群服務(social-networking service)之其他目的，而於2011年被美國聯邦貿易委員會認定爲欺罔消費者[56]。

同意必須特定，而爲了使同意符合特定的要件，同意必須清楚及精確地指出係針對特定個人資料處理的範圍及後續應用而爲之，而同意不得針對不設限、開放性的個人資料處理活動而爲之。

針對公務機關蒐集或處理個人資料之特定目的，在適用上的疑義，(電腦處理)個人資料保護法主管機關法務部曾爲諸多解釋，以下舉其要者，供相關公務機關法律適用之參考(新修正的個人資料保護法生效後，諸多修正前的法條與修正後的法條，縱使其遣詞用字稍有改變，但其主要內容與結構新舊法相去不遠，法務部於新法生效前所爲的解釋，仍應有參考的價值。)：

關於學校蒐集本校或他校畢業紀念冊，並利用畢業紀念冊內所載學生資料寄發升學資訊等疑義乙案，法務部認爲，按「電腦處理個人資料保護法」第18 條(參見新修正個人資料保護法第19條) 規定：「非公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得爲之：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3 條第7 款第2目有關之法規

[56] Shayndi Raice & Julia Angwin, Facebook 'Unfair' on Privacy, November 30, 2011, available at http://online.wsj.com/article/SB10001424052970203441704577068400622644374.html#ixzz1fAwiQlu7 (last visited July 30, 2012); FTC news, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network, available at http://www.ftc.gov/opa/2011/03/google.shtm (last visited July 30, 2012).

及其他法律有特別規定者。」學校蒐集或利用本校畢業紀念冊所載學生資料，如有法務部會同教育部所定之特定目的之一（例如代號079 學生資料管理）必要範圍內，且符合上開規定五種情形之一者，自非不得爲之。惟如屬他校畢業紀念冊之學生資料或用於寄發升學資訊者，則其特定目的係屬何種項目？不無待酌之處。又依電腦處理個人資料保護法施行細則第32 條第3 項規定：「本法第18 條第3 款所稱已公開之資料，指不特定之第三人得合法取得或知悉之個人資料。」係爲平衡個人權利的保護及促進資料的合理利用，並鑑於合法公開的資料原則上對隱私權的影響極微。至來函所載明個人資料之畢業紀念冊如僅發送或售予該校畢業生，是否該當以賡開之資料乙節，則屬事實認定，請參酌上開說明本於職權自行審酌。[57]

按電腦處理個人資料保護法第7 條(參見新修正個人資料保護法第15條)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。」又第8 條(參見新修正個人資料保護法第16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。…四、爲增進公共利益者。…」警政署爲辦理內政部警政署辦事細則第7 條第5款所定失蹤人口查尋之規劃、督導事項，蒐集有關失蹤人口之就醫時間、地點等個人資料並予利用，應屬本法第7 條第1 款及第8 條所定「於法令規定職掌必要範圍內者」，且符合「警政」之特定目的（本法特定目的項目代號090）。至中央健康保險局提供警政署失蹤人口上開資料，係屬該局對其蒐集之個人資料爲特定目的外之利用，其利用如能協助查尋失蹤人口且可免除當事人生命、身體、自由之急迫危險，應符合本法第8 條但書之規定。

[57] 法務部 94 年 2 月 23 日法律字第 0940003764 號函。

[58]

關於所詢設置全國不適用教師通報系統網路，供學校在網路查詢，防制具教育人員任用條例第31 條不得聘任之教師應聘，是否合於電腦處理個人資料保護法第7 條第1 款「在法令規定職掌必要範圍內」規定乙案，按本法第7 條規定：「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：1.於法令規定職掌必要範圍內者。2.經當事人書面同意者。3.對當事人權益無侵害之虞者。」第8 條本文規定：「公務機關對個人資料之利用，應於法令職掌必要範爲內爲之，並與蒐集之特定目的相符。」查「教育或訓練行政」，係屬蒐集或電腦處理個人資料之特定目的項目之一（代號053），另教育人員任用條例第31 條定有教育人員任用之消極資格，同條例第30 條復規定教師任用資格審查爲法定必經程序且教育部爲審查機關之一，故教育部基於教育人員任用條例主管機關立場，爲執行該條例相關規定，對於具有該條例第31 條所定教育人員任用消極資格之個人資料爲蒐集、電腦處理及提供相關學校、機關審查之用，應可認係符合上開本法第7 條第8 條規定。又本法第6 條、第17 條(參見新修正個人資料保護法第5、18條)規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」「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、竄取、毀損、滅失或洩漏。」故爲建置本件全國不適任教師通報系統網路，於從事個人資料之蒐集與利用時，宜請注意上開比例原則及資訊安全等規定，就相關技術性事項妥爲規劃。[59]

關於警察機關函請調解委員會提供受理調解事件中涉及傷害、毀損、恐、妨害自由等事件資料，應否提供乙案，法務部認爲， 警察機關函請提供之資料，

[58] 法務部97 年2 月12 日法律字第0970002314 號函。

[59] 法務部96 年10 月26 日法律字第0960035274 號函。

雖基於刑案數據資料需要，惟因涉及特定案件當事人之姓名、年籍、事件概略等，已屬電腦處理個人資料保護法第3 條第1 款(參見新修正個人資料保護法第2條第1 款)之「個人資料」，調解委員會對於上開資料之蒐集或電腦處理，依個資法第7 條規定須有特定目的，始得爲之。經查該特定目的應爲「電腦處理個人資料保護法之特定目的」中編號012「民政」項下之調解業務。又依同法第8 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，惟如符合同條但書所列九款情形之一者，得爲特定目的外之利用。本件調解委員會如將當事人資料提供給警察機關，與資料蒐集之特定目的（編號012「民政」項下之調解業務）有所不符。至於是否符合上開但書規定得爲特定目的外利用之情形，仍請本於權責衡酌之。[60]

關於親等關係資訊系統資料之利用疑義乙案，內政部規劃建置親等關係資訊系統，是否符合「戶政及戶口管理」之特定目的乙節，按電腦處理個人資料保護法第7 條規定：「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。…」戶政機關職司戶籍登記，包括結婚登記、收養登記，此類登記係屬行政處分，依行政程序法第36 條規定應職權調查，而結婚依民法第983 條，收養依民法第1073 條之1 均有親等限制，戶政機關基於職掌自得蒐集建置親等資料。故如基於戶政機關職掌必要範圍內建置該系統，與前揭個資法規定，似無不符。至於，內政部建置「親等關係資訊系統」之特定目的，係在於「戶政及戶口管理」，因此，戶政機關以外之其他機關對親等關係資料之利用，應屬特定目的外利用。又按檢察或司法警察機關依刑事訴訟法規定（第229 條、第230 條、第231 條）偵查犯罪，符合個資法第8條但書第1 款之「法令明文規定者」及第4 款「爲增進公共利益者」之情形，內政部應可援引上揭規定逕予提供。又關於辦理公法上金錢給付義務及相關強制執行作業部分：法務部行政執行署所屬各行政執行

[60]法務部95 年6 月28 日法律決字第0950022777 號函。

處爲辦理公法上金錢給付義務之強制執行，於執行事件進行中如須利用親等關係資料時，係本於實現國家債權之必要，應符合前揭條文但書第4 款「爲增進公共利益者」之情形，自得依該款規定提供之。[61]

關於法務部行政執行署所屬各行政執行處爲辦理公法上金錢給付義務之執行事件，有向中央健康保險局調閱義務人全民健康保險卡所附照片之必要，法務部認爲中央健保局提供義務人全民健康保險卡所附照片予法務部行政執行署所屬各行政執行處，應屬適法，其理由如下：（一） 按電腦處理個人資料保護法第7 條規定之：「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。」查行政執行法第4 條規定：「…但公法上金錢給付義務逾期不履行者，移送法務部行政執行署所屬行政執行處執行之。」行政執行處組織通則第3 條規定：「行政執行處掌理下列事項：一、關於公法上金錢給付義務之強制執行及其協調、聯繫事項。…」準此，法務部行政執行處爲執行上開法令規定之職掌，基於強制執行之特定目的，蒐集義務人全民健康保險卡所附之個人資料，應屬「法令規定職掌必要範圍內」，符合上揭個資料第7 條第1 款之規定。另個資法第8 條復規定：「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…四爲增進公共利益者。」各行政執行處請求提供義務人全民健康保險卡之個人資料，就中央健康保險局而言，乃屬特定目的外之利用，而各行政執行處爲依法辦理行政執行事件而請中央健康保險局提供資料，符合「增進公共利益」之規定，中央健康保險局自得依上開規定提供之。[62]

地政機關蒐集、電腦處理民眾之地籍相關資料，其特定目的應爲「土地行政」（本部85 年8 月7 日法八五令字第19745 號函頒之「電腦處理個人資料保

[61]法務部 97 年 7 月 9 日法律決字第 0970019933 號函。
[62] 法務部 93 年 7 月 15 日法律字第 0930028433 號函。

護法之特定目的」003 號參照）。準此，地政機關利用所蒐集之個人地籍資料（包括將資料提供給當事人以外之第三人），應符合「土地行政」之特定目的，始得爲之。至於各地農田水利會爲推動農田水利事業，需要搜集該會事業區域內受益土地之所有權人資料，對地政機關而言，係屬特定目的外之利用，應符合首揭法條但書規定所列九款情形之一者，始得提供。因此，地政機關得否將民眾之地籍資料提供給各地之農田水利會作特定目的外之利用，因屬事實認定問題，宜由持有該個人資料檔案之公務機關（即地政機關），本於權責審認之。另依同法第6 條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」是以，有關本件農田水利會及地政機關蒐集、利用民眾之地籍資料時，應遵照上開規定，不得逾越必要範圍，以保護民眾之權益。[63]

肆、使用限制原則（Use Limitation Principle）

即除非法令另有規定或當事人同意者外，個人資料之利用應符合蒐集之特定目的。按我國新修正的個人資料保護法第16條：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人書面同意。」及第20條第1項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：一、法律明文規定。二、爲增進公共

[63] 法務部94 年5 月10 日法律決字第0940017743 號函。

利益。三、為免除當事人之生命、身體、自由或財產上之危險。四、為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為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、經當事人書面同意。」可知，個人資料之利用應符合蒐集之特定目的，但倘有法定情形之一者，仍得為特定目的外之利用。

針對公務機關不經當事人同意而為特定目的外之利用之情形，在適用上的疑義，(電腦處理)個人資料保護法主管機關法務部曾為諸多解釋，以下舉其要者，供相關公務機關法律適用之參考：

一、交通部分

按電腦處理個人資料保護法第7 條(參見新修正個人資料保護法第15條第1項第1款)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，不得為之：一、於法令規定職掌必要範圍內者。…」第8 條(參見新修正個人資料保護法第16條第1項第1款)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。…」臺北縣政府為解決停車者長期將車輛停放於公有路外停車場之問題，建議交通部修正停車場法，增加該法主管機關得調閱（蒐集）車籍資料之法律依據，並使原車籍電資料保管機關得依前開規定，為原蒐集目的外之利用（提供），應符合本法上開規定。據此，主管機關得調閱車籍資訊，並利用該車籍資料，通知車輛所有人移置車輛，以維護路外停車場營運順暢及增進公眾停車之權益。[64]

關於警政署擬向交通部高速公路局取得電子收費系統（ETC）車行紀錄資料是否符合電腦處理個人資料保護法相關規定疑義案，法務部認為，按電腦處理個人資料保護法第7 條(參見新修正個人資料保護法第15條)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

[64] 法務部98 年12 月10 日法律決字第0980048995 號函。

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。」同法第8 條(參見新修正個人資料保護法第16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。…四、爲增進公共利益者。…」警政署爲依刑事訴訟法或其他法律規定調查或協助偵查犯罪而向交通部高速公路蒐集有關個人車行紀錄資料並予利用，應屬電腦處理個人資料保護法第7 條第1 款及第8 條所定之「法令規定職掌之必要範圍內」，並符合「刑事偵查」之特定目的。另就高公局而言，本件應屬對其蒐集之個人資料爲特定目的外之利用，又其利用係因警政署偵查犯罪之需而提供蒐集之個人車行紀錄資料，應符合電腦處理個人資料保護法第8條第4 款所定「爲增進公共利益」之情形。又依本法第6 條(參見新修正個人資料保護法第5條)規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」故警政署爲調查或協助偵查犯罪蒐集、利用車行紀錄資料及高公局利用上開資料時，並應符合本條規定。[65]

按電腦處理個人資料保護法第8 條規定：「公務機關對個人資料之利用，應於法令執掌必要範圍內爲之，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；…五、爲免除當事人之生命、身體、自由或財產上之急迫危險者。…八、有利於當事人權益者。…」本件中華汽車工業股份有限公司前出售之汽車，有事實足認有重大危害行車安全之虞，故應依法召回改正，而公路監理機關爲保障當事人權益及其生命、身體之急迫危險，故利用其蒐集之個人資料，代爲寄發中華汽車車主召回改正通知信函，係屬特定目的外之利用，其利用並符合上開條文但書第5 款及第8款所定情形。[66]

---

[65] 法務部96 年4 月10 日法律決字第0960700254 號函。

[66]法務部 95 年 1 月 5 日法律字第 0940046975 號函。

二、警政與司法部分

關於警察機關藉由戶役政資訊電子閘門系統查詢全面國民身分證所建立之相片影像檔，內政部意見認爲符合電腦處理個人資料保護法第7 條(參見新修正個人資料保護法第15條)規定，且內政部所蒐集國民身分證相片影像檔案提供警察機關利用，亦符合同法第8 條但書(參見新修正個人資料保護法第16條)規定特定目的外之利用等節，法務部敬表同意。[67]

有關地檢署使用臺中縣、市警局整合性查贓系統電腦資訊偵辦轄內竊盜及贓物案件，有無違反個人資料保護法疑義乙案，法務部認爲，按電腦處理個人資料保護法第7 條(參見新修正個人資料保護法第15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，不得爲之：1、於法令規定職掌必要範圍內者。…」另同法第8 條(參見新修正個人資料保護法第16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。…」查臺中縣、市警局，於法令規定刑事偵查職掌必要範圍內，基於「電腦處理個人資料保護法之特定目的及個人資料之類別」之014 代號「犯罪預防、刑事偵查、執行、矯正、保護處分或更生保護事務」特定目的，依本法第7 條及警察職權行使法第12 條規定，得蒐集或電腦處理由民間易銷贓場所業者自願性同意提供之個人資料整合性查贓系統。又臺中縣、市警局於上開法令職掌必要範圍內爲之，並與蒐集之特定目的相符，依本法第8 條及警察職權行使法第17 條規定，得利用該查贓系統，提供地檢署使用。又地檢署本於刑事偵查之特定目的，於法令職掌範間內使用查贓系統，蒐集、電腦處理並利用該系統之個人資料，應符令本法第7 條及第8 條規定。又有關其他行政機關向地檢署調取上間接合系統資訊，有無提供義務乙節，如其他行政機關之蒐集符合本法第7 條或有其他法律依據，由地檢署依個案情形審酌是否符合本法第8 條規定而提供之，當無疑義；惟地檢署有無提供義務，應視有無法律強制規範（例如：稅捐稽徵法第30 條第1 項或行政執行法第26 條準用強制執

[67]法務部 95 年 9 月 25 日法律字第 0950036704 號函。

行法第19 條第2 項規定）而定。末以本法第6 條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」及第17 條(參見新修正個人資料保護法第18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。」。[68]

檢察機關於法令規定檢察官職掌必要範圍內，基於「電腦處理個人資料保護法之特定目的及個人資料之類別」之014代號「犯罪預防、刑事偵查、執行、矯正、保護處分或更生保護事務」特定目的，依本法第7 條及法院組織法第60 條規定，得蒐集或電腦處理由司法警察機關函（移）送犯罪嫌疑人供述或調查所得而地檢署認有蒐集建置必要之相關個人資料。又地檢署於上開法令職掌必要範圍內，並與蒐集之特定目的相符，依本法第8 條本文規定，得利用上開蒐集建置之個人資料。至於對於上開個人資料之利用如屬特定目的外之利用，自應依本法第8 條但書規定由地檢署依個案情形審酌之。另本法第6 條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」及第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。」地檢署於蒐集、電腦處理或利用前開個人資料時，其執行程序應符合上開誠實信用及比例原則之規定，並請指定專人辦理個人資料安全維護事項（包括資料查詢等利用之稽核）[69]

公務機關對個人資料之利用，除於蒐集之特定目的必要範圍內之利用外，依本法第8 條但書規定，尚得爲「特定目的外」之利用，如有符合該條但書所定各款情形之一時，亦允許該個人資料蒐集機關得爲特定目的外之利用，以符合本法第1 條規定「合理利用個人資料」之宗旨。(本件警政署申請開放居留外僑動態管理系統之每月初辦居留外配名冊及外僑（勞）相片檔供其查詢，其目

[68]法務部 97 年 8 月 7 日法律決字第 0970700471 號函。
[69]法務部 98 年 10 月 7 日法律司字第 0980700632 號函。

的係爲打擊人口販運、維護公序良俗以及臨檢可疑人員時比對身分之用，應可認符合上開本法第8 條第4 款所定「爲增進公共利益」之要件，從而得爲特定目的外之利用；惟於提供資料時，仍請注意本法第6 條比例原則之規範意旨。)[70]

法務部每日將矯正機關收容人入出監異動資料送至內政部，以利全國戶政單位快速查詢，惟內政部對於「戶役政系統」提供戶政單位以外機關，有關「監所收容人」係比照「失蹤人口」註記爲「特殊人口」，而未顯示在監在押及矯正機關地址，致查詢機關無從由戶籍資料知悉當事人之在監事實。而戶政單位將收容人所在之矯正機關納入查詢戶籍資料範圍，係移送機關爲辦理行政處分文書之送達業務所需，應符合電腦處理個人資料保護法第8 條第4 款所定「爲增進公共利益」特定目的外之利用。[71]

查檢察或司法警察機關依刑事訴訟法規定偵查犯罪，符合電腦處理個人資料保護法第八條但書第一款之「法令明文規定者」、第四款「爲增進公共利益者」及同法第二十三條但書第一款「爲增進公共利益者」及第三款「爲防止他人權益之重大危害而有必要者」之情形，各醫療院所應可援引上揭規定提供個人資料，不得藉詞拒絕。[72]

三、民政部分

對於各公所製作之鄰長名冊是否適用或應如何適用方爲妥當，及得否於各公所建置網頁公布各鄰長姓名、地址等資訊一案，法務部認爲，按電腦處理個人資料保護法第8 條(參見新修正個人資料保護法第16條)規定，公務機關對個人資料之利用，應於法令職掌範圍內爲之，與蒐集之特定目的相符，但如符合同條但書所定情形之一者，得爲特定目的外之利用。又政府資訊公開法第2 條規定：「政府資訊之公開，依本法之規定。但其他法律另有規定者，依其規定。」是以，個人資料之利用如係其他法律明定應提供者，性質上爲政府資訊公開法

[70]法務部 99 年 5 月 26 日法律字第 0999022160 號函。
[71]法務部 97 年 2 月 26 日法律字第 0960049967 號函。
[72]法務部 86 年 5 月 8 日法律字第 12894 號函。

之特別規定，公務機關自得依該特別規定提供之。如無法律明定應提供者，不論屬特定目的範圍內利用或特定目外之利用，依政府資訊公開法第18 條第1 項第6 款規定，政府資訊之公開或提供，侵害個人隱私、職業上秘密等者，應限制公開或不予提供，但有公益上之必要或經當事人同意者不在此限。至於何謂「對公益有必要」，應由主管機關就「公開個人資料欲增進之公共利益」與「不公開個人資料所保護之隱私權益」間比較衡量判斷之，如經衡量判斷符合「公開個人資料所欲增進之公共利益」，而對於提供個人資料所侵害之隱私較爲輕微者，自得公開之。如認部分資訊確涉有隱私，而應限制公開者，依政府資訊公開法第18 條第2 項規定，得僅公開其餘未涉隱私部分。惟無論係特定目的範圍內或特定目的範圍外之利用，均應遵循同法第6 條(參見新修正個人資料保護法第5條)之規定：「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。」辦理。本件地方政府是否得將鄰長名冊建置網頁予以公布乙節，按該名冊爲經電腦處理之個人資料，依上所述，除有其他法律明定應予公布，否則主管機關應於「公益」與「私益」間比較衡量決定之。[73]

中央研究院經濟研究所爲學術研究問卷調查需要，向戶政機關申請提供個人姓名、地址、出生日期等個人戶籍資料乙節，就戶政機關利用個人資料性質觀之，應屬特定目的（戶政及戶口管理）外之利用，是否符合上開個資法第8 條第7 款規定所稱「爲學術研究而有必要且無害於當事人之重大利益」，宜本於權責審認之，其審酌事項宜包括例如：蒐集資料者是否簽有保密切結書，保證不洩漏當事人資料？當事人資料有無作匿名化處理，致研究報告公布或揭露時，不會識別特定當事人？提供之資料是否僅屬一般基本資料，未涉及當事人較敏感之資料等。另個資法第6 條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」故如

[73]法務部95 年7 月19 日法律字第0950021839 號函。

認符合前揭個資法第8 條第7 款規定而得爲目的外利用者，其所提供戶籍資料之範圍，仍應注意以該學術研究有必要者爲限，與該學術研究無關或非必要之資料，則不得提供。至於學術研究機關（構）對於個人資料之蒐集，自應視其爲公務機關或非公務機關，分別符合個資法第7 條或第18 條規定，始得爲之。[74]

關於學校或學術研究機構等以學術研究名義申請提供民眾戶籍資料，所涉及電腦處理個人資料保護法第8 條規定之適用疑義，法務部認爲，按個資法第8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。…四、爲增進公共利益者。…七、爲學術研究而有必要且無害於當事人之重大利益者。……九、當事人書面同意者。」復按行政資訊公開辦法第5 條第1 項第5 款規定，行政資訊之公開或提供有侵犯營業或職業上秘密、個人隱私者，應限制公開或提供；但法令另有規定、對公益有必要或經當事人同意者，不在此限。本件台灣大學心理系曹老師爲國科會專題研究計畫向台北市民政局請求提供新生兒資料乙節，就該局利用個人資料性質觀之，應屬特定目的（戶政及戶口管理）外利用之情形，是否符合個資法首開規定第7款所稱之「爲學術研究而有必要且無害於當事人之重大利益」，宜由該局本於權責審認之，其審酌事項宜包括例如：蒐集資料者是否簽有保密義務，保證不洩漏當事人資料？當事人資料有無作匿名化處理，致研究報告公布或揭露時，不會識別特定當事人？提供之資料是否僅屬一般基本資料，未涉及當事人較敏感之資料等。又如認符合前揭個資法第8條第7 款所稱「爲學術研究而有必要且無害於當事人之重大利益」而得爲目的外利用者，仍應依行政資訊公開辦法判斷有無限制公開或提供之情事。因該新生兒個人資料屬於個人隱私之一部分，依該辦法前揭條款規定，除有法令規定或經當事人同意者外，須「對公益有必要者」始得公開或提供之。至於上開所稱之「公益」及「有必要」，均屬不確定法律

[74] 法務部 98 年 11 月 16 日法律決字第 0980047501 號函。

概念，宜由受理請求提供資訊之機關，就「公開個人資料所欲增進之公共利益」與「不公開個人資料所保護之隱私權益」間比較衡量判斷之。是以，如該局經衡量判斷認爲本件符合「公開個人資料所欲增進之公共利益」，而對於提供個人資料所侵害之隱私權益較爲輕微者，自得提供之。另個資法第6 條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」本件於提供該新生兒之個人資料時，應注意所提供之資料，應以該學術研究有必要者爲限，與該學術研究無關之資料，則不得提供。[75]

就個資法部分而言，按個資法第8 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，但如符合同條但書所定情形之一者，得爲特定目的外之利用。第6 條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」本件公布莫拉克風災後未與親人聯繫者之姓名，符合民政、戶政及戶口管理、社會行政之特定目的，且屬於內政部法令規定職掌必要範圍內，與個資法第8 條規定尚無不合。惟來函僅謂將上開個人資料公布於政府網頁、發布新聞，並運用電子媒體刊登，籲請當事人與內政部聯絡。然實際採行之公布方式、媒介、時間、內容、範圍等細節事項並未敘明，建請內政部於公布前宜審慎斟酌公布之內容、程度及範圍，僅於可供一般人識別或判斷失蹤當事人身分之必要範圍爲之，例如：姓名、相片、性別、年齡等足資初步識別資料（不含出生年月日、身分證統一編號），以符合誠信原則與比例原則。就政資法部分而言，第2 條規定：「政府資訊之公開，依本法之規定。但其他法律另有規定者，依其規定。」政資法第18 條第1 項第6 款規定，政府資訊之公開或提供，侵害個人隱私、職業上秘密等者，應限制公開或不予提供，但有公益上之必要或經當事人同意者，不在此限。至於何謂「對公益有必要」，應就「公開個人

[75] 法務部94 年11 月1 日法律字第0940033446 號函。

資料所欲增進之公共利益」與「不公開個人資料所保護之隱私權益」間比較衡量判斷之，本件公布莫拉克風災後未與親人聯繫者之姓名，公布係於可供一般人識別或判斷失聯當事人身分同一性之程度及必要範圍內，雖有揭露失聯當事人之個人部分隱私，惟有利於各級主管機關結合民間力量協尋失聯民眾，健全民政、戶政管理或社會行政，降低政府協尋失聯民眾之成本，有利於公共利益之增進，適法性應無疑義。[76]

直轄市、縣（市）主管機關請求警政機關協助提供收養案件、監護案件當事人及保護案件兒童及少年父母或監護人之素行（危害兒童及少年人身安全的前科）等資料，如屬電腦處理之個人資料，就警政機關言，提供上開前科資料係依兒童及少年福利法第四十七條規定之協助配合義務，似符合電腦處理個人資料保護法第八條但書第一款所稱「法令明文規定者」。另社會福利主管機關依法爲保障兒童及少年權益及增進其福利，所爲收養、監護及保護案件當事人、父母或監護人等危害兒童及少年人身安全之前科資料之蒐集，似亦符合電腦處理個人資料保護法第八條第六款所稱「爲防止他人權益之重大危害而有必要者」之情形，準此，警政機關將蒐集之上開前科資料提供給社會福利主管機關，於法自無不合。[77]

四、勞工部分

關於勞委會規劃之「短期補習班聘僱外籍教師工作許可資訊查詢系統」是否符合電腦處理個人資料保護法相關規定疑義乙案，法務部認爲，依電腦處理個人資料保護法第8 條(參見新修正個人資料保護法第16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。除有同條但書9 款情形外，不得爲特定目的外之利用。準此，如依勞委會相關規定，認爲將外籍教師基本資料提供查詢尚未符合蒐集該個人資料之「特定目的」者，

[76] 法務部 98 年 11 月 9 日法律字第 0980036360 號函。
[77]法務部 93 年 8 月 19 日法律決字第 0930030855 號函。

則依本法第8 條規定，需符合同條但書所列9 款情形之一者，始得爲特定目的外之利用。是爲避免爭議，本案建請勞委會於蒐集個人資料時，取得該外籍教師同意將其資料上網供查詢之書面，至於現有個人資料亦可函詢當事人是否同意，以資周延，俾維護當事人權益。另將外籍教師個人資料提供當事人以外之第三人查詢時，不得逾越必要範圍（本法第6 條【參見新修正個人資料保護法第5條】規定參照），亦即，不得提供他人查詢「非必要」之個人資料。[78]

五、地政部分

關於臺南縣政府爲未領取之徵收補償費於依法存入保存專戶後，得否將未受領徵收補償費保管資料，於存入後第 10 年公布於政府網頁抑或提供民眾閱覽乙案，法務部認爲，按電腦處理個人資料保護法第8 條規定，公務機關對個人資料之利用，應於法令職掌範圍內爲之，並與蒐集之特定目的外之利用。又政府資訊公開法第2 條規定：「政府資訊之公開，依本法之規定。但其他法律另有規定者，依其規定。」是以，個人資料之利用如無法律明定應提供者，不論屬特定目的範圍內或特定目的外之利用，依政資法第18 條第1 項第6 款規定，政府資訊之公開或提供，侵害個人隱私、職業上秘密等者，應限制公開或不予提供，但有公益上之必要或經當事人同意者，不在此限。至於何謂「對公益有必要」，應由主管機關就「公開個人資料所欲增進之公共利益」與「不公開個人資料所保護之隱私權益」間比較衡量判斷之，如經衡量判斷符合「公開個人資料所欲增進之公共利益」，而對於提供個人資料所侵害之隱私較爲輕微者，自得公開之。如認部分資訊確涉有隱私，而應限制公開者，依政資法第18 條第2 項規定，得僅公開其餘未涉隱私部分。又無論係特定目的範圍內或特定目的外之利用，均應遵循個資法第6 條規定，不得逾越特定目的之必要範圍（本部95 年7 月19 日法律字第0950021839 號函參照）。本件臺南縣政府所爲徵收

[78]法務部95 年3 月24 日法律字第0950005051 號函。

補償戶個人資料之蒐集及建立保管專戶資料，以及爲利後續土地徵收程序之進行及達成該土地徵收法令所定之通知義務而利用上開個人資料，符合土地行政之特定目的，且屬於法令規定（土地徵收條例）職掌必要範圍內。惟是否得將上開個人資料公布於政府網頁或提供民眾閱覽，依上開說明，宜由主管機關審酌是否屬「公益上之必要」，以及執行通知義務而爲個人資料利用之方法（公布於政府網頁、提供民眾閱覽及其內容）有無逾越必要範圍予以判定。79

按依電腦處理個人資料保護法第八條規定，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，惟如有該條但書所列各款情形之一，亦得爲特定目的外之利用。台北縣政府擬將土地登記專業代理人之姓名、事務所地址、電話、各地政事務所之登記及測量案件補正駁回率等資料提供民眾電話及網路查詢，如未違其他相關法令規定，似可認與電腦處理個人資料保護法第八條但書第四款「爲增進公共利益者」或第六款「爲防止他人權益之重大危害而有必要者」之規定並無違背。[80]

六、稅捐稽徵部分

關於配合國稅局稽徵業務需要，商請地方政府衛生局轉請醫院提供病患就診與住院期間醫療情形之適法性乙案，法務部認爲，按電腦處理個人資料保護法第2 條規定：「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。」查稅捐稽徵法第30 條規定：「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。」準此，依特別法優於普通法之原則，稅捐稽徵機關或財政部賦稅署指定之調查人員亦得依上開稅捐稽徵法之規定，爲調查課稅資料之執行業務所需，得向有

[79]法務部98 年7 月13 日法律字第0980011751 號函

[80]法務部 87 年 9 月 9 日法律字第 031832 號函。

關機關、團體或個人進行調查，要求提示有關文件。又本法規定公務機關或非公務機關對個人資料之利用，除應於蒐集之特定目的必要範圍內之利用外，依本法第8 條但書及第23 條但書規定，尚包括「特定目的外」之利用，故於有各該但書規定各款情形之一時，即應允許爲特定目的外之利用，俾符合本法第1 條規定「合理利用個人資料」之宗旨（本部86 年5 月8 日法律字第12894 號函參照）。本件稅捐稽徵機關爲執行其法定職務，依稅捐稽徵法第30 條規定得向有關機關進行調查及要求提示有關文件，故政府及相關醫療機構符合本法第8 條但書第1 款或第4 款及第23 條但書第1 款所定「法令明文規定者」、「爲增進公共利益者」等之情形，自得依法爲特定目的外之利用。惟仍請注意本法第6條比例原則之規範意旨。[81]

按電腦處理個人資料保護法第8 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，惟如符合同條但書所列九款情形之一者，亦得爲特定目的外之利用。本件財政部爲辦理身心障礙者使用牌照稅減免業務，請內政部按月提供全國身心障礙者個案基本資料，雖與內政部資料蒐集之特定目的不符，惟如該等資料之提供，符合上開但書規定第4款「爲增進公共利益者」或第8款「有利於當事人權益者」之情形，自得爲特定目的外之利用。[82]

七、衛生醫療部分

有關地方政府爲查核健保身分（健保床）接受安置於醫療、療養機構就醫達3 個月以上之低收入戶身心障礙者資料，以避免溢發補助款是否符合「電腦處理個人資料保護法」第8 條(即99年4月27日立法院通過之新修正條文爲第16條)得爲特定目的外之利用案，法務部認爲本案係直轄市、縣（市）政府爲執行「身心

[81]法務部98 年1 月8 日法律決字第0970042838 號函。

[82]法務部 99 年 5 月 5 日法律字第 0999019675 號函。

障礙者生活托育養護費用補助辦法」第8 條第1 項第6 款規定而請求行政院衛生署中央健康保險局提供低收入戶身心障礙者以健保身分接受安置於醫療、療養機構就醫達3 個月以上之個人資料，旨在避免資源重疊浪費，該局為協助上開辦法規定而提供該等資料，應符合本法第8 條第4 款(即99年4月27日立法院通過之新修正條文為第16條第2款) 所定「增進公共利益」之情形。惟提供上開資料之機關，宜一併注意本法第6條之規定。[83]

按電腦處理個人資料保護法（以下簡稱本法）第8 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：１、法令明文規定者。２、有正當理由而僅供內部使用者。３、為維護國家安全者。４、為增進公共利益者。５、為免除當事人之生命、身體、自由或財產上之急迫危險者。６、為防止他人權益之重大危害而有必要者。７、為學術研究而有必要且無害於當事人之重大利益者。８、有利於當事人權益者。９、當事人書面同意者。」台南市政府向中央健保局索取資料之目的係為因應該市○○區中石化污染事件，針對鹿耳等3里里民持有重大傷病證明者，如經相關檢測，其檢測值超過一定標準者，將給予適當補助；準此，對於資料被提供之當事人而言，因尚須經一定程序之檢測與審核，始有可能獲得補助，故該資料之提供似非一概有利於當事人權益，是否符合上開本法第8 條第8 款所定情形，不無疑義。[84]

八、政府資訊公開部分

對於電腦處理個人資料保護法與政府資訊公開法之適用，並非何者絕對優先適用，原則上公務機關對個人資料之利用，應於法令職掌範圍內為之，並與蒐集之特定目的相符，但如符合電腦處理個人資料保護法第8 條但書所定情形

[83]法務部94 年8 月9 日法律字第0940025018 號函。

[84]法務部 94 年 10 月 31 日法律決字第 0940039601 號函。

之一者，得爲特定目的外之利用。若個人資料之利用係其他法律明定應提供者，性質上爲政府資訊公開法之特別規定，公務機關自得依該特別規定提供之。如無法律明定應提供者，不論屬特定目的範圍內利用或特定目外之利用，依政府資訊公開法第18 條第1 項第6 款規定，政府資訊之公開或提供，侵害個人隱私者，應限制公開或不予提供。但有公益上之必要或爲保護人民生命、身體、健康有必要或經當事人同意者不在此限。至於何謂「對公益有必要」，應由主管機關就「公開個人資料欲增進之公共利益」與「不公開個人資料所保護之隱私權益」間比較衡量判斷之，如經衡量判斷符合「公開個人資料所欲增進之公共利益」，而對於提供個人資料所侵害之隱私較爲輕微者，自得公開之（本部95 年7月19 日法律字第0950021839 號函意旨）。[85]

關對個人資料之利用，原則上應於法令職掌範圍內爲之，並與蒐集之特定目的相符，但如符合個資法第8條但書所定情形之一者，得爲特定目的外之利用。若個人資料之利用係其他法律明定應提供者，性質上爲政府資訊公開法之特別規定，公務機關自得依該特別規定提供之。如無法律明定應提供者，不論屬特定目的範圍內利用或特定目的外之利用，依政府資訊公開法第18 條第1 項第6 款規定，政府資訊之公開或提供，侵害個人隱私者，應限制公開或不予提供。但有公益上之必要或爲保護人民生命、身體、健康有必要或經當事人同意者不在此限（本部98 年1 月7 日法律決字第0970700924 號函參照）。本件申請提供之個人資料檔案，如經當事人書面同意，法院依其所請發給該等資料，核與個資法第8 條第9 款及政府資訊公開法第18 條第1 項第6 款規定，似無不符。[86]

按電腦處理個人資料保護法第8 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

[85]法務部 98 年 1 月 7 日法律決字第 0970700924 號函。
[86]法務部99 年5 月27 日法律決字第0999020000 號函。

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。」查立法委員請求提供台北縣各鄉鎮市民代表會代表名單電子檔者，應屬該等資料之特定目的外利用，是否符合上開本法第8 條但書規定情形，係屬事實認定問題，宜由相關權責機關本於職權審認之。[87]

有關議員服務處函請行政機關提供學生名冊之適法性疑義乙案，法務部意見認爲，查政府資訊公開法制定之目的條、爲保障人民知的權利，以便利人民公平利用政府依職權所作成或取得之資訊，增進人民對公共事務之瞭解、信賴及監督，並促進民主之參與。依該法第9 條第1 項規定，得申請政府機關提供政府資訊者爲具有中華民國國籍並在中華民國設籍之國民及其所設立之本國法人、團體，或持有中華民國護照僑居國外之國民。議員服務處固非上開規定之對象而無政資法適用之問題；如以議員或其個人身分申請提供，則有政資法之適用，惟如有同法第18 條第1 項第6 款所定應依法限制或不予提供之事由者，應限制公開或不予提供。又按電腦處理個人資料保護法第3 條第6款所稱「公務機關」係指依法行使公權力之中央或地方機關。議員服務處亦非屬該法規定之「公務機關」並無個資法第7 條規定之適用。至於教育局基於管理學校所搜集之學生名冊等個人資料檔案，如提供議員或其服務處作爲問政使用或民調使用，係屬於對個人資料之特定目的（079 學生資料管理）外利用，故教育局提供上開學生名冊資料，應符合個資法第8 條但書「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。但有在列情形之一者，得爲特定目的外之利用：一、法令明文規定者。…四、爲增進公共利益者。…八、有利於當事人權益者。九、當事人書面同意者。」所列各款情形之一，始

[87]法務部98 年2 月24 日法律決字第0980007233 號函。

符爲特定目的外之利用。本件議員服務處函請提供學生名冊，作爲問政使用或公費營養午餐專業民調使用，是否符令上開個資法第8 條但旦書規定任一款情形，宜由教育局本諸權責判斷。[88]

關於議會函請戶政機關提供戶長名冊，是否與電腦處理個人資料保護法、政府資訊公開法牴觸疑義一案，查政府資訊公開法制定之目的係爲保障人民知的權利，以便利人民公平利用政府依職權所作成或取得之資訊，增進人民對公共事務之瞭解、信賴及監督，並促進民主之參與。依該法第9 條第1 項規定，得申請政府機關提供政府資訊者爲具有中華民國國籍並在中華民國設籍之國民及其所設立之本國法人、團體，或持有中華民國護照僑居國外之國民。縣議會非上開規定適用之對象，自無政資法適用之問題（本部91 年10 月15 日法律字第0910035503 號函同此意旨）。按電腦處理個人資料保護法第3 條第6款所稱「公務機關」，係指依法行使公權力之中央或地方機關。準此，縣議會屬於該法規定之「公務機關」，並無疑義。因此，縣議會函請提供戶長名冊，應符合個資法第7 條規定，始得爲之。次按個資法第8 條對公務機關就個人資料爲特定目的外之利用者，定有嚴格之限制規定。依該條規定，戶政機關基於戶政及戶口管理之特定目的所蒐集之個人資料，如擬提供其他第三人作特定目的外利用者，須符合該條但書所列九款情形之一，始得爲之。縣議會即使符合個資法第7 條規定就議案涉及事項得蒐集民眾戶籍資料，但如不符合上揭個資法第8條所定得特定目的外利用個人資料情形之一者，戶政機關即不得提供。另本件來函所述「議案涉及事項」，究何所指？語意不明，非無探究之餘地。該「議案涉及事項」究與個資法第8 條但書所定九款情形中之何款相符，宜由受理請求提供個人資料之戶政機關本於權責判斷之。再者，個資法第6 條規定：「個人資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法爲之，不得逾越特定目的之必要範圍。」準此，戶政機關就所蒐集之個人資料爲特定目的外利用時，自應符合上揭法條所定之比例原則。此外，個資法第27 條及第30 條

[88]法務部 97 年 10 月 13 日法律決字第 0970037059 號函。

有關公務機關如違反該法規定，致當事人權益受損害者，應負國家損害賠償責任，亦應一併注意。[89]

九、電信

因近年來不法集團大量利用電信業者所提供之電信服務，做爲詐騙民眾之工具，已造成嚴重之社會治安問題，而非僅屬個案或突發事件。民眾接聽詐騙集團威嚇、利誘電話，不僅心生恐懼，更陷於財物遭詐騙之危險中，即使不爲所動，受話者之使用權益更嚴重遭受干擾，而有損使用者之消費權益。由於詐騙行爲層出不窮，影響民眾權益既深且廣，如何有效管理電信之傳遞使用，斷絕詐騙集團使用電信作爲犯罪工具，乃政府之當務之急。警政單位破獲詐騙案件後，對於作爲電信人頭之個人資料予以提供或揭露，避免該等電信人頭再度申請大量電話從事詐騙，應屬必要之打擊犯罪行爲。國家通訊傳播委員會基於通訊傳播事業主管機關之立場，本於「電信監理業務」之特定目的，蒐集及電腦處理警政單位提供之電信人頭個人資料，供電信業者與民眾締約前查詢徵信，以協助其依電信法第22 條之規定，拒絕或停止該等電信人頭大量申辦電話從事詐騙行爲，以確保其他正常使用電信服務之消費者權益，應屬國家通訊傳播委員會法令規定職掌必要範圍內，自符合電腦處理個人資料保護法第7 條、第8 條等相關規定。[90]

十、教育

個人資料當事人所任職學校以保護幼兒學童教養及安全需要，請求戶籍地縣市政府提供當事人體複檢之免役原因證明文件相關資料，核與電腦處理個人資料保護法第8 條第4 款所定「爲增進公共利益」之要件及政府資訊公開法第

[89]法務部95 年5 月8 日法律決字第0950015813 號函。

[90] 法務部 96 年 2 月 15 日法律字第 0960006377 號函。

18條第1 項第6 款但書規定，似無不符，從而得爲特定目的外之利用；惟於提供資料時，仍請注意本法第6 條比例原則之規範意旨。[91]

電腦處理個人資料保護法第八條規定，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，惟如符合同條但書所列九款情形之一者，得爲特定目的外之利用。內政部役政署執行小組要求警政署查詢、提供替代役駐校警衛役男入營前之前科資料，雖與資料蒐集之特定目的有所不符，惟如該等資料之查詢、提供登項，符合上開但書規定第四款「爲增進公共利益者」或第六款「爲防止他人權益之重大危害而有必要者」之情形，自得爲特定目的外之利用。[92]

伍、安全維護原則（Security Safeguards Principle）

即個人資料爲防止遺失、未經授權的接近、毀損、利用、變更或揭露之風險，應採取合理之安全保護措施。因此，我國個人資料保護法第六條第一項第二款規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。」第十八條規定：「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。」及第二十七條規定：「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。」又按2012年10月1日生效之「個人資料保護法施行細則」第九條規定:「本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱

[91] 法務部 99 年 8 月 12 日法律決字第 0999026180 號函。
[92] 法務部 89 年 10 月 13 日法律決字第 038212 號函。

適當之安全措施，指公務機關或非公務機關爲防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例爲原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」

按新修正個人資料保護法，非公務機關行業別限制取消，然而，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，第二十七條第二項乃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。[93]

陸、公開原則（Openness Principle）

即個人資料的蒐集、處理、利用及相關政策的制定，應對一般人公開之。事實上，從憲法角度言之，於蒐集、處理、利用個人資料時，應遵循「透明化」原則，使得當事人可以知悉其個人資料如何被蒐集、處理、利用，甚至可以進一步加以抗拒。[94]再者，因公務機關係全國最大的個人資料蒐集者，且基於公權力的行使，可以蒐集各類型的個人資料，因此，按政府資訊公開之精神，各級政府機關應將其所持有的個人資料之情形公諸於世，以便民眾得藉以行使相關權利。[95]

按我國個人資料保護法第十七條規定：「公務機關應將下列事項公開於電

[93] 個人資料保護法第二十七條之修正說明。
[94]許文義，「個人資料保護法論」，頁 197，台北，三民書局，2001 年 1 月。
[95]劉佐國、李世德，個人資料保護法釋義與實務--如何面臨個資保護的新時代，頁 85，台北，碁峰資訊股份有限公司，2012 年 8 月。

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。」 因此，公務機關保有個人資料檔案者，應公開於電腦網站或以其他適當方式供公眾查閱檔案之名稱、類別及保有機關名稱等；其有變更者，亦同。惟非公務機關則不在受拘束之列。

另外，鑑於目前國人使用網際網路極爲普遍，因此公務機關依現行條文規定應公告事項，如能張貼公開於機關電腦網站，將更有利於民眾查閱，惟慮及城鄉差距及電腦使用普及率等等因素，仍保留其他供公眾查閱之適當方式，例如：刊登政府公報等。[96]

柒、個人參與原則（Individual Participation Principle）

即個人資料當事人對於他人持有自己的資料，得行使一定程序的控制。按個人資料保護法第十條規定：「公務機關或非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。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」十一條規定：「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。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。違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。因可歸責於公務機關或非公務機關之事由，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。」可知，針對公務機關或

[96] 個人資料保護法第十七條之修正說明。

非公務機關蒐集之個人資料檔案，當事人得要求查詢、閱覽、製作複本、補充或更正；就個人資料正確性有爭議者，應主動或當事人得請求停止處理及利用。

另外，依個人資料保護法第十四條規定，查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。

捌、問責原則（Accountability Principle）

按個人資料保護法第二十八條規定：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，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，並得請求爲回復名譽之適當處分。依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元爲限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益爲限。同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。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。」第二十九條規定：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第六項規定。」第三十條規定：「損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」第三十一條規定：「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。」可知，公務機關或非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，應負損害賠償責任，而對於同一原因事實造成多數當事人權利受侵害之事件，經當事人

請求損害賠償者，其合計最高總額以新臺幣二億元爲限。。

再者，按個人資料保護法第三十四條規定：「對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，由法院併案審理。其他因同一原因事實受有損害之當事人，亦得聲請法院爲前項之公告。前二項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認爲必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。依第一項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。」可知，對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。

個人資料保護法除上開八大原則外，其他重要內容，分析如下：

玖、「個人資料」之定義

美國學者Alan Westin曾將「資訊隱私權」界定爲：「個人得決定何時、如何及在何種範圍向他人揭露其個人資料[97]。」我國司法院大法官第六○三號亦解釋：「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

[97]Daniel J. Solove, Paul M. Schwartz, Information Privacy law 28 (2003).

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。」據此，資訊隱私權乃控制個人資料蒐集、處理、使用或分享之權利。

按美國學界見解，個人資料的定義可解釋爲，用以描述資料與個人之間的關係，且係屬(1)與個人之間的作者關係、(2)對個人的敘述關係、或(3)對個人的指示關係。首先，作者關係乃將個人與其所製作用以跟他人溝通的資料之間連結起來，所以，電子郵件或信函皆足以構成個人資料；其次，個人資料用以敘述個人的生理或社會狀況，如性別、身高、體重、血型、生日、婚姻狀況、信用紀錄、宗教或政治團體的會員身份等皆是本類型之個人資料；最後，台灣的國民身份證號碼或美國的社會安全號碼，則是藉以指示或追索特定個人的個人資料類型之最佳例證。此種號碼乃由政府機關所賦予，以爲追蹤紀錄的方便[98]。再者，個人資料不僅包括文字類型的資訊[99]，也應包括足以辨識個人（不論當事人是否仍健在）的照片、影像或聲音紀錄。

資訊隱私權得用以防止或排除個人資料的不法蒐集、處理或利用，非個人的資料則不在適用之列，所以不受保護[100]。一般而言，非個人的資料包括「非人類的資料」、「匿名的資料」及「團體的資料」三者。非人類的資料，係指與人類無關聯之資料。匿名的資料多半將被視爲非個人的資料。然而，倘匿名的資料經由公開或研究而因此可得查知所牽涉個人的身分者，該匿名的資料將被歸類爲個人資料。此外，倘若資料所指涉者，係一群人所組成之團體而非特定之個人[101]，則該團體的資料將不被視爲個人資料。

按我國新修正之個人資料保護法第二條第一項第一款規定：「個人資料：

---

[98] Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1202-1203 (1998).

[99] Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 Ind. L. Rev. 173, 179 (1999).

[100] Henry M. Cooper, The Electronic Communications Privacy Act: Does The Answer to The Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis, 20 J. Marshall J. Computer & Info. L. 1, 3 (Fall 2001).

[101] Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1208-1211 (1998).

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。」新法與舊法的電腦處理個人資料保護法第三條第一項第一款[102]關於個人資料之定義相去不遠，二者定義皆採例示與概括規定並用方式爲之，其主要內容有三：（1）自然人；（2）關於屬人或與個人連結屬事之個別資料；及（3）其他足資識別該個人之資料[103]。

針對個人資料定義適用上的疑義，法務部曾爲相關解釋，分述如下：

所涉之指紋、聲紋、掌形等足資識別個人特徵之資料，自屬本法規範之「個人資料」。[104]

所稱「個人」，指生存之特定或得特定之自然人。簡言之，本法立法目的之一即在保護屬於人格權之隱私權，而唯有生命之自然人方有隱私權受侵害之恐懼情緒。至於已死亡之人，已無恐懼其隱私權受侵害之可能，且其個人資料已成爲歷史，故非在本法保護之列。從而，有關已亡故之人的個人資料處理或利用，尚不發生適用個人資料保護法之問題。[105] 事實上，新修正之個人資料保護法施行細則第二條亦明文規定：「本法所稱個人，指現生存之自然人。」

有關民意代表及建設公司等請求戶政機關提供某門牌地址內之戶數及設籍人數，如其並未與自然人之姓名等相結合，亦無從以此方式直接或間接識別該個人者，則該資料即非上開規定所稱之個人資料，並不發生適用個人資料保護法之問題。[106]

所稱當事人，係指個人資料之本人。準此，倘某一個別資料係涉及多數個人之間關於家庭、職業或社會活動等雙重或多重關係時，該多數關係人均爲當

---

[102] 電腦處理個人資料保護法第三條第一項第一款規定：「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。」

[103] 參見許文義，「個人資料保護法論」，頁 22，台北，三民書局，2001 年 1 月。

[104] 法務部 90 年 3 月 20 日法律字第 005734 號函。

[105]法務部 94 年 5 月 17 日法律字第 0940017828 號函。

[106] 法務部 94 年 10 月 27 日法律字第 0940039602 號函

事人。因此，所涉及之行動電話用戶向電信業者請求提供之受信通信紀錄，依所附通聯紀錄範例觀之，其上記載有發話號碼、受話號碼、通話種類、通話區域、通話日期、時間等項目，係屬有關發信人與受信人之社會活動之資料，應爲發信人與受信人所共享之個人資料，屬於上開個人資料保護法規定所稱個人資料之範圍，該發信人與受信人均屬個人資料保護法所稱之當事人，自有本法之適用。[107]

所稱當事人，係指個人資料之本人。有關建物之門牌、基地座落、格局、外觀、交易價格等資料，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，則該資料即非本法所稱之個人資料。[108]

有關仲介業收集他人房屋外觀資料提供查詢服務，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，則該資料即非上開規定所稱之個人資料。[109]

保護的個人資料，僅限於生存的特定或得特定的自然人資料，而不及於法人等組織資料的保護。[110]

拾、個人資料保護法其他重要用語之定義

按我國新修正之個人資料保護法第二條第二項第一至九款規定：「本法用詞，定義如下：

二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、蒐集：指以任何方式取得個人資料。

四、處理：指爲建立或利用個人資料檔案所爲資料之記錄、輸入、儲存、編輯、

[107]法務部 91 年 10 月 28 日法律字第 0910037677 號函。

[108] 法務部 92 年 8 月 29 日法律字第 0920035652 號函。

[109] 法務部 92 年 7 月 4 日法律字第 0920026192 號函。

[110]法務部92 年12 月30 日法律決字第0920054625 號函。

更正、複製、檢索、刪除、輸出、連結或內部傳送。

五、利用：指將蒐集之個人資料爲處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、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。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。」

其中，所稱「蒐集」者，乃以任何方式取得個人資料，包括直接向當事人蒐集或間接從第三人取得者，均屬之；其係以書或言詞爲之，亦在所不問。[111]

中國石油股份有限公司係屬營利性之公司組織，自非本法所稱「公務機關」。[112]

按個人資料保護法所稱之當事人，係指「個人資料之本人」，並不包括其繼承人等。如擬將繼承人、債權人及遺產管理人、遺囑執行人及破產管理人均納入得提供個人資料檔案之對象，涉及他人之隱私權，如無法律或法律明確授權之命令之依據，恐與憲法第二十三條、中央法規標準法第五條第二款之規定有違。[113]

拾壹、 必要原則

按我國新修正之個人資料保護法第五條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法爲之，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。」個人資料保護法第六條第一項第二、四款規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措

[111] 法務部 93 年 9 月 21 日法律字第 0930037825 號函。
[112]法務部 86 年 3 月 8 日法律決字第 08574 號函。
[113] 法務部 89 年 6 月 5 日法律字第 010671 號函。

施。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，爲統計或學術研究而有必要，且經一定程序所爲蒐集、處理或利用之個人資料。」第八條第二項第二款規定：「有下列情形之一者，得免爲前項之告知：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。」第九條第二項第四款規定：「有下列情形之一者，得免爲前項之告知：四、基於公共利益爲統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者爲限。」個人資料保護法第十五條第一項第一款規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。」個人資料保護法第十六條第一項第五款規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。」個人資料保護法第十九條第一項第四款規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：四、學術研究機構基於公共利益爲統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。」第二十條第一項第五款規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。」第二十五條第二項規定：「中央目的事業主管機關或直轄市、縣（市）政府爲前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法爲之。」等，均顯示公務機關或非公務機關於蒐集、處理或利用個人資料時，應受比例原則之拘束。

憲法上有「比例原則」，乃由法治國家原則衍生而來，在於強調國家進行行政行爲時，「不得爲達目的而不擇手段」，可知，比例原則在於強調目的與手段間之均衡，如西諺所云「不必以大砲打小鳥」或我國俗諺所云「殺雞焉用牛刀」。而廣義「比例原則」包括適當性原則(又稱合目的性原則)、必要性原則及過度禁止原則(即狹義比例原則)。[114]我國行政程序法第七條：「行政行爲，應依下列原則爲之：一、採取之方法應有助於目的之達成。二、有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三、採取之方法所造成之損害不得與欲達成目的之利益顯失均衡。 」

如上揭，「必要」用語出現於個人資料保護法諸多條文中，然而，「必要」係一不確定法律概念，需要在個案中一一予以具體化判斷，尤應審慎考量「目的」與「手段」之間的實質合乎比例。按個人資料保護法第五條規定：「個人資料之蒐集、處理或利用，……，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。」可知，個人資料之蒐集、處理或利用不僅不得逾越必要範圍，並應與蒐集目的具有手段上正當合理之關聯性，不得與其他目的爲不當之連結。例如，在資料蒐集時，必須先審查，該資料蒐集是否必要？其必須有嚴格標準予以衡量，僅在履行具體任務必要時，始得蒐集資料。在必要性之範圍中亦應審查，對於當事人蒐集個人資料時，是否會對其值得保護的利益將造成過度不當的侵害？倘若係肯定的，基於憲法上過度禁止原則，此蒐集個人資料行爲對於行政機關任務之達成，乃屬不必要的。[115]

關於「必要原則」，法務部曾針對諸多具體個案而爲解釋，例如，本件所提供之人員名冊含有出生年月日及身分證統一編號等重要個人資料，是否逾越必要範圍？有無必要性？應視提供該人員名冊之目的而定，如不提供出生年月日及身分證字號等資料亦能達到目的時，自不宜提供該等資料，以保護當事人

[114]李惠宗，憲法要義，頁 115，元照出版有限公司，2009 年 9 月。
[115]許文義，「個人資料保護法論」，頁 201，台北，三民書局，2001 年 1 月。

隱私權益。[116]

在兼顧「避免人格權受侵害」與「促進個人資料之合理利用」之情形下，如僅提供登記簿上委託人之姓名，即足以達成特定目的利用之本旨者，似不宜將姓名以外之其他個人資料併予提供。[117]

公布莫拉克風災後未與親人聯繫者之姓名，符合民政、戶政及戶口管理、社會行政之特定目的，且屬於內政部法令規定職掌必要範圍內。於公布前宜審慎斟酌公布之內容、程度及範圍，僅於可供一般人識別或判斷失蹤當事人身分之必要範圍爲之，例如：姓名、相片、性別、年齡等足資初步識別資料（不含出生年月日、身分證統一編號），以符合誠信原則與比例原則。且公布莫拉克風災後未與親人聯繫者之姓名，公布係於可供一般人識別或判斷失聯當事人身分同一性之程度及必要範圍內，雖有揭露失聯當事人之個人部分隱私，惟有利於各級主管機關結合民間力量協尋失聯民眾，健全民政、戶政管理或社會行政，降低政府協尋失聯民眾之成本，有利於公共利益之增進，適法性應無疑義。[118]惟是否得將上開個人資料公布於政府網頁或提供民眾閱覽，宜由主管機關審酌是否屬「公益上之必要」，以及執行通知義務而爲個人資料利用之方法（公布於政府網頁、提供民眾閱覽及其內容）有無逾越必要範圍予以判定。[119]
本件地方政府是否得將鄰長名冊建置網頁予以公布乙節，按該名冊爲經電腦處理之個人資料，除有其他法律明定應予公布，否則主管機關應於「公益」與「私益」間比較衡量決定之。[120]

本件於提供該新生兒之個人資料時，應注意所提供之資料，應以該學術研究有必要者爲限，與該學術研究無關之資料，則不得提供。[121]

於規劃「核發謄本注意事項」時，不論何種類之謄本，仍請參考上揭意旨，

[116] 法務部97 年2 月18 日法律字第0970005327 號函。
[117] 法務部93 年8 月31 日法律字第0930033677 號函。
[118] 法務部 98 年 11 月 9 日法律字第 0980036360 號函。
[119] 法務部 98 年 7 月 13 日法律字第 0980011751 號函。
[120] 法務部 95 年 7 月 19 日法律字第 0950021839 號函。
[121] 法務部 94 年 11 月 1 日法律字第 0940033446 號函。

一併審酌提供共有人或他項權利人除姓名以外之個人資料是否有其必要，如僅提供共有人或他項權利人之姓名，即足以達成特定目的利用之本旨者，似不宜將渠等除姓名以外之其他個人資料併予提供。[122]

拾貳、 特種資料禁止蒐集原則

按個人資料保護法第6條規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。三、當事人自行公開或其他已合法公開之個人資料。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，爲統計或學術研究而有必要，且經一定程序所爲蒐集、處理或利用之個人資料。前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。」可知，有關醫療、基因、性生活、健康檢查及犯罪前科等五類資料爲特種資料，除符合法定要件外，原則上不得蒐集、處理或利用。

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。[123]

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，原則上

[122] 法務部 93 年 3 月 24 日法律字第 0930012554 號函。
[123] 個人資料保護法第 6 條修正說明。

不得任意蒐集、處理或利用，惟如有法律明文規定者，自不在此限，爰爲第一款之規定。蒐集、處理或利用前述之特種資料，係屬公務機關執行法定職務或非公務機關履行法定義務，例如：檢警機關偵辦犯罪，蒐集或利用涉嫌人之犯罪前科資料；醫生發現疑似法定傳染病，蒐集相關醫療資料通報主管機關等，公務機關或非公務機關自得依法爲之，且依相關法令規定提供適當安全維護措施，爰仿一九九五年歐盟資料保護指令第八條(95/46/EC)及德國聯邦個人資料保護法第二十八條等外國立法例，而爲第二款之規定。[124]

再者，當事人已自行公開或其他合法公開之個人資料，隱私已無被侵害之虞，爰爲第三款之規定。基於統計或學術研究之目的，經常會蒐集、處理或利用前述之特種資料，惟爲避免寬濫，並加強保護特種或敏感個人資料，特規定適用本款限於爲基於醫療、衛生或犯罪預防等特定目的，且於統計或學術研究而有必要之範圍內，並經一定程序而爲蒐集、處理或利用之個人資料，始得蒐集、處理或利用，爰爲第四款之規定。[125]

爲確保依本條第一項第四款規定所爲因醫療、衛生或犯罪預防等目的而提供之個人資料，其提供者在合法必要範圍內提供，而蒐集者所蒐集之個人資料能獲得適當之安全維護，特種資料之提供者於其利用前，應特別審酌資料之提供範圍，以及提供時應經一定程序爲之。由於前開範圍、程序及其他應遵行事項，涉及個人資料是否經匿名化處理或依其揭露方式無從識別特定當事人，或者是否應得當事人明示之書面同意等之慎重考量，故授權由法務部會同特種資料之中央目的事業主管機關訂定相關特種資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，以保障當事人之特種個人資料，爰新增第二項規定。[126]

本條係新增條文，爲舊法所無，惟本條有關特種資料蒐集處理利用要件規定因過於嚴格，貿然施行對民眾及社會衝擊太大，乃被排除於新修正個人資料

[124] 個人資料保護法第 6 條修正說明。
[125] 個人資料保護法第 6 條修正說明。
[126] 個人資料保護法第 6 條修正說明。

保護法2012年10月1日生效條文之外。

拾參、 告知原則

一、直接蒐集個人資料之情形：

如前述，按個人資料保護法第8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。」可知，爲落實「告知後同意」原則，直接蒐集資料時，除符合得免告知情形者外，均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項。

由於個人資料之蒐集，事涉當事人之隱私權益。爲使當事人明知其個人資料被何人蒐集及其資料類別、蒐集目的等，於蒐集時應告知當事人之事項，俾使當事人能知悉其個人資料被他人蒐集之情形。原則上向當事人蒐集個人資料時，應告知當事人個人資料保護法第8條第一項所列事項，惟在部分特別情形下，或已有法律規定，或當事人已明知，履行第一項告知義務恐有礙職務之執行或無必要，爰於第二項規定得免告知之情形，其各款修正理由如次[127]：

1. 法律規定得免告知者，自勿庸再告知當事人第一項所列事項，爰爲第一款之規定。

2.資料之蒐集係公務機關執行其法定職務，例如：稅捐機關蒐集民眾收入所得資料；戶政機關蒐集民眾戶籍相關資料等，或非公務機關履行法律規定之義務，

[127] 個人資料保護法第 8 條修正說明。

例如：醫生發現疑似法定傳染病患者，應報告主管機關（傳染病防治法第二十九條）；各投保單位應備置蒐集僱用員工或會員名冊（勞工保險法第十條第一項）；金融機構對於達一定金額以上之通貨交易，應確認客戶身分及留存交易紀錄憑證（洗錢防制法第七條）等，爲提高行政效率，或避免執行上發生困擾，爰爲第二款之規定。

3.蒐集個人資料雖非屬公務機關之法定職掌，但公務機關執行其法定職務時，往往會涉及蒐集民眾之個人資料，例如：警察執行臨檢勤務；檢察機關偵辦刑事案件；行政執行機關辦理強制執行等，如依第一項規定告知當事人將發生妨害公務之執行時，自不宜告知當事人，爰爲第三款之規定。

4.履行第一項告知義務，如將妨害第三人之重大利益時，自得免爲告知，爰爲第四款之規定。

5.第一項規定之告知義務，其意旨在於讓當事人能充分瞭解資料蒐集之目的及用途。如當事人已明知應告知之內容者，自無必要再重複告知，爰爲第五之規定。

事實上，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，仍得依本法第三條規定請求查詢或閱覽；被請求之蒐集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。[128]

二、間接蒐集個人資料之情形：

按個人資料保護法第9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蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。有下列情形之一者，得免爲前項之告知：一、有前條第二項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人爲告知。四、

[128] 個人資料保護法第 8 條修正說明。

基於公共利益爲統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者爲限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。第一項之告知，得於首次對當事人爲利用時併同爲之。」亦可知，爲落實「告知後同意」原則，間接蒐集資料時，除符合得免告知情形者外，均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項。另爲減少勞費起見，允許得於首次對當事人爲利用時得併同告知。

個人資料保護法第9條部分，按蒐集個人資料除向當事人直接蒐集外，亦得自第三人取得之，此等間接蒐集個人資料，尤需告知當事人資料來源及其相關事項，俾使當事人明瞭其個人資料被蒐集情形，並得以判斷提供該個人資料之來源是否合法，並及早採取救濟措施，避免其個人資料遭不法濫用而損害其權益。是以，個人資料保護法第9條第一項明定間接蒐集個人資料者（因屬間接蒐集，自無從於蒐集時併爲告知），應於該資料處理或利用前，告知當事人資料來源及前條第一項第一款至第五款所列事項（第六款情形係屬當事人直接提供資料，於間接蒐集行爲，無從適用）。[129]

雖然，間接蒐集當事人之個人資料時，原則上應於處理該資料或利用前，告知當事人個人資料保護法第9條第一項所列事項。惟在部分特別情況下，告知恐有不宜或無必要，爰於第二項規定間接蒐集得免告知當事人之情形，其各款立法理由[130]如次：

1.第一款規定於直接蒐集個人資料時，得免告知義務，在間接蒐集時，亦得免爲告知，理由詳如前條說明。

2.間接蒐集之個人資料，如係當事人自行公開揭露或其他合法公開之資料，對其隱私權應無侵害之虞，自得免爲告知，爰爲第二款之規定。

3.爲保護當事人之權益，第一項規定間接蒐集個人資料時，應告知當事人相

[129] 個人資料保護法第 9 條修正說明。
[130] 個人資料保護法第 9 條修正說明。

關事項。惟客觀上顯然不能向當事人告知時，例如：當事人失蹤不知去向、昏迷不醒，亦無法得知其法定代理人爲何人時，自無從告知。另基於各款項內容之體系性安排，爰移列爲第三款規定。

4.基於統計或學術研究目的，經常會以間接蒐集方式蒐集個人資料，如依其統計或研究計畫，當事人資料經過匿名化處理，或其公布揭露方式無從再識別特定當事人者，應無侵害個人隱私權益之虞，應可免除告知當事人之義務。另爲避免以特定身分作爲排除告知義務之規範對象，刪除原修正條文學術研究機構等文字，以符合基於公共利益爲統計或學術研究之目的而有必要，且該資料須經處理後或依其揭露方式，無從識別特定當事人之客觀要件作爲判斷依據，爰爲第四款之規定。

5.大眾傳播業者基於報導新聞之目的，經常以間接方式蒐集特定人之個人資料，如需依第一項規定告知當事人資料來源等相關事項，恐會造成新聞報導之困擾。另揆諸一九九五年歐盟資料保護指令(95/46/EC)及部分外國立法例，亦有將新聞業者低度或排除適用之規定。又依中華民國報業道德規範之宗旨，自由報業爲自由社會之重要支柱，其主要責任在提高國民生活水準，服務民主政治，保障人民權利，增進公共利益與維護世界和平；新聞自由爲自由報業之靈魂，惟報紙新聞和意見之傳播速度太快，影響太廣，故應慎重運用此項權利。準此，新聞報導之目的應與上開宗旨相契合，以促進公共利益爲其最終目的。是以，爲尊重新聞自由及增進公共利益，爰爲第五款規定。

6.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，被請求之蒐集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。

另外，在間接蒐集個人資料之情形，原則上應於處理或利用前，向當事人告知個人資料來源等事項，但如能於首次對當事人爲利用時（例如：對當事人進行商品行銷），併同告知，不但能提高效率，亦可減少勞費，且無損於當事

人之權益，爰爲第三項規定。[131]

三、個人資料保護法修正施行前非由當事人提供之個人資料之情形：

個人資料保護法第五十四條規定：「本法修正施行前非由當事人提供之個人資料，依第九條規定應於處理或利用前向當事人爲告知者，應自本法修正施行之日起一年內完成告知，逾期未告知而處理或利用者，以違反第九條規定論處。」由於個人資料保護法修正條文擴大適用範圍，原本不受個人資料保護法規範從事個人資料蒐集、處理或利用者，修法後均將適用個人資料保護法，惟其在個人資料保護法修正施行前已蒐集完成之個人資料（該等資料大多屬於間接蒐集之情形），雖非違法，惟因當事人均不知資料被蒐集情形，如未給予規範而繼續利用，恐仍會損害當事人權益，是以自宜訂定過渡條款，明定一定期間內應向當事人完成告知，逾期未告知當事人仍處理或利用該資料者，則以違反第九條規定論處，期能兼顧當事人與資料蒐集者雙方權益。[132]

惟本條有關本法施行前間接蒐集個人資料應於一年內完成告知義務規定，過於嚴格，貿然施行對民眾及社會衝擊太大，乃被排除於新修正個人資料保護法2012年10月1日生效條文之外。

拾肆、 外洩通知義務

按個人資料保護法第12條規定：「公務機關或非公務機關違反本法規定，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。」可知，資料蒐集者於個人資料被竊取、洩漏、竄改或其他侵害時，應通知當事人。

雖然，按個人資料保護法第十八條及第二十七條第一項規定，應指定專人辦理安全維護事項或採行適當之安全措施，防止個人資料被竊取、竄改、毀損、

[131] 個人資料保護法第 9 條修正說明。
[132]個人資料保護法第五十四條修正說明。

滅失或洩漏。然而，於當事人之個人資料遭受違法侵害，往往無法得知，致不能提起救濟或請求損害賠償，因此，公務機關或非公務機關所蒐集之個人資料被竊取、洩漏、竄改或遭其他方式之侵害時，應立即查明事實，以適當方式（例如：人數不多者，得以電話、信函方式通知；人數眾多者，得以公告請當事人上網或電話查詢等），迅速通知當事人，讓其知曉，[133]避免損害發生或擴大，且得提起救濟或請求損害賠償。

公務機關違反個人資料保護法第12條規定而隱匿不為通知者，其上級機關應查明後令其改正，如有失職人員，得依法懲處；非公務機關違反本條規定而隱匿不為通知者，其主管機關得依個人資料保護法第四十八條第二款規定限期改正，屆期仍不改正者，得按次處以行政罰鍰。[134]

拾伍、 個人資料的跨國傳輸

關於個人資料的跨國傳輸，OECD為確保個人資料的跨國流通不受打斷，OECD上開「有關隱私權保護及個人資料跨國流通之準則」規定，會員國不得限制與其他會員國之間的個人資料流通，除非其他會員國未能提供同等的隱私保護或將再出口該個人資料而規避國內隱私法規。且會員國應避免以保護隱私或個人自由為名，制定某些超出OECD保護標準而構成個人資料跨國流通障礙之法律[135]。惟事實上，該準則僅具有道德上之拘束力，不具有強制拘束力，但其乃最低限制之基準[136]，仍提供許多國家或國際組織個人資料保護之立法參考。

歐洲理事會或歐洲委員會(The Council of Europe, CoE)於1981年制定「有關個人資料自動化處理保護個人公約」(the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)，其內容與OECD

[133]個人資料保護法第 12 條修正說明。
[134]個人資料保護法第 12 條修正說明。
[135] Jody R. Westby, American Bar Association, International Guide to Privacy 85-86 (2004); James Michael, Privacy and Human Rights— An International and Comparative Study, with Special Reference to Developments in Information Technology 40-41 (1994).
[136]許文義，「個人資料保護法論」，頁 161-163，台北，三民書局，2001 年 1 月。

「有關隱私權保護及個人資料跨國流通之準則」雷同，並於1999、2001年加以修訂。而按2001年「個人資料公約附加備忘錄」(Additional Protocol to the Personal Data Convention) 規定[137]，對於個人資料跨國傳遞至非締約國的限制，亦僅以該國未能提供充分水準的保障爲限。

如同CoE的「個人資料公約附加備忘錄」，歐盟資料保護指令亦限制將個人資料對外傳遞至保護標準低於歐盟的非會員國境內。按歐盟資料保護指令第25條[138]規定，個人資料禁止傳遞至歐盟疆界之外，除非個人資料接收國能夠提供「充分程度的保護」(an adequate level of protection)且經歐盟執委會或會員國資料保護主管機關的認可或符合法定的例外規定者。此項限制個人資料跨國傳遞的「資訊禁運」措施倘付諸實施，其威脅將十分巨大，例如，一家非歐盟會員國（如日本、台灣）的企業將難以蒐集及利用歐盟公民的個人金融資料，使得跨國金融業務將面臨癱瘓；同樣地，一家欲對於內部員工表現加以考核的多國籍公司，可能發現無法將相關雇傭紀錄由布魯塞爾傳遞至東京或台北。至於歐盟資料保護指令第25條的「充分程度的保護」的標準，則按個人資料的性質、蒐集目的及期間、接收國相關法令規範及安全保護措施等因素，綜合判斷[139]。迄今，僅阿根廷、加拿大、瑞士、歐盟與美國間的安全港協議、以及英國屬地的根西島(Guernsey)、馬恩島(the Isle of Man)、澤西島(Jersey)之相關法令經過歐盟執委會認定[140]提供充分程度的保護。

---

[137] Jody R. Westby, American Bar Association, International Guide to Privacy 89 (2004).

[138] According to Paragraph 1 of Article 25 of the EU Data Protection Directive, "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

[139] EU Data Protection Directive, art. 25 (2).

[140] Karin Retzer, Cynthia Rich, Morrison & Foerster LLP, GLOBAL SOLUTION FOR CROSS-BORDER DATA TRANSFERS: MAKING THE CASE FOR CORPORATE PRIVACY RULES, 38 Geo. J. Int'l L. 458 (Spring, 2007); Commission decisions on the adequacy of the protection of personal data in third countries, Available at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm (last visited August 31, 2012).

關於個人資料的跨國流通，按亞太經合會隱私綱領規定[141]，會員經濟體應審酌與個人資料保護有關之下列事項：(1)關於會員經濟體間之資訊交換：會員經濟體應(a)分享和交換對隱私保護有重大影響之資訊、調查及研究[142]；(b)分享調查違反隱私保護案件之各種技術與經驗[143]；(c)指定其管轄權內負責履行關於分享隱私保護相關資訊及執行跨國合作之主管機關，並通知予其他會員經濟體[144]；(2)關於調查與執行之跨國合作：會員經濟體應建構有助於跨國合作執行隱私保護相關法令之雙邊或多邊性機制[145]；(3)合作建構「跨境隱私規則」或「跨國隱私規則」(Cross-border Privacy Rules, CBPR)：會員經濟體應鼓勵「組織」或「機構」(organizations)建構及確保所採用的跨境隱私規則有助於保護個人資料及增進跨國資料傳遞，並不得對於跨國資料流通形成不必要的障礙（如不應對於企業或消費者增加額外的行政或官僚主義上之負擔[146]）。其中，如OECD前揭情形，同為APEC會員的澳洲及紐西蘭兩國隱私保護官2006年9月簽署的「協議備忘錄」，可視為雙邊協議方式實踐亞太經合會隱私綱領之資訊交換及跨國合作解決隱私議題的具體實例[147]。

關於我國對於個人資料跨國傳輸的規範，如同OECD、CoE或EU「限制個人資料的跨國流通，僅以資料接收國未能提供同等的隱私保護或將再出口該資

---

[141] Part B International Implementation of Part IV Implementation of APEC Privacy Framework, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited January 5, 2010).

[142] APEC Privacy Framework, para. 40, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited January 5, 2012).

[143] APEC Privacy Framework, para. 42, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited January 5, 2012).

[144] APEC Privacy Framework, para. 43, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited January 5, 2012).

[145] APEC Privacy Framework, para. 44, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited January 5, 2012).

[146] APEC Privacy Framework, para. 46 & para. 48, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1 (last visited January 5, 2012).

[147] Media Release: Australia & New Zealand - privacy regulators sign agreement, available at http://www.privacy.gov.au/materials/types/media/view/6246 (last visited July 5, 2012).

料而規避國內隱私法規者爲限」，我國亦有類似的機制。按個人資料保護法第二十一條：「非公務機關爲國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。」可知，按該條第一項第三及四款規定，非公務機關爲國際傳輸個人資料，而接受國對於個人資料保護未有完善之法規，致有損害當事人權益之虞者，或以迂迴方法向第三國(地區)傳輸個人資料規避本法者，中央目的事業主管機關得限制之。而所謂「國際傳輸」，不論是機關內部之資料傳送（屬資料處理），例如：總公司將資料傳送給分公司、公務機關將資料傳送給國外辦事處等；或將資料提供當事人以外第三人（屬資料利用），例如：母公司將資料提供給子公司或他公司、公務機關將資料傳送給他公務機關，只要該資料作跨國（境）之傳輸，不論是屬處理或利用行爲，皆屬本法所稱之「國際傳輸」。[148]

拾陸、 強化行政監督

按個人資料保護法第二十二條：「中央目的事業主管機關或直轄市、縣（市）政府爲執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員爲必要之說明、配合措施或提供相關證明資料。中央目的事業主管機關或直轄市、縣（市）政府爲前項檢查時，對於得沒入或可爲證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制爲之。中央目的事業主管機關或直轄市、縣（市）政府爲第一項檢查時，得率同資訊、電信或法律等專業人員共同爲之。對於第一項及第二項之進入、檢查或

[148] 個人資料保護法第 21 條修正說明。

處分，非公務機關及其相關人員不得規避、妨礙或拒絕。參與檢查之人員，因檢查而知悉他人資料者，負保密義務。」及個人資料保護法第二十三條：「對於前條第二項扣留物或複製物，應加封緘或其他標識，並爲適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。扣留物或複製物已無留存之必要，或決定不予處罰或未爲沒入之裁處者，應發還之。但應沒入或爲調查他案應留存者，不在此限。」可知，爲加強防制個人資料之濫用，中央目的事業主管機關或直轄市、縣（市）政府，發現非公務機關違反本法規定或認有必要時，得派員攜帶執行職務證明文件，進入檢查，如發現有違法情事，並得採取必要處分。

另外，按個人資料保護法第二十四條：「非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行爲不服者，得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議。前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府認爲有理由者，應立即停止或變更其行爲；認爲無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行爲逕行提起行政訴訟。」可知，中央目的事業主管機關或直轄市、縣（市）政府執行檢查時，所採取之措施，或相關強制、扣留或複製行爲，當事人如有不服，得聲明異議。

又非公務機關有違反個人資料保護法規定之情事者，按個人資料保護法第二十五條規定，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得爲下列處分：一、禁止蒐集、處理或利用個人資料。二、命令刪除經處理之個人資料檔案。三、沒入或命銷燬違法蒐集之個人資料。四、公布非公務機關之違法情形，及其姓名或名稱與負責人。中央目的事業主管機關或直轄市、縣（市）政府爲前項處分時，應於防制違反本法規定情事之必要

範圍內，採取對該非公務機關權益損害最少之方法爲之。再者，按個人資料保護法第四十七條規定，非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：一、違反第六條第一項規定。二、違反第十九條規定。三、違反第二十條第一項規定。四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。

拾柒、 團體訴訟制度之採用

按個人資料保護法第三十四條：「對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，由法院併案審理。其他因同一原因事實受有損害之當事人，亦得聲請法院爲前項之公告。前二項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認爲必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。依第一項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。」又按個人資料保護法第三十二條：「依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：一、財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。二、保護個人資料事項於其章程所定目的範圍內。三、許可設立三年以上。」可知，爲結合民間力量，發揮個人資料保護法保護個人資料之功能，乃增訂財團法人或公益社團法人符合個人資料保護法規定

者，得提起團體訴訟，以協助隱私權益遭侵害之當事人進行民事救濟。且爲鼓勵當事人透過團體訴訟主張權利，增訂團體訴訟裁判費減免之規定。

拾捌、 刑事責任：

按個人資料保護法第四十一至第四十六條，對於違法蒐集、處理或利用個人資料者，區別其是否具有「意圖營利」之主觀要件，課予程度不等之刑事責任。

拾玖、 不適用個人資料保護法規定之蒐集、處理或利用個人資料之情形

按個人資料保護法第五十一條第一項規定：「有下列情形之一者，不適用本法規定：一、自然人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。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」

依個人資料保護法第二條第八款規定，本法所稱非公務機關包括自然人，惟有關自然人爲單純個人（例如：社交活動等）或家庭活動（例如：建立親友通訊錄等）而蒐集、處理或利用個人資料，因係屬私生活目的所爲，與其職業或業務職掌無關，如納入本法之適用，恐造成民眾之不便亦無必要，因此，予以排除。再者，由於資訊科技及網際網路之發達，個人資料之蒐集、處理或利用甚爲普遍，尤其在網際網路上張貼之影音個人資料，亦屬表現自由之一部分。爲解決合照或其他在合理範圍內之影音資料須經其他當事人之書面同意始得爲蒐集、處理或利用個人資料之不便，且合照當事人彼此間均有同意之表示，其本身共同使用之合法目的亦相當清楚，因此，對於在公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，不適用本法之規定，回歸民法適用。[149]

[149]個人資料保護法第 51 條修正說明。

貳拾、 在我國領域外對於我國人民個人資料蒐集、處理或利用之情形

按個人資料保護法第五十一條第二項規定：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」由於科技之進步與網際網路使用普遍，即使在我國領域外蒐集、處理或利用國人之個人資料，亦非常容易。爲防範公務機關或非公務機關在我國領域外違法侵害國人個人資料之隱私權益，以規避法律責任，因此，明定在我國領域外，亦有本法之適用。

第四章　個人資料保護法的施行對台北市現行法規的衝擊暨其因應之道

第一節　警察局

壹、　訪談大要

一、 台北市政府警察局內各組織職掌業務涉及個人資料保護法之相關範圍

(一) 行政科

負責勤務規劃、警力配置等業務，如警察實施臨檢時所蒐集之個人資料、舊法電腦處理個人資料保護法下，法務部有函釋[1]其他單位不得不當利用警察執行臨檢所取得之資料。

(二) 保安科

槍砲彈藥之管制，針對持有人之身分，如槍照、刀照等。

(三) 訓練科

針對警察局內部人員之管理，如常年訓練之資料、公務人員終身學習時數之登錄、警察教育訓練進修、員警心理諮商輔導工作之策劃、執行與評核事項等資料。

(四) 戶口科

戶口查察之規劃推行及督導考核等事項。如口卡片，曾發生看守所要求提供口卡片資料作犯罪嫌疑人身分之比對，法務部有函釋[2]認應拒絕。且對於有前科素行之人亦會作訪查。另戶口科之業務亦有包含每季須調查是否有警察非因公務而濫用戶政資料之情形，若有違反將對該員警作行政處分。

[1] 法務部，101 年 1 月 20 日法律司字第 1000700819 號解釋。
[2] 法務部，92 年 9 月 3 日法律字第 0920037612 號解釋。

(五) 民防科

處理民防團隊編訓、防護之事項，如義警人員之名冊資料。

(六) 外事科

其業務涉及外僑管理、外國團體安全維護、駐華使領館與官員保護、外賓安全維護、涉外案件處理、歸國華僑安全維護等事項。例如良民證、涉外案件報告表。

(七) 後勤科

處理警察局內部人員之財產管理、廳舍營繕等事項。如內部人員之交通補助費、員警單身宿舍申請人之資料。

(八) 犯罪預防科

監視器之管理、守望相助隊及里長之資料。

(九) 秘書室

針對公文管理，檔案歸檔。

(十) 督察室

處理員警申訴、考核、教育輔導、違法犯紀查處、傷殘慰問救助等事項，如員警之風紀考核資料、考績資料。

(十一)　保防科

針對機密保護、防制滲透、安全資料蒐集處理及其他有關安全業務事項。如國防部若有施作工程時，要求警察局協助作身家調查。

(十二)　政風室

針對警察局內部員工之身家調查、財產申報部分。

(十三)　法規室

於處理國家賠償、訴願案件時，將涉及個人資料。

(十四)　公共關係室

處理與大眾傳播媒體、民意機關、公眾社團之聯繫事項，像與議員、媒體、警友會間之關係。如議員要求警局提供資料，現有「議員索取或調閱資料之處理原則」之規範。其中第一點針對議員索取資料之限制，雖有明定涉及個人隱私時應限制，惟其定義模糊，恐仍採個案判斷之方式，未有一統一標準。

(十五)　資訊室

警政資訊系統規劃與發展、電腦軟硬體設施操作、管理與維護、資訊教育訓練等事項。如統整各單位之資料，委託資策會利用軟體將個人資料作統整，以及防範個人資料從不正當的管道外洩。另外亦可再利用該統整後的資料庫，但其利用之權限設有條件限制。

(十六)　勤務指揮中心

警察勤務之指揮、聯繫與最新治安狀況之控制、一一Ｏ報案管理等事項。

(十七)　刑事鑑定中心

刑案現場勘察，證物處理、鑑識、分析，影像處理，罪犯照片沖洗、建檔及語音蒐證鑑定等事項。其中犯罪現場勘查之資料，如 DNA 係送交刑事局。

(十八)　民防管制中心

防情業（勤）務規劃、執行、演（訓）練等事項，如組訓人員之基本資料。

以下爲臺北市政府警察局刑事警察大隊內之特殊單位：

(一) 司法組

司法警察之業務，如經手移送書等。

(二) 肅竊組

如竊盜案件之個人資料。

(三) 經濟組

經濟犯罪相關業務等事項，如詐欺案件之個人資料。

(四) 紀錄組

查捕逃犯（兵）、犯罪紀錄運用及犯罪紀錄業務事項，如統計移送的案件數量，僅收集資料，無後續處理利用。

以下爲臺北市政府警察局少年警察隊職掌之特殊單位：

(一) 預防組

如少年事件之紀錄。

(二) 偵查組

少年警察隊處理少年刑事案件之資料。如校園查訪、校園安全維護、少年事件處理等資料。

二、 台北市政府警察局針對個人資料保護法施行後之標準作業流程(SOP)的欠缺一般係依據警政署頒布之標準作業流程來運作，但針對新的個人資料保護法施行後，尚未頒布標準作業流程。但警政署目前有計畫將依照新施行之個人資料保護法重新檢視過往頒布之內部作業流程是否有牴觸之處。

現階段若遇到個人資料保護法之問題，若是一般刑事案件，基於偵查不公開大多傾向以遮蔽方式處理，且以保護當事人權益爲考量；其他非刑事案件，則通常個案處理，如裁決書、遺失物遺失時，以往並不會披露出民眾之全名。

三、 北市警察局針對機關與機關之間，若有請求調閱資料之情況下，曾發生過建管處來函要有警察局提供受裁罰之人的戶政資料，通常警察局會拒絕提供。

四、 各員警使用之電腦均與戶政機關的系統連線，可直接查詢民眾的個人資料(戶籍資料、前科紀錄、車籍紀錄及欠費繳款紀錄)，而查詢的標的種類權限亦會針對各科室的業務範圍作限制，平均一個月高達十幾萬筆查詢數量，市警局無事前作防範個人資料外洩的規範，多採事後的稽查，由資訊室及政風室每季至各單位作稽查，針對是否有非因公務查詢之情形。而事後稽查的判斷標準，由於並無統一之標準，目前以過往辦案經驗累積，大致上以有查詢量是否異常、時間點及是否有遭人檢舉作判斷。

五、 針對現行個人資料保護法第 18 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。」台北市府警察局目前有設防火牆來防止外來具有攻擊性之網站。另外針對內部電腦產品故障或淘汰的處理方式，係委由廠商作報廢、捐贈或回收再利用，但事前會先作消磁的動作，惟特殊單位之電腦會控管不作捐贈或回收再利用。

六、 依個人資料保護法第 17 條規定，「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、個人資料類別。」目前台北市警察局亦已作成「臺北市政府警察局保有及管理個人資料之項目彙整表[3]」，並公開在台北市政府警察局網站中的個人資料保護專區內供大眾下載，且其公開之資訊僅有檔案名稱，並不會有該檔案中的詳細資料。惟是否會因有此項公開之檔案名稱，而造成有心人士藉由得之檔案名稱而突破防火牆之防範而取得該檔案之詳細內容，仍待觀察。

七、 若民眾要求警察局提供監視器之影像，必須先完成報案之程序後始有取得之權利，且影像資料之提供分爲四種，分別爲發布影像、調閱或閱覽、複製、拍攝(即翻拍)，而警局目前提供予民眾僅有調閱之權利。若民眾因訴訟上需要複製影像來保全證據時，則要求民眾先向地檢署或法院申請，由地檢署或法院來函後，警察局以函覆之方式複製影像予地檢署或法院。惟若民眾基於緊急之情況，例如，影像檔案將被洗掉時(原則上影像儲存時間爲一個月)，目前並無類似即時強制之手段可供民眾行使，有侵害民眾權利之虞。

八、 現監視器系統主要架設於易發生犯罪之地點、重要之路口、重要之巷弄，而此目的在用來追蹤犯罪嫌疑人進入犯罪現場及離開犯罪現場之路線。因臺北市錄影監視系統設置管理自治條例仍爲草案，故現仍依臺北市錄影監視系統設置管理暫行辦法之規範，該辦法對監視器之使用目的上限縮於兩種型態，一爲刑案之偵查案件、另一爲交通事故案

[3] 詳細網址 http://www.tcpd.taipei.gov.tw/content.asp?Cuitem=13783879&mp=108001

件。

且現已設有 44 套 LPR 車牌辨識系統(數位序碼檢識系統 License Plate Recognition Systems)，設置地點於台北市與新北市間的聯外橋梁道路中，該系統可將經過之車輛擷取其車牌號碼，直接連結贓車資料庫系統中比對。且未來預計增設 500 支 LPR 車牌辨識系統於台北市之重要路口。

九、 監視器之運用上並不會移作行政罰(例如交通違規上)之用。先前環保局亦有要求提供監視器影像作爲取締垃圾違規之證據，基於隱私權保障及比例原則，亦拒絕之。

貳、 個人資料保護法與警察行政之衝擊──以「監視器」為討論中心

一、 前言

按監視系統對個人之基本權影響甚鉅，主要涉及到隱私權與自由權。事實上，設置監視系統所涉之基本權可分爲：（一）資訊自決權或資訊隱私權，以及（二）行爲自由[4]。實務上設置監視器一直存在著憲法上之爭議。

本報告研究期間，正逢台北市議會討論以自治條例之方式－即「台北市錄影監視系統設置管理自治條例」（草案）規範台北市的錄影監視系統。而現行實務上，台北市對於錄影監視系統僅有透過行政規則或內部規定爲管理。目前有由台北市政府所定之「台北市錄影監視系統設置管理暫行辦法」與台北市政府警察局

[4] 詳情請參閱李震山，從公共場所或公眾得出入之場所普設監視器論個人資料之保護，東吳大學法律學報第 16 卷第 2 期，2004 年，第 57 頁到第 67 頁。

所定之「台北市政府警察局管理錄影監視系統注意事項」及「台北市政府警察局錄影監視系統影像處理、利用補充規定」。因此，以下將就 101 年 10 月 1 日才生效之「個人資料保護法」對於上開規定之影響做分析，並探討上開規定與錄影監視系統之設置實務上可能會遇到的問題。

二、　個人資料保護法是否適用於錄影監視系統（監視器）之探討

關於個人資料保護法是否適用於錄影監視系統（監視器），可按錄影監視系統（監視器）所蒐集、處理或利用之影音資料是否於公開場所或公開活動中所爲之，以及是否與其他個人資料結合，而分別加以探討之：

(一) 監視器於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料

按外國立法例，爲了避免個人資料保護法制對人民之其他自由權（例如言論自由、新聞自由等）或日常生活造成妨礙，設計上多有排除適用之規定。[5]而我國法的排除規定在上開個人資料保護法第 51 條第 1 項：「有下列情形之一者，不適用本法規定：一、自然人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。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」問題之緣起即在於，倘利用監視器針對公共場所或公開活動爲攝錄所得之影音資料且未與其他個人資料結合者，是否可以援引個人資料保護法第 51 條第 2 款之「於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料」而主張不適用個人資料保護法之規定？對此，則有不同見解，詳如下述：

[5] 劉定基，同前註 36，第 51 頁。

1、個人資料保護法不適用於監視器於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料之依據

按個人資料保護法第 51 條第 1 項第 2 款規定：「有下列情形之一者，不適用本法規定：二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」可知，經由監視器於公開場所或公開活動中所蒐集、處理或利用之個人影音資料，倘未與其他個人資料結合者，則不適用個人資料保護法。

又按於個人資料保護法修正之前，關於金融機構「營業處所前道路」納入攝錄範圍適法性疑義乙案，法務部曾對舊法作成 99 年 4 月 13 日法律字第 0999009760 號函釋，其主要內容為：「……二、按電腦處理個人資料保護法（以下簡稱個資法）第 3 條第 1 款及第 4 款規定：『個人資料：指自然人之姓名、出生年月日、身分證統一編號…及其他足資識別該個人之資料。』『蒐集：指為建立個人資料檔案而取得個人資料。』另個資法施行細則第 2 條亦規定：『本法所稱個人，指生存之特定或得特定之自然人。』本件貴署提案修正『金融機構安全維護管理辦法』第 5 條第 6 款，擬將金融機構『營業處所前道路』納入攝錄範圍，其取得之資料須為建立個人資料檔案而取得足資識別該個人之影像資料，予以電腦處理者，始有個資法之適用。若尚無建立個人資料檔案，且僅錄存不特定自然人影像而未予識別該個人以前，相關監視錄影系統之設置管理問題，應無個資法之適用，合先敘明。三、次按所謂隱私權，乃係不讓他人無端地干預個人私領域之權利（臺灣高等法院 93 年度上更（一）字第 19 號民事判決參照）。此種人格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，爲司法院釋字第 585 號及第 603 號解釋所揭示。惟人群共處，營社會生活，應受保護之隱私必須有所界限，即對隱私須有合理期待，如當事人欠缺對隱私合理期待時，自難認其隱私遭受侵害（王澤鑑著「人格權保護的課題與展望（三）人格權的具體化與保護範圍（6）－隱私權」，刊於台灣本土法學第 99 期，96 年 8 月，頁 53-54）。本件金融機構『營業處所前道路』，一般情形下應非『個人生活私密領域』，來函所詢將其納入攝錄範圍有無侵犯『社會大眾隱私權』乙節，應視民眾對於上揭場所之活動有無隱私合理期待而定，請參考前開說明，本於職權自行審認之。又本件『營業處所前道路』裝設監視器，係基於偵查犯罪之目的，有無涉及警察職權行使法第 10 條之適用，請一併注意。」按上開法務部之見解，認爲監視系統（此案例事實爲金融機構所裝置）所錄得之影像等資料，如「非爲建立個人資料檔案」且「未識別該人」者，即不適用電腦處理個人資料保護法。[6]再者，金融機構「營業處所前道路」，倘當事人欠缺對隱私合理期待時，自難認其隱私遭受侵害。

然而，就 101 年 10 月 1 日才生效之個人資料保護法第 2 條第 1 項第 3 款規定：「蒐集：指以任何方式取得個人資料。」可知，蒐集不以「建立個人資料檔案」而取得個人資料爲限，凡以「任何方式取得個人資料」均是。又監視錄影系統所取得之個人影像資料是否屬於個人資料保護法第 2 條第 1 項第 1 款規定之「得以直接或間接方式識別該個人之資料」不無再探討之餘地。據此，法務部上開解釋在新修正的個人資料保護法生效後，是否繼續有適用性，大有疑義。

[6]劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外－以監視錄影爲例（上），月旦法學教室第 115 期，2012 年，第 51 頁。

２、個人資料保護法適用於監視器於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料之見解

(1) 監視器所蒐集、處理或利用之影音資料並非個人資料保護法第 51 條第 2 款立法目的所容許之合理範圍

觀察個資法第 51 條第 2 款之規定，可將其分成兩個要件：第一，影音資料須在「公共場所或公開活動」中所蒐集、處理或利用。第二，影音資料須「未與其他個人資料相結合」。就第一個要件而言，參考論者所謂：「基於資訊科技及網際網路的發達，個人資料的蒐集、處理及利用甚爲普遍，尤其在網際網路上張貼之影音個人資料，亦屬表現自由之一部份，爲解決合照或其他在合理範圍內之影音資料須經其他當事人之書面同意始得爲蒐集、處理或利用個人資料之不便，加諸合照當事人彼此間均有同意之表示，其本身共同使用之合法目的相當清楚，是於公共場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，亦不適用本法之規定。[7]」另有學者指出，在這裡的典型案例有：「戶外旅遊的合照」、「公開研討會的合照或錄音」[8]。由此可知，個資法第 51 條第 2 款之在「公共場所或公開活動」中所蒐集、處理或利用之影音資料，應限於人與人乃至於團體間之影音資料，此時當事人有充分地互動，而且事實上當事人已就此處的蒐集、處理或利用已有明示或默示的同意。例如在出外旅遊合影之情形，所有入鏡的人應該都可以瞭解到拍照之目的爲何（如爲了留作紀念）、照片的後續利用爲何（如上傳到 facebook）。因此，這裡的「公共場所或公開活動」之蒐集、處理或利用應該是社會生活中極爲常見的。

[7] 呂丁旺，修正《個人資料保護法》的釋義與實踐（上），國會月刊第 38 卷第 11 期，2010 年，第 26 頁。

[8] 林秀蓮，「個人資料保護法」初探，萬國法律第 176 期，2011 年，第 3 頁。

然而在監視器所錄得之影音資料，並非爲了與他人爲任何交流，而係裝置者單方面爲蒐集、處理或利用。以監視系統爲蒐集、處理或利用所因應的狀況不是社會生活中的常態，而是如犯罪等異常情形。且在攝錄前倘未告知當事人，則當事人根本不會知道有此監視器之存在，遑論得到當事人同意，是以此處即有透過個人資料保護法保障當事人權利之必要。

(2) 監視器於公開場所或公開活動中所蒐集、處理或利用之影音資料不應完全不受法律保護

針對公開場所(如前開法務部 99 年 4 月 13 日法律字第 0999009760 號函釋所指之金融機構「營業處所前道路」)或公開活動中所蒐集、處理或利用之個人資料(如影音資料)是否即完全欠缺「隱私的合理期待」(reasonable expectation of privacy)而不受資訊隱私權或個人資料保護法之保護？換言之，個人資料是否限於未經公開而具有私密性者才受資訊隱私權保障？

論者主張：「一般來說，在公共場所，人們請求他人加入宗教團體、在圖書館自習或社會人際方面的活動，這些個人層面中和公眾生活有深切關係的部份，固然可能被其他人所攝錄，但第三人和國家最大的區別在於－『第三人不太可能知道何時我們會出現在哪或我們是誰』，以及『第三人通常只是過客而僅占行爲人人生片段中短暫的一瞬』」[9]亦即，一般狀況下對公共場所或公開活動中所爲的蒐集、處理或利用只是短暫的、片段的、偶而爲之的。然而，監視系統的建置卻是長期的、全面的、有計劃的蒐集大眾之個人資料。

日本學說亦有認爲，置身於公共場所之個人，與他人間具有「匿名性」與「暫時性」之特性，亦即除特別情況外，多爲偶然相遇、一瞬間之印象。反觀監視系統之使用，紀錄後之影帶可長久保存，即不符所謂之「暫時性」。再加上公務機關如警察機關等，原即掌握大量個資，倘加以紀錄、分析、比對及追蹤後，將可

[9] 柯玉倫，論設置監視器的憲法疑義，國立台北大學法律學系碩士論文，2009 年，第 110 頁。

對個人之私生活有所掌握，前開之「匿名性」亦不復存在矣[10]！正如學者 Edward Bloustein 之見解，倘一個人的每一種想法、需要或慾望皆公諸於世而持續地受到嚴密審視(scrutiny)，其個人特性及人性尊嚴將因此受到剝奪；而由於被赤裸裸地攤在陽光下，其意見將不敢與眾不同、其志向也不敢標新立異、所流露的感情也喪失個人獨特性而流於媚俗；如此的人類雖是有感覺的，但只是可互相替代的，因此，不再是一個獨立個體了[11]。因之，監視系統所得的個人資料是否會遭到濫用，委實令人憂心，故必須受到法律的規範。否則，個人資料的濫用會對當事人言行舉止、人際互動或社會生活產生「寒蟬效應」。[12]

又對此，林子儀大法官在司法院大法官第六○三號解釋協同意見書提及：「所謂已公開的資訊即不受隱私權之保障，並非的論。至多僅得謂：已為眾所週知或相當多數之人所知之資訊，或個人自願公開之資訊，並在其授權公開之範圍內，即難以再主張受到隱私權之侵害。且基於重視個人資訊隱私權之保障之觀點，縱係個人自願公開資訊下，也不意謂第一次的授權之後，個人對其自願公開之資訊即因此完全喪失控制，而不能對違反其授權目的或範圍的侵害行為有所主張。……將資訊隱私權所欲保護之對象限於個人私密之資訊，毋寧過分限縮，而不能因應現今資訊科技發展所可能對個人造成之侵害。蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。本院釋字第五八五號解釋亦係有鑑於此，而將個人資訊之自主控制權納入隱私權保障範圍內，不限於個人秘密不受揭露的自由。」

---

[10] 范姜真媺，監視攝影系統設置、使用之法律問題，律師雜誌第 307 期，2005 年，第 33 頁。

[11] Jeanette Teh, *Note, Privacy Wars in Cyberspace: An Examination of the Legal and Business Tensions in Information Privacy*, 4 Yale Symp. on L. & Tech. 1, 13-14 (2001-2002).

[12]劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外－以監視錄影為例（下），月旦法學教室第 119 期，2012 年，第 54 頁。

再按我國個人資料保護法第 2 條第 1 項第 1 款規定:「 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」可知，適用於隱私權或個人資料保護法保障範圍之個人資料，亦不限於未經公開而具有私密性者。

至於，公共場域中得合理期待其私密領域不受他人干擾之自由或個人資料自主之範圍，按司法院大法官第六八九號解釋理由：「基於人性尊嚴之理念，個人主體性及人格之自由發展，應受憲法保障（本院釋字第六０三號解釋參照）。爲維護個人主體性及人格自由發展，除憲法已保障之各項自由外，於不妨害社會秩序公共利益之前提下，人民依其意志作爲或不作爲之一般行爲自由，亦受憲法第二十二條所保障。人民隨時任意前往他方或停留一定處所之行動自由（本院釋字第五三五號解釋參照），自在一般行爲自由保障範圍之內。……爲人民免於身心傷害之身體權、行動自由、生活私密領域不受 侵擾之自由、個人資料之自主權。其中生活私密領域不受侵擾之自由及個人資料之自主權，屬憲法所保障之權利，迭經本院解釋在案（本院釋字第五八五號、第六０三號解釋參照）；免於身心傷害之身體權亦與上開闡釋之一般行爲自由相同，雖非憲法明文列舉之自由權利，惟基於人性尊嚴理念，維護個人主體性及人格自由發展，亦屬憲法第二十二條所保障之基本權利。對個人前述自由權利之保護，並不因其身處公共場域，而失其必要性。在公共場域中，人人皆有受憲法保障之行動自由。惟在參與社會生活時，個人之行動自由，難免受他人行動自由之干擾，於合理範圍內，須相互容忍，乃屬當然。如行使行動自由，逾越合理範圍侵擾他人行動自由時，自得依法予以限制。在身體權或行動自由受到侵害之情形，該侵害行爲固應受限制，即他人之私密領域及個人資料自主，在公共場域亦有可能受到干擾，而超出可容忍之範圍，該干擾行爲亦有加以限制之必要。蓋個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響

其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者。」可知，人民隨時任意前往他方或停留一定處所之行動自由，自在一般行為自由保障範圍之內。而個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護，惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限。進一步言，個人資料(如影像)之蒐集倘係於「公眾得出入場所」進行，「但吾人於公眾場所之行動，在『目視可能及範圍』內(目視原則)，固然沒有隱私合理期待，但超過『目視可能』，而以儀器器材進行人身動作及影像的蒐集，或超過『目視範圍』則屬可主張隱私權的範疇。」[13]

綜上，監視器於公開場所或公開活動中所蒐集、處理或利用之影音資料不應完全不受法律保護，仍應有受隱私權或個人資料保護法保障之餘地。

(3) 監視器於公開場所或公開活動中所蒐集、處理或利用之影音資料將易於與其他個人資料結合

再就個人資料保護法第 51 條第 2 款之第二個要件「影音資料未與其他個人資料結合」而言，在一般狀況下，例如參加某次婚宴後，新人與眾賓客合影。而這張照片只會作留念之用，我們會發現「某人的身影出現在這張照片上」，但是拍攝這張照片並非用來找出「這個人到底是誰？」、「住在哪裡？」。相較於以監視器取得個人資料的情形，學說認為：縱然在監視系統攝錄當時未與個人資料

[13] 李惠宗，憲法要義，頁 385，元照出版有限公司，2012 年 9 月。

連結，似符合第二款之規定，惟此等影音資料的蒐集、處理與未來利用均以識別特定個人爲主要目的[14]。

換言之，即使監視器係當下機械式的將攝錄範圍內的影像統統記錄下來，可是蒐集、處理與利用這些影像時必定會與其他個人資料相結合。例如說雖然某支監視器只是單純拍攝某條道路，但是警方會過濾這支監視器所有的畫面，試圖找出嫌疑犯的身影，找到嫌疑犯的身影後，還會進一步比對，發掘更多的資訊，如找出他的姓名、地址等等。也就是說，以監視器取得他人的個人資料，就是爲了要以此項個資爲線索，進而追根究底，取得更多個人資訊，本質上即不可能符合個人資料保護法第 51 條第 2 款之第二個要件之「不與其他個人資料結合」的要求！更何況監視系統通常係政府所建置，或許監視器只能取得一小部份個人資料，但政府絕對有資源且有能力藉由這一丁點個人資料去挖掘出全部的個人資料！參考上述日本學界對「匿名性」的要求，如何不令人憂心監視系統是否會遭到濫用！安能謂此時不適用個人資料保護法之規定乎？

又個人資料保護法修正施行後，有學者認爲，個人資料保護法的保護客體已包含「得以間接方法識別的個人資料」，且監視攝影的目的就在於「將來可識別特定人」，況縱然未實際識別，仍有可能遭濫用，以致於侵害人民權利。因此，監視器在新法修正後，即應受新個人資料保護法之規範。[15]蓋監視器的爭議一直存在，衡諸個人資料保護法第 1 條「爲規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」保護個人人格權之精神，不應使監視器成爲個人資料保護法的「漏網之魚」。

3、小結

由於監視錄影系統之事實樣態與一般社會生活中在公開狀況下蒐集、處理或利用他人個人資料並不完全相同，且監視器有侵犯人權之虞，因此本文以爲，在

[14] 同前註
[15] 同前註

監視系統的情形，不符合個人資料保護法第 51 條第 2 款規定之要件，故不應排除個人資料保護法之適用。

此外，實務上設置監視器一直存在著憲法上之爭議，而林子儀大法官在其就釋字第 603 號解釋的協同意見書中提到：「如果一個社會裡的成員，人人皆盡透明，沒有什麼動態可以逃脫於國家的監視之下，所有成員的資訊都鉅細靡遺地掌握在國家機器之中，並且可以輕易地透過某一則個人資訊追溯其全部行蹤與活動，這或許將是一個零犯罪的社會，而且很可能是一個非常有效率的政府，但人們也可能將過著充滿被監視恐懼的生活。治安與效率都是國家應該追求之重大公益，惟其終究必須停留在某個界限之後，不能無止境地一昧向前，犧牲其他一切。」[16]。雖然釋字第 603 號解釋是關於戶籍法要求全民指紋建檔之案例事實，惟監視器同樣有可能淪爲統治者「監控」或「追蹤」人民的工具，一如著名小說「一九八四」或電影「全民公敵」中的情節。學者陳運財更將個人之指紋與監視攝影相比較，氏認爲：就量而言，公共場所下之監視攝影較採集指紋涉及更廣泛之不特定人；就質而言，公共場合下之肖像或舉止之隱私性故較指紋爲弱，惟肖像或舉止倘一經紀錄，被濫用的可能性更高。況一整天二十四小時，機械性、長時間的攝影，所造成之侵害遠較指紋資訊爲大！[17]據此，對於監視錄影系統，不僅釋字第 603 號解釋所建構之資訊隱私權原則應有其適用性，亦應有必要受個人資料保護法規範之必要。

其實，在本報告所進行之訪談過程中，台北市政府警察局相關業務負責同仁即有所認知，即使監視系統可以依個人資料保護法第 51 條第 2 款之規定而不適用個人資料保護法，但警察局仍會持續踐行個人資料保護法所規定之各項義務。對此，本文認爲，台北市政府警察局堅持保護民眾個人資料與資訊隱私權之立場，符合現代法治國家之保障人民基本權利之精神，實值得肯定。

[16]林子儀，釋字 603 號解釋協同意見書，釋字 603 號解釋抄本，2005 年，第 63 頁。請參閱 http://www.judicial.gov.tw/constitutionalcourt/uploadfile/C100/%E6%8A%84%E6%9C%AC603.pdf

[17] 陳運財，監視攝影與正當程序之保障，台灣本土法學第 85 期，2006 年，第 89 頁。

(二) 監視器於公開場所或公開活動中所蒐集、處理或利用之與其他個人資料結合之影音資料

由於監視器涉及個人資料之蒐集、處理或利用，故如前揭，按我國個人資料保護法第 51 條第 1 項第 2 款規定：「有下列情形之一者，不適用本法規定：二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」可知，監視器所爲個人資料之蒐集、處理或利用，不適用個人資料保護法之情形，限於（一）於公開場所或公開活動中所蒐集、處理或利用之影音資料、及（二）未與其他個人資料結合。否則，雖於公開場所或公開活動中所蒐集、處理或利用之影音資料但當時或其後與其他個人資料結合(例如，因爲追查某特定罪犯而去調閱原本未與其他個人資料結合之錄影畫面)者，均有適用個人資料保護法之餘地。

（三）監視器於非公開場所或非公開活動中所蒐集、處理或利用之與其他個人資料結合或未與其他個人資料結合之影音資料

如同上述，按我國個人資料保護法第 51 條第 1 項第 2 款規定，可知，倘於非公開場所或非公開活動中所蒐集、處理或利用之影音資料者，不論當時或其後是否與其他個人資料結合者，均有適用個人資料保護法之餘地。

三、 個人資料保護法中涉及「台北市自治法規所規範之監視器」之相關條文分析

如前揭，經由監視器所蒐集、處理或利用之影音資料，在諸多情形中，將會有個人資料保護法之適用。因此，僅就新修正之個人資料保護法中涉及「台北市自治法規所規範之監視器」之相關條文，分析如下：

（一）於公共場所或公眾得出入場所蒐集、處理或利用之個人資料：個資法第51條

按「台北市錄影監視系統設置管理暫行辦法」第3條規定：「本辦法所稱錄影監視系統，指針對公共場所或公眾得出入場所設置之攝錄影音設備。」按「台北市政府警察局管理錄影監視系統注意事項」第2條規定：「本注意事項所稱錄影監視系統，係指本局基於治安需要，於臺北市公共場所或公眾得出入場所建置、維護之攝錄影音設備。」又按「臺北市錄影監視系統設置管理自治條例（草案）」第3條規定：「本自治條例所稱錄影監視系統，係指針對本市公共場所或公眾得出入場所設置之攝錄影音設備。」可知，台北市相關自治法規所規範之監視器主要係指，於臺北市公共場所或公眾得出入場所建置、維護之攝錄影音設備。至於，非於公共場所或公眾得出入場所設置之攝錄影音設備，則不在適用之列。

由於監視器所蒐集之影音資料應屬個人資料保護法所規範之個人資料，應無疑義，惟既然監視器係設置於公共場所或攝錄公開場合，則依據個人資料保護法第51條第第1項第2款之規定，是否可排除個人資料保護法之適用呢？已詳如前述。

（二）蒐集、處理或利用個人資料之法律依據：個資法第15條、第16條

按我國新修正的個人資料保護法第15條1項規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之

一者：公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人書面同意。三、對當事人權益無侵害。」第 16 條 1 項本文規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。」可知，除經當事人書面同意或對當事人權益無侵害外，公務機關經由監視器進行個人影音資料之蒐集、處理或利用，應屬於「執行法定職務必要範圍內」。因此，公務機關欲合法經由監視器進行個人影音資料之蒐集、處理或利用，必須探討其是否有法律授權。

按「台北市錄影監視系統設置管理暫行辦法」第 1 條規定：「臺北市政府（以下簡稱本府）為健全本府所屬各機關及里辦公處錄影監視系統設置管理，以維護治安，並兼顧人民權益保障，特訂定本辦法。本府所屬各機關及里辦公處錄影監視系統之設置及管理，依本辦法之規定。本辦法未規定者，適用其他法規之規定。」又按「台北市政府警察局管理錄影監視系統注意事項」第 2 條規定：「本注意事項所稱錄影監視系統，係指本局基於治安需要，於臺北市公共場所或公眾得出入場所建置、維護之攝錄影音設備。」及第 4 條規定：「錄影監視系統攝錄影像資料之處理、利用，以治安維護、交通事故處理有必要者為原則，並恪遵『檢察、警察暨調查機關偵查刑事案件新聞處理注意要點』等相關規定。」 再按「臺北市錄影監視系統設置管理自治條例（草案）」第 4 條規定：「錄影監視系統之設置，應以維護公共安全、社會秩序、預防及偵查犯罪有必要者為限，且應以對人民權益侵害最少之適當方法為之。」綜上可知，除其他法律另有規定外，上開法律規定某程度上或可做為台北市政府所屬之公務機關經由監視器進行個人影音資料之蒐集、處理或利用之法定職務之法律依據。由於個人影音資料之蒐集、處理或利用可能涉及人民基本權利（如隱私權、遷徙自由、表現自由）之限制，按憲法第 23 條規定：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要者外，不得以法律限制之。」上開「台北市錄影監視系統設置管理暫行辦法」及「台北市政府警察局管理錄影監

視系統注意事項」之行政命令恐難謂符合憲法第 23 條「法律保留」之要求，因此，「臺北市錄影監視系統設置管理自治條例（草案）」或類似位階之法律應儘速完成立法爲當。

（三）蒐集、處理或利用個人資料之特定目的：個資法第 15 條、第 16 條

按我國個人資料保護法第 15 條規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人書面同意。三、對當事人權益無侵害。」第 16 條本文規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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。」可知，個人資料蒐集、處理或利用之特定目的應加以明確化。

查現行「台北市錄影監視系統設置管理暫行辦法」第 4 條第 1 項但書規定係將「本府交通局因交通監控、維護場站與行車安全等目的所設置之錄影監視系統」排除在外。又「台北市政府警察局管理錄影監視系統注意事項」第 2 條則規定「本局『基於治安需要』」及第 4 條規定：「錄影監視系統攝錄影像資料之處理、利用，以治安維護、交通事故處理有必要者爲原則，……。」另外，刻正研擬訂定之「台北市錄影監視系統設置管理自治條例」（草案），未來將以自治條理之位階，統合規範市政府所屬各機關所設置管理之監視系統。其第 4 條規定：「錄影監視系統之設置，應以維護公共安全、社會秩序、犯罪預防及偵查爲目的，並兼顧人民權益，以適當方法爲之，不得逾達成目的之必要限度。」可知，台北市政府所屬之公務機關經由監視器進行個人影音資料之蒐集、處理或利用，乃以公共安全、社會秩序、犯罪預防及偵查（治安維護）、交通事故處理（應可適用法務部依個人資料保護法第 53 條所指定「特定目的」之「犯罪預防」、「交通行政」、「刑案資料管理」、「警政」等）爲特定目的。

（四）「特定目的」外之利用：個資法第 16 條

按個人資料保護法第 16 條：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人書面同意。」可知，個人資料之利用應符合蒐集之特定目的，但倘有法定情形之一者，仍得爲特定目的外之利用。針對公務機關不經當事人同意而爲特定目的外之利用之情形，在適用上的疑義，法務部曾爲諸多解釋，可供法律適用之參考，已如前述。

就本案，如上揭，台北市政府所屬之公務機關經由監視器進行個人影音資料之蒐集、處理或利用，乃以公共安全、社會秩序、犯罪預防及偵查（治安維護）、交通事故處理（應可適用法務部依個人資料保護法第 53 條所指定「特定目的」之「犯罪預防」、「交通行政」、「刑案資料管理」、「警政」等）爲特定目的。然而，是否可供其他目的之利用？實務上，環保局曾向警察局要求調閱監視器影帶，欲找出違規棄置垃圾之人予以裁罰，惟警察局予以婉拒。蓋警察局經由監視器進行個人影音資料蒐集之目的，如前揭，乃以治安維護、交通事故處理爲主，至於欲找出違規棄置垃圾之人予以行政裁罰，係逾越個人資料蒐集之原始目的，除非符合個人資料保護法第 16 條但書之規定，否則，不宜遽然移作他用。對此，

台北市環保局乃改以自行購買之「移動式監視器」架設在垃圾丟包熱點，以找出違規棄置垃圾之人予以裁罰。[18]

（五）告知義務：個資法第 8 條

按個人資料保護法第 8 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。」可知，除符合得免告知情形者外，公務機關須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項。惟倘個人資料之蒐集係公務機關執行法定職務所必要，則得免爲告知。

如前揭，倘「台北市錄影監視系統設置管理暫行辦法」、「台北市政府警察局管理錄影監視系統注意事項」及「臺北市錄影監視系統設置管理自治條例（草案）」或其他法律能合法賦與台北市政府所屬之公務機關爲執行公共安全、社會秩序、犯罪預防及偵查（治安維護）、交通事故處理之法定職務且有以監視器進行個人影音資料之蒐集之必要者，則得免爲告知。而所謂「必要」之判斷，必須按個人資料保護法第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法爲之，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。」而爲之。

[18] 蘋果日報，垃圾亂丟 監視器 10 天揪 38 件，2012 年 10 月 12 日。

然而，倘若以監視器進行個人影音資料之蒐集卻不符上開「公務機關執行法定職務所必要」之要件者，則仍應履行上開個人資料保護法第 8 條之告知義務。而關於告知方式，依個人資料保護法施行細則第 16 條規定：「依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。」因此，公務機關得使用各種方法告知當事人，參考國外立法例（詳如下述），不只可以透過張貼告示或設置告示牌，如果公務機關用其他方法提示當事人監視器之存在亦可。例如，針對盲人以聲音為告知、用網際網路或目前常見的 LED 跑馬燈等等，皆無不可。

（六）當事人之書面同意：個資法第 7 條、第 15 條、第 16 條

按我國新修正的個人資料保護法第 15 條 1 項 2 款規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：二、經當事人書面同意。」第 16 條 1 項 7 款規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 七、經當事人書面同意。」第 7 條規定：「第十五條第二款及第十九條第五款所稱書面同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。第十六條第七款、第二十條第一項第六款所稱書面同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。」可知，公務機關對於個人資料的蒐集、處理或利用，除有其他法定原因外，亦得經告知法定事項後之當事人書面同意而為之。

然而，本案中，經由監視器於公開場所(如公眾得自由出入之街道)或公開活動(如遊行示威或廟會)中所蒐集、處理之影音資料前，應一一經當事人書面同意，實務操作上，恐困難重重。

事實上，「同意」的機制在公、私部門所扮演的角色顯不同，當事人（消費者）的同意在私部門規範體制係居於核心地位，賦予當事人較大空間協商個人資料的保護，但公部門規範體制較少依賴當事人（公民）同意的取得，而較多依賴立法機關賦予公務機關得不經當事人同意而仍蒐集、處理或利用個人資料之例外性強制規定19(例如，前揭之台北市監視器相關之自治法規)。

（七）當事人參與權利：個資法第 10 條

按個人資料保護法第 10 條規定：「公務機關或非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。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」可知，除有法定例外事項外，針對公務機關蒐集之個人資料檔案，當事人得要求查詢、閱覽、製作複本。

按「台北市錄影監視系統設置管理暫行辦法」第 14 條規定：「第三人因正當理由有調閱前項影音之必要者，得報經主管機關同意後向管理人申調閱覽。」又按「台北市政府警察局管理錄影監視系統注意事項」第 4 條規定：「錄影監視系統攝錄影像資料之處理、利用，以治安維護、交通事故處理有必要者爲原則，並恪遵『檢察、警察暨調查機關偵查刑事案件新聞處理注意要點』等相關規定。除下列各款情形外，不得檢視、複製、拍攝：（一）法令明文規定者。（二）爲維護國家安全、社會秩序或增進公共利益之必要者。（三）免除當事人生命、身體、自由或財產之危害者。」第 12 條規定：「民眾申請調閱影像畫面，應敘明調閱事由，並完成相關報（備）案紀錄、切結保密後，依第十點規定提出申請。受理申請單位應儘速將結果告知申請人，至遲不得逾五日；如爲同意調閱，應派員陪同閱覽，不得複製、拍攝。如發現得作爲證據資料者，應

[19] Ian Kerr, Carole Lucock & Valerie Steeves, Lessons from the Identity Trail—Anonymity, Privacy and Identity in a Networked Society 42 (2009).

另依相關規定辦理證據保全。」第 13 條規定：「受理申請調閱影像畫面，應查明申請人身分、調閱事由之必要性及關聯性等事項，並請申請人提示相關證明及完成紀錄後，始得受理。」再按「臺北市錄影監視系統設置管理自治條例（草案）」第 16 條規定：「調閱錄影監視系統攝錄影音資料，應向管理人申請。」綜上，上開規定亦賦與當事人得要求閱覽、調閱及證據保全之權，亦屬於當事人參與權利。

然而，按上開「台北市政府警察局管理錄影監視系統注意事項」第 12 條規定，民眾申請調閱影像畫面，除應敘明調閱事由外，並完成相關報（備）案紀錄、切結保密後，才得提出申請，如爲同意調閱，應派員陪同閱覽，不得複製、拍攝。如發現得作爲證據資料者，應另依相關規定辦理證據保全。又按「台北市政府警察局錄影監視系統影像處理、利用補充規定」之「調閱或閱覽」之「審核原則」，必須先完成報案程序，始執行調閱或閱覽，惟不得由民眾或相關人員自行操作工作站或單獨爲之，以避免錄監影像遭到拍攝(俗稱翻拍)，致發生違反相關法令之情事。因此，倘民眾向台北市警察局請求調閱或閱覽監視器所錄得之影音資料時，現行實務作法[20]，乃要求民眾須報案後方得閱覽，是否將違反個人資料保護法第 10 條之規定？觀察該條本文與但書規定可知，當事人要求查詢、閱覽、製作複本權利之主張乃以沒有「一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」爲前提，並非絕對不受限制之權利。據此，上開規定要求，「民眾申請調閱影像畫面，應敘明調閱事由，並完成相關報（備）案紀錄、切結保密後」，才得依法提出申請，其目的乃在於透過報案可以確立當事人及案件之存在，亦可增加案件處理過程之透明性，並於程序進行上避免民眾自行翻拍、造成資料之濫用，以免妨害公務機關執行法定職務、或該蒐集機關或第三人之重大利益，應肯認目的與手段有所關聯，應無明顯牴觸比例原則之虞。惟在立法技術上，仍應注意法律保留原則之遵守。

[20] 請參閱「台北市政府警察局錄影監視系統影像處理、利用補充規定」之「調閱或閱覽」

四、 台北市監視器相關自治法規之檢討與建議

（一）錄影監視系統設置之目的用語過於廣泛

依臺北市錄影監視系統設置管理自治條例(草案)第四條規定：「錄影監視系統之設置，應以維護公共安全、社會秩序、預防及偵查犯罪有必要者爲限，且應以對人民權益侵害最少之適當方法爲之。」其中「公共安全、社會秩序、預防及偵查犯罪」之目的過於廣泛，導致如環保局要求基於維護社會秩序之目的，請求給予亂丟垃圾之民眾的影像時，將有疑慮。且個人資料保護法之訂定，其中一重要之目的，即在避免該項個人資料遭受到特定目的外之使用，故針對草案第四條第一項之目的應作限縮較妥，或經檢討後可考慮酌以刪除。

（二）監視器設置地點應有明確標準

無論是現行之「暫行辦法」、「注意事項」，或是「自治條例」草案，皆未對監視器可以設置之位置或地點作出明確的規範。本文以爲，實應至少有一個可供參考的標準。否則，即形同各機關可隨意到處安裝監視器，有侵害人民隱私等基本權利之虞。事實上，監視器應採重點式裝設，而非毫無限制地全面性裝設。此時可參考警政上之「犯罪熱點」[21]。另外，在具有「私密性」之公共場所，例如游泳池、溫泉等，則應特別就當事人之利益與安裝監視系統所保護的利益進行衡量，必須要在設置監視系統所保護之利益大於當事人之利益時，方可考慮裝設[22]。至於設置之基準[23]，應以統計之方式，就「治安要點、交通要衝、重要路口、

[21] 許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 33 頁。
[22] 同前註
[23] 許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 59 頁。

偏僻巷弄、治安死角」等治安、交通或其他公共安全上有需要之公共場所或公眾得出入之場所進行挑選。

（三）監視器設置地點之公告

按現行之「台北市錄影監視系統設置管理暫行辦法」第 11 條規定：「依本辦法設置錄影監視系統之地點，主管機關應定期刊登政府公報或運用其他方式，適時公布或公告。」學者認爲[24]，所謂「刊登政府公報」之方式是否符合「當事人參與原則」，即有疑問。「台北市錄影系統設置管理自治條例」草案第 12 條亦規定：「依本自治條例核准使用錄影監視系統之地點，警察局應刊登於網站。」原則上，就監視器設置之區位予以公告之作法值得贊同，惟爲加強對民眾之保障，學者建議除登載在網路或政府公報外，並公告監視器之數量與位置圖。[25]此項作法較之於僅刊登在網路或政府公報上，更有助於使民眾知悉何處有監視器。

（四）監督機關

按現行之「台北市錄影監視系統設置管理暫行辦法」僅有在第 2 條第 1 項規定主管機關爲台北市政府警察局。而「台北市錄影系統設置管理自治條例」草案第 2 條第 1 項同樣只有規定「本自治條例之主管機關爲市政府警察局」。兩者皆未定有負責監督之機關。

參照學說見解，監視器之設置是否符合規定，立法上實應有設置「監督機關」之必要。[26]本文以爲，不只是監視器之設置，整個錄影監視系統的運作，包含後續影像之利用、複製、保存、銷毀等等作爲，都需要有一個監督機關來審查相關作爲是否符合暫行辦法、自治條例或其他法律(如個人資料保護法)之規定。尤

[24] 黃慧娟，我國設置監視器之法制現況及檢討，中央警察大學警政論叢第 8 期，2008 年，第 260 頁。

[25] 同前註

[26]黃慧娟，我國設置監視器之法制現況及檢討，中央警察大學警政論叢第 8 期，2008 年，第 260 頁。

其，監視系統多由警方自行建置，除了警察局內部應設有單位負責自我監督外，亦應有外部單位進行監督，否則即淪爲「球員兼裁判」的情形。查「台北市錄影監視系統設置管理暫行辦法」第 1 條第 1 項規定：「臺北市政府（以下簡稱本府）爲健全本府所屬各機關及里辦公處錄影監視系統設置管理，以維護治安，並兼顧人民權益保障，特訂定本辦法。」與第 2 條規定：「本辦法之主管機關爲本府警察局。主管機關得將辦理會勘、查核及調閱事項委任轄區分局執行之。」就此，學者批評爲：「警察本是被監督者，搖身一變成爲監督者。」[27]目前大多數縣市都缺乏這種外部監督機制[28]，台北市宜開風氣之先，無論是由市政府本身或由市府設立一個委員會，都需要有一個外部機制來監督市府轄下的各個機關。

（五） 教育訓練

按個人資料保護法第 18 條規定：「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。」又按個人資料保護法施行細則第 12 條規定：「本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關爲防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例爲原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維

[27]李震山，從公共場所或公眾得出入之場所普設監視器論個人資料之保護，東吳大學法律學報第 16 卷第 2 期，2004 年，第 79 頁。

[28]許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 52 頁。

護之整體持續改善。」可知，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，而其中，教育訓練亦屬重要一環。

學者[29]有參照英美等國之作法而認爲，相較於英美等國立法例中，對於監視系統的操作人員之教育訓練都有要求。教育訓練亦應納入「監視錄影系統使用管理規範之核心項目」當中。查現行的「台北市錄影監視系統設置暫行管理辦法」與「台北市政府警察局管理錄影監視系統注意事項」或「台北市錄影系統設置管理自治條例」草案中都沒有規範到操作人員的教育訓練，未來至少應該將強操作人員的法治素養，特別是對個人資料保護法（如上開安全維護事項）的認識，並將此明文化，納入法規範之中。另外，學者認爲[30]，設置機關應有相關訓練計畫，使人員能瞭解監視系統與設置目的之關聯。

（六）定期檢討

按現行「台北市錄影監視系統設置管理暫行辦法」、「台北市政府警察局管理錄影監視系統注意事項」、「台北市錄影系統設置管理自治條例」草案，都缺乏定期檢討之機制。學者[31]認爲，應定期評估監視系統有無達到設置目的？是否已違法侵害人民權益？如果監視系統未達預期之目的或發現有嚴重侵害人權之情事時，即應停止設置。另有學者[32]認爲，可以參考修正前之德國 Nordhein-Westfalen 邦警察法第 15a 條第 4 項之規定爲「每年檢討一次」。未來修法增訂定期檢討機制時，亦可仿照此項德國立法例。

（七）「監視器」設置所在處所之標示

[29]許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 52 頁。

[30]許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 60 頁。

[31]許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 62 頁。

[32] 黃慧娟，我國設置監視器之法制現況及檢討，中央警察大學警政論叢第 8 期，2008 年，第 62 頁。

按個人資料保護法第 8 條規定，向當事人蒐集個人資料時，除符合得免告知情形者外，公務機關須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項。惟如前揭，倘若以監視器進行個人影音資料之蒐集符合上開「公務機關執行法定職務所必要」之要件者，則得免爲告知；否則，則仍應履行個人資料保護法第 8 條之告知義務。

事實上，由於監視器長時間的錄影而蒐集個人資料，對於民眾隱私、遷徙自由、表現自由等產生寒蟬效應，因此，諸多國家均會在「監視器」設置所在處所爲一定之標示，提醒監視器之存在與個人影像資料被蒐集。

然而，無論是「台北市錄影監視系統設置管理暫行辦法」條、「台北市政府警察局管理錄影監視系統注意事項」或「台北市錄影系統設置管理自治條例」草案皆未對以監視器蒐集民眾個資時應如何爲告知作出具體規範。目前台北市政府僅在監視器之機身上張貼「台北市政府警察局守護您」之標語，機身上的字體可能太小，以至於無法使民眾清楚可見。查英國立法例[33]有認爲，告示的大小應視現場情況而定。例如在建築物的入口處之監視器，至少需要 A4 尺寸的標示；而在停車場提醒駕駛人有監視系統之標示，則需 A3 大小。現行作法僅張貼相當於監視器機身大小之標語，顯然小於前述之 A4 尺寸，更何況位於道路上的告示尺寸上應該更爲放大。

再者，參考日本立法例[34]，日本東京都係在設置地區通行道路上醒目之處所，設有「監視器設置標示板」，以告知附近住民。學者認爲[35]，日本東京都此項在同條道路上設置告示板之作法，對一般民眾而言較有效果，足供我國參考。本文認爲，目前設有固定式測速照相機處，多設有告示板提醒用路人「前方有

[33] 英國 CCTV Code of Practice，參閱許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 25 頁。

[34] 東京都街頭監視器運用要綱，參閱黃慧娟，日本防犯監視器規制法制之實況與動向，中央警察大學學報第 46 期，2009 年，第 77 頁。

[35] 黃慧娟，我國設置監視器之法制現況及檢討，中央警察大學警政論叢第 8 期，2008 年，第 254 頁。

測速照相」，可仿照測速照相機，至少在重要道路，例如幹道、快速道路、交流道、十字路口等之監視器設置此項看板。學者認爲，測速照相以拍攝車牌號碼爲主，而非直接涉及人格。既然未涉及人格之測速照相都要清楚標示，則對於涉及人格之監視錄影，更無排除標示之理。[36]

又有認爲告示板或各項標示應設立在進入監視範圍以外即能知悉之處，而非待人民已置身於監視範圍以內之後，才發現有告示而知有監視器的。按如此方能確保人民在該範圍內有爲或不爲一定行爲之自由。[37]本文認爲此項見解較符合個人資料保護法「事前同意」之精神，以落實對於人民隱私、遷徙自由、表現自由等之保障。蓋人民應在進入監視範圍內之前即獲告知，如果渠不願意曝光在監視系統之下，則其有權利不進入或避開監視範圍。在這裡，告示板的尺寸再度成爲重點。蓋告示板需達足夠的大小，人民方能於監視範圍外望見並清楚得知，而決定是否踏進此一範圍。

告示之方式，學說上認爲尚應視個別情況決之。學者參考德國法認爲，如在盲人出入之處，尚需以聲音爲表示。而在不懂本國文字之人出入之處（例如警察局外事單位）則應以外文或圖示爲之[38]。本文認爲台北市已躋身國際性大都市之林，各國人士出入頻繁，實應考慮以各種外語爲標示，以顧及外籍人士之隱私權等基本人權。除了應以最常用的英文爲標示之外，考量我國有許多日籍旅客造訪以及來自泰國、越南、印尼等外籍勞工，不妨以多國語言標示之。

又關於監視器運作時段，參考外國立法例[39]，尚應標示監視器運作之時段。縱然我國監視器通常係 24 小時監視，亦應充分爲告知，使民眾能得知被監視之時間。

---

[36] 李震山，從公共場所或公眾得出入之場所普設監視錄影器論個人資料之保護，東吳大學法律學報第 16 卷第 2 期，2004 年，第 84 頁。

[37] 彭旭成，國家設置、運用監視器與資訊隱私權之衡平，天主教輔仁大學財經法律研究所碩士論文，2011 年，第 204 頁。

[38] 李震山，監視錄影器設置的合法性－對「電眼」的恐懼 vs.還好老天有「眼」！，台灣本土法學第 78 期，2006 年，第 156 頁。

[39] 英國 CCTV Code of Practice，許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 29 頁。

至於監視器負責之單位，按德國聯邦個人資料保護法第 6b 條第 2 項規定，監視攝影器設置，「應以適當之方式，使人知悉監視之情況及負責之單位」。[40]英國法亦認為，告知的內容應包括該系統負責之個人或組織團體、設置目的、聯絡方式。[41]查現行之方式，只有「台北市政府警察局守護您」一行標語，並未詳為告知該監視系統負責之人與聯絡方式。雖不必告知承辦人員之姓名，但至少應該明示為台北市政府轄下何單位所負責，例如標示「台北市政府犯罪預防科」，俾使人民可以直接找到對口之單位。此外，最好能明示監視系統之目的，例如標示「犯罪防治監視器」或「道路交通監視器」等。而聯絡方式，亦應明示設置或負責單位之電話號碼。學說[42]認為：設置在公共場所之監視錄影系統，由於當事人較難以判斷何人為蒐集資料之主體，則標示內容應較詳細，至少應包括「設置相關設備者的名稱、蒐集目的及取得法定告知事項資訊的方式（如網址或聯絡電話）」。另有學者亦提出英國資料保護官所建議之標示：「為了防範犯罪及公共安全，本場所設有監視錄影設備。相關影像由○○機關蒐集、處理。欲知詳情，請洽（電話號碼或網址）」[43]，可供未來參考。

[40] 黃慧娟，我國設置監視器之法制現況及檢討，中央警察大學警政論叢第 8 期，2008 年，第 20 頁。

[41]許福生，我國運用監視錄影系統法制規範之回顧與展望，中央警察大學學報第 46 期，2009 年，第 25 頁。

[42] 劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外－以監視錄影為例（下），月旦法學教室第 119 期，2012 年，第 48 頁。

[43] 同前註，第 48 頁，註 82

第二節　教育局

壹、　訪談大要

本研究團隊最初訪談重點主要針對「臺北市政府教育局維護校區安寧實施要點[44]」，該要點中第 13 點規定「各校應隨時向警察單位提供因不良行爲退學、休學學生名單（學生名單按姓名、年齡、籍貫、住址造冊送轄區派出所及少年隊）及校區附近不良青少年幫派活動情形不正當遊樂場所資料，藉以追蹤輔導及時防制與取締。」、第 14 點規定「各校應於每學期切實調查寄居校外學生分佈情形，除指定適當教職員專責輔導其生活及其安全維護外，並分區（以警察分局轄區爲準）造具名冊送函送轄區警察分局配合辦理。」、第 22 點中第 7、11 項「商請警察機關協助支援事項：(七)對學校附近青少年不良分子應建立完整資料，嚴密查訪，積極誘導規勸，防止其犯罪。(十一) 將轄區內各學校附近之義警名冊及連絡電話通知學校，以更就近請求支援，維護校園安寧。」以上規定中，均有由學校主動將特定學生之個人資料提供給警察機關之情形，有違反個人資料保護法規定之虞。惟經訪談後，得知目前台北市政府教育局已無適用此校園安寧實施要點之情況，該要點已形同虛設，故無探討之必要。因此，本研究團隊乃又針對「臺北市政府教育局電腦處理個人資料作業程序[45]」作訪談重點，因該作業程序係依照舊法電腦處理個人資料保護法所制定，應可依現行個人資料保護法探討修正之必要，惟臺北市政府教育局人員亦表示該作業流程現亦不再使用，已形同虛設，故亦無討論之意義。

最後，本研究團隊本次訪談重點乃針對台北市政府教育局目前推行經由「數位學生證」管理而建置「校園出入管理系統」政策進行訪談，由於以數位學生證而建置「校園出入管理系統」政策目前臺北市政府並無訂定內部規範，故乃依現

[44] 中華民國七十二年十月二十四日臺北市政府(72)北市教訓字第二九０四號函訂頒

[45] 中華民國八十五年十月十五日臺北市政府教育局(85)北市教統字第八五二四六二二五號函訂頒

行個人資料保護法之規定，檢視以數位學生證而建置「校園出入管理系統」之程序是否有違反個人資料保護法之虞，並提出相關建議。

貳、 數位學生證之「無線射頻辨識系統」與個人資料保護法之探討

一、無線射頻辨識系統(RFID，Radio Frequency Identification)

台北市政府教育局目前以數位學生證而建置「校園出入管理系統」，其所採用的「無線射頻辨識系統」(RFID)，是一種無線通訊技術，可通過無線電訊號識別特定目標並讀寫相關數據，而無需識別系統與特定目標之間建立機械或光學接觸。無線電的訊號是通過調成無線電頻率的電磁場，把數據從附著在物品上的標籤上傳送出去，以自動辨識與追蹤該物品。某些標籤在識別時從識別器發出的電磁場中就可以得到能量，並不需要電池；也有標籤本身擁有電源，並可以主動發出無線電波（調成無線電頻率的電磁場）。標籤包含了電子存儲的資訊，數公尺之內都可識別。與條形碼不同的是，射頻標籤不需要處在識別器視線之內，也可以嵌入被追蹤物體之內。因此，依無線射頻辨識系統(RFID)技術的特性，該技術能夠隨時的追蹤物件，並且將利用追蹤的物件連結至大型資料庫中，進行資料的比對後可取得特定人的個人資料，如此一來可輕易的做到資料之蒐集與處理[46]。並且依照無線射頻辨識系統(RFID)技術的特性，可能得在人們不知情、毫無受到告知的情況下，追蹤人民的現在地點，而受追蹤之人民並無法有效查覺其個人資料遭到蒐集、處理或利用，而造成蒐集者與被蒐集者資訊不對等之地位。[47]

現許多行業皆有運用了無線射頻辨識技術。如將標籤附著在一輛正在生產中

[46] 廖淑君，智慧網聯之發展與個人資訊隱私保護課題：以歐盟之因應爲例，法學新論，二○一一年十一月，頁 25。

[47] http://zh.wikipedia.org/wiki/%E5%B0%84%E9%A2%91%E8%AF%86%E5%88%AB

的汽車，廠方便可以追蹤此車在生產線上的進度、倉庫可以追蹤藥品的所在、射頻標籤也可以附於牲畜與寵物上，方便對牲畜與寵物的積極識別（積極識別意思係防止數隻牲畜使用同一個身份）。無線射頻辨識的身份識別卡可以使員工得以進入建築鎖住的區域，汽車上的射頻應答器也可以用在收費路段與停車場等處所。另某些射頻標籤附在衣物、個人財物上，甚至於植入人體之內。由於此 RFID 技術可能會在未經本人許可的情況下讀取個人資訊，明顯有侵犯個人隱私之隱憂。[48]

台北市政府教育局目前以數位學生證而建置「校園出入管理系統」，即應用此無線射頻辨識系統(RFID)功能，藉由學生上下學經由數位學生證的刷卡，使系統蒐集學生何時抵達學校、何時離開學校、學生缺席、或中途離校未刷卡，若學生有遲到或者缺席情形之個人資料，而此運作數位學生證之系統將會自動的寄發簡訊至支付費用之學生家長之手機中，告知學生的即時情況。事實上，目前有權直接或間接接近、利用數位學生證系統中之個人資料者，有下列四類型：包括學校、臺北市政府教育局、學生家長及建置維修數位學生證無線射頻辨識系統(RFID)之廠商。其中，學校主要得查詢學生數位學生證內之個人資料者爲資訊組長及導師。而台北市政府教育局亦可連線數位學生證之電腦資料庫，另學生家長除透過其手機接收孩子到校、離校之時間，亦可主動來電詢問。

二、個人資料保護法對於數位學生證之「無線射頻辨識系統」之規範

台北市政府教育局目前以數位學生證而建置「校園出入管理系統」，但其並未制定任何專門的行政命令對其加以規範，故以下僅從個人資料保護法規範的角度，加以分析：

(一) 個人資料保護法之蒐集限制原則

[48] http://zh.wikipedia.org/wiki/%E5%B0%84%E9%A2%91%E8%AF%86%E5%88%AB

1. 「告知後同意」之要求

依個人資料保護法第 15 條 1 項 2 款規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：二、經當事人書面同意。」第 16 條 1 項 7 款規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 七、經當事人書面同意。」又按第 7 條第 1 項規定：「第十五條第二款及第十九條第五款所稱書面同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。」可知，資料蒐集者對於個人資料的蒐集、處理或利用，除有其他法定原因外，應經當事人書面同意。再者，立法者亦有意藉由所謂「告知後同意」或「告知後選擇」之原則，進一步落實對個人資料所指涉當事人之保護。

又依個人資料保護法第 8 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，得免為前項之告知：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。」及第 9 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蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。有下列情形之一者，得免為前項之告知：一、有前條第二項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人爲告知。四、基於公共利益爲統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者爲限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。第一項之告知，得於首次對當事人爲利用時併同爲之。」可知，個人資料保護法明文規定，不論是直接或間接蒐集資料，除符合得免告知情形者外，均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項，以利當事人爲「告知後同意」。

而其告知方式，依個人資料保護法施行細則第 16 條規定：「依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式爲之。」

綜上可知，公務機關對於個人資料的蒐集、處理或利用，除有其他法定原因外，應經當事人書面同意。此處之同意，參考外國立法例，欲使同意有效，必須經告知才可，而所提供的隱私權政策通知應清楚即明確地指出何種個人資料將被搜集、如何被利用、與誰分享，且不得有欺罔、誤導或錯誤之情事，否則，同意將會無效。

而台北市政府教育局目前以數位學生證而建置「校園出入管理系統」政策中，各學校將會發給學生使用數位學生證的同意書，同意書之內容係詢問學生是否繳交使用數位學生證之費用以開通數位學生證之功能。實際上數位學生證之運用上，將涉及學生的出缺席個人資料及學生家長之行動電話資料，惟台北市目前各學校在發給學生的同意書中，僅告知學生及家長是否同意繳交使用數位學生證系統之費用，並未針對數位學生證之使用將蒐集到的個人資料(如學生到校時間、離校時間、未到學校、學生家長之手機電話等) 之目的與用途等，而按個人資料保護法第 8 條第 1 項所列之蒐集機關名稱、蒐集目的、資料類別、利用方式源等相關事項作明確的告知，此有違個人資料

保護法之虞，因此，除有免爲告知之情事外，各學校仍應注意第 8 條第 1 項所列各款之資訊之確實告知。

另外，經由台北市政府所屬各學校而間接蒐集數位學生證建置「校園出入管理系統」之相關學生個人資料之台北市政府教育局，亦未針對經由數位學生證所蒐集個人資料之目的與用途等，按個人資料保護法第 9 條第 1 項所列之蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項作明確的告知，此有違個人資料保護法之虞，因此，除有免爲告知之情事外，台北市政府教育局仍應注意第 9 條第 1 項所列各款之資訊之確實告知。

2. 同意適用之排除

按新修正的個人資料保護法規定，有下列情形之一者，縱未經當事人書面同意，仍得蒐集、處理個人資料，例如，按第 15 條第一項第一、三款規定:「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。三、對當事人權益無侵害。」本案中，學校蒐集學生之個人資料是否屬於執行法定職務之必要範圍內而可免除同意告知之義務，受訪之臺北市政府教育局同仁認爲，依照臺北市國民中小學學生學籍管理辦法第六條第二項之規定，「學生依規定編班後，各校應依照學號之順序，繕造入學學生名冊存查，並製發學生證。」故學校有製作學生證並點名確認其出缺席狀況之法定職權，應符合無庸當事人「同意」之例外情形。

惟學校雖屬有製作學生證並點名確認其出缺席狀況之法定職務，但學校得否將學生出缺席等個人資料傳輸予教育局呢？對此，按法務部函釋[49]可知：「按臺北市政府教育局基於數位學生證之管理，建置『校園出入管理系統』依現行電腦處理個人資料保護法（以下簡稱本法）第 3 條第 1 款、第 3

[49] 法務部 100 年 4 月 26 日法律字第 0999051925 號函。

款、第 4 款及第 5 款之規定，應屬個人資料之蒐集、電腦處理與利用，依同法第 7 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。』及第 8：『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，並與蒐集之定目的相符。但有左列情形之一者，得爲特定目的外之利用…。』之規定以觀，臺北市政府教育局掌理臺北市市立學校教育範圍內，並與蒐集之特定目的（教育行政或學生資料管理）相符，得爲個人資料之蒐集、電腦處理及利用行爲，合先敘明。」可知，臺北市政府教育局掌理臺北市市立學校教育範圍內，並與蒐集之特定目的（教育行政或學生資料管理）相符，因此，得爲個人資料(如經由數位學生證所蒐集之學生到校時間、離校時間、未到學校等資訊)之蒐集、處理及利用行爲。惟家長手機號碼之蒐集，是否屬於上開教育行政或學生資料管理之特定目的之內而無庸取得當事人書面同意，不無疑義。

惟應注意者，縱使各學校或臺北市政府教育局得不經當事人同意而得爲數位學生證之相關個人資料之蒐集、處理及利用行爲，但除有免爲告知之情事外，仍應注意個人資料保護法第 8 條第 1 項或第 9 條第 1 項所列各款之資訊之確實告知。

(二) 目的明確原則

依個人資料保護法第 15 條規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人書面同意。三、對當事人權益無侵害。」本案中，臺北市政府教育局乃出於「教育行政」或「學生資料管理」之特定目的而經由數位學生證之無線射頻辨識系統(RFID)特性，隨時掌握學

生之動態，而進行個人資料之蒐集或處理，應符合個人保護法所要求之目的明確原則。

(三) 使用限制原則

依個人資料保護法第 16 條：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人書面同意。」可知，個人資料之利用應符合蒐集之特定目的，但倘有法定情形之一者，仍得爲特定目的外之利用。

目前學校使用數位學生證對個人資料之蒐集，主要係用於學生到校、離校點名，學生家長亦可來電至臺北市政府教育局詢問，經由數位學生證之資料庫查詢其孩子是否已到學校。可知，臺北市政府教育局利用電腦連線而蒐集學生數位學生證之個人資料（學生是否到校）而統計學生出缺席狀況，如前揭法務部 100 年 4 月 26 日法律字第 0999051925 號函，亦屬北市政府教育局掌理臺北市市立學校教育範圍內，並與蒐集之特定目的（教育行政或學生資料管理）相符，因此，得爲上開個人資料之蒐集、處理及利用行爲。

目前臺北市政府教育局關於數位學生證無線射頻辨識系統之架設及維修係委託廠商進行，因此，委託廠商亦有機會接近數位學生證內之個人資料，而依個人資料保護法第 4 條之規定「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」又按法務部

函釋[50]可知，受委託廠商受臺北市政府教育局委託，於接獲數位學生證掛失通知後，得依其授權權限進入臺北市政府教育局之『校園出入管理系統』辦理掛失數位學生證並終止悠遊卡功能，係屬個人資料之蒐集、電腦處理及利用行爲，則於臺北市政府教育局蒐集之特定目的，及受委託處理範圍內所爲行爲，視同臺北市政府教育局之行爲（本部 98 年 12 月 28 日法律字第 0980047722 號函參照），並以臺北市政府教育局爲權責歸屬機關。據此，受委託廠商因數位學生證業務而蒐集、電腦處理及利用個人資料之行爲，並非特定目的外之利用，不適用上開個人資料保護法第 16 條之規定。

(四) 安全維護原則

依個人資料保護法第 18 條規定：「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。」、個人資料保護法施行細則第 12 條規定:「本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關爲防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例爲原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善」可知公務機關針對其所蒐集之個人資料有安全維護之義務，且該安全維護措施須符合比例原則。

[50] 法務部 100 年 4 月 26 日法律字第 0999051925 號函

關於處理數位學生證之無線射頻辨識系統(RFID)，除各學校設置數量不等之刷卡感應器外，其伺服器主機乃設置於臺北市政府教育局，而對於其安全維護，有諸多防護措施。其中，針對外來之入侵性行爲，設有防火牆，依臺北市政府教育局所提供之「系統與網路安全檢查表」可知，目前每日皆會作系統安全檢查及網路連線之網路安全檢查。又如「台北市教育網路中心通信與作業管理程序書」中第 5.3.2 項規定對惡意軟體之防範「應安裝病毒偵測與修復軟體，並不定期更新病毒資訊，並於每日中午執行掃毒工作，以防止病毒之攻擊。伺服器主機防毒軟體系統應設定主動掃瞄檢查，或由網路系統管理人員定期執行掃瞄檢查作業。」另外，防火牆亦於每個月作一次安全檢查，且該防火牆係針對數位學生證之無線射頻辨識系統及臺北市政府內其他系統一起作連線，一同受該防火牆防範。另有對入侵防禦偵測作事前之防範，若有重大入侵情形時，依「台北市教育網路中心存取控制管理程序書」第 5.9 項可知，針對系統被入侵時的異常處理規定「立即拒絕入侵者任何存取動作（例如關閉可疑帳號），防止災害繼續擴大。關閉受侵害的主機，並立即與網路離線。檢查防火牆及系統紀錄，研判入侵管道方式，必要時作安全漏洞修補。通知主機供應商提供必要的回復協助。如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復止，最後再將該主機重新上線。」故可知實體斷線爲最後防禦手段。另針對已經入侵之違法行爲，系統可透過事後軌跡資料作追蹤，查詢違法行爲之來源。

又如前揭，數位學生證之無線射頻辨識系統(RFID)之軟硬體設備，乃臺北市政府教育局乃委託廠商加以建置及維修，而有學生及家長個人資料之蒐集、處理及利用行爲之機會。而關於其安全維護措施，於本研究案訪談時，相關人員表示，臺北市政府教育局與廠商亦有簽保密切結，要求廠商應負保密義務，廠商之行爲亦將受到教育局之稽核，以確保個人資料之安全。且廠

商若欲取得個人資料，須先向台北市政府教育局填寫系統需求申請與回覆單，待教育局發文予廠商後，廠商始得享有權限進入系統搜尋資料，且教育局於發文中亦有限制廠商進入系統之時間，若於允許外之時間係無法進入系統取得資料。

再者，目前臺北市政府教育局定內部規範「台北市教育網路中心存取控制管理程序書」中，針對享有權限可取得個人資料之行爲人，定有限制其使用目的之規範，依該存取控制管理程序書中第 5.5.1 項對資訊存取之限制規定「應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。例如：新增、刪除或執行等。應用系統之敏感與機密性資訊，應與一般資訊作適當區隔，並加強權限控管措施。」故針對數位學生證所涉及個人資料之應用，應僅限於業務相關。並且依該程序書中第 5.6.2 項規定「網路管理人員應定期檢視網路存取之紀錄，並留存查核記錄。」可知，將定期查核是否有非業務相關之違反情形。

(五) 數位學生證所蒐集個人資料之處理

依個人資料保護法第 2 條第 4 款之規定，個人資料之處理係：「指爲建立或利用個人資料檔案所爲資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。」目前台北市政府教育局以數位學生證而建置「校園出入管理系統」，針對數位學生證所蒐集個人資料之處理有紀錄、儲存、更正、複製、檢索、刪除、輸出、連結及內部傳輸，其中，更正如導師發現學生上學忘記刷到校記錄時，導師可進入系統替其更改爲到校。

第三節　衛生局

壹、 訪談大要

一、TIPSPA 傷害監測系統，係透過檢視所有事故傷害之原因或地點，瞭解到各種事故傷害會對不同的年齡或族群造成何種影響。例如，將事故區分爲交通事故、燙傷事故等等。事故發生的地點則以山區等等爲區分。或將事故發生的族群分爲老人、小孩等等。總共有 8 種表格，上面的欄位有：教育程度、性別、是否酗酒、醫院檢傷之等級、事故類別及誘因等等。

由急診室或健康服務中心醫護人員匯整所有事故之情形，於急診端作登錄，蒐集資料作長期研究之用。研究的成果則提供市府各局處，跨單位作決策時之參考。另外，所得的成果也會回饋予社區。舉例而言，我們爲了預防老人跌倒，我們必須知道老人在何處跌倒。同時亦涉及傷害事故之等級。研究成果可以幫助我們提醒家中有老人的民眾去注意何處容易引發老人跌倒事故。目前此系統仍在持續運作中。

二、TIPSPA 傷害監測系統的法源爲何？依個資法第 15 條，是否符合「法定職務」？仍有待釐清，有認爲似可依人體研究法。

三、爲 TIPSPA 傷害監測系統而蒐集當事人個資時，並未進行告知，因爲蒐集當事人個資時，多半處於緊急狀況，如果要求一定要取得同意的話，實務上相當困難。

四、TIPSPA 傷害監測系統建置是一個獨立系統，並未與醫院有連結。其資料庫是屬於 WEB 的系統。

五、就離職人員而言，關於其 TIPSPA 傷害監測系統之帳號，只要是循正常管道離職，人事方面會爲通知，一定會銷除其帳號。此外，政風單位皆會爲稽查。

六、關於資訊安全之標準，現在係採用 ISO27001 的標準。另外，參考行政院資通中心數年前就各單位所訂之標準。又，ISMS 從民國 89 年開始，將全國各機關分成 A、B、C、D 四級，本局屬於 C 級，即每年須稽核一次。

七、關於個資法是否有窒礙難行之處，法務局曾經發函要各單位編列關於個人資料保護法賠償案件的賠償預算額度。但是實際上賠償金額爲何，實難預料。或許應該由法務局統一編列之。

貳、傷害監測資料與個人資料保護法之探討

一、前言

按台北市政府衛生局於民國97年8月11日訂定「台北市政府衛生局傷害監測資料管理注意事項」（下稱「注意事項」），並建置「TIPSPA傷害監測系統」。所謂「TIPSPA傷害監測系統」係「由臺灣事故傷害預防與安全促進學會（TIPSPA）開發之事故傷害外因資料登錄、資料管理、資料下載等網路應用軟體及作業程序。」（ 注意事項第2條第4項）又「TIPSPA傷害監測系統」之目的爲「爲推動安全社區政策，了解臺北市事故傷害發生之頻率與導因，促進公共衛生與安全，與臺灣事故傷害預防與安全促進學會合作，並採用其開發之『TIPSPA傷害監測系統』，進行本市傷害監測資料之登錄與管理相關事宜」（注意事項第1條）。而所謂之「本市傷害監測資料」則係「指衛生局推動安全社區政策，以社區爲平台，與台北市部分設有急診室之醫療院所與市立聯合醫院五個綜合醫院院區合作，於急診室蒐集事故傷害發生相關資料，了解事故傷害發生之頻率與導因，加以記錄

分析應用」（注意事項第2條第3項）。

就「TIPSPA傷害監測系統」之實際運作而言，建立事故傷害監測系統是推動安全社區重要基礎，有了事故傷害資料，才能夠找出高危險群、高危險環境及事故發生原因，提供具體的社區安全介入策略，助於成功推動安全促進計畫。從不同社區的經驗來觀察，醫院是建立監測系統重要的一環，需要有社區醫院的支持及行動，先行蒐集事故傷害資料；接著，要有社區健康中心協助資料鍵入；城市健康部門控制資料的應用；專業輔助單位提供資訊系統管理及資料報告[51]。亦即，藉由建立傷害監測管理系統，相關單位可以找到事故傷害的成因，進一步防止事故傷害的發生。就台北市的角度，這樣一個傷害監測系統是由衛生局、十二區健康服務中心與台北市內眾多的合作醫院協力完成的。[52]

本文在研究過程中，發覺到「台北市政府衛生局傷害監測資料管理注意事項」中部分條文規定似與新修正之個人資料保護法之規定有所扞格，因此不揣淺陋，爰就相關規定與現行法律衝突之處略作探討。

二、新修正個人資料保護法施行後對於台北市政府衛生局傷害監測資料管理影響之問題與分析

（一）「蒐集」傷害事故相關資料已涉及個人資料之蒐集

按自前開所引之「台北市政府衛生局傷害監測資料管理注意事項」第2條第2項規定可知，「TIPSPA傷害監測系統」（下稱「傷害監測系統」）係透過台北市各

[51]臺北市政府衛生局，第 5 屆亞洲安全社區會議出國報告，2010 年，第 14 頁到 15 頁。請參閱：http://www.openreport.taipei.gov.tw/OpenFront/report/report_detail.jsp?sysId=C09802703

[52] 台北市政府衛生局傷害監測資料管理注意事項第 2 項第 2 款：「本市傷害監測資料：指本局推動安全社區政策，以社區爲平臺，與本市部分設有急診室之醫療院所與市立聯合醫院五個綜合醫院院區合作，於急診室收集事故傷害發生相關資料，了解事故傷害發生之頻率與導因，加以記錄分析應用。」第 5 款：「使用單位：指本局、十二區健康服務中心、本市收集傷害監測資料之醫院（以下簡稱合作醫院）等，各使用單位可使用之功能依帳號權限而有不同。」

大醫療院所之急診室「收集」(「蒐集」) 事故傷害相關資料。在蒐集此項事故傷害相關資料時，臺灣事故傷害預防和安全促進學會開發的傷害監測系統，其登錄的表單共有8種，包含道路運輸事故、跌倒墜落、撞壓砸夾割刺絞傷、梗塞窒息、中毒、燒燙傷、人及動植物致傷、溺水等；需由醫院急診室受過訓練之護理人員進行登錄[53]。亦即，現行作法是由現場醫護人員填寫「台北市衛生局事故傷害外因登錄表」，並將相關資料皆記錄於「台北市衛生局事故傷害外因登錄表」上。

查「台北市衛生局事故傷害外因登錄表」之各項欄位，其中不乏涉及病人之個人資料者。例如：「病歷號」、「生日」、「傷者教育程度」、「檢傷等級」、「受傷前疾病史」、「受傷前平日服用藥物狀況」、「急診後傷患動向」及「預後推估」等等。對照個人資料保護法第2條第1款就個人資料所作之定義，可整理如下表：

【表 1】

個人資料保護法第 2 條第 1 款	台北市衛生局事故傷害外因登錄表
出生年月日	生日（年/月/日）
教育	傷者教育程度（不識字/小學/國中/高中/高職/大專（學）以上/其他）
病歷	✧ 病歷號 ✧ 檢傷等級 ✧ 受傷前疾病史（正常/行動不便/視障/高血壓/糖尿病/癲癇/其他） ✧ 受傷前平日服用藥物狀況（沒有/有→種類爲：高血壓/糖尿病/心臟病/其他）

[53]臺北市政府衛生局，第 5 屆亞洲安全社區會議出國報告，2010 年，第 14 頁。請參閱：http://www.openreport.taipei.gov.tw/OpenFront/report/report_detail.jsp?sysId=C09802703

	✧ 急診後傷患動向(治療後遵醫囑出院/轉門診/轉一般住院/轉ICU/轉送他院/不遵醫囑出院/病危出院/急救後死亡/到院時已死亡） ✧ 預後推估（可能康復/可能造成永久傷殘/可能長期臥床/可能死亡或成爲植物人）

參照上表，復依個人資料保護法第 1 條「爲規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」之規定可知，此處「蒐集」事故傷害相關資料應有個人資料保護法之適用。

（二）蒐集、處理個人資料之特定目的及法源依據爲何

按個人資料保護法第 15 條 1 項規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人書面同意。三、對當事人權益無侵害。」可知，公務機關對於個人資料的蒐集或處理，應有特定目的，並除應經當事人書面同意或對當事人權益無侵害外，應屬執行法定職務必要範圍內。

另按個人資料保護法第 6 條規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。三、當事人自行公開或其他已合法公開之個人資料。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，爲統計或學術研究而有必要，且經一定程序所爲蒐集、處理或利用之個人資料。」可知，除法律明文規定、公務機關執行法定職務所必要、或公務機關基於醫療、衛生或犯罪預防之目的而爲統計或學術研究而有必要等外，有關醫療、健康檢查之個人資

料，不得蒐集。 惟應特別注意者，本條不在 101 年 10 月 1 日新修正個人資料保護法生效條文之列。

承前所述，衛生局非但「蒐集」了大批傷患之個人資料，而且對資料加以分析、解釋與傳佈[54]。可知，衛生局確實蒐集、處理、利用他人個人資料。依個人資料保護法第 15 條規定，衛生局必須有特定目的，且有該條文中一款所規定之要件，方得蒐集、處理或利用個人資料。查「台北市政府衛生局傷害監測資料管理注意事項」第 1 條係規定：「臺北市政府衛生局（以下簡稱本局）爲推動安全社區政策，了解臺北市（以下簡稱本市）事故傷害發生之頻率與導因，促進公共衛生與安全，與臺灣事故傷害預防與安全促進學會合作，並採用其開發之『TIPSPA 傷害監測系統』，進行本市傷害監測資料之登錄與管理相關事宜，特訂定本注意事項。」則衛生局之目的應係爲「促進公共衛生與安全」。準此，蒐集、處理或利用他人個資已有特定目的。

雖然，衛生局出於特定目的而蒐集、處理、利用個人資料（如個人基本資料、病歷資料），惟其是否符合個人資料保護法第 15 及 6 條各款之要件，則分析如下：

1．個人資料保護法第 15 條要件之分析

按個人資料保護法第 15 條規定，公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

(1) 個人資料保護法第 15 條第 1 款係規定「執行法定職務必要範圍內」，則蒐集、處理、利用事故相關資料，建置「TIPSPA 傷害監測系統」是否爲衛生

[54] 台北市政府衛生局傷害監測資料管理注意事項第 2 項第 1 款：「監測：根據世界衛生組織傷害監測指引之定義，監測一詞於公共衛生領域中，意指持續且有系統地進行健康相關資料之收集、分析、解釋與傳佈。」又第 2 款規定：「本市傷害監測資料：指本局推動安全社區政策，以社區爲平臺，與本市部分設有急診室之醫療院所與市立聯合醫院五個綜合醫院院區合作，於急診室收集事故傷害發生相關資料，了解事故傷害發生之頻率與導因，加以記錄分析應用。」

局之「法定職務必要範圍」？若認爲合於法定職務，則有何法源依據？查現行各項法規關於「TIPSPA 傷害監測系統」者，僅有「台北市政府衛生局傷害監測資料管理注意事項」而已，別無其他規定。若認爲該注意事項第 1 條之「促進公共衛生與安全」即衛生局之法定職務，惟「促進公共衛生與安全」本身即屬一抽象不確定法律概念，而法定職務範圍應依法律具體劃定，僅以「促進公共衛生與安全」即作爲衛生局之法定職務實過於空泛。否則就其他機關而言，例如環保局，同樣也可以「促進公共衛生與安全」爲其法定職務，則環保局是否也可以建置傷害監測系統？再者，該規定係爲管理 TIPSPA 傷害監測系統與傷害監測資料，則如此大規模蒐集民眾個人資料的法規授權爲何？況傷害監測系統已涉及人民之隱私權之限制，豈可在沒有法規授權的情形下任意爲之？因此，在立法技術上，應注意法律保留原則之遵守。

(2) 個人資料保護法第 15 條第 2 款係規定須「經當事人書面同意」。惟個人資料保護法第 7 條第 1 項規定：「第十五條第二款及第十九條第五款所稱書面同意，指當事人經蒐集者告知本法所定應告知事項後，所爲允許之書面意思表示。」可知，立法者有意藉由所謂「告知後同意」或「告知後選擇」之原則，進一步落實對個人資料所指涉當事人之保護。因此，衛生局亦可履行法定告知義務後而取得當事人書面同意，再進行本案傷害監測所需個人資料之蒐集、處理或利用。由於必須一一當事人書面同意，恐非易事。

(3) 個人資料保護法第 15 條第 3 款規定「對當事人權益無侵害」，衛生局目前基於傷害監測而蒐集、處理或利用個人資料，是否爲對於當事人權益（如隱私權）未造成侵害，實不無疑義。

2．個人資料保護法第 6 條但書各款要件之分析

按個人資料保護法第 6 條規定，有關醫療、健康檢查等個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

(1) 個人資料保護法第 6 條第 1 款係規定須「法律明文規定」及第 2 款係規定須「公務機關執行法定職務」，才可蒐集醫療、健康檢查之個人資料。查現行各項法規關於「TIPSPA 傷害監測系統」者，僅有「台北市政府衛生局傷害監測資料管理注意事項」而已，別無其他規定。由於傷害監測系統已涉及人民之隱私權之限制，上開「台北市政府衛生局傷害監測資料管理注意事項」是否已遵守法律保留原則而認爲符合「法律明文規定」及賦與公務機關「法定職務」，不無疑義。

(2) 個人資料保護法第 6 條第 3 款係規定須「當事人自行公開或其他已合法公開之個人資料」。因此，倘衛生局進行本案傷害監測所需醫療、健康檢查等個人資料係來自於當事人自行公開或其他已合法公開之個人資料，自無疑義。

(3) 個人資料保護法第 6 條第 3 款係規定須「公務機關基於醫療、衛生或犯罪預防之目的，爲統計或學術研究而有必要，且經一定程序所爲蒐集、處理或利用之個人資料。」因此，倘傷害監測系統係衛生局（公務機關）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，且經一定程序所爲蒐集、處理或利用之個人資料，而符合本款之規定，自可爲醫療、健康檢查等個人資料之蒐集、處理或利用。

(三) 特定目的外之利用

在本文訪談過程中，衛生局方面表示，該傷害監測系統研究所得之成果，除了作爲衛生局進行事故傷害防治之外，亦可作爲其他單位形成或改進公共政策或

公共設施之參考。例如，經由分析事故傷害相關資料後，發現某處之公共設施（如天橋、公園、馬路）已有損壞，因而容易造成民眾受傷。則工務局或其他單位即可透過傷害監測資料，發覺問題，進而修復此一公共設施。此際，如果認爲衛生局蒐集、處理或利用個人資料之目的在於公共衛生與安全（應可適用法務部依個人資料保護法第 53 條所指定「特定目的」之「公共衛生」、「衛生行政」、「調查、統計與研究分析」、「學術研究」等）的話，則協助其他單位執行職務，倘符合上開公共衛生與安全目的，則非特定目的外之利用。否則，倘不符原來蒐集、處理個人資料之目的，而屬特定目的外之利用。

而就個人資料爲特定目的外之利用而言，依個人資料保護法第 16 條之規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人書面同意。」因此，倘衛生局傷害監測系統研究所得之成果，用於協助其他單位執行職務，倘不符上開公共衛生與安全目的，則屬特定目的外之利用。此時，本文認爲這裡比較有可能適用的是第 2 款之「爲維護國家安全或增進公共利益」，也就是說，有可能符合「增進公共利益」，而例外地得爲特定目的外之利用。

另外，參照「台北市政府衛生局傷害監測資料管理注意事項」相關規定[55]，除十二個區的健康服務中心、合作醫院以及受衛生局或十二區健康服務中心委託

[55]台北市政府衛生局傷害監測資料管理注意事項第 5 項第 4 款第 2 目：「其他非上述單位：.....

2)研究案所需：填寫「臺北市政府衛生局受理使用『TIPSPA 傷害監測系統』資料申請保密切結書」（附件 2）與「臺北市政府衛生局受理申請使用『TIPSPA 傷害監測系統』資料申請表」（附

研究單位外，其他非屬上述之單位，若爲研究案所需，亦得申請衛生局提供傷害監測系統之資料。本文認爲，此處似有個人資料保護法第 16 條第 5 款「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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人」之適用。

(四) 必要原則

按新修正之個人資料保護法第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法爲之，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。」個人資料保護法第 6 條第 1 項第 2、4 款規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，爲統計或學術研究而有必要，且經一定程序所爲蒐集、處理或利用之個人資料。」個人資料保護法第 15 條第一項第一款規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。」個人資料保護法第 16 條第 1 項第 5 款規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，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，得爲特定目的外之利用：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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。」等，均顯示公務機關於蒐集、處理或利用個人資料時，應受比例原則之拘束。

所謂「比例原則」，乃由法治國家原則衍生而來，在於強調國家進行行政行爲時，「不得爲達目的而不擇手段」，可知，比例原則在於強調目的與手段間之

件 3），經申請單位主管核章後，連同研究計畫摘要函送本局審核，經本局審核通過後，由本局線上篩選資料並下載後，以 Excel 格式提供，且不含身分證字號或病歷號。」

均衡，如西諺所云「不必以大砲打小鳥」或孔子曰「殺雞焉用牛刀」。而廣義「比例原則」包括適當性原則(又稱合目的性原則)、必要性原則及過度禁止原則(即狹義比例原則)。[56]另參照我國行政程序法第 7 條：「行政行爲，應依下列原則爲之：一、採取之方法應有助於目的之達成。二、有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三、採取之方法所造成之損害不得與欲達成目的之利益顯失均衡。」亦屬比例原則之規定。

就個人資料保護法而言，個人資料之蒐集、處理或利用不僅不得逾越必要範圍，並應與蒐集目的具有手段上正當合理之關聯性，不得與其他目的爲不當之連結。例如，在資料蒐集時，必須先審查，該資料蒐集是否必要？其必須有嚴格標準予以衡量，僅在履行具體任務必要時，始得蒐集資料。在必要性之範圍中亦應審查，對於當事人蒐集個人資料時，是否會對其值得保護的利益將造成過度不當的侵害？倘若係肯定的，基於憲法上過度禁止原則，此蒐集個人資料行爲對於行政機關任務之達成，乃屬不必要的。[57]

按法務部 97 年 2 月 18 日法律字第 0970005327 號函釋謂：「本件所提供之人員名冊含有出生年月日及身分證統一編號等重要個人資料，是否逾越必要範圍？有無必要性？應視提供該人員名冊之目的而定，如不提供出生年月日及身分證字號等資料亦能達到目的時，依上開規定，自不宜提供該等資料，以保護當事人隱私權益。」由此可知，蒐集、利用個人資料時，亟應審查其必要性及目的與手段之關聯性。然而，衛生局在建制傷害監測系統，蒐集事故相關資料，因而取得病人個資時是否符合比例原則？換言之，衛生局在取得、處理或利用個人資料時，其目的是否正當？手段是否適當？亦即，所實施之方法是否有必要？目的與手段間是否有合理之關聯？也就是說，所採之方法是否有助於目的之達成？

[56]李惠宗，憲法要義，頁 115，元照出版有限公司，2009 年 9 月。
[57]許文義，「個人資料保護法論」，頁 201，台北，三民書局，2001 年 1 月。

根據本研究之訪談所得資料可知，「台北市衛生局事故傷害外因登錄表」中要求登錄傷者之出生年月日，然而若是需要比較不同年齡層的傷患的事故發生原因，則實際上只需要紀錄出生年份即可，何必完整紀錄出生日期？又例如「台北市衛生局事故傷害外因登錄表」中要求登錄病歷號，然而登錄病歷號之目的究竟爲何？縱然係爲了區別不同件的傷害事故，惟藉由病歷號即可查出當事人之病歷，進一步可直接溯及當事人本人並知悉其他資訊，則此處蒐集病歷號之手段是否過當？爲什麼不另外編製號碼而一定要用病歷號？況且傷害監測系統應該使用「台北市衛生局事故傷害外因登錄表」上的資料即爲已足，不需要再動用病歷資料，病歷本身依其他法律亦應予保密[58]，如果用不到病歷內容，那爲何要病歷號？

就蒐集醫療資訊而言，吾人尚可參考行政院衛生署於民國93年12月17日所訂定之「醫療資訊安全與隱私保護指導綱領草案（最終版）」[59]。在該指導綱領之第3條規定：「蒐集醫療資訊的目的必須遵守相關法律規範及符合最小需求原則。任何醫療機構或醫事相關人員應在符合本綱領所訂之要件下，方可進行蒐集醫療資訊；醫療資訊的蒐集，其目的及範圍應限於保護生命及促進健康之最小需求，並須遵守現行法規。」又第6條係規定：「蒐集醫療資訊的方法必須合法且符合公平正義。醫療機構或醫事相關人員蒐集醫療資訊時，不可採用下列方法：一、使用不法手段；二、不公正的方法；三、對病人的私人事務超越合理期待之探詢。」上開條文，亦可視爲係「比例原則」之具體化規定。另觀察外國立法例，諸如紐西蘭之「醫療資訊隱私條例」[60]，其第1條係規定：「任何醫療機構/人員皆不可蒐

[58] 例如醫療法第 72 條規定：「醫療機構及其人員因業務而知悉或持有病人病情或健康資訊，不得無故洩漏。」

[59] 行政院衛生署，93 年度「確立及推廣醫療資訊安全與隱私保護之政策計畫」期末成果報告，2004 年，第 88 頁到 97 頁。請參閱 http://www.doh.gov.tw/CHT2006/DM/DM2_p01.aspx?class_no=94&now_fod_list_no=8919&level_no=4&doc_no=40772

[60] 請參閱 http://www.doh.gov.tw/ufile/doc/%E7%B4%90%E8%A5%BF%E8%98%AD1994%E5%B9%B4%E9%86%AB%E7%99%82%E8%B3%87%E8%A8%8A%E9%9A%B1%E7%A7%81%E5%AE%88%E5%89%87.pdf

集醫療資訊，只有在符合下列情況時，才可進行蒐集：(a) 資料的蒐集，其目的必須合乎法律，且與醫療機構/人員的職責或活動相關；且(b) 資料的蒐集必須是達到該目的不可或缺的要素。」其第4條則規定：「醫療機構/人員：蒐集醫療資訊時，不可採用下列方法：(a) 使用非法手段；或(b) 在一些情況下，採用下列方法：(i) 不公正的方法；或(ii) 對相關當事人的私人事務有不合理程度之干預。」本文以為，上開條文之規定，無論是我國抑或是外國之規定皆可視為是「比例原則」之具體化規定。

除此之外，該指導綱領亦提出「最小需求原則」，依指導綱領之前言：「.....本綱領提出以下九項原則：壹、最小需求原則：當醫療機構或醫事相關人員蒐集、使用或揭露醫療資訊時，或向另一醫療機構或醫事相關人員要求醫療資訊時，該醫療機構或該醫事相關人員必須做合理之努力，將蒐集、使用或揭露醫療資訊的範圍降至最低限度.....」準此，在蒐集、利用醫療資訊時，非但僅得於必要範圍內為之，而且應盡量限縮其範圍。因此，所取得之資訊應越少越好。另可參考外國法之規定。按美國之「可辨識個人身分的醫療資訊隱私標準」[61]之45CFR§164.502(b)(1)規定：「適用最低限度規定：使用或揭露受保護醫療資訊時，或向另一涵蓋實體要求受保護醫療資訊時，涵蓋實體必須做合理之努力，將揭露或使用之受保護醫療資訊降至最低限度，來達成使用、揭露、或要求的目的。」又按英國「一般電子醫療紀錄之良好運作方針」（Good practice guidelines for general practice electronic patient records）提出了「必須知道」（need-to-know）原則。學者認為，「必須知道原則」與上開美國法相當，都是為了避免醫療資訊的不當使用與揭露，是個人醫療資訊隱私保護的核心理念之一。[62]

本文認為，前開「醫療資訊安全與隱私保護指導綱領草案（最終版）」之相

---

[61] 請參閱 http://www.doh.gov.tw/ufile/doc/%E7%BE%8E%E5%9C%8B%E5%8F%AF%E8%BE%A8%E8%AD%98%E5%80%8B%E4%BA%BA%E8%BA%AB%E4%BB%BD%E7%9A%84%E9%86%AB%E7%99%82%E8%B3%87%E8%A8%8A%E9%9A%B1%E7%A7%81%E6%A8%99%E6%BA%96.pdf

[62] 張乃文、宋佩珊，各國個人醫療資訊隱私標準之法制研析，醫事法學第 17 卷第 2 期，2010 年，第 82 頁

關規定與所謂的「最小需求原則」亦可適用於衛生局為進行傷害監測系統而蒐集、利用事故相關資料之情形。尤其是傷害監測系統所需之資料，目前皆是由第一線之急診室護理人員負責蒐集，護理人員即符合「醫療資訊安全與隱私保護指導綱領草案（最終版）」前開條文中之「醫事相關人員」。再就「最小需求原則」而言，衛生局亦應留意之，即使所蒐集之資訊係屬必要，也不能蒐集太多。故「台北市衛生局事故傷害外因登錄表」應更為精簡。例如，前開所舉之「出生年月日」部分，出生之月日即屬多餘，或學歷調查亦可能為多餘。

(五) 告知義務

按個人資料保護法第 8 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，得免為前項之告知：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。」又按個人資料保護法第 9 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蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。有下列情形之一者，得免為前項之告知：一、有前條第二項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人為告知。四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。第一項之告知，得於首次對當事人為利用時併同為之。」可知，為落實「告知後同意」原

則，間接蒐集資料時，除符合得免告知情形者外，均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項。另爲減少勞費起見，允許得於首次對當事人爲利用時得併同告知。

蓋個人資料之蒐集，事涉當事人之隱私權益。爲使當事人明知其個人資料被何人蒐集及其資料類別、蒐集目的等，於蒐集時或處理、利用前應告知當事人之事項，俾使當事人能知悉其個人資料被他人蒐集或處理或利用之情形。因此，蒐集、處理或利用個人資料之公務機關，原則上負有告知之義務。

本案中，衛生局縱係由醫院急診室醫護人員處「間接」蒐集事故傷害資料，因此，，衛生局仍應向當事人善盡告知義務。或謂衛生局可依個人資料保護法第 8 條第 2 項第 2 款之「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」或第 9 條第 2 項第 4 款之「基於公共利益爲統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者爲限」）而主張免爲告知，惟本文認爲此處是否爲衛生局之法定職務範圍仍有疑問或其蒐集之個人資料仍可識別特定當事人，已前所述。在釐清之前，依「例外從嚴」之原則，且本於保護當事人權益之立法意旨，衛生局仍不得免其告知義務。

事實上，就告知義務而言，本文認爲，在本件之衛生局建置傷害監測資料庫的情形，可參考學說上針對設立全民基因資料庫之討論。蓋兩者同樣都是蒐集、處理個人資料，又皆影響隱私權甚鉅。況個人資料保護法第 6 條第 1 項亦將醫療資料與基因資料同樣列爲「特種資料」，是以兩者可相提並論。學者認爲，在醫學相關研究中，若以人爲研究對象時，必須取得個別研究對象之在經過說明，充分明瞭後所爲之自願同意，此即所謂的「告知後同意」原則[63]。之所以須先爲告知並取得同意，其理由有二：第一，尊重被研究對象之「人的尊嚴」與「個人自主性」。蓋這些資料與當事人密切相關，甚而有很多資料連當事人本人自己也弄

[63] 劉宏恩，冰島設立全民醫療及基因資料庫之法律政策評析－論其經驗及爭議對我國之啓示，台北大學法學論叢第 54 期，2004 年，第 85 頁。

不清楚，這些資料已涉及其私領域範圍。況研究者進一步爲利用之結果有可能會影響當事人之生活或他人對當事人之認知，故應使當事人知情，並使當事人得以選擇是否參與。否則，即可能侵犯當事人之私人空間，損及當事人之自主性與選擇自由。[64]第二，爲保護當事人免於受到無從預料或防範的傷害。例如，資料有安全保密上的疑慮、資料會轉交第三人使用等。況研究者與當事人之利益未必一致，容易造成「利益衝突」的情形。[65]

本案中，特別是衛生局在建置了傷害監測資料系統後，如又接受其他人之申請且提供資料[66]時他人就傷害監測資料的利用，有可能對當事人造成不利的後果。因此，除了衛生局有義務防止資料遭到濫用外，至少應讓當事人有被告知的機會。

(六) 個人參與原則

按個人資料保護法第 10 條規定：「公務機關或非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。但有下列情形之

[64]劉宏恩，冰島設立全民醫療及基因資料庫之法律政策評析－論其經驗及爭議對我國之啓示，台北大學法學論叢第 54 期，2004 年，第 86 頁。

[65]劉宏恩，冰島設立全民醫療及基因資料庫之法律政策評析－論其經驗及爭議對我國之啓示，台北大學法學論叢第 54 期，2004 年，第 87 頁。

[66] 按有權申請之人的範圍很廣，參照台北市政府衛生局傷害監測資料管理注意事項第 5 條第 1 項：「申請資格：十二區健康服務中心、合作醫院、本局或十二區健康服務中心委託研究單位、其他非上述單位。」條文中所指之「非上述單位」即無其他限制。又同條第 2 項第 4 款：「其他非上述單位：(1)推動事故傷害預防與安全促進實務所需：填寫「臺北市政府衛生局受理使用『TIPSPA 傷害監測系統』資料申請保密切結書」（附件 2）與「臺北市政府衛生局受理申請使用『TIPSPA 傷害監測系統』資料申請表」（附件 3），經申請單位主管核章後，函送本局審核，經本局審核通過後，由本局線上篩選資料並下載後，以 Excel 格式提供，且不含身分證字號或病歷號。(2)研究案所需：填寫「臺北市政府衛生局受理使用『TIPSPA 傷害監測系統』資料申請保密切結書」（附件 2）與「臺北市政府衛生局受理申請使用『TIPSPA 傷害監測系統』資料申請表」（附件 3），經申請單位主管核章後，連同研究計畫摘要函送本局審核，經本局審核通過後，由本局線上篩選資料並下載後，以 Excel 格式提供，且不含身分證字號或病歷號。」由此可知，其他單位僅須爲「推動事故傷害預防與安全促進實務所需」或「研究案所需」即可申請。

一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」十一條規定：「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。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。違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。」可知，針對公務機關蒐集之個人資料檔案，當事人得要求查詢、閱覽、製作複本、補充或更正；就個人資料正確性有爭議者，應主動或當事人得請求停止處理及利用。

因此，倘當事人出面請求停止或刪除傷害監測資料中的個人資料部分時，應如何處理？當事人依個人資料保護法之權利就應如何行使，在上開「台北市政府衛生局傷害監測資料管理注意事項」完全付之闕如，此為一重大的立法漏洞，亟應修補之。

第四節　社會局

壹、 與個資法有關的社會局業務概覽

台北市社會局就其所職掌業務範圍，會有大量蒐集、處理或利用個人資料需要之行政事務者，主要係依社會救助法、身心障礙者權益保障法、老人福利法、兒童及少年福利與權益保障法、特殊境遇家庭扶助條例等，受理各類福利服務對象之各項補助案申請；或依人民團體法、合作社法等，人民團體或合作社需提供理（董）、監事名冊予社會局，詳細清單如下：[67]

1. 社會救助類：包含綜合處理、低收入戶及中低收入戶、中低收入老人生活津貼、身心障礙者生活補助、舊系統資料查詢、醫療補助、代賑工審核等。
2. 身障福利服務類：房屋租金補貼、參加社會保險保險費補助、身心障礙者日間照顧及住宿式照顧費用補助、身心障礙者生活輔助器具費用補助、發展遲緩兒童療育補助、參加社會保險保險費補助等。
3. 老人福利服務類：老人收容安置費用補助、中低收入長者修繕住屋補助、老人健保自付額補助、老人乘車補助、重陽敬老禮金補助、中低特別照顧津貼等。
4. 婦女福利及幼兒托育服務類：助妳好孕-育兒津貼、臨時托育補助、第三胎以上家庭部分托育費用補助、非就業者弱勢家庭臨時托育費用補助、就業者家庭部分托育費用補助、弱勢家庭兒童托育補助、特殊需求兒童補助及特殊境遇家庭扶助補助、婦女庇護安置補助等。
5. 兒少福利服務類：弱勢家庭兒童及少年緊急生活扶助、低收入戶暨弱勢兒童及少年醫療補助、中低收入戶兒童及少年全民健康保險保險費自付額補助。
6. 社會工作類：各類福利服務對象之個案資料等。

[67] 參閱附件一（社會局訪談協力事項說明回覆）。

7. 人民團體、合作社、財團法人基金會部分：發起人名冊、會員名冊、選任人員（理監事）簡歷冊、社員名冊、清算人就任報告書、 董事（監察人）名冊等。
8. 各類公立兒少老殘機構部分：申請登記進住、個案處理及住民基本資料等。
9. 其他部分：員工薪資及外聘專家學者出席費所得申報；另文書處理部分因總收文、發文人員及檔管人員作業所需，需接觸處理大量的民眾申請案件及所檢附之相關個人資料等。

針對上述社會局的職掌攸關個人資料保護的部分，經由與社會局承辦人員的訪談，研究團隊歸納出以下幾個問題面向：

貳、 社會局主動蒐集之資料

一、 直接從當事人獲取

依照個人資料保護法第十五條之規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人書面同意。三、對當事人權益無侵害。」社會局執掌台北市社會福利服務之規劃與推展，舉凡救助服務、不同族群與對象之保護、支持、成長與發展等福利政策與措施、社區工作、志願服務等均屬業務範疇，爲完成上述任務，社會局主動蒐集處理欲協助對象的個人資料，往往是履行上述職責的第一步。

例如，依照「**臺北市老人自費安養機構進住自治條例**」、「臺北市立陽明教養院入出院自治條例」、「臺北市政府婦女中途之家管理辦法」，有居住與安置需求的老人、身心障礙者與女性單親家庭，若申請進入市府所設的各種安養機構與中途之家，依規定必須要提出一定的申請文件，社會局方得審核其入住之請求。

[68]準此，一個在個資上可能面臨的疑慮是：人民若主動申請中途之家，若只是短期入住而後離開，社會局會不會依據該人於申請時所提供的資料，後續再去針對申請人作一些申請範圍以外的社會福利的提供？ 例如發現其剛好是低收入戶或是身障者，在未經其同意的情況下，主動請社工人員提供各種社會福利申請上的協助？

就此問題，於訪談中，社會局人員答覆以：「通常住宿機構入住後都會住到 65 歲，鮮有中途離開問題。若發現其有額外的需要，通常亦係由社工去告知其家屬來替她作申請，社工員則上不會主動替其申請。」

實則，以單親女性家庭的中途之家爲例，依「臺北市政府婦女中途之家管理辦法」第七條規定，進住人進住期間以一年爲原則，是以實務上仍存有短期居住的可能性，而依同辦法第八條並規定：「進住人於進住期間內，社會局得依其個別家庭狀況，擬定服務計畫，結合社區資源，提供家庭支持性服務，協助其心理及社會適應。」是以若在進住人進住期間，不論是從其申請文件上抑或是從實際入住期間的生活表現，社會局人員得知其有需協助之處，自應盡輔導之責，此一責任，解釋上並不應因進住人搬離而有異，蓋畢竟在社會局的資料中，既已曾有當事人受輔導之記錄，社會局社工人員持續的追蹤與關心，仍屬合於社會局行政目的內之行爲。故本研究團隊認爲，相關法規有必要明白將此一追蹤輔導的義務明文化，俾利行政機關將來有需要延續運用相關個資時，其資料運用合目的性的主張免受質疑。

二、 透過其他公務或非公務機關獲取

[68] 例如「臺北市政府婦女中途之家管理辦法」第五條即規定：「申請人應檢附下列文件，向社會局提出申請：一、申請書。二、國稅局開立之最新年度全家各類所得資料清單及財產歸屬資料清單。三、最近三個月內全戶戶籍謄本。四、申請人及其子女最近三個月內公私立區域級以上醫院出具之健康檢查證明（含胸部 X 光檢查）。五、其他相關證明文件。（第一項）社會局受理申請後，派員進行訪視評估，並於十日內函復審核結果。第一項第二款及第三款文件，得由申請人授權社會局自行調閱。（第二項）」

社會局透過其他機關獲取資料，在個人資料保護法上呈現的主要問題點，在於此種非直接向當事人所爲的資訊蒐集，是否合乎個資法第九條的規範要求。[69] 以社會局與稅務機關的往來資訊流通爲例，根據「臺北市身心障礙者生活托育養護費用補助須知」之規定，身心障礙者依「身心障礙者生活托育養護費用補助辦法」申請生活補助費時，主管機關須分別函請國稅局及稅捐稽徵單位提供申請人全戶人口所得及財產資料並據以審核，[70] 對於此一資料蒐集的職務履行，在個資法施行後，是否對社會局（以及負責第一線執行的區公所）構成特別的障礙？

就研究團隊此一疑問，社會局人員認爲個資法的實施尚不構成障礙，因爲此爲社會局執行身心障礙者福利措施的基礎前提事項，就此中央主管機關內政部與財政部事先已有協調，故就社會局這一部分而言，並沒有資料獲取上的困難。[71] 儘管如此，研究團隊以爲，就前述個資法第九條的規範要求，在此一補助關係中，社會局原則上仍有依法履行事前告知義務的責任，始符合本研究第三章所揭示的個人資料「蒐集限制原則」。對此，行政機關習以個資法第八條第二項第二款「個人資料之蒐集係公務機關執行法定職務所必要」作爲豁免告知義務的事由，但實則，在「管轄法定原則」之下，行政機關原本即不得爲法定職務外之行爲，[72] 本款規定之立法不當十分明顯。故本研究團隊認爲，行政機關仍宜在補助辦法或補助須知中，將事前告知的手續明確化，以杜爭議。

再者，針對訪談前的書面提問，社會局曾回答該局在執行業務時，爲審核之需要常須請求其他單位協助提供資料，其中亦包含不少非公務機關。例如，社會局幾乎所有的業務都會涉及到財稅調查，調查中有一個項目爲動產，動產內部就

[69] 個人資料保護法第九條：「公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。」

[70] 臺北市身心障礙者生活托育養護費用補助須知第 4 條第 2 項第 3 款：「（區公所負責）統一造冊，分別函請國稅局及稅捐稽徵單位提供申請人全戶人口所得及財產資料並據以審核。有關造冊函查之資料，應依稅捐稽徵法第三十三條規定負保密責任。」

[71] 當然，就作爲資料直接蒐集者的國稅局，將所掌管的資料移轉予其他機關，是否合於個資法第 15 條、第 16 條之規定，則屬另外的問題。

[72] 關於管轄法定原則，參 吳志光，行政法，頁 123（2010）；蔡震榮，管轄權之意義，收於：「行政法爭議問題研究（上）」頁 315-316（2000）。

會包含「投資」此一項目，所以個人投資與證券往來都是社會局所須審核的對象。而基於對審查正確性的要求，有必要項此種資料的匯集地──「集保中心」請求資料。[73] 但因爲集保中心的資料是來自於各個證券商，且非公務機關罰則也較重，造成他們在資料提供方面很爲難也很謹慎。但在個資法實施後，「集保中心」明確表示礙於個資法，不願提供資料予社會局審核，且目前仍無法協調。[74]

社會福利工作的推動是社會局主要職責，因爲國家資源的有限性，國家的給付往往只能爲限定性分配而難以雨露均沾，主管機關必須確保其作爲係將國家資源作最有效的利用，分配給最有需要的人。準此，若補助申請人只要將其財產變爲股票，社會局即無管道知悉申請人有多少資產的話，此一行政目的勢將難以達成。是以，爲解決此一難題，恐怕仍應寄望「法律明文」始爲正途。而考慮到此等社會福利行政上的需要有全國一致性，研究團隊認爲中央主管機關應該要制定法規命令做爲地方主管機關向集保中心（以及類似機構）取得資料法源。在中央未立法前，建議台北市政府可針對台北市政府的社會福利補助事項，在同時特定社會局取得資料的應用範圍之配套下，訂定自治條例以爲規範。

參、 社會局從他機關被動獲取資料

除了社會局主動透過其他機構獲得資料外，實務上社會局亦有許多被動接收其他公務機關或非公務機關移轉資訊的機會，如果此一資訊具有「個案性」、屬於可透過直接或間接方式識別的個人資料，即生個資法適用上的問題。[75]例如，

[73] 雖然社會局亦可向國稅局請求提供資料，但因爲國稅局的資料有不少也基於課稅需要自他處間接取得，且其資料亦較集保中心還要舊，有時效性的問題（因爲國稅局蒐集資料室爲了前一年度的「報稅」，與集保中心所擁有的最新且及時的「投資」資料有一段不小的落差）。

[74] 「集保中心」的態度較爲強硬實有跡可尋，蓋集保中心的資料是來自於各個證券商，而非直接從當事人取得；加以集保中心乃非公務機關，個資法上的罰則較重，是以在資料提供方面採取較爲保守謹慎的態度，應可理解。

[75] 相對地，如果社會局獲取的資料是屬於「一般性」，例如統計性質的資料，基本上就不生個資法問題。例如研究團隊曾詢問社會局有關社會福利行政委外業務的監督、管理與獎勵的過程中，社會局的資訊獲取問題，社會局的回答是：委外機構所呈報的績效資料，基本上都是非個案的數據等，社會局的審查標準完全依照內政部頒布的「身心障礙福利機構獎勵辦法」，

低收入戶在遷戶籍之時，依「臺北市低收入戶生活扶助及低收入戶、中低收入戶調查及審核作業要點」第 18 條規定，戶政機關須副知社會局，就此，即生戶政機關在受理戶籍遷移時有無主動告知人民將來會將此一資訊轉知社會局的疑義。

對此，社會局人員回答：「因爲對於低收入戶的生活扶助，低收入戶本有此一業務屬於社會局業務的認知，公所與戶政機關都只是窗口。且若遷移戶口後社會局找不到人，受補助的資格就會被取消。所以人民爲了維護他本身的權益，甚至還會主動告知。此外，雖然受理戶籍遷移的戶政機關並未告知申請人，但此一通報義務在低收入戶最初向社會局申請補助時，社會局就已經有告知，因此不生違反個資法的問題。」

類似的情形，還有「臺北市低收入戶生活扶助及低收入戶、中低收入戶調查及審核作業規定」，將調查與審和職責區分成兩塊，一部分由社會局，另一部分由區公所執行。如是若有些事務的辦理，有些人直接找社會局，有些人找區公所，在後者情況由區公所所收集的資料，如何以合於現行個資法的方式，將資料移轉由社會局來作使用？ 對此，社會局的回答則是：「社會救助法就此已有規定，地方自治團體可自行對地方執行生活扶助的審查業務作分工，所以市府就此其實是直接委託授權給社會局跟各區公所來辦理社會救助審查業務。且一開始在文件上就有很明白的揭露此類資料之後會交由社會局來作複審。就此類法律有明文規定的情況，與現行個資法並無違背。」

純就此一問題觀之，社會局的回答並無問題，蓋基於補助之需要獲取當事人資訊，對當事人而言係無權益侵害（甚至是有利於當事人權益）之行爲；[76] 再者，戶政機關轉呈的資料多僅爲設籍住所、財產清冊等資料，性質較爲單純，故較無爭議。但若有其他補助業務，相關機關轉呈的資料係屬於「敏感性資料」者，

原則上審查的重點也不在於個案的好壞。

[76] 個資法第十六條第一項第六款甚至將「有利於當事人權益」列爲可對資訊作目的外使用的事由。當然，本款規定，所謂的「『有利』於當事人」固易滋生判斷上的疑難，但起碼就政府補助一事，係對當事人有利應無疑義。

那麼處理上恐怕就必須作更審慎的考量。[77]　例如，依照「臺北市低收入戶生活扶助及低收入戶、中低收入戶調查及審核作業規定」第十七條第六款、第八款的規定，關於「入獄服刑、因案羈押或依法拘禁」以及「因病經醫師診斷需住院三個月以上之治療或療養」等資料，受補助的低收入戶皆有陳報區公所的義務。而依照個資法第六條之規定，縱使公務機關爲執行法定職務，有蒐集、處理、利用敏感性資料的必要，仍須有「適當安全防護措施」的配合，但目前主管機關似乎對於敏感性資料應該要有更進一步的「適當防護措施」的意識。[78] 對此，研究團隊認爲有進一步在機關的作業要點中，明訂應如何防護資料不當外洩與利用的規定，始爲妥適，如是方合乎「安全維護原則」的要求。

肆、 其他機關向社會局調閱資料

社會局就其所掌業務所保有的資料，其他機關請求調閱的情況亦所在多有，例如關於依據身心障礙者權益保障法第七十一條第一項第六款的規定，地方政府得提供身心障礙者房屋租金補貼。爲獲得此一補助，身心障礙者須要出具確實租約來申請，但一般民眾的認知是，一旦領取租屋補助，房東就會被國稅局查稅，社會大眾的疑問是：爲何房東沒有主動申報，而承租人向社會局申請補助，到最後卻被國稅局查到進而向房東課稅？ 社會局提供資料給國稅局是否有違個資法

[77] 雖然依據法務部的命令，個資法第六條關於敏感性資料的規定尚未施行，但爲未雨綢繆，本計畫仍將其列入研究範圍。

[78] 研究團隊於訪談過程中，曾以「臺北市政府補助低收入戶老人孕產婦及嬰幼兒營養品代金實施要點」第三條要求申請人需檢附「公私立醫療院所診斷證明書」爲例，詢問社會局人員，在個資法施行後，有無採取特別的「安全維護措施」，社會局人員則答以：「此類資料送給審核人員經過程和及歸進檔案室過程中，只有負責審核的人得以看見，且此資料不會電腦建檔，沒有權限控制的問題，情形較爲簡單。」

在敏感性資料之外，依據社會局的說明，目前已建立的一般性的資訊安全防護機制，有「每年辦理 2 次平時檢核及 2 次內部稽核，並已辦理 4 梯次講習加強同仁個資保護觀念。同仁在蒐集、處理部分會更謹慎，利用部分原則從嚴，例如：個資法施行後資料保管上會增加保密機制（書面資料在資料櫃內加鎖處理，電子檔則加密保管），並由專人負責。處理與利用上會增設無法直接識別個人資料之機制（如隱蔽姓名之 1 字、身分字號隱蔽後 5 碼等機制）。倘有其他公務機關索取個人資料，應以正式公文敘明索取理由及使用用途，經本局評估、簽核後始提供，又本局會提醒索取單位亦應遵守個人資料保護原則。」參附件四（社會局訪談協力事項說明回覆）。

「原則禁止『目的外的使用』」[79] 的規定？ 對此，社會局人員第一時間的回答係「內政部跟財政部就此已有協調，就財稅稽核必要之資料，可要求各單位提供而且要求各縣市一律配合。」 經本研究團隊提醒，縱使中央機關已有協調，社會局提供補助申請人的租屋資料給稅捐稽徵機關，仍屬百分之百的「目的外使用」而有悖於「使用限制原則」，社會局人員方答以目前已在租屋補助的申請文件上加註告知人民。準此，確可解爲當事人申請時，即已同意社會局將資料轉交給稅捐稽徵機關，而可免於違反個資法的指摘。

另一個實務上引發社會局困擾的案例，國家通訊傳播委員會（NCC）爲加速我國通訊傳播數位化的進程，推動電視數位化的政策，爲鼓勵民眾收看高畫質的數位節目，針對低收入戶，提出免費提供數位電視機上盒的方案，爲此，希望各縣市政府提供相關名冊以爲配合。對社會局而言，此一要求的爲難之處在於並非所有的低收入戶皆有使用機上盒收視的意願，但 NCC 以公共利益之名要求社會局必須提供資料，內政部亦行文要求各縣市配合，社會局配合的結果，卻引來民眾對於其低收入戶身分曝光感到不舒服的抱怨，上述問題，

關於此一爭議，突顯出下列兩個個資法在適用上的問題：

第一：雖然說社會局保有低收入戶的相關資訊，其目的多半與「補助」有關，但數位機上盒的補助，主管機關卻是中央的 NCC，此時社會局將低收入戶的資料提供給 NCC，解釋上是否仍在社會局的業務範圍內，且屬於合於「行政目的」的使用？

第二：若認爲數位機上盒的免費提供，完全與社會局的業務無關，社會局提供低收入戶資料予 NCC 已經構成「目的外使用」，那麼此一行爲是否得以個資法第十六條第二款「增進公共利益」或是同條第六款「有利於當事人權益」，允許行政機關對持有的資訊作目的外使用的規定予以正當化？

[79] 個資法第十六條參照。

研究團隊以爲，數位電視的收看，現階段仍難被認爲係「人民生活的基本需要」，除非相關的社會福利法規有明文規定，否則依現行的法規結構觀之，數位電視機上盒的免費提供，係通訊傳播產業政策的一環，將其納入社會局的職責範疇，實過於牽強。職是之故，社會局提供低收入戶的清冊給 NCC，實已構成於「目的外使用」，個資法第十六條雖然列有例外得對資料爲「目的外使用」之規定，但以前舉的兩款規定爲例，恐怕都有過於概括之嫌，容易引發爭議。行政機關的行政行爲，要說都沒有公益、公共性的成分，恐怕很難，要是有一點跟公益沾上邊，就可以對資料作目的外使用，那麼個資法的規定無異形同具文，是以，本款的規定，解釋上其公益的份量必須相當高度、充分始足以正當化。就提供少數的低收入戶數位電視機上盒，對於我國電視數位化的政策目標之達成，是否已經有顯著的效果，而可認爲達到「高度」公益的標準，恐不無疑問。又若是以「對當事人有利」作爲理由，亦屬片面，蓋若一項給付行政的措施帶有效果的「雙面性」——亦即該給付同時對當事人帶來「授益」與「侵益」的效果，那麼是否仍屬「對當事人有利」？ 所謂的「對當事人有利」在判斷上是否應該排除當事人「主觀」的認知？ 凡此，皆屬運用此款規定正當化「目的外使用」時可能產生的爭議。

是以，研究團隊認爲，正本清源之道，還是以「回歸法治」爲宜。要之，行政機關如欲對資料作目的外使用，應盡量援用個資法第十六條第一款的「法律明文規定」作爲準據，[80]就此，市政府或可考慮行文中央主管機關，請求其於修訂相關法規時，將數位化業務的執行需地方政府的協力明文化；又或者是將推動的權限在地方的層級，直接下放給地方政府，讓推動電視數位化的補助業務納爲地方社會福利措施的一部份，才是根本解決之道。

伍、 人民請求社會局停止利用或刪除資料

[80] 誠然，有法律依據只是解決行政法層次的合法性問題，中央於立法之際，必須注意規範內容不可對人民的隱私造成過度的侵害，以免衍生合憲性的爭議。

依照個資法第三條第四、第五兩款之規定，當事人得請求主管機關停止蒐集、處理或利用，甚至是請求刪除個人資料，此一規定之意義，實乃個資法中尊重「個人資料掌控」精神的落實，在社會行政實務上，可能的問題，例如本來是低收入戶後來變成非低收入戶後要求社會局將其資料刪除，或是身心障礙者爲避免在就業等方面遭受困難或負面的烙印效應，要求主管機關刪除其曾領取補助的紀錄。對此，社會局人員答以：「已較常發生的身心障礙的案例爲例，本局曾詢問過內政部，但內政部表示基本上身心障礙的鑑定表要永久保存，儘管這麼做沒有法律依據，但後來經過協商之後，決定將該等資料作「永久隱藏」，因爲有些人在要求刪除後隔一段時間會再要求回復該身分，所以不刪除有其實務執行上需要。再者，身心障礙手冊等文件的核發，其辦法是中央所訂定，地方機關不能超越母法去作規定。」

就此問題，研究團隊以爲，雖然現階段尚無人民對於「永久隱藏」此種作法表示不滿，且研究團隊亦不否認「永久隱藏」是一種合乎社會福利行政目的的折衷作法（畢竟人民的目的只是不要那些資料在機關與機關間或機關對外的資訊交換間出現）。但考慮到個資法第三條既然已經給予當事人請求「刪除」資料的權利，「永久隱藏」仍然只能算是一種「權宜措施」，爲求整體社會福利法制的完善，將選擇進入或退出社會福利機制的選擇權交還人民；加以考慮到社會福利行政和其他行政領域相較，恐怕存有更高的「隱私保護」的需求性，[81]即便因應行政作業的需要，須採取「永久隱藏」以代替「刪除資料」，此一作法，未來仍有在相關法規修訂時，一併予以明文化的需要。

[81] 關於社會國原則下的給付行政措施，爲何有更高的隱私權需求，參 孫迺翊，「社會給付請求權、當事人協力義務與隱私權保障」，收於：司法院主辦，司法院大法官一百年度學術研討會論文集（下冊），2011 年 12 月 3 日。

第五節　民政局

壹、 民政局與個資法有關的業務概覽

台北市民政局就其所職掌業務範圍，會有大量蒐集、處理或利用個人資料需要之行政事務者，主要有下列行政事務：

1. 本市各區里長、鄰長等之個人資料。
2. 宗教財團法人董事及監事名單、祭祀公業派下員。
3. 戶籍資料。
4. 新移民資料。

就民政局上述其認爲有可能會牽涉到個資法的部分，經由研究團隊研擬訪談問題後，大概可將訪談結果分成幾個面向呈現：第一係「其依職權主動蒐集人民個人資料所衍生的問題」、再者係「其他機關行政機關向該局索取資料之情形」、第三是「人民向其索取他人個人資料的問題」、第四則是「其他重要問題」，以下分述之：

貳、 民政局主動蒐集之資料

一、 直接從當事人獲取

原則上凡民眾出生、結婚、離婚、死亡、遷徙等資料皆爲戶政系統資料中顯現，故民政局所擁有的民眾個人資料可說是多以民眾主動提供爲大宗。有鑑於民政局掌握如此大量的個人資料，研究團隊提出了一個疑問：民政局所掌多半爲民眾的基本資料，該等資料往往有助於其他行政機關執行職務，而有非常大的可能會在行政機關間流通。而依現行個人資料保護法第十六條但書第七款，若要將當初人民提供的資料作原蒐集目的範圍外之使用時，必須經當事人書面之同意。然而，經研究團隊訪談後發現，民政局在給予人民申請戶籍的申請書中，並無類似的告知條款。惟依照民政局說法，若其他行政機關對此等資料欲爲利用時，由於

此項使用逸出原本民政局蒐集此等資料的目的，從而其並不會提供此等資料。

而且由於針對戶政資訊的部分，主要皆依內政部相關規定辦理，[82] 就此民政局依法能置喙的空間有限，從而在內政部因應個資法採取進一步措施之前，爲避免滋生牴觸個資法的疑慮，民政局受訪人員表示，若其他機關對此類資料有使用上之需求，將在該項之料欄位上加註「告知條款」，使人民知悉該資料有可能會被其他機關所利用，並徵求其同意，並請求其簽名，以符合「蒐集限制原則」中「告知後同意」的要求。

研究團隊認爲，加註「告知條款」的作法確實可解決大部分民政局保管之資料是否得流通至其他行政機關的問題，至於其他機關應合於何種要件，始得向民政局請求調閱民眾資料，則應屬於本節第貳部分層次的問題。

二、透過其他機關獲取──以新移民個人資料爲例

研究團隊於訪談時，詢問民政局人員：「貴機關有無非經當事人本人所集得之資料？ 就該資訊處理或提供時，實務上有無遵守第九條告知義務或者因爲存在有同條第二項免於告知之情形而豁免此一義務的情事？」就此，民政局人員以新移民個人資料的蒐集與處理爲例作說明，在日常行政作業上，有關新移民的個人資料，民政局並非直接向當事人蒐集取得，實務上多係由移民署蒐集後，送至內政部，民政局再間接取得。

有鑑於一旦民政局使用該資料係在其執行法定職務範圍內所必要者，依現行個人資料保護法第九條第一款規定，機關若有「執行法定職務」之必要，得免除此項通知義務。對此，研究團隊一貫的立場是：行政機關本來僅只能在法定職務範圍內爲各項行爲，若僅以「執行法定職務」作爲限制之要件，仍有無法達到個人資料保護法立法目的之疑慮，蓋行政機關絕大部分對於個人資料之利用，應皆

[82] 內政部對於各縣市民政局的業務處理，常制訂相關辦法或是透過行政函釋予以指示和督導。例如針對無戶籍人口補辦戶籍登記，訂定有「無戶籍人口補辦戶籍登記注意事項」；爲提供各機關應用戶役政資訊，發揮資訊資源共享效益，內政部戶政司訂有「各機關應用戶役政資訊連結作業及管理要點」等。

可該當「執行法定職務」之要件。因此，爲澈底杜絕爭議，針對此類的「間接蒐集」，民政局仍以訂定作業性的行政規則，建立明確的標準作業程序爲宜。

參、 其他機關向民政局調閱資料

從訪談內容中，研究小組得知其他機關向民政局索取資料的情形在其平常處理的業務當中，亦佔了極大的部分，諸如社會局、衛生局、稅捐處、健保局等機關，基於業務需要，時常向民政局索取個人資料。對此，受訪的民政局人員並表示，機關與機關之間檔案傳輸部分，現階段主要係遵循內政部網站所規定的連結介面而爲規範，惟在遵守上述內政部的辦法之外，民政局人員表示民政局還是會作某種程度的審核，包括：在機關間索取個人資料時，除須檢具「申請目的」、詳列「申請理由」外，還須檢具「內部稽核作業管制流程」，惟這種作法本身並非出於具體的法規根據，而是實務上藉由反覆的施行所形成的慣例。

在訪談中，民政局人員反映在實務上，針對其他機關向民政局索取資料的情形，下列情形常令承辦人員十分困擾：「很多機關會向我們民政局要資料，而且都會主張他們是在執行其『法定職務』。但很多我們認爲根本不屬所謂的『法定職務』，而只是機關單純想要了解詳情，就會來跟民政局要資料。例如僅僅訂個抽象的計劃、甚或主張是市長交辦的政策，就要求民政局提供有關資料，難道這樣我們就必須提供嗎？」

就此問題，研究團隊初步認爲，所謂「機關的政策」或長官「交辦」的任務，如果請求機關確實提出「具體明確的會議記錄」作爲請求提供資訊的根據，那麼從機關協力的角度觀之，民政局恐怕也是沒有拒絕餘地。但爲求執法明確起見，對於其他機關請求民政局提供當事人的戶政資料，民政局內部宜針對「請求移轉資料機關的說明義務」、「請求機關應提出何種具體的文件資料佐證」與「資料移轉的手續與相關資訊安全維護措施」等事項，訂定作業準則以資規範。

肆、 一般民眾向民政局索取他人個人資料之情形

對於一般人民向民政局請求其他人之戶籍資料者，民政局表示，其大體上悉依政府資訊公開法以及檔案法之相關規定〈例如：政府資訊公開法第十八條第六款之「公開或提供有侵害個人隱私、職業上秘密……」則不予公開之〉爲辦理，惟手續上並無如同警察局有另訂定資料索取規則，而皆參照市府相關規定辦理。試分就下列情形，進一步說明如下：

一、里長向戶所申請提供里民個人資料：

就此情形民政局則表示，會視區公所審核里長申請民眾個資之事由，但原則上區公所多半不會同意里長僅因舉辦活動便欲申請里民個資之申請，因僅就活動或領取紀念品等事由而欲索取民眾個資，民眾會有疑義，只要向里長說明係可溝通，其問題並不若法務局所稱那麼嚴重。

二、學校、學術研究機構或醫院因學術研究需要申請提供民眾戶籍資料：[83]

關於研究資料之提供，民政局會先視申請人研究計畫之報告，必須是要無從識別當事人爲限且必須有益於公益，但若欲索取如：職業別、職業數等統計數字，則原則上民政局會提供。但實務上經核准者很少，因爲要達到「無從識別」的要求困難度很高。關於資訊提供限縮於「無從識別」之要件，則係出自內政部民國九十四年所作函釋。[84]

三、利害關係人申請他人之戶籍登記資料：

依據內政部所訂定的「申請戶籍謄本及閱覽戶籍登記資料處理原則」第一條之規定，戶籍謄本及閱覽戶籍登記資料之申請人，限於：「當事人」、「利

[83] 參照「臺北市各區戶政事務所受理閱覽抄錄及交付戶籍登記資料作業要點」第十一條規定：「學校、學術研究機構或醫院因學術研究需要申請提供民眾戶籍資料者，須有民政局核准之證明文件，始得提供。」

[84] 94 年 11 月 8 日台內戶字第 0940016658 號函釋：「…其審認事項宜包括例如：蒐集資料者是否簽有保密切結書，保證不洩漏當事人資料？當事人資料有無作匿名化處理，致研究報告公布或揭露時，不會識別特定當事人？」

害關係人」以及「受委託人」。從而在民政局不公開他人戶籍資料予一般人民的原則下，第三人若要取得非本人之戶籍資料，必須合於所謂利害關係人之要件。復，依照上述處理原則第二點，所謂利害關係人，須具備下列各款情形之一：「一、契約未履行或債務未清償。二、同為公司行號之股東或合夥人，且為執行職務所必要。三、訴訟繫屬中之兩造當事人。四、當事人之配偶、直系血親、直系姻親或旁系三親等內之血親。五、戶長與戶內人口。六、其他確有法律上權利義務得喪變更之關係。」[85] 與政府資訊公開法第九條[86] 之規定相較，內政部所頒布的規則可謂嚴格限縮了得請求他人戶籍資料的要件，似乎結果變成，人民若根據政府資訊公開法請求行政機關開示他人戶籍資料，民政局除了依政府資訊公開法審核其要件外，亦須就內政部的規則與函釋判斷其是否具備「利害關係人」之資格，從個人資料保護的角度出發，此等作法為人民的資料安全提供了較周延的防護，從個人隱私保護作為政府資訊公開之界限觀之，[87] 亦屬有據。但研究團隊認為值得進一步思考的事，若申請人僅僅是要求一些與「資料主體之人格權關連程度較低的資料」是否仍應依照如此嚴格的要件來作審核〈例如：僅僅請求公開他人之「姓名」而不涉及其他進一步的個人資訊〉？ 就此內政部的規則是否有不當「增加法所無之限制」之疑義，恐不無疑問。

伍、 其他個資法問題

一、市議會議員向各區公所要求提供個人資料之情形：

[85] 針對祭祀公業管理人，內政部 97 年 4 月 11 日內授中民字第 0970032003 號函釋謂：「有關祭祀公業管理人、派下員或利害關係人申請閱覽抄寫、複印或攝影祭祀公業向民政機關(單位)申請或備查之文件，前經本部 89 年 11 月 20 日台內民字第 8907616 號函及 96 年 7 月 17 日內授中民字第 0960034063 號函釋有案。所謂『利害關係人』係指對其主張之權利有法律上之利害關係人，例如與當事人有契約或債務、債權關係，與當事人為訴訟對造人，或其他確有權利義務關係者等。」

[86] 「具有中華民國國籍並在中華民國設籍之國民及其所設立之本國法人、團體，得依本法規定申請政府機關提供政府資訊。」

[87] 按政府資訊公開法第十八條第六款之規定，一旦資訊之公開或提供有侵害個人隱私、職業上秘密者，得不予公開。可見個人隱私的保護即構成政府資訊公開之界限。

依據民政局所頒布的「臺北市各區戶政事務所受理閱覽抄錄及交付戶籍登記資料作業要點」第十二條規定：「本市議會議員因市政研究或問政需要本市各區戶長名冊資料者，由民政局檢附經市議會大會或委員會決議之文件函轉戶政所提供。」對此，研究團隊的質疑是：個人資料保護法的實施，意味著重視個人資料的自主決定以及重視個人資訊隱私價值的時代來臨，但今日竟然仍有僅憑市議會大會決議，甚或「委員會」的決議即可要求戶政所提供人民戶籍資料之規定，明顯與上述個資法的立法精神背道而馳。

訪談過程中，民政局對研究團隊此點質疑，則是從資訊提供的技術面回應，稱此要點係依早期內政部公文之規定而來，當初其所針對的資訊內容主要係指戶長名冊之類的資訊，況且今日實務上並不會提供議員民眾可識別的個人資料，而僅係提供一般性的統計數據，此應屬個人資料保護法所稱「不可識別」，即無從識別特定當事人者等匿名、去連結化之統計資料。至於所稱「戶長名冊」其內容則爲戶長姓名及地址，亦無其他個人資料。

研究團隊認爲，依照民政局的回應，實務上的實踐確實沒有違反個資法的問題，但從規範的觀點，此一資料提供內容上的限制並未能從上述作業要點中得知，從體系整備與明確的觀點，研究團隊認爲有必要在上述的作業要點中，明確規定議會得要求民政局提供的資料，以「統計數據」等不可識別個人身份的資料爲限，將更爲妥適。

二、 經「公告」的資料＝「已合法公開」的資料？

經民政局公告過的資料，是否當然屬於個人資料保護法中的「已經合法公開的個人資料」？ 而可以令民政局在處理、利用非由當事人提供的資料時，得因之免除個資法第九條第一項所定的告知當事人之義務？ 此處所指民政局「公告過的資料」，係指依法公告以徵詢有無異議的情形，例如祭祀公業的派下成員名單或財產清冊的公告即屬之。實務上常出現祭祀公業或神

明會可能出現兩派在爭管理人，欲爭執的一方爲求勝常請求民政局提供名冊，對此，民政局人員於訪談中表示，以往曾有根據行政程序法第四十六條閱覽卷宗之規定申請公開者，但多被民政局以此一爭執非屬「行政程序」中之爭議，故民政局無法根據此一條文開示資訊而駁回人民申請。但也因爲這樣，若今日申請人正確地以政府資訊公開法第九條之規定申請，雖然資訊公開法看似沒有限定請求公開的主體之身分，但資訊公開法第十八條既然規定涉及當事人隱私者不得公開，從體系解釋的觀點，有無「涉及當事人隱私」即應結合個資法之規定而爲觀察。[88]

民政局此時公開資訊的顧慮，便在於名冊中派下成員的資訊，並非完全都是直接蒐集得來，依照個資法第九條之規定，如果要進一步處理這些資訊（提供與第三人閱覽），則必須要盡第八條第一項的告知義務。但因爲個資法第九條第二項第二款又規定「已合法公開之個人資料」得豁免此告知義務，實務上遂產生「曾公告」是否等同於「已合法公開」的資訊之爭議。

就此，研究團隊初步認爲民政局公開過的資料不該當「已經合法公開的個人資料」。蓋公告的目的是在於「將該資訊在一定期間內公布使民眾週知，亦使得該資訊中之錯誤部分得因他人之異議而改正」，當公告期限屆至後，解釋上該等資訊即非處於公開於眾的狀態。研究團隊認爲個人資料保護法所規定的「已合法公開之個人資料」者，應解爲「穩定持續公開狀態之資料」方屬相當，蓋此等資料既處於各界隨時得以共見共聞的狀態，無造成資訊侵害之虞，因此才有豁免行政機關的告知義務的理由。[89]此與法定異議期間的公告，係爲了「特定目的而暫時公開」迥然有別。

---

[88] 關於個人資料保護法對政府資訊公開制度的衝擊的本土研究，請參閱范姜真媺、郭介恆、王毓正，「政府資訊限制公開或提供事由審查基準及改進救濟程序之研究」（法務部委託研究計畫），頁 86、179（2011）。

[89] *See* P. STEPHEN GIDIERE III, THE FEDERAL INFORMATION MANUAL—HOW THE GOVERNJMENT COLLECTS, MANAGES, AND DISCLOSES INFOLRMATION UNDER FOIA AND OTHER STATUTES 284 (2006).