臺大管理論叢 2017/5
第 27 卷第 2S 期 93-118
DOI:10.6226/NTUMR.2017.JUL.F104-009

巨量資料應用在台灣個資法架構下的法律風險

Personal Information Protection Act and the Legal Risk of Big Data Applications in Taiwan

彭金隆 / 國立政治大學風險管理與保險學系副教授
Jin-Lung Peng / Associate Professor, Department of Risk Management and Insurance, National Chengchi University

陳俞沛 / 國立成功大學醫學系臨床助理教授
Yu-Pei Chen / Assistant Professor, Department of Medicine, National Cheng Kung University

孫群 / 國立政治大學風險管理與保險學系博士生
Aureola Sun / Ph.D. Student, Department of Risk Management and Insurance, National Chengchi University

Received, 2015/6, Final revision received 2016/7

摘 要

巨量資料使用如涉及個人資料的蒐集、處理與利用，將面臨諸多潛在法律風險。本研究以我國 2010 年大幅修正之個人資料保護法出發[1]，研究發現，因為巨量資料的大量性、強調速度與資料多樣性等特質，適用我國個資法架構時可能發生以下問題：(1) 無法完全履行個資法第 8 條與第 9 條對於個人資料於蒐集、處理或利用時之告知義務、(2) 不易符合個資法第 11 條在特定目的消失或契約到期後，不得持有、處理或利用資料的規定、(3) 部分蒐集方可能不符個資法第 19 條須具有特定目的之要求、(4) 無法充分執行個資法第 20 條對特定目的外之利用及停止行銷相關要求、(5) 無法配合個資法第 54 條於首次利用時告知之要求等，顯見我國現行個資法可能對巨量資料應用產生重大法律風險。

【關鍵字】巨量資料、個人資料保護法、隱私權

Abstract

In spite of their underlying values, big data now present enormous challenges as their collection, processing and application are potentially susceptible to the legal risks under Personal Information Protection Act (PIPA 2010) in Taiwan. By putting big data under the analysis framework of PIPA, this paper notes that by taking into consideration the staggering volume, velocity and variety claimed by big data and the enactment of PIPA, problems might arise in a number of ways: (1) In terms of information disclosure, data collection and processing would not meet the requirement of Article 8 and Article 9 of PIPA; (2) Data controllers are very likely to breach the duty stipulated by Article 11 of PIPA, which is, deleting and discontinuing to process or use when the specific purpose no longer exists or contract period expires; (3) Some data collectors might fail to satisfy the specific purpose requirement set by Article 19 of PIPA; (4) Data controllers might violate Article 20 of PIPA at the first marketing action; (5) They also might not meet Article 54 of PIPA that requires a notification may be given at the time where such personal information is first used.

【Keywords】big data, Personal Information Protection Act, the right to privacy

1 我國個人資料保護法於 2010 年間修訂通過後，各界反應部分條文過於嚴格，因此保留第 6 條及第 54 條暫未施行，立法院遲至 2015 年 12 月 15 日三讀通過部分條文修正案，並於 12 月 30 日總統公布修正第 6-8、11、15、16、19、20、41、45、53、54 條條文。

壹、緒論

巨量資料的發展不僅帶來思維上的變革，也昭示新商業模式的開展，同時使巨量資料成為最熱門議題之一[2]。但巨量資料的應用，必然涉及許多個人資料的蒐集、處理與利用，亦可能充滿許多法律上的障礙與陷阱，此為研究巨量資料不可或缺的課題。雖然已有文獻討論巨量資料與隱私權（如 President's Council of Advisors on Science and Technology, 2014），但直接討論巨量資料應用與我國「個人資料保護法」適法性之文獻仍未有所見。

隱私權的觀念形成可追溯至 1361 年英國的 Justices of the Peace Act，至十八世紀英國國會議員 William Pitt 主張「極貧窮者亦有確保陋居不受任何侵擾之權」，開啟了個人領地隱私權 (Territorial Privacy) 的概念。而個人隱私權在美國 Warren and Brandeis (1890) 兩位發表「隱私權」(The Right to Privacy) 這篇極具影響力的文章後開始受到重視 (Langheinrich, 2001)，Brandeis 與 Warren 定義隱私權為「不受干擾的權利」(The Right to be Let Alone)。然隱私權保護觀念的演進，與科技技術的發展有密切相關。1930 年代通訊隱私權 (Communication Privacy) 保護的概念開始興起。到 1960 及 70 年代個人資料隱私 (Information Privacy) 的保護漸漸成為一個重要的趨勢。德國的漢斯邦 (Hesse) 在 1970 年訂定全世界第一部資料保護法，美國則在 1974 年制定美國隱私權法案 (US Privacy Act of 1974)，並提出影響個資保護立法極為深遠的公平資訊實務準則 (Fair Information Practices Principles; FIPPs)，但當時美國隱私權立法並沒有立即落實這些原則 (Langheinrich, 2001)，反而是 1980 年國際經濟暨合作組織 (OECD) 根據 FIPPs 的精神，訂定了 OECD 的個資隱私保護準則。在 1995 年歐盟制訂資訊保護指令 (The European Union's Directive 95/46/EC)，保障個人資料被處理以及自由移動的權利，該指令在 1998 年生效，是個人資料保護劃時代的里程碑。歐盟資訊保護指令主張明示同意 (Explicit Consent)，做為使用與處理個人資料的基本前提。由上述可知，隱私權的定義係隨社會環境改變而演化，由原先「不受干擾的權利」逐步演變為「選擇對何人提供何種個人資訊的權利」(Westin, 1968; Langheinrich, 2001)。上述隱私權的立法，則已普遍存在於世界各國的法律（如我國個資法）甚至是憲法的架構中，用以保護民眾之基本權利。

現今許多國家的隱私權保護法規之基礎，主要根基於 40 餘年前的觀念原則。1990 至 2000 年間，各國逐步將此等個資保護原則轉換成法律與相關規範時，卻逐漸被窄化成狹隘的法規文字，如通知資料當事人原則 (The Notice Principle) 與資料當事

2 透過 google 查詢 Big data 一詞，出現 95,800,000 項結果（查詢日期為 2016 年 6 月 30 日），可見其熱門程度。

人選擇原則 (The Choice Principle) 等，強調程序上的合法性，更重於實質對社會或個人的福利增進 (Cate, 2006)，導致流於形式保護，被批評沒有實質增加社會或個人的福利 (Cate, 2006)。此外，許多法規賦予資料當事人過多的選擇權利，過度擴張資料當事人權利的結果，常常會衍生出更多的問題 (Cate, 2006)，也突顯個人資料保護法規與實務運作扞格之處。台灣個資法立法過程中，經過幾十年的變化，科技與技術的發展早已不可同日而語，顯然我國個資法許多立法基礎是「老觀念」，但巨量資料應用卻是「新技術」，二者間勢必有許多衝突與適用上的障礙值得探討。

我國自「電腦處理個人資料保護法」（以下稱舊法）1995 年完成立法後，在 2010 年大幅修正並更名為「個人資料保護法」（以下稱個資法或新法）後，不論是適用對象廣度與規範強度均有極大改變 （劉佐國，2005），許多規定與現今巨量資料應用趨勢有明顯歧異之處。過去探討我國個資法的文獻雖多（如王志誠、陳春山、李智仁、李金樺與鄭少珏，2005；湯德宗，2008；翁清坤，2010；劉佐國，2005；呂丁旺，2010；林秀蓮，2011；范姜真媺，2012 等），但對於巨量資料之蒐集、處理與利用時，如何適用我國現行個資法相關規定，則仍鮮有討論。因此本文主要目的，即在於分析非公務機關[3] 有關巨量資料之蒐集、處理與利用，在我國現行個資法規範下之適法性問題。

本文結構如下，除第一節緒論外，第二節為外國立法例與比較，第三節討論巨量資料應用與個資保護之相關問題，第四節針對巨量資料蒐集處理、利用與保管等適法性議題逐項討論，第五節為個案分析，第六節為可行策略分析與修法建議，最後為本文結論與建議。

貳、國外隱私權與個資保護立法例

一、國際經濟暨合作組織 OECD

1980 年 OECD 關於「保護隱私和個人資料跨國流通指導原則」將個人資訊保護原則，確定為 1. 開放原則、2. 個人參與原則、3. 責任原則、4. 使用限制原則、5. 資料品質原則、6. 蒐集限制原則、7. 特殊目的與安全原則等 (Organization for Economic Co-operation and Development, 1980)，並為各國個資保護立法確立了最低標準。該指導原則同時以自由流通與合法限制為原則，對個資跨國流通進行規範。1999 年 OECD 發布「電子商務消費者保護指導原則」，要求從事電子商務業者應貫徹 1980「指導原則」與「全球網路隱私保障宣言」有關個資隱私保護之規定 (Organization for Economic Co-operation and Development, 1999)。

3 個資法適用之規範對象包括公務機關與非公務機關，但本文僅以非公務機關之觀點進行分析。

二、歐盟

1995 年歐盟制定「個人資料保護指令」，將資料當事人對其個資之控制視為消費者之基本人權，並為消費者創設「不履行規則」，僅消費者積極主動表示願為個資之揭露，相對方才可使用該個資，藉以平衡雙方權益。即使如此，企業或商家也需取得本人同意，且本人可保留排除之權利 (European Union, 1995)。另外，該指令 Article 25 (4) 授權歐洲委員會可以限制對個資傳送至低於歐盟保護標準之國家。受該條款影響，歐盟之個資保護高標準做法為多國仿行，逐漸取代美國以隱私權保護為基礎之個資保護模式。2012 年初歐盟委員會制定個人資料保護改革方案，以個資控制權為核心，將個資主體權利界定為知情權、更正權、被遺忘權、可攜帶權及資訊蒐集拒絕權等 (European Commission, 2012)。該改革方案一大舉措，是將理論界熱議之「被遺忘權」(Right to be Forgotten) 細化為一項具體個資權利，具體的表現如我國個資法中的「刪除資料權」。依據此項權利，資料當事人對於已無蒐集或處理個資之必要、本人已經聲明或已明確表示不允許其個資被蒐集、所蒐集之個資已過時效限制以及法律上無處理必要性時，除維護本人基本權益或維持公共利益，以及合法許可外，均有權要求有關機構刪除其個資 (European Commission, 2012)。

三、普通法系－美國

美國隱私權研究始於 19 世紀後期，美國立法者將個資視作個人隱私組成部分，對個資之侵犯認為實際等同侵害個人隱私，易言之，個資保護立法係將重心放在個人隱私保護，對個人隱私之保護即對公民尊嚴與自由之保護。美國個資保護制度，以判例與部門單行法為基礎。1977 年 Whalen v. Roe 一案，以最高法院判決之形式，承認隱私權包括個資隱私與自決隱私，其後美國司法界一直致力於個資隱私概念之塑造與發展。

單行法規方面，美國先後頒布「公平信用報告法」(Fair Credit Reporting Act, Federal Government (1970)) 與「聯邦隱私權法」(Privacy Act of 1974)[4]。於 1970 年通過之「公平信用報告法」，為美國首部保護個人信用資訊之法律。該法最初未對個資採集及使用範圍作強制規定，而是留待市場抉擇，即只要市場有需求且使用目的合法，徵信機構均可蒐集並出售，無需取得消費者同意。該法後經 1996 年與 2003 年兩次修訂，依據修訂後規定，消費者對其負面消息之蒐集應有知情權，另對政治立場、宗教信仰、健康狀況、種族等敏感性個資予以排除，禁止徵信機構蒐集此類資訊。我國個資法第 6 條也有類似敏感性資料蒐集之限制[5]。

4　鑒於 1974 年《聯邦隱私權法》主要用以限制聯邦政府部門個人資訊使用，與本文主旨不符，此處不贅述。

5　我國於 2015 年 12 月 30 日公布新修訂個資法第 6 條有關敏感性資料之蒐集、處理與利用限制。

該法對消費者隱私保護主要集中於個資使用端，若需納入其他資訊，則需由消費者自行要求或經消費者同意。更為重要者，信用報告之使用需遵循其法定用途，不能逾越法定用途而用作他途。除公平信用報告法外，美國立法者著力對特定領域及特殊人群之個資保護加以規範。典型代表「1986 電子通信隱私法」(Electronic Communications Privacy Act; ECPA) 與 1996 年「健康保險攜帶與責任法案」(Health Insurance Portability and Accountability Act; HIPAA)。1999 年「金融服務現代化法案」(Gramm Leach-Bliley Act; GLBA)，要求金融機構就其隱私權政策明確告知金融消費者，由消費者自由選擇是否同意個資之傳遞。

政府政策方面，1970 年代的 FIPPs 為美國個資保護制度之基石。美國商務部於 1997 發布「資訊時代隱私與自治報告」，為美國以行業自律為主導之個資保護機制奠定基礎。2012 年白宮發布消費者資料隱私權報告，希望於巨量資料時代構建個資隱私保護新架構。該法案對消費者個資控制權、隱私權與資訊透明度、個資蒐集、使用與披露之環境、個資可修改性與準確性、與企業責任等予以規範。該法要求保有個資之企業，應尊重蒐集與使用消費者個資之背景環境，在合理限度內蒐集與保存，以此取代目的說明。該法並未創設嚴格細則，僅樹立一般原則，充分尊重各企業消費者個資保護之自主權。縱觀美國個資保護制度之歷史沿革，可發現美國並無針對非公務機關個資保護之聯邦統一立法，僅對特定行業、特定群體予以特殊保護 。早期以事後救濟為主，對個資隱私因被侵入之侵權損害予以填補 。

面對巨量資料的趨勢，美國總統科學和技術顧問委員會 (PCAST)，於 2014 年提出「巨量資料與隱私權報告」中指出，以「事前知情並同意」的基本架構，於巨量資料時代保護個資已不合時宜，因此建議政策重心應著重巨量資料之實際運用結果，防範運用過程中之個資濫用，而非過度集中於其蒐集與分析等 (PCAST, 2014)。2014 年美國白宮發布巨量資料白皮書，就個資保護提出通過市場機制保護個人隱私價值、持續穩定之巨量資料與個資使用教育等建議 (Executive Office of the President, 2014)。

四、大陸法系－德國與日本

（一）德國

德國作為個資保護立法先驅，主要採統一立法模式， 1970 年德國聯邦之一的漢斯邦 (Hesse) 制定了世界第一部個資保護成文法，1977 年「德國聯邦個人資料保護法」則集其大成[6]，其立法目的在於兼顧個人資料處理過程中之個資隱私保護，與通過立法規範個資處理行為（許文義，2001）。1983 年德國憲法法院判決聯邦政府頒布之「人

6 參見 German Government (1977)。

口普查法案」違憲，聯邦憲法法院認為該法案未能區別個資蒐集與使用目的，違反憲法規定，該判例引入資訊自決權，正式賦予個資權利憲法地位。

所謂資訊自決權，即視個資權為人格權之一種，僅法律有權對個資權利作出限制，個資蒐集應受嚴格目的限制，資訊自決權強調個人自治與自決，符合德國立法對個人尊嚴之追求（彭禮堂與饒傳平，2006），對後續個資保護法規影響深遠。德國法中「一般人格權」之內涵與美國隱私權頗為類似，遂逐漸從隱私權理論向人格權理論傾斜，逐步將個資與隱私分離開來，視個資為人格尊嚴之組成部分，是獨立於隱私權之人格權，應採人格權保護模式保障個資（祝蓓蓓，2007），因此德國走向個資之積極控制狀態。1990 年「個人資料保護法」因而誕生，該法經數次修訂，為個資保護確立許多原則，包括直接原則、更正原則、目的明確原則、安全保護原則、公開原則與限制利用原則等。

（二）日本

日本個人資料保護法令，始於 1973 年德島市「關於保護電子電腦處理之個人資訊條例」，日本中央政府之個資保護制度則與該國電子化政府之發展息息相關，因電子化操作必然涉及個資之蒐集與利用，政府與民間對個資保護之關注日益增多。此背景下，「有關行政機關電子電腦自動化處理個人資訊保護法」、「個人資訊條例」等規範相繼頒布。基於前述經驗，日本政府著力於完整個資保護制度構建，「個人資訊保護法」、「行政機關個人資訊保護法」以及「行政機關個人資訊保護法等施行準備法」等於 2003 年 5 月相繼由日本國會通過，宣告日本以個人資訊保護法為基礎，並以部門單行法為補充之個資保護法律架構正式形成。2014 年，日本政府開始針對巨量資料對個資之挑戰，擬對相關個人資料保護法案進行改革，對特定情形下之個資當事人同意權予以限制，並進一步界定敏感個資之範疇。

日本個資保護制度汲取美國（隱私權理念）與歐盟（個資保護立法模式）等經驗，但同時保留了自身特色，其不分公私機構之綜合立法係以歐盟為借鏡，同時仿行美國對傳統隱私權理論進行擴張，融入主體個資控制權理念。在個資概念界定上，與其他大陸法系國家相仿，同採「識別說」。另外，日本針對非公務機構之個資蒐集、持有與利用，依目的明確化原則、利用限制原則、蒐集限制原則、資料內容完整正確原則、安全保護原則、公開原則、責任原則及個人參加原則等加以規範，給予醫療、金融等特殊領域個資蒐集與利用特別保護；至於其他民間應採標準，則由各行業從行業實務需要出發自行訂立個資保護標準，試圖於個資保護與個資自由流動之間尋求平衡。在爭議處理方面，設兼具資訊蒐集與個資保護職能之審查會制度，建立民間認證制度（謝青，2006），同時允許設立民間團體參與個資糾紛之處理，以突出個資保護之靈活性（姚嶽絨，2012）。較之歐美國家，亞洲個資保護相對薄弱，但日本之個資保護頗具特色，可視為美國與德國模式之折衷。

五、普通法系與大陸法系個資保護比較

縱觀各國個資保護制度可發現，普通法系國家立法之目的，是以保護個人不欲為他人所知之資訊內容為主，因此對個資保護常以隱私權保護法方式呈現，如加拿大「聯邦隱私法」與澳洲「隱私法」等。大陸法系國家則將姓名、性別、身高、血型、住所、職業、財產及婚姻狀況等，凡所有足以構成對個人「識別」之資訊內容，均視同立法保護所涵蓋之個人資訊，因此多以個人資料保護法概念為主，如日本「個人資訊保護法」與韓國「公共機構之個人資料保護法」（梅紹祖，2005），我國也採相同之立法例。普通法系主要秉持「自由流通」觀點，給予資訊自由流通與充分尊重，僅於特定行業有濫用個資、侵犯隱私之虞時方訴諸立法手段，且立法重點主要在於限制政府對公民隱私之侵犯（洪海林，2007）。大陸法系國家試圖通過個資蒐集目的、使用及轉移之知情權、參與權、決定權（進入權與退出權）、修改權、刪除權等多重限制全方位捍衛個人人格尊嚴（孔令傑，2009）。

普通法系國家採隱私說，以隱私權理論為基礎（張軍，2007）。大陸法系則採識別說（陳紅，2008），以人格權理論為基礎，以人格尊嚴為根本價值追求。以美國為代表之普通法系國家秉持分配正義，更多是以社會利益為出發點，將個資視為具經濟價值之商品，縱使個資隱私會受到限制，若對於促進交易繁榮市場有利，仍有許多開放空間，故美國個資隱私保護體系主要由特定部門法律法規與市場自律機制構成（陳起行，2000）。以德國為代表之大陸法系國家，大都通過國家立法，將個資視作具崇高地位之基本人權予以全面保障，保護標準嚴格（洪海林，2007）。以「被遺忘權」為例，大陸法系國家會傾向保護「被遺忘權」，普通法系國家則相反，常將言論自由置於「被遺忘權」之上（邵國松，2013）。面臨巨量資料之挑戰，大陸法系立法明顯較不利於個資自由流通，我國採取較偏向大陸法系立法例，因此在巨量資料應用與個人資料保護之衝突相對也會較為明顯。

參、巨量資料對個資保護之影響

巨量資料應用價值不言自明，但巨量資料與小量資料有明顯不同，可能衍生諸多特有的問題，包括對傳統個資保護架構構成威脅，以及以小量資料為背景制定的個資法，將產生適用上的困難，茲討論問題如下：

一、巨量資料對個資保護之衝擊

（一）反匿名與重新識別威脅

我國與其他大陸法系國家同採所謂「識別說」，即個資概念以「可識別性」作為核心特徵，已經去識別化後之資料，即不在個資法規範之列，但這可能只在小量資料假設下才能成立。在小量資料時代，通過有效匿名以及去識別化後，自然對於資料當

事人之危害已不存在。但巨量資料時代下，經由大規模資料與複雜運算技術，大大加強資料間聚合能力與關聯性分析，原本在小量資料認為已經屬去識別化之資料，大都可透過彼此聯繫與印證，藉由多方面資訊追溯至特定個人，並進行反匿名與重新識別身分，這會給傳統個資保護架構，帶來很大的挑戰與威脅 (Mayer-Schönberger and Cukier, 2013)。

（二）不當蒐集與資料濫用

巨量資料時代個資濫用可能性大增，甚至有衝擊個人基本權利之隱憂，例如網路技術改變個資蒐集方式與內容，許多企業或機構對個資之蒐集幾乎時刻進行，且該蒐集行為常常以隱性方式為之，令資料當事人難以察覺，對個資之侵害威脅也隨之加大。再者，日後用於各種延伸用途已遠超過原始的蒐集目的等，對資料當事人而言，不論個資之存儲位置與延伸用途等均甚難知悉，當然資料當事人的個資權利，則可能得不到應有的保障。

二、巨量資料與個資法之衝突

美國 PCAST 二位共同主席 John Holdren 與 Eric Lander，於 2014 年 5 月聯合致函其總統指出，「巨量資料時代對於個人隱私權保護最大的挑戰，源自於遠超過資料當事人所想像的多量資料與高效率分析技術發展」(PCAST, 2014) ，清楚點出巨量資料與小量資料時代資料保護觀念的不同，也是為何美國 PCAST 報告指出，若個資仍須使用傳統以「知情並同意」的基本管理架構，是導致不符巨量資料時代所需的主因。

經由前述對個資保護立法與沿革分析可知，各國個資法立法當時，有關個資法內容，可合理推知均係以當時小量資料環境為其基本假設，因為立法者並無法事前預知後續有所謂巨量資料時代的來臨。我國個資法目前雖已公布施行，但適用在屬於小量資料的個人資料蒐集，在施行初期即已經遭遇許多困難[7]，更遑論巨量資料時代下的蒐集處理與利用。

反觀在巨量資料時代，資料的蒐集早已不限於傳統「面對面」為主的蒐集方式，誠如 PCAST (2014) 所稱巨量資料的蒐集，已經 “from sensors in everything from phones to parking lots”，巨量資料時代的資料蒐集早已無所不在。面對這些蒐集與利用個資的全新方式，現有許多個資法的規定就可能產生窒礙難行之處。例如我國個資法第 8 條有關知情權的規定，因為巨量資料的蒐集經常是不可察覺，而且是在個人不知情情況下進行 （如前述 from sensors in everything），事實上根本無法逐一事前取得個人同意後再進行蒐集，如要完全適用，就會面臨到執行時效與成本上的問題。

7 個資法雖於 2010 年通過，但各界反應衝擊過大，延遲至 2012 年 10 月 1 日才正式施行，但對於其中爭議性較高的第 6 條以及第 54 條條文，則一度被凍結並未同時施行。

以上各點都突顯了個資保護在小量資料時代下，也許不是難解的問題，但在巨量資料應用上就會有其衝突性。這也是為何美國 PCAST 面對這些難解問題，會具體建議政府應該把監理重點放在個資使用的結果 (Outcomes)，而不是一味關注如何使用 (How) 個資的程序末節 (PCAST, 2014)[8]。Mayer-Schönberger and Cukier (2013) 也提出相同的看法，否則只要涉及個人巨量資料應用，都會受到法規極大的限制。

肆、巨量資料應用於我國個資法下適法性分析

一、巨量資料有關蒐集處理之適法性分析

我國個資法參照 APEC 隱私權保護架構 (APEC Privacy Framework) 的通知原則 (The Notice Principle) 要求[9]，於個資法第 8 條第 1 項規定資料蒐集者，直接向當事人蒐集個人資料時，必須向資料當事人明確告知相關重要事項，包括機關名稱、蒐集目的、個人資料類別、個人資料利用之期間、地區、對象及方式、當事人依第三條規定[10]得行使之權利及方式及當事人得自由選擇提供個人資料時對其權益之影響等，以保護資料當事人「知」的權利（彭金隆，2012）。若屬間接蒐集者，仍須依第 9 條第 1 項之規定，應於處理或利用前，補行告知第 8 條第 1 項所列各款事項，但可以在日後首次對當事人為利用（如首次進行銷售）時，併同為告知即可（個資法第 9 條）。但在個資法修正施行前已蒐集完成之個人資料，個資法第 54 條乃明定，非由當事人提供之個人資料，必須自該條文公布施行之日起，於處理或利用前必須完成告知，或於首次利用時併同告知[11]。

我國個資法雖未於法條中明列，但以個資法第 8 條或第 19 條等條文觀之，是以「事先同意」為核心之個資事前保護機制設計，故可以推知其立法假設，係建立小量資料環境概念下，以對個別或少數當事人逐一蒐集為主的思考，在小量資料時代適用此一規範，過程雖然繁複但執行窒礙之處尚屬可以克服。然巨量資料具有資料規模龐大，強調速度性且資料來源多元等特性，面對以「事先同意」為前提的機制下，對於大量仰賴自動化方式蒐集個人資料的巨量資料蒐集方而言，要事前逐一告知資料當事人，顯然有其適用上的困難。

---

8 PCAST recommends that policy focus primarily on whether specific uses of information about people affect privacy adversely. It also recommends that policy focus on outcomes, on the "what" rather than the "how."

9 參見 APEC Privacy Framework, para. 15. Available at http://publications.apec.org/publication-detail.php?pub_id=390。

10 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。

11 本條於個資法修正通過後，行政院考量衝擊過大，本條條文暫時凍結並未公布施行，法務部另送修正條文至立法院審議，並經立法院修正通過 2015 年 12 月 30 日總統公布之條文。

此外，在資料蒐集時，根據個資法第 19 條即應基於「特定目的」而為蒐集，然而，不論依第 8 條向當事人直接蒐集個人資料，或依第 9 條間接蒐集非由當事人提供之個人資料，由於巨量資料的蒐集範圍極廣，可能包含個人刷卡資料、通訊、社交資料、言論意見、行動資訊、上網紀錄以及各種媒體資料等，在該資料蒐集當下，蒐集方是否皆有所謂特定之目的存在？或是否於合理範圍內蒐集，其實都無法完全排除有上述適法疑義的可能。

在蒐集資料時，依個資法規定，即須立即告知資料當事人個人資料利用之對象及方式等資訊，除非巨量資料蒐集方，在第一次蒐集前有一定時間通知當事人，並等待資料當事人確認已經收悉告知事項，否則不可蒐集取得該資料。但以巨量資料的數量、規模與速度性等特質，要達成上述規定有極大困難。即便假設巨量資料蒐集方，當下得以清楚確定並說明並取得當事人確認，但也無法預知未來可能延伸之使用用途而予以事先告知。一旦日後隨環境變更，當有新的使用目的、適用對象及使用方式出現時，則依個資法之規定，勢必應重新取得資料當事人之同意，否則將會有違反個資法規定的疑慮。

本文以為，巨量資料之蒐集，於直接蒐集之新個人資料，要符合第 8 條第 2 項免為告知之情況機會極低，一般而言，須向當事人明確告知第 8 條第 1 項各款事項，然其形式或可不拘，以第 19 條第 1 項各款之理由為蒐集者，可以定型化契約之概括同意條款為之。因此，若網路平台提供者與其他使用者間，當使用者於網路平台使用之時，依第 19 條第 1 項第 5 款，事先以定型化契約條款告知第 8 條第 1 項各款事項，讓使用者知悉其使用網路平台時，部分使用資訊將被提供平台之業者蒐集，並為特定目的之使用，似無不可，否則若直接要求蒐集者依第 19 條第 1 項第 5 款，當事人須個別單獨之同意，以「巨量」資料大量蒐集情況而言，幾乎難以做到。蒐集者另一可能大量蒐集個人資料之方法，則是依第 9 條為間接蒐集，除非有符合第 9 條第 2 項免為告知或第 51 條不適用個資法之情形，否則也是必須要履行相同之告知義務。

綜上，若巨量資料之蒐集者所蒐集的資料，屬於個資法所保護之個人資料，則於資料蒐集時，須要先有一「特定目的」，且應具第 19 條第 1 項各款情形之一，若向當事人直接蒐集，則應為第 8 條第 1 項各款事項之告知，並確認資料當事人已經收悉該等告知事項後始得為之；若間接蒐集非由當事人提供之個人資料，除有第 9 條第 2 項各款之情形外，亦須於處理或首次利用時，向當事人告知個人資料來源及第 8 條第 1 項第 1 至 5 款之事項。顯然要完全執行上述規定，對於巨量資料蒐集方有很大的困難。

二、巨量資料應用有關利用之適法性分析

個人資料之利用最常見者為行銷活動，對於巨量資料蒐集方來說，若利用資料分析後欲對資料當事人進行行銷活動，個資法第 20 條第 2 項規定當事人表示拒絕行銷

時，應立即停止再利用其個人資料，同條第 3 項規定，非公務機關對當事人進行首次行銷時，應同時告知資料當事人未來拒絕被行銷之方式。

上述規定在實務適用會遭遇許多困難，若以電話行銷方式，因為行銷意圖明確且可以透過錄音加以證明，可能較無問題。但若是透過網路、郵件、簡訊、通訊軟體或是其他方式，則對於是否屬於行銷用途將不易認定，而且資料當事人也很難對行銷方進行拒絕之相對意思表示。至於第 3 項課行銷方於首次行銷時，應同時告知資料當事人未來拒絕被行銷方式之責任，也同樣會有上述認定問題外，事實上更有窒礙難行之處。上述法條規定，適用少量資料時即已經有許多困難，在巨量資料應用上，其難度更是可以想見。

如前節所述，依我國個資法對於巨量資料的利用，原則上均應於蒐集之「特定目的」必要範圍內為之，除非有第 20 條第 1 項但書各款之情形，始得為特定目的外之使用。在巨量資料時代，強調的是各資料庫間的結合利用，如果蒐集巨量資料之機構，欲將資料移轉至第三人進行整合分析與利用時，就有可能屬於非特定目的內的利用，要符合個資法之規定條件之一（如學術利用、為增進公共利益、為免除當事人之生命身體自由或財產上危險、以及防止他人權益之重大危害等）的可能性極低。若選擇以第 6 款「經當事人同意」後，做特定目的外之使用，則此同意，必須與一般同意區隔，而須以單獨所為之意思表示，又不得以定型化契約為之，以巨量資料之規模，若要符合個資法逐一取得同意，其難度也極高。

三、巨量資料應用有關資料保管之適法性分析

巨量資料之來源若是因雙方進行交易所蒐集而來之個資，就會面臨到雙方契約已經終止後無法保有該資料的問題。根據個資法第 11 條第 3 項之規定，除非有法定原因或因執行職務或業務所必須事項，或是經當事人書面同意者外。當對個人資料蒐集之特定目的消失或期限屆滿時，資料持有者即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。顯然根據前述法規文意，若巨量資料中含有「過去舊客戶」之個人資料，且無前述適法性原因的存在而繼續加以使用時，則會違反個資法之規定。

本條內容係於 1995 年初訂時，已於立法說明中敘明係參考日本與德國法立法例，主張個人資訊之特定目的已消失或保有期限已屆滿，應將資訊刪除或停止處理及利用。以巨量資料之蒐集而言，資料大都是因為交易後所蒐集而來，因此除長期契約（如壽險契約）外，屬一次性交易性質者，於交易完成之後，如無法律規範必須保存一定期限、資料當事人書面同意或法定事項[12]之一時，就符合了前述資料蒐集之特定目的

12 參見個資法施行細則第 21 條，有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由。

消失或持有期限已屆滿之情況，資料持有人應予以刪除或停止處理或利用該資料。

個資法施行細則第 20 條規定，特定目的消失指下列情形之一：1. 公務機關經裁撤或改組而無承受業務機關。2. 非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。3. 特定目的已達成而無繼續處理或利用之必要。4. 其他事由足認該特定目的已無法達成或不存在。根據前述規定，所謂特定目的消失原因，如果持有巨量資料之一方，已經不具有執行某項業務之法定條件，或原本可從事該業務者，被撤銷營業許可或喪失法定資格要件；或雖非因喪失前項法定條件，但資料持有人已經不再從事該項業務（如自行結束營業），自然就不具保有資料之必要與正當性，因此必須主動刪除或停止處理與利用。

即使特定目的雖仍存在，當雙方契約有效期間已經結束後，資料持有方即失去繼續保有對方資料之正當性與必要性，因此就應刪除或停止處理利用該客戶之資料。有時雖契約已經屆滿，但相關法令規定應持續保存一定期間者，則可以繼續保有該資料，但在該保管期間內應不得進行利用。但保存期間不得繼續利用該個人資料進行任何利用之行為。若繼續對於該等資料進行分析整理甚至行銷，則有踰越法令之問題。依據上述法規之規定，資料持有人必須嚴格檢視所持有之資料，並審查是否已符合前述應與刪除與停止處理利用之條件，否則就有違法之風險。

因為新法規定較舊法嚴格，對於新法施行日（2012 年 10 月 1 日）前已經蒐集之資料該如何調和新舊制度適用？根據個資法施行細則第 32 條規定[13]，修正施行日前透過直接蒐集之個人資料，於修正施行後，如果是屬於特定目的內之利用，則可以不必受到新法之拘束，繼續進行特定目的內的合理利用，但若是想要進行特定目的外的利用時，則應適用新法的規定辦理。以巨量資料持有人來說，過去若未適用舊法之行業，可以自由使用個人資料，並不受到舊法的約束，但新法施行後，因為適用對象擴及所有行業與個人，因此對於特定目的外之利用，就必須受到新法的約束，最具體的規範在新法第 20 條，除非符合特定法定要件[14]者，不可以做特定目的外之利用。

其次就已經間接蒐集而來之資料該如何處理部分，規定於個資法第 54 條，規定若非由當事人提供之個人資料，應於處理或利用前向當事人為告知，或得於首次對當

13 個資法施行細則 32 條規定，本法修正施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得繼續為處理及特定目的內之利用；其為特定目的外之利用者，應依本法修正施行後之規定為之。

14 個資法第 20 條規定：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為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。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、經當事人同意。七、有利於當事人權益。

事人為利用時併同為之。雖然免除了原條文一年內完成告知之時限問題，或許對於紓解小量資料之利用困境有其作用，但通常巨量資料利用之資料均十分龐大，依規定仍必須於首次利用之瞬間，即須一次履行告知義務，還是有實質上的困難未解。

伍、實務分析

為探討巨量資料的應用適法性狀況，本研究蒐集國外巨量資料應用實務個案，並假設在我國個資法規範下之進行適法性分析。其次，以國內某金融機構之實際資料分析個案探討其適法性。在次級資料巨量資料應用個案上，由於國內並無足夠且公開之巨量資料運用案例，因此本文以已出版巨量資料專書所舉例討論之案例共擷取 59 個個案[15]，加上於網路上搜集個案 43 個，共取得分析個案 102 個加以分析。國內個案部分，則為國內某金融機構實際應用之個案。其分析內容如下：

一、國外案例適法性分析

國外案例以美國的案例最多（占 74.56%），資料顯示美國為現今巨量資料應用最發達與成熟之國家，可能與美國個資保護規範相對較為寬鬆有關（見前述美國立法例之分析）。應用巨量資料行業以資料公司比率最高，金融保險業次之，分佈如表 1 及表 2。

表 1 個案國籍與行業分布

國家別	美國	日本	英國	歐盟	加拿大	中國	其他	合計
案件數	76	9	5	4	3	3	2	102
百分比	74.5%	8.8%	4.9%	3.9%	2.9%	2.9%	1.9%	100%

行業別	搜尋引擎	社群網站	金融保險	政府	資料公司	電力電信	網路業者	學術機構	醫療機構	其他
案件數	7	4	15	8	17	6	9	2	6	28
百分比	6.8%	3.9%	14.7%	7.8%	16.6%	5.8%	8.8%	1.9%	5.8%	27.4%

全部案例中有 57 個（約占 56%）使用到個人資料，其餘非屬於個人資料（使用交通流量、氣象資料或商品購買數量等）。若這些個案發生在我國，有一半以上個案必須適用個資法。根據前述有關我國個資法適法性分析可知，個人資料之蒐集與處理

15 選擇 Mayer-Schönberger and Cukier (2013) 合著 Big Data: A Revolution that will Transform How We Live, Work, and Think 一書，Mayer-Schönberger 為牛津大學網路研究所教授，並曾擔任微軟、世界經濟論壇等大公司和組織的顧問，是大數據領域公認的專家，其書中所舉之案例亦具有一定之代表性，本研究擷取此書 49 個可分析之個案。另本研究另外選取日本 Nomura Research Institute 的 Shirota (2012) 所著 “Big Data No Shougeki” 一書所舉出 10 個個案。

要合法，必須符合特定目的、具有法定要件與履行告知義務三項前提。案例中資料使用者所蒐集之個人資料，如屬以往來客戶或是業務範圍內（例如 Google 在線上蒐集客戶的活動資料），符合特定目的範圍內較無問題，且可視為雙方具有契約或類似契約之關係，應該可滿足第二個要件，最後一個要件為蒐集前必須履行告知義務。若依據我國個資法第 8 條規定，資料蒐集時就必須向資料當事人說明至少七項重要事項，但由統計發現，蒐集之方式雖以直接向資料當事人蒐集者居多（約 73%）（見表 2），但大部分都是在資料當事人不知情或是沒有事先同意情況下所為之蒐集，雖符合我國個資蒐集前兩項要件，但可能無法滿足個資法第 8 條與第 9 條所要求之告知義務。

我國個資法第 11 條第 3 項，規定當特定目的消失或期限屆滿時，應刪除、停止處理或利用該個人資料。約六成的案例在契約有效期間內，但其餘 40% 可能涉及過去客戶的資料。依據規定，除非證明有上述例外之情形（如客戶已事前同意），否則就不能再繼續保有或是處理利用這些「過去客戶」的資料。顯現這些巨量資料應用案例中，有不小的比率與我國個資法第 11 條適用有牴觸之疑慮。此外，在這些使用到個資案例中，大部分被利用來從事商業行銷用途（約 63%），依據我國個資法第 41 條罰則規定，意圖為自己或第三人不法之利益或損害他人之利益者罰則將加重。

表 2 屬個人資料個案性質分析表

個資使用狀況	案例數	比率
屬匿名資料	3	5.26%
取得事先同意	7	12.28%
屬行銷個案	36	63.16%
直接蒐集	42	73.68%
屬公開資料	4	7.02%
當事人事先知情	7	12.28%
在契約期間內	34	59.65%
合計	57	100%

二、國內個案適法性分析

本研究另以國內某中大型金融機構[16]對其存款客戶資料進行實際分析個案為例。本個案資料類別超過 100 項以上，包括 1. 個人基本資料（如 ID、性別、地址等）。2. 與本機構之交易資料：包括各項交易之次數、交易時間、交易金額等。3. 非本機構交易資料：如薪轉公司、保險交易（產險、壽險）、共同基金交易等。該金融機構整理

16 該金融機構為國內中大型銀行，全國分行數超過 80 個以上，信用發行量為前十名以內之金融機構。

資料主要目的為進行本業商品及跨售商品（主要是保險商品）。依據前述有關個資法討論之架構，逐一分析本實務個案之適法性問題。

1. 本案使用資料均為客戶之交易資料，具有可與資料當事人連結之基本資料等，符合我國個資法第 2 條之規範，屬個資法規範之範疇。
2. 個案中第一類資料直接向資料當事人（客戶）蒐集而來，並非經由第三人取得個人資料，既屬客戶資料，應符合個資法第 19 條特定目的，以及該條第 2 款因契約關係所為之蒐集與處理。
3. 本案有整合該金融機構內部其他眾多資料庫資料，並累積涵蓋多年交易資料，其中因時間不同有新舊法不同適用的問題。新法施行後的新交易客戶，雖已依照銀行公會所定「會員履行個人資料保護法第 8 條第 1 項告知義務注意事項暨告知義務內容參考範本」（下稱參考範本），告知資料當事人相關事項，但該文字文意含混不明，且以本案狀況，該金融機構事後對客戶資料進行大數據分析，用以提高金融商品的銷售之利用方式，似乎無法被涵蓋在前述規範之使用範圍內，且又未於資料蒐集時事先告知客戶，故可能有不符個資法第 8 條規定之問題。
4. 本個案所使用之定存客戶個人資料中，有包括部分已經終止存款關係之舊客戶資料，其中部分資料當事人雖仍保有定存以外其他交易關係（如貸款），但就與定存相關資料而言，其資料分析之範圍已經包含部分或全部終止契約客戶資料，且事前可能並未全部取得客戶書面同意，故可能有不符個資法第 11 條第 3 項規定之問題。
5. 本案數據分析結果，會提供理財人員選擇銷售對象以及推銷可能購買產品之資訊、由電話行銷單位直接針對特定資料當事人推銷、或對特定群體客戶進行網絡與實體郵寄產品行銷方案訊息給特定客戶等，前二項用途因為有銷售人員涉入其中，執行上尚無問題，但透過網路、郵件、簡訊、通訊軟體或是其他方式遞送產品資訊，是否屬法條規定之「首次行銷」並不明確，且本案並無於產品訊息傳遞時同時提供當事人表示拒絕接受行銷之方式，如未來此行為被認定不僅屬廣告行為而為行銷行為時，則可能會有不符法律規定之問題。

經由上述兩類型個案討論可知，雖受限於資料量雖然無法代表業界全貌，但可梗概瞭解即使在國外成功案例，如果套用在我國個資法架構下，仍有違反個資法的可能，另由國內金融機構案例比對可知，實務上確有法律風險存在，即使屬高度監理之金融機構，於巨量個資資料分析應用上仍有許多適法性疑義，更遑論其他未受監理的產業。

陸、因應策略

一、不修改法令下之因應做法

面對前述各項適法性問題，巨量資料之應用應該有妥善對策，若在不修法的前提下，本文提出三項因應做法。首先，若巨量資料分析之對象，不涉及自然人身分人格相

關資料，則自然毋需受到個資法之限制與約束，為降低適用個資法之法律風險，可優先應用不涉及個資之資料。其次，可將個人資料去識別化後利用。面對嚴峻的個資法規定，若不理會上述個資法規範，勢必冒極大之法律風險，但若要等待法令放寬規範，終究緩不濟急。因此對於已具有眾多個人資料者，若能去識別化將其與自然人之連結去除，則自然可以降低個資法之約束。再者，應重新規劃個人資料蒐集程序使其合法化，對於未來新蒐集之資料，在個資法規定已經非常明確的狀況下，應可以從新規劃個人資料蒐集的流程，讓未來個資取得符合法令規範，以解決後續可能的法律風險。

二、修法建議

如採以修改法令方式因應，本文認為思考方向有二。首先，為解決上述巨量個人資料使用問題方式之一，可回歸至各特別法規範，由各目的事業主管機關，依據行業別特性透過特別法之修訂，以排除個資法部分適用障礙應屬可行（例如現有金融控股公司法第 43 條共同行銷之規定）。本法優點在於可考量不同行業之特性給予適性的規範，且因為影響層面有限修法技術也較為簡單；但缺點在於未來個資保護可能因產業不同而標準不一，且須逐一單獨立法，成本浩大且時效可能延宕等。

其次，則可採直接修改個資法解決之。國際上對於巨量資料應用與個人隱私權衝突的解決，有建議以「使用監理導向」取代舊有「資料蒐集監理導向」，包括美國總統科學和技術顧問委員會及 Mayer-Schönberger and Cukier (2013) 都持這樣主張。他們主張對於巨量資料的應用，應該採用事後管理而非事前管理，資料使用者如事先能負起確認巨量個資之利用不會傷害到資料當事人權益之責任，便可以直接蒐集處理與利用，就是將使用責任加諸於資料使用者身上，若事後發現仍有損於資料當事人權益時，自應負相關賠償與法律責任 (Mayer-Schönberger and Cukier, 2013)。同時也可以在企業內部設立「資料保護人」或是「個資保護長」(Chief Privacy Officers) 等類似功能的個資保護專業專職人員，在外部則可設置類似獨立稽核或會計師角色的獨立隱私權專家 (Privacy Expertise) 或稱為「外部演算學家」(Algorithmist) (Mayer-Schönberger and Cukier, 2013)，協助企業或個資使用者判斷或稽核是否違反客戶隱私權。

但以我國個資法架構下，若欲將此一理念入法，因與現行個資法基本架構不甚相符，如直接針對巨量資料應用之特性，修正前述適用有疑慮之各條文（如個資法第 8 條、第 9 條、第 11 條、第 19 條、第 20 條與第 54 條等），因條文牽涉過多並非易事。本文淺見認為若考量時效性以及修訂個資法最小範圍為考量，並參酌前述「事後管理」而非「事前管理」的理念，本文建議或許可於個資法第 51 條增列第二項規定，在符合個資保護的一定規範下，對已提出具體防止損害資料當事人權益之計畫，並向主管機關申請核准所進行之巨量資料蒐集、處理或利用，得排除部分對於巨量資料應用產生窒礙個資法條文的適用（如個資法第 8 條、第 9 條、第 11 條、第 20 條與第 54 條等），

並明確授權由主管機關另訂巨量資料管理辦法，以結構上解決巨量資料適用的問題。

但為考量個資法有關資料當事人的各項權利，係屬我國憲法層次對個人資訊自主權所衍生之各種請求權，此權利即使主管機關採行前述事前審核機制，亦不可限縮資料當事人受保護之範圍，亦即對資料當事人權益之保障，並不得因為配合巨量資料使用而有所減損。因此亦可參酌 Mayer-Schönberger and Cukier (2013) 之見解，資料使用之責任必須加諸於資料使用者身上，即使通過上述主管機關審核程序，若事後發現仍有損於資料當事人權益時，仍應負相關賠償與法律責任方向處理，故建議於個資法第 48 條增訂相關連結之罰則。上述建議僅規定不適用部分現行個資法分條文，但並不意指巨量資料應用均毋須符合該等條文保護個資之本意，因此建議於第 51 條中增列第三項，授權主管機關統一針對巨量資料分析之定義、範圍、資料使用人申請條件等，以及參酌巨量資料特性以及個資保護精神，訂定資料使用人對個人資料當事人權益維護應遵循事項管理辦法（亦可包括前述內部與外部個資專家的設置與查核等亦可納入規範）等，另外訂定授權命令以為遵循。

本文嘗試整合前述文獻與建議，試擬我國個資法修訂條條文內容如下：

1. 於個資法第 51 條增訂第二項及第三項文字如下：

   非公務機關已提出具體防止損害資料當事人權益計畫並經主管機關核准進行之巨量資料蒐集、處理或利用，得不適用本法第 8 條、第 9 條、第 11 條、第 20 條與第 54 條。（第二項）

   前項有關巨量資料之定義、範圍、申請條件及對個人資料當事人權益維護事項之管理辦法，由主管機關定之。（第三項）

2. 個資法第 48 條第一項（罰則）增訂第五款文字如下：

   五、未依第五十一條第三項訂定個人資料當事人權益維護計畫事項之管理辦法。

柒、結論與建議

巨量資料的應用若涉及個人資料的蒐集處理與利用，基於法律對隱私權與人格權的保護，將面臨諸多法律上的障礙，若使用稍有不慎，很有可能陷入嚴重法律風險威脅中。國際上對個人資料保護訂有各項原則，包括個人資料及隱私保護政策的開放性原則、強調個人有權獲知資訊使用的個人參與原則、明定管理者對個人資訊之保管承擔相應責任的責任原則、不得超出蒐集目的使用與任意提供給第三者的使用限制原則、以及目的須明確且不可超範圍利用的蒐集限制原則等，為各國個資保護立法確立了最低標準，也是我國個人資料保護法立法的基本精神。

由各國立法例分析可知，大陸法系國家與普通法系國家對個資保護基本觀點有明顯不同，美國作為普通法系代表國家採隱私說，一方面以隱私權為基礎以個資控制權為核心，比較能以社會宏觀經濟利益角度切入，主張以自律模式處理私部門個資問題，

因此對個資流通對個資保護有較大限度容忍度，比較有利於巨量資料的應用。但大陸法系國家則採識別說，例如德國以人格權為基礎以個資自決權為核心，構築個資保護體系，對個資保護較於普通法系嚴格，我國個資法立法比較屬於後者，在基本概念已經對巨量資料應用採取較嚴格的態度，也比較不利於巨量資料的使用。

觀察國際上，普遍存在個資立法無法配合科技社會演進之困難，我國個資法立法過程也面臨到相同問題，現今科技與技術的發展早已不可同日而語，巨量資料觀念的形成與蒐集處理技術的突破，在國內均是近年的發展，有關隱私權保護的法律觀點，許多已不符現今巨量資料應用所需，二者間衝突與適用障礙非常明顯，也成為巨量資料應用未來發展的無形障礙之一。

根據本文比對我國個資法相關條文，與巨量資料蒐集處理與利用間之關係，以現階段巨量資料之蒐集與應用，在我國個資法架構下，若其資料確屬個人資料，可能會面臨到以下幾個適法性問題，包括；一、巨大之資料蒐集量，導致無法部分或全部履行個資法第 8 條第 9 條對於特定個人資料，於蒐集處理時應盡之告知義務。二、現在持有大量資料中，因為許多屬於契約已經終止的舊客戶資料，不符合個資法第 11 條於特定目的消失或契約到期後，不得持有處理或利用的規定。三、部分蒐集方因為特定目的不清楚，可能不符個資法第 19 條須具有特定目的之要求。四、因為資料的特質所限，巨量資料若要進行行銷應用，可能無法充分執行個資法第 20 條對特定目的外利用及行銷停止相關規定與要求。五、資料量巨大到可能無法配合個資法第 54 條於首次利用即需補告知完成要求等。本文對國內外巨量資料使用案例分析，亦證明前述疑慮的存在。

現階段看來，以巨量資料特質想要突破法律障礙均非易事，建議在許多法規疑義未釐清與未放寬前，應優先應用不涉及自然人人格相關之資料或將個人資料去識別化後利用。對於新蒐集之資料，則應重新規劃個人資料蒐集流程與方法，將資料合法化，以解決後續可能之法律風險。但為順應巨量資料趨勢促進個資合理合法利用，本文建議似可採修訂個資法部分條文方式，解決個人資料保護與巨量資料應用衝突的問題。

Personal Information Protection Act and the Legal Risk of Big Data Applications in Taiwan

Jin-Lung Peng, Associate Professor, Department of Risk Management and Insurance, National Chengchi University

Yu-Pei Chen, Assistant Professor, Department of Medicine, National Cheng Kung University

Aureola Sun, Ph.D. Student, Department of Risk Management and Insurance, National Chengchi University

Summary

In spite of their underlying values, big data application now presents a unique challenge to the world of practice and research alike. This is because the talk of privacy and personality rights has become an increasing focus of governments and international organizations, resulting in successive pieces of legislation that expand their jurisdictional turf to include both privacy and personality rights. Thereby, the utilization of big data, i.e., their collection, processing and application, are potentially susceptible to the legal risks of impinging on both rights.

A glance over a series of important countries across the world would reveal the fact that there is a split of opinion between jurisdictions with common law systems and those with civil law systems on the issue of personal information protection. Free flow of personal information is apt to gain more support in countries with common law systems where efficient ideas are gaining ground, allowing for such regulations to be promulgated, which can contribute to the staggering development of big data analysis among these countries. But such opinion does not carry over to civil law systems where the deep-seated respect for personal information protection persists and drives the governments' regulatory zeal. Taiwan, which also falls into this category, frames this question in a similar vein and thereby encounters snags in wide application of big data analysis.

To date, however, those policy recipes with privacy protection occupying the central place have brought the governments an awkward position, as they might fall behind the pace of scientific and social development, which is currently the case in Taiwan. The whole society have undergone significant changes in the past decades, not only in relation to changes promoted by the advent of concepts associated with big data, but also in relation to the changes stemming from the exponential rise in the adoption of big data collection and processing technologies within the business circles. Regrettably, those legal perspectives with their predominant focus on such high-profile issue as privacy right protection appear in many cases too antithetical to big data applications and have increasingly been recognized as

a pertinent factor that stands in the way of progress on big data analysis.

This paper, by carefully examining relevant articles of Personal Information Protection Act 2010 in Taiwan, and the legal challenges faced by the collection, processing and utilization of personal big data, followed by the introduction and implementation of these articles; notes that the following number of potential practical problems might beset big data applications within the context of current Personal Information Protection Act 2010: (1) In terms of information disclosure, data collection and processing would not meet the requirement of Article 8 and Article 9 of PIPA; (2) Data controllers are very likely to breach the duty stipulated by Article 11 of PIPA, which is, deleting and discontinuing to process or use when the specific purpose no longer exists or contract period expires; (3) Some data collectors might fail to satisfy the specific purpose requirement set by Article 19 of PIPA; (4) Data controllers might violate Article 20 of PIPA at the first marketing action; (5) They also might not to meet Article 54 of PIPA which requires a notification to be given at the time where such personal information is first used.

To further illustrate the point, a variety of big data application examples are exploited, mapped and analyzed in this paper. Interestingly, most of these examples in this paper draw on the American experience, a country where personal information protection rules are applied less stringently and thus encourages, rather than inhibit, big data analysis. Another message conveyed by this analysis relate to industry type. Stated specifically, big data analysis has very broad application to a diverse range of information processing circumstances. Besides, financial and insurance sectors have also echoed this trend, leading to rapid proliferation of big data applications as compared to other industries.

Among half of the examples, personal information have come to rest in the hands of data processors, heightening the importance of having particular personal information protection framework in place for dealing with big data applications. Moreover, the legal appropriateness of big data collection, processing and utilization behind these examples has also been placed under the spotlight and the result points out a disturbingly high propensity of data breach, given the absence of ex ante approval of information owners and the lack of ex ante notification of data collectors in most examples. On the other hand, the rise of big data analysis inside domestic institutions also merits attention. As the specific case study stands, the requirements set by the Personal Information Protection Act 2010 have actually been poorly attended to, sometimes even left out of account in practice. The foregoing sample analysis and case study might have some inherent limitations; the relative small sample scale, for instance, could impair the effectiveness of the results. But such endeavors

prove to be enlightening in that they provide a relatively realistic picture of big data applications involving personal information and in that they offer an in-depth refection on major enforcement obstacles confronted by Personal Information Protection Act.

Largely determined by its fundamental nature and defining features, the big data architecture inherently contrasts with Personal Information Protection Act, and consequently, data breach seems to be a real and easy possibility. Avoidance might be a proper method of handling risk for the present moment when gaps between rules and reality still remain. To be specific, since many relevant legal concepts are still awaiting further scrutiny and classification, avoiding the use of personal information might to some extent appease un-secured data controllers. As for those institutions with abundant personal information, the way forward might be information de-identification, a necessary first step in the right direction to prevent running into data breach problems by virtue of escaping the rigor of Personal Information Protection Act without losing track of the economic values deeply embedded in personal information. With respect to new information collection, both renewed and specially-designed collection process and approaches are in great need to lend legitimacy to such data and to come to grips with the potential legal risks posed by data breach.

Both civil law systems and common law systems offer certain strengths and entail certain disadvantages. The enormous social benefits provided by personal information protection must be recognized. But such benefits might be easily obscured by too many restrictions resulting from the legislators' single-minded focus on personal information protection, which gives little room for the development of big data analysis. Germany and Japan are receiving positive international appraisal for their efforts to protect personal information. It is fairly understandable that Taiwan chose to follow a similar pattern to these two countries regarding personal information protection as Taiwan bears much resemblance to Germany and Japan in view of legal system. However, there presently exists a global impetus to promote big data applications; current personal information protection rules indeed fails to capture the power of big data applications, thus building the case for further improvement is necessary. In order to seize the opportunities and meet the challenges associated with big data, American legislators' attitude on information free-flow could profitably be taken on board when revisiting this issue. This paper, hoping to advance rational utilization of big data while managing potential conflicts and finding the right balance between efficiency and fairness in the meantime, proposes a radical shift towards utilizer accountability approach, complemented with well-performed right relief mechanisms, rather than right-claiming on the part of information owners.

參考文獻

孔令傑，2009，***個人資料隱私的法律保護***，武漢，中國：武漢大學出版社。(Kung, Ling-Chieh. 2009. ***Legal Protection of Personal Data Privacy***. Wuhan, China: Wuhan University Press.)

王志誠、陳春山、李智仁、李金樺與鄭少珏，2005，由個資法修正草案論對金融聯合徵信中心及金融機構之影響及因應途徑，***金融風險管理季刊***，1 卷 4 期：107-142。(Wang, Chih-Cheng, Chen, Chun-Shan, Li, Chih-Jen, Li, Jing-Hua, and Zheng, Shao-Jue. 2005. Assessing the impacts of the amended draft of personal information protection act on joint credit information center and financial institutions. ***Review of Financial Risk Management***, 1 (4): 107-142.)

呂丁旺，2010，淺析修正「個人資料保護法」，***月旦法學雜誌***，183 期：131-146。(Lu, Ding-Wang. 2010. The amendment to personal information protection act: A review and discussion. ***The Taiwan Law Review***, 183: 131-146.)

林秀蓮，2011，「個人資料保護法」初探，***萬國法律***，176 期：2-13。(Lin, Xiu-Lian. 2011. A pilot study of personal information protection act. ***FT Law Review***, 176: 2-13.)

邵國松，2013，「被遺忘的權利」：個人信息保護的新問題及對策，***南京社會科學***，13 卷 2 期：104-125。(Shao, Guo-Song. 2013. "The right to be forgotten" : A new proposal for personal data protection. ***Social Sciences in Nanjing***, 13 (2): 104-125.)

姚嶽絨，2012，***日本：混合型個人資訊立法保護***，http://www.legaldaily.com.cn/bm/content/2012-06/19/content_3648746.htm?node=20738，搜尋日期：2015 年 5 月 1 日。(Yao, Yue-Rong. 2012. ***The mixed personal information protection in Japan***. http://www.legaldaily.com.cn/bm/content/2012-06/19/content_3648746.htm?node=20738. Accessed May. 1, 2015.)

洪海林，2007，個人信息保護立法理念探究－在信息保護與信息流通之間，***河北法學***，25 卷 1 期：108-113。(Hong, Hai-Lin. 2007. On the legislation idea of personal information protection–Between information protection and freedom of information circulation. ***Hebei Law Science***, 25 (1): 108-113.)

范姜真媺，2012，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：69-103。(Fan Jiang, Chen-Mei. 2012. The protection of personal data and the free flow of such data. ***Law Journal***, 57 (1): 69-103.)

祝蓓蓓，2007，論個人信息的保護，***貴陽學院學報：社會科學版***，2007 卷 2 期：47-49。(Zhu, Bei-Bei. 2007. On the protection of individual information. ***Journal of Guiyang College: Social Sciences***, 2007 (2): 47-49.)

翁清坤，2010，論個人資料保護標準之全球化，***東吳法律學報***，22 卷 1 期：1-60。(Ueng, Ching-Kuen. 2010. The globalization of personal information protection standards. ***Soochow Law Journal***, 22 (1): 1-60.)

張軍，2007，***憲法隱私權研究***，北京，中國：中國社會科學出版社。(Zhang, Jun. 2007. ***Xian Fa Yin Si Quan Yan Jiu***. Beijing, China: China Social Sciences Press.)

梅紹祖，2005，個人信息保護的基礎性問題研究，***蘇州大學學報（哲學社會科學版）***，2005 卷 2 期：26-28。(Mei, Shao-Zu. 2005. Basic issues behind personal information protection. ***Academic Journal of Suzhou University***, 2005 (2): 26-28.)

許文義，2001，***個人資料保護法論***，台北，台灣：三民書局。(Xu, Wen-Yi. 2001. ***Research on Personal Information Protection Act***. Taipei, Taiwan: San Min Book.)

陳紅，2008，個人信息保護的法律問題研究，***浙江學刊***，2008 卷 3 期：147-150。(Chen, Hong. 2008. A review of the legal issues of personal information protection. ***Zhejiang Academic Journal***, 2008 (3): 147-150.)

陳起行，2000，資訊隱私權法理探討－以美國法為中心，***政大法學評論***，64 期：297-341。(Chen, Chi-Shing. 2000. A jurisprudential inquiry of information privacy based on the American law. ***Chengchi Law Review***, 64: 297-341.)

彭金隆，2012，銀行保險業務個人資料保護之法律遵循風險分析，***風險管理學報***，14 卷 1 期：75-92。(Peng, Jin-Lung. 2012. Legal compliance risk analysis of personal information protection on bancassurance. ***Journal of Risk Management***, 14 (1): 75-92.)

彭禮堂與饒傳平，2006，網絡隱私權的屬性：從傳統人格權到資訊自決權，***法學評論***，2006 卷 1 期：57-62。(Peng, Li-Tang, and Rao, Chuan-Pin. 2006. The character of the right to the internet privacy. ***Law Review***, 2006 (1): 57-62.)

湯德宗，2008，***電腦處理個人資料保護法 2008 修正草案評釋***，台灣法學會 2008 年年度法學會議，台北，台灣。(Tang, De-Zong. 2008. ***A study of amended draft of Computer-processed Personal Data Protection Law 2008***. Paper presented at the 2008 annual conference on empirical legal studies, Taipei, Taiwan.)

劉佐國，2005，我國個人資料隱私權益之保護－論「電腦處理個人資料保護法」之立法與修法過程，***律師雜誌***，307 期：42-51。(Liu, Zuo-Guo. 2005. Reflections on Taiwan personal information protection: The legislative process and the amending process of Computer-processed Personal Data Protection Law. ***Taipei Bar Journal***, 307: 42-51.)

謝青，2006，日本的個人信息保護法制及啟示，***政治與法律***，2006 卷 6 期：152-157。(Xie, Qing. 2006. Inspirations from personal information protection law in Japan. ***Political Science and Law***, 2006 (6): 152-157.)

Cate, F. H. 2006. The failure of fair information practice principles. In Winn, J. K. (Ed.), ***Consumer Protection in the Age of the 'Information Economy'***: 343-379. Oxford, UK: Routledge.

European Commission. 2012. ***Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)***. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed Aug. 16, 2015.

European Union. 1995. ***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***. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Accessed Aug. 19, 2015.

Executive Office of the President. 2014. ***Big data: Seize opportunities, preserving values***. https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. Accessed Oct. 1, 2015.

Federal Government. 1970. ***Fair Credit Reporting Act***. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act. Accessed May. 1, 2015.

German Government. 1977. ***Gesetz zum schutz vor mißbrauch personenbezogener daten bei der datenverarbeitung [Act concerning the abuse of data in data processing]***. http://www.gesetze-im-internet.de/bdsg_1990/. Accessed Oct. 3, 2015.

Langheinrich, M. 2001. Privacy by design–Principles of privacy-aware ubiquitous systems. In Abowd, G. D., Brumitt, B., and Shafer, S. A. N. (Eds.), ***Lecture Notes in Computer Science: Vol. 2201. Ubicomp 2001: Ubiquitous Computing***: 273-291. Berlin, Germany: Springer. doi: 10.1007/3-540-45427-6_23

Mayer-Schönberger, V., and Cukier, K. 2013. ***Big Data: A Revolution that will Transform How We Live, Work, and Think***. Boston, MA: Houghton Mifflin Harcourt.

Organization for Economic Co-operation and Development. 1980. ***OECD guidelines on the protection of privacy and transborder flows of personal data***. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpe

rsonaldata.htm. Accessed Aug. 22, 2015.

_____. 1999. ***OECD guidelines for consumer protection in the context of electronic commerce***. http://www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm. Accessed Aug. 24, 2015.

President's Council of Advisors on Science and Technology. 2014. ***Report to the president. Big data and privacy: A technological perspective***. https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf. Accessed Aug. 10, 2015.

Shirota, M. 2012. ***Big Data No Shougeki***. Tokyo, Japan: Toyo Keizai.

Warren, S. D., and Brandeis, L. D. 1890. The right to privacy. ***Harvard Law Review***, 4 (5): 193-220. doi: 10.2307/1321160

Westin, A. F. 1968. Privacy and freedom. ***Washington and Lee Law Review***, 25 (1): 166.

Whalen v. Roe, 429 U.S. 589, 1977

作者簡介

*** 彭金隆**

國立政治大學風險管理與保險學系副教授。國立政治大學企業管理博士，主要研究領域為銀行保險、資訊不對稱、金融控股公司、個人資料保護等。學術期刊曾發表在經濟論文、管理評論、臺大管理論叢、Journal of Financial Studies、The Geneva Risk and Insurance Review、The Geneva Papers on Risk and Insurance - Issues and Practice、The North-American Journal of Economics and Finance、Journal of Insurance Issue 等。

陳俞沛

國立成功大學醫學系及藥學系臨床助理教授，國立成功大學法律系兼任副教授，衛生福利部台南醫院中醫科主任。國立政治大學風險管理與保險博士，主要研究領域為醫療法規、全民健保與醫療保險。學術期刊曾發表在醫療品質雜誌、國立中正大學法學集刊、東吳法律學報、風險管理學報與臺灣法學雜誌等。

孫群

國立政治大學風險管理與保險學系博士生。

E-mail: jlpeng@nccu.edu.tw