大數據時代下隱私權之保護
——可能之影響暨對策*

許炳華**

要　目

DOI：10.3966/199516202016110020003

* 本文特別感謝兩位匿名審稿委員惠賜之寶貴意見，初稿內文與註解經修改增訂後成為本文，當然，一切文責仍由筆者自負。

** 臺灣高雄地方法院檢察署檢察事務官兼組長，國立中正大學法學博士。

投稿日期：一〇五年三月二十二日；接受刊登日期：一〇五年八月十四日

摘　要

大數據直到近來才躍升為主流名詞，在二〇一二年之前，大數據僅為存在於工程師及科學家間用以描述數位通訊、數值計算、資料儲存發展之行話。大數據代表龐大遽增的能力，以飆速、微成本來蒐集、儲存及分析先前殊難想像其數量之資料，而為維護治安、國家安全、醫療、商業及其他重要領域帶來無邊之利益，大數據時代已經到來，卻同時以幾乎不受監督之方式影響個人之基本權利，這當中，可確定遭受危害最鉅者為隱私權，隱私為重要之人類價值，科技之進步固然危及個人隱私，卻也是反思如何加強保障隱私之契機，就如同其他新興科技，大數據亦呈現引領人類進入嶄新之發現及創造世紀的高度可能性，然而，在我們每天的日常生活，大家均合理地期待，即便自己參與的是公開活動，個人還是都能保持某種程度之隱密性，大數據使得隱私保障之問題更為艱鉅及重要，大數據時代究為隱私之死亡或為重生，恐怕還端視如何因應，本文將重點放在大數據時代對於隱私權之影響，列舉厥為重要之維護治安、醫療及商業領域，並提出適用正當法律程序，尤其在政府自第三人處取得個人資料，健康隱私特殊論及消費者隱私實定法化、被遺忘的權利之概念，希冀能作為大數據時代下隱私權保護可能之對策。

關鍵詞： 大數據、隱私權、美國聯邦憲法增修條文第四條、正當法律程序、被遺忘的權利

壹、前　言

今天的人們處身於資料世紀，根據統計目前每天有幾近2.5百萬[3]位元組的資料被創造，然而，世界上有90%的資料是在最近兩年才被產出，大數據（big data）直到近來才躍升爲主流名詞，在二〇一二年之前，大數據僅爲存在於工程師及科學家間用以描述「數位通訊」（digital communications）、數值計算、資料儲存發展之行話[1]。大數據代表龐大遽增的能力，以飆速、微成本來蒐集、儲存及分析先前殊難想像其數量之資料，而爲維護治安、國家安全、醫療、商業及其他重要領域帶來無邊之利益，大數據時代已經到來，卻同時以幾乎不受監督之方式影響個人之基本權利，這當中，可確定遭受危害最鉅者爲隱私權，隱私權之保護在大數據時代可能具有超乎想像之重要性，對於隱私權保護之基本理論約略有：獨處權理論[2]、親密關係自治理論[3]、一般人格權理論[4]、合理隱私期待[5]，本文將重點放在大數據時代對於隱私權之影響，列舉厥爲重要之維護治安、醫療及商業領域，並

1 Joseph Jerome, Big Data: Catalyst for a Privacy Conversation, 48 IND. L. REV. 213, 214 (2014).

2 1890年美國最高法院大法官Louis D. Brandeis及律師Samuel D. Warren在其聯手發表之重要文獻——「隱私權論」（The Right to Privacy），提出「隱私權亦即不受他人干擾之權利」（the right to privacy equated to be let alone by other people），即使個人選擇將其思想、感情、情緒傳達予他人，仍保留限制公開範圍之權利，Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 213 (1890).

3 本說認為所謂的隱私權，乃對於所謂的公眾或社會生活，與私人之生活、私密作一區分，因隱私是一切信賴關係的基礎，針對專屬個人之「親密關係」（intimacy）加以保障，Ferdinard D. Schoeman, Privacy and Social Freedom, 1992，轉引自陳起行，資訊隱私權法理探討——以美國法為中心，政大法學評論，第64期，2000年12月，頁306。

4 本說主張隱私權之定義實質上與一般的人格權具有同樣的功能，與大陸法系對於個人私密資訊之處理異曲同工，LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 886-89 (1978).

5 最早由John Harlan大法官在Katz v. U.S.案提出用以限定隱私受到保護的基準，係對隱私須有合理期待，Katz v. United States, 389 U.S. 347, 389 (1967).

提出適用正當法律程序，尤其在政府自第三人處取得個人資料，健康隱私特殊論及消費者隱私實定法化、被遺忘的權利之概念，期待能在上開基本理論之導引下，能作爲大數據時代下隱私權保護可能之對策，並提供我國作爲反思。又本文所引用之資料多數爲美國文獻，因此後述之舉例及法律分析亦多擇取自美國素材及在該等脈絡下所爲，附此敘明。

貳、大數據時代

一、何謂大數據

大數據意指該等資料組之匯集過於龐大及複雜，傳統之資料庫系統已無法有效地處理及運作[6]，世界頂尖資訊科技研究公司Gartner之分析師Doug Laney曾將大數據定義爲「巨量」（high-volume）、「極速」（high-velocity）、「高度多樣性」（high-variety, 3V's[7]）之資料資源，而以成本效益及革新之方式來進行處理，達成促進遠見及決策[8]。然而，大數據是否已發展出一個一般性可普爲接受之定義，尚有疑問[9]，或僅可謂大數據乃一個廣義且不精確的名詞，指涉在資訊科學及預測分析中龐大資料之使用[10]。

也因此，或許用描述的方式，更能體現大數據之精神，大數據是

6 Darren S. Tucker & Hill B. Wellford, Big Mistakes Regarding Big Data, 14(2) ANTITRUST SRC. 6, 6 (2014).

7 亦有加上「超真實性」（high-veracity）而成為4V's, What is Big Data, University Alliance, http://www.villanovau.com/resources/bi/what-is-big-data/#.VVhXa2Aw_m4 (last visited: 2015.05.17).

8 Big Data, Gartner, http://www.gartner.com/it-glossary/big-data (last visited: 2015.05.17).

9 Mark A. Rothstein, Ethical Issues in Big Data Health Research, Ethical Issues in Big Data Health Research, 43 J.L. MED. & ETHICS 425, 425 (2015).

10 Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B. C. L. REV. 93, 95 (2014).

一種無法量化之資料神話，其價值顯現於文化、科技、學術[11]，在該等現象下，整個世界將轉變成足供探勘之資料藍海，並提供我們全新之視野[12]，該等資料之規模及範圍所賦予之展望及價值最終將改變人際間之互動[13]。此外，大數據爲一種全新的實證調查方法[14]，今日的學術界、政府機關、民間企業利用該等方法來改善醫療品質、增進國家智慧電網的效率、暢通公路交通流量、預測全球財物交易流量等，可說沒有任何一項人類努力的成果不會受到該項新科技的影響[15]。

二、演　進

大數據資料其背景之發展乃大數據與隱私權間互動之關鍵[16]，臺拉維夫大學（Tel Aviv University）法學院教授Michael Birnhack曾以其間典型之參與者、相互關係、資料數量、資料之來源及性質、造成隱私損害之類型來劃分資料演進之連續階段[17]。前後演進固然有其時序關係，然後階段之到來並不表示前階段之爭議完全消失匿跡。

㈠小型資料

小型（small）資料僅牽涉單一團體及個人，所損害者亦僅爲另一人之少數位元資料，雙方間通常具備某種程度（血緣、社交、職場）關係，例如鄰居、同事，這個階段促使美國最高法院法官Louis

11 Danah Boyd & Kate Crawford, Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon, 15 INFO., COMM. & SOC'Y 662, 663 (2012).

12 VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 7 (2013).

13 *Id*. at 6-7.

14 *Id*. at 6.

15 Michael Mattioli, Disclosing Big Data, 99 MINN. L. REV. 535, 539 (2014).

16 HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 52 (2009).

17 Michael Birnhack, S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm, http://ssrn.com/abstract=2310700 (last visited: 2015.05.19).

Brandeis、律師Samuel Warren提出「不受干擾之權利」（right to be let alone）[18]及侵權法權威William L. Prosser臚列出隱私侵權之類型[19]，本階段法律企求維護個人本身之隱密空間，由於兩造間存有一定之關係，社會規範可能尚有其效果存在[20]。

㈡中型資料

此階段雖然仍只有兩方當事人，但差別在於資料之數量及平衡之力量，相較於小型資料階段之一次性侵害，中型（medium）資料階段之一方當事人躍升爲資料控制者，蒐集資料並重複使用，例如雇主及員工、保險公司及消費者，本階段法律嘗試考量資料控制者之正當目的，例如美國「家庭教育權利及隱私法」（Family Educational Rights and Privacy Act, FERPA），在確保學生之資料不會遭受濫用，當政府機關爲資料控制者時，美國憲法增修條文第四條[21]（以下簡稱「增修條文第四條」）被援引以爲平衡之機制[22]。

㈢大型資料

進入一九七〇年之「大型」（large）資料年代，隨著科技之進步，蒐集個人資料更形容易，資料控制者與資料主體間可能也不再存在任何親近關係，雙方間不平等之關係更爲加劇，典型的情況爲單一資料控制者於一資料庫中處理眾多個人資料，而基於不同使用目的，

---

18 當然，此階段亦隨著科技之進步，兩造間亦可能轉變成不具契約或信賴等一定關係，而有求助承認隱私權之必要性，Warren & Brandeis, *supra* note 2, at 193.

19 William L. Prosser, Privacy, 48 CAL. L. REV. 383, 422 (1960).

20 Birnhack, *supra* note 17.

21 美國憲法增修條文第4條規定：「人民有保護其身體、住所、文件與財物之權，不受無理拘捕、搜索與扣押，並不得非法侵犯。除有正當理由，經宣誓或代誓宣言，並詳載搜索之地點、拘捕之人或收押之物外，不得頒發搜索票、拘票或扣押狀。」原文為“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

22 Birnhack, *supra* note 17.

並將之傳遞於「第三人」（the third party），社會規範已不具任何效力，個人資料一旦進入資料庫，資料主體對於該等資料之利用幾乎無置喙之餘地，資料庫可能在未經資料主體之同意下被惡意濫用以進行差別待遇或以新的目的重新使用[23]。於是在此時期資料保護相關法律遂起，美國一九七四年之「隱私法」（Privacy Act of 1974）[24]即爲重要里程碑，繼而有一九八〇年「經濟合作暨發展組織」（Organization for Economic Co-operation and Development, OECD）之「隱私權保障及個人資料跨國境流通指導準則」（OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data），隨後則有現爲全球執行一九九五年之「歐盟資料保護指令」（EU Data Protection Directive），以一系列防禦型或「同意導向」（content-based）之立法來作爲因應[25]。

㈣超大型資料

一旦由「百萬位元」（megabytes）進入「萬億位元」（terabytes），個人資料之風險更爲急遽攀升，此即爲「超大型」（extra-large）資料年代，亦即大數據，個人資料經由多樣性之來源被蒐集，資料控制者爲何已不必然清楚，控制之方式亦不斷改變，個人資料無所不包地被蒐集，資料被「去脈絡化」（decontextualized）後再以不同方式「再脈絡化」（recontextualize），原有之「通知及同意」（notice and consent）機制不復可能，在「極大化」（maximization）法則下運作之大數據，可能使得現行法律體系無法因應[26]。

---

23 *Id*.

24 *See* 5 U.S.C. § 552.

25 Birnhack, *supra* note 17.

26 不過亦有持對立看法者，認為既有之個人資料保護原則，在大數據時代仍得以運作，Article 29 Data Protection Working Party, Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU, http://ec.europa.eu/justice/data-

而從另一個角度觀察大數據之革命進程，乃由微處理器計算之能力，進入接受大數據以進行連結，再進入認知大數據以進行預測[27]。

三、正反評價

㈠正面評價

1. 新契機

大數據分析得以提高經濟生產力，並改進消費者及政府服務，甚至遏阻恐怖分子及拯救生命，例如：「物聯網」（Internet of Things）融合了產業與資訊經濟；美國醫療照護與醫療救助服務中心（The Center for Madicare & Medicaid Service, CMS）開始使用預測分析軟體來於醫療給付前先行警示賠償詐騙個案；阿富汗戰爭期間，美國國防高等研究計畫署（Defense Advanced Research Projects Agency, DARPA）研發出「Nexus 7」，結合衛星及監控資料來定位及摧毀土製炸彈以對抗恐怖分子；醫學研究綜合百萬筆資料樣本來判斷新生兒中易受病菌感染者[28]。

2. 客製化

在整合許多不同資料後，得以在顧客未提出詢問前即傳遞正確的訊息、產品及服務，集合多筆資料亦可描繪出個別顧客清晰之圖像以預測其行為，該等詳細之資料檔案及客製經驗在消費者行銷充分發揮效益[29]。

3. 資料永久存在

在數位時代，資訊被高精確度地留存、複製、分享及移轉，相較

---

protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf (last visited: 2016.06.18).

27 Neil M. Richards & Jonathan H. King, Big Data Ethics, 49 WAKE FOREST L. REV. 393, 397-408 (2014).

28 John Podesta et al., Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, https://www.whitehouse.gov/sites/default/files/docs/big_ data_privacy_report_may_1_2014.pdf (last visited: 2015.05.17).

29 *Id*.

於過往保存資料之昂貴性，大數據時代之資料則僅以極低成本之晶片即可保存，資料只要一經產生，幾乎可以有效地永恆存在[30]。

4. 無所不能

計算機的能力使得「海底撈針」不再是夢想，在以往搜尋龐大資料必須該等資料業經過組織，且還需擇取適當指令方能獲得答案，大數據分析則不但可收納任何未結構化之資料，甚至進一步找出其中之不規則性或軌跡[31]。

㈡負面評價

1. 對隱私之衝擊

大數據爆發之科技能量固然帶來新契機，但應注意該等契機伴隨而來之社會、倫理危機；而客製化可能帶來價格、服務之差別待遇，且大公司擁有顧客之偏好等所有資料，但顧客本身卻無從知悉該等資料如何被蒐集、使用及再利用；另當個人資料永久地掌控在他人手裡時，如何確保資料無外洩之安全顧慮；至於爲求能獲得特定之小成果，則必須擁有更爲大量的資料，此亦爲個人隱私最大之隱憂[32]。

2. 迷　思

大數據確然掌握了未來無限的可能性，然其間有三個迷思，其一，「透明度」（transparency）之迷思，大數據分析倚賴個別資料包括人、地點、事物之輸入，該等資料蒐集之過程可謂不著痕跡，利用大數據之目的原意在使世界更透明，然其蒐集資料之方式卻幾近無形，使用之工具及技術使人無法察覺，該等祕密監控的系統及無法受到監督的決策過程委實無法令人接受[33]；其二，「認同」（identity）之迷思，大數據之目的在找出同一性，然也威脅到認同感，人類本能

30 *Id.*
31 *Id.*
32 *Id.*
33 Neil M. Richards, The Dangers of Surveillance, 126 HARV. L. REV. 1934, 1959 (2013).

企求對自我之認同，然在大數據時代下，自我之空間逐漸萎縮，因大數據將比任何人還瞭解其自己，大數據之力量透過資料來刺激、說服、影響、甚至限制自我認同[34]；其三，「權力」（power）之迷思，大數據被形塑爲權力的工具，讓使用人觀看更爲精確及清晰的世界圖像，然大數據之力量僅掌握在少數之有權者，而非一般民眾[35]。

四、類　比

大數據時代爲社會帶來諸多利益，就如同人類之前發現石油，而使世界改觀一樣，同樣利弊互現，若將石油世紀與大數據時代作比較，更能對照兩者對於隱私及環境之互動關係[36]。

㈠資料外洩

石油之淬鍊、運輸及儲存無可避免導致石油外溢，石油外溢損害了海岸線、海灘、環流系統及飲水品質，亦衝擊漁業及旅遊等產業，資料外洩亦復如此，自二〇〇五年起，業有超過4,000起資料外洩事故，近來大規模之事件包含二〇一一年之Sony資安事件，外洩超過12百萬筆加密之信用卡卡號；二〇一三年之Target感恩節、耶誕節購物資安事件，外洩大約70-110百萬筆客戶資料[37]；資料掮客爲求取利益，不擇手段任意蒐集個人資料再加以出售之亂象，更惡化資料外洩的問題，其所造成之損害包括個人身分遭竊取、敏感性資料流出使個人遭標籤化，就如同石油外溢一樣，些許資料之外洩往往釀成大災害[38]。

---

34 *Id*. at 1955-56.

35 Neil M. Richards & Jonathan H. King, Three Paradoxes of Big Data, 66 STAN. L. REV. ONLINE 41, 42 (2013).

36 Dennis D. Hirsch, The Glass House Effect: Big Data, the New Oil, and the Power of Analogy, 66 ME. L. REV. 373, 377 (2014).

37 *Id*. at 378.

38 *Id*. at 380.

㈡玻璃屋效應

石油燃燒產生二氧化碳堆積在上流空氣層而引發「溫室效應」（greenhouse effect），促使全球暖化及氣候變遷，損害人類居住環境；同樣地，大數據科技產生之資料在近兩年以光速成長，就如同溫室效應下匯聚了太陽光，大數據亦蒐羅了個人有關醫療狀況、性傾向、政治喜好及其他敏感性資料，這種現象或可稱爲「玻璃屋效應」（glass house effect），大數據創造了一個世界讓每個人逐漸身處玻璃屋內，個人之特徵包括人際關係、政治信仰、嗜好、前科、財務狀況及更多的資料，都一覽無遺，任人觀賞[39]。溫室效應改變地球氣候而不利人居住，玻璃屋效應亦影響社會氛圍而戕害人類身心靈發展，若任由該等現象持續發酵，恐怕會激起對於大數據在社會及政治上之反撲[40]。

五、小　結

史丹佛網路暨社會研究中心（Stanford Center for Internet and Society）教授Omer Tene曾提出既存之人類組織面臨三大社會－技術－商業（socio-technological-business）轉變之挑戰，第一個即大數據及分析之浪潮[41]。然如前所述，大數據時代之來臨正反評價互現，其對於隱私之影響就如同石油世紀對於環境之效應，均可能帶來全面性無法彌補之損害。因此，若大數據爲人類之未來，則隱私在未來還有無容身之處？隱私之價值在於認同、平等、安全、信任，隱私作爲一種社會價值[42]，應成爲資訊社會發展之界線[43]。

---

39 *Id*. at 381.

40 MAYER-SCHÖNBERGER & CUKIER, *supra* note 12, at 4.

41 另兩個分別為社群網路革命及雲端運算，Omer Tene, Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws, 74 OHIO ST. L.J. 1217, 1228 (2013).

42 Gordon Hull, Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data, http://ssrn.com/abstract=2533057 (last visited: 2015.06.02).

43 Neil M. Richards & Jonathan H. King, Big Data and the Future for Privacy,

參、大數據對於隱私權之影響

大數據之影響由以上之論述略可觀之，以下針對其對於隱私權之影響進行更爲細膩之探討，事實上，大數據對於隱私權之影響層面甚爲廣泛，例如：選民隱私，政黨對於選民資料庫之利用，不但危及選民政治意向之隱私，亦傷害民主過程[44]；又例如：刑事被告之隱私，審判程序中電子化證據開示有其重要性，但若未有「正當法律程序」（due process）之強調，隱私權將岌岌可危[45]。本文則提出大數據對於隱私權影響最爲深刻且嚴峻的三個層面：「維護治安」（policing）[46]、醫療、商業[47]以供探討。

一、維護治安

執法機關可謂欣然接受大數據時代之到來[48]，治安工作包含蒐集犯罪活動及犯罪嫌疑人之資料，大數據提供一個嶄新及絕佳之蒐集、分析資料之工具，並從該等資料確認特定之嫌疑人及犯罪模式以追蹤及預防犯罪[49]。在績效導向下，不管有意或無意，可能對於隱私之侵害採取漠視之態度。

---

http://ssrn.com/abstract=2512069 (last visited: 2015.05.23).

44 Ira S. Rubinstein, Voter Privacy in the Age of Big Data, 5 WIS. L. REV. 861, 862-65 (2014).

45 Brandon L. Garrett, Big Data and Due Process, 99 CORNELL L. REV. 207, 216 (2014).

46 維護治安及審判程序大致上亦可歸類為廣義之刑事程序，然相較於審判程序之個案特定，且係在公開之法庭及專業之法官面前進行，維護治安之層面顯然廣泛而不特定，亦彰顯其影響之深遠。

47 民眾之資料在政治活動及商業活動中均有被利用之可能，然畢竟不是每位民眾均熱衷政治活動，惟在商業行為發達之今天，每個人在日常生活中卻均可能為消費者，而受到不特定之影響。

48 Chris Jay Hoofnagle, Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N. C. J. INT'L L. & COM. REG. 595, 596 (2004).

49 Andrew G. Ferguson, Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards, 66 OKLA. L. REV. 831, 835 (2014).

㈠運　用

1. 蒐集資料

資料庫及「資料探勘」（data mining）之運作雖已有相當歷史[50]，但進入大數據時代仍有極大幅度的改變[51]，由於資料容量持續成長，每一筆公共資料、犯罪紀錄、財務資訊均爲第三人之團體[52]所蒐集，而這些團體則將上開資料出售予政府執法部門[53]，自二〇〇一年九月十一日起，美國「司法部」（Department of Justice）不只透過聯邦調查局（Federal Bureau of Investigation, FBI）以反恐之名義蒐集數千筆美國人之電話通話紀錄、銀行帳戶資料及其他個人資訊，亦以偵查一般刑事案件之名義來取得前揭資料[54]；另執法部門亦得以迅速地由當地警察局之電腦獲得個人資料，此對於偵查人員而言，有莫大之破案利益[55]。

2. 預測分析

以前開蒐集資料爲根基，全美國之執法機構競以大數據之治安預測模式希望解決懸案或預防未來之犯罪[56]，該等模式使用近期發生犯罪之日期、時間、類型、地點其組合，以歷史之犯罪資料來確認「犯罪熱區」（hot spots）[57]。治安預測科技之理論基礎在於犯罪乃習慣之

---

50 Fred H. Cate, Government Data Mining: The Need for a Legal Framework, 43 HARV. C. R.- C. L. REV. 435, 442 (2008).

51 Anita L. Allen, Privacy Law: Positive Theory and Normative Practice, 126 HARV. L. REV. F. 241, 246 (2013).

52 個人資料為第三人掌控之情形隨著民營化現象將愈見明顯，以我國而言，電信業民營化及高速公路收費系統委由遠通電收營運均為著例。

53 Stephen Rushin, The Judicial Response to Mass Police Surveillance, 2011 U. ILL. JL TECH. & POL'Y 281, 288 (2011).

54 Christopher Slobogin, Government Data Mining and the Fourth Amendment, 75 U. CHI. L. REV. 317, 317 (2008).

55 Ferguson, *supra* note 49, at 839.

56 類似的場景或許可參見電影「關鍵報告」（The Minority Report）：主要描述一個能夠預測犯罪並在罪犯犯罪以前逮捕他們的未來世界。

57 Crawford & Schultz, *supra* note 10, at 103.

產物，犯罪人慣行於同一區域、相同時段以類似手法進行犯罪[58]，最新之治安預測軟體業使用大數據分析來確認特定類型犯罪之高度密度性，將該區標示後以派遣巡邏勤務[59]。大數據將大幅度影響警察維護治安之工作，其一，透過姓名及包含前科、個人歷史資料，連接臉部辨識及其他生物統計確認科技，得使未知之嫌疑犯曝光；其二，從資料中分析出之模式，得由嫌疑人過去之犯罪行為預測其未來之犯罪可能性，大數據之發展可能改寫警察街頭巡邏勤務之相關作為及法制[60]，由於得以預防機先，警察可以將被動且漫無目的之街頭巡邏勤務轉變為主動且事先擘畫之查緝，而因為事先及主動之特性，亦得以大幅度降低與歹徒在街頭猝遇而衍生之諸如使用警械過當、人員傷亡等問題。

3. 大監控

電子監控系統長期以來成為警方之利器[61]，紐約市警察局（New York City Police Department, N.Y.P.D.）業使用整合市區3,000支監視錄影器、200套車牌自動辨識系統、2,000組熱感應器及警察資料庫以形成區域警戒系統（Domain Awareness System, DAS）[62]來確認可能之威

58 Andrew G. Ferguson, Predictive Policing and Reasonable Suspicion, 62 EMORY L.J. 259, 262 (2012).

59 Kelly K. Koss, Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow World, 90 CHI.-KENT L. R. 301, 307 (2015).

60 Andrew G. Ferguson, Big Data and Predictive Reasonable Suspicion, 163 U. PA. L. REV. 327, 351 (2015).

61 我國使用電子監控系統亦引發爭議，「台北市長柯文哲日前曾說要開放監視器抓違停，引發各界熱議。台北市交通局長鍾慧諭受訪表示，監視器抓違停將先暫緩，因為法令爭議仍在討論中，等到各界都有共識後才會推行。」中央通訊社網站，http://www.cna.com.tw/news/firstnews/201505095012-1.aspx，造訪日期：2015年5月27日。

62 利用國道監控系統即要求第三人提供資料來進行犯罪偵查在我國亦引起爭議，「媒體報導，警政署發文給交通部高速公路局以及遠通電收，要求高公局協助，正式通知遠通公司提供所代為蒐集的全部國道行車紀錄資料，引發爭議。」中央通訊社網站，http://www.cna.com.tw/news/firstnews/201401110016-

脅，包括「無主行李箱」（unattended bags），該局宣稱區域警戒系統得以車輛來定位犯罪嫌疑人，並回溯追蹤其過往之蹤跡，同時可以將車牌號碼與名單進行比對，立即提供警方車主之前科，二〇一三年十一月紐約市警察局即仰賴上開系統來監控紐約馬拉松大賽以預防可能之恐怖分子[63]，小都市之執法機關亦不遑多讓，奧克蘭市警察局（Oakland Police Department, OPD）並援用上揭系統以整合警消勤務派遣、「槍響定位」（gunshot detectors）、車牌辨識、社群媒體[64]。

*4.*DNA資料庫

另一個運用面向看似平靜無波，然相較於大監控等運用其影響力絲毫不減者爲「去氧核醣核酸」（deoxyribonucleic acid, DNA）資料庫之建置，二〇一三年六月爲止，美國業蒐集1,070萬筆罪犯及170萬筆被逮捕人之資料以建置全世界最大型之DNA資料庫，執法機關使用「DNA檢索整合系統」（Combined DNA Indexing System, CODIS）連結全國不同DNA資料庫，將犯罪現場之跡證與資料庫內之罪犯、被逮捕人進行比對以進行偵查，然DNA資料庫仰賴DNA之強制採集，採集之範圍由最初之暴力及性侵害重刑犯，逐步擴展到妨害風化之輕罪類型，紐約更率先於二〇一二年將該等採集範圍涵蓋至全部類型之犯罪行爲人[65]，而在經過最高法院Maryland v. King案肯認拘留所人員依法以棉棒擦拭被逮捕人的口腔二側黏膜細胞以取得DNA樣本爲合理搜索後[66]，可預見各州將起而效尤[67]。

㈡影　響

大數據之使用容或讓執法機關在維護治安上如虎添翼，然對於隱

1.aspx，造訪日期：2015年6月2日。

63 Elizabeth E. Joh, Policing by Numbers: Big Data and the Fourth Amendment, 89 WASH. L. REV. 35, 49-50 (2014).

64 *Id*. at 50.

65 Joh, *supra* note 63, at 51.

66 *See* Maryland v. King, 133 S. Ct. 1958 (2013).

67 Joh, *supra* note 63, at 51-52.

私帶來間接及直接之重大影響，實令人憂心。

1. 錯誤資料

資料庫仰賴正確、即時之資料，然前開警方獲得之資料並無法保證其正確性，即連FBI之資料庫都曾被發現上千筆錯誤的資料，若資料係來自公部門外之第三人將使問題更形惡化，全球第三大聯播網CBS無線電視台在二〇一三年即曾報導，有4,000萬名之美國民眾其在散處各處資料庫之信用資料出現錯誤，然也因爲大數據之過於龐大，現今並無任何機制得以修改這些錯誤[68]。美國最高法院大法官Ruth Ginsburg在Herring v. United States案即曾警示：「資料庫內不正確之資料對於個人自由之影響值得關注，僅僅因爲無法維持資料庫內正確之資料而形成之錯誤，對於在街上遭受逮捕、上銬、搜索之公民尊嚴實屬莫大之侵犯」[69]。在缺乏透明度下，亦難以期待任何公私部門負起稽核日漸龐大之兩部門資料庫，無怪乎招致：「大數據所獲得之犯罪懷疑可能立基於不良的資料」（big data suspicious may be based on bad data）之批判[70]。

2. 誤　判

縱然假設前開資料均無錯誤，亦可能產生誤判，上揭預測分析乃基於特定個人之前科紀錄，而非該行爲人之現況及實際行爲，無異成爲特定人之「紅字烙印」（scarlet letter），徵諸美國歷史，窮人及有色人種成爲最有可能列入資料庫黑名單之族群，根據美國公民自由聯盟（American Civil Liberties Union, ACLU）於二〇一三年之統計，即使犯罪紀錄相同，非裔美國人在街上被逮捕之機率遠高於其他族群，故而如何蒐集、選擇及解讀資料亦爲一大問題，前開所謂治安預測也可能因偏見而遭致誤判[71]。

---

68 Ferguson, *supra* note 60, at 399.

69 *See* Herring v. United States, 555 U.S. 135, 155 (2009).

70 Ferguson, *supra* note 60, at 400.

71 *Id*. at 402.

3. 株連效應

DNA資料庫所導出的問題則爲家族DNA比對，其假設最近親屬間分享更多之基因資訊，「家族DNA搜尋」（familial DNA search）乃利用已建檔者的DNA紀錄，進一步鎖定其尚未建檔親屬作爲嫌疑人的資料庫應用方法，該等偵查方法不但同樣使得少數族群受到不公平之對待，亦侵犯尚未建檔親屬之隱私，實可謂另一種「基因監控」（genetic surveillance）[72]。

4. 無所遁形

在前開大監控（mass surveillance）下，透過大數據得以比本人更了解其個人之情況[73]，二〇一三年之「斯諾登」（Snowden）事件[74]更使人們驚覺於政府「老大哥」（big brother）如何以國家安全爲由讓民眾無所遁形[75]，美國「國家安全局」（National Security Agency, NSA）以棱鏡計畫（Prism Program）[76]、XKeyscore計畫[77]爲名，大規

---

72 Joh, *supra* note 63, at 52.

73 Brad Turner, When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People's Data, 16 N. C. J. L. & TECH. 377, 395 (2015).

74 「美國國家安全局承包商前雇員史諾登（Edward Snowden）揭發美國大量擷取網路伺服器和海底纜線上傳輸的資料，並監控歐盟友邦的通訊資料，引起歐洲人對網路安全的關注及疑慮。」中央通訊社網站，http://www.cna.com.tw/news/ait/201412050313-1.aspx，造訪日期：2015年6月3日。

75 類似的場景或許可參見電影「全民公敵」（Enemy of the State）：「片中男主角隱私權遭美國國家安全局嚴重侵犯，所衍生出的驚悚情節令人印象深刻：信用卡被停用、家居生活被隱藏式攝影機窺伺、行動電話被竊聽，不管人逃到哪裡，很快就在全球定位系統的螢幕上被鎖定等。」

76 「稜鏡計畫允許美國國家安全局和聯邦調查局等，任意使用合作公司網路伺服器中任何人的私密資料，而且這項行動對外以最高機密等級保密。該計畫涉及的網路公司共有9間，分別為Microsoft、Google、Yahoo!、Facebook、PalTalk、YouTube、Skype、AOL及Apple」，專利知識庫網站，http://www.naipo.com/Portals/1/web_tw/Knowledge_Center/Laws/US-77.htm，造訪日期：2016年6月16日。

77 「『Xkeyscore』的監控計畫『幾乎可以涵蓋所有網上資訊』，可以最大範圍收集互聯網資料，內容包括電子郵件、網站資訊、搜索和聊天記錄等等。根據相關資料，美國情報機構分析人員甚至可以通過『Xkeyscore』計畫對個人的互聯網活動進行即時監控。2012年『Xkeyscore』在1個月內存儲的各類監控資

模蒐集個人資料及資訊，包含電子郵件內容、「網路流量」（internet traffic）[78]，最高法院在Clapper v. Amnesty International案即直陳政府得以執行全面監控之能力[79]。

5.不受規範

國家經由政府之資料庫蒐集及利用資料對於隱私之侵害業如前述，然更嚴重的可能爲國家透過第三人來取得資料之模式，因可能根本不受相關法令規範，美國憲法在人民與政府間建構一套權力分享之關係，增修條文第四條就如同其他「權利法案」（Bill of Rights）一樣，對於國家之行爲進行制衡[80]，民眾雖知悉其將己身資料交付第三人（例如銀行、電信公司等），然國家是否得不受任何限制自第三人取得該等資料，並加以利用在偵查犯罪上[81]？在美國，有人統計政府自第三人處取得資料可能有下列手段：其一，透過法院命令；其二，透過「傳票」（subpoena）；其三，以執法機關名義要求；其四，以金錢購買；最後，私底下以竊聽、植入木馬程式等不正當手段取得[82]，除了第一及第二個手段，其餘之手段恐怕適法性均有質疑之空間。

二、醫　療

病歷電子化及醫療資訊網路化提供公共衛生、改進醫療產出及學術研究大量之資料，該等資料裨益於公共衛生、行銷、研究、藥品研

料記錄高達410億條。」中央日報網站，http://www.cdnews.com.tw/cdnews_site/docDetail. jsp?coluid=109&docid=102405741，造訪日期：2016年6月16日。

78 Megan Blass, The New Data Marketplace: Protecting Personal Data, Electronic Communications, and Individual Privacy in the Age of Mass Surveillance Through a Return to a Property-Based Approach to the Fourth Amendment, 42 HASTINGS CONST. L. Q. 577, 579 (2015).

79 *See* Clapper v. Amnesty, 133 S. Ct. 1138, 1158 (2013).

80 *See* United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976).

81 Ferguson, *supra* note 60, at 403.

82 Turner, *supra* note 73, at 403.

發、確認副作用、「生物監測」（biosurveillance）等[83]。

㈠運　用

1. 電子病歷

資料長期以來成爲健康照護之一部分，健康照護提供者業開始使用「電子病歷」（electronic health records），該等資料大幅增加以便提供臨床醫生、研究者及病患使用[84]。從紙本病歷轉變成電子病歷在促進資料互通及分析上對於公共衛生助益甚大[85]，甚而，在許多醫療院所不願意承擔擁有及管理電子病歷軟硬體之責任下，這股趨勢朝向「雲端運算」（cloud computing）發展，來解決儲存、溝通及分析之需求[86]。

2. 藥品安全

美國「食品藥品管理局」（Food and Drug Administration, FDA）向來困擾於評估藥品之安全性及功效，也因此該局開始嘗試使用觀察性資料（observational data）來估算風險，例如「藥物不良反應通報系統」（FDA Adverse Event Reporting System, FAERS）資料庫，二〇〇八年五月復開發更大型之國家及電子資料庫——「哨兵系統」（Sentinel System）以追蹤市場上之藥品安全，至二〇一二年底已達到監控超過1億件之不良產品，除了個案評估之外，食品藥品管理局更以「經驗性貝氏伽瑪泊松分布縮檢法」（Multi-item Gamma Poisson Shrinker, MGPS）之資料探勘來進行藥物不良反應通報系統及藥物間交互作用之分析[87]。

---

83 Bonnie Kaplan, How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales, http://ssrn.com/abstract=2510013 (last visited: 2015.05.23).

84 Podesta et al., *supra* note 28.

85 Sharona Hoffman & Andy Podgurski, Big Bad Data: Law, Public Policy, and Biomedical Databases, https://www.chrp.org/pdf/HSR01182013_Abstract.pdf (last visited: 2015.05.24).

86 Frank Pasquale & Tara Adams Ragone, Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing, 17 STAN. TECH. L. REV. 595, 596 (2014).

87 Ryan Abbott, Big Data and Pharmacovigilance: Using Health Information Ex-

3.學術研究

大數據之分析被認定在妥適醫療照護之品質及效益上居功厥偉，其間之預測分析可用以追蹤醫院之供給及改善管理成本，據統計至二〇一二年，全美國之醫療院所在使用大數據上有40%之成長率[88]，將大數據使用於學術研究上除了研發出上述之藥物不良反應通報系統，還包括「流感趨勢系統」（Google Flu Trends）[89]，以預測及確認流感之爆發，「國家醫療用品零售監視系統」（National Retail Data Monitor, NRDM），以預測疾病傳染之走向等[90]，醫學研究領域之大數據分析使得公共政策亦受到影響，英國首相卡麥隆（David Cameron）即在二〇一一年宣稱該國「國民保健署」（National Health Service, NHS）所屬之病患都將成爲「研究病患」（research patient），其等之醫療紀錄均將公開供研究之用[91]。

㈡影　響

1.規範不足

對於病患相關醫療大數據之使用最大之風險即爲對隱私之侵害，即連在美國，縱然揭露醫療紀錄受到隱私法[92]、健康保險流通暨責任法（Health Insurance Portability and Accountability Act, HIPAA）及各州相關法令規範，然該等規範卻不足以涵蓋所有資料擁有者，甚者，「去識別化」（de-identified）以供公共使用之資料向來即豁免於前揭法規範，然而資料縱使經過去識別化後，對於隱私仍可能有相關細微

---

changes to Revolutionize Drug Safety, 99 IOWA L. REV. 225, 238-39 (2013).

88 Nicolas P. Terry, Protecting Patient Privacy in the Age of Big Data, 81 UMKC L. REV. 385, 409 (2012).

89 Google Flu Trends雖有其引領性，然亦受到質疑正確性不高，有其侷限，Bryan Walsh, Google's Flu Project Shows the Failings of Big Data, http://time.com/23782/google-flu-trends-big-data-problems/ (last visited: 2015.01.18).

90 Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 NW. J. TECH. & INTELL. PROP. 239, 246 (2013).

91 *Id*. at 247.

92 *See* 5 U.S.C. § 552a (2010).

之風險[93]，因一方面如資料尚屬可用，即非完全去識別化；另一方面，去識別化後仍可能經由科技爲再識別化。

2.角色衝突

醫療資料之研究機構爲政府所資助者所在多有，則是否政府即得以任意使用該等資料？而前開學術研究既使用病患之資料，似應獲得病患之同意，然在研究人員恐於若無法取得同意將減損資料之品質及學術之價值下，若要訴諸研究人員之自律，無異緣木求魚[94]；另有人雖爭辯該等作爲研究之醫療資料可能均屬去識別化之資料，然去識別化之資料不必然無隱私之疑慮，業如前述，況「任何資料不可能既具備實用性又全然無識別性」[95]，則對於隱私可能造成之影響概見一般。

3.二次利用

由於上開醫療資料之珍貴性，該等資料之二次利用被認爲裨益於個人、公共利益及學術研究，資料之跨境流動雖受到諸如「跨太平洋夥伴協定」（The Trans-Pacific Partnership, TPP）等相關國際條約所規範，然醫療資料確實在全球間，以不同目的銷售給不特定人，以基因資料爲例，雖爲研究、醫藥及「生物資料庫」（BioBanking）所需，卻也可能使得個人及群體受損，二〇〇〇年冰島國會出售其建置之27萬5,000名公民的基因資料庫予美國deCODE公司，冰島最高法院在二〇〇三年十一月二十七日以系爭資料並非無法辨識個人身分之匿名資料、相關安全保密措施不足等而未適當保障個人隱私爲由判決前開建置資料庫爲違憲[96]。

---

93 Sharona Hoffman, Citizen Science: The Law and Ethics of Public Access to Medical Big Data, http://ssrn.com/abstract=2491054 (last visited: 2015.06.10).

94 Terry, *supra* note 88, at 412.

95 Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. REV. 1701, 1704 (2010).

96 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啟示，臺北大學法學論叢，第54期，2004年6月，頁80。

三、商　業

過往各通路零售商持續蒐集每一位進入店內消費顧客之資料，逐步匯聚成一龐大之資料群[97]。

㈠運　用

1. 行　銷

大數據的長處在於預測未來，對於商業行爲之助益亦甚大[98]。帳單資料得以連結顧客及其消費模式，亦得以修正對客戶之供給[99]，資料分析並被使用於研究消費者之行爲以改進商店之陳列、產品之調製、貨架之位置等，零售商業進一步利用大數據來追蹤消費者之購買模式[100]，而各大線上科技公司，諸如：Google、Facebook、Microsoft、Apple、Amazon等，利用大數據來尋找商機，更不在話下[101]。

2. 客製化服務

今日之消費者由於電腦使用之便利性，透過網路進行商業交易已司空見慣，以線上廣告產業爲例，其在顧客瀏覽網頁或使用行動電話服務之際，就將客製化之廣告送到顧客面前，由於獲得大量之顧客個人資料，產品得以針對個人特質、偏好、社會影響力程度、財務狀況、工作進行產製，在比顧客本人都了解其自己的情況下，結合前開行銷作爲，讓顧客在商業互動中充分享受深得我心之服務[102]。

---

97 Anjanette H. Raymond, The Dilemma of Private Justice Systems: Big Data Sources, the Cloud and Predictive Analytics, http://www.alsb.org/wp-content/uploads/2015/01/NP-2014-The-dilemma-of-private-justice-systems-Raymond.pdf (last visited: 2015.06.10).

98 Dennis D. Hirsch, That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority, 103 KY. L.J. 345, 345 (2015).

99 Frank Pasquale, Grand Bargains for Big Data: The Emerging Law of Health Information, 72 MD. L. REV. 682, 722 (2013).

100 Tene & Polonetsky, *supra* note 90, at 249.

101 *Id*. at 250.

102 Podesta et al., *supra* note 28.

㈡影　響

1. 消費者隱私

大數據科技伴隨著物聯網的發展，只要從家用無線網路即可測知該家戶人數及坐落位置，「臉部辨識科技」（facial recognition technology）在本人上網時即得以線上照片加以確認[103]，由於各資料管理者所蒐集之資料均以難以想像之速度增加，對於消費者隱私及資訊安全所造成之風險亦不斷攀升[104]，而所謂提供客製化服務所帶來對隱私之侵害亦不遑多讓，Target量販店事件即爲一例[105]。至於在網路安全薄弱的今天，資料外洩所受到之侵害更形嚴峻[106]。

2. 自主性

在個人龐大之資料被積極蒐集及分析之大數據時代下，個人卻毫無參與之空間，有如站在一面資料導向的單面鏡前，導致居於資料管理者之政府或產業較其本人對於己身知悉得更爲透徹，資料演算之結果有如創造了一個重申及窄化個人思想及信念之「回音箱」（echo chamber），網路組織者先驅Eli Pariser即曾提出在Google不斷改進及

---

103 *Id*.

104 Christin S. McMeley, Protecting Consumer Privacy and Information in the Age of the Internet of Things, 29 ANTITRUST ABA 71, 72 (2014).

105 「紐約時報近日一篇報導指出，購物商場的精準行銷，居然做到在一位父親發現女兒懷孕之前，就已經先分析出來。塔吉特（Target）是美國第二大百貨集團，紐約時報採訪其分析師Andrew Pole所做的報導中，分享了一個有趣案例。某位憤怒的父親衝進塔吉特要求與經理談話『我的女兒還是高中生，你們怎麼寄這種優惠券給她？』『你們是鼓勵她早點懷孕嗎？』店經理一頭霧水，經了解後發現，原來是塔吉特寄了一堆關於孕婦裝、育嬰家具及嬰兒圖片的優惠券給他女兒。店經理當場向該父親致歉，並在數日後再一次致電道歉。不過在第二次電話中，該位父親不好意思的表示，在與女兒深談後，發現女兒確實懷孕了。原來塔吉特針對懷孕消費者容易改變購物行為的關鍵時刻，精準投放育嬰相關廣告優惠」，今日新聞網站，http://www.nownews.com/n/2012/02/23/42676，造訪日期：2015年6月2日。

106 John P. Holdren et al., Big Data: A Technological Perspective, Executive Office of the President, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (last visited: 2015.06.12).

客製化搜尋引擎之功能下，將出現「過濾泡沫」（filter bubbles）現象，因爲Google之搜尋功能，讓個人都不知道已被Google過濾掉的選擇[107]，如此一來，不但個人自主受到壓抑，核心民主價值亦受到損害，由於被自動分類而困於邊緣化，也因爲自覺受到監控，公民論壇亦產生「寒蟬效應」（chilling effect）[108]。

3.差別待遇

大數據分析得以基於個人特質、偏好等來進行分類[109]，運用在商業上，最明顯的例子爲差別訂價，航空業者被公認爲最擅長差別訂價，同樣的服務或商品，卻有不同之訂價，消費者間自然出現贏家及輸家[110]。然而最可議之處在於往往消費者對於被分類而遭差別訂價毫無所悉，惟隱私的問題不只是何人蒐集該等資料，更在於該等資料是否得以利用，消費者對於知悉如何被分類及差別訂價上應有合理之期待[111]。

四、小　結

大數據對於隱私帶來之風險可能有四種：其一，蒐集，政府直接或從第三人無限制地取得、儲存有關資料主體之資料，甚至爲敏感性資料；其二，濫用，政府以不正當之方式使用或揭露該等資料；其三，匯集，政府匯聚各種不同種類之敏感性資料；其四，滋擾，即便是合法之刑事程序[112]。上開態樣或多或少顯現在各個領域，大數據時代確然有如一個新時代之翻轉，帶來新希望、新氣象，然而大數據時代對於隱私之影響絕對不只在維護治安、醫療及商業層面上，本文僅

---

107 ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK 25 (2012).

108 Jerome, *supra* note 1, at 220.

109 Tene & Polonetsky, *supra* note 90, at 355.

110 Jerome, *supra* note 1, at 229.

111 Raymond, *supra* note 97.

112 Jane R. Bambauer, The Lost Nuanc of Big Data Policing, 94 TEX. L. REV. 1, 12-16 (2015).

舉出影響較爲廣泛及深遠之面向者，然從中亦可觀察出，受益於大數據越大者，隱私所遭受之侵害亦可能越大。

肆、可能之對策

對於資料隱私之關注有兩個層面，其一，資料取得面向；其二，資料可能在儲存、傳送、使用上遭到揭露[113]，如何因應大數據時代下對於隱私權侵害潛在之影響，在近來逐漸獲得重視，有認爲應訴諸倫理，因該等科技並非自然存在，乃人類決定下之產物而影響人類之價值，必須確保該等科技所形塑的社會是吾人所要的[114]，倫理固爲人性自覺可貴之一面，然在欠缺強制性下，恐怕難以賦予隱私權適度之保護；亦有認爲應以資料主體之「同意」（consent）爲前提，以尊重自主性[115]，告知後同意本爲基本要件，然一旦同意是否即無置喙之餘地，僅有告知後同意之要件似尚不足夠；或有強調事後追懲對於隱私權造成侵害者[116]，相關民刑事追訴固有阻遏之效，然對於當事人隱私權之保障，恐尚失之於被動，本文認爲上開對策均有其功效，但亦有其不足之處，尤其是政府接近使用第三人資料庫之資料雖非必然出現問題，然應有合理之限制[117]，因應大數據時代下對於隱私權之保護，應有兩項要求，其一，發揮法律作爲規範、正當性基礎、防禦之功能[118]；其二，不但要求告知後同意，個人還應該擁有「退出」

113 MIN CHEN, SHIWEN MAOAND, YIN ZHANG & VICTOR CM LEUNG, BIG DATA: RELATED TECHNOLOGIES, CHALLENGES AND FUTURE PROSPECTS 85 (2014).

114 Richards & King, *supra* note 27, at 426.

115 Rothstein, *supra* note 9, at 431.

116 Dirk Helbing & Stefano Balietti, Big Data, Privacy, and Trusted Web: What Needs to Be Done, http://ssrn.com/abstract=2322082 (last visited: 2015.06.15).

117 Chris Jay Hoofnagle, Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, https://epic.org/privacy/choicepoint/cp_article.pdf (last visited: 2015.06.15).

118 Meg Leta Ambrose, Lessons from the Avalanche of Numbers: Big Data in Historical Perspective, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 201, 250 (2015).

（opting out）之權利[119]。

一、維護治安之管制：正當法律程序之適用

㈠大數據時代下之正當法律程序思維

大監控社會之到來早在數十年前即被預言，透過資訊科技之運用系統性地來監視人們的行爲或溝通被描述爲「資料監視」（dataveillance），從較早之攝錄影機至現今之「無人飛機」（airborne drone）及大量自動化蒐集消費者資訊，只要數位革命持續，各式各樣之監控工具將層出不窮[120]。

也因此，面臨科技時代對於正當法律程序採取新觀念，在保護自上個世紀以來之相關法律規範有其必要性[121]，大數據分析所做成自動化決定之過程可能侵害個人之自由及權利，而有構成適用增修條文第四條等正當法律程序之充足要件[122]，美國最高法院在過往亦均力求在容許執法機關利用新興科技及守護增修條文第四條之價值間取得平衡[123]，增修條文第四條之法理應作爲大數據時代對於隱私權造成影響之回應[124]。

㈡障礙——第三人理論

1. 理論面

「第三人理論」[125]（the third party doctrine）向被視爲研究增修

---

119 Nicolas P. Terry, Big Data Proxies and Health Privacy Exceptionalism, 21 HEALTH MATRIX 65, 97 (2014).

120 Shaun B. Spencer, The Surveillance Society and the Third-Party Privacy Problem, 65 S. C. L. REV. 373, 390 (2013).

121 Danielle Keats Citron, Technological Due Process, 85 WASH. U. L. REV. 1249, 1250 (2008).

122 *Id*. at 1281.

123 Koss, *supra* note 59, at 324.

124 Lon A. Berk, After Jones, The Deluge: The Fourth Amendment's Treatment of Information, Big Data and the Cloud, 14 J. HIGH TECH. L. 1, 9 (2014).

125 國內對於「第三人理論」之介紹，請參見李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，第115期，2010年6月，頁120-121。

條文第四條的學者之最憎[126]，第三人理論提出若個人係在故意之情況下將己身資料暴露予第三人，即不受增修條文第四條之保護，該理論假設個人業預見第三人會將該等資料提供給包含政府等他人之風險，而需自我承擔該等風險（assumes the risk）[127]，在該等理論下，並不問該等資料是否基於特定目的而揭露，僅論個人是否應該知悉該等資料將被其他團體接近使用[128]。

2.實務面

自一九七〇年代末期，美國最高法院開始出現認爲當個人將己身資料分享予第三人時，增修條文第四條並不提供保護，其說理基礎即來自於第三人理論[129]，在United States v. Miller案，法院認爲銀行客戶對於保管在銀行之財務紀錄欠缺隱私之「合理期待」（reasonable expectation），因爲該等紀錄乃由顧客自願提出，並以一般商業常規揭露予銀行職員[130]；而在Smith v. Maryland案，法院認爲個人對於所撥出之電話號碼並無隱私之合理期待，因個人知悉其必須將該等電話資料傳達予電話公司，無法懷有任何期待上揭電話號碼得成爲機密[131]。

3.批　評

美國最高法院大法官William Brennan、Thurgood Marshall、Potter Stewart針對前開案件提出不同意見書，Brennan提出個人對於其銀行紀錄應保有隱私之期待，Marshall則認爲即使電話使用人得以預見基

126 Orin S. Kerr, The Case for the Third-Party Doctrine, 107 MICH. L. REV. 561, 563 (2009).

127 Philip H. Marcus, A Fourth Amendment Gag Order — Upholding Third Party Searches at the Expense of First Amendment Freedom of Association Guarantees, 47 U. PITT. L. REV. 257, 276 (1985).

128 Matthew D. Lawless, The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection, 2007 UCLA J.L. & TECH. 2, 6 (2007).

129 Gabriel R. Schlabach, Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act, 67 STAN. L. REV. 677, 691 (2015).

130 *See* United States v. Miller, 425 U.S. 435, 438 (1976).

131 *See* Smith v. Maryland, 442 U.S. 735, 743 (1979).

於內部因素，電話公司將記錄其通訊之電話號碼，然並不表示個人期待該等資料將提供公眾，尤其是政府，身處當代社會之個人乃別無選擇而需揭露其資料予銀行及電話公司，Stewart並指出電話號碼並非無「內容」（content）之資料，其質疑會有任何人樂意使撥打之每通電話號碼任意散布[132]。至於學術界之批評則有兩個面向：

⑴理論錯誤之詮釋

第三人理論並未正確地適用隱私之合理期待理論，個人通常對於其銀行紀錄、電話通訊資料及其他掌握在第三人之資料具有隱私之期待[133]，該等期待不但普遍亦且合理[134]而所謂自我承擔風險之假設，乃因個人在現實世界並無任何選擇[135]，第三人理論基於不正確地理解隱私之概念，認爲隱私等同於完全之祕密[136]，隱私並不代表拒絕與他人分享資料，僅志願揭露資訊予特定人與公諸於世迥然有異，因隱私亦有程度之區分[137]。

⑵功能不當之擴張

第三人理論賦予政府之權利與自由、開放之社會有所扞格，增修條文第四條在保障無辜者，適用第三人理論給予警察過大之權力來侵擾無辜之民眾[138]，如任由第三人理論來支撐政府之監控行爲，增修條文第四條幾乎無法規制政府之監控，政府得以蒐集及匯聚任何數位檔

132 Schlabach, *supra* note 129, at 692.

133 Christopher Slobogin & Joseph E. Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society", 42 DUKE L.J. 727, 732 (1993); Gerald G. Ashdown, The Fourth Amendment and the "Legitimate Expectation of Privacy", 34 VAND. L. REV. 1289, 1315 (1981).

134 Kerr, *supra* note 126, at 571.

135 *Id*.

136 Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. 1083, 1086 (2002).

137 Sherry F. Colb, What is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 STAN. L. REV. 119, 122 (2002).

138 Arnold H. Loewy, The Fourth Amendment as a Device for Protecting the Innocent, 81 MICH. L. REV. 1229, 1229 (1983).

案而不受增修條文第四條之審查[139]。

從實證的觀點來看，民眾必然期待隱私受到保障，而認爲第三人理論之適用應予嚴格，聲稱民眾缺乏對己身資料之主觀隱私期待恐怕昧於現實[140]。

㈢契機——馬賽克理論

有鑒於上開實務與學術對於第三人理論之批判，不管立基於反制第三人理論或創設該理論之例外，「馬賽克理論」（mosaic theory）乃應運而生。

1. 理論面

馬賽克理論提出一個簡明的概念：「當明顯無害的片段資料被拼湊起來時，可能顯露出一幅有害之圖像」[141]，該理論認爲增修條文第四條所定義之「搜索」（search），不但指警察之單一行爲，亦包含整個偵查活動中一連串之作爲，就後者而言，警察個別之行爲有如馬賽克拼圖中之一塊，應將個別行爲組成之整個圖像放在增修條文第四條下來檢視，當警察個別之行爲均不足以達到須接受合憲性審查之門檻時，若將個別行爲組成之圖像進行分析，可能即構成增修條文第四條之搜索[142]。

2. 實務面

馬賽克理論最早在最高法院United States v. Maynard案被提出，該案認爲警察機關利用GPS定位系統，連續二十八日全天候不間斷地追

---

139 Joseph T. Thai, Is Data Mining Ever a Search under Justice Stevens's Fourth Amendment?, 74 FORDHAM L. REV. 1731, 1736 (2006).

140 Devin W. Ness, Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It, 31 CARDOZO ARTS & ENT L.J. 925, 955 (2013).

141 Jace C. Gatewood, District of Columbia Jones and the Mosaic Theory — In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory, 92 NEB. L. REV. 504, 523 (2014).

142 Steven M. Bellovin, When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning, 8 NYU J.L. & LIBERTY 556, 571 (2014).

蹤犯罪嫌疑人車輛之路徑，已侵害嫌疑人合理之隱私期待，因爲實際上沒有任何人可以如此鉅細靡遺地掌握他人一整個月之行蹤，即使個別行蹤屬於公開性質，但整體而言這些個別活動之集合也可能揭露嫌疑人不爲人知之私人生活圖像[143]，而在最高法院Uinted States v. Jones案，大法官Samuel Alito在協同意見書表示應審酌當事人隱私之合理期待是否已被長期之監控行爲所侵害[144]；而大法官Sonia Sotomayor之協同意見亦聚焦於增修條文第四條之權利應存在於個人公開活動之總和[145]。

*3.*運　用

密集之資料探勘及預測分析之使用正爲馬賽克理論之關注點，民眾應無懼於其生活之私人細節將遭致一點一滴之蒐集、儲存及分析[146]。將馬賽克理論套用在管制維護治安運用大數據上，在美國已有若干提議，其一，喬治華盛頓大學（George Washington University）法學院教授Orin S. Kerr所倡議修正「聯邦儲存通信監察法」（The Stored Communications Act, SCA）第二七〇三條，在政府自第三人處取得資料上架構出三階層的保護，中階層之保護即融合馬賽克理論，政府若自單一資料提供者取得累積超過七天之資料即應取得令狀[147]；其二，二〇〇九年美國司法部對於「資訊自由法」（The Freedom of Information Act, FOIA）制定之準則，即使當特定資料之片段不受保密、亦對國家安全無任何損害，然只要係該領域之專家點點滴滴匯聚充足之該等資料，即已形成全圖像，而應受到保護[148]。

---

143 Benjamin M. Ostrander, The Mosaic Theory and Fourth Amendment Law, 86 NOTRE DAME L. REV. 1733, 1743 (2011).

144 Gatewood, *supra* note 141, at 527.

145 *Id*. at 528.

146 Robert Sprague, Privacy Implications of Big Data and Predictive Analytics, http://www.alsb.org/wp-content/uploads/2015/01/NP-2014-Privacy-implications-of-big-data-Sprague.pdf (last visited: 2015.07.01).

147 Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1230 (2004).

148 H. Bryan Cunningham, Tiny Constables in the Mosaic: Modernizing Oversight of Surveillance in the Age of Big Data, 65 RUTGERS L. REV. 983, 992 (2013).

*4.*批　評

馬賽克理論企圖以總和評價，亦即將乍看之下個人未受隱私侵害之片段活動，以逐步加總顯現全貌之方式使隱私之利益浮現[149]，亦受到不少批評，對於馬賽克理論之批評主要來自於三方面：

⑴邏輯層面

馬賽克理論在邏輯上有其矛盾之處，因爲馬賽克理論意欲保護的是個別不具體的隱私合理期待，然個別不確定之零價值，總合起來仍爲零價值，假使前開個別活動均不具備隱私之合理期待，總合起來亦無即具備之空間[150]，該等理論實牴觸算術之基本原理[151]。

⑵執行層面

馬賽克理論嘗試在是否受保護之間劃出另一道界線，然該等任務恐怕相當艱鉅[152]，其一，劃定界線之標準爲何？馬賽克理論提供之標準並不明確[153]；其二，上揭個別行爲之本質及類型均不相同，如何加總以分析其合理性[154]？

㈣立法面向

第三人理論及馬賽克理論各有其利弊互現業如前述，馬賽克理論似亦無法取代第三人理論來解決政府自第三人取得個人資料之問題，威得恩大學（Widener University）法學院教授Stephen E. Henderson即提出在適用第三人理論時，應同時審酌下列要素：揭露之目的、資料

149 Jessica Gutierrez Alm, The Privacies Life: Automatic License Plate Recognition Is Unconstitutional under the Mosaic Theory of Fourth Amendment Privacy Law, 38 HAMLINE L. REV. 127, 142 (2014).

150 Monu Bedi, Social Networks, Government Surveillance, and the Mosaic Theory, 94 B. U. L. REV. 1809, 1838 (2014).

151 David C. Gray & Danielle Keats Citron, A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, 14 N. C. J. L. & TECH. 381, 398 (2013).

152 *Id*. at 409.

153 Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 MICH. L. REV. 311, 329 (2012).

154 *Id*.

之個人特質、資料之數量、政府之需求、變動之社會規範[155]，以求限縮該等理論之適用；而Kerr則認爲應由國會立法來處理新科技之隱私問題[156]。

事實上美國律師公會（American Bar Association）即認執法機關在從第三人團體諸如銀行、醫院及「網際網路服務業者」（Internet Service Provider, ISP）等蒐集、取得資料之規範向來受到忽視，乃自二〇〇六年起，起草提出「執法機關接近使用第三人資料規範」（ABA Standards for Criminal Justice Law Enforcement Access to Third Party Records, LEATPR Standards）[157]，於二〇一三年已修訂至第三版，上開規範乃規制政府機關由第三人處之資料取得證據來使用於偵查、調查或預防犯罪[158]。該等規範並不挑戰前開第三人理論[159]，其最核心之立法邏輯在於隱私之等級、資料之類型化與接近使用該等資料要件寬嚴之交互關係，並與增修條文第四條之法理、刑事司法程序業已運作良久之「關聯性」（relevancy）、「合理懷疑」（reasonable suspicious）、「相當事由」（probable cause）標準互爲搭配輝映[160]。

---

155 Stephen E. Henderson, Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too, 34 PEPP. L. REV. 975, 989 (2007).

156 Kerr, *supra* note 153, at 350.

157 「執法機關接近使用第三人資料規範」（ABA Standards for Criminal Justice Law Enforcement Access to Third Party Records）共分為6章：第1章為定義；第2章為通則；第3章為資料及保護之類型化；第4章為接近使用資料，包含授權使用之類型及接近使用之要件等；第5章為資料之保存及揭露；第6章為罰則，規定可謂鉅細靡遺，然限於篇幅，本文爰不為詳細介紹，請參見ABA Standards for Criminal Justice Law Enforcement Access to Third Party Records, http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf (last visited: 2015.06.29).

158 Stephen E. Henderson, Our Records Panopticon and the American Bar Association Standards for Criminal Justice, 66 OKLA. L. REV. 699, 712 (2014).

159 David C. Gray, Law Enforcement Access to Third Party Records: Critical Perspectives from a Technology — Centered Approach to Quantitative Privacy, 66 OKLA. L. REV. 919, 932 (2014).

160 Ferguson, *supra* note 49, at 844.

LEATPR在豐富審酌之因素、類型化之保護及適度限縮適用第三人理論上堪足以提供國會就該等事項富具價值之指引[161]。

㈤通知、陳述意見暨接受公正裁決

1.通　知

維護治安層面運用大數據可能有錯誤資料及誤判之影響業如前述，也因此有必要思考在上開預測及決策過程中，是否賦予隱私可能遭受損害者機會來介入該等過程，該等機會可以是某種形式之通知，所揭露者不只是政府所爲預測之類型，還應包括資料之來源，以前述之犯罪熱區爲例，應告知居住或工作於該區民眾，係使用何種預測分析及公共紀錄來得出及劃定熱區之範圍[162]。

2.陳述意見

在前開通知程序後，緊接著須思考的爲民眾如何對於預測及決策過程提出質疑，因此民眾應有陳述意見之機會，甚至在必要時要求更正錯誤之資料，這當中包含資料之輸入及該等分析適用之運算，如此一來，才能符合正當程序之要求：決定之正確性、公平之展現、可預測性、透明度、合理性[163]。

3.接受公正裁決

大數據常讓人產生迷思即該等產出應無人爲偏好（bias）而純然客觀[164]，然如前述，由於烙印而可能使治安預測蒙上有色眼鏡，因此，可能應考量成立中立之仲裁機關，以對於民眾前開陳述意見進行調查，檢驗整個預測及決策過程[165]。

---

161 Susan Freiwald, How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records, 66 OKLA. L. REV. 875, 908 (2014).

162 Crawford & Schultz, *supra* note 10, at 125-26.

163 *Id*. at 127.

164 Boyd & Crawford, *supra* note 11, at 667.

165 Crawford & Schultz, *supra* note 10, at 127.

二、醫療實務之安全閥：健康隱私特殊論

㈠健康隱私特殊論

在美國，政策制定者、病患及醫生大多接受「健康隱私特殊論」（health privacy exceptionalism），亦即醫療資料較諸其他類型之資料應受到更高程度之保護，這種特殊性來自於自主之核心價值，由於資料私密性之本質，是否同意他人近用該等資料與否應屬基本權利，在醫療照護領域，當個人交出其資料以求獲得更好之醫療，係基於該等資料保密性之信賴及承諾，如他人未經授權近用，則已侵害要求個人保密之權利及隱私，這種特殊論的模式更爲當代醫療身分遭竊取現象之增長所強化[166]。

在上開理論下，催生了一九九六年之HIPAA，後來於二〇〇九年又加重違法之處罰而修法爲「經濟暨臨床健康資訊科技法」（The Health Information Technology for Economic and Clinical Health Act, HITECH），HIPAA之隱私規則鉅細靡遺地規範了個人資訊之限制使用、取得、更正及當事人同意等，並臚列相關特殊規定，例如：最小必要原則、去識別化等[167]。HIPAA在健康照護提供者間促進隱私文化[168]。

㈡再檢討

1. 規範仍不足

HIPAA之隱私規則規定在揭露當事人醫療資訊予第三人時必須取得當事人同意，然受規範者並不涵蓋政府機關及資料庫經營者，恐有規範之漏洞[169]。其二，HIPAA僅保護個人可識別之健康資訊，去識別

---

166 Terry, *supra* note 88, at 401.

167 關於HIPAA國內文獻之詳細介紹請參見楊智傑，美國醫療資訊保護法規之初探——以HIPAA/HITECH之隱私規則與資安規則為中心，軍法專刊，第60卷第5期，2014年10月，頁83-100。

168 Terry, *supra* note 88, at 402.

169 Hoffman, *supra* note 93.

化之資訊即不在保護之範圍，然如係使用再識別化之資訊呢？此部分之保護亦有待加強[170]。

2.部門導向之質疑

HIPAA在形式上爲「部門導向」（sector-based），亦即僅適用於健康照護「被涵蓋之機構」（covered entities）[171]，然原受HIPAA保護之資料亦可能轉換至未受保護或低度保護之區域，該等相關規範在未來應朝向放棄特定產業限制之思維方向，HITECH之立法即在非健康照護之領域亦能發揮部分保護健康資料之功能，其規定之「違反規定通知」（breach notification）亦適用於「個人健康紀錄」（Personal health record, PHR）提供者，新的隱私規則應普及適用於所有部門方能持續處理未經授權而揭露資料之問題[172]。

三、商業世界之緩衝：保障消費者隱私實定法化暨被遺忘的權利

㈠保障消費者隱私實定法化

1.實定法化

二〇一二年二月美國政府提出起草「消費者隱私權法案」（Consumer Privacy Bill of Rights, CPBR），企求規範個人資料之商業上利用及彰顯隱私價值，該法案可區分爲兩大面向：資料持有人、分析者、利用人之責任及消費者之授權[173]。

在責任面向包含幾個要素，其一，尊重資料主體：消費者有權期待私人企業在蒐集、利用、揭露個人資料之方式必須與消費者提供該等資料之背景相符；其二，蒐集之限制：消費者有權合理限制私人企業蒐集及保存其個人資料；其三，安全性：消費者有權要求其個人資料之處理受到保護；其四，課責性：消費者有權要求私人企業處理其

170 *Id*.
171 45 C. F. R. § 160.103 (2012).
172 Terry, *supra* note 88, at 407.
173 Holdren et al., *supra* note 106.

個人資料必須採取適當之措施以確保遵循消費者隱私權法案[174]。

在消費者授權面向亦包含幾個要素，其一，個人掌控：消費者有權瞭解何人蒐集其資料其該等資料如何被利用；其二，透明度：消費者得以輕易地瞭解及近用隱私安全之資訊；其三，近用性及正確性：消費者有權要求查詢及更正其個人資料[175]。

然而伴隨大數據之變動性科技，上開消費者隱私權法案之有效可操作性出現危機，二〇一四年美國總統科技顧問委員會（President's Council of Advisors on Science and Technology, PCAST）就科技觀點作出大數據與隱私之報告，提出若干進一步之建議，其一，資料主體尊重之範圍應予擴大：在該等個人資料已演變成不必然由消費者本人提供之背景下，利用該等資料應具備正當之目的，更應確保其利用不致造成對消費者負面之影響；其二，資料之蒐集不但應有所限制，更應盡量藉由科技達到去識別化；其三，個人資料不僅包含蒐集所得者，還包括資料分析之結果，消費者應可期待得以要求證實及更正分析之結果，並採取行動來降低因不正確之資料而造成對消費者負面影響之風險；舉證之責任應由掌握大數據之商業實體負擔[176]。

2.執法機關

法案之執行決定成效之良窳，上開PCAST提出之報告特別建議國會賦予聯邦貿易委員會（Federal Trade Commission, FTC）職權來執行消費者隱私權法案，一方面企業體對於其保障隱私之責任有清楚之準則；一方面由特定執法機關來捍衛隱私權亦裨益消費者[177]。

㈡被遺忘的權利

1.源　起

因應大數據時代對於隱私之影響另一個可能之對策即創設「被遺

174 *Id.*
175 *Id.*
176 *Id.*
177 *Id.*

忘的權利」（right to be forgotton）[178]，大數據根本性地改變了以往搜尋及擷取資料之方式，卻使個人資料之暴露超乎想像，當數位記憶越趨普及及盛行，被遺忘的權利無疑地成爲處理網路上各式問題強有力之武器[179]。蒂爾堡大學（Tilburg University）法學院教授Bert-Jaap Koops即指出我們身處大數據時代，大數據之所以爲「大」乃繫諸於時間及空間不斷地累積，更重要的是，這些資料不只由本人主動提供，更來自於其他人蒐集及散布而形成，質言之，我們的微量數位紀錄已快速成長爲數位足跡，使得形塑被遺忘的權利格外重要[180]。事實上，不只歐盟，即連對於隱私權之定位迥異於歐盟之美國[181]，在前開大數據與隱私之報告中，亦認爲當資料已經不再存有價值時，不論爲何類資料都應被刪除[182]。

在大數據時代下，個人資料在不同之時間、地點被匯集，這些以「皆位元組」（zettabytes）被傳遞之資料不只是由人們主動創造，更來自於其他人在蒐集或散布該等資料所留下之痕跡，而後者在今日之發展可謂倍增於前者，益見形塑被遺忘的權利其重要性[183]，被遺忘的權利得使本人掌控其個人資料並加諸資料管理者其責任[184]，當然，面

178 Michael Birnhack, Reverse Engineering Informational Privacy Law, 15 YALE J.L. & TECH. 24, 67 (2013).

179 Zhile He, Daoli Huang & Yunting Lei, Legislation of "Right to Be Forgotten" in Big Data Environment., http://www.atlantis-press.com/php/pub.php?publication=icssr-14&frame=http%3A//www.atlantis-press.com/php/paper-details.php%3Fid%3D11865 (last visited: 2016.01.27).

180 Bert-Jaap Koops, Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice, http://ssrn.com/abstract=1986719 (last visited: 2015.07.01).

181 美國與歐盟間對於隱私權定位不同之比較法觀察，國內文獻請參考許炳華，被遺忘的權利：比較法之觀察，東吳法律學報，第27卷第1期，2015年7月，頁147-154。

182 Holdren et al., *supra* note 106.

183 Koops, *supra* note 180.

184 Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, http://lsr.nellco.org/cgi/viewcontent.cgi?article=1359&context=nyu_plltwp (last visited: 2015.07.01).

對快速之科技變化，投注予隱私關注之最佳途徑仍爲立法，而非僅觀念之提出[185]。

2. 正當性基礎

被遺忘的權利被視爲一種安全閥來處理無形之隱私爭議，在今天之資訊社會，事實上很難預測個人資料遭受使用後所有可能之負面效應，即使得以預見某些後果，所呈現之狀況亦屬抽象、模糊及不確定，之所以抽象的原因在於對於隱私之傷害時常涵蓋社會、心理及其他議題，之所以模糊的原因則在於該等後果未必馬上浮現，而之所以不確定乃因可能最終不會發生或以不可預期之方式發生，結果，縱然個人睿智地理解其資料遭受利用可能之負面效果，卻無充足之能力得以改變其行爲模式[186]。

又「個人資料」其概念本身雖屬籠統，卻不應僅視爲統計上之名詞，隨著時間轉換，資料用途之不同，該等資料可能隨時與本人進行連結或脫鉤，也因此，被遺忘的權利在動態之時空下得以提供個人有效利用之途徑，因其不斷變動之目的來重新評價該等資料之使用，將得以強化個人對於其識別性（identify）之掌控，簡而言之，從政策之觀點觀之，被遺忘的權利將帶來諸多利益[187]。

3. 內　涵

被遺忘的權利可能包含兩個面向：「遺忘的權利」（right to oblivion）及「刪除的權利」（right to erasure），遺忘的權利在免於受到尊嚴、人格、聲譽、認同之傷害，但與其他基本權利可能有所衝突，然而該等權利之實現並不難，因爲使用人可將其希望公眾忘記之資料運用與搜尋相同之技術來予以下架；刪除的權利則爲一種技術性

185 Stephanie Segovia, Privacy: An Issue of Priority, 11 HASTINGS BUS. L.J. 193, 209 (2015).

186 Hans Graux, Jef Ausloos & Peggy Valcke, The Right to Be Forgotten in the Internet Era, 17 Interdisciplinary Centre for Law and ICT, http://ssrn.com/abstract=2174896 (last visited: 2015.10.13).

187 *Id*.

的權利，允許將已經揭露之資料移除[188]。

在大數據時代下被遺忘的權利應可能有三種態樣：使得資料在特定時間後得以要求刪除之權利、「清盤」（clean plate）的權利、要求僅能連結現在資料的權利[189]，Koops將上開第一及第二種權利進行比較[190]：

	特定時間後得以要求刪除之權利	清盤之權利
客　體	資料刪除	封鎖資料之使用
類　型	資料主體之權利	資料處理者之義務
焦　點	資料蒐集及儲存	使用資料以決策
範　圍	一般	特定
法律領域	資料保護法律	特定部門法律

而上開第二種及第三種之權利頗爲相近，重點均放在如可能受到損害，個人過去之資料不得永遠都能被連結獲得[191]，惟既然都強調個人對其過去資料適當之控制，Koops復未進一步將第二種及第三種之權利進行比較論述，在區隔之界線未明確化下，是否有必要逕區分爲兩種分類，實屬有疑，似以清盤的權利涵蓋要求僅能連結現在資料的權利即可。

4. 司法層面

二〇一四年五月十三日歐盟法院（The European Court of Justice, ECJ）大法庭（Grand Chamber）作出Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González案之判決，其案例事實爲西班牙人Mario Costeja González於二〇〇九年十一月向La Vanguardia日報客訴指出只要將其名字輸入Google搜尋引擎，

188 Meg Leta Ambrose & Jef Ausloos, The Right to Be Forgotten Across the Pond, 3 J. INFO. POL'Y 1, 14 (2013).
189 Koops, *supra* note 180.
190 *Id*. at 265.
191 *Id*.

即會連結該日報曾刊登其因積欠社會保險債務而遭強制拍賣財產之公告，然該等強制拍賣事項已結案多年，González要求將與其相關之資料移除遭拒而提起訴訟[192]。

歐盟法院於判決中指出依據「歐盟個人資料保護指令」（Data Protection Directive, 95/46/EC）第七條第一項第(f)款之規定[193]，在考量到網路使用人近用資料之正當利益，應力求該等利益與資料主體基本權利間合理之平衡，尤其是隱私權及個人資料保護之權利，該等平衡在特定個案必須植基於系爭資料之本質、資料主體隱私生活之敏感性及資料主體在公眾生活所扮演之角色[194]。歐盟個人資料保護指令是否賦予資料主體得要求在特定時間後與其私人有關係之資料被遺忘及至該網頁間之連結刪除，就此應採肯定之態度，依上揭指令第十二條第一項第(b)款之規定[195]，即使最初系爭資料正確且係合法地被處理，只要該等資料在後來已不正確、不再有何相關或逾越先前處理之目的，即與歐盟個人資料保護指令扞格，再依同指令第十四條第一項第(a)款之規定[196]，當資料主體提出反對，即應特別檢驗系爭資料是否與

192 *See* Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Court of Justice of the European Union Press Release, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (last visited: 2015.07.01).

193 原文為"Member States shall provide that personal data may be processed only if: (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

194 *See* Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, *supra* note 192.

195 原文為"Member States shall guarantee every data subject the right to obtain from the controller: (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."

196 原文為" Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him,

其個人相關，是否以其姓名搜尋可得，若答案為肯定，包含該等資料之網頁連結即必須去除，除非具有特別之事由，例如資料主體在公眾生活扮演之角色，以正當化公眾在近用系爭資料具有優勢之利益[197]，故資料主體應得以依歐盟個人資料保護指令前開規定要求將系爭資料之連結移除[198]。

5. 立法層面

被遺忘的權利在歐盟新起草之「保護個人有關個人資料處理及自由流通規章（一般性資料保護規章）」（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）被承認並納入，該規章於二〇一三年六月進入歐洲議會（European Parliament）、理事會（European Council）、執委會（European Commission）的三方協商，並於同年十月二十一日歐洲議會公民、司法與內政委員會（Committee on Civil Liberties, Justice and Home Affairs）審議通過，二〇一六年六月二十七日復將條文進行修正，當中第十七條規定：「資料主體在下列情形有權要求資料控制者立即刪除與其相關之個人資料：

a. 資料提供蒐集或處理之目的已不存在。
b. 資料主體撤銷同意或資料處理之法律依據已不存在。
c. 資料主體依第21條(1)之規定反對其個人資料之處理。
d. 資料遭非法處理者。
e. 依據歐盟或會員國法律之義務，該個人資料必須被刪除。

---

save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data."

197 *See* Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, *supra* note 192.

198 *Id*.

f. 遭蒐集之個人資料乃有關資訊社會服務提供之如第8條(1)兒童之情況」[199]。

四、小　結

個人隱私爲基本權利，且應包含防止其個人資料遭受蒐集及散布之權能[200]，本文針對大數據時代下隱私權之保護在維護治安之管制上提出正當法律程序之適用，並將論述焦點放在增修條文第四條，因由前所列舉大數據時代對於隱私之影響層面，以政府取得資料可能產生之危害爲鉅，若將該等取得適度援用增修條文第四條之法理加以規制，對於人民之隱私權當有最基礎之保障。在醫療面向，希望提出健康隱私特殊論爲安全閥，並以美國之HIPAA進行再檢討。另在商業面向則希冀消費者隱私保護實定法化及創設被遺忘的權利，以發揮主動保護之功能，然就如同資訊倫理、告知後同意及事後追懲等機制，亦均有其盲點及尚待審酌之處。就政府自第三人處取得資料方面，美國最高法院在過往三十年來均傾向支持第三人理論[201]，換言之，掌握於

199 原文為"1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

200 Madelaine Virginia Ford, Mosaic Theory and the Fourth Amendment: How. Jones Can Save Privacy in the Fact of Evolving Technology, 19 AM. U. J. GENDER SOC. POL'Y & L. 1351, 1370 (2011).

201 我國司法實務就個人資料之保障厥為重要者為司法院釋字第603號解釋，其謂：「……國家基於特定重大公益之目的而有大規模蒐集、錄存人民指紋、並

第三人處之資料並不受增修條文第四條之保護，然而增修條文第四條與科技間向來有著流動之關係，科技越形進步，司法實務及學術界越奮力於加強對於隱私之保護，上開馬賽克理論對於增修條文第四條之捍衛提供了其正當性基礎以因應發展中之科技，前揭Jones案之協同意見更試圖取回新科技強大監控與增修條文第四條其間之平衡，惟儘管立意極佳，由於馬賽克理論引發前開嶄新及困難之問題，無異開啓潘朵拉的盒子，則此部分要求全面受到增修條文第四條之審查，似還有待理論更臻成熟及標準更形明確之餘地。而HIPAA則還有檢討空間，且必須解決過度部門導向之問題。另如美國消費者隱私權法案尚停留於草案階段，實定法之路還有待努力。至於被遺忘的權利之提出，自有其前瞻及崇高理想之處[202]，惟先不論其對於未來搜索引擎及伺服器如何經營及運作之影響，被遺忘的權利在現階段實尚難認屬普世之價值，美國之司法實務告訴我們，即使該國法律保護隱私，在法庭上，隱私往往爲另一所謂更高價值之利益——言論自由所凌駕[203]，被遺忘

有建立資料庫儲存之必要者，則應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。」參見司法院大法官解釋檢索系統，http://www.judicial.gov.tw/constitutionalcourt/p03.asp，造訪日期：2015年10月15日。然本號解釋著重於「國家蒐集人民之資料」，尚未涉及前開美國司法實務面對第三人理論之困境。

202 我國學者李震山早於1997年即富具遠見地提出「資訊自決權」之概念，並定義為：「係指每個人基本上有權自行決定，是否將其個人基本資料交付與供利用」，李震山，論資訊自決權，載現代國家與憲法——李鴻禧教授六秩華誕祝壽論文集，1997年7月，頁710，然依該等定義，是否得以涵蓋保障至個人同意交付資料後，要求其資料刪除或被遺忘之權利，尚屬有疑，可能因當時之科技環境尚不盡然能預見前述「被遺忘的權利」之態樣，惜至2005年之司法院釋字第603號解釋，雖已意識個人資訊隱私權之重要性，而謂：「……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……」，同前註，然當中之「控制權」是否能解釋該等保障及於被遺忘的權利，亦不明確，若對照後述之行政法院判決，更形悲觀。

203 Jasmine McNealy, The Emerging Conflict Between Newsworthiness and the Right to Be Forgotten, 39 N. KY. L. REV. 119, 132 (2012).

的權利在美國似乎尚無更多發展之空間[204]；即連前開歐盟法院Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González案，似乎重點亦僅放在承認資料主體得要求在特定時間後與其私人有關係之資料被遺忘及至該網頁間之連結刪除，則上揭一般性資料保護規章所規定得以要求終局性刪除與其相關之個人資料之超前立法，恐怕在完全保障個人隱私及維持大數據資料庫完整資料分析之正確性以帶來諸多利益之間，其間價值取捨似尚有衡量之空間[205]。

伍、反思我國

一、維護治安

我國治安主管機關對於將大數據運用在維護治安上似趨之若鶩[206]，而犯罪防治學界亦不遑多讓[207]，此部分會產生上述之影響應可

---

204 Franz Werro, The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash, http://ssrn.com/abstract=1401357 (last visited: 2015.07.08).

205 此亦為本文暫時僅在商業領域進行被遺忘的權利之論述及探討之理，被遺忘的權利確實可能適用在各個領域，然因治安資料庫所涉及者可能為治安之良窳，醫療資料庫所涉及者可能為病患之生命、身體及醫學研究，兩者均具備濃厚之公共利益，資料是否完整正確，實動一髮而牽全身，至於商業領域，原則上所涉及者僅為私益，容有先予以進行嘗試之空間。

206 「運用大數據分析毒品相關數據　查緝更具著力點」，行政院網站，http://www.ey.gov.tw/News_Content2.aspx?n=F8BAEBE9491FC830&sms=99606AC2FCD53A3A&s=94995E85EA0261E5，造訪日期：2016年2月3日；「科技建警　警政署治安策略研討強調大數據」，中時電子報網站，http://www.chinatimes.com/realtimenews/20150921004898-260402，造訪日期：2016年2月3日。

207 江守寰，以大數據探勘技術分析「視覺化管理」在監視錄影系統之運用——臺中市政府警察局為例，犯罪學期刊，第18卷第2期，2016年1月，頁1-29；甘炎民、郭士豪、黃冠豪、李承龍，大數據資料系統分析運用在偵查實務之研究，警察通識叢刊，第5期，2015年11月，頁140-159；刑事雙月刊第69期以「辦案新思維——大數據於犯罪偵防上的運用」為主題，探討治安維護工作上，警用資料庫於犯罪偵防上運用及發展趨勢，並利用大數據分析技術，掌握問題核心、犯罪模式及犯罪脈動，研擬有效偵防對策，適時提供各警察機關分享運用，提高破案率為議題，刑事雙月刊網站，https://www.cib.gov.tw/Upload/

想見，重點在於我國對於第三人理論及馬賽克理論之回應，遍尋我國相關法令及實務見解，當然並無該二理論之明文，然通訊保障及監察法第二十九條第三款[208]，隱然似乎有「風險自我承擔」之痕跡，而另一個值得關注的為林子儀大法官在大法官釋字第六〇三號協同意見書強調：「……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。……」[209]，前開馬賽克理論之體現躍然其中，是爾後之實務判決若能以之來作為相關案件「侵害手段」要件之審酌，不失為良性之發展。

另個人資料保護法可謂我國資料保護之普通法，適用在維護治安之領域，尤應格遵個人資料保護法上最重要之原則，亦即「目的拘束原則」[210]，學者譽為個人資料保護法之帝王條款，其內涵包括蒐集、處理及利用個資必須在公務機關法定職掌範圍內，且屬於職權必要範圍內，不可以過度蒐集，且該蒐集、處理及利用目的須具有明確性，令人民可以事先理解，可預見將來如何被利用，並可以受司法審查[211]，若能善用此條款作為維護治安之前提[212]，當可與正當法律程序

Files/5400.pdf，造訪日期：2016年2月3日。

208 我國通訊保障及監察法第29條第3款規定：「監察他人之通訊，而有下列情形之一者，不罰：三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

209 司法院釋字第234號解釋，司法院大法官解釋檢索系統：http://www.judicial.gov.tw/constitutionalcourt/p03_01.asp?expno=234，造訪日期：2016年2月3日。

210 我國個人資料保護法第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，依誠實及信用方法為之，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。」

211 李惠宗，個人資料保護法上的帝王條款——目的拘束原則，法令月刊，第64卷第1期，2013年1月，頁61。

之適用同爲管制之利器。

二、醫　療

我國之醫療水準向在水平之上，亦不會自外於大數據時代之外[213]，然而醫療、健康隱私在我國之定位如何呢？相較於美國前開所揭櫫之健康隱私特殊論，我國在二〇一五年十二月三十日修正之個人資料保護法第六條規定：「有關病歷、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必要範圍內，且事前或事後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，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、爲協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意

212 當然從犯罪偵查的觀點可能會有不同看法，參見田炎欣，警察偵查犯罪侵害個人資料保護法「目的拘束原則」之探討，台灣法學雜誌，第257期，2014年10月，頁93。

213 「以互聯網和大數據研究為發展特色的台北醫學大學管理學院，舉辦『2015大數據論壇——Taiwan』，兩天的論壇中邀集了數十位產官學界專家，共同探討大數據的創新運用，結論之一為台灣在大數據的發展上，軟體和硬體都不是問題，如何應用大數據提供更安全的醫療照護，或更多創新的醫療應用，是醫療大數據關注的重點」，東森新聞雲網站，http://www.ettoday.net/news/20150816/550489.htm，造訪日期：2016年2月3日；「在現今醫療資訊高度發展的台灣，看診程序從網路掛號、候診順序、診間病歷調閱、醫師醫令、處方開立、放射影像存取、檢查檢驗資料儲存等，無數的數據資訊便在醫院中傳遞、交換、儲存。同時大多數的生理檢驗資訊在你回診時得以從電子病歷中檢索，這些我們認為理所當然的資訊處理，在台灣我們只要花費少許的時間如一個早上便完成了，而這一切正是仰賴醫學資訊分析與醫療大數據的交換處理」，中時電子報，http://www.chinatimes.com/newspapers/20160107000162-260205，造訪日期：2016年2月3日。

願者，不在此限。依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。」該條文規範「敏感性資料」之蒐集、處理與利用，當屬正面呼應上開美國之健康隱私特殊論[214]，惟有學者認為法條中將「醫療」、「病歷」與「健康檢查」並列為個人資料並不妥適，實得參照外國之立法例，逕以「健康」取代三者即可[215]，而本條文最大之困境恐怕還是在於同法第五十六條第一項規定施行日期尚需由行政院另定之[216]。另我國亦未如美國針對醫療資訊隱私而有HIPAA、HITECH般之專門立法[217]，在考量國情下，曾有「醫療資訊安全與隱私保護指導綱領草案」之提出[218]，惜亦尚停留於紙上談兵之階段，另當然部門性立法所可能遭致之批評業如前述，然在一體適用性之立法無法施行，個別部門性之立法亦闕如之情況下，我國

214 其立法理由謂：「……按個人資料中有部分資料性質較為特殊或具敏感性，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為嚴格，須符合所列要件，始得為之，以加強保護個人之隱私權益。」

215 蕭奕弘，論個人資料保護法之法制性問題，成大法學，第23期，2012年6月，頁168。

216 之所以謂困境乃因該法「被視為『全世界最嚴格的個資法』，一上路，就面臨修法命運。這部保護個人隱私的最高憲法，原本立意良善，卻為何窒礙難行？個資法該怎麼修，才能符合社會期待？……而個資法沒有明定主管機關，亦是一大問題」，天下雜誌網站，http://www.cw.com.tw/article/article.action?id=5046294，造訪日期：2016年6月21日。

217 事實上行政院衛生署（現改制為衛生福利部）曾委託研究「確立及推廣醫療資訊安全與隱私保護之政策」，當中考量導入HIPAA，衛生福利部網站，http://emr.mohw.gov.tw/doc/93%E5%B9%B4%E5%BB%A0%E5%95%86%E5%BB%BA%E8%AD%B0%E6%9B%B8930722.pdf，造訪日期：2016年2月4日。

218 當中揭櫫有九大原則包含最小需要原則、直接取得原則、尊重及告知原則、公平正義原則、依法原則、合理範圍內保障最大安全原則、病患權利保障原則、未經同意不可揭露原則、生命權及公共利益保障原則。

醫療、健康隱私之保障令人擔憂。

三、商　業

我國企業亦嘗試追趕大數據世紀之腳步[219]，然對於消費者之隱私，我國並未有前開美國消費者隱私權法案之芻議，消費者保護之主管機關並非公平交易委員會，而係行政院消費者保護會及各縣市政府之消費者保護官，然消費者隱私之保護並未見諸於消費者保護法，自無執法之權責。而就被遺忘的權利，我國立法層面甚爲保守，雖有認我國個人資料保護法第二十條第二項[220]已有個人同意之「退出權」概念[221]，然實與本文上開所述被遺忘的權利尚有若干差距，至司法層面亦難謂有何前瞻之處[222]。

---

219 「台灣的銀行採用了一項能夠支援地理資訊視覺化的大數據分析工具，藉以進行ATM設置地點與銀聯卡刷卡交易量之間的關聯分析也利用類似分析工具，旨在進行分行設立的分析，透過地理資訊找出所有金融機構交易最高的地區，藉以確認是否具備設點潛力。」企業IT網站，http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?cnlid=13&packageid=10096&id=0000456896_LR375G75L1SBNE5LK56I8&cat=50，造訪日期：2016年2月3日；「我國已有皮膚保養業者利用系統分析消費者消費行為，不但找到自身產品定位價格，連擴展商圈時，也可以利用大數據分析，找到對的地段開設分店，並鎖定主力消費客群」，聯合新聞網，http://udn.com/news/story/7238/1349270，造訪日期：2016年2月3日。

220 我國個人資料保護法第20條第2項規定：「非公務機關依項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。」

221 翁清坤，告知後同意與消費者個人資料之保護，臺北大學法學論叢，第87期，2013年9月，頁293。

222 我國台北高等行政法院102年度訴字第36號判決乃有關原告民眾拒絕被告衛生福利部中央健康保險署將其所蒐集之民眾個人健保資料釋出給第三者，用於健保相關業務以外之目的的爭議，其謂：「……基於個人資訊隱私權並非絕對權利，立法者自得在保障個人資料之隱私，以及合理利用個人資料之平衡考量下，限制個人資訊隱私權。因此，原告雖主張資訊自主權有事前與事後控制權，然就權利本質而言，兩者應屬一體之兩面，法律既已限制事前同意權，亦應同時限制事後排除權，否則被告得不經個人同意利用其資料，個人卻能任意行使排除權，則法律所欲達到合理利用個人資料、增進公共利益之目的顯無以達成，如此一來，個人資訊自決權反成絕對權利，當非立法本質，是原告主張其有『事後退出權』乙節，尚無依據。……」，參見司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm，造訪日期：2015年10月13日。判決中

四、小　結

大數據時代下隱私權保護之可能對策，就我國現況而言，業歷經幾次修法之個人資料保護法應屬可馬上在各領域發揮管制功能之法制，然相較之下，歐盟執行委員會在二〇〇四年即設立專屬及獨立之「歐洲資料保護監督官」（European Data Protection Supervisor, EDPS），來確保歐盟所屬機構及會員國在處理個人資料時尊重個人隱私[223、224]，是我國建構專門保障個人資訊隱私之獨立機關，應屬可以先行考慮之方向，順著這個脈絡，針對上開個人資料保護法第六條確實窒礙難行之處再進行如何之調整，以求該敏感性個資條款能盡早施行而發揮其功能，是高舉個人資料保護法之「目的拘束原則」爲帝王條款以在各領域成爲上位階之指導原則，再結合正當法律程序之思惟，應能在維護治安上發揮管制之功能。至於就醫療資訊隱私的部分是否如美國專門立法？或在消費者保護法增加保障消費者隱私之條款則爲爲下一階段可以討論之重點。而被遺忘的權利其開創性之理念自

否定個人對其資料之事後退出權，隱隱透露不採被遺忘的權利之概念，僅以「合理利用個人資料」為由，即置個人隱私權保護為次要，該等案例事實對於個人資料之利用是否屬於「合理」，固有討論之空間，然不無以國家本位之立場，而要求人民基本權利必須退讓之意味，後最高行政法院103年度判字第600號判決將上開判決廢棄，而謂：「……公務機關對於個人資料之利用，原則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……並應注意其手段有助於目的之達成，選擇對人民權益損害最少之方式，對人民權益造成之損害不得與欲達成目的之利益顯失衡平，且其利用不得逾越特定目的之必要範圍，應與蒐集之目的具有正當合理之關聯……」參見司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm，造訪日期：2015年10月13日。然對於個人得以行使如何之權利並未多所著墨，後續發展還有待觀察，相較於歐盟前開Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González案之精神，尚未見有何前瞻之處。

223 歐盟網站，http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm，造訪日期：2016年6月22日。

224 我國學者范姜真媺亦介紹日本個資法現行之監督機制，而倡言建立獨立機關監督個資法施行之必要性，參見范姜真媺，日本個人編號法對我國之借鏡——以個人資料保護監督機制之建立為主，東吳法律學報，第26卷第2期，2014年10月，頁1-12。

有足資參考之處，然即連走在最前端之歐盟直至今年度仍在進行修法，美國亦因背後長久文化及哲學思惟之差異下，尚存觀望態度，審酌我國在立法及司法層面仍有相當差距之背景，是否即驟然予以全盤採納，本文則尚持保留之觀點。

陸、結　語

隱私爲重要之人類價值，科技之進步固然危及個人隱私，卻也是反思如何加強保障隱私之契機，就如同其他新興科技，大數據亦呈現引領人類進入嶄新之發現及創造世紀的高度可能性，然而，在我們每天的日常生活，大家均合理地期待，即便自己參與的是公開活動，個人還是都能保持某種程度之隱密性，不僅是我們希冀該等細節屬於個人所有，更在於不欲任何人偷偷地潛進個人生活中，大數據使得隱私保障之問題更爲艱鉅及重要，然隱私權及透過政府監控達到安全需求等諸多利益之間必須求其平衡，大數據時代究爲隱私之死亡或爲重生，恐怕還端視如何因應，對於隱私權保護之理論，從合理隱私期待來作爲基準，自必須強調正當法律程序之適用，另從親密關係自治理論觀之，則有提出健康隱私特殊論之必要[225]，再從一般人格權理論著眼，保障消費者隱私實定法化之工作不容忽視[226]，而追溯最早之獨處權理論，反而能導引出新型態之被遺忘的權利，本文上開建議均有其逐步成熟及精緻化之空間，業如前述，自非保障隱私之萬靈丹，然期盼作爲大數據時代下隱私權保障之可能選項，以獲致利益平衡而提供對策討論之抉擇。

---

225 因多半存在於可能具備信賴關係之醫病之間。

226 消費者隱私權不斷被侵犯的事實使得消費者隱私權的保護備受關注，法律中沒有將隱私權作為一項獨立的人格權，可能使得在實踐中消費者隱私權無法得到有效的保護，莫小春，消費者隱私權保護的現狀及途徑探究，特區經濟期刊，第9期，2009年9月，頁5。

參考文獻

一、中　文

㈠專　書

◎李震山，論資訊自決權，載現代國家與憲法——李鴻禧教授六秩華誕祝壽論文集，1997年7月，頁709-755。

㈡期刊論文

1. 田炎欣，警察偵查犯罪侵害個人資料保護法「目的拘束原則」之探討，台灣法學雜誌，第257期，2014年10月，頁85-94。
2. 江守寰，以大數據探勘技術分析「視覺化管理」在監視錄影系統之運用——臺中市政府警察局爲例，犯罪學期刊，第18卷第2期，2016年1月，頁1-29。
3. 甘炎民、郭士豪、黃冠豪、李承龍，大數據資料系統分析運用在偵查實務之研究，警察通識期刊，第5期，2015年11月，頁140-159。
4. 李惠宗，個人資料保護法上的帝王條款——目的拘束原則，法令月刊，第64卷第1期，2013年1月，頁37-61。
5. 李榮耕，論偵查機關對通信紀錄的調取，政大法學評論，第115期，2010年6月，頁115-147。
6. 范姜真媺，日本個人編號法對我國之借鏡——以個人資料保護監督機制之建立爲主，東吳法律學報，第26卷第2期，2014年10月，頁1-33。
7. 翁清坤，告知後同意與消費者個人資料之保護，臺北大學法學論叢，第87期，2013年9月，頁217-322。
8. 莫小春，消費者隱私權保護的現狀及途徑探究，特區經濟期刊，第9期，2009年9月，頁1-25。
9. 許炳華，被遺忘的權利：比較法之觀察，東吳法律學報，第27卷第1期，2015年7月，頁125-163。
10. 陳起行，資訊隱私權法理探討——以美國法爲中心，政大法學評論，第64期，2000年12月，頁297-341。
11. 楊智傑，美國醫療資訊保護法規之初探——以HIPAA/HITECH之隱

私規則與資安規則爲中心，軍法專刊，第60卷第5期，2014年10月，頁79-116。
12. 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，臺北大學法學論叢，第54期，2004年6月，頁41-99。
13. 蕭奕弘，論個人資料保護法之法制性問題，成大法學，第23期，2012年6月，頁141-191。

二、英　文

㈠專　書

1. CHEN, MIN, MAOAND, SHIWEN, ZHANG, YIN & LEUNG, VICTOR CM, BIG DATA: RELATED TECHNOLOGIES, CHALLENGES AND FUTURE PROSPECTS (2014).
2. MAYER-SCHÖNBERGER, VIKTOR & CUKIER, KENNETH, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).
3. NISSENBAUM, HELEN, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).
4. PARISER, ELI, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK (2012).
5. TRIBE, LAURENCE H., AMERICAN CONSTITUTIONAL LAW (1978).

㈡期刊論文

1. Abbott, Ryan, Big Data and Pharmacovigilance: Using Health Information Exchanges to Revolutionize Drug Safety, 99 IOWA L. REV. 225 (2013).
2. Allen, Anita L., Privacy Law: Positive Theory and Normative Practice, 126 HARV. L. REV. F. 241 (2013).
3. Alm, Jessica Gutierrez, The Privacies Life: Automatic License Plate Recognition Is Unconstitutional under the Mosaic Theory of Fourth

Amendment Privacy Law, 38 HAMLINE L. REV. 127 (2014).
4. Ambrose, Meg Leta, Lessons from the Avalanche of Numbers: Big Data in Historical Perspective, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 201 (2015).
5. Ashdown, Gerald G., The Fourth Amendment and the "Legitimate Expectation of Privacy", 34 VAND. L. REV. 1289 (1981).
6. Ambrose, Meg Leta & Ausloos, Jef, The Right to Be Forgotten Across the Pond, 3 J. INFO. POL'Y 1 (2013).
7. Bambauer, Jane R., The Lost Nuanc of Big Data Policing, 94 TEX. L. REV. 1 (2015).
8. Bedi, Monu, Social Networks, Government Surveillance, and the Mosaic Theory, 94 B. U. L. REV. 1809 (2014).
9. Bellovin, Steven M., When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning, 8 NYU J.L. & LIBERTY 556 (2014).
10. Berk, Lon A., After Jones, The Deluge: The Fourth Amendment's Treatment of Information, Big Data and the Cloud, 14 J. HIGH TECH. L. 1 (2014).
11. Birnhack, Michael, Reverse Engineering Informational Privacy Law, 15 YALE J.L. & TECH. 24 (2013).
12. Blass, Megan, The New Data Marketplace: Protecting Personal Data, Electronic Communications, and Individual Privacy in the Age of Mass Surveillance Through a Return to a Property-Based Approach to the Fourth Amendment, 42 HASTINGS CONST. L. Q. 577 (2015).
13. Boyd, Danah & Crawford, Kate, Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon, 15 INFO., COMM. & SOC'Y 662 (2012).
14. Cate, Fred H., Government Data Mining: The Need for a Legal Framework, 43 HARV. C. R.- C. L. REV. 435 (2008).
15. Citron, Danielle Keats, Technological Due Process, 85 WASH. U. L. REV. 1249 (2008).
16. Colb, Sherry F., What is a Search: Two Conceptual Flaws in Fourth

Amendment Doctrine and Some Hints of a Remedy, 55 STAN. L. REV. 119 (2002).
17. Crawford, Kate & Schultz, Jason, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B. C. L. REV. 93 (2014).
18. Cunningham, H. Bryan, Tiny Constables in the Mosaic: Modernizing Oversight of Surveillance in the Age of Big Data, 65 RUTGERS L. REV. 983 (2013).
19. Ferguson, Andrew G., Predictive Policing and Reasonable Suspicion, 62 EMORY L.J. 259 (2012).
20. Ferguson, Andrew G., Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards, 66 OKLA. L. REV. 831 (2014).
21. Ferguson, Andrew G., Big Data and Predictive Reasonable Suspicion, 163 U. PA. L. REV. 327 (2015).
22. Ford, Madelaine Virginia, Mosaic Theory and the Fourth Amendment: How. Jones Can Save Privacy in the Fact of Evolving Technology, 19 AM. U. J. GENDER SOC. POL'Y & L. 1351 (2011).
23. Freiwald, Susan, How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records, 66 OKLA. L. REV. 875 (2014).
24. Garrett, Brandon L., Big Data and Due Process, 99 CORNELL L. REV. 207 (2014).
25. Gatewood, Jace C., District of Columbia Jones and the Mosaic Theory — In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory, 92 NEB. L. REV. 504 (2014).
26. Gray, David C. & Citron, Danielle Keats, A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, 14 N. C. J. L. & TECH. 381 (2013).
27. Gray, David C., Law Enforcement Access to Third Party Records: Critical Perspectives from a Technology — Centered Approach to Quantitative Privacy, 66 OKLA. L. REV. 919 (2014).
28. Henderson, Stephen E., Beyond the (Current) Fourth Amendment: Pro-

tecting Third-Party Information, Third Parties, and the Rest of Us Too, 34 PEPP. L. REV. 975 (2007).

29. Henderson, Stephen E., Our Records Panopticon and the American Bar Association Standards for Criminal Justice, 66 OKLA. L. REV. 699 (2014).

30. Hirsch, Dennis D., The Glass House Effect: Big Data, the New Oil, and the Power of Analogy, 66 ME. L. REV. 373 (2014).

31. Hirsch, Dennis D., That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority, 103 KY. L.J. 345 (2015).

32. Hoofnagle, Chris Jay, Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N. C. J. INT'L L. & COM. REG. 595 (2004).

33. Jerome, Joseph, Big Data: Catalyst for a Privacy Conversation, 48 IND. L. REV. 213 (2014).

34. Joh, Elizabeth E., Policing by Numbers: Big Data and the Fourth Amendment, 89 WASH. L. REV. 35 (2014).

35. Kerr, Orin S., A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208 (2004).

36. Kerr, Orin S., The Case for the Third-Party Doctrine, 107 MICH. L. REV. 561 (2009).

37. Kerr, Orin S., The Mosaic Theory of the Fourth Amendment, 111 MICH. L. REV. 311 (2012).

38. Koss, Kelly K., Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow World, 90 CHI.- KENT L. R. 301 (2015).

39. Lawless, Matthew D., The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection, 2007 UCLA J.L. & TECH. 2 (2007).

40. Loewy, Arnold H., The Fourth Amendment as a Device for Protecting the Innocent, 81 MICH. L. REV. 1229 (1983).

41. Marcus, Philip H., A Fourth Amendment Gag Order — Upholding

Third Party Searches at the Expense of First Amendment Freedom of Association Guarantees, 47 U. PITT. L. REV. 257 (1985).
42. Mattioli, Michael, Disclosing Big Data, 99 MINN. L. REV. 535 (2014).
43. McMeley, Christin S., Protecting Consumer Privacy and Information in the Age of the Internet of Things, 29 ANTITRUST ABA 71 (2014).
44. McNealy, Jasmine, The Emerging Conflict Between Newsworthiness and the Right to Be Forgotten, 39 N. KY. L. REV. 119 (2012).
45. Ness, Devin W., Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It, 31 CARDOZO ARTS & ENT L.J. 925 (2013).
46. Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. REV. 1701 (2010).
47. Ostrander, Benjamin M., The Mosaic Theory and Fourth Amendment Law, 86 NOTRE DAME L. REV. 1733 (2011).
48. Pasquale, Frank & Ragone, Tara Adams, Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing, 17 STAN. TECH. L. REV. 595 (2014).
49. Pasquale, Frank, Grand Bargains for Big Data: The Emerging Law of Health Information, 72 MD. L. REV. 682 (2013).
50. Prosser, William L., Privacy, 48 CAL. L. REV. 383 (1960).
51. Richards, Neil M., The Dangers of Surveillance, 126 HARV. L. REV. 1934 (2013).
52. Richards, Neil M. & King, Jonathan H., Three Paradoxes of Big Data, 66 STAN. L. REV. ONLINE 41 (2013).
53. Richards, Neil M. & King, Jonathan H., Big Data Ethics, 49 WAKE FOREST L. REV. 393 (2014).
54. Rothstein, Mark A., Ethical Issues in Big Data Health Research, Ethical Issues in Big Data Health Research, 43 J.L. MED. & ETHICS 425 (2015).
55. Rubinstein, Ira S., Voter Privacy in the Age of Big Data, 5 WIS. L. REV. 861 (2014).
56. Rushin, Stephen, The Judicial Response to Mass Police Surveillance,

2011 U. ILL. JL TECH. & POL'Y 281 (2011).
57. Schlabach, Gabriel R., Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act, 67 STAN. L. REV. 677 (2015).
58. Segovia, Stephanie, Privacy: An Issue of Priority, 11 HASTINGS BUS. L.J. 193 (2015).
59. Slobogin, Christopher & Schumacher, Joseph E., Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society", 42 DUKE L.J. 727 (1993).
60. Slobogin, Christopher, Government Data Mining and the Fourth Amendment, 75 U. CHI. L. REV. 317 (2008).
61. Solove, Daniel J., Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. 1083 (2002).
62. Spencer, Shaun B., The Surveillance Society and the Third-Party Privacy Problem, 65 S. C. L. REV. 373 (2013).
63. Tene, Omer & Polonetsky, Jules, Big Data for All: Privacy and User Control in the Age of Analytics, 11 NW. J. TECH. & INTELL. PROP. 239 (2013).
64. Tene, Omer, Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws, 74 OHIO ST. L.J. 1217 (2013).
65. Terry, Nicolas P., Protecting Patient Privacy in the Age of Big Data, 81 UMKC L. REV. 385 (2012).
66. Terry, Nicolas P., Big Data Proxies and Health Privacy Exceptionalism, 21 HEALTH MATRIX 65 (2014).
67. Thai, Joseph T., Is Data Mining Ever a Search under Justice Stevens's Fourth Amendment?, 74 FORDHAM L. REV. 1731 (2006).
68. Tucker, Darren S. & Wellford, Hill B., Big Mistakes Regarding Big Data, 14(2) ANTITRUST SRC. 6 (2014).
69. Turner, Brad, When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People's Data, 16 N. C. J. L. & TECH. 377 (2015).

70. Warren, Samuel D. & Brandeis, Louis D., The Right to Privacy, 4 HARV. L. REV. 193 (1890).

㈢網頁文獻

1. ABA Standards for Criminal Justice Law Enforcement Access to Third Party Records, http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf (last visited: 2015.06.29).
2. Article 29 Data Protection Working Party, Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf (last visited: 2016.06.18).
3. Big Data, Gartner, http://www.gartner.com/it-glossary/big-data (last visited: 2015.05.17).
4. Birnhack, Michael, S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm, http://ssrn.com/abstract=2310700 (last visited: 2015.05.19).
5. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Court of Justice of the European Union Press Release, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (last visited: 2015.07.01).
6. Graux, Hans, Ausloos, Jef & Valcke, Peggy, The Right to Be Forgotten in the Internet Era, 17 Interdisciplinary Centre for Law and ICT, 17 Interdisciplinary Centre for Law and ICT, http://ssrn.com/abstract=2174896 (last visited: 2015.10.13).
7. He, Zhile, Huang, Daoli & Lei, Yunting, Legislation of "Right to Be Forgotten" in Big Data Environment, http://www.atlantis-press.com/php/pub.php?publication=icssr-14&frame=http%3A//www.atlantis-press.com/php/paper-details.php%3Fid%3D11865 (last visited: 2016.01.27).
8. Helbing, Dirk & Balietti, Stefano, Big Data, Privacy, and Trusted Web:

What Needs to Be Done, http://ssrn.com/abstract=2322082 (last visited: 2015.06.15).

9. Hoffman, Sharona & Podgurski, Andy, Big Bad Data: Law, Public Policy, and Biomedical Databases, https://www.chrp.org/pdf/HSR01182013_Abstract.pdf (last visited: 2015.05.24).

10. Hoffman, Sharona, Citizen Science: The Law and Ethics of Public Access to Medical Big Data, http://ssrn.com/abstract=2491054 (last visited: 2015.06.10).

11. Hoofnagle, Chris Jay, Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, https://epic.org/privacy/choicepoint/cp_article.pdf(last visited: 2015.06.15).

12. Hull, Gordon, Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data, http://ssrn.com/abstract=2533057 (last visited: 2015.06.02).

13. Holdren, John P. et al., Big Data: A Technological Perspective, Executive Office of the President, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (last visited: 2015.06.12).

14. Kaplan, Bonnie, How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales, http://ssrn.com/abstract=2510013 (last visited: 2015.05.23).

15. Koops, Bert-Jaap, Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice, http://ssrn.com/abstract=1986719 (last visited: 2015.07.01).

16. Podesta, John et al., Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (last visited: 2015.05.17).

17. Raymond, Anjanette H., The Dilemma of Private Justice Systems: Big Data Sources, the Cloud and Predictive Analytics, http://www.alsb.org/wp-content/uploads/2015/01/NP-2014-The-dilemma-of-private-justice-

systems-Raymond.pdf (last visited: 2015.06.10).
18. Richards, Neil M. & King, Jonathan H., Big Data and the Future for Privacy, http://ssrn.com/abstract=2512069 (last visited: 2015.05.23).
19. Rubinstein, Ira S., Big Data: The End of Privacy or a New Beginning?, http://lsr.nellco.org/cgi/viewcontent.cgi?article=1359&context=nyu_pll twp (last visited: 2015.07.01).
20. Sprague, Robert, Privacy Implications of Big Data and Predictive Analytics, http://www.alsb.org/wp-content/uploads/2015/01/NP-2014-Privacy-implications-of-big-data-Sprague.pdf (last visited: 2015.07.01).
21. Walsh, Bryan, Google's Flu Project Shows the Failings of Big Data, http://time.com/23782/google-flu-trends-big-data-problems/ (last visited: 2015.01.18).
22. Werro, Franz, The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash, http://ssrn.com/abstract=1401357 (last visited: 2015.07.08).
23. What is Big Data, University Alliance, http://www.villanovau.com/resources/bi/what-is-big-data/#.VVhXa2Aw_m4 (last visited: 2015.05.17).

The Protection of Right to Privacy in Big Data Era: Possible Impacts and Countermeasures

Pin-Hua Hsu *

Abstract

Big data has only recently gone mainstream. Prior to 2012, big data was a buzzword used by engineers and scientists to describe advances in digital communications, computation and data storage. Big data—the enhanced ability to collect store and analyze previously unimaginable quantities in tremendous speed and with negligible costs, deliver immense benefits in policing, national security, healthcare, business and many other critical areas. The big data age has arrived. At the same time, it affects fundamental rights of individual in ways, which are hard to fully oversee. Among these, the right to privacy is surely one of the most endangered. Privacy is an important human value. The advance of technology both threatens personal privacy and provides opportunities to enhance protection. Like other novel technologies, big data presents amazing possibility to usher in a new age of discovery and innovation for mankind. But, it is simply that in everyday life, we expect even in public, certain facts concerning our daily comings and goings will remain private, not because we

* Prosecutor Investigator, Kaohsiung District Prosecutors Office; Ph.D. in Law, National Chung-Cheng University.

Received: March 22, 2016; accepted: August 14, 2016

intend for them to be private, but because we do not except that any one person would be privy to all of our day's events. Big data does make the protection of right to privacy both considerably more difficult and important. The age of big data is the death or rebirth of privacy? It depends on how to face it. This thesis puts stress on the impacts of big data. And provide the application of due process, especially government obtain information from third parties, health data exceptionalism and the concept of "right to be forgotten", as the options of countermeasures of protection of right to privacy in big data era.

Keywords: Big Data, Right to Privacy, The Fourth Amendment, Due Process, Right to be Forgotten