國立臺灣大學進修推廣學院事業經營法務碩士在職學位學程

碩士論文

Professional Master's Program of Law in Business Administration

School of Professional Education and Continuing Studies

National Taiwan University

Master Thesis

大數據應用世代下的資訊隱私規範

Information Privacy Regulations in The Era of Big Data

張文憶

Wen-I Chang

指導教授：黃銘傑 博士

Advisor: Ming-Jye Huang, Ph.D.

中華民國 109 年 7 月

July 2020

doi:10.6342/NTU202002857

國立臺灣大學碩士學位論文
口試委員會審定書

大數據應用世代下的資訊隱私規範

Information Privacy Regulations in The Era of Big Data

本論文係張文憶君（P07E42020）在國立臺灣大學事業經營法務碩士在職學位學程完成之碩士學位論文，於民國 109 年 07 月 18 日承下列考試委員審查通過及口試及格，特此證明。

口試委員：

（指導教授）

所　　長：

中華民國　109　年　07　月　18　日

doi:10.6342/NTU202002857

中文摘要

在傳統以自主、自治、自決理論為基礎的隱私規範下，各國資訊隱私法規紛紛以建置個資當事人「通知與選擇」機制為規範主軸，所規範者多著重於規定通知個資當事人之方式、應通知之內容、個資當事人選擇或同意的方式以及同意的範圍等。然而，隨著網路科技的快速發展，人民的基礎生活不但越來越依賴資訊網路，甚至在某些情形下因為產業趨勢或政府力推電子化政策的結果，人民的許多日常生活機能幾乎已離不開網路，那麼，人民是否真能自主「選擇」揭露其資訊呢？又在大數據與人工智慧 AI 技術的蓬勃發展下，資訊的應用透過程式演算法自動學習與擴大運用，同時業者間錯縱複雜的合縱連橫合作關係，導致個資當事人即使收悉資訊蒐集者的「通知」，他（她）不但無法即時消化冗長的隱私政策內容，也無法自行評估未來資訊應用所可能產生的實際風險，且由於營業秘密法的保護，人民並無法獲悉與監督資訊蒐集者對其資訊的實際利用狀況。有不少論者即推估，在現行的資訊隱私規範下，個資隱私的未來將往兩個極端的方向發展，一是未來將沒有個資隱私。這是因為當人民習慣性地揭露個資，習慣性地不審視與評估風險，科技的發展使大數據應用越見容易拼湊完整的個人資訊，並能輕易跨境跨領域的傳輸與利用，未來個資將無所不在；或者，二是未來 AI 大數據的發展將受到嚴重阻礙。因為當人民對資訊控制者的個資處理與保護失去信任，人民將傾向不揭露個資，導致資訊流通受到束縛，在沒有足夠的基礎資訊下，AI 大數據分析亦將難以精確地運算與發展。

傳統隱私規範之目的是否真同於資訊隱私之規範目的？究竟人類社會應首重保護個資還是應以鼓勵資訊交流為目標？GDPR 的硬性規定究是有益或有害資訊科技發展？軟性規範是否更適合資訊隱私所遇到的困境？本文藉由資訊揭露本質的分析討論，輔以大數據應用世代生活上的實際案例與經驗，以及資訊揭露者與蒐集者間存在長期被忽略的信任關係等討論，推導資訊蒐集者在資訊隱私議題所應當扮演的角色與應擔負的責任，並建議資訊隱私規範應以資訊信託的角度來立法，輔以設計隱私等軟性規範，俾能同時保護個資隱私與促進大數據與 AI 科技的發展，應用科技增進人類福祉。

關鍵字：資訊隱私、設計隱私、大數據、通知與選擇、資訊信託、歐盟資料保護規則

doi:10.6342/NTU202002857

Abstract

Based upon the traditional concept of privacy which derived from the theory of democracy, autonomy and self-determination, data privacy laws in most of modern countries emphasize on the establishment of a comprehensive notice-and-choice mechanism, which ordinarily include the ruling of means of notices, content of notices, meaningful ways of choices and agreements, the scope of agreements and so forth. However, as the speedy development in internet technologies, not only does people's daily life heavily rely upon information technology, but also people in the modern age are more and more often forced to carry out their life tasks in electronic ways because of industrial trend or governmental policies of digitalization. In such circumstances, can people really discretionally "choose" to or not to disclose their personal information? Moreover, as quick development in big data and artificial intelligence (AI) technology, the ways of information application are sophistically adopted by AI algorism which may learn and improve by itself. Accompanied by the complicated inter-industry data sharing scheme, data subjects usually are not capable of comprehending the actual utilization after and risk of information disclosure, even if they are noticed with lengthy information privacy policies by the data collectors. Furthermore, under the protection of trade secret laws, ordinary people don't have the access to the big data analysis algorisms and application techniques adopted by data controllers, thus people cannot monitor the actual processing of their information. Consequently, many scholars predict that the future of data privacy will eventually either become no privacy at all, on the cause that people will gradually be used to reveal their personal information without trying to evaluate the risks, which provides the AI with the opportunities of easily analyzing big data to identify any person; or hinder AI and big data technology from further development, on the cause that when people lose trust on data collectors and begin to suspect that their interests may be harmed, people will cease providing their personal data, which will curtail free flow of data and AI technology won't be able to rely upon precise raw data in developing useful functions for the benefit of our society in the future.

Whether the purposes of traditional privacy regulations are identical to that of information privacy? Whether our society would be more beneficial by focusing on blind protection of personal data or by facilitating free data transmissions? Whether soft regulations would be a more appropriate resolution for issues of information privacy

doi:10.6342/NTU202002857

than hard, rigid regulations? Through the analysis of nature of information disclosure, accompanied by practical real life cases, experience in the era of big data application and the relations between information disclosers and receivers, this thesis suggests that data collectors shall act as the role of information trust, and information privacy regulations shall be re-designed from the perspective of information trust which may be practically implemented by privacy-by-design concept in order to achieve both goals of privacy protection and stimulating development of big data and AI technologies. Consequently, our society may well take advantage of big data and AI technologies in improving general welfare of humanity.

Key Words: Information Privacy, Privacy by Design, Big Data, Notice and Choice, Information Trust, GDPR

doi:10.6342/NTU202002857

目錄

口試委員會審定書 I

中文摘要 II

ABSTRACT III

目錄 V

第一章 緒論 1

第一節 研究動機 1

第二節 研究方法 5

第三節 研究架構 6

第四節 名詞定義及補充說明 7

第二章 傳統資訊隱私規範的立法基礎 9

第一節 社會對「隱私」的傳統定義影響「資訊隱私」規範的制定 9

第一項 視隱私為個人「私密而免於受干擾」的基本權（消極的保護） 11

第二項 視隱私權為確保個人對其資訊「主宰操控與自治」的權利（積極的保護） 14

第二節 對以「主宰控制、管理」為基礎資訊隱私權規範的批評 16

第三節 個資是否應以新財產權規範？ 17

第一項 個資在傳統財產權下所受的保護程度 18

第二項 為個資創造專屬財產權可能產生的問題 22

第四節 言論自由與資訊隱私規範的衝突與調和 24

第一項 網路業者對個資的使用是否受言論自由的保護？ 24

第二項 商業言論（Commercial Speech）論點 25

第三項 合約約束模式觀點 26

第四項 加諸個資控制者資訊受託義務責任是否即侵害其言論自由？ 28

第五項 被遺忘權（Right to be Forgotten）與言論自由 30

第六項 保護智慧財產權規範對言論自由的挑戰 32

第五節 通知與選擇（notice-and-choice）規範主流的形成 33

第三章 美國與歐盟資訊隱私規範概述 37

第一節 美國資訊隱私規範 37

第二節 歐盟資訊隱私規範 41

第三節 美國與歐盟資訊隱私規範下產生的若干差異 48

doi:10.6342/NTU202002857

第四節 歐盟式規範對大數據人工智慧產業發展的衝擊 51
第四章 資訊揭露的基礎來自對資訊蒐集者的「信任」 56
第一節 通知與選擇（notice-and-choice）機制的利與弊 56
第一項 個人無從判斷風險 58
第二項 選擇退出(Opt-Out)與選擇參加(Opt-in) 63
第三項 同意、撤回同意與刪除權所帶來的困窘 65
第四項 科技網路與大數據資訊利用的特性 67
第二節 社會社交觀點理論下的資訊隱私 72
第一項 人際社交與資訊隱私的關係 72
第二項 依據個資當事人與個資蒐集者的「關係」來辯識資訊的隱私性質 74
第三項 資訊隱私意識的本質應包含資訊揭露當下之背景條件（Context） 75
第三節 資訊蒐集者建立個資當事人「信任」的意義 77
第四節 以「信任」為基礎建立資訊隱私規範 80
第一項 「侵害資訊隱私」在以「權力」及「信任」為基礎資訊隱私規範下的意義 80
第二項 以信任為基礎的資訊隱私 83
第三項 強化資料受託者的受託義務（Fiduciary Duty） 84
第四項 以信託為基礎規範資訊隱私的優勢 92
第五節 Privacy by Design 93
第一項 基本意義 93
第二項 國際資訊隱私法規範相關 Privacy by Design 概念之援引 96
第三項 Privacy by Design 的優勢與可解決的問題 99
第五章 結論 103
附件一、GDPR 與 CCPA 概要比較表 108
參考文獻 109

doi:10.6342/NTU202002857

第一章 緒論

第一節 研究動機

世界許多大型科技網路公司近年一方面向社會大眾推廣，透過網絡、App 或網路社群等與他人交流與分享資訊已成為新時代下之社交活動主流形態，鼓吹默守個資隱私或執著被遺忘權等已是過時的觀念，但另一方面，卻又積極從各種管道蒐集個資大數據，並試圖從中尋找各種人類行為之預測，擷取精準預測人類行為所帶來的各種經濟、社會、政治與經營策略應用上的價值。個人的網路使用習慣也在社會風氣與生活便利誘因的帶動下，逐漸信賴網路交易與各類型的線上活動，甚至著實已相當依賴資訊網絡所帶來的新便利生活、工作與社交模式。然而，使用網路交易或進行活動的個人，是否真正明瞭他（她）向網路設備所揭露的資訊未來可能如何被利用呢？試想過往前往零售賣場購買一部音響的經驗，消費者在賣場頂多與銷售員工口頭聊聊音響的功能與價格，給付現金後即可打包帶回家。但在現今的資訊網路生活世代下，已經很少人會直接殺到實體賣場購買音響了，通常會在網路上先瀏覽與比較一番，再來可能透過社群網絡跟好友、行家或甚至陌生人討論個幾輪，再到電商平台上提供各種個人資料後加入會員，以信用卡或行動支付在網站上消費，收到產品後可能立即上網發個開箱文，上 Facebook 與各方網路好友炫耀或分享，此時若購買的是一部智能音響，它可能正無時不刻地仔細聆聽周遭的指令與對話，也可能透過家用網路與家中或同網域上的其它智能設備展開一些連消費者都不知情的各種資訊交流或溝通。想想整個過程下來消費者共揭露了多少的個人資訊，而消費者真正不在乎個資遭他人知悉與利用嗎？亦或是個人誤認為每項資訊都將在各自功能目的完成後被自動銷毀呢？亦又或者是個人因為生活的便利而選擇暫時忽略資訊安全的風險？

doi:10.6342/NTU202002857

還是在某些情況下，由於業務運行模式已全然數位化的結果，個人根本無從選擇呢？

於個資外洩或遭不法濫用情形層出不窮之際，各國政府便開始制定各類消費者或個人資訊保護法規，隨著便開始有了個資屬性上的討論，然而個人資訊是否真如個人身體私密隱私般，應被歸類為人類隱私的基本權呢？另一方面，大數據與 AI 技術所帶來的資訊革命勢在必行，且確實也為人類帶來深遠廣大的福祉，在巨大公益性考量下，如何與個人對個資的私益相調和呢？

- **大數據應用的特徵**

資訊科技奠基在大數據資料庫的建置，世界對於「大數據」(「Big Data」或稱「巨量資料」) 尚未有一個標準的定義，但較常見者乃指：藉由大規模的資料庫使用，萃取或創造出新形態的資料價值，以某種形式改變了銷售市場、組織，或人民與政府間之關係等層面[1]。美國科技諮詢委員會 (President's Council of Advisors on Science and Technology) 曾於西元 2014 年提出的「大數據與隱私：技術性觀點 (Big Data and Privacy: A Technological Perspective)」報告書中指出，大數據具兩方面特徵：一是展現在可被取得處理資料的量 (quantity) 與多樣性 (variety) 上；另一是指在可被運用於此資料上的分析規模，而資料分析結果將產出某些推論或結論[2]。概括而言，大數據應用可被歸納為具有海量性、多樣性、

[1] Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands,* 66 STAN. L. REV. ONLINE 81, 81 (2013). ("'Big data' can be defined as a problem-solving philosophy that leverages massive datasets and algorithmic analysis to extract 'hidden information and surprising correlations.'"); Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion*, Big Data, and Policing, 10 HARV. L. & POL'Y REV. 15, 20-21 (2016).

[2] President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective (2014). https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf (最後瀏覽日: 2020/2/29).

doi:10.6342/NTU202002857

高速性與易變性等四大特色，以及包含數據類型繁多、數據價值密度相對較低，與處理速度快、時效性要求高等三大特性。

- **精準行銷目的的個資應用**

消費者資訊對於網路業者（「網路業者」予本文之定義請見本章第四節）來說，已不再只是用戶資料，衍然已成為「產品」，用戶資料已大量被應用於各種行銷目的。例如，於西元 2007 年間，臉書 Facebook 啓動一個稱為 Facebook Beacon 的專案，利用用戶電腦端的 Cookies （一種網站用來紀錄瀏覽者在網頁上所有動作的紀錄檔）來紀錄與分析用戶的興趣與近期活動等資訊，並與廠商包括紐約時報、百世達影視、Yelp 等合作，針對 Facebook 用戶的當前興趣，主動推播相應的商品與服務廣告，部分使用者因為不時收到來自四面八方與自己最近網路活動相關的商品廣告，使用者因而感受到自己隱私已遭受侵害[3]，後來因為該專案違反若干美國聯邦法律，例如美國的影片隱私保護法案 (Video Privacy Protection Act) 禁止影視公司在沒有獲得個人書面同意前揭露任何個資，當時 Facebook 被迫改以當用戶主動選擇參與該專案時，才對用戶進行潛在消費分析，並承諾不儲存用戶的網路活動資料。

另一個著名案例為美國大型連鎖零售商 Target 的行銷手法，Target 曾藉由蒐集與分析會員消費者的消費習慣，並結合消費者的財務狀況等資料，甚至向第三方資料經紀公司購買消費者資訊，私下進行交叉比對，以推估其會員產品需求與需求時間，精準地向會員推銷特定產品。而 Target 為了避免引起會員消費者對其隱私安全的注意，Target 還會在向會員推銷產品時，刻意夾雜一些該會員一定不

[3] C.G. Lynch, *A Wake-Up Call for Users in Facebook-Beacon Controversy*, CIO. https://www.cio.com/article/2437512/a-wake-up-call-for-users-in-facebook-beacon-controversy.html (最後瀏覽日：2020/5/12).

doi:10.6342/NTU202002857

會產生任何興趣的商品[4]。

世界最大網路公司 Google 也曾結合用戶在 Google 搜尋引擎與 YouTube 等網站的活動紀錄，分析用戶的潛在消費興趣與消費能力，再以分等分級分價位的方式，將分析所得之訊息銷售給商品或服務供應商[5]。結果是，不同的使用者個人可能收到不同商品類別與價位水平的商品廣告，並且這些結果是使用者個人無法自主掌控的，更具爭議的是使用者並不知曉其個資其實已成為 Google 販售與營利的「商品」。

- **隱私疑慮的種類**

若個資的利用僅是網路業者為了瞭解與預測消費者潛在需求而做的消費資訊分析，大眾大可不必太過擔心，因為即使廠商提供精準商品行銷，購不購買的決定最終仍舊在於個人；然而，大眾真正需要擔心的是，網路業者還可能將所蒐集與分析的結果挪作其它相關或不相關用途，或者分享給第三方，並且任何資料庫系統均可能被駭而造成資料當事人的損失或危險，事實上一直以來不乏網路犯罪集團專為想方設法竊取個資敏感資料的案例。

網路業者對於個資的分析與利用，將可能對個資當事人造成以下四大類實質侵害疑慮：第一，網路業者的後台分析可能使個資當事人洩露了他不欲為人所知的私密訊息或生活習慣。個資當事人可能僅僅利用網路平台滿足某些生活需求，但當個資當事人的網路平台使用紀錄被與其它資訊結合與分析後，將導致某

[4] Jeffrey Rosen, Privacy, Property, and Free Speech: Law and the Constitution in the 21st Century, 91-92 (2012).

[5] Miguel Helft, *Google Told to Turn Over User Data of YouTube*, The New York Times. https://www.nytimes.com/2008/07/04/technology/04youtube.html?searchResultPosition=2 (最後瀏覽日：2020/5/12).

doi:10.6342/NTU202002857

組織或個人輾轉獲知個資當事人不希望其所知悉的特定訊息；第二，當個資一再被不當傳送予第三方時，可能最終造成資料被公開的結果，而該公開是個資當事人所不預期或不期望的；第三，網路業者對個資的分析或不當的保管可能造成個人識別性資料的盜竊，直接或間接造成個資當事人財務的損失或名譽的損害；第四，當某業者依據所蒐集與分析的個資做成商業決策時，個資當事人可能因此受到差別待遇或其它負面的影響。例如，保險公司或貸款銀行可能依個人資訊提供不同條件的契約。又例如，商品廠商也可能依使用者的財務狀況與消費習慣施以差別訂價等。又在某些情形下，個資當事人的潛在雇主也可能取得其個資，並依據該資訊先入為主地直接否決與個人的僱傭計劃。抽象一點的情況還包括，若業者將個資當成是一種買賣或交易的商品，有論者質疑個資當事人應有權向業者索求適當的交易對價或利潤分享。

本文希望藉由對「資訊隱私」本質的探究，對歐美資訊隱私規範背景的討論分析，並從應用實務角度逐一檢討現行規範的缺失與失焦之處，最終希望以資訊隱私所能帶給社會進步的價值為核心，企圖重新找回資訊隱私規範的真義與適當的管理汪道。

第二節 研究方法

本文使用常見之比較法研究作為主軸，比較世界二大隱私規範主流--歐盟與美國個資保護制度特點，分析相關立法基礎理論與其管制手段。比較法研究能分成三個階段: 第一個階段為「閱讀、探索、訪談、諮詢與拓展對於特定議題的了解」;第二個階段為「描述、分析、分類、組織、討論、評價等對於資料之詮釋」;第三個階段為「溝通、呈現等對外之發表」[6]。對於歐盟、美國之資訊隱私法規

[6] Mark Van Hoecke, *Methodology of Comparative Legal Research*, 12 Law and Method, 5-21(2015).

doi:10.6342/NTU202002857

範的研究，本文主要以外文文獻為主要參考資料，除介紹資訊隱私相關理論基礎與管制規範外，主要分析其應用對於大數據科技產業產生的衝擊，同時輔以相關案例，協助讀者從中瞭解理論與應用實務間的明顯落差，並就資訊隱私與社交本質的內涵，提出較為妥適的隱私規範基礎與方法。

第三節 研究架構

本文共分為五章，第一章為緒論，發掘與定義本文所究問題與研究範圍，中間分為三章討論何以改進現行資訊規範制度，最後一章為結論。本文第二章先介紹傳統個資隱私規範的立法基礎，透過對隱私理論的探究，歸納現行資訊隱私法規範的制定邏輯，同時探討隱私規範應用於大數據科技發展下所產生的矛盾與衝突，指出現行規範適用上所面臨的難題－無法同時兼顧個人對資訊隱私風險規避的期望與普遍鼓勵大數據產業發展的公共政策。第三章介紹美國與歐盟資訊隱私實體法中相關大數據科技應用之規範，比較兩者規範間的根本差異與原由，並探究歐盟 GDPR 強制規範下對大數據科技產業發展所帶來的各種衝擊。第四章則先就現行各國資訊隱私規範下所通用的通知與選擇（notice-and-choice）機制進行檢討，個資當事人是否真如預期得到適當的風險通知，是否系在瞭解個資揭露風險後能自主與有意義地作出「選擇」。隨後本文就資訊揭露的本質與社會社交間的關係提出討論，細究「信任」在個資當事人與個資蒐集者或控制者間所扮演的重要角色，檢討資訊隱私規範制定的基礎，引導讀者思考資訊隱私的目的究竟應是維持人與人間的距離，保護個人不被外界侵犯，亦或者應是用以縮短人與人間的距離，促進人際間交流，並鼓勵個人在信任的基礎下揭露個資，助長大數據與 AI 科技產業的發展，以追求更大社會公益。又從企業經營與永續發展的角度思考，思考如何在近來各國資訊隱私規範急遽變動的年代，同時做好資訊

doi:10.6342/NTU202002857

隱私法令遵循的準備，並善盡企業社會責任。最後自企業總體策略角度思考，資訊隱私的不確定法制，對企業而言會是一種威脅，又或是一個執行差異化競爭策略的機會呢？

本文第五章結論總結前述觀點，認為若要使資訊隱私規範成為大數據應用世代發展的助力而非阻力，就應要依據資訊揭露與交流中存在的「信任」本質，在相關規範中置入「信任」或「資訊信託」的觀念以及受託者義務責任，並認為為使資訊隱私規範在快速變動與發展的大數據與 AI 技術應用環境中靈活地被適用，應要在產品或服務開發過程間即導入可被公開檢視的隱私設計(privacy by design)概念，同時以信任為基礎之資訊隱私規範亦能構建於隱私設計程序之中，形成一系列與目的相符合的資訊隱私法制與企業策略。

第四節 名詞定義及補充說明

或許對於某些相同意義的標的，本文於論理描述過程中使用與他文不同的用語，然為使讀者閱讀理解之便利，並統一本文用語，定義與解釋如下：

一、 個人資訊（或個人資料、個資）：指與個資當事人相關的任何資訊。

二、 個資當事人（或個資主體）：指由個人資訊得識別或已識別之自然人。

三、 個資蒐集者：指向個資當事人或其它個資控制者蒐集個資之商業組織，可能亦同時是個資控制者。

四、 個資控制者：指實際掌握個資，並有能力應用、轉讓、分析或處理個資的商業組織。

五、 GDPR：係指歐洲議會與歐盟理事會於西元 2016 年 4 月 27 日決議取代第 95/46/EC 號指令，所通過保護自然人有關個人個資處理及資料自由流通的第 2016/679 號「一般資料保護規則」(General Data Protection Regulation)。

doi:10.6342/NTU202002857

六、 網路業者：泛指大量透過互聯網科技與應用大數據分析向社會大眾行銷、銷售或提供產品或服務之營利事業。

doi:10.6342/NTU202002857

第二章 傳統資訊隱私規範的立法基礎

本章首先回顧現行資訊隱私規範的立法基礎與背景邏輯，藉由探求「隱私」對人類社會觀念的各種意義與性質，區別「隱私」與「資訊隱私」的範籌及規範目的，並以實務案例討論強加傳統隱私權概念予資訊隱私規範後產生的種種不相調和方枘圓鑿之現象，尤其大數據應用世代下人類生活模式的快速改變，個人資訊不斷有意、無意間曝露於雲霧繚繞（雲端運算）之中，雲裡看花的人們搞不清楚狀況，殊不知已成為騰雲駕霧的資訊蒐集者最有價值的待售商品。

隨後討論既然個資衍然成為有價值的商品，那麼財產權化個資是否能是一個可行的方向，縱使現行動產與不動產財產權、營業秘密、智慧財產權與競爭法等在特定情況下對個資權利有若干不同面向的保護，但終究不若財產權之賦與來得完整，然而囿於個資人格性的本質，完全的商品化個資亦顯得捨本逐末。本章後半部則討論政府以行政法角度介入個資利用的管制，是否與人民言論自由基本權利產生衝突？並探討應如何加以調和以符合個資隱私規範的法理邏輯。

本章末節則討論現行各國個資隱私管制的通用法則—通知與選擇（notice-and-choice）機制的出線，通知與選擇機制之所以廣受採用，無非因為它既符合傳統隱私自主管理、自治及民主的精神，又具有行政執行的便利優勢，然而它是否在大數據應用世代下仍然左右逢源卻是有待商榷，此將銜接下章美國與歐盟的資訊隱私實體法實踐中一併討論。

第一節 社會對「隱私」的傳統定義影響「資訊隱私」規範的制定

由於早年並沒有數位與網路資訊科技的發達與應用，資訊隱私被視為是傳統人身隱私的一環。而探究隱私概念的緣起，可朔自早期著名英國哲學家 John Locke 提出的基礎概念，他主張雖然人人有平等的機會去享受所有土地，但若某

doi:10.6342/NTU202002857

人藉由他（她）的勞力使某土地增加了價值而產生了質變時，該人就應要有權可擁有該成果，使其為「私有」，意義上即產生可「排除」他人或外力入侵與近用的權利。啓蒙時代德意志哲學家 Immanuel Kant 認為，人類之所以值得被敬重，是因為人類得以理性地「管理」屬於自己的事物，而不是僅僅受大自然力量支配或者隨社會壓力而行事。John Locke 及 Immanuel Kant 兩位哲學家對於人類可管理、自治與處理自己事物的哲學理念，深刻影響後續法學者對人類隱私權權力的定義，以及建立起以「防禦外力干涉」為基礎的隱私權規範[7]。

在西元 1809 年，著名的美國律師 Samuel Warren 與美國最高法院法官 Louis Brandeis 合著出版於哈佛法學評論的一編論文 – 【隱私的權利】 ("the Right to Privacy")，堪稱是影響美國隱私權規範最深遠的一部著作。基於當年（西元 1850-1900）美國媒體快速蓬勃發展的背景下，個人（惟當時系指高階社會地位人士）大多害怕自己的生活與行為受到媒體的探詢，故該論文提出一個以人民具有「不受干擾權利」（right to be let alone）（亦有譯為「獨處權」）為基石的隱私權概念，該文認為個人對自己的思想、情緒和感受等與自身相關的事務，應有決定公開與否的權利，但該文也同時主張，隱私權不是絕對的，必須受到公共利益以及當事人同意例外的限制[8]。這個以「隔離」為基本概念的隱私權，陸續得到許多法學者與社會學者的贊同。其中包括，著名法學者 Anita Allen 主張：隱私權必須使個人得以將自己與他人分離，否則個人的生活將會不斷地被外界所打擾。著名社會科學家 David O'Brien 主張：隱私的意義在於限制他人近用個人資訊[9]。著名哲學家 Howard White 與 Sissela Bok 主張：隱私應是一種個人對抗世界以及其它個

[7] Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age, 12-15 (2018).

[8] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890).

[9] David M. O'Brien, Privacy, Law, And Public Policy, 16 (1979).

doi:10.6342/NTU202002857

人所不喜好之外力的權利[10]。社會學家 Donald Ball 將隱私定義為：一個使自己得自由參與任何活動而免於受監視的權利[11]。著名法學者 Milton Konvitz 則主張，隱私應該是一個公眾不能任意進入或控制的個人空間[12]。

第一項 視隱私為個人「私密而免於受干擾」的基本權（消極的保護）

個人資訊隱私曾被視為是人身私領域的一部分，就像個人的身體、房間或放置在個人上鎖抽屜內的東西一般，個人為了予以保護，可藉由穿衣、築牆、上鎖等手段達成保護之目的，也就是以各種「隔離」的方來與外界區隔，並藉由區隔以形成保護。

諸多哲學家及學者贊同以「隔離」及「排它」作為保護或建立隱私的方式，例如，Alan Bates 認為隱私是「個人一種排除他人干涉某事物的感覺」[13]；Jeffrey Reiman 認為隱私授與人們存在的頭銜並且允許人們對自我思想與作為主張完全的佔有權[14]；Samuel Warren 與 Louis Brandeis 認為人類「不容打擊的人格性是指我們具有排除他人介入我們的思想、觀點與情緒之權利」[15]。他們認為，透過「界定」一個專屬個人的領域，未經個人允許前，外人即不得進入或窺視個人私領域空間者，系為隱私權之真義。此以「隔離」為中心的隱私定義，某種程度上系繼

---

[10] Howard B. White, *The Right to Privacy*, 18 Soc. Res. 171, 172 (1951); Sissela Bok, Secrets: On The Ethics of Concealment and Revelation, 10-11 (1983).

[11] Donale W. Ball, *Privacy, Publicity, Deviance and Control*, 18 Pac. Soc. Rev. 259, 260 (1975).

[12] Waldman, *supra* note 7, at 15-19.

[13] Alan P. Bates, *Privacy – A Useful Concept?*, 42 Soc. Forces 429, 429 (1964). (Privacy is "a person's feeling that others should be excluded from something.")

[14] Jeffrey H. Reiman, *Privacy, Intimacy and Personhood*, 6(1) Phil. & Pub. Aff. 26, at 39, 42-44 (1976).

[15] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 205 (1890). (Our "inviolate personality" meant that we had a right to exclude others from our thoughts, sentiments, and emotions.)

doi:10.6342/NTU202002857

受自西方文化強調個人主義（individualism）之思想。

然而，就法律權利主張的角度而言，此等規範基礎其實是破壞了隱私的保障，原因是因為如此定義下的隱私權缺乏任何可被證明的「金錢價值」，也就是當個人隱私遭受不當或不法揭露時，除了抽象的理想與概念外，個資當事人常常無法合理證明該資訊到底能折合多少的「金錢價值」。[16]

以現今社會網路生活習慣觀察，這樣的資訊隱私觀念並無法與之相契合，例如，現代社會生活中，人們已經逐漸習慣於透過臉書 Facebook、部落格、社群媒體 App 等社群社交工具，向好友或群組成員傳遞個人資訊，以達與他人交流的目的，然而在揭露的同時，縱使個人暫時放棄了對該等隱私資訊的「隔離」狀態，但並非即意指就此放棄隱私，因為此舉只是就某些特定目的而為的訊息交流。

在本觀念下，關於如何界定某資訊是否屬個人「親密與私密性」訊息的問題，部分學者主張應以資訊本身之意義是否屬於或具有「人身」親密及私密性之性質來界定，例如，人的性向、生育、家庭、健康資訊等。相較於前述使用資訊是否存在於私領域來定義隱私資訊的方式，以資訊本身意義來區分的好處在於，界線定義上較易被理解，原因是通常國家已有諸多法律保護某些訊息的私密性，例如，醫療與金融法規通常分別明文保護個人健康與財務資訊等。又或者某些話題已有相當確定之基礎隱私定性，例如，性向、同性戀等訊息已根深蒂固地被一般大眾認定為屬個人親密與私密性質的隱私訊息。然而，這個區別方式還是存在缺失，例如，每個人實際上對於人身私密感覺（或稱，接受尺度）可能不竟相同，若只將資訊隱私侷限在人身親密及私密性訊息，最終也將產生定義不夠精確的問題。

應用上來說，這個以「人身親密及私密性」的隱私訊息界定，將產生四個主

[16] In re JetBlue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (E.D.N.Y. 2005).

doi:10.6342/NTU202002857

要問題：第一，縱使人們習慣於把具私密性的訊息告知單一或某些特定群組，該揭露行為或習慣仍不代表該私密性訊息已不再私密。例如，男女朋友間拍攝裸照供對方保存，並不代表該照片不再是私密照片；又例如，將個人罹患性病一事告知閨密，也不代表患病一事不再私密。實際上，把個人私密之事揭露給特定人的行為，應是一般社交活動的常態，再正常也不過，揭露並不代表放棄私密狀態。

第二，有論者認為私密的事（也就是個人不希望他人知悉的事）其實大多是負面的資訊。例如，個人的某些隱疾、個人私底下對他人的批評、個人異於常人的特殊僻好等等，據此進一步質疑法規範對於這些不好的或者負面的資訊予以周全保護的必要性。也就是說，若以人身私密性性質來定義資訊隱私，可能亦缺乏法律保護的正當性。

第三，若只保護人身「私密」訊息，將無法同時保護我們經常透過網路揭露不屬私密的訊息，例如個人消費習慣、交通路徑、消費項目等等都非謂具有「人身親密及私密性」性質之訊息，豈不是直接被排除在外？然而，縱使該等訊息非具人身親密及私密性，卻也不見得是一般個資當事人普遍想對全世界揭露的個人資訊。換句話說，此等分類將產生受保護訊息含蓋範圍不夠廣泛的問題。

第四，邏輯上來說，以強調個人私密性訊息的資訊隱私定義下，只有自己或相當少數人知悉的資訊，才像是「私密」資訊，當資料當事人主動對外揭露後，該等訊息理應不再具有所謂的「私密」性質，故不應再受資訊隱私規範的保護。然而，在現今網路科技時代下的生活，如此的結論將使個人越來越沒有隱私，因為個資的揭露在許多的情況下不僅已是必然，並且相當自然，人們常常需要被迫透過網路平台揭露訊息予他方以換取得各種服務或便利，若僅以該訊息是否存在私密性質來做為受隱私規範保護之判別，對個人私密資訊的保護將明顯不夠

doi:10.6342/NTU202002857

周全[17]。

第二項 視隱私權為確保個人對其資訊「主宰操控與自治」的權利（積極的保護）

本主張強調個資當事人對其個資應具有完整自主的處置、使用、控制的權利，亦即，個資當事人應可自主決定由「誰」、於「何時」、於何「場合」與在何「條件」下可近用或利用自己的個資訊息，這是一種展現個人有絕對權利來「主宰控制與管理」個人與他人界線的觀點。

本觀點源自人民「自治」與「自決」的基礎概念與原則，其中強調，個人唯有透過不被干擾的自主思考以及自由地私下討論，才能夠真正使個人自由表達自我意識。著名哲學家 George Kateb 主張，光是人民被監視的現象，即已對人民自治與自決造成實質的傷害，因為，它降低了人民的人格性，當人民知道他（她）們可能處於被監視的狀態，個人的獨立理性思考、評判能力與自由即已經被嚴重剝奪，人民將因遭受各種壓力而不得不選擇迎合他人或組織，如此的話，真實的自我必將隨之遭受扭曲[18]。

哲學家 Jeffrey Rosen 認為，「監視」活動易造成對被監視者的歧視，因為監視者藉由監視所得到的資訊，不見得就是個人真實的資訊或狀態，而當利害關係人參考或依賴那些資訊時，即可能產生不利於個資當事人的各種刻板印象，而使其遭受不平等或不利益的行為結果[19]。此現象在大數據科技發展時代下之商業活動尤其頻繁與顯著，例如，當某機構組織監視紀錄某人日常在 Google 搜尋引擎的搜尋歷史，在經過演算法的運算分析（black box algorithms）後，斷定個人的喜好、個性、財務狀況等，並據以提供特定的商品或服務，或以特定的條件提供

---

[17] Waldman, *supra* note 7, at 12-24.

[18] George Kateb, *On Being Watched and Known*, 68 Soc. Res. 269, 274-275 (2001).

[19] Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy In America, 7-9 (2000).

doi:10.6342/NTU202002857

某商品或服務時，個人即可能已遭受不平等對待，侵犯了他（她）追求平等與自主決定的基本權利。

另一方面，人民主宰控制與管理「誰」、在「何時」與「何地」知悉與使用其個資訊息的權利，也被若干哲學家及學者認為是個資隱私權最重要的核心權利之一。例如，哥倫比亞大學著名的政治思想學教授 Jean Cohen 認為：「隱私是一個個人可以『選擇』是否、何時、與誰分享其親密訊息的權利。」[20]哥倫比亞大學教授 Alan Westin 也持類似的看法[21]。著名學者 Evoking Goffman 與 Charles Fried 主張，個人之所以有不同親密程度的朋友，即是因為個人選擇和親密的朋友談論較為私密的資訊，與不那麼熟悉的朋友交談時，選擇傾向不向其透露個人太私密的訊息[22]。也就是說，個人自由『選擇』讓哪些人知悉他(她)的私密訊息，即是個人對資訊隱私控制權權利的表現。著名哲學家 Steve Matthews 亦主張：「隱私即是個人控制與管理個人與他人的界線。」[23]

此以「主宰控制、管理」個資為基礎的隱私權概念，深刻影響多數包括美國及歐盟的資訊隱私規範。例如，美國衛生教育福利部（Department of Housing, Education, and Welfare）於西元 1973 年所頒布的公平資訊實施原則（Fair Information Practices Principles）中強調，個人必須可以「控制」其個資。又例如，美國聯邦貿易委員會（Federal Trade Commission, FTC）為保護消費者免於遭受不公平或欺瞞的商業行為，於西元 2000 年促使國會通過法案，要求商業網站均

---

[20] Jean L. Cohen, *The Necessity of Privacy*, 68 Soc. Res. 318, 319 (2001).

[21] Alan F. Westin, Privacy and Freedom, 7 (1967). (Privacy "is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.")

[22] Charles Fried, *Privacy*, 77 Yale L.J., 475, 484 (1968).

[23] Steve Matthews, *Anonymity And The Social Self*, 47 Am. Phil. Q. 351, 351 (2010).

doi:10.6342/NTU202002857

需向個人揭露其個人資訊利用的部分、時間及方式。又例如，經濟合作暨發展組織 OECD 於西元 2001 年公布的指導原則指出，資料搜集者有揭露資訊蒐集目的、蒐集範圍、資料保密機制以及所有資料使用者的義務[24]。對個資當事人的「通知」相關規定，已被世界各重要國家與組織認為是屬個人隱私保護相當重要的一環[25]。事實上，美國與歐盟資訊隱私法規的核心機制即是「**通知與選擇原則（Notice-and-Choice）**」，該規定要求資訊蒐集者必須明確告知個資當事人資訊蒐集目的、方法以及後續轉分享對象等資訊，使個人可以選擇同意或反對，並選擇是否參加或選擇其它產品或服務。「通知與選擇原則」機制即是在於確認個人得「主宰控制與管理」其個資的規範設計。

第二節　對以「主宰控制、管理」為基礎資訊隱私權規範的批評

雖然理論上個人藉由被告知與自主選擇的機制應可協助個資當事人實現「管理與控制」其個資的目的，但在網路科技應用日益普及的生活形態下，實際上個人時常是在非自願的情況下揭露個人訊息，例如，網路上購物時被迫向網路商店提供信用卡資料的財務訊息，同時交易過程中網路業者透過網站平台任意紀錄個人消費習慣、IP 位址與電腦軟硬體設備，以及個人使用手機 App 時亦可能非自主地揭露的地理位置資訊、上線時間、個人點擊連結的項目或個人所使用的瀏覽器類型、電腦作為業系統等個資。如此非自願性的個資揭露是否即等同個

---

[24] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing (2002). https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (最後瀏覽日: 2020/6/1).

[25] FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress (2000). https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (最後瀏覽日: 2020/6/1).

doi:10.6342/NTU202002857

資當事人自主效棄對該個資的主宰控制與排他的管理權利呢？美國過去的司法見解對此持肯定的態度，認為個人既然已對外揭露個資訊息，即已破壞了個人對其個資繼續維持私密的合理期待，可被視為個人已放棄對該等資訊的主宰控制。

對此規範的另一批評是，個人對於是否揭露其隱私訊息並非總是理性的，原因可能是在某些情況下，個人並無法瞭解其資訊揭露或被利用後的後果，又有學者研究發現，個人對於是否揭露其個人資訊的決策容易受眾多環境週圍因素的影響，例如，個人可能參考其它大部分人是否揭露的事實，來決定自己是否跟進揭露，又個人可能因為個資蒐集者網站設計的美觀程度、個人對特定網站的情感與依賴程度等來決定揭露其個資，然而該決定並非真正是基於風險考量而放棄對個資控制與管理的結果。

以上無論由消極或積極面思考為出發的隱私權保護規範，都具有一個共通特性：即把個人隱私視為個人的基本權利，並且認為它可被用來與世界所有其它人「對抗或分割」。然而，在網際網路主宰的生活世代裡，已經無法再適用如此以自我基本權力為核心的資訊隱私權觀念，在網路生活世代下，個人時常必需透過網路揭露各種訊息以換取各種服務，若因揭露即代表同意完全放棄對個資的控制與管理，或者個人與外界的隔離或獨立，也就是若強加傳統隱私概觀念予大數據網路下之資訊隱私規範，將會產生兩種極端的後果，不是人民的個資隱私將逐漸消失，就是資訊的交流將因為大眾對個資風險的擔憂而逐漸遭受阻礙。

第三節 個資是否應以新財產權規範？

歐盟與美國論者近年提出以財產權觀念來規範大數據時代下越來越多、越來越有價值的個人資訊，個資財產權論點主要著眼於，越來越多的網路業者任意蒐集與利用個資，但卻未對個資當事人或個資提供者給付適當的金錢對價，個資

doi:10.6342/NTU202002857

蒐集者通常只對願意提供資訊的個資當事人提供某些便利的網路服務或網站訊息，卻持續地追蹤與紀錄獲取相關於當事人的各類個資。因此，論者認為若能為個資創造一個專屬的財產權，可能有助業者以價金或其它交易對價向個資當事人以購買、取得授權或租賃等方式換取個資或利用權利。另外一方面，有個資財產權化支持者提出，因為財產權具市場自由買賣與移轉的特質，個資的財產權化將有助提升大數據蒐集者辛苦蒐集資訊而創造出來的價值，個資將由單純的資料或情報轉變為有市值的資產，可激勵大數據事業的持續發展。尤其關於那些個人在日常生活中，不斷地被被動蒐集的各種個資，例如，個人的行動軌跡、購物習慣與偏好、駕駛路線與慣性、手機與網頁的瀏覽紀錄等非屬個人親密性的個資，這類個資有個共同特性，在蒐集的當下個資當事人通常並不認為具有任何顯著經濟價值，且無法預見資訊蒐集者未來對其利用所能產生的效益，但對於大數據或網路科技業者來說，該類資訊卻蘊含龐大商機，所以儘管在蒐集階段尚未有具體的利用規劃，個資蒐集者仍然積極地累積與儲存個資資料庫，以備未來的應用所需。鉅觀而言，在資訊不對等的狀態下，彷彿個資當事人被個資蒐集者佔盡便宜。然而，賦予前述個資新財產權又存在若干實務上難解的議題，以及在個資保護程度上過猶不及與畫蛇添足的隱憂。

第一項 個資在傳統財產權下所受的保護程度

不動產產權對於已附著於不動產上的資訊，例如刻蝕於石碑或樹木的告示資訊、石洞壁上的畫作、漆在路地上的訊息等，不動產所有權人對其具有如同不動產權般的所有權，包括可佔有、排除他人踐越等權利，但不動產權利並不延伸至訊息本身，即不動產所有權人不能對訊息本身主張所有權，例如禁止他人攝影該訊息，也不能禁止他人對訊息進行評論、利用、重製或散布等行為。同樣地，

doi:10.6342/NTU202002857

動產產權所有人亦對於附著於動產之資訊，有排除他人佔有或任意移轉的權利，但該權利僅限於附著於實體物[26]的資訊，並不能禁止他人閱讀、使用、重製、披露或展示任何顯示於動產上之資訊。亦即，動產產權所有人對於顯示於動產上之資訊本身，並無排它權之財產權權利。

營業秘密保護法貌似提供予機密資訊所有人一個類似財產權的保護，但仔細檢視仍有顯著區別，企業主張營業秘密保護之通常條件為：1)該資訊不為一般人所知悉；2) 該資訊具有一定程度的商業價值；3)企業已採取必要合理保護措施，保護與維持該訊息之秘密性等。營業秘密規範的立法目的系為防止競爭對手採取不正當競爭手段與之競爭，例如託請商業間諜竊取機密文件或資料等，但並非著眼於為營業秘密所有人創造一個財產權權利，營業秘密所有人並不具有排它權，且一旦該訊息被他人合法知悉，或他人透過自行研發、反向工程研究等方法得知時，營業秘密所有人並不能依營業秘密法主張權利侵害。是以，本質上而言，營業秘密規範提供給營業秘密所有人的保護，較類似侵權行為的防範，而並非如財產權規範對財產（營業秘密）本身的絕對保護。另一方面，即使個資是存放在網路業者提供給用戶端之設備內，因為網路業者通常在缺乏個人同意的情況下，並無法取得直接近用設備中用戶個資的權利，故網路業者也無法對用戶個資主張營業秘密的保護。而用戶也無法對其個資主張營業秘密保護，因為，個人用戶對其個資並無法聲稱任何商業競爭價值，又況且大數據時代下許多的個資，都是在個人無意間或者公開地被所蒐集，該等訊息是否能滿足營業秘密規範要求的秘密性仍有疑問。是以，營業秘密規範並沒有為個資創造所有權的財產權權利，而僅是提供一個杜絕不肖商業競爭者進行不公平競爭的工具。

[26] 大陸法系通常要求動產必須是有形實物（tangible things），英美法系通常定義個人動產財產為任何不屬於不動產之物，且必須是與實體物（physical items）相關連。

doi:10.6342/NTU202002857

智慧財產權如專利、商標及著作權等，雖然提供所有權人某種財產權權利，但卻均排除組成的基本訊息、想法或自然現象。例如，各國專利權通常排除自然法則、自然現象與抽象概念的專利權授與，因為這些項目通常被認為是科學發展的重要基礎工具，不宜被獨佔，否則將阻礙創新。基此，縱使大數據的運算、整理儲存或應用可被授與專利權，但基礎資訊如個資，即不在可專利的範圍內。

同樣地，商標權規範的目的在於創造企業及其商品的識別性，避免使消費者造成混淆與形塑品牌價值，雖然某些個資，如個人的姓名等，可被用來申請註冊為商標，但商標法並不因此對該姓名本身創造一個財產權，而僅是使商標所有權人能排除他人使用該商標販售商品或服務，或其它可能構成消費者混淆的行銷手段之權利。

在著作權方面，各國著作權為保護所有權人對於思想或概念的表達，雖然著作權人得排除他人利用、複製、散布、演示或發表其著作，但在定義上則直接地排除了對著作物中想法或概念本身的保護，大數據資料下的個資系屬基礎資訊，通常因此也不屬著作權保護的範疇。同時，著作表達受著作權保護的另一重要要件系該表達必須是著作人具有創意性的詮釋，雖然著作權法對著作人創意程度的要求是相對低的，而亦非基礎資訊即可滿足。析言之，大數據下的個資基礎資訊，除非是著作人將所蒐集的基礎個資作有意義或富創意性地整理或編排，否則即不受著作權保護。大數據世代生活下的資訊蒐集，除非著作人撰寫程式時，將各種基礎資訊串聯使用，進而創造出具有創意價值的著作物，才受著作權保護，例如 GPS 導航系統，它同時應用所蒐集的駕駛人位置、地圖、都市地點分類、位址資訊以及當時交通路況等資訊。相對地，對於個別的基礎資訊蒐集，例如，智能汽車蒐集駕駛人駕駛資訊，基本上是以無腦、機械性持續偵測的方式蒐集，

doi:10.6342/NTU202002857

由於資訊累積的過程中並沒有太多的人為創意介入，尚難滿足著作權授與之要件。又即使是對大眾資訊的串聯使用與具創意性的編輯，著作權所提供的保護，也僅是具有創意性編輯的部分，而並非禁止他人從著作物中粹取出組成的基礎資訊再做其它用途，並且，該用途通常也落入合理使用的例外規範。總而言之，著作權不但沒有對構成著作的元素基礎資訊創造財產權權利，反而是刻意地排除了基礎事實資訊的著作權授與[27]。

關於對資料庫的保護，為避免不肖業者有搭便車等不正當競爭行為情形，歐盟設有資料庫保護指令[28]，保護資料蒐集者與編撰者的競爭優勢。美國司法實務見解上，除了著作權法之外，亦以不公平競爭（unfair competition）以及普通法的盜用（misappropriation）禁止等規範方式加以處理，新聞媒體業也可依賴類似的法規，防止競爭業者盜用具有流行火熱話題性的新聞報導。但無論如何，該類規範系為保護業者間的公平競爭秩序，並非授與資料所有者真正的財產權權利，也並無絕對性的排它權，同時也通常排除資料庫中個別個資權利，所有者僅能就有意義性且具有計劃性投資與設計而得之資料庫主張保護[29]。

最後，縱使現行各國的資訊隱私規範，著重於使個資當事人對其個資有某種程度的排它權利，但也僅止於限制公部門或私部門商業業者利用其個資，並非對任何人或家戶使用皆有所限制，甚至如美國的資訊隱私規範，僅系依照特定產業別設置特定的規則，並非一體適用。另一方面，資訊隱私規範通常也並沒有對個資所有權權利移轉訂有規則。是以，現行資訊隱私規範並非將個資視同個人財產

---

[27] Lothar Determann, *No One Owns Data,* 70(1) Hastings L. J. 1, 17-20 (2018).

[28] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20. https://op.europa.eu/en/publication-detail/-/publication/b48976b5-b31a-4dba-a052-87133e17d65e/language-en (最後瀏覽日: 2020/4/1).

[29] Determann, *supra* note 27, at 20-22.

doi:10.6342/NTU202002857

般同等對待，而僅是以保障個人自由與人格為主要目的法規範設計[30]。

第二項 為個資創造專屬財產權可能產生的問題

近年有論者爭辯是否應為個人資料創造一個新的財產權，這個考量無非需衡平思考兩個面向：究竟是資訊控制者對個資控制能力重要，亦或是確保個資不受資訊控制者完全操控重要？支持前者的主要理由為，個資資料庫財產權化有助於保護個資蒐集者辛苦蒐集資訊的成果以及編撰的創意，可刺激大數據科技的開發與進步，並且也有助保護個人隱私；支持後者的主要理由為，資訊的自由分享乃是言論自由的重要實踐，也是市場維持公平競爭秩序的展現，個資若淪為個人可排它利用的財產權，則將阻礙言論自由發展與公平競爭秩序的維持[31]。

個資財產權化可能將創造一個有產值與交易秩序的「資訊市場」，有了市場價值，資訊開發者將更有動力去投資資訊的研究與應用，培養資訊價值鏈，也由於有對價，個資當事人或個資所有人也將較願意授權與分享資料予他人。然而，從近年大數據科技應用高速發展的現象觀之，即使個資蒐集者與控制者尚未對其所蒐制或控制之個資握有財產權，各類大數據應用產業仍舊不斷高速發展，各式新興商業模式，如共享經濟或開放原始碼等，使資訊的開放與保護不必須依賴傳統的財產權或智慧財產權規範，此也間接說明了大數據科技的發展似乎不太需要個資財產權化的刺激即可快速成長。[32]

相對的，個資財產權化將會伴隨著法規遵循與業界就個資交流合作時的複雜化程度。個資所有者與個資當事人的權利也將產生拉鋸，使資訊市場對權利人

---

[30] Determann, *supra* note 27, at 22-25.

[31] Margaret Jane Radin, *A Comment on Information Propertization and Its Legal Milieu*, 54 Clev. St. L. Rev. 23, 23-26 (2006).

[32] Determann, *supra* note 27, at 34-37.

doi:10.6342/NTU202002857

的歸屬確認產生困難。同時，還有可能產生如專利蟑螂般的個資蟑螂，使個資大數據的發展增加許多不必要的成本。

再者，個資財產權化可能將與個資保護法保護個資主體尊嚴與人格的基本目的相悖。個資一旦財產權化，個資將可因為買賣、讓與等法律行為使個資當事人被迫無法再擁有、管理或利用其關於他（她）個人的資料，並且透過個資所有者的再交易，個資將可能受個資當事人不熟識之第三方完全控制，排除個資當事人利用自己個資的現象，此現象亦不合乎資訊隱私法規範之目的。

個資財產權化的最重要目的之一，是希望個資當事人能因此獲得個資蒐集者與利用者的金錢對價補償，但個資財產權化無可避免地將產生財產權管制的行政成本，甚至需要立法者訂定補償個資當事人的最低給付標準等規範，此對於需要大量利用個資的網路科技業來說，將造成營運成本的大幅增加或成本轉嫁予消費者的結果，反而可能使個人原本可自網路業者享受的免費服務不覆存在。再者，又因為財產權所有人通常僅能獲得補償性或賠償性質的責任權利，在某些情況下個資當事人將可能被迫放棄其個資財產，加再上政府對財產固有的徵收與干預等權利，最終可能損及個資當事人的實質利益[33]。

除此之外，尚有一些細微卻值得思考的批評論點，例如，資訊的蒐集與流通本身多被認為是屬於言論自由的重要一環，原因是個資的蒐集與接收將有助人民提升知識，使人民進行各項活動與評論。而個資財產權化的結果將使個資資訊被掌控在某些人手裡，可能阻礙資訊的流通，故有稱已違反言論自由之基本人權。又例如，對維安公權力的執行也將產生一些不必要的阻礙，為推廣科技辦案，許多城市已布滿監視設備，紀錄交通要道或治安管控區域等人流動態，個資財產權

[33] *Id.* at 37-38.

doi:10.6342/NTU202002857

化的結果也將使這些個人資料在利用上更加的不便與複雜。另從公平競爭法角度而言，由於個資財產權化將使個資流動性降低，為個資控制者及所有者塑造更高程度的競爭壁壘，勢必將增加資訊經濟規模獨佔或壟斷的可能與危險。再者，個資當事人因個資轉讓所產生的個人收益及稅收，亦會是行政規範上的難題[34]。綜上所述，個資似乎不應以財產權規範，也就是說，個資不應隸屬於任何人或實體。

第四節 言論自由與資訊隱私規範的衝突與調和

政府立法限制個人資訊的蒐集與利用所遭受到最大的挑戰之一即來自人民的言論自由基本權，本節主要討論隱私資訊的利用限制如何與言論自由權相抵觸，政府又在哪些理論基礎下得以介入規制，以及所涉公共利益正當性之討論。

第一項 網路業者對個資的使用是否受言論自由的保護？

幾乎所有民主國家均以憲法層級法規範保障人民的言論自由，在言論自由保障的基礎上，人民得自由地對其所獲知之資訊加以評論或進行應用，而網路業者應用所蒐集資訊的行為，無論是應用於大數據分析個資以獲知潛在目標客戶並加以行銷，亦或將其所蒐集之個資或資訊分析結果銷售予他方，使其進行與用戶不具直接利害關係之研究等行為（例如瞭解某選區政治傾向，或者預估選舉投票結果等），誠屬憲法所保護之言論自由範疇，只要該等資訊為真實，又不對個資當事人造成名譽的毀損或威脅，豈有予以限制或禁止之道理？

美國法學者 Engene Volokh 認為，那些限制網路業者不得銷售或揭露所蒐集之個資的個資隱私規範，有違反美國憲法第一條修正案關於言論自由保障規範

[34] *Id.* at 38-42.

doi:10.6342/NTU202002857

之虞[35]。對於因為隱私權的規範限制，使個人不能被談論，甚至就連關於個人的真實訊息也不能被自由談論的規定，Engene Volokh 主張，隱私權規範對於憲法第一條修正案言論自由的侵害，並不能僅因為該資訊相關私人事務而即應當被合理化或忽視[36]。

然而，亦有論者對於將網路業者對個資蒐集、使用、分析或銷售行為歸屬於「言論自由」的看法提出了批評，批評者主要認為，對網路業者而言，其所蒐集與利用的個人資訊本質上應該是「商品」，而不是「言論」，故不應受憲法言論自由的保護。就此等區分，美國大法官 Justice Kennedy 提出反面質疑，他認為言論自由所保護的言論，並不應該因為言論的「形式」而有所差別，例如，當期刊發表文章包含某「統計資料」時，並不能稱該統計資料並不是文章本文言論，即斷言不受言論自由的保護[37]。此說法似乎意指，言論自由除了保護言論本身的自由外，尚還包括其它有助言論發表或思想表達的條件。

第二項 商業言論（Commercial Speech）論點

為合理化政府以隱私權規範，適度限制網路業者仗著言論自由理論而無限制利用與揭露個資的作為，美國有論者提出應以商業言論看待網路業者處理、應用及銷售合法取得個資之行為。在美國，就商業言論的言論自由程度已有相當期間的爭辯，主要爭執商業言論是否應該受到某種程度的限制，司法應該以何種審查標準來檢驗一個對商業言論限制的法規是否已侵犯憲法所保障之言論自由。

---

[35] Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You.* Available at SSRN: https://ssrn.com/abstract=200469 (最後瀏覽日: 2020/4/1).

[36] *Id.* at 48-51.

[37] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1196 (2016).

doi:10.6342/NTU202002857

對於商業言論是否受到憲法言論自由保障的議題，美國最高法院在態度與觀點上曾產生過數次的反覆轉變，歸納上來看，相關商業言論判例的發展大致依序可以分為以下幾個階段：商業言論不獲保障、商業言論獲得保障與價值基礎、商業言論只獲得較低程度保障、商業言論審理標準的形成、以及商業言論審理標準受到挑戰等五個不同階段[38]。

然而，商業言論終究只能解決資訊隱私規範之於言論自由衝突的少部分問題，原因是因為判斷言論是否屬商業言論之定性，通常系以言論本身的內容意涵來觀察，亦即是去辨別系爭言論所涉及之社會目的是否系為促進某商業交易，但與言論是否為商業機構所發表並無直接關聯，例如，商業週刊上的訂閱廣告與優惠方案，屬商業言論，但是商業週刊上所刊載的公共議題文章，則非屬商業言論。應用於本文議題而言，網路業者對於個資的蒐集、分析或分享等行為，也並不必然就是為促進商業交易，例如 Google 若將某區域人口的政治傾向大數據分析揭露給某侯選陣營，則並非為促使商業交易之態樣。準此以觀，以商業言論分類來合理化資訊隱私規範，試圖解釋商業個資大數據應用與言論自由保護衝突的觀點，並非合乎常理[39]。

第三項 合約約束模式觀點

當網路業者與個人用戶以合約約定所揭露之個資資訊不得加以分析、利用或再揭露予他方時，若個人以此約定要求網路業者履行約定之承諾，則對網路業者的限制自然不違反憲法所保障之言論自由。事實上，目前多數網路業者對於個資的處理即是以此方式進行，網路業者向個人用戶公告其資訊處理政策，以此政

[38] 賴祥蔚（2010 年 6 月），〈商業言論與憲法的言論自由保障〉，《台灣政治學刊》第十四卷第一期，頁 168。

[39] Balkin, *supra* note 37, at 1197-1199.

doi:10.6342/NTU202002857

策向個資當事人承諾將不會向不關聯之他方任意揭露其個資，當個資當事人使用其服務時，即等同與網路業者締結完成包含該政策內容之合約。

但很顯然的，以合約義務觀點處理資訊隱私的不當利用、分析與揭露的方式，在實際執行上存在若干嚴重的問題。首先，網路業者容易在所承諾的隱私政策上使用很模糊或迂迴的敘述語言，一般個人難以理解，試想多少次我們真正認真讀過網站上的個資隱私政策？甚至該資訊處理政策上可能還藏有資訊控制者得隨時單方面變更與取消政策內容的約定，又或者政策內容含有廣泛的免責事由設計等條款內容，都使得一般個資當事人容易不自主忽略。即使個人仔細閱讀網站隱私政策，又有多少人能真正瞭解個資被利用或揭露後所可能帶來的損害與風險呢？

合約約束觀點其實是將個資視為個人的財產，個資當事人得同意或不同意資訊蒐集者對其財產的利用、分析或轉交付，若未約定，則適用合法取得資訊的個資蒐集者得以自由使用、分析與向它人揭露的默認規則，如此與言論自由規範自然無違。然而，就過去的實際案例而言，個人直接以合約違反之主張對網路業者起訴成功的案例卻相當罕見，即使是在民事訴訟頻繁的國家如美國，多數關於消費者隱私資訊遭受侵害的案件，還是多由 FTC 依相關行政規則或法規之違反來執行與制止[40]。

至於如何以合約約束模式來解釋那些已經被法規所限制揭露資訊的問題，例如醫療相關法規要求醫療機構必須對病患資料擔負保密責任，又例如金融相關法規要求金融機構必須對客戶之財務資料擔負保密責任等，對此學者 Volokh 主張，就該類對隱私訊息的揭露限制，縱使未明文以合約與客戶約定，但仍可歸

[40] *Id.* at 1200.

doi:10.6342/NTU202002857

類為合約的默示條款[41]。Volokh 認為，這些保密義務都是任何業者與客戶基於過往交易經驗均可合理預期的約定，故可被視為合約條件的一部分。

Volokh 的論點固然看似合理，但仍存在若干未能解決的衝突：首先，若將上述保密約定視為默示條款，基於契約自由原則，當事人應可自由地於合約約定時予以否定，若遭否定，則原先規定即無法產生保護用戶隱私資訊的效用，但事實卻不是如此。第二，無論是醫療或金融機構，協力處理客戶資訊者應還包含許多週邊相關組織，但通常僅原與個資當事人建立法律關係的資訊蒐集者間會有所謂的合約約定，那些週邊相關組織與個資當事人間並無契約關係，自然也難以適用原合約默示條款的約束。第三，默示條款觀念上僅適用於既有且長期營運的商業關係，對於新創公司與新營運活動而言，則難謂有因習慣而成立的默示條款之應用[42]，又甚至有時那些個資保密規則其實並非屬合約中自然被雙方所討論與約定之項目[43]。從前述的觀念分析，可看出那些所謂默示的保密義務，本質上應該較屬於民法上的侵權禁止性質之規範，而非僅為屬商業活動中雙方間自由形成的權利義務約定[44]。

第四項 加諸個資控制者資訊受託義務責任是否即侵害其言論自由？

言論自由系為保護民主，但其內涵不僅是使人民得自由談論政治議題，它還包含確保人民可自由的談論與聽取/近用除政治以外的任何議題，這是因為人民的觀念培養系透過人與人間的各種互動而產生，人際間對於各種議題的自由表

---

[41] Volokh, *supra* note 35, at 8 (“In many contexts, people reasonably expect — because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract — that part of what their contracting partner is promising is confidentiality.”)

[42] Balkin, *supra* note 37, at 1201.

[43] *Id.* at 1202.

[44] *Id.* at 1204.

doi:10.6342/NTU202002857

述與聽取/近用將有助形成一個民主社會，民主社會將形成某種社會風氣或偏好，人民生活在民主社會並受該社會風氣或偏好所影響，人民在民主社會裡養成各種自我意識，故藉言論自由形成民主社會的過程也應受憲法言論自由的保護[45]。

然而，並非社會上所有的言論均為影響整體民主社會風氣與偏好，有些言論僅是為使雙方或多方間完成某些特定商業目的，例如當某人利用華麗的說辭或具說服性言論向他人要約，或引誘締結契約，則該言論即非完全屬言論自由所保護的言論，相對地，言論自由所要保護的是，民眾可聽取與近用該商業言論的言論自由，而商業言論之所以對民眾有價值，就必須確保該言論至少是真實或至少是不致於誤導民眾的言論，因此政府為此可予以規制，例如消費者保護法、公平交易法中對商業行為與言論的規範與限制即屬此類。這也解釋了為什麼政府可以干預廠商在其商品上的標示方式與內容、限制金融機構對民眾的廣告用語等。言論自由保護民眾接收與近用各類商業訊息的自由，也即是憲法言論自由的重要內涵之一[46]。

同樣地，當言論發表者與接收者間存在一受託責任關係時，言論發表者與接受者間通常存在一個資訊不對稱的現象，也就是接收者信賴發表者的某種專業知識與能力，接收者沒有足夠能力得以判斷言論之真偽，在這樣的情況下，若政府對該類言論不加以規制，言論發表者即容易利用言論接收者的無知與信賴基礎，誤導或甚至欺瞞言論接收者，對言論接收者造成傷害，故政府即應採取作為保護言論接收者。換句話說，該言論是否受到憲法言論自由的保護，並不是取決於言論本身的內容，而是基於言論發表者與接受者的關係。當然，若言論發表者與接受者間不具有任何信賴或其它具意義的商業關係，則該言論即應當受憲法

[45] *Id.* at 1212.

[46] *Id.* at 1213-1214.

doi:10.6342/NTU202002857

言論自由的保護，政府即不應干預。

網路業者相對於個人用戶而言，不但經常存在某種商業關係，且當個人提供隱私資訊予網路業者時，從前文分析可得知，網路業者與個資當人間應存在著某程度的資訊受託者關係，是以，網路業者對於資訊的蒐集、利用、分享等行為則並非一般的公眾言論，難稱仍完全在憲法言論自由保護之範疇內，所以，政府基於保護資訊不對稱現象下居於劣勢的個人，當可對網路業者言論加以規制，並不致生憲法言論自由侵害的疑慮[47]。

第五項 被遺忘權（Right to be Forgotten）與言論自由

根據歐盟相關被遺忘權之規定，當個資當事人要求資訊控制者刪除跟他（她）個人有關的資料時，除非根據各國當地法律之定義與規定，該資料系為自由表達權利所必要，或者該資料的處理僅為新聞、藝術或文學表達目的，否則，資訊控制者必須立即刪除該個人資料。歐盟規範把舉證責任加置於資訊控制者身上，資訊控制者必須證明，縱然系爭資料令當事人困窘，但仍具有合法的新聞、文學或藝術等價值或目的等。這個被遺忘權除了可對在歐盟的資訊控制者主張外，在歐盟法院的 Google Spain v. AEPD 判決中[48]，法院確認甚至可視個案情形要求搜索引擎網站 Google 刪除相關鏈結，以及將置放於歐盟地區以外的相關個資也刪除。理由是，無論個資置放於何處，察看個人認為不相關聯的個資已經侵犯個資當事人的隱私權[49]。本判決招致部分歷史學家的異議，他們認為若過往相關資訊全面

---

[47] *Id.* at 1218-1220.

[48] Google Spain SL v. Agencia Española de Proteccíon de Datos ¶ 93, (Court of Justice of the European Union, Case C 131/12).

[49] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the Implementation of the Court of Justice of the European Union Judgment in "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles C-131/12" 3 (Nov. 26, 2014). Retrieved

doi:10.6342/NTU202002857

遭到刪除，將使得還原歷史社會真實面貌的工作變得相當困難。然而，該判決也強調，Google 必需要適當衡平資料當事人個資移除請求的利益與其它包含公眾近用資訊等利益，也就是說，刪除義務僅限於不相關社會價值的個人負面資訊[50]。（本文將相關被遺忘權討論置於第三章第二節討論。）

對此，美國持與歐盟不同的態度，美國觀點認為被遺忘權的規定根本上與美國憲法第一條修正案的言論自由相抵觸，因為公開發表某人真實的犯罪紀錄受美國第一條修正案言論自由所保護[51]。美國法認為，若僅依他人的要求即刪除第三人的言論發表，顯然有違言論自由的基本精神，美國聯邦最高法院已確認，只要是合法取得的訊息，僅管該訊息令某些人感覺困窘，美國各州不得立法限制媒體散布真實訊息[52]。Google 公司的隱私總顧問對此議題認為，因為被遺忘權規定不僅適用於資料當事人自主同意揭露的個資，還同時適用於所有可在網路上查找到的個資，因此將會對言論自由帶來很大的威脅[53]。然而，社會學家們認為，落實被遺忘權的結果將使資訊蒐集系統採以匿名資訊的預設設置，因此將使世界喪失許多資訊[54]。學者 Mitrou 與 Karyda 則提出較為折中的觀點，認為被遺忘

---

from https://www.pdpjournals.com/docs/88502.pdf (最後瀏覽日: 2020/5/1). ("In order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. . . . In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.")

[50] Ludo Gorzeman & Paulan Korenhof, *Escaping The Panopticon Over Time*, Phil & Technol 30, 73-92 (2017).

[51] Rosen, *supra* note 4, at 180 (2012).

[52] *Id.* at 181.

[53] Jeffrey Rosen, *The Right To Be Forgotten,* 64 Stan. L. Rev. Online 88, 89-90 (2012).

[54] Bernd Malle, Peter Kieseberg, Edgar Weippl, et al. *The Right To Be Forgotten: Towards Machine Learning On Perturbed Knowledge Bases,* International Conference on Availability, Reliability, and Security, 251–266 (2016).

doi:10.6342/NTU202002857

權並不等同於對於歷史的完全抹滅，況且，對社會與歷史探索利益的追求，並不高過因強迫個人承受困窘個資所帶給個人的極大不利益[55]。

第六項 保護智慧財產權規範對言論自由的挑戰

美國於 1998 年通過 Digital Millennium Copyright Act (DCMA) 法規，要求網路業者在收到權利人的侵權主張時，必須移除相關內容。又 The Online Copyright Infringement Liability Limitation Act (DCMA 的一部分)授權行政部門對那些協助侵權的網路業者罰款，該法規提供給網路業者一個安全港規定(safe harbor rule)，若網路業者在收到侵權通知後立即採取行動刪除侵權的內容，則網路業者即可免責。權利人如此簡捷的挑戰方式對於網路業者的言論自由確實造成一些威脅，且可能被競爭業者挪用作為阻礙其著作推廣的活動，例如，網路業者 YouTube 在網站上放置某 Youtuber 自製拍攝的影片，當其它競爭者 Youtuber 或著作權人向網路業者主張其影片含有侵權內容時，網路業者為了免責，即可能直接刪除所指影片[56]，此被認為有侵害言論自由的疑慮。

亦有認為以上所述競爭，其實不僅止於是內容創作者間的競爭，更應該是新舊媒體間（或新舊商業模式間）的競爭，傳統內容製作公司耗費大量資源製作內容，並靠著向觀眾收取授權費以維持營運，但新電子媒體如 YouTube 或相關網路平台業者卻僅是提供空間供他人置放創作內容，即可擁有大量流量，賺取豐厚的廣告費用收入，並且導致消費者不再直接向舊媒體購買或租賃創作內容，改變

---

[55] Lilian Mitrou & Maria Karyda, *EU's data protection reform and the right to be forgotten: A legal response to a technological challenge?* 5th International Conference of Information Law and Ethics (2012). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245 (最後瀏覽日: 2020/4/2).

[56] Jeffrey Rosen, *supra* note 4, at 183.

doi:10.6342/NTU202002857

觀看習慣僅使用網路業者的線上服務，以極低的成本滿足了原有的娛樂需求，故舊媒體利用此智權保護法規以為商業利益競爭手段，企圖阻礙競爭網路產業的未來發展[57]。短期間來看，助長網路事業的發展可能讓消費者節省了荷包，但長期來看，傳統的內容製作業者可能再也沒有豐沛的財源得以支持創新著作的製作成本與開銷，因而降低著作品質或者甚至停止產出新著作，此結果對消費者來說也不見得是一件好事。而對於資訊隱私權的保護亦同，強制規範的同時應考量，是否已可能將被產業競爭者用作商業利益競爭之手段。

第五節 通知與選擇（notice-and-choice）規範主流的形成

個資當事人同意機制之目的系在於提供個資蒐集者或控制者一個合法蒐集、利用或移轉個資的理由。雖然各國相關法規可能均訂有各種使個資控制者得處理個資的規定，但基於人民自治與民主的主流觀念，當事人同意機制在各國個資隱私規範下均是相當重要的一個合法基礎。

當事人「同意」有許多種不同的形式，處理風險事務上最常被使用的概念即是「知情同意」(Informed consent)，即是當事人在被充分告知並瞭解背景事實、含意及後果等情形下而做的決定。知情同意的機制可溯至二次世界大戰前德國紐倫堡公約(the Nuremberg Code)對受試驗者所訂定的同意標準，當時認為知情同意不僅是為保障受試驗者在安全、受保護與有尊嚴的條件下受試，也是試驗本身完整性的一部分[58]。知情同意的形式包含明示或暗示同意、積極或消極同意與書面或口頭同意等。積極同意指當事人須採取行動給予同意的表示，例如回答具體同意與否的問題等，現行應用於隱私規範的選擇加入（Opt-in）即是積極同意

[57] *Id.* at 184-185.

[58] Ilka H. Gleibs, *Turning virtual public spaces into laboratories: thoughts on conducting online field studies using social network sites*, 14 Anal. Soc. Issues Public Policy 352, 356 (2014).

doi:10.6342/NTU202002857

的一種表現。另一方面，「概括同意」（broad consent）是指當事人同意潛在未知的應用，被廣泛應用於生物技術試驗領域，當事人同意試驗機構可基於未來研究原因使用當事人所提供之生物樣本。事實上大數據科技的應用在性質上與前述應頗為相似，因為科技進步的發展未知，許多事實背景與風險並無法在個資蒐集時即被瞭解與確定，故個資當事人的概括同意將有助創新技術研究與發展[59]。

通知與選擇（notice-and-choice）系為以個人對自我資訊「主宰控制、管理」權力為基礎下所衍生出的資訊隱私規範。在美國，通知與選擇（notice-and-choice）源起於 1973 年美國聯邦家庭教育福利部（Department of Housing, Education, and Welfare）的一則報告[60]，其中提及以 Fair Information Practices Principles（FIPPs）為核心的個資處理原則，FIPPs 指出：「不應存在有任何秘密而不為人知悉的個資蒐集與紀錄保存活動，任何組織都應該有相關個資蒐集與紀錄『公開』的政策」[61]。該報告要求任何政府機關蒐集市民資訊時皆必須公告資訊使用方法及目的，使市民得以修正他（她）們的個人資訊，並且在使用資訊予其它目的前均應徵得個別市民的同意。亦即，「通知與選擇」機制的本意在於落實個資蒐集與紀錄活動的公開。FIPPs 並不是一個立法規範，而是提供一個在衡平隱私需要與其它利益衝突下的一個框架性原則[62]。在經濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）於 1980 年發表 Guidelines Governing the

---

[59] Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, 4 J. Cybersecur. 1, 5 (2018).

[60] U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).

[61] U.S. Department of Health, Education, and Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973). Retrieved from http://epic.org/privacy/hew1973report/default.html. (最後瀏覽日: 2020/5/1).

[62] Government Accountability Office, In-car Location-based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers (GAO-14-81) (Dec. 6, 2013).

doi:10.6342/NTU202002857

Protection of Privacy and Transborder Data Flow of Personal Data 一文後[63]，「通知」機制開始被國際間廣泛地應用於資訊隱私相關立法規範，各國相關資訊隱私的法規、國際合約、產業作業準則以及歐盟資料保護綱領（European Union's Directive 95/46/EC: the Data Protection Directive）等均以該文為基礎，設置以「通知」機制為標準的資訊隱私規範。美國 FTC 隨後遊說國會通過法律，要求私人企業也須公告其使用或處理個人資訊的方式、時機以及種類項目等。美國雖然沒有全國統一的資訊隱私法規，但聯邦政府與各州已就某些特定資訊類別訂定類似要求通知與選擇（notice-and-choice）的資訊隱私規範[64]。例如，美國加州的線上隱私保護法案（Online Privacy Protection Act）要求所有商業網站或其它透過網路提供服務而須蒐集加州市民資訊的網站，均須公告資訊使用政策，並且遵照該方法處理資訊，而所公告資訊處理政策必需描述所蒐集資訊的種類、分享的對象、資訊使用的方法，以及當資訊處理政策改變時，個資當事人將如何被告知等訊息[65]。雖然是加州法律，但因為網路商業網站有州際交易的本質，而且又是全美國資訊科技業最集中的加州地區之法律，該法律即等同間接對全美國網路商業經營業者要求設置資訊隱私政策之「通知」機制。而我國個人資料保護法則仿效歐盟資料保護綱領令規定，於個資法第 7 條、第 8 條、第 9 條、第 15 條、第 16 條、第 19 條及第 20 條等均有告知後同意原則之規定。

---

[63] Organization for Economic Co-operation and Development, Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data. Retrieved from https://www.google.com/url?client=internal-element-cse&cx=012432601748511391518:xzeadub0b0a&q=https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm&sa=U&ved=2ahUKEwjV1rXhyKPoAhXMKqYKHZTbC7IQFjAAegQIBBAB&usg=AOvVaw0u40M6DQHlqVK7LJ-EilOM (最後瀏覽日: 2020/3/18).

[64] Daniel J. Solove & Paul M. Schwartz, Information Privacy Law, 37–39 (4th ed., 2011).

[65] See Cal. Bus. & Prof. Code §§ 22575–22579 (West 2017).

doi:10.6342/NTU202002857

美國 FTC 一直以來把資訊隱私規範的執法重點放在資訊蒐集者對個資當事人在資訊處理準則的通知上，要求資訊蒐集者必須依法詳盡、完整地羅列資訊處理的程序與作業準則。早期在美國有以產業別而發展的隱私政策自治導引，在同產業的所有業者被鼓勵採行某些相同資訊處理與隱私政策，例如在西元 1988 年成立的一個非官方組織—線上隱私聯盟（Online Privacy Alliance），它制定了一系列適用於網路環境的行為準則，並要求所有會員採用及公告一個固定的資訊隱私公告，強調業者應「通知」個資當事人關於資訊使用目的、傳送、近用、修正、資訊安全以及幼童資料的蒐集與限制等[66]。如此的產業行為準則雖非可被直接執行的法規範，但 FTC 據此準則為執法規範標準，若資訊蒐集者未向個資當事人揭露詳實具體的資訊處理程序準則，或實際上未依照所公告之處理程序準則處理資訊[67]，FTC 則予以起訴，惟迄今多數案例多以和解作收，和解條件通常系為要求資訊蒐集者修正公告之資訊處理程序準則，並以不違背準則之方式處理個人資訊[68]，操作目的仍在使個資當事人能夠在完全知情的情況下做出對業者揭露個資或自由選擇另尋替代業者的決定。

---

[66] Privacy Alliance, Guidelines for Online Privacy Policies. Retrieved from http://www.privacyalliance.org/resources (最後瀏覽日: 3/19/2020).（註：OPA 現已不存續。）

[67] 美國聯邦貿易委員會執行之法源依據為，Federal Trade Commission Act 第五章授權委員會調查並遏止可能影響州際間商業活動的任何「不公平」或「欺騙」的行為。See, 15 U.S.C § 45 (2012).

[68] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 610-11, 614-619 (2014).

doi:10.6342/NTU202002857

第三章 美國與歐盟資訊隱私規範概述

本章主要討論世界二大規範體系–美國與歐盟於處理資訊隱私問題上的基礎思維與立場，美國法原則上系自消費者保護立場介入資訊隱私規制，歐盟則將個資隱私上綱人民基本權利範疇，視個資隱私環境為人民生活品質的一環。基此，美國與歐盟在資訊隱私實體法的應用上具有顯著差異，也分別影響兩地區私部門企業在個人資料處理上所採行的不同策略與態度。近年歐盟積極藉由廣大市場影響力企圖將其資訊隱私法規範「出口」至世界其它國家與地區，加上歐盟規範的直球設計，使它國在法規參酌或移植上相對容易與便利，世界緒多國家近年改採或增加與歐盟之硬性、明文化資訊隱私規範相仿之規制。然而，歐盟式的強制規範卻對於大數據應用，尤其是人工智慧 AI 大數據分析產業之發展帶來不小的衝擊與阻礙，影響所及不僅是 AI 產業選擇避免立基歐盟，更影響未來 AI 技術應用發展所能為人民創造的福祉。

第一節 美國資訊隱私規範

在美國聯邦憲法裡，關於美國權利法案條文並未明文將人民資訊隱私權之保障列於其中[69]，而與隱私權較為相關的僅為保障人民免於不合理搜索與扣押的憲法第四條增補條文，與第十四條增補條文中所保障的正當法律程序，然而，聯邦法院的長年判決意見中均不見正面肯認此即代表聯邦憲法確有保障人民資訊隱私，至多僅以推定該權存在的方式判斷爭議法規是否違反人民之資訊隱私權[70]。

[69] 相對而言，美國部分州於憲法中已明確賦予隱私權憲法保障，包括 Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina 等州明文承認隱私權之保障。

[70] 顏于嘉（2017），〈由美國資訊隱私法制觀察被遺忘權在美國的發展〉，《萬國法律》，第 211 期，頁 26-27。

doi:10.6342/NTU202002857

在法律位階上，美國並沒有一部統一規範個人資料隱私保護的法律，但對於某些特定領域或產業則有特殊規範分別就相關個資處理的限制與方法予以規範，例如在健康醫療、財務金融與兒童個資等部門領域均設置有專法規範資訊隱私處理原則。舉例而言，在健康領域個資處理上，Healthcare Insurance Portability and Accessibility Act of 1996 法案規範了醫療保健業者處理具個人識別性資料的準則，它列舉了業者可使用或揭露個人健康資訊的時機情況，並且要求業者採取某類特殊通訊協定及方法來保護個資免於遭不法近用、利用或洩露[71]，若必要揭露個資，亦規定必需在最少必要性(minimum necessity)的標準下揭露[72]。在財務金融領域個資規範上，例如 Fair Credit Reporting Act 規定消費者信評機構要採以公平合理的評量方法，並需要在保密的條件下利用信評資訊，消費者有知悉其信評報告的權利，而且機構只能在符合列舉目的與必要的範圍內揭露個人信評資訊予合規的資訊需求者[73]。在兒童個資規範上，美國早期有以 Fair Information Practice Principles 將關於兒童資料蒐集的原則成文化規範，1998 年立法的 Children's Online Privacy Protection Act 增加了許多明確的規定，例如除非得到兒童父母親的同意，否則禁止業者蒐集 13 歲以下兒童的個資[74]，並且兒童父母親有權要求個資蒐集者銷毀該兒童資料[75]。

美國聯邦最高法院在處理隱私爭議案件時，肯認隱私是含有眾多不同利益保障的權利以及多面向權利意涵的概念，於司法見解上將隱私權區分為三種類型：(1) 親密性事務的自主決定隱私權類別，包含婚姻、生育、避孕、性傾向、

---

[71] See 45 C.F.R. §§ 164.500, 506 (2019).

[72] See 45 C.F.R. § 164.502(b) (2019).

[73] See 15 U.S.C. § 1681 (2012).

[74] See 15 U.S.C. §§ 6501-6506 (2012).

[75] See 16 C.F.R. § 312.6 (2019).

doi:10.6342/NTU202002857

家庭關係、兒童扶育等事務與議題；(2) 空間隱私權或身體隱私權類別，包含個人私密空間與身體不受政府機關不合理侵擾、搜索與扣押範疇；(3) 資訊隱私權類別，包含個人資訊免於被政府強迫揭露的侵害，以及個人得以主宰控制其個資的權利[76]。本文所探討之主題即為上述第三種類型之隱私。然而，美國司法在資訊隱私案件的法規範應用上，卻經常援引其它二類隱私案件的分析方法與法理邏輯作為資訊隱私案件的判解基礎。

美國憲法第四條修正案保障人民有免於受無正當理由搜索與奪取的權力，此權利被擴大解釋為對人民私密性通話、郵件及個資等隱私訊息的保護，但美國憲法及修正案依憲政體制僅能管轄政府機關行為，對於非屬政府組織的資訊蒐集者，人民是否有權利要求其保護個資的議題，在西元 1979 年著名的聯邦最高法院案例 Smith v. Maryland[77]中獲得了較明確的判別準則，該案多數法官認為，一旦個人將其個人資訊揭露給他方，個人即不能合理地期待資訊接收方將不再轉洩露給第三方或利用該資訊。也就是說，個人因為主動揭露已失去資訊隱私的司法保護，個人不能合理期待他方為其保密。值此，在美國過去資訊隱私的司法案件中，個資當事人能否「合理期待」所揭露個資的持續秘密性，成為相當關鍵的司法裁判要件。

就私部門是否有為個人個資承擔保密義務的議題，通常僅能依賴私部門與個人間的相關個資保密的合約約定，若私部門向個人保證採取某些手段為其保護個資，則私部門即必須遵守履行是項保密承諾。在美國通常由 FTC 對私部門企業進行相關行為的違約調查，惟對於違反約定的私人企業，除了少數造成嚴重

[76] 張陳弘（2018），〈新興科技下的資訊隱私保護:「告知後同意原則」的侷限性與修正方法之提出〉，《臺大法學論叢》，第 47 卷第 1 期，頁 242-43。

[77] Smith v. Maryland, 442 U.S. 735 (1979).

doi:10.6342/NTU202002857

後果的案例外，通常 FTC 的處理方法也僅止於要求私部門設置完善個資處理機制，或要求其嚴格落實與個資當事人間的保密義務約定。

近年 FTC 對於私部門因違反保密約定而裁罰的著名案例之一為臉書與劍橋分析公司的個資洩露醜聞案（Cambridge Analytica Scandal），在該案，劍橋分析公司(Cambridge Analytica Ltd.) 建置了一個性格分析 APP 來蒐集個資，且非法自臉書 Facebook 取得 5000 萬個用戶資料，透過 Facebook、Google、Twitter、YouTube 等數據建立用戶資料之分析模型與演算法進行分析，於 2016 年美國總統大選期間，針對這些用戶選民在各社群媒體投放各式各樣的假新聞及個人化廣告，企圖影響中間選民使他們能夠支持某特定候選人。FTC 調查後認為 Facebook 違反其與用戶間的保密約定，非法分享用戶資料予他方，FTC 最終決定裁罰 Facebook 五百萬美元，但即使是如此鉅額的罰金，對於 Facebook 的營運與財務則似乎未能產生任何衝擊，也不見 Facebook 因此改變它利用用戶資訊營利的營運模式[78]。

美國加州於西元 2018 年 6 月 28 日立法通過一個較類似歐盟 GDPR 的隱私資料保護規範--加州消費者隱私保護法案（California Consumer Privacy Act, CCPA），該法案已於 2020 年 1 月 1 日生效。然而 CCPA 對於違規的處罰力道不若 GDPR 重，且 CCPA 對於企業規範的範圍也不若 GDPR 廣泛，例如，CCPA 在個資的定義上，在某些情況下僅考慮由消費者提供的資訊，並不包括向第三方購買或透過第三方獲取的個資，但 GDPR 並未對此加以區分，GDPR 涵蓋了所有個資資訊，無論該資訊的來源為何[79]。縱使細部規範異於 GDPR，但 CCPA 仍

[78] Jennifer Golbeck, Taking Control of Your Personal Data, 101-103 (2020).

[79] David Zetonny, California Consumer Privacy Act (CCPA) Practical Guide, Bryan Cave Leighton Paisner LLP (2019). Retrieved from https://ccpa-info.com/wp-content/uploads/2019/09/bclp-practical-guide-to-the-ccpa.pdf (最後瀏覽日: 3/19/2020)

doi:10.6342/NTU202002857

是以一個異於以往美國法規範，而改採較為「一致性」的資訊隱私規範方式，使該州州民擁要較多對其個資的主宰控制能力。(重要規定比較請參考本文［附件一］。)

第二節 歐盟資訊隱私規範

相對於美國法而言，歐盟的個人資訊隱私規範則較為嚴苛。學者認為原因之一為在當時納粹大屠殺事件中，荷蘭因為對人口及人民活動資料維護較完整，使荷蘭猶太人被大量的殺害，而其它國家則因為保存較少的人民及活動資訊，使它國猶太人存活率明顯較高。另一個原因為，歐盟視個人隱私的保護狀況為人民生活品質條件之一，歐盟人民也普遍認為，當地完整的資訊隱私保護規範將有助於促進商業活動[80]。

在歐盟法的大架構下，人民的隱私被視為是「人民的基本權利」，歐盟基本權利憲章（European Charter of Fundamental Rights）第八條即明文規定：人人均享有個人資料保護的權利[81]。從另一個角度可解讀為，人民應擁有描述關於他(她)個人的所有資料。在歐盟一般資料保護規範 GDPR 施行以前，關於個資保護主要規範於歐盟資料保護指令 (European Union Data Protection Directive)，歐盟隱私規範大多同時適用於公部門與私部門，並且是不分產業別的一體適用(此與美國法區分產業的差別適用法則大不相同)，該指令所規範的資訊，包含任何具個人識別性的資料，雖然說該指令本身並不當然具有執行力，需由歐盟各國自行決定是否參照該指令制定國內法以執行相關規範，然而自 1995 年該指令發佈以來，

[80] Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy, 306-307 (2016).

[81] Charter of Fundamental Rights of The European Union. (Article 8 - Protection of Personal Data, "Everyone has the right to the protection of personal data concerning him or her.") Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf (最後瀏覽日: 2020/2/21).

doi:10.6342/NTU202002857

所有歐盟國家均已參照該指令制定法規制定個資保護與處理方法。

歐盟法與美國法的另一重大差異在於個資處理的預設規定，在美國法下，除非違反法律規定，私部門基本上得自由地運用所有合法取得的任何個資；但在歐盟法下的預設規範是，除非所取得的個資已符合個資法規所要求的各種規範，否則私部門不得任意予以處理或運用。歐盟資料保護指令明文規定，任何個資的蒐集都必須有明確且合法的目的，對於私部門而言，合法目的通常是指履行契約義務的必要行為，歐盟資料保護指令並且明文要求資料蒐集者不得儲存個資超過必要或法規範的期限、必須向個人告知與解釋個資蒐集之目的以及個資處理的過程與方法等，亦有規定私部門須確保資料當事人得近用、檢視、修正其個資，且個資當事人應有拒絕私部門向第三方揭露其個資的權利[82]。

於西元 2018 年生效的 GDPR，更是一部可直接適用執行於所有歐盟國家的法規，相較於需由歐盟各國制定國內法律才得以執行的歐盟資料保護指令而言，GDPR 的統一適用將有益於跨國公司制定其隱私規範政策與進行法遵作業。同時，GDPR 又加強確立了歐盟市民對其個資的掌控權利，GDPR 一方面加重對個資蒐集者與控制者違法的罰責，一方面使歐盟市民有權力要求資料蒐集者與控制者必需使個資當事人知悉與管控與其個資相關之狀態、分享、利用與刪除等作為，並且無論資料蒐集者是否為歐盟企業，只要個資當事人為歐盟市民，都強制要求一併適用該規範[83]，影響甚廣，舉例而言，GDPR 實施後，臉書 Facebook 已為歐盟市民開啟一個可以完全下載個人所有留存在 Facebook 紀錄檔個人資料的功能[84]。以下僅就與本文主題最相關部分規定提出討論。

---

[82] Hoofnagle, *supra* note 80, at 310-311.

[83] Golbeck, *supra* note 78, at 105-106.

[84] See, https://www.facebook.com/help/1701730696756992?helpref=hc_global_nav (最後瀏覽日: 2020/2/22).

doi:10.6342/NTU202002857

- **適足性認定要求**（Adequacy Requirement)

歐盟自 1970 年代制定嚴格的個資保護規範時即肯認，若其資訊規範僅止於歐盟地區，而不是持續隨著個資的移轉流動規範的話，將無法落實保護歐盟人民個資的目的，故歐盟法規使個資管理機關得禁止歐盟人民個資被傳向未妥善保護個資的國家、地區或組織。對於個資跨境傳輸，歐盟資料保護指令與之後的 GDPR 均採原則禁止,例外允許的規範。GDPR 規定個資傳輸至歐盟以外的國家，除非有符合法定例外之情形，應確認該國家取得適足性認定（adequacy decision），或者企業自主採行符合規範之適當保護措施[85]。適足性認定之評估項目包括：目的地國家法制環境、目的地國家是否具獨立監管機關、是否簽訂國際協定或合約、目的地國家與歐盟間雙邊經貿關係、資料傳輸量與頻率、目的地國家是否為該地區隱私保護的先進國、政治關係與目的地國家隱私保護系統是否與歐盟保護程度相當等要素[86]，而歐盟認可的企業自主採行適當保護之措施包括：企業是否採行標準個資保護契約條款 (Standard Contractual Clauses)、拘束性企業規則 (Binding Corporate Rules)、適當的行為守則 (Codes of Conduct)與是否取得歐盟會員國的特定認證（Certification）等[87]。

本規範等同於將歐盟隱私規範技巧性地延伸至域外其它國家。以日本為例，在西元 2004 年間，澳州法學教授 Graham Greenleaf 曾批評日本當時的資訊隱私規範為「保護的錯覺」(the illusion of protection)[88]，他分析當時的日本規範認為該隱私規範具有過多易於被操縱的例外規定、疏於管制的資訊輸出、規範未能被

---

[85] Paul M. Schwartz, *Global Data Privacy: The EU Way, Forthcoming,* 94 N.Y.U. L. Rev., 771, 784-786 (2019).

[86] Art. 45, GDPR (Transfers on the basis of an adequacy decision).

[87] Art. 46, GDPR (Transfers subject to appropriate safeguards).

[88] Graham Greenleaf, *Asian Data Privacy Laws*, 227 (2014).

doi:10.6342/NTU202002857

有效執行與未能產生實效等缺失。然而，在短短的 3 年期間，日本為了與歐盟進行更多的商業交流，日本除修正國內個資保護法規(Act on the Protection of Personal Information)，使其與歐盟法規範在重要的規定上極為相似外，甚至包含了要求資料接收國要有與日本有類似的資訊隱私保護架構，或者要求個資接收者採取日本個資主管機關核準的預防措施，效果上等同於又協助歐盟向其它國家推廣了歐盟式的資訊隱私概念。當然，最終日本也因此取得歐盟的互惠性規範對待，歐盟的許多個資保護規範也同時適用於來自日本的個資資訊，在歐盟宣布日本成為適足性認定的白名單同時，雙方也同時宣布達成多項的經濟貿易夥伴協議[89]。此類以個資保護修訂換取經濟合作的模式也正在其它國家上演，使世界隱私規範向歐盟規範靠籠。

就連世界上較具磋商能力的美國也不得不採以溝通妥協的方式配合 GDPR 的規範。在西元 2005 年之前，美國企業憑藉美國與歐盟協調的安全港原則 (Safe Harbor)傳輸處理歐盟人民個資，但歐盟法院在 *Schrems v. Data Protection Commissioner*[90] 一案宣告安全港原則中含有多項未達歐盟個資保護指令對個資保護的規範，著眼於資料的跨界傳輸與處理仍世代產業發展的關鍵，美國與歐盟協商簽訂替代協議，經過大幅度修正原有安全港原則的規範，使其向 GDPR 規範靠攏，於 2016 簽訂隱私盾協議（EU-US Privacy Shield），並接受歐盟定期就協議的落實情況進行審查，在眾多的規範變化中，也對個資當事人的「同意」利用作了相當的限縮，使個資蒐集者無法一如往常僅憑藉個事當事人的一只同意，即毫無所限制地進行個資的利用[91]。

---

[89] Schwartz, *supra* note 85, at 787-790.

[90] Case C-362/14, Schrems vs. Data Protection Commissioner (2015).

[91] Schwartz, *supra* note 85, at 793-795.

doi:10.6342/NTU202002857

歐盟為使世界採行與其個資保護指令下相同標準的資訊隱私權規範，除了以經貿為誘因以及積極進行雙邊協議制定外，對它國有關資訊隱私的創新規範也採開放納入的作法，爭取他國認同。例如，GDPR 參考並納入了美國兒童線上隱私保護法案 (Children's Online Privacy Protection Act, 1998) 的規定[92]，對於兒童個資的蒐集利用有特別嚴格的限制；又例如，GDPR 採納了源自加拿大安大略省的隱私設計（privacy-by-design）政策[93]，要求資訊控制者在設計處理系統以及運用該系統時，必須採取適當的技術以及相關的組織措施。除此之外，對照處理個人資料目的之必要性，個人資料應具有適當性、具有關聯性，並且僅限在最小限度內。循此發展下的歐盟資訊隱私權規範，未來將持續對個資的蒐集與利用設置越來越多的限制。

- **被遺忘權**（right to be forgotten）

相較於美國規範個資蒐集與使用範圍的立法，歐盟法有較為不同的規範原則 – 即著名的人民「被遺忘的權利」(the right to be forgotten)，在此權利下，個資當事人得要求個資控制者刪除所有相關於他（她）的個資，且無論該資料是否為真實，個資控制者皆須配合是項刪除之要求。近年相關此權利爭議的著名案例為 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)，該案原告的房屋於西元 1998 年間因為債務清償的原因遭到法院拍賣，僅管原告後來已清償了所有債務，但一直到西元 2004 年，他的債務紀錄卻依然被記載於某一新聞報刊媒體，當原告向西班牙資料保護主管機

---

[92] Daniel J. Solove & Paul M. Schwartz, *Privacy Law Fundamentals,* 205 (4th ed., 2017).

[93] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (2009), Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (最後瀏覽日: 2020/4/23).

doi:10.6342/NTU202002857

關要求該紀錄自網站資料刪除時，主管機關聲稱因為該資料是正確且合法取得之資料，拒絕原告的要求。然而，主管機關卻同意依原告要求令 Google 刪除其搜尋引擎中的相關原告資訊的鏈結，其原因在於，Google 的關鍵字搜尋功能使原告的資訊可被一般社會大眾所知悉與近用。該案判決迫使網路業者必須依個資當事人之要求刪除所有相關個資的鏈結[94]，除非該資訊具有一定程度的公共利益目的。

歐盟的被遺忘權可朔源至法國法律，法國法律的被遺忘權（“the right of oblivion”, or “le droit à l’oubli”）允許刑事罪犯在完成服刑與重建後，得拒絕並要求任何出版發表不得再提及任何相關於他（她）的先前犯行或者服刑的事實。歐盟 GDPR 第十七條被遺忘權條款允許個資當事人要求資訊控制者向前刪除其個人資訊，無論其個資是因為當事人先前主動提供，又或者是因為個資蒐集者自行自其它管道所獲取的資料。除了資料不正確或不完整外，當具有其他法定理由時(例如:非法處理個人資料、資料當事人同意已經撤回等六種情況)，個人均可要求資訊控制者刪除其所掌控的所有個人資訊[95]。這個規定也等同迫使第一手資訊蒐集者必須建置一個得隨時追蹤後續資料控制者的機制，然而，要求初始資訊控制者證明其它下游資訊控制者均已依當事人要求刪除個資的任務其實是相當困難的，縱使 GDPR 第十九條有規定前述義務豁免事由（例如證明是不可能做到或者有違比例原則的情形），但該豁免規定也招致歐盟被遺忘權規定範疇不明確的質疑[96]。

---

[94] Paul Rosenzweig, *The Surveillance State Big Data, Freedom, and You*, 151-155 (2016).

[95] Article 17 Right to Erasure (‘right to be forgotten’), GDPR.

[96] See item No.141 of Opinion of The European Data Protection Supervisor on The Data Protection Reform Package. Retrieved from https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (最後瀏覽日: 2020/5/1).

doi:10.6342/NTU202002857

被遺忘權存在的必要性歷經了眾學者們的激烈爭辯，著名的論述包括法國哲學家 Paul Ricoeur 的主張，他認為遺忘的力量是人類所有動作所必需具備的，他主張遺忘的力量使個人得以治癒過去的創傷、取代所失去的事物以及重建損壞的自我[97]。德國哲學家 Friedrich Nietzsche 也曾主張，要一個人沒有遺忘過去地活著幾乎是個不可能的事[98]。牛津大學教授 Viktor Mayer-Schönberger 在其著名的 Delete: The Virtue of Forgetting in the Digital Age 著作中亦主張，遺忘使個人能夠自個人經驗中獲得歸納與粹練，它使個人能夠接受理解，人類其實如同宇宙萬物般，不斷地在改變[99]。甚至關於醫學科學界中對超憶症患者的研究中也發現，不尋常的記憶嚴重干擾他(她)們的生活，患者形容超憶對他(她)們是一種沈重的負擔[100]。

在過去未有數位儲存的生活環境下，人們已習慣因時間消逝而逐漸淡忘過往的生活經驗，但在數位新生活時代下，這個自然被遺忘的經驗假設已被打破，使我們的記憶與遺忘失去原有的平衡，數位記憶將使遺忘成為例外，個人建構自我識別性的能力也隨之受到威脅。有學者更認為被遺忘應屬於人民自主選擇與過去自己不同的基本權利[101]。準此以觀，遺忘與被遺忘的選項是對人類具有價值的，也因此有主張應該在數位儲存程式中預設性地建置被遺忘的特徵。美國著名的隱私領域法學教授 Daniel Solove 曾主張：網路資訊流動越是自由，個人的生

---

[97] Paul Ricoeur, Memory, History, Forgetting 486-506 (2004).

[98] Friedrich Wilhelm Nietzsche, On the Use and Abuse of History for Life 3 (2008). Available at https://pdfs.semanticscholar.org/6784/b376131703bcfa6458f48ee005ae75b8f4fa.pdf?_ga=2.226574301.1793891829.1593310936-1947095177.1593310936 (最後瀏覽日: 2020/5/3).

[99] Viktor Mayer-Sho¨nberger, Delete: The Virtue of Forgetting in the Digital Age (2011).

[100] Elizabeth S. Parker, Larry Cahill & James L. McGaugh, *A Case of Unusual Autobiographical Remembering*, 12 Neurocase 1 (2006).

[101] Alessia GhezziÂngela Guimarães PereiraLucia Vesnić-Alujević, The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten 67-68 (2014).

doi:10.6342/NTU202002857

活就將越不自由，因為個人過去的事蹟將可能阻礙個人未來的發展。再加上未來智能蒐索，結合人工智慧發展，將使個人資料的被蒐集與整合越來越快速與全面[102]，對於個人的影響力也將倍數增加。受以上支持論述影響，使歐盟在隱私規範上選擇賦予資料當事人行使被遺忘權權利。

第三節 美國與歐盟資訊隱私規範下產生的若干差異

本節主要整理在美國與歐盟的資訊隱私規範下，長久下來對私部門與個人在資訊隱私的實務落實上產生的重要差異。

- **商譽與市場力量**

不少法學者認為，由於美國資訊隱私規範欠缺明確與具體的規定與要求，使美國私部門傾向於避免主動領導內部資訊隱私管理措施，故主張美國法應該在資訊隱私制度規範上採行更為全面性的規範，才能刺激私部門積實極施保護個資之措施[103]。然而，法學教授 Kenneth Bamberger 與 Deirdre Mulligan 卻於面談眾多頂尖私部門企業內部負責隱私管理工作之部門主管後，發現三大不同的見解與現象：第一，美國私部門主管普遍認為，事業單位對客戶個資的保護政策，不僅只是一般的法規遵循作業，資訊隱私策略的成效更將直接影響私部門的「商譽」；第二，美國 FTC 對資訊隱私事件擁有具彈性且廣泛的管轄能力，得在一定的範圍內訂定符合需要的規則或準則，要求私部門事業單位配合，並且 FTC 要求私部門必須通知個資當事人關於私部門資安違規的作法，已使得私部門因為害怕自家商譽受損而多選擇主動採取措施保護資訊隱私的現況；第三，社會上資

[102] Eugenia Politou, Efthimios Alepis & Constantinos Patsakis, *supra* note 59, at 9-10.

[103] Hoofnagle, *supra* note 80, at 314. (citing: H. Jeff Smith, Managing Privacy: Information Technology and Corporate America (1994))

doi:10.6342/NTU202002857

訊隱私擁護者對於私部門的壓力，已逐漸使資訊隱私保護形成一種標準社會行為準則，再加上掌管資訊隱私工作的私部門主管傾向追求專業主義，促使私部門形成了為自己行為擔負全責的預期[104]。也就是說，Kenneth Bamberger 與 Deirdre Mulligan 教授認為，美國法的彈性使私部門的資訊隱私管理部門能夠主動地引導企業實施資訊隱私保護有效作為，而且私部門內資訊隱私管理部門也因此對其所推導的資訊隱私策略有較大的詮釋與發展空間；另一方面，美國資訊隱私的模糊規範也使得私部門較願意對外分享其所採行的個資保護方法與政策，且使私部門較勇於檢舉糾正其它商業競爭者所採行之偏誤的個資處理作為。

然而，仍有許多學者指出美國規範的多項缺失，其中包括，美國法由於欠缺統一的法律規範，私部門傾向朝對自己事業發展有利的方向去詮釋其資訊隱私保護措施，當問題產生時，易傾向為其所採行之資訊隱私策略加以辯解，若有具爭議性的個資處理作為，也較易選擇以掩飾或迴避的方式處理。對此，法學教授 Kenneth Bamberger 與 Deirdre Mulligan 雖然認為健全的市場機制使私部門對隱私信譽的建立具有誘因，且美國規範的彈性也較歐盟統一的規定更能夠誘使企業採行有效的隱私管理措施，但同時也承認，這樣的結論並不適用於一些不需直接面對終端消費者的私部門，因為資訊隱私商譽對不需直接面對消費者的 B2B 私部門而言，並不容易產生直接的激勵效用[105]。

- **「同意」效力的差異**

美國法在消費者保護法規範之實務操作上，多允許私部門僅以定型化契約之形式取得個資當事人對個資利用的「同意」之表示，個資當事人只需在網頁上

[104] *Id.* at 314.

[105] *Id.* at 315.

doi:10.6342/NTU202002857

出現的對話眶上點選「我同意」後，通常即具授權私部門處理其個資的效力。但相對的在歐盟資料保護規範上，只有當個資當事人在自由意志、具體明示，且在已被私部門完善告知相關風險的清況下所表示的同意才具實質效力。並且，在歐盟規範下，個資當事人得隨時撤銷同意，一旦經個資當事人撤銷同意，私部門即必需立即停止處理其個資。歐盟規範並不認為個資當事人得以「默示」方式同意個資的利用，且即使私部門已取得個資當事人合法的同意表示，資料控制者仍然必須在資料蒐集最少化、確保資訊安全以及符合既定蒐集目的等前提下，才能處理或利用個資[106]。此規定已造成歐、美兩地區在個資蒐集與保護作業上很大的差異。實務經驗觀察，隨著線上活動的普及，人們已經越來越容易忽略網頁上的隱私通知訊息，大多網路使用者為求便利與速度，習慣性看也不看地直接勾選「同意」，基此，本文認為美國法規範對於個資當事人的同意表示效力，似乎有必要再稍加嚴謹，以發揮其應有的風險告知效果。

- **對真實與公開個資利用的規範差異**

歐盟規範對某些特定類別之個人資料（或稱敏感性資料）有較一般資料嚴格的處理規定，例如個人的種族血統、政治立場、政黨、醫療狀況、性向等個資，除非法律規定授權或個資當事人已明示同意外，網路業者均不得處理與利用，在歐盟法體制下，即使是公眾可由公開管道取得的資料，該資料仍受歐盟資料保護法規範保護而被限制使用。然而，在美國法規範下，原則上只要個資訊息已被確認為真實且經公開者，私部門通常可恣意使用該等資料[107]。美國與歐盟就此規範各有利弊，實難斷言熟優熟劣，但長久下來仍將漸漸影響並建立起人們對個資的

[106] *Id.* at 316.

[107] *Id.* at 315.

doi:10.6342/NTU202002857

使用習慣，形成差異化的在地個資資訊使用之社會準則。

第四節 歐盟式規範對大數據人工智慧產業發展的衝擊

大數據未來最重要的發展即在於人工智慧技術（AI）的應用，AI 有能力高效率地處理大量的資訊，並且透過自我學習能夠找出新的應用，同時亦能排除或降低人為蓄意為不法目的所造成的資安與資訊隱私風險。然而，GDPR 的實施將對歐盟地區大數據 AI 產業發展帶來顯著的負面衝擊，使歐盟地區 AI 產業處於全球競爭的不利益地位。就具體的 GDPR 規定內容觀察，至少有以下幾項顯著的不利影響：

一、GDPR 第 22 條規定，個資當事人應有權不受自動化決策之拘束(not to be subject to decision)，該決策包括對其產生法律效果或類似之重大影響，而係以自動化處理來評估其個人特徵之措施。即使為締結或履行個資當事人與資訊控制者間之契約所必要或個資當事人已明確同意，資訊控制者仍應確保個資當事人得要求人為參與(human intervention)、表達意見(to express his or her point of view)及獲得挑戰該決策(contest the decision)之機會，以保護個資當事人之權利、自由及正當利益[108]。然而，AI 技術的優勢即在於能夠快速、低成本與準確地處理巨量資料，被冀望能夠取代傳統人力無法有效率完成的大數據運算，但此時 AI 應用網路業者為配合 GDPR 的規範，需要保留人為介入審查的機制，且根據個人資料處理保護小組[109]（Working Party）指導網領，該人為介入必需為實質意義的介入，即需考量所有 AI 技術所納入運算之資料，當 AI 透過自我學習所應用於運算模型越來越複雜時，要求網

[108] 財團法人金融聯合徵信中心 (2017)，歐盟個人資料保護規則，頁 9。

[109] GDPR 下由「歐洲資料保護委員會」取代原「個人資料處理保護小組」組織與功能。

doi:10.6342/NTU202002857

路業者保留回歸人為理解與審查工作將是一相當耗費人力與成本的法遵作業，最終中小型業者在成本控制的考量下，可能選擇減少納入數據資料運算的種類與數量，或者直接避免使用 AI 技術。況且，要求人為介入事實上反而可能造成個資隱私風險，人為有意識的介入大數據分析顯然較無人為介入的 AI 運算更易使個資資料庫遭到人為有目的性地利用而損害了個資當事人權益[110]。

二、GDPR 第 13~15 條賦予資料當事人一個獲悉足以理解 AI 運算邏輯的有意義資訊（meaningful information about the logic involved）之權利 (Right to Explanation)，然而 GDPR 卻沒有對何謂「有意義資訊」做清礎的定義，此將留給執法者或司法部門個案解釋如何的資訊才是能夠足以使個資當事人足以理解系爭 AI 運算，當加入 AI 運算的參數越多元，人腦也就越難以理解，更遑論是要讓沒有電腦科學知識訓練的一般個資當事人亦得以理解，將是個艱鉅的任務，故普遍認為此規定亦將犧牲 AI 技術的精密運算程度，而促使 AI 應用業者採以易於解釋(但通常只具有較低的精確度)的運算程序，此再一次地與冀望 AI 能自主學習與運算人類無法完成的大數據應用之初始目的大相違背[111]。

三、GDPR 第 17 條的資訊刪除權亦不利 AI 技術的發展，在通知與選擇機制下，在無其它法律強制例外規定的情形，GDPR 容許個資當事人得撤回同意利用之表示，要求個資控制者刪除個資。然而，AI 需要透過自我學習，而 AI 學

---

[110] Daniel Castro and Alan McQuinn, *AI Offers Opportunity to Increase Privacy for Users*, International Association of Privacy Professionals (2018). Retrieved from https://iapp.org/news/a/ai-offers-opportunity-to-increase-privacy-for-users/ (最後瀏覽日：6/1/2020).

[111] Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7(4) Int. Data Priv. L. 233, 236-238 (2017).

doi:10.6342/NTU202002857

習的基礎即是「記憶」並分析所應用的大數據資料，資料的中途刪除指令將阻礙 AI 科技的學習，降低 AI 學習成果的正確性，若有眾多個資當事人作此刪除請求，甚至可能破壞 AI 的學習模型[112]，再加上 GDPR 第 17 條要求不得無故拖延（undue delay）之規定，由於資訊控制者尚須判斷資訊流與對 AI 運算的影響程度，故此規定對網路業者而言也是一個耗力、耗時與耗成本的法遵作業程序。

四、GDPR 第 6 條要求個資控制者對個資的利用必需是在個資當事人所同意的目的範圍內，任何超出目的的利用必需取得個資當事人的同意，故當 AI 學習的結果產生新的應用功能時，網路業者必須先取得個資當事人的同意才得以合法利用，此除需耗費大量成本予以配合法遵外，也破壞 AI 應用業者在未來技術應用策略的商業秘密性，同時將阻礙 AI 技術得快速應用於相關領域或功能的潛在能力。

五、GDPR 的複雜規定使得 AI 應用業者幾乎均需要僱用隱私規範專業人力取得協助才能確保不生違法之情事，如此的成本對於 AI 新創事業來說將不見得能夠負擔，故將阻礙歐盟地區 AI 新創事業的起飛，也不利於鼓勵外國 AI 業者進入歐盟地區發展。

六、GDPR 對於違約者的罰款為至多 4%的全球營業額或 2 仟萬歐元（以較多者為準）的金額，因為小型公司通常賺取較少的收益，故以最大罰款金額來算的話，相對而言將對小型公司較為不利，多數新創事業並無法負擔 2 仟萬歐元的罰金，故此規定亦提升了新創 AI 事業的營運風險。

---

[112] Bernd Malle, Peter Kieseberg, Edgar Weippl, Andreas Holzinger. *The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases*, International Conference on Availability, Reliability, and Security (CD-ARES), Salzburg, Austria, 251-266 (2016).

doi:10.6342/NTU202002857

七、GDPR 第五章羅列其對個資資訊流的強勁控制，例如要求個資控制者必須將個資儲存於歐盟境內，不得將個資傳輸至歐盟以外不獲 GDPR 規範認可的國家地區或組織，此規定減少了歐盟以外雲端服務供應商的競爭，因此提高了資料儲存與處理的成本，然而 GDPR 並未體認其實資料存放的地理位置不見得就是對個資隱私或安全有所威脅，只要資訊儲存與處理者同意依照歐盟個資規定並受歐盟法律及法院管轄，即能管控個資處理風險，似乎沒有必要強行要求資料儲存設備必需座落於歐盟境內或者 GDPR 認可的國家地區。

八、GDPR 第 20 條規定的資料可攜性權利雖然整體而言有益於 AI 大數據者間的商業競爭，但對於龐大資料的移轉成本，GDPR 卻未妥善的予以分配，此將造成歐盟 AI 應用業者的成本負擔，使網路業者於初始階段即對投入大數據 AI 應用裹足不前。

本文認為歐盟式規範下相關個資處理的透明度、證據力、監督管理或可解釋性等規定所欲防範的風險，應該視大數據 AI 運算結果之應用的性質與重要性而分別決定，並非只因為系 AI 大數據的應用就必然與人為操作有所不同。另外，歐盟國家在網路資訊經濟崛起年代已經缺席，歐盟幾乎未擁有任何世界網路巨擘公司，AI 大數據產業對歐盟業者來說原本應該是一個機會，但 GDPR 如此嚴苛強制的法規範使歐盟業者難以與他國業者競爭，阻礙了歐盟 AI 產業的發展[113]。

歐盟 GDPR 原冀望藉由資訊法規的一致性規定，增加個資資訊在歐盟各國家間之交流，歐盟同時也以全球最大單一市場的優勢對他國施加壓力，說服他國

[113] Nick Wallace and Daniel Castro, *The Impact of the EU's New Data Protection Regulation on AI,* Center for Data Innovation, 21-22 (2018). Retrieved from http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf (最後瀏覽日：6/1/2020)

doi:10.6342/NTU202002857

採行歐盟式統一的資訊隱私規範，若全球真能如歐盟所願趨於統一的資訊隱私規範，也許將不致於不利歐盟大數據 AI 產業的競爭，但事實卻非如此，其它國家地區尚可藉由與歐盟達成協議的方式，持續處理來自歐盟地區的資訊，例如磋商能力佳的美國，即是以雙邊的隱私盾協議成功抗拒採行與歐盟相同的隱私規範，加上 GDPR 嚴格的規範所帶給企業的法遵成本，將使受歐盟規範的大數據 AI 產業發展受挫。其它欲仿效歐盟 GDPR 式規範資訊隱私的國家應引以為戒，畢竟，大數據資訊產業生態是個極度依賴跨國界應用的產業，國家的規範除了對個資當事人隱私資訊保護的考量外，更應著眼於協助相關事業進行全球化競爭的使命，以創造更好的產業環境，尋求國家與國民之最大利益。

doi:10.6342/NTU202002857

第四章 資訊揭露的基礎來自對資訊蒐集者的「信任」

本章結構上先討論通知與選擇(notice-and-choice)這個主流資訊隱私規範機制的特點，以及它在大數據世代實務適用上的各種先天侷限與曾被嘗試的各種挽救手段及成效。隨後自資訊揭露者的角度思考，提出社會社交觀點上的資訊隱私理論，細緻討論個人資訊於人際間流動的功能與目的，思索相比傳統隱私規制的隔離或控制之目的，資訊隱私法規是否其實更應以輔助人際資訊交流為宗旨？

在社會社交資訊隱私觀點的基礎上觀察，「信任」衍然在資訊揭露與接收之間扮演相當關鍵的角色，資訊不對稱的現象在大數據應用世代下的個人與網路業者之間默默地快速擴大，然而資訊控制者卻未因此被要求擔負起應有的受託者管理責任，此時市場機制逐漸失靈，個人表面上有著被通知與主動選擇的絕對權利，但事實上卻無從實施與兌現，久而久之，個人早已習以為常、反射性地在所有彈跳出來的對話框裡點選同意，毫無抵抗的意願與能力，網路巨擘正如溫水煮青蛙般在個人盲目的「同意」下慢慢近逼，要思考的是，個人對資訊蒐集者的信任是否已悄悄變質為資訊蒐集者的放任？

本章最後討論重建資訊受託者義務責任的重要性與可行性，復提出隱私設計（privacy by design）在大數據應用世代下可展現的成效，資訊隱私應該可以是一種預設設計、應可被公開監督、更應可被風險評估與承擔。易位自事業經營角度觀之，資訊隱私則不應只是一個法規遵循的流程，它更可能是變動時代下企業進行商業競爭的利器。

第一節 通知與選擇（notice-and-choice）機制的利與弊

通知與選擇機制的建構基礎主要源自兩個理論思考：一是個資當事人主宰控制自身資訊之權利，即個資當事人透過自主表達來展現該控制權能；另一理論

doi:10.6342/NTU202002857

基礎則是源自自由市場之概念，在自由市場下，個資當事人與個資蒐集者或控制者間，自然會就資訊的使用利益與個資隱私保護利益找到最佳的平衡[114]，當網路業者的資訊處理與隱私政策被公開，個資當事人一來能就資訊安全風險自我衡量，二來也能與其它業者比較，選擇適合自己偏好的隱私政策業者，或者可以選擇拒絕或接受與某網路業者條件而與之交易。而它之所以被普遍使用的原因主要在於，對資料蒐集者而言執行成本較低，尤其對於科技新創事業而言，撰擬一些資訊隱私政策文稿即可使之合規，確實是相當低成本的作法；另一方面就秩序管制者政府而言，也相對較易於要求資料蒐集者執行或履行合約義務，況且要求資料當事人為自己行為負責，也似乎相當合理。再者，因為是以明文規範的形式呈現，若真有違反之情形，也使行政或司法機關較易於以客觀的判斷標準予以論斷。

暫不論「通知」機制是否能真正達到它預期的效果，但就強迫網路業者將其資訊處理方式對個資當事人與外界公告的政策而言，確具可取之處，因為它使資訊隱私促進團體或者有興趣的個人得以檢視資訊蒐集者或資訊控制者的資訊處理作為，並可測試驗證資訊蒐集者與控制者的實際作為是否符合或明顯違反其所訂定之資訊處理政策，儘管未必能透過司法管道循求個人的救濟（因為損害與因果關係也許難以被明確證明），但個資當事人與公益團體仍能藉由訴諸媒體與輿論方式對資料蒐集者與控制者形成一定的壓力，促使其採行較能保護個資當事人權益的資訊處理措施[115]。另一顯著優點為，它迫使業者編撰資訊處理與隱私政策的同時，也是協助業者去瞭解與分析內部的資訊處理流程，協同相關專業人

[114] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 Daedalus 32, 34-35,41-42 (2011).

[115] Paula J. Bruening & Mary J. Culnan, *Through a Glass Darkly: From Privacy Notices to Effective Transparency*, 17 N.C.J.L. & Tech. 515, 540 (2016).

doi:10.6342/NTU202002857

員設計與檢討資訊流中的各處理程序，包括應蒐集的個資項目及其必要性、分享的對象、對資訊控制部門的信任度、資訊的保全措施以及面對新的資安威脅時之因應方式等等。它提供了網路業者建置一個針對內部資訊隱私政策檢討與更新討論平台的誘因，也間接促使業者將資訊隱私納入產品或服務設計的考量要件[116]。

儘管如此，從現實面觀察，通知與選擇機制仍然存在許多實務面難解的問題，以下僅就若干關鍵性障礙試行分析討論。

第一項 個人無從判斷風險

絕大部分的個人用戶不會去詳讀網路業者所公告張貼的資訊隱私政策，雖有論者因此推論，這代表其實個人用戶並不是那麼的在乎資訊隱私，否則個人用戶就至少會去閱讀網路業者公告的隱私政策。然而，從消費者保護的觀點而言，前述論點並不合乎邏輯與社會經驗，消費者對受保護的期待是會隨著消費者保護機制的建立而改變的。例如，汽車發展之初，汽車業者普遍認為汽車選購者在乎的是汽車炫麗的外觀設計與性能，而並不在乎安全性，但於 1950 年代，當汽車安全帶開始被列為一選擇配備時，安全帶配備立即受到消費者相當大的歡迎[117]。資訊隱私保護機制也是一樣，使用者不閱讀隱私政策並不代表使用者不在乎個資與隱私，而只是通知與選擇機制存在許多先天上的缺失。

一般而言，個人並不會知曉網路業者未來如何運用他們在業者伺服端裡所留下的個資，隨著資訊科技的快速進步，商業模式不斷的變化，商品或服務性質也一直推陳出新，即使個人在某程度上可預測科技發展的未來趨勢，但個人於揭

---

[116] *Id.* at 541-542.

[117] Hoofnagle, *supra* note 80, at 340.

doi:10.6342/NTU202002857

露個資時並無法確切地預期網路業者未來的營運活動會不會對自己的權益造成侵害。例如，臉書 Facebook 曾主動藉選新聞推播來影響用戶的情緒，臉書 Facebook 用戶瀏覽 App 時均會被動地閱讀 App 所推播的新聞，臉書 Facebook 曾試驗性地把正面及愉悅的新聞推播給某部分用戶，而同時把負面的、悲觀的或令人憤怒的新聞持續推播給另一群用戶，而 Facebook 得出實驗的結果為，接收正面新聞推播者變得較常在其 App 發表正面留言訊息，而接收負面新聞推播者則較易發表負面留言訊息。然而，從臉書 Facebook 當時公告的資料處理與隱私政策來看，這個研究似乎是合乎其政策所規定的（臉書 Facebook 當時公告的資料處理政策為：”Facebook users relinquish the use of their data for ‘data analysis, testing, [and] research’.” 譯：用戶資料可被 Facebook 用以「分析、測試與研究」），縱然如此，有多少用戶會預期臉書 Facebook 會因此直接操作推播新聞訊息，企圖影響用戶日常生活情緒，況且，Facebook 所取得之研究結果對個人用戶而言並無任何益處？[118] 也有論者從當事人同意範疇的觀點分析，認為臉書 Facebook 個資的應用可能實際上已違反當事人意願，屬未獲當事人同意即進行的非法利用[119]。

除科技變化與商業模式快速之因素外，使個人無從由通知內容判斷風險的重要原因之一還包含政策告知書的慣用書寫方式，又長又難以理解的迂迴文字

---

[118] Robinson Meyer, *Everything We Know about Facebook's Secret Mood Manipulation Experiment*, The Atlantic (June 28, 2014). Retrieved from https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

[119] Adam D. Kramer, Jamie E. Guillory, Jeffrey T. Hancock, *Experimental Evidence Of Massive-Scale Emotional Contagion Through Social Networks*, Proceedings of the National Academy of Sciences, Pnas, 111(24), 8788-8790 (2014). Retrieved from https://www.pnas.org/content/pnas/111/24/8788.full.pdf

doi:10.6342/NTU202002857

表述、字體小、格式擁擠、用色單調等等編排通常都令人難以舒適閱讀，有時甚至內容置放的位置也可能造成用戶的查詢困難。例如，三星智慧電視也曾爆發可能竊聽使用者對話，然而在其冗長的個資隱私條款內容卻夾帶標註「語音訊息的個人或敏感資料，將會被擷取傳送給第三方」的描述。

由於各國法規並無統一要求網路業者必需依照某固定的格式、內容、長度或方式等撰擬個資隱私政策。並且政策一旦擬定與公告，將被視為是個資蒐集者對其用戶的合約義務，故可想而知，業者當然會想方設法去降低違約風險，確保在萬一違約的情形下可有解釋的空間，於資訊隱私政策中包含模糊不清或模擬兩可的描述即是業者常用的方式之一。例如，當政策內容描述「組織可能將部分個人資訊分享給協作第三方，如行銷伙伴等」，試問個資當事人如何能依此判斷風險呢？行銷伙伴是誰？行銷標的為何？還有哪些協作第三方？..... 況且，一旦個人用戶瀏覽了網站內容，個人用戶又要如何能確知他（她）的瀏覽行為未被業者所紀錄、追蹤或分享呢？換句話說，個人要能發現並舉證業者違反其隱私政策是相當困難的？

此外，通知與選擇的主流機制也招致不切實際的批評，以現今大多數人的生活型態而言，每個人每天瀏覽會蒐集或利用個資的網站與手機 App 為數眾多，現實上並不可能去期待每個人都能有閒暇將所有網站或 App 的隱私權策略完整閱讀，這是時間與成本所不容許的任務。又政策的公告在本質來說，是一種屬於日常生活例行公事般的資訊披露，造成一種學者所稱的「積累問題」(accumulation problem)，即個人接觸過多例行公事的披露，大多數的披露自然無法被個人所消化[120]。另一方面，大數據與資訊科技又常被應用在各種智能設備或基礎設施中，

[120] Omar Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosures*, 159 U. Pa. L. Rev. 647, 705–708 (2011).

doi:10.6342/NTU202002857

例如智慧駕駛汽車、智能公路系統、車站的智能售票或資訊系統等，由於設施上可顯示空間有限（通常只是一個解析度不太高的小型顯示器），以及使用者可停留閱讀的時間相當短暫等因素，使得傳統個資政策的「通知」目的難以有效的被達成[121]。針對上述問題，曾被嘗試的解決方法包括以下：

- 歐盟多層次通知法

歐盟資料保護工作小組(Article 29 Data Protection Working Party)曾提出資訊蒐集者應以「多層次通知」（multi-layered notice）的方式協助個資主體了解隱私資訊處理及風險，第一層次為簡短通知，僅通知歐盟資料保護指令第 10 條要求的基本重要資訊，即資料蒐集者的實體與聯絡資料以及個資的蒐集與利用目的。第二層次為濃縮通知，通知個資主體所有歐盟資料保護指令要求通知的訊息，包括公司名稱、資訊處理目的、個資接收者分類、是否移轉予他方以及個資主體近用、修改、拒絕權利等。第三層次再為完整的通知，包含所有歐盟國家的法律要求與特異性[122]。然而，如此的分層方式固然可以使個資當事人剛開始更願意與容易閱讀吸收所通知之內容，但其實也僅只於第一層次或頂多到第二層次，尤其現代數位生活中，當個人需使用越來越多的網路服務時，即使連第一層次也會被當成是例行公事般被不經意地跳過不讀，故本方法並不符實際應用。

- **標準化格式通知法**

當一事件具有相當的複雜性並且又頻繁出現時，最有效率的處理方式之一即是標準化，例如當產品生產需要有成百上千的零組件，且零組件又各具規格，

---

[121] Bruening & Culnan, *supra* note 115, at 521.

[122] Article 29 Data Protection Working Party (WP29), Opinion 10/2004 on More Harmonised Information Provisions, v (Nov. 25, 2004). Retrieved from www.statewatch.org/news/2004/dec/wp100.pdf. (最後瀏覽日: 2020/5/2).

doi:10.6342/NTU202002857

此時產品在應用上將產生困難，產業界為求簡化與加速應用，就會開始推動規格標準化的活動，要求同類零組件統一規格與標示，除可加速產業運用外，又可減少資源浪費。又例如，現行各國食品或藥品法規，多要求食品與藥品必須依某標準格式及內容標示成分、組成及使用方式等資訊，透過標準化格式，使用者不僅能快速找尋所需資訊，並且能夠便利地與競爭者產品做比較，又能避免廠商標示資訊有所遺漏之情形。美國卡內基美隆大學的「CyLab 實用隱私與安全實驗室(The CyLab Usable Privacy and Security Lab)」[123]研究傳統的告知方法後發現，標準化表格的告知方式效果最佳，而其成功的關鍵在於使用「表格格式」 與「標準化語言」。

若所有的資訊蒐集者就其資訊隱私政策的通知方式均能被劃分成標準的公告格式，確實可能有助於一般個人快速瞭解政策所載內容。然而，這個提案也面臨若干重要挑戰：第一，由於科技服務發展日新月異，新的商業模式本身即可能藉由大數據分析的結果而產生，故實際上亦難在資訊蒐集階段即能定義完整的個資處理方式。第二，各國對個資訊處理要求的法規不一，大數據時代下的服務與資訊交流通常有著全球化的特性，故實際上亦難以統一標示格式以滿足各國資訊隱私規範。第三，食品營養標示之所以能以標準化方式有效協助購買者理解，有幾個很重要的原因，包括營養標示內容本身能夠被量化，因而消費者容易與其它食品做比較，又所標示內容能被公正實驗室以各種科學檢測實驗很客觀準確地被證實，並且，食品所標示之內容與數值不太可能在短期內即有太大的變動等特徵。這些特性都與網路業者在資訊處理與隱私政策本質上具有相當的差異。第四，食品或藥品等都是在消費者購買後，消費者仍有控制與決定如何食用之權利；

[123] CyLab Usable Privacy and Security Laboratory. See, http://cups.cs.cmu.edu/ (最後瀏覽日: 2020/3/1).

doi:10.6342/NTU202002857

但對於個資蒐集者未來的個資處理，個資當事人一旦提供個資後，個人幾乎無從得知與過問，應用上將完全掌握在資訊控制者手裡，更遑論個資可能在資訊控制者組織內外的各個部門或事業體間流竄的事實，使資訊控制者根本無法準確地將個資處理方式在所公告的隱私通知政策書上清礎說明[124]。

- 個資當事人隱私政策自動檢核程式的開發

亦有軟體公司曾開發個資政策自動檢核程式，個人用戶可事先在檢核程序中設定好自己的隱私要求偏好，該程序即會主動的替個人用戶閱讀資訊蒐集者的資訊隱私政策，判斷是否符合用戶個人的隱私要求，以節省個人自行閱讀與消化各業者政策說明的時間。微軟公司即是早期參與這類試驗的公司，微軟在其 IE 瀏覽器服務上，加上了一個使用者可設置隱私要求的功能，並會自動評估網站的隱私權政策是否符合使用者的隱私偏好設置[125]。本方法反應出本文下章即將討論相關於資訊隱私「信任」的本質，將隱私資訊要求規範回歸到「個資當事人偏好」之模式，即個資當事人依照其對資訊蒐集者的信任程度，以及資訊交付之背景原因等來選擇個資利用的範圍。然而，雖然立意良好，但實際執行上仍缺乏效率，因為個資當事人必須去瞭解每個網路業者的營運後才能判斷其資訊隱私偏好，並且每次都要重新評估或者重新設定偏好，亦是相當的耗時耗力，基此，個人用戶使用該機制之意願相當低落[126]。

第二項 選擇退出(Opt-Out)與選擇參加(Opt-in)

為解決前項所討論之問題，始有 Opt-out 與 Opt-in 機制設計的提出。Opt-out

---

[124] Bruening & Culnan, *supra* note 115, at 559-560.

[125] 張陳弘，同前註 76，頁 227-228。

[126] Bruening & Culnan, *supra* note 115, at 553.

doi:10.6342/NTU202002857

是指個資當事人主動告知網路業者不願意被蒐集或分享其個資，這個方法等同是將告知責任放置在個資當事人身上，即若個資當事人未主動告知個資蒐集者，則視同同意蒐集者依其政策利用與分享個資。相對地，Opt-in 機制則較為嚴苛，要求網路業者需要先行取得個資當事人主動的選擇同意分享個資，在未取得個資當事人指令前，資訊蒐集者即不得蒐集與分享其個資，且若資訊蒐集者使用或分享個資的方式有所變更，也必須要另外再取得個資當事人的同意[127]。

雖然 Opt-in 與 Opt-out 表面上看起來能提供個資當事人多一點的保護，但主要問題卻仍舊存在，即一般個人當事人是否有能力真正瞭解他（她）們所同意的內容？或者，在頻繁通知與決策的情況下，已經變為例行公事，當通知畫面在網頁出現時，連看也沒看的直接勾選同意呢？ 如此一來，個人的「選擇」是否仍具意義？ 早期網路業者多直接從個資當事人在網頁上所填寫的資訊來蒐集各種個資，但由於近年資訊應用的蓬勃發展，個人資訊自多元管道不斷地被蒐集，例如，各類型監測器、消費者追蹤機制或各類型的分析報告等，再加上廠商間的合作關係越行複雜，個資在廠商間交換或移轉的現象自然也越加頻繁，故個人「選擇」公不公開個資所具有的實質意義性已越來越低。另一方面，個資資訊分享與處理的社會功能在現時世代已越來越不可或缺，例如，政府為蒐尋失蹤人口、網路交易安全維護、醫學研究所需、詐欺防範及偵測等等社會公益目的，均強制要求個資的蒐集與存檔利用。再者，由於資料來源的多樣性，資料當事人甚至不知曉網路業者或 AI 科技公司擁有他們的個資，故也難言資料當事人得以「選擇退出（Opt-out）」不參與個資的儲存或利用了。準此以觀，資訊的公開或利用並

[127] Joanna Penn, *Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet*, 64(3) Fed. Comm. L. J. 599, 612-615 (2012).

doi:10.6342/NTU202002857

不適合再依賴舊有的個人「選擇與同意」制度[128]。

第三項 同意、撤回同意與刪除權所帶來的困窘

各國基於個人自治概念所設置的資訊隱私規範，在當事人同意或告知與選擇的機制下，通常也伴隨著有同意後撤銷或撤回同意表示的規定。例如，GDPR 第七條第 3 款規定：個資當事人有權隨時撤回其同意，且個資當事人為同意前，個資當事人應被告知是項隨時撤回同意之權利[129]; GDPR 第十三條第 2 款第(c)目規定：個資控管者於取得個人資料時，應提供個資當事人得隨時撤回其同意權利之進階資訊，以確保公平及透明之處理[130]；GDPR 第十七條(刪除權，又稱「被遺忘權」)第 1 款第(b)目規定：當個資當事人撤回其資料處理同意之表示時，資料控制者有義務刪除相關個資，且不得無故拖延[131]。我國個人資料保護法亦有類似的規定，個人資料保護法第 11 條第 3 項規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」[132]

可想而知，對於網路業者來說，配合個資當事人的資料刪除與處理同意撤銷及撤回之要求，絕對是個管理實務上的挑戰。其中大致可分為已儲存資料的刪除與個資使用的中止，若系要求刪除已儲存個資，則將涉及資料當時的定位蒐索，有時可能涉及硬體物件的銷毀，然網路業者是否完全遵循此類規範卻相當難以被證明。另一方面，亦有造成經濟資源浪費與公眾利益違反的爭議，例如，若個

---

[128] Bruening & Culnan, *supra* note 115, at 546-547.

[129] See Section 3 of Article 7 Conditions for Consent, GDPR.

[130] See Section 2 of Article 13 Information to be provided where personal data are collected from the data subject, GDPR.

[131] See Section 1 of Article 17 Right to Erasure (‘right to be forgotten’).

[132] 個人資料保護法第 11 條第 3 項。

doi:10.6342/NTU202002857

資被用作為生物技術的研究開發，過程中若因個資的刪除或者繼續利用的禁止造成研發成果的不成就，那犧牲的將不止是已投入的龐大資源，更是大眾的福祉利益[133]。再者，刪除權的行使將使某些機構在資訊的備份與儲存上產生法遵上的困難，例如，為使資通訊技術得到使用者的信賴，業者通常基於安全考量被要求去定期備份資料，包含數位備份以及轉存於硬件設備的備分，此時若某些資料當事人要求刪除其個資，勢必破壞資訊完整度，更可能導致業者為免除法遵稽核所帶來的麻煩，故意設法隱藏資料，如此將與應有的處理透明原則相悖。類似的情形在金融業界尤其明顯，基於付款或帳款移轉紀錄的保全，或甚至在地金融法規的要求，相關業者必須保存完整、可信賴以及高度透明度的資訊處理紀錄，面對 GDPR 的刪除權或被遺忘權規定，將明顯產生法規遵循的衝突[134]。

為處理資訊流在一連串儲存與處理過程中，所可能面臨的當事人同意不明確、撤回、撤銷以及同意範疇問題，社會已投入大量資源研究各種方案。例如，在醫學研究領域，有論者認為最有效率的知情同意方法即是不對當事人同意加以任何強制約束，根據美國一研究合法同意專案的知情同意框架- Portable Legal Consent 建議，研究參與者雖應被賦予隨時撤回同意的選擇，但參與者應被事前清礎告知，他(她)的資料可能基於實際實驗情況無法被完全刪除或類似之警語，藉由清礎的表述以增進參與者與研究者間的誠實對待與信任程度[135]。又例如，為解決當個資被由原始蒐集者移轉至下游控制者或再更下游處理者時，下游處理者未遵循原始同意範圍，或者未能及即回應個資當事人撤回同意之要求的問題，學者 Kaye 教授團隊[136]曾設計一個動態同意的加密機制，使資料於傳輸與使用時

[133] Politou, Alepis & Patsakis, *supra* note 59, at 5.

[134] *Id.* at 12.

[135] Gleibs, *supra* note 58.

[136] Kaye J, Curren L, Anderson N, et al., *From patients to partners: participant-centric initiatives in*

doi:10.6342/NTU202002857

均須加密處理，連同資料的處理結果也進行加密，以對個資資訊流獲得最大的掌控[137]。其它機制還包括隱私代理(privacy agents)軟體的設計，使用者在代理軟體上依選項設置隱私管控喜好，由軟體來代為執行[138]。也有發明「同意收據」(Consent Receipt) 的設計，要求個資蒐集者須發給資料當事人一個可供追蹤的收據，使個資當事人則可依同意收據上所戴資訊追蹤與檢視其個資利用情況[139]。其它亦有以國家為單位所發行的同意追蹤紀錄管理機制，例如芬蘭開發 My Data Initiative，藉由標準化與嚴謹的同意機制設置，使個資利用的同意紀錄可於同一官方平台上被隨時查詢與更新[140]。

以上僅列舉少數範例，眾多同意確認機制正在世界各地、官方與民間持續地研究開發中，然而本文所強調者為，個資與資訊流是未來科技事業發展的關鍵，並且具有跨國際與跨組織的特性，過多與繁雜的確認程序其實是大數據科技發展的阻礙，更遑論同一資訊又必需同時符合多種管制規範，豈非是莫大的資源浪費。故本文認為應該重新審思資訊隱私的基礎意義，再依基礎意義與務實目的來發展具實效的規範，以免疊床架屋、欲速則不達。

第四項 科技網路與大數據資訊利用的特性

本項目的在以實務應用角度整理若干大數據資訊科技與應用的特性，探究傳統資訊隱私規範對它們的干預，以及如何直接或間接影響個資當事人使用大

---

biomedical research, NAT REV GENET. 2012;13(5):371-376. Published 2012 Apr 3. Retrieved from https://pubmed.ncbi.nlm.nih.gov/22473380/ (最後瀏覽日: 2020/4/25)

[137] Gentry C. Fully, *Homomorphic Encryption Using Ideal Lattices,* STOC, 169-178 (2009). https://dl.acm.org/doi/10.1145/1536414.1536440 (最後瀏覽日: 2020/5/25).

[138] Sarah Spiekermann & Alexander Novotny, *A Vision For Global Privacy Bridges: Technical And Legal Measures For International Data Markets*, COMP L & SEC REV, 181-200 (2015).

[139] See https://kantarainitiative.org/confluence/display/LC/2017/01/08/ (最後瀏覽日: 2020/4/30).

[140] See http://hiit.github.io/mydata-stack/ (最後瀏覽日: 2020/4/30).

doi:10.6342/NTU202002857

數據科技之意願與資訊隱私之風險成本。

- 應用發展無可預期性

受到大數據演算法日新月異、網路業者間供應鏈關係越漸複雜、資訊透過各類感測器蒐集以及即時分析技術的發展等本質，已使一般個資當事人難以理解個資的實際利用情況，又資訊控制者隨時可能更新演算法，並結合外來數據進行交叉分析，產生對個資當事人的行為預估，以為商業、政治或其他用途。因為期間已融入不同來源之資訊進行演算，個資當事人已實無預期之可能，加上第三人資料綜合處理的情形，例如，締結個資同意利用之雙方以外的第三人蒐集、使用個資，或締結同意之雙方以外的第三人被蒐集、使用個資的情形，足使個資當事人完全被摒除在整個資訊流之外，既無從得知，也無從就個資的利用做決定[141]。

以西元 2016 年間，美國網路公司 Yahoo 曾遭指控侵權案為例，當時 Yahoo 曾對用戶電子郵件內容進行析，並依據分析結果對用戶提供精準行銷廣告，Yahoo 在其免費電子信箱服務的隱私權政策說明中提及：「Yahoo 的自動化系統分析會分析所有通訊內容，以提供包括但不限於下列的服務：提供與您相關的產品功能和內容、進行比對與提供精準式行銷廣告……等；系統會在傳送、接收和儲存所有通訊內容時進行分析，包括與您 Yahoo 帳號同步的服務的通話內容」。當 Yahoo 電子郵箱用戶點選同意該政策，在美國判例法下，除了用戶本身可能已喪失對郵件內容合理的隱私期待[142]，還可能涉及該用戶之聯絡人，縱使他方使

[141] 張陳弘，同前註 76，頁 206。

[142] See United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). 本案法官比較電子郵件服務與傳統的電話與信件之聯絡方式，雖認為如同電信公司接線生在合法的範圍內可能聽取對話內容，又如郵局在合法的範圍下可能拆閱檢查內容以保護公設機關一般，並不影響通話者與捎信者對其對話內容的合理隱私期待，縱使 ISP 業者具有近用用戶電子郵件內容的管道，電子郵件用仍擁有對郵件內容的合理隱私期待；然而，若 ISP 業者在其與用戶的使用約定上，明確表示將會進

doi:10.6342/NTU202002857

用的電子郵箱服務並非同為 Yahoo 所提供的電子郵箱服務，也並未同意 Yahoo 的隱私權政策說明，Yahoo 用戶的同意選擇效果仍可能擴及於使用電子郵件與其聯絡的他方聯絡人[143]。

除此之外，行動裝置的普及，又較電腦網頁的使用增加了通知與選擇機制實施的困難度，行動裝置可在使用者未意識狀態下蒐集個資，例如地理位置、聯絡人訊息以及使用者相片辨識等個資，甚至有時應用程式會蒐集與使用功能無相關的資訊，例如，使用手電筒照明功能的同時蒐集地理位置訊息。若應用程式未及時的告知使用者，使用者將無從知悉其個資正被蒐集與利用。即使應用程式主動通知使用者，另一個問題是，應在何時將該蒐集個資之動作向使用者通知？畢竟，太過頻繁的通知與選擇勢必將造成使用者使用經驗的困擾與阻礙[144]。

就大數據科技發展下新產品或服務在個資應用上具有不可預期性的特性，繁複的設計耗費資源，且減少了原本流暢的用戶使用經驗[145]，有論者主張，當事人同意的隱私規範機制可能同時導致對科技創新與社會公益創造上的阻礙；但相對地，亦有學者持不同看法，認為當事人同意是個人對其個資管控上的最後一道防線，尤其若從人民自主的觀點考量，在並無充分理由的情形下，當事人同意機制並不應任意被取消[146]。

行稽查、檢查與監視郵件內容時，則郵件用戶的合理隱私期待將可能被否定。

[143] 張陳弘，同前註 76，頁 208-209.

[144] Bruening & Culnan, *supra* note 115, at 564-565.

[145] Politou, Alepis & Patsakis, *supra* note 59, at 5.

[146] Paual de Hert, Vagelis Papakonstantinou, *The New General Data Protection Regulation: Still A Sound System For The Protection Of Individuals?* 32 Comput. L. & Secur. Rev. 179, 186-188 (2016).

doi:10.6342/NTU202002857

- 對個資當事人權利造成實質侵害

a. **無時不刻對個人行為分析與預測**

在人手一機（或者不只一機）的世代，手機無時不刻在人們身邊，人們常以為只有當個人主動輸入訊息或使用手機時，業者才可能取得其資訊，但其實不然，即使當用戶晚上睡眠，手機在旁邊充電時，手機裡的 App 仍可能正在傳輸個人作息資訊，且當 App 運行時，將可能不只 App 所屬資料庫取得個資，它可能同時傳輸給數個合作業者資料庫，儘管 App 業者遵守其隱私政策，但它的合作業者卻不見得遵守，或甚至不具有任何資訊隱私保護機制或政策，個人的行為與行蹤就如此在不知不覺的情況下，被傳往許多不知名的端點，當需要時，業者即對個人資訊進行分析並從中獲益[147]。

b. **網路使用自主權的干預**

在大數據應用的時代裡，個人知識恐怕將越來越狹隘，大數據分析使現代人最常賴以接收外界資訊的電子設備，因為智能學習與分析結果，均傾向為使用者蒐選內容，預測使用者喜好，自動向使用者推薦或推播使用者較可能感興趣的資訊類別，使用者的時間因此越來越多被半強迫地花費在自己原本就有基礎知識或有興趣的事物上，因而減少了對新事物的接觸機會。Facebook 的使用經驗即是很明顯的例子，用戶登入並滑動 Facebook App 所瀏覽的訊息，多是經過 App 主動的內容挑選與順序編排的，其中還包含特定廣告的置入頁面，縱使用戶還是能自行手動滑過不喜好之內容或直接忽略，但長年累月卻還是已佔據用戶相當的時間與精神，而個人對資訊接收的選擇也因此被嚴重地干預。

---

147 Geoffrey A. Fowler., *It's the Middle of the Night. Do You Know Who Your iPhone Is Talking To?,*" The Washington Post (May 28, 2019). https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/ (最後瀏覽日: 2020/4/30).

doi:10.6342/NTU202002857

c. 對使用者造成歧視

經由對使用者個資的大數據分析，除可能產生有利於商業行銷或產品研發的資訊外，還可能被用來針對個人或特定群體進行的各種歧視行為，傳統上人為利用資料庫分析的結果，有意識地進行違法的歧視行為時，即有法律明文予以禁止，例如法律明文禁止各種種族、性別歧視等行為。然而，當 AI 介入學習，產生自我學習成果的數據運算規則時，由於並非能總是在人為的監視範圍內運作，一旦發生類似違法事件，資訊控制者之可歸責性即受到挑戰。

例如，於西元 2018 年間，美國 Amazon 公司自家的 AI 科技設計，原本希望藉由對公司現有員工進行各種資訊與工作績效分析，產生出較科學與可靠的未來用人標準，應用於應試者的履歷篩選，但事後發現，Amazon 公司的 AI 科技竟能自行透過學習、分析與歸納，自我產生新的演算法則，而該法則明顯傾向於選擇保留男性的履歷進行面談，而排除女性[148]。如此看似具有正當理由與目的，且在正常範圍內的個資利用，若未有妥善的監督管控，最終也可能產生違法的結果。

- 駭客入侵竊取個資

縱然網路業者透過蒐集與分析用戶資料，以提供用戶更為便利的生活之商業模式，立意上良好，又縱使網路業者也遵從基本的保密義務，然而，儲存在網路業者資料庫內的個資仍可能因為系統被駭，而使用戶蒙受損失。在背後龐大利益的趨使下，這樣的風險似乎是沒有辦法以加裝幾個防毒軟體，或者簡單的幾條

[148] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women*, REUTERS, (October 9, 2018). Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (最後瀏覽日: 2020/4/30).

doi:10.6342/NTU202002857

法規範即可完全避免[149]。電腦駭客的問題本質上並不完全歸屬於業者操守或設備技術問題，它是一個動態的威脅，建置防火牆等防駭技術當然具有它的必要性，但技術精密度本身卻是一個程度的問題，因為實際上並不可能要求每一個中小型事業，都必需建置如同美國五角大廈規格的防駭技術，在成本與效率的權衡下，勢必得找尋出新的折衷方法。此時，技術面、法規範面與經營管理面即需同時介入，除了要求其在技術上要能符合某些標準的網絡安全設計外，業者的內部管理制度建置與相關制度的執行落實程度等也都是風險的來源

綜上所述，通知與選擇機制在大數據與 AI 科技的發展與相關特殊性下，已不足為個資當事人建構妥適的保護，並且在許多應用上已顯現對大數據科技發展推動的阻礙，是以，處理大數據科技的資訊隱私問題，社會真正需要的是一個富具彈性的新資訊隱私管理機制。

第二節 社會社交觀點理論下的資訊隱私

本節旨在討論於社會人際社交活動與功能下，個人資訊揭露在其中所扮演的角色，資訊隱私的目的究竟系為防堵人際干預或是應為促進人際交流呢？個資當事人每次的資訊揭露都應有其特殊的背景、原因與目的，它們影響個人對於資訊隱私的期待，那麼，資訊隱私規範是否應該將這些背景、原因與目的因素融入考量才能更貼近規範目的與個資當事人期待呢？

第一項 人際社交與資訊隱私的關係

人際間的社交活動其實是建立在資訊隱私的基礎上，個人通常只會對關係親密或較信賴的友人分享較為私密的個人資訊，對於較疏遠的友人，通常僅願分

[149] Jennifer Golbeck, *supra* note 78, at 117-119.

doi:10.6342/NTU202002857

享較不屬私密的訊息。如此的資訊選擇與溝通即構成了社會社交，也正因為個人對隱私的期待，相信資訊接受者願意為其保守秘密，使個人願意揭露分享個資，是以，自社會社交觀點的角度觀察，資訊隱私其實是「促進」社會社交訊息「分享與流動」的關鍵，若個人沒有隱私資訊將持續受保護的期待，訊息的揭露將會減少，最終導致訊息無法有效率的在社會中流動，因為有了隱私保護的期待，個人才得以建構與他人間的關係，形成各式各樣的社會行為慣例，致使人際間能夠持續產生各種多元的互動[150]。本社交理論觀點與傳統以「權利」、「隔離」或「控制」為基礎發展而成的資訊隱私權概念形成強烈對比，基本觀念截然不同。

隱私讓個人在社會中可同時滿足多種不同角色的扮演，例如，餐廳服務生在餐桌邊及顧客前表現出專業、嚴謹與有禮貌的一面，而在餐廳內的工作區域時，與同事間的相處則可表現較為輕鬆、調皮、愛談論是非的另一面。這是人類在社會中相當自然的表現，也是使人類在輕重緩急交錯的生活中得到適當的調節與休養，這些行為表現的差異其實是符合社會一般所期待的，而正是因為有隱私，使個人得以有適時適所的表現[151]。但這並不代表隱私就只是被利用來隱藏不欲人知的負面訊息或消極面，更也不是被個人利用來控制或抵制他人瞭解自己的工具。人人自然希望在不同場合能形塑自己所喜愛的獨特形象，有了不同的形象，個人即得以自在、輕鬆的方式與他人互動，這即是隱私在社會社交功能上所扮演的重要角色。

美國著名的隱私領域法學教授 Daniel Solove 曾提出，資訊隱私的定義不應該是建立在「隔離」或「控制」觀點的大觀念上，因為籠統的大觀念容易讓隱私

---

[150] 社會學家 Robert Merton and Erving Goffman 主張，我們每個人在社會上都扮演多種角色，在不同角色裡，我們說不同的話、為不同之行為、以不同方式與他人互動，而隱私的存在正是允許（或協助）我們扮演各種不同角色。

[151] Erving Goffman, The Presentation of Self in Every Day Life,75 (1959).

doi:10.6342/NTU202002857

規範應用於日新月異科技發展下日常生活顯得窒礙難行；他主張應該由個資當事人於資訊揭露時，以及個資使用時之事實背景、文化及科技應用等實際情況來定義資訊隱私規範[152]。 他並認為法院審判資訊隱私案件時應認知，資訊隱私規範不僅是用來保護個人隱私，而應考量其嘉惠社會社交功能之目的[153]。換句話說，隱私不僅在於保護個人的自治與自由，更是背負了促進人際交流與進步的重要使命。

第二項 依據個資當事人與個資蒐集者的「關係」來辯識資訊的隱私性質

本節所討論的「關係」理論系由前節討論之社會社交觀點所衍生的資訊隱私概念，主要強調不應再僅依訊息的內容作為隱私訊息屬性與否的分類，而是就訊息接受者相對於訊息揭露者間之關係加以分析討論。例如，病患於就診期間，自然會向他（她）的「醫師」揭露自己的健康情況、生活習慣、用藥資訊等個資，因為醫病關係，病患自然能合理期待其所揭露之資訊能被醫師所保密，即使在未有任何保密約定的情形下揭露給醫師，該訊息仍被期待應維持隱私狀態；相對地，如果病患是在醫院的走廊上，跟其他病患聊起自己的健康資訊，那病患自然不會有維持資訊隱私狀態的期待。又例如，訴訟當事人於司法程序準備期間向其「委任律師」所揭露的各項案件事實、行為、想法、動機等等，當事人自然期待其委任律師為其保密，故該等訊息雖經揭露，仍被期待應保有隱私訊息之屬性；相對地，當訴訟當事人向陌生人或者非深交熟識的友人透露案件訊息時，當事人則無法合理期待資訊接收者陌生人將會如同其委任律師般予以保密，故該等訊息自然不應被認為在揭露後仍保有隱私之屬性。是以，司法判斷某訊息是否屬個人隱

---

[152] Daniel J. Solove, The Digital Person,50-65 (2004).

[153] *Id.* at 84-88.

doi:10.6342/NTU202002857

私時，應同時探詢個資當事人與個資蒐集者間的社交「關係」，以正確地判別個資當事人是否可合理期待系爭訊息隱私狀態之維持[154]。

然而，這個純粹以個資當事人與個資蒐集者間「關係」來定義或判定隱私訊息的觀點，卻具有若干缺點：第一，司法法官將因此被要求介入，並以其個人生活經驗來判斷當事人間之社交關係，如此，法官將不自覺融入其個人主觀意識予以評價，容易推導出不符合當事人預期，或者個資當事人與個資蒐集者間實際存在的社交關係。第二，在科技網絡生活世代裡，個資當事人多將其訊息交給網路雲端上的「陌生人」；又或者，個人在臉書 Facebook 帳戶裡非常陌生的「朋友」，也可能因為使用 Facebook 服務而取得個人個資。若依「關係」為基礎來判斷隱私資訊之屬性，在網路平台上所揭露之訊息都將被認定非屬個人能合理期待維持隱私屬性之訊息，但此結果又顯然與一般網路使用者之期待有所違背。第三，此以資訊流作為判斷準則的基礎，其實並未考量個人於揭露個資當時的心理期待與背景原因，然而，它們卻是悠關個資當事人是否真正期待所揭露個資隱私狀態之維持[155]。

第三項 資訊隱私意識的本質應包含資訊揭露當下之背景條件 (Context)

判別已揭露訊息是否仍維持個人隱私之屬性，除前文所列各種考量外，例如個資揭露者或個資當事人與資訊蒐集者的關係、訊息本身的性質、社交網絡的性質等，著名學者 Helen Nissenbaum 曾提出以「資訊揭露當下背景條件」為判斷基準的理論。社會應認同隱私是日常社交生活的重要基礎之一，人際間的隱私系社交結構一個重要的構成要素，直接影響人際間的互動。因此，資訊隱私應該就要

---

[154] Waldman, *supra* note 7, at 39-40.

[155] *Id.* at 42.

doi:10.6342/NTU202002857

從日常社交生活來觀察與定義。Helen Nissenbaum 主張，任何訊息是否為應屬個人隱私，應該要依據不斷變動的時空背景來決定，包括訊息交換當下的情境、訊息與該情境或背景的關聯、訊息接受者的角色、訊息接受者與個資當事人的關係、個資當事人分享個資的條件以及個資蒐集者將個資再分享的條件等。[156]

Helen Nissenbaum 又認為，在時空文化背景下大家所認同的某種社會準則（Social Norms）也應作為資訊隱私屬性重要的判斷依據，她認為所有資訊揭露的情形都應該會有一個可茲歸屬的社會準則，而個資當事人與個資蒐集者被期待依照該社會準則來扮演各自的角色，以完成某共通目的。以本文先前所舉醫病關係的例子而言，病患之所以向醫師揭露個人隱私資訊，即是希望醫師有足夠的資訊作專業的醫療診斷以及正確的治療（此即醫師的角色），以期待達到疾病治癒的結果（此即共通目的），若醫師將病患所提供的資訊再揭露給其它患者或者不相關的第三人，則有違在資訊揭露背景條件當下的「社會準則」，因而侵犯了病患的隱私。又例如，消費者於商場內購物結帳時，將其信用卡訊息交付給賣方，以使賣方得向所屬銀行請領正確的銷售款項（此即賣方的角色），以達消費者履行債務或完成交付買賣對價的結果（此即共通目的）。若賣方將該信用卡資訊再揭露給與交易付款不相關聯的其它人，則賣方即違反買賣收付款背景條件下的「社會準則」，因而侵犯了消費者的資訊隱私。

「社會準則」系隨國家在地風俗民情特色不同而變動，考量的是當地大多數人對某交易或某關係的認知，也是當地人民普世價值的一個展現，社會準則可能

---

[156] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 101, 137-138 (2004) ("Whether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination.")

doi:10.6342/NTU202002857

隨著時代的進步而進化，相較於傳統對隱私的定義，這種以資訊揭露當下背景條件為基礎的分析，富有彈性與靈活的優點，Hellen Nissenbaum 的分析將使資訊隱私規範更能合理地被適用，特別是在科技發展快速的網絡世代，人際間交流的方式不斷在改變，各種新科技下的交易模式也將會產生專屬、有別於傳統交易活動的「社會準則」。除此之外，就司法在實務的審查與判斷上，適用的社會準則亦可藉由各種調查報告被證實。例如，根據美國消費者聯盟（Consumers Union）對網路使用者所進行的一項調查顯示，對於網路公司將他們的網路瀏覽歷史提供給第三方公司或者利用來做為行銷目的的作為，有超過一半的網路使用者感到相當不安[157]。此即可用以證實在某時期某地區相關網路訊息分享的「社會準則」，要求網路業者遵從是項社會準則即顯得相當合理，並且當發生爭執時，類似的調查研究亦有助司法對資訊隱私侵權與否的客觀判定。

第三節 資訊蒐集者建立個資當事人「信任」的意義

從事業經營的實務面觀察，科技網路業者採行各種方式保護用戶資訊，與制定資訊隱私政策保護個資的重要目的之一，即是為取得用戶或資料當事人對它的「信任」，當個資當事人對某網路業者「信任」的程度越高，個資當事人就越願意與之進行交易往來，並較願易向其揭露個資[158]。

以蘋果公司（Apple Inc.）的雲端服務為例，當用戶在轉換個人電子設備而登入蘋果公司的雲端資料庫帳戶時，多會收到系統發給用戶的詢問訊息：「請問您是否信任某某新設備？」。像這樣的設計無非在於取得用戶對蘋果公司在個資處理機制上的「信任」，使用戶感受到蘋果公司相當重視任何用戶個人隱私的態

157 Penn, *supra* note 127, at 606-607.

158 林錦郎、卓麗香、張松山（2017），〈資訊隱私機制與信任對 Facebook 社群網站使用者行為意圖影響之研究〉，《全球商業經營管理學報》，第 9 期，頁 22-23。

doi:10.6342/NTU202002857

度。同樣的，臉書 Facebook 也時常藉由用戶界面的設計、隱私設置的詢問、近用帳戶郵件提醒等功能，設法取得用戶對臉書 Facebook 的在個資處理制度上的「信任」，一旦用戶越是信任臉書 Facebook 服務，用戶即越容易於將其個資與個人活動在臉書 Facebook 平台上分享。

美國司法部曾針對網路相關事業單位調查發現，網路事業單位普遍認為，個人對網路資訊隱私的信任程度對於互聯網商業活動極為重要，若個人對網路資訊隱私的信任程度減損，將會抑制互聯網新興科技應用的進展[159]。

「信任」不僅僅是網路業者用以蒐集個資的手段之一，「信任」其實也是個資當事人決定交付自己資訊予他人的最重要「社會準則」之一，故有學者認為，資訊隱私之規範應該要以「信任」或「信託」概念為核心設計與發展。是以，違反資訊隱私的真正意義，其實應該等同於違反個資交付情境背景條件下個資當事人對資訊蒐集者的信任或信託內涵。

「信任」是人類社交活動下自然衍生的一個良善工具，也是社交資本（Social Capital）的一部分，它協助社會群眾間為了共同的利益而進行各式各樣的合作與交流，互通有無。如同個人交付其重要物品予他人代為保管般，基於交付者在某種相應的社會準則下對受託者的「信任」，而同時交付者在社會準則規範下也甘冒相當的風險，交付者冒著受託者可能未妥善保管其物品或挪作他用的風險，交付者與受託者間的「信任」即是交付者用來處理該未知風險的策略，且該「信任」的建立，使交付者與受託者皆取得某種共同的利益。例如，交付者取得物品保存與便利，受託者則取得了保管費的收入對價等[160]。

---

[159] Molly Jennings, *To Track Or Not To Track: Recent Legislative Proposals To Protect Consumer Privacy,* 49(1) Har. J. On Legis. 193, 197-98 (2012).

[160] Waldman, *supra* note 7, at 50-52

doi:10.6342/NTU202002857

- 個資當事人於資訊揭露前產生「信任」的來源 （trust contexts）

個資當事人對個資蒐集者的信任，除了來自於個資蒐集者的隱私政策宣傳外，還包括了許多情境式因素，例如（1）個資當事人自身或友人曾使用資訊蒐集者相關服務，基於過往活動紀錄而產生的信任；(2) 基於資訊蒐集者的身分、學位或名氣等，使個資當事人產生投射性的信任；(3) 基於個資當事人與個資蒐集者間的法律關係而產生信任，諸如銀行與存戶、律師與委託人、員工與雇主等；（4）基於雙方所簽訂之保密合約，或者雙方約定之損失賠償承諾等而產生的信任；(5) 基於互惠（reciprocity）所生之信任。例如，個人在臉書 Facebook 上好友對其發文按贊，或者他人對自己在發文下的正面留言等，也會使個人對該好友或甚至臉書 Facebook 平台產生信任；(6) 基於社會通念而產生的信任，例如，與親密好友分享個人親密關係資訊或與性相關之訊息，訊息接收方通常會認知該等話題不應任意加以散播；(7) 個資當事人之好友對資訊蒐集者的推薦，也會使個資當事人對陌生的資訊蒐集者產生一定程度的信任而交付個資；(8) 資訊蒐集者若擁有數量龐大的用戶，通常也容易增加個人對其之信任；(9) 個人與其它熟識用戶的社群連結，也會使個人因為熟識感到安全，把對熟識用戶的信任轉嫁到了資訊蒐集者上；(10) 臉書 Facebook 藉由協助個人與朋友間的相互活動推播，也會增加了個人對臉書 Facebook 的信任，使個人願意揭露信息給臉書 Facebook，另外臉書 Facebook 的朋友功能也促使個人對臉書 Facebook 信任，研究發現，當臉書 Facebook 用戶擁有越多親近朋友時，該用戶也越願意在臉書 Facebook 分享越多的個人訊息[161]；當用戶與他人有越多共同社群時，也會增加對他人的信任，用戶也越願意將其加為朋友。然而，研究也發現，只有 27%的臉

[161] 郭明煌、廖鴻圖、蕭麗齡、王亭雅（2014），〈資訊隱私顧慮對社群網站使用者使用意圖影響之研究－以 Facebook 為例〉，《資訊管理學報》，第 21 卷 4 期，頁 358-359。

doi:10.6342/NTU202002857

書 Facebook 用戶願意把那些永遠不會見面的用戶加到朋友圈，此研究也間接說明了「匿名」並不會增加個人揭露訊息的意願，但與訊息接受者相互間的「信任」，卻會增加個人分享個資的意願[162]。

第四節 以「信任」為基礎建立資訊隱私規範

基於資訊隱私與信任間之緊密關係，學者 Neil Richards & Woodrow Hartzog 主張，資訊隱私應立基在「信任」積成的基礎上，而非建立在「防範」侵犯的基礎上。隱私能夠鼓勵個人因為「信任」而分享訊息，能促進社會交流與進步[163]。也就是認為，資訊隱私規範其實應是以保護與促進「訊息分享」為主要目的，而絕非僅是為捍衛個人疆域、抵禦外侮，或者謹為保護抽象而過於廣泛的個人控制概念。

第一項 「侵害資訊隱私」在以「權力」及「信任」為基礎資訊隱私規範下的意義

試想當個人於某網路平台準備點入某商品鏈結時，網頁跳出一對話方框，告知個資當事人將會蒐集其個資，個資當事人點選同意進入商品網頁，之後網路平台利用所蒐集之當事人個資，是否侵害個資當事人資訊隱私？一般人乍看之下都會認為是不侵害。但試想網路平台所蒐集的個資將包括，使用者瀏覽的項目、停留的時間、瀏覽的時段、活動的地點、付款的方式、消費的統計、交叉查詢的項目……等，前述資訊也許分開個別來看都不算是使用者的私密訊息（尤其當使用者已同意並主動揭露給網路業者或它方的資訊）。然而，網路平台業者卻可能

---

[162] *Id.* at 58-59.

[163] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 Stan. Tech. L. Rev. 431, 464 (2016).

doi:10.6342/NTU202002857

利用這些訊息進行「整合分析」，結合外來個資資料進行「交叉比對分析」，並對使用者進行差別行銷，或甚至有時直接影響使用者在網路平台的使用經驗。例如 Google 會根據使用者的瀏覽內容，在頁面顯示依大數據資訊分析所認為與特定使用者喜好相關的商品或服務廣告，或者 Google 也可能分享其大數據分析結果予其它業者，作為其它行銷或非行銷目的，例如選舉候選人或選區選民政治立場分析等等。如此的利用算不算已侵害個資當事人的資訊隱私呢？

以「權利」為基礎的隱私規範通常認為，一旦經個資當事人同意蒐集，所揭露之個資即不再維持個人隱私訊息之狀態。而關於個人的網路網頁使用習慣等訊息，就如同路人在路上的走路方式一般，任何人得觀察與紀錄，且路人也應知悉他人可能察覺或紀錄該等資訊，又個人網路瀏覽習性等訊息僅為零碎資訊，並不具所謂的個人識別性，況且資訊的蒐集與利用並沒有造成個人任何實質或財務上的損害，應不可謂侵害個人資訊隱私。

然而相對的，對以「信任」為基礎的資訊隱私規範而言，如同醫師獲悉病患資訊，或者律師獲悉當事人訊息一般，Google 應扮演一個資訊受託者（fiduciary）的角色，有義務在相對應的社會準則（social norms）下處理受託付的個資，擔負相應的保密義務。相較之下，前章節所論以「權利」為基礎的隱私規範主張即存在若干謬誤：第一、Google 的資訊利用方式有違使用者使用一般網路平台的期待。個人揭露個資訊予網路業者通常系為完成某項交易或使用某些業者提供的服務，但個人未必預期 Google 會轉利用其個資予其它用途。而 Google 對個資的蒐集與使用應該要符合個資當事人的期待，毫無拘束的使用與分析，並利用於行銷、行為預測、差別待遇等目的，由於不符當事人期待或與當事人期待相悖，都應被視為已侵害當事人的資訊隱私。

doi:10.6342/NTU202002857

第二，個資當事人在網路使用過程中產生的瑣碎資訊雖然不具個人辨識性，但集合起來經過演算分析後，還是可能產生高準度的個人辨識性資訊。縱然因為科技的侷限，暫時無法產生具識別性的資訊，但未來發展進步後仍隨時可能使原本不具識別性的訊息轉為具有個人識別性的訊息。又根據馬塞克理論，縱使具個人識別性的資訊被刪除，但當大量資訊集合起來時，由於只有極少的可能他人也揭露相同組合的資訊，去識別性資訊即可能被識別[164]。是以，與其以所蒐集之資訊內容與類別來判斷該資訊是否具個人識別性（例如，台灣個資法現行規定特殊資訊為具識別性訊息），再爭執是否可能結合其它資訊產生具個人識別性的資訊，以分別套用個資法硬性規定的規制方式，不如以系爭個資的利用是否違反個資當事人對資訊蒐集者的「信任」程度以及相應的「社會準則」來判定資訊隱私的侵犯與否，較能符合大數據時代下個資揭露與利用的實際情況。

第三，個資當事人在網路平台所揭露的資料往往並非出於主動與自願，個人並非是在衡量所有個資未來被利用所產生的風險後才選擇揭露，而通常只是為完成某一目的時的衝動，或者是不得以已的程序。例如，本文撰寫期間因應 2019 大陸新冠肺炎（COVID-19）的防疫，各國口罩供應與分配均產生緊張局勢，台灣政府應用大數據科技使民眾利用手機購買口罩，一般民眾在實體店面或藥局購買十分不便利的情況下，選擇自手機透過政府 App 與網站購買口罩，即是一種不得已向網路資訊平台揭露個資的態樣。況且，如前所討論，資訊蒐集者透過網路平台設計包裝，取信於個資當事人，使個資當事人對它產生錯誤或過度的資訊隱私保護假設性期待，誤以為其個資將被完整保護。更遑論如前章節所討論，網路平台資訊隱私政策之告示，通常以超長篇幅加上小字體，個人根本無法有足

[164] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment,* 111(3) Mich. L. Rev. 311 (2012).

doi:10.6342/NTU202002857

夠時間去閱讀與瞭解。故個資當事人事實上並非對其所揭露個資放棄主張隱私的權利。

第四，資訊蒐集者對個資的利用，縱使未必造成個資當事人實質的財務損害，但據相關研究顯示，光是「被預測」這樣的現象，已經造成個資當事人相當程度的困擾與恐懼[165]。並且，若資訊蒐集者濫用個人對它的信任，取得個資後任意挪用，實已未履行資訊受託者義務，無需待損害的發生，個資當事人即應有權向資訊控制者主張違約責任。

第二項 以信任為基礎的資訊隱私

向他人揭露資訊不僅為社會社交的必要過程，亦為社會社交之本質，而個人之所以願意揭露，即是因為個人對他人存在某程度的「信任」，信任個資蒐集者不會濫用或擅自揭露給個人不期待知悉的它方。是以，資訊隱私規範的設計上應要促進個人以「信任」為基礎揭露個資的社會社交功能。

在科技網路高度發展的時代，人人基於生活所需，很難不向外界揭露某些個人資訊。即使個人不使用臉書 Facebook 或部落格、不使用社群軟體與他人交流、不主動在網站上發表含有個資的文章，且不在他人發表下按讚或留言，然為滿足基本生活所需，例如透過網路購物、申辦公務、瀏覽網頁內容或使用網路銀行服務等等，都可能被迫著去揭露個資，包括信用卡信息、瀏覽活動、消費習慣、所在位置以及上網習慣等，在此情況下揭露個資，並不能說是完全出自個人的自主決定。

現行資訊隱私規範，由於受 Warren and Brandeis 所提出「不受干擾權」(right

---

[165] Blasé Ur it al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, at 1, 6-7 (2012). Retrieved from https://cups.cs.cmu.edu/soups/2012/proceedings/a4_Ur (最後瀏覽日: 2020/6/1).

doi:10.6342/NTU202002857

to be let alone）概念、行政機關保護弱勢消費者使其免於受侵害之觀念、或甚至是歐盟的「被遺忘權」（right to be forgotten）觀念之影響，通常把重心放在保護個人自由，使個人免受侵擾之目的。但以「信任」為基礎的隱私規範支持者則認為，當個資隱私遭侵犯時，亦同時破壞了社會的社交交流機制，或違反了某些一般社會大眾公認的社會準則。

就法理而言，以信任為基礎的資訊隱私規範，也為那些無法證實實際損害或財務損害的案件，找到了一個合理的權利主張基礎，當個資蒐集者任意洩露個資，即已違反了它與個資當事人間如同信託關係般的資訊受託者責任義務，個資當事人因此有賠償請求權基礎。事實上，個資遭不當揭露時，個資當事人所受的常是心理的恐懼與萬一個資遭不法利用的擔憂[166]。

另若從積極面的角度觀察，以信任為基礎的資訊隱私規範能強化社會人際間的「信任」，而當個人對組織的信任度越高，個人揭露個資的意願就越高，組織也就能蒐集越多的個資，也就能發展越多越精準的大數據科技技術，向社會推展更有益的應用服務，也能有越多的商機。隨著未來技術快速發展，人類的生活交易形態將不斷變化，以「信任」為基礎的資訊規範將能靈活應用，因為該規範將會隨著當時形成的社會準則變化而變化，適應時空背景下的新交易概念，而不再侷限於以權利為基礎的僵化定義，故本文認為以「信任」為基礎的資訊隱私規範將有助社會的快速發展。

第三項 強化資料受託者的受託義務（Fiduciary Duty）

在傳統以「自主控制、管理」為基礎、「通知與選擇（notice and choice）」為手段的資訊隱私規範制度下，資訊蒐集者一旦於資訊蒐集時羅列其相關資訊處

[166] Spokeo, Inc. v. Robins, 578 U.S. ___ (2016).

doi:10.6342/NTU202002857

理原則，並取得個資當事人同意揭露後，只要其行為不違背所羅列的處理原則，通常無需對個資當事人擔負任何其它責任。表面上看似合情合理，但若將本規範應用於時下資訊科技世代，對於個資當事人的保護則顯為不足。原因是，在資訊科技世代下的生活模式，個人的數位網路生活經驗，幾乎完全取決於程式演算法的設計，即使資訊蒐集者主觀意識上未不法揭露或挪用所蒐集之個資，但經由資訊大數據的程式分析以及應用的結果，亦將影響個人的數位網路生活經驗，並且也可能直接對個資當事人生活造成負面影響。例如，富邦 Momo 購物平台會將其用戶曾經在其購物網站上瀏覽或加入購物車的商品訊息，分享給 Google 或其它業者，當用戶使用 Google 或其它業者服務時，頁面將會自動推薦類似商品給用戶（或者是使用用戶設備的他人），此作為在某些情形下將對用戶造成困擾，例如若個人瀏覽私密性質藥品或減肥美容等產品，他通常不希望類似訊息同時在他工作用的網頁也不斷地出現。

若以「資訊信託」的角度看待資訊隱私，由於資訊蒐集者具有處理、分析與應用資訊的專業能力，且資訊蒐集者的確也想方設法採取各種手段，使個資當事人「信任」其未來會妥善處理個資，資訊蒐集者與個資當事人間即形成一種特殊的信任或信託關係，資訊蒐集者對個資的保密義務並非來自訊息內容或訊息性質本身，而是來自於資訊蒐集者與個資當事人間的「信賴關係」[167]，如此一來，資訊蒐集者無論對個資進行必要或非必要的分析或利用時，即對個資當事人負有相當於善良管理人注意與忠實義務之責任[168]，除不應主動採取違背個資當事人利益之作為，並應確保個資的利用或再揭露不對個資當事人權益產生負面影

[167] Balkin, *supra* note 37, at 1205.

[168] *Id.* at 1183.

doi:10.6342/NTU202002857

響[169]。許多學者也贊同，資訊蒐集者相對於個資當事人的角色與責任，猶如醫師之於病人、律師之於案件委託人，不但應對個資保密，還應擔負不進行與個資當事人利益有衝突之行為的受託義務[170]。

亦有學者主張，使資訊蒐集者擔負受託者責任，將有助平衡網路業者與一般個人間存在巨大磋商能力差異之現象[171]。網路巨擘如 Google、臉書 Facebook 等，對於用戶的線上行為可說是瞭若指掌，但用戶卻對於它們的運作以及大數據應用與演算法毫不知情，就連數據資訊的演算程式也通常受各國營業密秘保護法規的保護，無法被強制要求揭露，用戶僅能完全「信任」網路業者對其個資的處理。因此，這些資訊蒐集者不應只是被動的採取作為，更應有義務採取積極作為為個資當事人利益把關，以符合個資當事人在社會準則下的合理期待[172]。

換言之，從資訊信託的角度觀察，資訊受託者的責任應非僅止於將資訊處理方法及政策撰寫於一只書面通知書上，資訊受託者應注意個資的使用結果不得對個資當事人產生不利影響。例如當 Google 經用戶資訊分析得知某用戶早上有喝咖啡的習慣，Google 可能在收取某咖啡店的行銷服務費後，於導航用戶最佳或最速達路徑上，刻意使該用戶繞道經過該咖啡廳，在用戶不知情的情況下，致使用戶多耗費了不必要的交通時間，此即已對用戶造成不利影響的例子。又例如，當資訊蒐集者將用戶訊息提供予第三方分析使用時，資訊蒐集者應確保該第三方也採行與其相同或不低其資訊處理準則的資訊隱私標準，若第三方採取不同的方法或較低的資訊處理標準，陷個資當事人於不利益時，則原資訊蒐集者亦可說是違背了資訊受託者義務責任。

---

169 *Id.* at 1209.

170 *Id.* at 1208-1209.

171 Waldman, *supra* note 7, at 85.

172 Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground, 67-68 (2015).

doi:10.6342/NTU202002857

資訊受託者亦不應操作與違背個資當事人對它的「信任」。如先前章節所述，科技網路時代下的資訊蒐集者經常利用各種方法使個人產生「信任」，當資訊蒐集者利用用戶對它的信任，謀求其它利益用途時，亦可謂構成違反其受託義務責任。例如，臉書 Facebook 利用用戶接受朋友訊息分享的功能，使用戶願意向 Facebook 提供基本資訊與時常更新其狀態，當用戶朋友參與某活動時，亦提示給用戶，讓用戶產生情感上的連結與信任，當用戶的朋友更新狀態時，亦隨時對用戶推播，塑造用戶能取得第一手資訊的印象。然而，Facebook 卻時常利用用戶因此所產生的信任謀取利益，例如，Facebook 常在用戶瀏覽朋友訊息的首頁中插入各類廣告，並且使廣告內容呈現方式與用戶的發文樣式相似，或直接標示用戶的某某朋友或多少朋友也對該廣告或產品表示喜歡或按讚等信息，企圖將用戶對朋友的「信任」轉移至對所推廣產品或活動上，從資訊信託的角度而言，此亦有違資訊受託人的受託者義務責任[173]。

綜上所述，資訊蒐集者實際上扮演資訊受託者的角色，所應擔負的責任，除受託合約上的義務及民法上的責任外，尚應包含依相關行業行為準則與社會通念以及委託人的合理期待，善盡管理人注意與忠實之義務。

- 違反資訊受託者受託義務的類型

資訊控制者的受託義務之違反主要可分為四種不同態樣，分別基於不同理論：第一，使用者操縱之禁止 (Anti-Manipulation of the User)。資訊蒐集者基於自身的利益考量，隱蔽地運用個資當事人資訊於其營業計劃，此又可分為 2 種情形，一是資訊控制者違反個資當事人的對個資應用的選擇自主，私自挪用個資而違反個資當事人意志；二是資訊控制者在未詢問個資當事人的情況下，擅自為個

[173] Waldman, *supra* note 7, at 88-92.

doi:10.6342/NTU202002857

資當事人選擇個資利用項目，有論者認為，唯有個資當事人事先知悉所有選項，他（她）才能夠真正做出有利於己的決定，而資訊控制者擅自為個資當事人決定即已違反受託義務。另一個與本態樣相關的作為是目標導向廣告（Target Advertising），也就是資訊控制者基於分析所得之個資當事人興趣播送廣告，但此作為並不能說是違反受託義務，原因是基於社會常態的長期運作，個資當事人早已熟悉廣告業者如此的操作手法，個資當事人已有足夠戒心，故通常並不見得會盡信此等行銷廣告，故並不能合理期待使用者因而被該行銷廣告所操縱。[174]

第二，反歧視（Antidiscrimination）。資訊控制者利用個資大數據分析對不同個資當事人施以差別待遇不但可能已違反一般憲法保障的平等權，也被視為違反受託義務。通當可細分為三種形式，一是網路業者基於個資選擇性地允許或拒絕提供服務；二是網路業者基於個資分析，對不同個人施以同樣商品差別定價；三是網路業者基於個資分析，為特定個資當事人標註特性，例如網路保險業者拒絕提供某些保險服務或利益給居住於特定地區的居民；又或者曾經發生於美國補教業的例子，普林斯頓機構報價給亞裔的 SAT 考試準備學費較其它種族貴，原因可能是因為，經分析亞裔學生對於補教學習通常較願意花大錢，儘管有論者以市場自然供需為其辯解，但仍不應允許業者基於種族而為歧視之措施[175]。

第三，第三方資訊分享的限制（Limited Sharing with Third Parties）。即資訊控制者分享給包含所謂合作夥伴的第三方，首先當然是必須判斷該第三方是否符合一般個資當事人所應預期，例如若使用網路平台購物，又選擇信用卡付費，則消費者即應預期其信用卡財務資訊會被轉送給銀行或信用卡公司，但若網路平

---

[174] Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33(1) Berkeley Tech. L. J. 1, 18-21 (2018).

[175] *Id.* at 26-30.

doi:10.6342/NTU202002857

台將個資轉傳給其它網路平台或其它研究機構做個資分析，則因為個資當事人可能不知曉第三方的存在，或者第三方未能履行如同資訊控制者相同的義務，而被認為是違反資訊受託義務[176]。

最後第四，也是最常見的違反公司自己的隱私政策（Violating the Company's Own Privacy Policy）。個資當事人通常也期待網路業者將以其所公告的個資隱私政策處理所託付之個資，若有違反也將被認為是同時違反了資訊受託者的受託義務[177]。

- **網路科技業者應擔負多少資訊受託義務責任？**

若肯認為網路業者須對個人用戶擔負資訊受託者責任，那麼下一個問題是，究竟應擔負多少責任才算足夠。就此，有論者主張，商業市場的競爭自然會迫使網路業者主動去採取較為完善的資訊隱私措施，擔負起應有的受託義務責任，以網路產業之產業特性與市場面思考，個資的蒐集與應用對於某部分網路業者的營運而言至為重要，譬如像 Google 或臉書 Facebook，對這類依賴資訊量與資訊分析作為發展創新服務的網路業者而言，個資是最有價值的資產，也是經營成敗的關鍵，市場機制會對其形成一定程度的壓力與約束力，而個人在自由的市場裡自然會選擇與那些採行較完整嚴密之資訊隱私政策業者進行交易，業者為了獲得客戶青睞，自然會去加強資訊隱私保護，也會與其競爭者在資訊保護措施上較勁。

然而，不可否認的，市場機制的運作可以淘汰一些對於資訊隱私管理較鬆散或者屢傳爭議的業者或資訊蒐集者，但市場機制卻無法隨時有效率地監控所有

[176] *Id.* at 36-39.

[177] *Id.* at 43-45.

doi:10.6342/NTU202002857

進行中的個資濫用行為，那是因為網路業者與個人用戶間存在相當顯著的資訊不對等現象，一來是網路業者的大數據演算法通常被歸列為非公開的營業秘密，二來是即使網路業者公開大數據分析及應用方法，大部分的個人用戶仍然無法實際監督業者是否如實履行承諾，更無法預知網路業者未來是否採行或採行何種變更與創新的資料分析方法與商業模式，個人用戶無從分析與瞭解業界競爭者在未來的個資處理與運用是否實不違背用戶利益，且當掌握個資數據企業大到一定程度，貢獻資料的個資當事人對其將失去議價能力。個人用戶頂多僅能依賴網路業者的一般性評價或者商譽，想像其個資與利益「大概」會被某有名氣的網路業者完好的保護。

所謂過猶不及，若法規範上要求所有網路業者皆必須盡到如同律師之於委託人、醫師之於病患、或金融業者之於客戶般同等高規格的資訊受託者義務責任，則顯然是矯枉過正。在資訊科技快度發展的世代裡，網路業者的經營本質應是創意、創新與富具變化的，其經營模式、商業模式、產品與服務模式以及資訊分析方法等都正持續不斷的改變與優化，要求網路業者應要擔負如醫師、律師、金融機構同樣固定且絕對的保密與資訊受託義務，恐將有礙網路科技產業的快速發展，亦非社會所樂見。畢竟，個資本身就是大數據科技產業發展中最重要的資源。

既然受託義務源自個人用戶對網路業者的「信任」，則網路業者受託義務責任之輕重即應與該「信任」的程度成正相關。由於網路業者經營的形態、項目、行銷模式等等均有所不同，並不應要求所有網路業者都應擔負完全相同程度的資訊受託者者義務責任，對於那些大量宣傳將會對用戶資訊嚴密保護或傳遞類似訊息的網路業者而言，個人用戶對其信賴程度自然越高，個人對它保護個資的期待自然也就越顯著。例如，Apple 公司一直以以不斷向其手機與線上服務用戶

doi:10.6342/NTU202002857

保證，將會以最高科技與嚴密的機制保護用戶個資，未經用戶同意絕不向他人揭露個資。經過了十數年的經營，Apple 公司產品用戶普遍也「信任」Apple 公司的隱私保護政策與措施，故 Apple 公司即需擔負較其它小型網路業者較重的資訊受託者義務責任。

衡量受託義務責任的輕重時，除了網路業者本身主動對外的承諾外，還應考量網路業者所屬之經營項目的、性質與產業類別，應用網路與大數據科技為經營手段的網路業者何其多元，而當某類型經營模式的慣性因為長期的存在已經形成時，該類型網路業者即應該被賦予符合其大部分用戶期待的隱私資訊受託義務責任。例如，手機支付業者由於處理了消費者的財務資訊，如信用卡、銀行帳戶等，即使未主動積極地向使用者保證保護其隱私資訊，在以信託為基礎規範的資訊隱私責任下，也應被賦予較重的資訊受託者義務責任[178]。又例如，家庭智能設備提供者 Amazon 向客戶販售一種可以人聲控制設備系統的產品 – Alexa，Alexa 能夠隨時聆聽學習週遭的對話聲音，音訊將傳至 Amazon 公司伺服器儲存，個人在家庭內的對話通常是極為私密的，客戶自然信任並期待 Amazon 將不會因為人為或系統的錯誤等將其日常生活對話洩漏予他方[179]。

關於網路業者的資訊受託者義務責任設計，靈活度顯得相當的重要，除不同屬性的網路業者應適用不同程度的資訊受託責任外，對於同一屬性下的個別網路業者，亦應保留部分業者得自行定義的隱私政策與承諾的空間。有論者提出，政府應就已形成社會共識或行為準則的部分，強制網路業者必須履行資訊受託

---

[178] Balkin, *supra* note 37, at 1222-1225.

[179] Caroline Haskins, Am*azon Sent 1,700 Alexa Recordings to the Wrong Person*, VICE, (December 20, 2018). Retrieved from https://www.vice.com/en_us/article/pa54g8/amazon-sent-1700-alexa-recordings-to-the-wrong-person （最後瀏覽日: 2020/5/1）（Amazon 將某 Alexa 用戶的 1700 多則家庭錄音檔內容誤傳給其它用戶。）

doi:10.6342/NTU202002857

者義務責任，而對於尚未形成明顯社會行為準則的部分，政府可提出若干不同類型的激勵方案，例如，若網路業者履行某類隱私資訊處理標準或作為，則可取得稅制上的優惠、司法調查上的安全港原則待遇等。如此的作法將可使網路業者的資訊隱私受託者責任同時在符合市競爭機制，以及不低於社會期待的原則下，仍然兼具保護個資當事人利益及不阻礙大數據科技的發展[180]。

第四項　以信託為基礎規範資訊隱私的優勢

以信託為基礎的資訊隱私規範至少具有以下幾項重要優勢：

第一，以信任或信託觀點規範的資訊隱私是一個以人類社會行為為基礎的規範，它從人際關係與社會互動的角度出發，仔細考量資訊揭露與交付時的各種情境，因而使資訊隱私規範的真義更趨近於當事人所真正認知與需要。否則，若法官僅依據關於蒐集、處理與利用等硬邦邦的個資法令規定審酌資訊隱私案件，即等同司法被迫莫視資訊隱私應具有的社會價值，以及被迫忽略資訊隱私所維護的社交促進之公益目的。

第二，人際交流除了使個人獲得所需資源外，自宏觀角度而言，也促進了社會民主。在網路社群與大數據應用的發展下，透過大數據演算法對個人的分析，人們常常因此被侷限於接收與自己興趣或理念相同的訊息，大幅地減少個人接觸與自己觀點不同或陌生觀點刺激與比較的機會，反而有礙個人自由探索與選擇的權利。與陌生人及它人觀點的交流是需要被相關規範所支持與鼓勵的，資訊科技生活世代下的資訊隱私規範即應當擔負此重責大任，協助個人與陌生人（例如，只有偶然交易或造訪的網站）得無憂地交流，以信任為基礎的資訊隱私規範正可考量個人資訊交流的情境，要求資訊接收者對個資作符合當下情境與社會

[180] Balkin, *supra* note 37, at 1227-1230.

doi:10.6342/NTU202002857

準則的個資處理，而不拘泥於當事人間關係與交流之形式。

第三，由於網路數位的交流具有匿名的先天優勢，使人們原本僅向親密友人談論的資訊，較願意藉由網路與素昧平生的他人交流，此時，以信任或信託為基礎的資訊隱私規範也等同促進了線上的社會交流。

最後，信任或信託的概念在現行相關人際互動的法規範下並不陌生，例如我國的民法第 148 條第二項規定：「行使權利，履行義務，應依誠實及信用方法。」[181]民法第 535 條關於委任之規定：「受任人處理委任事務，應依委任人之指示，並與處理自己事務為同一之注意，其受有報酬者，應以善良管理人之注意為之。」[182]前揭規範下的「誠實及信用方法」與「善良管理人之注意義務」即是基於人際交流所默認的「信任或信託」社會準則概念而來。又例如美國契約法，預設適用於所有契約的誠實善意與公平處理默示約定 (covenant of good faith and fair dealing)[183]亦被認為是源自於信任或信託的社會準則，若締約的雙方沒有對彼此的信任，那麼雙方將會鉅細靡遺的把所有互動的細節寫入合約條款，則將使合約與合作窒礙難行[184]。是以，以信任與信託為基礎規範資訊私不但不違背法規體制，並且有助於在個資交流上落實既有的社會通念與期待。

第五節 Privacy by Design

第一項 基本意義

Privacy by Design 的基本意義源自系統工程概念，強調從產品或服務的設計

---

[181] 民法第 148 條第 2 項。

[182] 民法第 535 條。

[183] Harold Dubroff, *The Implied Covenant of Good Faith in Contract Interpretation and Gap-Filling: Reviling a Revered Relic*, 80(2) St. John's L. Rev. 559, 559–620 (2006).

[184] Waldman, *supra* note 7, at 93-94.

doi:10.6342/NTU202002857

階段，一直到產品或服務的生命週期期間，包含所有組織的所有層級，均納入資訊隱私的考量設計。民主與科技中心（Democracy and Technology Center; by Ann Cavoukian）曾對 Privacy by Design 提出了七大基本原則：第一，主動而非被動反應；預防而非補救 （Proactive, not Reactive; Preventative, not Remedial）；第二，隱私為預設機制 (Privacy as the Default)；第三，將隱私機制嵌入設計 (Privacy Embedded into Design)；第四，以完整實用的正和為目標，而非零和概念 (Full Functionality – Positive-Sum, not Zero-Sum)；第五，由始至終全生命週期的保護 (End-to-End Lifecycle Protection)；第六，具可見度與透明度 (Visibility and Transparency)；第七，尊重使用者隱私 (Respect for User Privacy)[185]。Privacy by Design 的原則應融入世界隱私相關法規範常見的相關準則，包括通知與選擇、知情同意、在地隱私規範適用、匿名與去個人識別化、資訊安全，近用與傳輸途徑規範等規定[186]。尤其在大數據科技領域產品與服務迅速發展之特性下，複雜的資訊流容易產生隱藏的資訊隱私風險，故 Privacy by Design 概念更應被重視，因為一旦產品與服務開發完成，要再回過頭去修改基礎架構將相當困難[187]。

Privacy by Design 的應用上，除了由產品或服務本身的設計著手外，於大數據與人工智慧科技高度發展的世代，資料控制者所利用的個資，可能早已經過多次的移轉，與先前個資蒐集時的初始使用目的也可能已大不相同，故有學者主張，錯誤或偏差的基礎個資，將導致之後資訊分析與應用上產生各種錯誤結論，而此錯誤的結論，將可能在連個資當事人都不知情的情況下，對當事人造成某些實際

---

[185] Center for Democracy and Technology, *The Role of Privacy by Design in Protecting Consumer Privacy* (Jan. 28, 2010). Retrieved from https://cdt.org/insights/the-role-of-privacy-by-design-in-protecting-consumer-privacy-1/. (最後瀏覽日: 2020/5/2).

[186] Eric Everson, *Privacy by Design: Taking Control of Big Data,* 65 Clev. St. L. Rev. 27, 29 (2016).

[187] Peter Schaar, *Privacy by Design*, 3 Identity Info. Soc'Y 267 (2010).

doi:10.6342/NTU202002857

的不利益。例如，金融貸款機構可能因為依賴來自第三方錯誤的個資與信用資訊，提高了當事人的可貸利率或降低了可貸額度；又例如，潛在僱主可能因為依賴他方提供的偏差個資分析，低估了候選人的能力，或拒絕其求職申請。為解決這個問題，學者認為應提早於數據的蒐集與管理階段即融入隱私設計，而維持蒐集過程的高度透明被多數學者認為是確保基礎個資資訊正確的有效方法之一，也就是說，透過 Privacy by Design 的概念，在資訊蒐集與確認階段即應要求處理流程透明，並且嵌入各種必要的交互驗證機制，包含來自資料當事人同意與意見的輸入校正，並彈性適當地調整評估方法，再依評估結果隨時對所蒐集之資料作調整或修正。隨時要求維持個資蒐集與管理程序高透明度的另一個好處是，未來視需要可彈性邀集公私立獨立審查組織或團體隨時介入協助資料正確性的鑑定。關於執行前揭步驟所可能增加的成本，學者也主張，將可與未來因為資訊使用與結論錯誤率降低而減少的成本相抵消[188]。

可想見，Privacy by Design 全面性考量的特質，將使業者在設計與執行上具有一定程度的複雜度，設計者必須同時考慮當地社會準則、隱私法規與道德倫理等層面。然而，Privacy by Design 所能帶給組織的機會卻是相當顯著的，它將促使企業或組織從組織架構與企業文化面，根深蒂固地構建一個重視資訊隱私管理的系統結構，上至經營管理層，下至企業與產品品牌信賴度與品牌價值的建置[189]。

---

[188] Shlomit Yanisky-Ravid & Sean K. Hallisey, *Equality and Privacy by Design: A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes*, 46 Fordham Urb. L.J. 428, 479 (2019).

[189] Everson, *supra* note 186, at 29-30.

doi:10.6342/NTU202002857

第二項 國際資訊隱私法規範相關 Privacy by Design 概念之援引

世界主要國家法規範已陸續可見 Privacy by Design 概念的應用。例如，美國主要推動資訊隱私規範與執行的 FTC，於 2106 年發表了一份報告 *"Big Data: A Tool for Inclusion or Exclusion?"*，該報告顯著地影響了包含美國公平信評法案(Fair Credit Reporting Act)、平等機會相關法規[190]與聯邦貿易委員會法案(Federal Trade Commission Act)等相關大數據領域資訊隱私規範的適用。該報告將個人資訊的應用生命週期劃分為四個不同的階段，分別是蒐集、匯整與儲存、挖掘與分析以及利用等階段，採以類似 Privacy by Design 概念，針對資訊生命週期的不同階段，提出具差異性的資訊處理指導準則。例如，FTC 建議資訊處理或控制業者，除必須在其組織內推廣，並且需於產品發展的每個流程都持續推動消費者隱私維護的必要措施。該報告並具體提出應用之方法，例如執行資安保護、合理的資訊蒐集範圍界定、採用可信賴的儲存設備與處置方法，與資訊正確性確認等程序[191]。歐盟也在 GDPR 第 23 條-義務總則內定有相關 Privacy by Design 之約定。其它國際法規範上，例如第 32 次國際資料保護與隱私委員會通過的設計隱私決議案中，亦有相關 Privacy by Design 的應用援引[192]。

跨國企業組織，或者常態須處理國際業務的事業組織，將最迫切於實施

---

[190] 包含 Equal Credit Opportunity Act, Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Housing Act, and the Genetic Information Nondiscrimination Act. *See*, FTC, Big Data: A Tool For Inclusion Or Exclusion? (2016). Retrieved from https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. (最後瀏覽日: 2020/5/8).

[191] Everson, *supra* note 186, at 34-36.

[192] 32nd Int'l Conference of Data Prot. & Privacy Comm'rs, Resolution on Privacy by Design 1-2 (2010), Retrieved from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/10-10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf. (最後瀏覽日: 2020/5/8).

doi:10.6342/NTU202002857

Privacy by Design。很顯然的，縱使世界對隱私保護的大觀念相似，但各國與各區域資私隱私法規則與細部規定各有不同，近年隨著科技應用創新，相關資訊隱私規範也正不斷演進變化，當資訊跨國界傳輸、移轉與利用時，事業組織業務常常不及等待當地法規範確立後再行變更產品或服務的設計來符合新法規的要求，尤其在立法資訊快速透明的年代，各國競相模仿他國較佳或較嚴厲的資訊隱私規範，例如歐盟的 GDPR，即是各國模仿參考的重要資訊隱私法規範之一。即使企業所註冊國家尚未採以同樣高規格的法制，但難保其業務不會頓時間受新隱私規範影響，故企業組織即有必要建置一套可供動態適用的資訊隱私政策與法遵機制，此時，Privacy by Design 的價值即被彰顯出。

以 PwC 會計事務所為例，為服務全球客戶與符合各國的隱私相關規範，在 Privacy by Design 概念導入的引領下，從資料生命週期的各個環節去分別評估適用的資訊隱私政策，根據 PwC 的實務操作，常須徵詢的主要隱私項目例示如下：

- ✓ 當地國家是否有全國性統一適用的隱私法規？該法規是否強制適用於某些客戶或客戶的資訊？是否有統一適用於某產業領域的資訊隱私規範？客戶必須至少完成哪些項目才能證明合乎資訊隱私規範？
- ✓ 國外法規是否有易讀易懂的版本可供快速與有效的風險分析？
- ✓ 在系爭國家裡，「個人資料」與「敏感性資料」或其它類似的名稱是否代表著不同的意義？分別構成的定義要素有哪些？是否因此須要求客戶採行較高規格的隱私維護措施？
- ✓ 依規定是否必需特別告知資料當事人個資的蒐集目的、使用方法、或者是個資控制者的資訊隱私政策等？
- ✓ 必需提供給資料當事人何等程度的個資近用權利？
- ✓ 資料當事人應必須有何等修改或修正其個資的權利？
- ✓ 客戶、員工、或協力廠商是否可將自系爭國家蒐集的個資跨境

doi:10.6342/NTU202002857

傳輸至其它國家或地區？又個資是否可在其它國家或地區處理分析後，再傳送回原始國？

- ✓ 何種隱私與資安的基本防護是適用的強制性要求？
- ✓ 是否須在系爭國家的資訊隱私監管機關進行必要的註冊或登記？
- ✓ 當地政府機關是否有權要求近用某些個資、搜索個資處理設施或者禁止客戶使用或傳輸某類個資？
- ✓ 當資安出現異常或破口事件時，是否有通報的義務？
- ✓ 組織是否有針對相關人員施行資訊隱私相關訓練的必要？
- ✓ 供應商是否能夠外包相關個資處理的工作？對於外包商是否有盡職調查、簽署合約約定、或監督執行的義務？
- ✓ 當客戶違反某國家法規時，所可能承擔或受裁罰的風險程度為何？[193]

既然有許多隱私規範暫時來說並非於所有國家都強制適用，自然從經營者重視成本角度的考量下，即成為組織 Privacy by Design 推動裹足不前的原因。但企業有必要從競爭優勢的角度來思考，資訊隱私既然是消費者越形重視的項目，施行 Privacy by Design 的企業，由於有較完整的全盤規劃，將較不易產生個資遭濫用或資料處理違法的事件，影響企業組織辛苦建立的品牌形象。操作得好的話，Privacy by Design 與相關保護客戶個資的措施更也能成為品牌推廣的重要利器。以全球最具品牌價值的企業 Apple 公司為例，Apple 公司不僅在產品操作功能上創新，產品行銷全球，近年所增加拓展的影視、雲端、娛樂等事業領域，所處理的全球客戶個資早已打破國界，然而對於個資隱私議題，Apple 公司不但不閃躲，反而是將個資隱私的維護，視為它的重要企業使命。Apple 公司主張已視個資隱

[193] Everson, *supra* note 186, at 39-40.

doi:10.6342/NTU202002857

私為人類的基本權，Apple 公司不僅視保護客戶隱私為其企業使命與價值，並認為保護隱私是 Apple 企業的重要「創新」[194]。也就是說，Apple 不僅止於力求在個資處理上合法，並且致力於從客戶觀點思考、進行隱私設計，此符合前述 Privacy by Design 第七個最高原則的「尊重使用者隱私」，更甚者，Apple 公司將隱私設計定位為產品與服務的重要創新功能。Apple 公司的策略的確奏效，相對於其它競爭者而言，例如華為、三星等，Apple 已搶先在全球市場上建立起高規格隱私設計的品牌形象與品牌價值，以 Privacy by Design 在大數據應用世代下創造了雙贏局面。

第三項 Privacy by Design 的優勢與可解決的問題

- **彌補通知與選擇主流規制的漏洞**

在網路生活逐漸成為生活主流的狀態下，個資的蒐集的方式，已不僅只是來自於個人在各類網站上主動提供的個人資料，更多的資訊還來自個人於網路活動期間所留下的資訊，包含業者設置的用戶端資料 cookie（使用來紀錄網站用戶的各種網頁活動歷程），以及第三方蓄意設置的間諜程式(spyware)以及 deep pocket inspection 程式等，一般個人用戶不易察覺，或不知如何去檢查[195]。同時，越來越多網路業者的經營模式已是把用戶個資的揭露作為交易或服務的對價，若個人不提供資訊，則個人可能立即被拒絕繼續使用網站內容或服務[196]等。

現行通知與選擇（notice-and-choice）的規範，實質上頂多僅能做到「告知」風險，但即使用戶被告知，個人用戶也多不知如何去採取行動，在個資遭違法利

---

194 See, Privacy, APPLE.COM, http://www.apple.com/privacy/ (最後瀏覽日: 2020/5/8).

195 Jennings, *supra* note 159, at 194-195.

196 *Id.* at 201.

doi:10.6342/NTU202002857

用時，個人常不知道如何去減少損失的擴大，無法真正做到「保護」個資隱私的目標。相對的，Privacy by Design 的實施不僅能使業者採取預設措施保護個資，在個資違規事件發生時，亦能使組織即早發現，促使組織快速反應，採行補救措施以降低損害[197]。

另一方面，Privacy by Design 可增加通知與選擇的實質效果。傳統的資訊隱私政策通知內容通常都是由律師在產品或服務開發完成後，再依基本法規範進行撰擬，與產品或服務的開發及應用過程並無相關聯，充其量只是把產品開發者對於個資利用之希望與決定寫入書面聲明，或甚至業者可能直接委由外部事務所，依照制式化的隱私權告知書模版稍加修改後產生，由於撰寫通常是整個流程的最後一步，並無法藉由改變或優化產品或服務的設計與流程來使個資蒐集與利用對個人造成的侵害降到最低，且也無法反應產品或服務隨著應用發展下，對個資的真實應用情形。相對的，在 Privacy by Design 的概念下，由於在產品或服務開發階段即與法規範人員與資訊隱私管理者進行溝通，進行個資蒐集必要性與利用方式等之審視檢討，包括蒐集範圍、儲存期限、分享對象以及應用環節、何種適當的通知方式（文字、聲音、圖文等）才能使個人在特定情境下瞭解個資被利用之情形等。如此的設計能夠使資訊隱私的通知成為產品與服務系統中不可分割的一部分，也由於每次通知內容經過產品設計者與法遵人員的溝通，將使所通知內容更貼近產品與服務的特質，並能反應使用者使用產品或服務當下的情境背景[198]，使通知與選擇更具它應有的實質意義。

---

[197] Jennings, *supra* note 159, at 203.

[198] Bruening & Culnan, *supra* note 115, at 571-573.

doi:10.6342/NTU202002857

- Privacy by Design 與 Privacy Enhancing Technologies(PETs)的區別

PETs 系指強化隱私保護技術的開發，例如，加密軟體、匿名技術、瀏覽器外掛程式資料保護技術……等，而 Privacy by Design 系包含更廣泛的隱私規範導入範疇。PETs 技術固然重要，但 PETs 僅能對於那些瞭解科技網路應用與相關隱私風險的個人用戶有價值，對於那些不瞭解，卻又在科技網路生活世代下被迫或誘使在網絡上進行交易或使用服務的個人用戶而言，所形成的保護則顯得相當不足。故應鼓勵企業採行 Privacy by Design 規範原則，將資訊控制者的責任拉展至產品或服務的研發規劃階段，類似防呆設計的概念，在某些一般人容易忽視風險處，加以預設隱私的設計，或者作具體有意義的提示，最終目標確保網路使用經驗是貼進個人對隱私資訊的保護期待，長期而言，建立起用戶與個資蒐集者或控制間的信任，共同促進科技網路應用的發展[199]。

- 解決網路行銷利益誘使下的實際問題

追蹤消費者需求並不是什麼新商業策略，在傳統的商業模式下已行之有年。例如，當消費者為了換取商品折扣或入會贈品而同意加入某零售商的會員時，消費者即等同同意零售商追蹤其消費行為，零售商從消費者的購物行為，分析消費者需求與喜好，再向消費者行銷商品，亦或可提供予廠商設計商品以及預估需求[200]。儘管如此，此相較於網路業者利用如 cookies tracking 技術追蹤消費者網路行為，仍具有顯著差別，網路使用者於瀏覽網頁時，並不如在實體商場購物般做出主動的購買決定，網路使用者可能僅因為與友人談論時，或對某新事物的好奇，亦或者僅為研究或比較某些商品或服務等，因為使用的方便而選擇上網瀏覽相

[199] Center For Democracy and Tech, *supra* note 185.

[200] Penn, *supra* note 127, at 601.

doi:10.6342/NTU202002857

關資訊，但卻因為使用者可能曾在網頁上點擊同意網站利用 cookies 收集資訊的選項，就不自覺地持續地揭露自己在網頁上的行為及隱私資訊。而且，不同於傳統零售商所蒐集的購物訊息，網路業者能透過與使用者在其它網路活動上的各種紀錄，經過精密設計的演算法，推算出使用者的各種隱私資訊[201]。不難理解的，若能掌握潛在消費者的喜好以及需求時機，產品與服務的銷售效率將如虎添翼，自然廠商願意花大錢向那些能準確蒐集個資的資訊蒐集者購買精準的行銷汪道，即使個人自行使用相關防密軟體，企圖保護自己的資訊，然而但在龐大利益的趨使下，網路業者仍會採取各種破解防護的手段以取得個資，並且當個資在網路業者間傳遞時，在傳遞過程或技術上若沒有適當的隱私保護規範，亦可能造成個資不當地被揭露與利用。是以，要求所有資訊處理相關事業單位必需採以 Privacy by Design 規範即顯得相當必要。

[201] Penn, *supra* note 127, at 602.

doi:10.6342/NTU202002857

第五章 結論

資訊隱私就字面上意義經常被解讀為基本隱私權的範疇，而早期即以傳統人身隱私的觀念予以規範，傳統隱私的概念系源自哲學家對人類隱私需求的解釋及定義，通常以人際間的「隔離」手段為核心，例如早期美國以不受干擾權（right to be let alone）為隱私規範基礎，強調個人對自己的思想、情緒和感受等與自身相關的事務，應有決定公開與否的權利。其中又可分為消極的隱私保護與積極的隱私保護，消極的隱私保護系指個人採取各種方法排除對自身事物的外界干擾，與外界作區隔，並藉由區隔來形成對個人隱私的保護，上鎖、穿衣或建置藩籬等即是常見的消極隱私保護手段；而積極的隱私保護系指個資當事人應當要有主宰控制與管理自己事物的權利，亦即人人應可自主決定由「誰」、於「何時」、於何「場合」與在何「條件」下可近用或利用關於自己事物的權利，以展現個人有絕對權利來控制與管理與他人的界線，此觀點源自人民「自治」與「自決」的基礎原則，強調個人唯有透過不被干擾的自主思考以及私下討論，才能夠真正自由表達自我意識。從哲學的觀點來說，個人被監視的事實即已降低了其人格性，當人民生活在被監視之狀態，個人的獨立理性思考、評判能力與自由即被剝奪，人民真實的自我隨之遭受扭曲，除此之外，也易造成對被監視者的歧視。此以「主宰控制、管理」個人事物為基礎的隱私權概念，深刻影響包括美國及歐盟的資訊隱私規範，現行多數資訊隱私法規中通用的通知與選擇機制即是源自於主宰控制與管理自我資訊的概念。

縱使傳統隱私概念與規範立意良好，但其強調個人意識決定個資狀態的基本精神，於大數據世代下資訊隱私的應用上卻顯得格格不入。觀察個資當事人在大數據世代下的生活，經常是在不知情或別無選擇的情況揭露個資，從個人電腦、

doi:10.6342/NTU202002857

網頁瀏覽器、手持裝置到家用、商用與公用的各種感測器，個人資訊無時不刻的被揭露與蒐集，而其中許多的揭露並未涉及個人自主意識的決定，因而產生網路業者對個資的利用是否真正符合個資當事人所同意與期待之質疑，再加上個資資訊流在各網路業者間秘密的流動，令人不甚懷疑，在大數據應用世代裡，個資當事人是否早已失去對其個資的主宰控制與管理能力？

有鑑於此，學者專家始對個人資訊與揭露的本質從新審視，在大數據科技快速發展的時代，數據被稱為是 21 世紀最有價值的資源與新時代引擎的石油[202]。個資不但是大數據發展最重要基礎資料，也是大數據產業創造商業價值的重要資源，有論者主張個資對網路業者來說早已不再只是基本用戶資料，而是名副其實的「產品」，網路業者得販售、移轉、分析或利用個資以獲利，亦有論者因而主張應該為個資創造一類新財產權，一方面使個資當事人得以取得交換對價，另一方面又可激勵投注資源建置大數據資料庫與創造價值的網路業者，加速大數據科技產業的發展。然而，賦予個資財產權是否等同是商品化個人資訊，此似乎與保護個資當事人尊嚴與人格的個資隱私規範重要目的相悖，加上行政上管理權利歸屬的困難，以及與相關政府部門對個人財產徵收的法理衝突等，使個資財產權化的構想備受質疑。

然而，保護個人資訊隱私的最大挑戰之一系來自於與言論自由的衝突，除了人民表達的自由外，人民評論與接收各種資訊均被視為言論自由的一環，因為唯有人民充分地汲取各類真實訊息，人民才有能力就自我意識與價值自由地表達與評論，而若因為個資隱私規範的原因使人民無法評論或知悉某些真實的訊息，則似乎違反人民基本的言論自由權。有論者提出以商業言論理論為其解套，但因

[202] 羅鈺珊 (2018)，〈數據經濟下共融成長的挑戰：大數據的兩面刃〉，《經濟前瞻》，第 178 期，頁 87-93。

doi:10.6342/NTU202002857

為並非所有出現於商業活動中之言論都具有單純的商業目的，故難以完整解釋；也有論者提出合約理論，視個資為個資當事人財產，試圖以個資當事人與蒐集者締約的觀點，解釋何以以合約限制個資控制者不得揭露與利用個資的規定並不違反言論自由之基本權，而就法規上關於個資處理的強制規定，則以合約的默示條款釋義，然而，此論點就默示條款無法被締約當事人所變更、個資當事人是否具有締約自由以及默示條款如何適用於無交易慣例可循的新創大數據事業等問題，亦無法提出令人滿意的答案。最後，有論者以個資當事人與大數據蒐集者間資訊嚴重不平等的現象觀察，認為政府介入規制系為確保人民能接收到正確訊息，以捍衛人民言論自由之理由，找到了規範個資利用的合理解釋。

美國與歐盟的資訊隱私法規範基礎結構不同，美國法原則上從消費者保護的角度出發，僅依特別需求對於特定的產業領域設有個資處理規範，例如在健康醫療、財務金融與兒童個資等部門領域均有相關規定；歐盟則基於納粹大屠殺事件的相關歷史淵源，對個人資訊隱私規範較為嚴苛，歐盟視個人隱私的保護狀況為重要的生活品質條件之一，並認為完整的資訊隱私保護得促進商業活動，甚且歐盟對人民個資的保護更直接被列於歐盟基本權利憲章中，人民的隱私被視為是人民的基本權利。但基於人民自治與民主大觀念、自由市場概念與規範執行上的便利性等考量，美國與歐盟最終均以個資當事人「通知與選擇」機制作為主要的資訊隱私規範機制。

雖然「通知與選擇」機制看似合情合理，但卻有它先天上的缺失，例如在現今資訊時代下，電子交易與電子信息平台幾乎已融入一般人的日常生活與各項機能，從手機、電腦、網頁到各式各樣的自動化設備，人們早已對於彈跳出來的個資政策通知不以為意，例行公事般的恣意點核。況且個資當事人大多不具評估

doi:10.6342/NTU202002857

資訊隱私風險的能力，一方面因為大數據科技發展對個資利用之程度尚無可預期，另一方面個人並無法知悉或查核個資控制者實際對於個資的利用情形。在又長又難以理解的個資隱私政策衍然成為常態之際，如此的政策通知對於個資當事人而言是否仍具意義？又鑑於大數據科技與相關商業模式靈活發展的特性，本文認為在大數據應用世代下的資訊隱私問題上，社會真正需要的是一個富具彈性的新資訊隱私管理與激勵機制。

從個人揭露資訊的本質與目的觀察，個資當事人對個資隱私的期待其實系與資訊接收方與自己的關係、交易性質、揭露當下背景情境與當地社會準則等習習相關，就社會社交的角度觀察，個人資訊的揭露是促進人際社交不可或缺的要素，個資當事人系基於對資訊接收者的「信任」而向其交付個資，網路業者如 Facebook、Google 等均以各種方式建構使用者的信任，以減少個資蒐集的障礙，在信任的基礎下，以及個人與網路業者在資訊及知識高度不對等的情況下，是否即應當適用信託關係，並賦予個資蒐集者資訊受託者之善良管理人注意與忠實義務？有了受託義務責任，個資控制者即不應以不利於個資當事人，或者超越個資當事人委託的範圍利用個資，此規範亦為資訊隱私侵害案例中個資當事人往往因證明困難而無法主張損害賠償的困境找到了一個出口。

由於大數據應用世代下的個資揭露與流通的高度頻繁與不可預測性，始有主張應結合相關社會準則，預設性地將資訊隱私思維在產品或服務的設計開發階段即予以納入，並且一直到生產、銷售、服務過程均一併融入設計隱私（privacy by design）的概念。從企業永續經營的角度而言，面對各個法制對於資訊隱私規範的未定性與持續變化，企業應即時納入設計隱私，以因應法規範變更彈性調整企業營運策略。更有企業如 Apple 公司已視企業與產品的隱私功能為一商業競

doi:10.6342/NTU202002857

爭優勢，以此強化品牌形象與商譽。最後，企業的資訊隱私落實也可成為企業社會責任推動的一環。

綜上所述，資訊隱私規範應該從自我保護與隔離的立法基礎，轉變為以促進交流與分享的積極規範；資訊隱私規範方式應該從條文化的硬性規定(hard law)，轉變為一容許因地因時制宜、分等分級分類的軟性法規範 (soft law)，反而能更有效地同時激勵資訊控制者與個資當事人對資訊隱私的重視。與其執著於個資的所有權權利歸屬，不如重視個資的利用權益與衍生利益的分享。有了資訊隱私，個人將更願意分享個資，有了越多的個資，也就越能促進大數據應用科技的進步，為社會大眾帶來越多的生活便利與福祉，這才是資訊隱私規範最重要的目標。

doi:10.6342/NTU202002857

附件一、 GDPR 與 CCPA 概要比較表

	GDPA	CCPA
Individual Rights	✓ Notices to data subjects ✓ Right to access data ✓ Right to be forgotten ✓ Right to fix errors ✓ Right to object to processing/revoke consent	✓ Notices to data subjects ✓ Right to access data ✓ Right to be forgotten ✓ Right to opt-out of sale of information ✓ Right to receive services on equal terms
Security	✓ Appropriate data security required ✓ Breach notification	✓ Appropriate data security required
Service provider	✓ Contractual requirements in service provider agreements	✓ Contractual requirements in service provider agreements
Ability to process data	✓ Permissible Purpose ✓ Data Minimization	None
Data transfers outside geographic location	✓ Adequacy measures required for any country determined to have laws that do not parallel European Economic Area	None
Accountability/ governance	✓ Internal documentation and record keeping ü Designated DPO (if necessary) or other responsible individual	None

資料來源：California Consumer Privacy Act (CCPA) Practical Guide, Bryan Cave Leighton Paisner LLP (Feb. 2020).

doi:10.6342/NTU202002857

參考文獻

一、 中文部分

（一） 書籍

邱文聰（2018），⟨初探人工智慧中的個資保護發展趨勢與潛在的反歧視難題⟩，載於劉靜怡(主編)，《人工智慧相關法律議題芻議》(152-180 頁)。臺北:元照。

財團法人金融聯合徵信中心（2017），《歐盟個人資料保護規則》。臺北：金融聯合徵信。

張陳弘，莊植寧（2019），《新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明》。臺北：新學森。

黃繼兒（2017），《注意!這是我的個人資料隱私》。香港：香港城市大學。

羅伯特·席爾（著），林麗雪（譯）（2020），《隱私危機》。臺北:好優文化。(原著出版年：2016 年)

（二） 期刊

王志誠（2006），〈美國金融隱私權保護法制之發展〉，《台灣金融財務季刊》，7 輯 1 期，頁 71-90。

何明諠(2016)，〈數位時代的隱私邊界:以健保資料庫與 ETC 交通資料庫為例〉，《台灣人權學刊》，3 卷 4 期，頁 139-153。

林其樺（2016），〈個人資料保護、利用與匿名化-歐盟法制趨勢觀察〉，《科技法律透析》，28 卷 6 期，頁 35-42。

林其樺（2017），〈數位浪潮:由歐盟個人資料管理制度與英國匿名化探索資料合理使用〉，《科技法律透析》，29 卷 1 期，頁 17-25。

林錦郎、卓麗香、張松山（2017），〈資訊隱私機制與信任對 Facebook 社群網站使用者行為意圖影響之研究〉，《全球商業經營管理學報》，9 期，頁 13-25。

doi:10.6342/NTU202002857

范姜真嫩（2016），〈網路時代個人資料保護之強化–被遺忘權利之主張〉，《興大法學》，19 期，頁 61-106。

翁清坤 (2013)，〈告知後同意與消費者個人資料之保護〉，《臺北大學法學論叢》，87 期，頁 217-322。

張志偉（2016），〈記憶或遺忘，抑或相忘於網路——從歐洲法院被遺忘權判決，檢視資訊時代下的個人資料保護〉，《政大法學評論》，148 期，頁 1-68。

張志偉 (2017)，〈從資訊自決與資訊隱私的概念區分，檢視被遺忘權的證立問題〉，《萬國法律》，211 期，頁 2-15。

張陳弘（2018），〈新興科技下的資訊隱私保護:「告知後同意原則」的侷限性與修正方法之提出〉，《臺大法學論叢》，47 卷 1 期，頁 201-297。

許炳華 (2016)，〈大數據時代下隱私權之保護-可能之影響暨對策〉，《興大法學》，20 期，頁 129-191。

郭戎晉 (2012)，〈論數位環境下個人資料保護法制之發展與難題–以「數位 足跡」之評價為核心〉，《科技法律透析》，24 卷 4 期，頁 18-40。

郭明煌、廖鴻圖、蕭麗齡、王亭雅（2014），〈資訊隱私顧慮對社群網站使用者使用意圖影響之研究－以 Facebook 為例〉，《資訊管理學報》，21 卷 4 期，頁 341-363。

葉志良 (2016)，〈大數據應用下個人資料定義的檢討:以我國法院判決為例〉，《資訊社會研究》，31 期，頁 1-36。

葉志良（2018），〈因應物聯網發展資料保護法制的革新──歐盟法制的發展與啟示〉，《中原財法學》，40 期，頁 61-127。

詹文凱 (1999)，〈美國法上個人資訊隱私權的相關判決〉，《律師雜誌》，233 期，頁 30-40。

劉定基（2013），〈析論個人資料保護法上「當事人同意」的概念〉，《月旦法學雜誌》，218 期，頁 146-167。

劉定基（2017），〈大數據與物聯網時代的個人資料自主權〉，《憲政時代》，42 卷

doi:10.6342/NTU202002857

3 期，頁 265-308。

劉靜怡（2002），〈網際網路時代的資訊使用與隱私權保護規範:個人、政府與市場的拔河〉，《資訊管理研究》，4 卷 3 期，頁 137-161。

劉靜怡（2010），〈雲端運算趨勢與個人資訊隱私保護〉，《全國律師》，14 卷，2 期，頁 1-14。

劉靜怡 (2012)，〈社群網路時代的隱私困境:以 Facebook 為討論對象〉，《台大法學論叢》，41 卷 1 期，頁 1-70。

賴祥蔚（2010），〈商業言論與憲法的言論自由保障〉，《台灣政治學刊》，14 卷 1 期，頁 159-199。

簡奕寬（2018），〈資料隱私市場與管制政策方向初探〉，《科技法律透析》，30 卷 7 期，頁 33-38。

顏于嘉 (2017)，〈由美國資訊隱私法制觀察被遺忘權在美國的發展〉，《萬國法律》，211 期，頁 25-33。

羅鈺珊 (2018)，〈數據經濟下共融成長的挑戰：大數據的兩面刃〉，《經濟前瞻》，178 期，頁 87-93。

蘇慧婕（2016），〈歐盟被遺忘權的概念發展–以歐盟法院 Google Spain v. AEPD 判決分析為中心〉，《憲政時代》，41 卷 4 期，頁 473-516。

（三） 論文

李誠偉（2015）。《巨量資料產生的刑事爭議-以資訊隱私權為核心》。私立東吳大學法律學系法律專業組碩士論文。

張幼文（2018）。《健康資料之個人資料類別屬性研究—以 IoT 設備之蒐集、處理或利用為中心》。國立政治大學科技管理與智慧財產研究所碩士論文。

張容涵（2018）。《從比較法觀點探討我國個資保護制度之轉型》。國立臺灣大學法律學研究所碩士論文。

doi:10.6342/NTU202002857

陳裕涵（2013）。《網路空間中之隱私權保–以社群網站為中心》。國立台灣大學法律學研究所碩士論文。

黃亦若（2017）。《物聯網時代隱私權問題探討以平衡科技發展與個人資料保護為中心》。國立中央大學產業經濟研究所碩士論文。

劉脩然（2018）。《論社交軟體個人資料之權利性質及其保護》。私立東吳大學法學院法律學系碩士論文。

賴羿慈（2017）。《個人資料保護法制中研究例外規定之比較分析》。國立清華大學科技法律研究所碩士論文。

謝怡均（2018）。《個資法上被遺忘權之研究─從歐盟法出發》。國立中興大學法律學系碩士班學位論文。

鍾孝宇（2017）。《巨量資料與隱私權—個人資料保護機制的再思考》。國立政治大學法律學系碩士班碩士論文。

二、 外文部分

（一） 書籍

Bamberger, K. A. & Mulligan, D. K. (2015). *Privacy on the Ground.* Massachusetts: MIT Press.

Bok, S. (1983). *Secrets: On The Ethics of Concealment and Revelation.* New York: Vintage Books.

Ghezzi, A. et al. (2014). *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten.* London, UK: Palgrave Macmillan.

Goffman, E. (1959). *The Presentation of Self in Every Day Life*. New York: Doubleday.

Golbeck, J. (2020). *Taking Control of Your Personal Data.* Virginia: The Teaching Company.

Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade & Human Rights Perspectives.* Oxford, England*:* Oxford University Press. Retrieved 28 Jun. 2020, from

doi:10.6342/NTU202002857

https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199679669.001.0001/acprof-9780199679669

Hoofnagle, C. J. (2016). *Federal Trade Commission Privacy Law and Policy*. Cambridge, UK: Cambridge University Press.

Mayer-Sho¨nberger, V. (2011). *Delete: The Virtue of Forgetting in the Digital Age*. New Jersey: Princeton University Press.

O'Brien, D. M. (1979). *Privacy, Law, And Public Policy*. New York: Praeger Publishers.

OECD (2002). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, France: OECD Publishing.

Ricoeur, P. (2004). *Memory, History, Forgetting, Chicago.* Illinois: The University of Chicago Press.

Rosen, J. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Vintage Books.

Rosen, J. (2012). *Privacy, Property, and Free Speech: Law and the Constitution in the 21st Century*. Virginia: The Teaching Company.

Rosenzweig, P. (2016). *The Surveillance State Big Data, Freedom, and You, The Great Courses*. Virginia: The Teaching Company.

Smith, H. J. (1994). *Managing Privacy: Information Technology and Corporate America.* North Carolina: The University of North Carolina Press.

Solove, D. J. & Schwartz, P. M. (2011). *Information Privacy Law* (4th ed.). Illinois: Aspen Publishers.

Solove, D. J. & Schwartz, P. M. (2017). *Privacy Law Fundamentals* (4th ed.). New Hampshire: International Association of Privacy Professionals.

Solove, D. J. (2004). *The Digital Person.* New York: NYU Press. Available at SSRN: https://ssrn.com/abstract=2899131

Waldman, A. E. (2018). *Privacy as Trust: Information Privacy for an Information Age*. (1st ed.). Cambridge, UK: Cambridge University Press.

doi:10.6342/NTU202002857

Waldman, A. F. (2018). *Privacy as Trust: Information Privacy for an Information Age*, New York: Cambridge University Press.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

Zetonny, D. (2019). *California Consumer Privacy Act (CCPA) Practical Guide*, Bryan Cave Leighton Paisner LLP.

（二） 期刊

Bagnoli, V. (2015). Competition for the Effectiveness of Big Data Benefits. *International Review of Intellectual Property and Competition Law*, 46(6), 629-631.

Balkin, J. M. (2016). Information Fiduciaries and the First Amendment. *UC Davis Law Review*, 49, 1183-1234.

Ball, D. W. (1975). Privacy, Publicity, Deviance and Control. *Pacific Sociological Review*, 18(3), 259-278.

Bates, A. P. (1964). Privacy – A Useful Concept? *Social Forces*, 42, 429-434.

Ben-Shahar, O. & Schneider, C. E. (2011). The Failure of Mandated Disclosures. *University of Pennsylvania Law Review*, 159, 647-749.

Bruening, P. J. & Mary J. Culnan, M. J. (2016). Through a Glass Darkly: From Privacy Notices to Effective Transparency. *North Carolina Journal of Law and Technology*, 17(4), 515-580.

Chirica, S. (2017). The Main Novelties and Implications of the New General Data Protection Regulation. *Perspective Business Law Journal*, 6(1), 159-176.

Cohen, J. L. (2001). The Necessity of Privacy. *Social Research*, 68, 318-327.

de Hert, P., & Papakonstantinou, V. (2016). The new general data protection regulation: Still a sound system for the protection of individuals. *Computer Law and Security Review*, 32, 179–194.

Determann, L. (2018). No One Owns Data. *Hastings Law Journal*, 70(1), 1-44.

doi:10.6342/NTU202002857

Dobkin, A. (2018). Information Fiduciaries in Practice: Data Privacy and User Expectations. *Berkeley Technology Law Journal*, 33(1), 1-50.

Parker, E. S., Cahill, L., Mcgaugh, J. L. (2006). A Case of Unusual Autobiographical Remembering. *Neurocase*, 12(1), 35-49.

Everson, E. (2016). Privacy by Design: Taking Control of Big Data. *Cleveland Stata Law Review*, 65, 27-43.

Fried, C. (1968). Privacy. *The Yale Law Journal*, 77(3), 475-493.

Gleibs I. H. (2014). Turning Virtual Public Spaces Into Laboratories: Thoughts On Conducting Online Field Studies Using Social Network Sites. *Analyses of Social Issues and Public Policy*, 14(1), 352-370.

Gleibs I. H. (2014). Turning virtual public spaces into laboratories: thoughts on conducting online field studies using social network sites. *Analyses of Social Issues and Public Policy*, 14(1), 352-370.

Harold, D. (2006). The Implied Covenant of Good Faith in Contract Interpretation and Gap-Filling: Reviling a Revered Relic. *St. John's Law Review*, 80(2), 559–620.

Hartzog, W. & Selinger, E. (2013). Big Data in Small Hands. *Stanford Law Review Online*, 66, 81-88.

Hirsch, D. (2011). The Law and Policy of Online Privacy: Regulation, Self- Regulation, or Co-Regulation? *Seattle University Law Review*, 34, 439-480.

Hoecke, M. V. (2015). Methodology of Comparative Legal Research. Retrieved from https://www.bjutijdschriften.nl/tijdschrift/lawandmethod/2015/12/RENM-D-14-00001

Jennings, M. (2012). To Track Or Not To Track: Recent Legislative Proposals To Protect Consumer Privacy. *Harvard Journal on Legislation*, 49(1), 193-206. Available at SSRN: https://ssrn.com/abstract=2074376

Jerome, J. (2015). Big Data: Catalyst for a Privacy Conversation. *Indiana Law Review*, 48, 213-242.

Joh, E. E. (2016). The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing. *Harvard Law & Policy Review*, 10, 15-42.

doi:10.6342/NTU202002857

Joyce, D. (2015). Privacy in the Digital Era: Human Rights Online. *Melbourne Journal of International Law*, 16(1), 270-285.

Kateb, G. (2001). On Being Watched and Known. *Social Research*, 68, 269-298.

Kerr, O. S. (2012). The Mosaic Theory of the Fourth Amendment. *Michigan Law Review*, 111(3), 311-354.

Matthews, S. (2010). Anonymity and The Social Self. *American Philosophical Quarterly*, 47(4), 351-363.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79, 101-139.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus,* 140(4), 32-48.

Pagallo, U. (2017). The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection. *European Data Protection Law Review*, 3(1), 36-46.

Penn, J. (2012). Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet. *Federal Communications Law Journal*, 64(3), 599-616.

Politou, E., Alepis, E., Patsakis, C. (2018). Forgetting Personal Data and Revoking Consent Under The GDPR: Challenges And Proposed Solutions. *Journal of Cybersecurity*, 4(1), 1-20.

Radin, M. J. (2006). A Comment on Information Propertization and Its Legal Milieu. *Cleveland State Law Review*, 54, 23-39.

Reiman, J. H. (1976). Privacy, Intimacy and Personhood. *Philosophy and Public Affairs*, 6(1), 26-44 (1976).

Richards, N. & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review*, 19, 431-472.

Rubinstein, I.S., Lee, R.D., Schwartz, P.M. (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *The University of Chicago Law Review*, 75, 261-285.

doi:10.6342/NTU202002857

Schaar, P. (2010). Privacy by Design. *Identity in The Information Society*, 3, 267-274.

Schwartz, P. M. (2019). Global Data Privacy: The EU Way, Forthcoming. *New York University Law Review*, 94, 771-818.

Selbst, A. D. & Powles, J. (2017). Meaningful Information and the Right to Explanation. *International Privacy Law*, 7(4), 233-242.

Solove, D. J. & Hartzog, W. (2014). The FTC and the New Common Law of Privacy. *Columbia Law Review*, 114, 583-676.

Spiekermann, S. & Novotny, A. (2015). A Vision for Global Privacy Bridges: Technical and Legal Measures For International Data Markets. *Computer Law & Security Review*. Available at SSRN: https://ssrn.com/abstract=3599993

Volokh, E. (2000). Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You. *Stanford Law Review*, 52, 1-65.

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220.

White H. B. (1951). The Right to Privacy. *Social Research*, 18(2), 171-202.

Yanisky-Ravid, S. & Hallisey, S. K. (2019). Equality and Privacy by Design: A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes. *Fordham Urban Law Journal*, 46(2), 428-486.

三、 網路資料

32nd Int'l Conference of Data Prot. & Privacy Comm'rs, Resolution on Privacy by Design 1-2 (2010). Retrieved from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/10-10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf.

Kramer, A. D., Guillory, J. E. & Hancock, J. T. (2014). *Experimental Evidence Of Massive-Scale Emotional Contagion Through Social Networks*. Proceedings of the National Academy of Sciences, PNAS, 111(24), 8788-8790. Retrieved from https://www.pnas.org/content/pnas/111/24/8788.full.pdf

doi:10.6342/NTU202002857

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Article 29 Data Protection Working Party (WP29), Opinion 10/2004 on More Harmonised Information Provisions, v (Nov. 25, 2004), available at www.statewatch.org/news/2004/dec/wp100.pdf.

Malle, B., Kieseberg, P., Weippl, P. & Holzinger, A. (2016). *The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases*. International Conference on Availability, Reliability, and Security (CD-ARES), Aug 2016, Salzburg, Austria. pp.251-266, ff10.1007/978-3-319-45507-5_17ff. ffhal-01635002f. Retrieved from https://hal.inria.fr/hal-01635002/document

Blasé Ur it al. (July, 2012). *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*. Retrieved from https://cups.cs.cmu.edu/soups/2012/proceedings/a4_Ur

C.G. Lynch, A Wake-Up Call for Users in Facebook-Beacon Controversy, CIO. https://www.cio.com/article/2437512/a-wake-up-call-for-users-in-facebook-beacon-controversy.html

CyLab Usable Privacy and Security Laboratory. Retrieved from http://cups.cs.cmu.edu/

Castro, D. and McQuinn A. (2018). *AI Offers Opportunity to Increase Privacy for Users*, International Association of Privacy Professionals. Retrieved from https://iapp.org/news/a/ai-offers-opportunity-to-increase-privacy-for-users/

Dastin, J. (October 9, 2018). *Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women.* Reuters. Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20. https://op.europa.eu/en/publication-detail/-/publication/b48976b5-b31a-4dba-a052-87133e17d65e/language-en.

doi:10.6342/NTU202002857

European Charter of Fundamental Rights. Article 8 Protection of Personal Data states, “Everyone has the right to the protection of personal data concerning him or her.” https://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Commission, ARTICLE 29 DATA PROTECTION WORKING PARTY. (2018). *Guidelines on Consent under Regulation 2016/679*. Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

European Commission, ARTICLE 29 DATA PROTECTION WORKING PARTY. (2017). *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*, Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

European Commission, ARTICLE 29 DATA PROTECTION WORKING PARTY. (2014). *Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks*. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/file s/2014/wp218_en.pdf

European Commission, ARTICLE 29 DATA PROTECTION WORKING PARTY. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing is “likely to result in a high risk” for the Purposes of Regulation 2016/679*. Retrieved from https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=611236

FTC (2010). *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymaker*s. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission -bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101 201privacyreport.pdf

FTC (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-infor mation-practices-electronic-marketplace-federal-trade-commissionreport/privacy2 000text.pdf

Nietzsche, F. (1874), *On The Use And Abuse Of History For Life.* (Translated by Ian Johnston, Vancouver Island University, Nanaimo, BC, Canada). Retrieved from https://pdfs.semanticscholar.org/6784/b376131703bcfa6458f48ee005ae75b8f4f

doi:10.6342/NTU202002857

a.pdf?_ga=2.226574301.1793891829.1593310936-1947095177.1593310936
http://la.utexas.edu/users/hcleaver/330T/350kPEENietzscheAbuseTableAll.pdf

FTC, *Big Data: A Tool For Inclusion Or Exclusion?*: Understanding The Issues (2016), available at https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

Gentry, C. (2009). F*ully Homomorphic Encryption Using Ideal Lattices. In Proceedings of The Forty-First Annual ACM Symposium on Theory of Computing* (STOC '09). Association for Computing Machinery, New York, NY, USA, 169–178. Retrieved from https://dl.acm.org/doi/10.1145/1536414.1536440

Fowler, G. A. (May 28, 2019). *It's the Middle of the Night. Do You Know Who Your iPhone Is Talking To?* The Washington Post. Retrieved from https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/

Haskins, C. (December 20, 2018). *Amazon Sent 1,700 Alexa Recordings to the Wrong Person.* VICE. Retrieved from https://www.vice.com/en_us/article/pa54g8/amazon-sent-1700-alexa-recordings-to-the-wrong-person

Helft, M. (July 4, 2008). *Google Told to Turn Over User Data of YouTube*. The New York Times. Retrieved from https://www.nytimes.com/2008/07/04/technology/04youtube.html?searchResultPosition=2

Item No.141 of European Data Protection Supervisor, "Opinion of the EDPS on the data protection reform package". Retrieved from https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf

Kaye, J., Curren, L., Anderson, N., Edwards, K., Fullerton, S. M., Kanellopoulou, N., Lund, D., MacArthur, D. G., Mascalzoni, D., Shepherd, J., Taylor, P. L., Terry, S. F., & Winter, S. F. (2012). F*rom patients to partners: participant-centric initiatives in biomedical research*. Nature reviews. Genetics, *13*(5), 371–376. Retrieved from https://pubmed.ncbi.nlm.nih.gov/22473380/

doi:10.6342/NTU202002857

Meyer, R. (June 28, 2014). *Everything We Know about Facebook's Secret Mood Manipulation Experiment*. The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

Malle, B. et al. (2016). *The right to be forgotten: towards machine learning on perturbed knowledge bases.* International Conference on Availability, Reliability, and Security, 251–266 (2016). Retrieved from file:///Users/brian15/Downloads/PAML.pdf

Wallace, N. and Castro, D. (2018). *The Impact of the EU's New Data Protection Regulation on AI*. Center For Data Innovation. Retrieved from http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf

President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective (2014). Retrieved from https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf

Privacy Online: Fair Information Practices in Electronic Marketplace: Prepared Statement of the Fed. Trade Comm'n Before the S. Comm. On Commerce, Sci., & Transps. (May 25, 2000). Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health Education and Welfare. Retrieved from http://epic.org/privacy/hew1973report/default.html

Center for Democracy and Tech (Jan. 28, 2010). *The Role of Privacy by Design in Protecting Consumer Privacy.* Retrieved from https://cdt.org/insights/the-role-of-privacy-by-design-in-protecting-consumer-privacy-1/

國家發展委員會，《歐盟個人資料保護規則本文部分》，載於:

https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhl

doi:10.6342/NTU202002857

My00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf

國家發展委員會，《歐盟個人資料保護規則前言部分》，載於:

https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS8wNzMwYmJkZC0yNTVjLTRhN2MtYjc5NS1hMWQ5ODY3OTEwYTYucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5YmN6KiA6YOo5YiGKFJlY2l0YWxzKS5wZGY%3d&icon=..pdf

doi:10.6342/NTU202002857