計畫編號：Y106-A19

106 年委託研究報告

通訊傳播產業資料加值與創新應用趨勢及法令研析之研究

計畫委託機關：國家通訊傳播委員會

中華民國 107 年 1 月

計畫編號：Y106-A19

106 年委託研究報告

PG10607-0163

通訊傳播產業資料加值與創新應用趨勢及法令研析之研究

受委託單位

財團法人資訊工業策進會

計畫主持人

宋佩珊

研究人員

吳柏凭、王德瀛

中華民國 107 年 1 月

目　次

表　次

圖　次

計畫摘要

關鍵詞：通訊傳播、資料加值應用、開放資料、隱私、個人資料保護

一、研究緣起

許多國家近年來大力倡議及推動「開放資料（Open Data）」做為國家發展之重要策略，在各國紛紛跟進推動開放資料的情況下，已逐漸形成一股資料應用革新的新浪潮。這股浪潮以釋出各種全方位資料作為基礎，透過前端科技等工具，將資料附加價值最大化，以創造資料為導向的數位經濟(Digital Economy)。而作為推動數位經濟基礎的科技、媒體和通信（Technology，Media，Telecom，簡稱 TMT)產業，在現今開放資料的發展過程中自然應該扮演不可或缺的重要角色。透過其所保有大量資料為核心，以提供創新及加值服務為目的，其蘊藏的價值極具開發潛力，特別是通訊傳播產業所保有的個人資料，其未來潛在產值更是不可限量。

二、研究方法及過程

為了擘劃我國關於通訊傳播產業資料應用的發展架構，本計畫擬蒐集美國、英國及日本等國家之通訊傳播產業資料加值、資料保護及創新應用等之現況、案例及法制，同時分析、歸納及整理出通訊傳播產業或資料保護之主管機關所採取的相關政策或措施，並檢視於我國現行法令下，通訊傳播產業於資料加值、資料保護與創新應用之際，可能面臨的法令議題，例如：個人資料保護、跨境傳輸、隱私權爭議，以作為我國未來政策與推動措施規劃之參考。

三、主要發現及建議意見

本計畫彙整重要國家通訊傳播產業資料加值與創新相關法制彙整，完成蒐集美國、英國和日本共計 3 個國家或區域之通訊傳播產業將資料加值案例，並分析通訊傳播產業資料加值與創新應用服務等現況、案例及法制。通訊傳播產業資料加值與創新應用相關法制研析，就所蒐集、案例及法制等資料開始分析、歸納及整理出通訊傳播產業或資料保護之主管機關所採取的相關政策或措施及未來趨勢。同時就我國通訊傳播產業資料加

值與創新應用之法制盤點，檢視於我國現行法令下，通訊傳播產業於資料加值、資料保護與創新應用服務可能作法、相關法令限制及挑戰、未來法規修正等議題，所探討的議題包括：個人資料去識別化的標準與應用、資料應用分析產生的歧視議題和資料跨境傳輸與在地化之資訊蒐集及監理趨勢等。並針對前述相關通訊傳播資料加值與創新應用服務之研究，提供我國未來法制政策之建議。

Abstract

Keywords：Communication, value added service, open data, privacy, personal data protection

Many countries have promoted "open data" as a strategy for national development recently, and this lead to a new trend of data revolution. It is to use data from all aspects as foundation, and utilizing high-technical tools to add value for such data to create Digital Economy. Whereas TMT industries TMT inquires which provide their creative and value added services through humongous data shall take important roles in this new trend. The potential of the data is worthy of development and personal data of communication industries is especially invaluable.

In order to organize the framework for development of communication industries using data, this research plans to collect situations, cases, and legal frameworks of value added services, data protections, and creative data using in the U.S., the U.K., and Japan to analyze, conclude, and arrange the policy and strategies of communication or data protection authorities. The research would also overview the legal issues regarding value added services, data protections, and creative data using including personal data protection, cross-border data transferring, and privacy disputes, etc. as references for organizing policies and strategies of enhancing data use in Taiwan in the future.

The research is to Synthesize the legal frameworks of creative and value added services in key countries, completing collecting value added services cases in the U.S., the U.K., and Japan, and to analyze the situations, cases, and legal frameworks of value added services, data protections, and creative data using. Also, we conclude and arrange the policy, strategies, and future trends of

communication or data protection authorities. Besides, categorizing the legal frameworks of value added services and creative data using in Taiwan and over-viewing the possible approaches, legal restrictions, challenges, and legal amendments of communication industries in value added services, data protections, and creative data using, which include standard and usage of anonymous personal data, discrimination from data analyzing, and the trend of authorizing cross-border data transferring and data localization. By researching the previously mentioned issues of value added services and creative data use of communications data, we have provided suggestions for policy of future legal frameworks in Taiwan.

第一章　前　言

第一節 背景分析與研究目的

一、背景分析

早年「開放資料（Open Data）」一詞多用於科學研究領域，參與特定研究計畫合作的科學家有時被要求應對計畫成員「開放資料」，以達成共同研究目標。然而因為當時傳輸技術及儲存媒體的限制，資料分享並非易事，因此開放資料僅止於有限範圍。然而在進入本世紀後，資訊通信技術的革新讓開放資料的成本大幅降低，使得這個議題受到重視。如何讓包括政府、民間業者將手上的資料釋出，和其他不同種類的資料混合、應用，創造新的產值就成為當今最熱門的課題。

歐美主要國家近年來大力倡議及推動「開放資料」做為國家發展之重要策略，在各國紛紛跟進推動開放資料的情況下，已逐漸形成一股資料應用革新的新浪潮。這股浪潮透過前端科技等工具，將資料附加價值最大化，創造以資料為基礎的數位經濟(Digital Economy)。根據艾森哲（Accenture）公司估計，預測 2020 年全球數位經濟產值將達 24.6 兆美元，占 GDP 25%[1]，同時還呈現直線上升的趨勢。

我國也認知到發展數位經濟的重要性，並將開放資料視為發展數位經濟的基礎，故從 2012 年由行政院開始積極推動開放資料的工作。我國在 2015[2]及 2016[3]年連續兩年在開放知識基金會(Open Knowledge Foundation)公布開放資料指標(Open Data Index)評比中名

---

[1] Accenture strategy, DIGITAL DISRUPTION: THE GROWTH MULTIPLIER, https://www.accenture.com/us-en/insight-digital-disruption-growth-multiplier（last visited Oct. 24, 2017）.

[2] Global Open Data Index, http://2015.index.okfn.org/place/ （last visited Oct. 24, 2017）.

[3] Global Open Data Index, http://2016.index.okfn.org/place/ （last visited Oct. 24, 2017）.

列全球第 1，足見相關政策推動的成果。

而作為推動數位經濟基礎的科技、媒體和通信（Technology，Media，Telecom，簡稱TMT)產業，在我國現今開放資料發展的過程中自然應該扮演不可或缺的重要角色。透過其所保有大量資料為核心，以提供創新及加值服務為目的，其蘊藏的價值極具開發潛力，特別是通訊傳播產業所保有的個人資料，對於相關科技之應用、商業模式的創新，都有很大的影響力，其未來潛在產值更是不可限量。然部分資料加值運用方式所涉及個人資料法規之遵循、隱私保護甚至是資安議題，如何在資料應用與權益保護中取得衡平，將會是通訊傳播產業未來提升競爭力的重要關鍵。

二、研究主旨與工作項目

衡酌開放資料發展之趨勢與國家通訊傳播委員會之權責，本計畫擬蒐集美國、英國及日本等國家之通訊傳播產業資料加值、資料保護及創新應用等之現況、案例及法制，同時分析、歸納及整理出通訊傳播產業或資料保護之主管機關所採取的相關政策或措施，並檢視於我國現行法令下，數位匯流產業於資料加值、資料保護與創新應用之際，可能面臨的法令議題，例如：個人資料保護、跨境傳輸、開放授權、資安法制等議題，以作為我國未來政策與推動措施規劃之參考。為達成此目的，本計畫預計工作內容可概分如下：

（一） 重要國家通訊傳播產業資料加值與創新相關法制彙整：

完成蒐集美國、英國和日本共計 3 個國家或區域之通訊傳播產業將資料加值案例，並分析通訊傳播產業資料加值與創新應用服務等現況、案例及法制。

（二） 通訊傳播產業資料加值與創新應用相關法制研析：

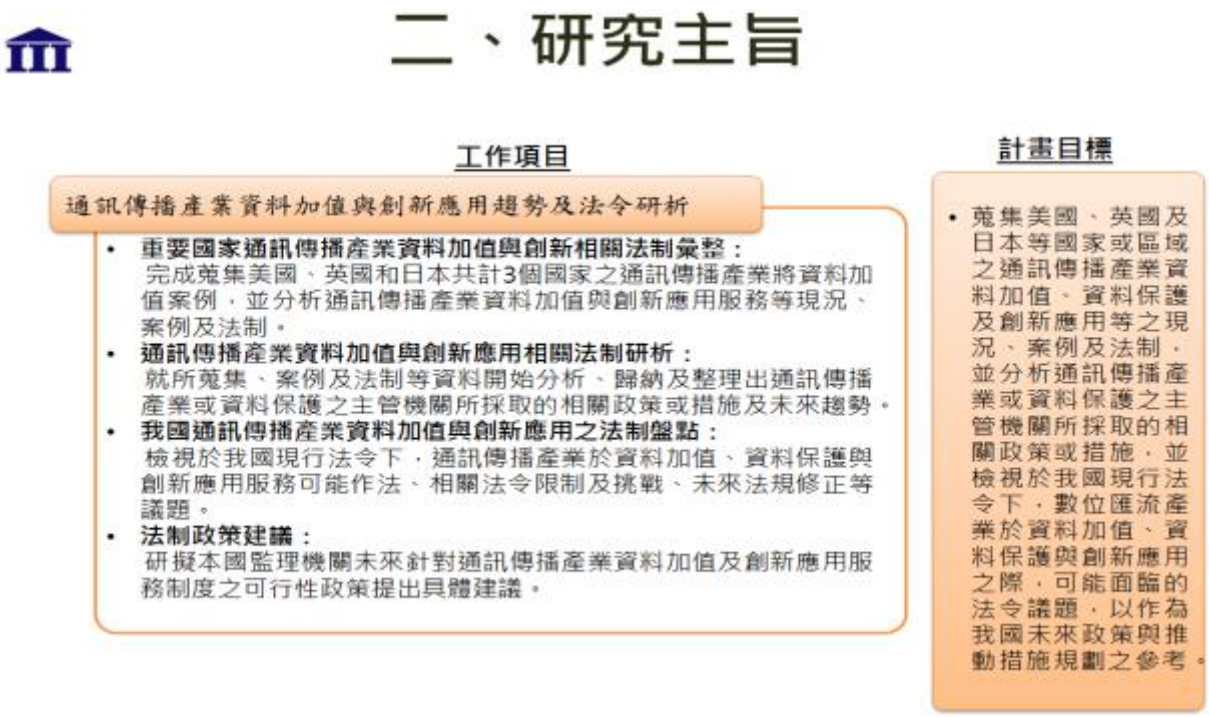
就所蒐集、案例及法制等資料開始分析、歸納及整理出通訊傳播產業或資料保護之主管機關所採取的相關政策或措施及未來趨勢。

（三） 我國通訊傳播產業資料加值與創新應用之法制盤點：

檢視於我國現行法令下，通訊傳播產業於資料加值、資料保護與創新應用服務可能作法、相關法令限制及挑戰、未來法規修正等議題。

（四） 法制政策建議：

研擬本國監理機關未來針對通訊傳播產業資料加值及創新應用服務制度之可行性政策提出具體建議。



資料來源：本研究自行繪製

圖 1-1　計畫架構與目標

第二節 研究方法及步驟

一、研究方法

本計畫之實施將依循計畫執行團隊長期所建立的研究方法論進行本專案之相關研究

(參見圖 1-2 計畫研究方法論)。此一研究方法論主要立基於比較法之研究，其實施步驟主要為（1）確認施政需求(即研究議題)，(2）國際相關政策、法規與措施研析，(3）我國政策與法制現況檢視，(4）研提相關之政策、推動措施或法規調適建議。

（一） 確認施政需求(即研究議題)

計畫執行團隊於委託研究計畫履約期間將與「國家通訊傳播委員會(以下簡稱 NCC)」密切聯繫合作。於簽約後，將透過窗口與 NCC 確認研究範圍、方向等相關細節。於專案執行期間，將隨時配合 NCC 就研究主題範圍內之諮詢，依據 NCC 之需要，提出相關個案資料蒐集及研析建議，作為研究工作項目之一部分。另將評估本案工作項目是否需要進行性別統計分析，並將評估結果列入研究報告及說明理由。

（二） 國際相關政策、法規與措施研析

透過文獻蒐集等方式，檢視追踪國際產業、政策或法規之趨勢，觀測主題主要如下：

1. 蒐集美國、英國和日本共計 3 個國家之通訊傳播產業將資料加值案例。以業者間相互交換資料或是對外開放資料為主。透過案例解析勾畫出整體資料應用的架構。
2. 蒐集美國、英國和日本共計 3 個國家之開放資料法制與政策，分析對於通訊傳播產業資料應用所造成的影響。
3. 就蒐集、案例及法制等資料開始分析、歸納及整理出通訊傳播產業或資料保護之主管機關所採取的相關政策或措施及未來趨勢。

前揭議題之研究分析，選擇美國、英國及日本三個在開放資料有代表性國家之資料為資訊來源，預計將要蒐集的資料除了政府網站像是美國的聯邦通訊傳播委員會（Federal Communications Commission，FCC)、英國的通訊局(Office of Communications; OFCOM)、日本的經產省、總務省外，更包括推動開放資料的私人團體例如：開放資料研究所（Open Data Institute，簡稱 ODI）等。此外，來自各個民營業者的資料也是蒐集的重點，像是美國 AT&T 和 Verizon、英國的 Billmonitor、日本的 Softbank、NTT 等公司的網站，都是重要的開放資料範例資訊來源。

（三） 我國產業、政策或法規之現況檢視

蒐集我國現行法規及現行做法，提出與國外作法之異同比較分析，預期處理的議題如下：

1. 我國通訊傳播產業於資料加值、資料保護與創新應用服務可能作法。
2. 我國通訊傳播產業於資料加值、資料保護與創新應用在法令限制及挑戰。例如：個人資料、隱私、資訊安全及智慧財產權等議題。
3. 我國主管機關對於推動資料加值、資料保護與創新應用服務可行的措施。

（四） 研提相關之政策、推動措施或法規調適建議

本於前揭之研究基礎，提出我國如何推動通訊傳播產業資料加值與創新應用之建議，並就本研究重點以主管機關，亦即是 NCC 的觀點提出相關具體調適建議，以作為未來政策之參考。

採取前揭之研究方法，有以下之正面效益，首先是可以掌握委託單位之需求，能為研究方向進行設定與適時調整。其次是可以透過比較法，標竿國際經驗，作為我國推動措施研擬之參考。最後是透過文獻資料之蒐集，可以掌握國內產業所面臨之問題或政策措施之缺口，同時也可以就所研擬推動之措施廣納意見並凝聚共識，強化相關措施建議之有效性。

二、步驟與流程

本計畫擬在「通訊傳播產業資料加值與創新應用趨勢及法令研析」之框架下進行，參考開放資料或通訊傳播發展法制政策之先進國家，對於通訊傳播產業資料應用發展的現況與推動政策，並提出適合我國的通訊傳播產業資料應用的發展策略。以利作為未來與相關部會協調或合作推動資料應用政策規劃或制度調整之參考。本計畫預計於期中報告完成蒐集彙整美國、日本與英國之通訊傳播產業資料加值應用之案例與法制政策，而期末報告將結合期中報告之研析，盤點我國相關之法制規定，研析我國適合之通訊傳播產業資料加值創新應用之模式，並提出適合我國通訊傳播產業之相關法制政策建議。

資料來源：本研究自行繪製

圖 1-2　計畫進行步驟

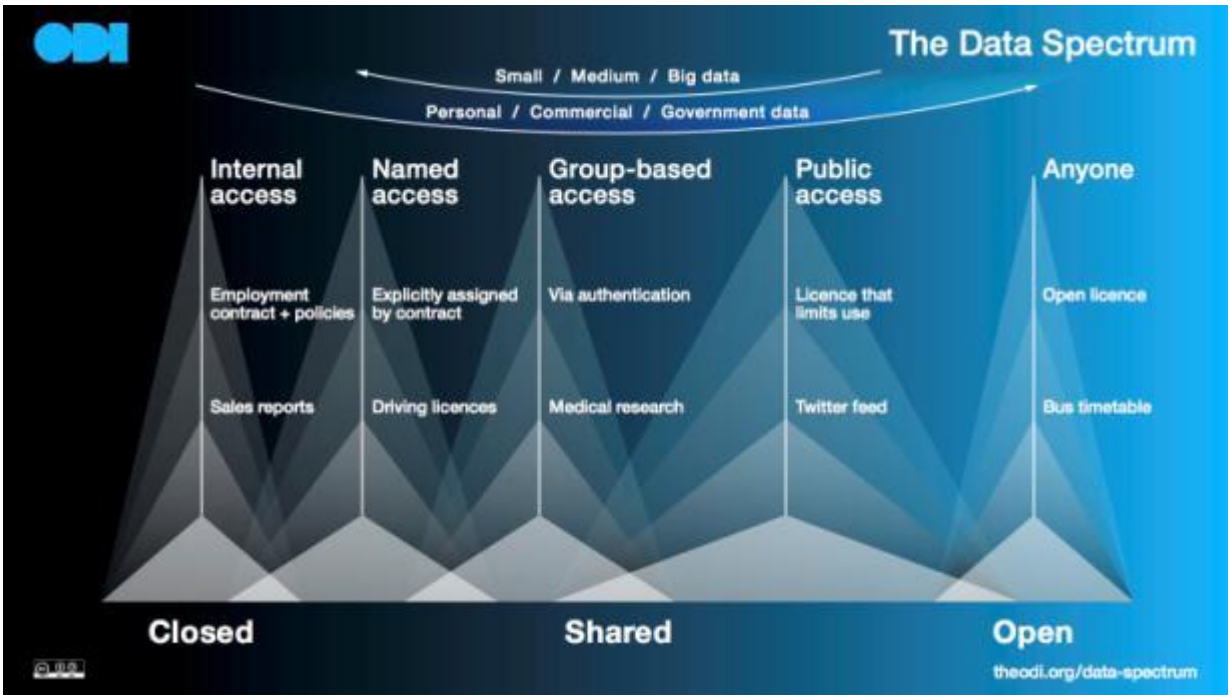
第二章　重要國家通訊傳播產業加值與創新相關法制彙整

第一節 前言

有關資料的分類，原則上可以區分成三種。分別為封閉資料（Closed data）、分享資料（Shared data）、以及開放資料（Open data）。封閉資料為不得對外開放的資料，許多未經法律許可處理、利用的個人資料都屬於此類。而分享資料則是在一定條件下，透過授權得應用之資料，許多公司機關的資料、著作物都屬於此類。相對之下，現在最常討論的開放資料，在細節與操作上具些微的不同，除具有可近用性（例如：開放格式、機械可判讀格式）之技術面要求外，在規範面上則要求「可再利用性」（例如：開放授權條款）。英國「開放資料平台」（data.gov.uk）在詞彙表提供開放資料的定義為：「可被任何人使用、再利用、再傳遞的資料，但僅最多加諸標示、相同方式分享的要求。開放資料的提供可能伴隨費用的收取（charge），但通常不會超出再行產製的成本支出。」[4] 而英國「開放資料研究所」（Open Data Institute, 簡稱為 ODI）將開放資料定義為：「由組織、企業與個人所提供之任何人均可以近用、使用和分享的資料。」[5]不過，資料的種類並非是非黑即白，往往兼有許多性質，介於開放與不開放之間，其分類方式可以參考下圖：

[4] Data.gov.uk, Open Data Glossary, http://data.gov.uk/glossary#letter_o （last visited Dec. 12, 2017）.

[5] Open Data Institute, What is Open Data? http://theodi.org/what-is-open-data （last visited Dec. 12, 2017）.



資料來源：Open Data Institute

圖 2-1 The Data Spectrum

以下關於各國資料應用，也會根據這樣的資料分類模式來分析其開放模式。但需要注意的是，關於分享資料與開放資料的定義分界並非如此鮮明，也有一些設有限制使用條件的資料被當作是開放資料，而與各開放資料組織中定義的開放資料定義有所扞格，在此先予敘明。

第二節 美國

一、概說

美國總統歐巴馬（Obama）於 2009 年上任當日即簽署「透明與開放政府備忘錄」（Transparency and Open Government Memorandum），先行以「政府開放資料」（Open Government Data）為原則進行推動政府資料加值與創新應用。在相關配套公布後，各機關已逐漸發展出用戶參與及釋出資料程序，透過「Data.gov」這個開放政府資料平台，聯

邦政府、各州及城市共開放 194,452（截至 2016 年 3 月止） 項資料集[6]。

雖然美國的政府資料加值與創新應用側重在施政透明化的目的，但不代表美國輕忽資料應用的發展。在 2016 年推出新的資料加值與創新應用工作—「機會計畫」（The Opportunity Project）[7]，從中央建立管道，設立推動「智慧城市」為目標，將政府保有的資料給智慧城市應用的開發者。資料加值與創新應用包含犯罪紀錄、房價、教育、政府職缺等，同時也提供開發工具給開發者，方便進行下一步開發。這個新計畫揭示政府推動資料應用的新方向。

二、應用案例

在這個計畫發展的脈絡下，聯邦通訊傳播委員會(Federal Communication Commission, FCC)就透過平台開放自己保有的資料，並且提供開發工具供程式開發者使用。**該資料使用美國政府的授權宣告，不分是否營利目的，沒有任何使用、分享限制，同時具有機器可判讀性(Machine readable)資料符合所謂開放資料的定義。**

[6] Data.gov, http://catalog.data.gov/dataset (last visited Oct. 26, 2017).

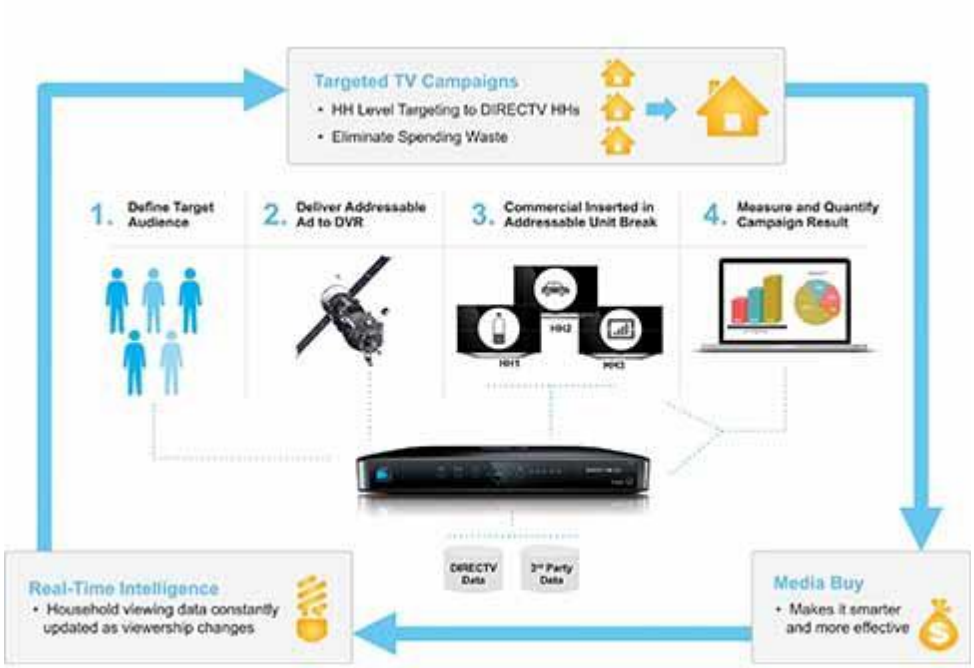
[7] The White House, Fact Sheet: The White House Launches The Opportunity Project," Utilizing Open Data to Build Stronger Ladders of Opportunity for All, https://www.whitehouse.gov/the-press-office/2016/03/07/fact-sheet-white-house-launches-opportunity-project-utilizing-open-data (last visited Oct. 26, 2017).

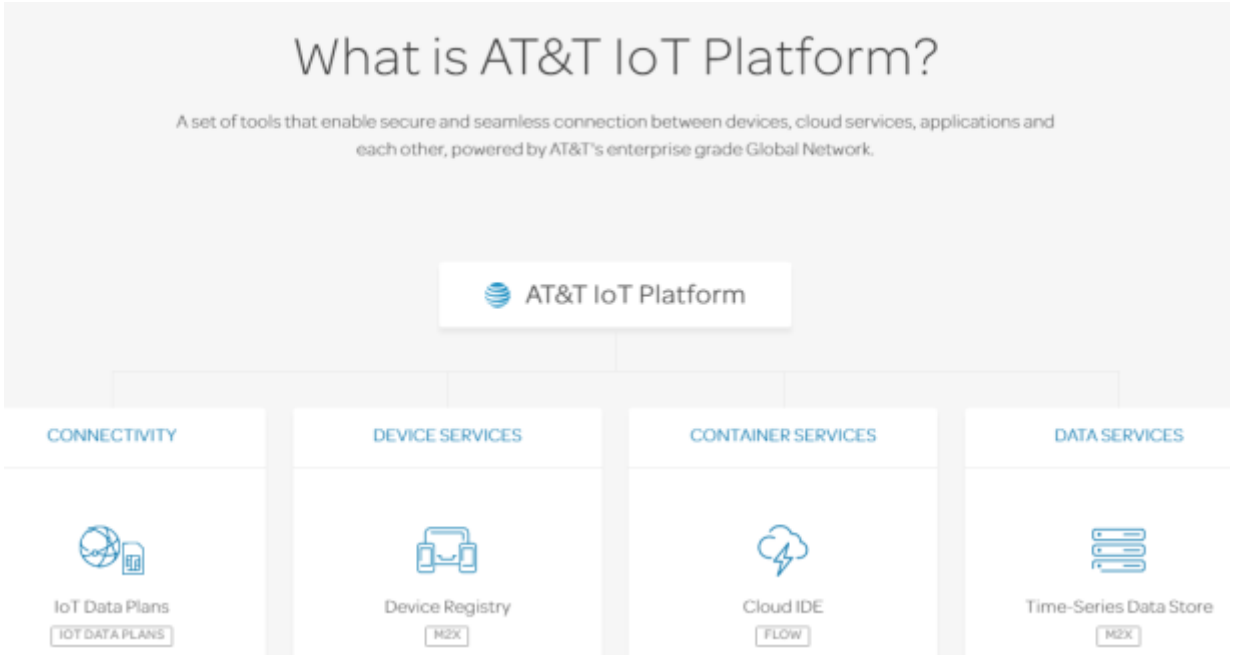
資料來源：opendata.fcc.gov

圖 2-2 美國 FCC Opendata 網頁

另一方面，通訊傳播產業的資料加值與創新應用則是發展盛行。以美國 AT&T 為例，這間公司最大的固網電話服務供應商及第一大的行動電話服務供應商除了有通訊網路服務外，還提供寬頻及收費電視服務。合共 1.5 億戶提供服務，當中 8,510 萬戶為無線用戶。

AT & T 近年推動 IoT 發展，已連接逾 3,000 萬個 IoT 裝置，服務遍及 200 多個國家／地區。透過 IoT 平台不僅能管理大量裝置，且具靈活性和擴展性。用戶毋須重新設計核心 IoT 平台，即可嘗試不同類型的裝置、網路、應用程式、應用程式介面(API)和雲端環境。同時 AT & T 和和 IBM 合作測試了將其 IoT 資料轉化為可分析的形式。通過此項新服務，AT&T 和 IBM 計畫為 AT&T 的企業使用者發掘其工業 IoT 資料的價值，並且將這些資料回饋給參與合作的業者。



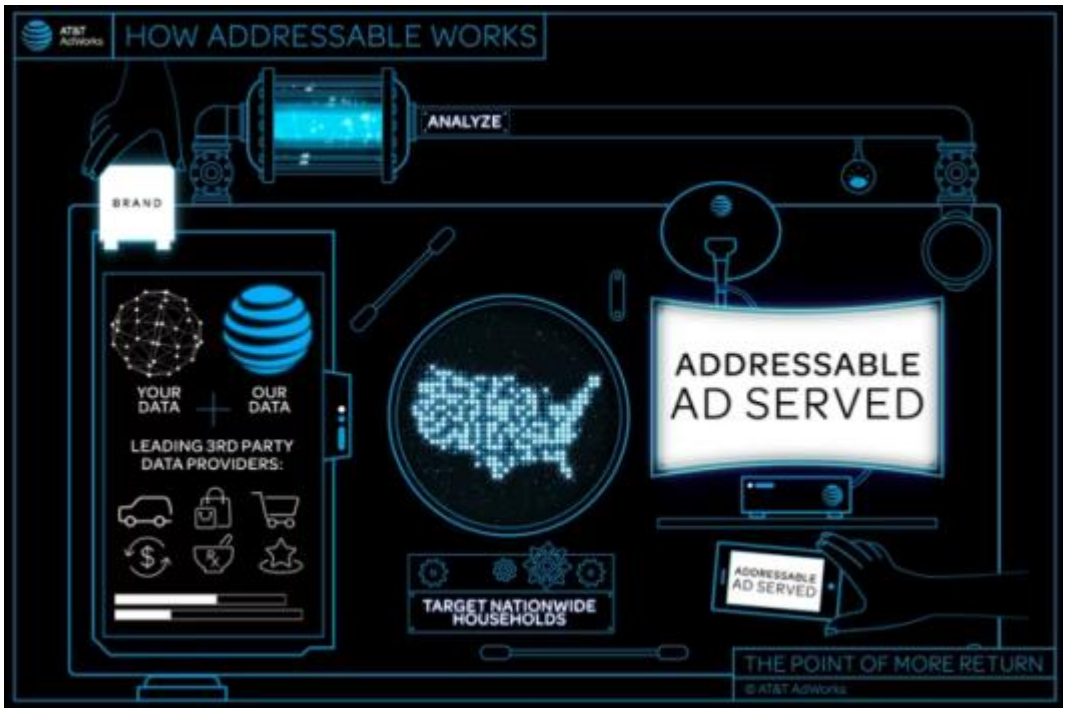


資料來源：AT&T Inc

圖 2-3 AT&T iot 資料加值與創新應用平台

此外，AT&T 和 Verizon 也加入開放運算計畫（Open Compute Project，OCP），這個由 facebook 主導的非營利計畫，OCP 成立至今已 5 年，提供網路、伺服器、儲存、開放

式機架等開源貢獻，並供企業以符合經濟效益的原則打造運算架構，目前已有 Intel、AMD、Broadcom、Cumulus Networks、Mellanox、Accton、VMware 等超過 50 家的軟、硬體業者加入。過去該計畫聚焦於雲端供應商和大企業，現在邀請電信業者加入，將公開電信業用在全球通訊網路的強大交換器和其他設備的設計規格，以增加工作效率、彈性和客製化資料中心技術。



資料來源：Adworks.att.com

圖 2-4 Addressable Plus 功能圖

AT&T 與運營商 DirecTV 合併後將 DirecTV 的電視定向功能與 AT&T AdWorks 資料驅動的 TV Blueprint 解決方案相結合。前者是美國最大的可尋址電視廣告平台。合併後的業務名為 Addressable Plus，目標客戶是有意購買全國電視廣告的廣告商。DirecTV 的定址廣告（Addressable Advertising）平台利用機上盒和第三方資料，以家庭為單位向付費電視用戶推送廣告活動。TV Blueprint 則利用來自數百萬機上盒的匿名和總收視人群專有資料，開發訂製化的、最優化的媒體計劃，以便能更好地將廣告推送給廣告商的目標受

眾群體。這個機制由 AT&T Labs 開發，並對收視群體行為進行逐秒分析。

三、相關法規

（一） 個人資料定義

美國對於個人資料並沒有一個通用的定義存在，不過 2015 年 2 月 27 日發布的「消費者隱私權法」(Consumer Privacy Bill of Rights Act) 草案中對於個人資料有定義。依照第四條[8]的規定，所謂個人資料是指：「對象業者所管理的資料，且一般大眾無法合法地

[8] CONSUMER PRIVACY BILL OF RIGHTS ACT SEC. 4. Definitions:

(a) "Personal data"

(1) In General.—"Personal data" means any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual, including but not limited to—

(A) the first name (or initial) and last name;

(B) a postal or email address;

(C) a telephone or fax number;

(D) a social security number, tax identification number, passport number, driver's license number, or any other unique government-issued identification number;

(E) any biometric identifier, such as a fingerprint or voice print;

(F) any unique persistent identifier, including a number or alphanumeric string that uniquely identifies a networked device; commercially issued identification numbers and service account numbers, such as a financial account number, credit card or debit card number, health care account number, retail account number; unique vehicle identifiers, including Vehicle Identification Numbers or license plate numbers; or any required security code, access code, or password that is necessary to access an individual's service account;

(G) unique identifiers or other uniquely assigned or descriptive information about personal computing or communication devices; or

取得，包括對象業者得連結，或是實務上得以連結到個人，或是關係個人，或是得以連結個人日常使用機器的資料。」，而資料種類包括但不限於姓名、地址、電話、社會安全號碼、護照號碼、指紋、聲紋等生理識別資訊、數字或是字母的網路識別資訊、個人電腦的識別資訊等。

上述規定因為是尚未通過之草案，所以現在仍然不存在通用的個人資料定義。不過其他相關法律像是健康保險可攜式及責任法(Health Insurance Portability and Accountability Act,下稱HIPPA)或是兒童線上隱私保護法(Children's Online Privacy Act）這些特定領域的個人資料保護法律，對於個人資料也都有定義。

（二） 個人資料保護

在美國並沒有針對個人資料保護的專法，而是因應時代變化和領域採取個別立法的措施。1973 年開始確立行動電話和電子郵件的技術、1890 年網際網路商用化開始，於是出現針對這些新技術的個人資料保護政策。而在網際網路開始普及的 1990 年代開始導入關於處理電子資料的法律。而在恐怖活動開始頻繁出現的 2000 年以後，為了維護國家安全的個人識別資訊、以及有識別個人可能性資訊保護法律也開始制定。所以，美國在個資保護的特色，屬於特定部門（sector-based）的保護模式。以下是美國關於個人資料保護的主要相關法律：

表 2-1：美國關於個人資料保護的主要相關法律

內容	法律名稱（中）	法律名稱（英）	制定時間

(H) any data that are collected, created, processed, used, disclosed, stored, or otherwise maintained and linked, or as a practical matter linkable by the covered entity, to any of the foregoing.

確立隱私權的概念	美國資訊自由法	Freedom of Information Act	1974
因應 IT 產業發展，對政府部門進行規制的個人隱私保護法律	美國隱私法	Privacy Act of 1974	1974
金融業的個人隱私保護法律	美國金融隱私權法	Right to financial privacy act	1978
規範收視紀錄使用	視訊隱私保護法	Video Privacy Protection Act	1988
關係電信業的個人資料保護法律	電話消費者保護法	Telephone Consumer Protection Act	1991
生醫領域的個人資料保護專法	健康保險可攜式及責任法	Health Insurance Portability and Accountability Act	1996
針對兒童個人資料保護的強化法律	兒童線上隱私保護法	Children’s Online Privacy Act，下稱 COPPA	1998
防範恐怖攻擊專法，其中有許多關於個人資料保護的規定。	美國愛國者法案	USA PATRIOT Act	2001
防範恐怖攻擊專	國土安全法	Homeland Security Act	2002

法，其中有許多關於個人資料保護的規定。			
關於消費者保護的個人資料保護法	美國公平與正確信用交易法	Fair and Accurate Credit. Transaction Act	2003
關於醫療保險的個人資料保護法律	經濟與臨床健康資訊科技法	The Health Information Technology for Economic and Clinical Health Act	2009

資料來源：A Brief History of Information Privacy Law[9]

其中 1996 年制定通過的 HIPPA，規範目的在於保護個人醫療資料的隱私，對於進出醫療領域的 IT 產業提供一個重要的生醫個人資料保護的標準。同時依照該法規定，生醫資料的開示原則上都需要經過去識別化的過程，所以該法對於去識別化也提供了可供遵循的標準，在下面的章節將會詳述。

歐巴馬政府因為受到 2013 年愛德華・史諾登（Edward Snowden）事件[10]影響，因此開始推出許多關於個人資料保護新法案。2014 年 1 月開始發表關於國家安全局(National Security Agency/NSA)的改革案，限縮 NSA 蒐集、儲存電話紀錄的權限[11]。同年 5 月公布

[9] A Brief History of Information Privacy Law, http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications （last visited Oct. 26, 2017).

[10] Edward Snowden: the whistleblower behind the NSA surveillance revelations, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (last visited Oct. 26, 2017).

[11] Transcript of President Obama’s Jan. 17 speech on NSA reforms, https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsareforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html （last visited Oct. 26, 2017).

重視消費者隱私的大數據政策的報告書[12]。而後歐巴馬總統在美國聯邦貿易委員會（Federal Trade Commission，下稱 FTC）2015 年 1 月 12 日所舉辦的會議上[13]，呼籲聯邦政府應制定「個人資料通知與保護法」(The Personal Data Notification and Protection Act)，該法要求企業必須在資料遭盜取之日起三十天內通報客戶，以保護美國大眾之隱私。同時，歐巴馬總統亦提出制定「學生數位隱私法」(The Student Digital Privacy Act）之呼籲，該法將禁止企業為獲取利益經由學校取得學生資料。而「網路情報分享及保護法」(Cyber Intelligence Sharing and Protection Act，CISPA）[14]也在 2015 年 6 月通過，該法特別強化其網路使用者保護之部份規定；其中包括加強公私部門合作以及深化網路防護安全，藉此妥善處理網路犯罪、保護國土安全等相關問題。

除了上述聯邦法外，還有各州的州法在規範個人資料保護。例如說華盛頓特區和 47 州制定的「資安違反通知法」(Security Breach Notification Laws)，規定當發生個人資料洩漏情事時的通知義務。

（三） 通訊傳播隱私規範

1. 收視紀錄隱私[15]

關於收視紀錄的隱私規範主要是美國在 1988 年因為聯邦最高法院大法官提名人租借

---

[12] The White House Big Data Report: The Good, The Bad, and The Missing, https://www.eff.org/deeplinks/2014/05/white-house-big-data-report-good-bad-and-missing （last visited Oct. 26, 2017).

[13] The White House Office of the Press Secretary,FACT SHEET: Safeguarding American Consumers & Families(2015), http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families （last visited Oct. 26, 2017）

[14] House Passes Controversial Cybersecurity Information-Sharing Bil, http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families （last visited Oct. 26, 2017).

[15]鄭美華, 大數據分析與個人資料保護之衝突：從收視行為調查談起，2017 年 7 月

錄影帶紀錄被公開而制定的視訊隱私保護法（Video Privacy Protection Act，VPPA)。該法主要規範關於錄影帶或類似視訊資料租借、買賣或傳遞上的隱私。依據視訊隱私保護法的規定，視訊內容服務提供者（例如錄影帶出租店）要向他人揭露消費者的個人資料，必須於告知後取得消費者的書面同意[16]。該法對於資料的利用，直接規定只要視訊內容服務提供者曾經以清楚、明瞭的方式給予消費者拒絕的機會，便能在不涉及任何視訊資料的名稱、描述或主題（subject matter）的狀況下，對他人揭露消費者姓名及地址；但如果單純是為了直接對消費者行銷商品或服務，則關於視訊內容主題的揭露就可以例外不受限制[17]。

而在有線電視領域，美國於 1984 年修正 1934 年通訊傳播法（Communications Act of 1934)，增訂「有線通訊傳播（Cable Communications)」專章；其中參考 1980 年的 OECD 的隱私準則，制定了「有線電視隱私法（Cable TV Privacy Act，CTVPA)」，以保障有線電視訂閱戶的隱私權利。其規範內容包括：禁止系統業者在未取得當事人的書面同意下，利用有線電視系統「蒐集」，或向第三人「揭露」有關客戶的「可識別個人資料」[18]；同時規範系統業者必須提供必要措施保護可識別個人資料免於他人的非法存取、並且給予訂戶合理機會以更正相關資料，當原蒐集目的消失後銷毀相關資料[19]。

2. 網際網路隱私

美國於 1996 年修正通過的「電信法」(Telecommunication Act）中第 222 條規定「消費者的隱私保護」，針對電信業者使用消費者的個人資料為限制，除非符合法律規定或取得客戶同意，否則僅能在提供電信服務的範圍內使用客戶專線資訊。但是如果移除客戶識

[16] 18 U.S.C. §2710 (b)(2)(B).

[17] 18 U.S.C. §2710 (b)(2)(D).

[18] 47 U.S.C. 551(b),(c)(A),(c) (B).

[19] 47 U.S.C. 551(d),(e).

別資訊的話，則例外可以在電信服務目的以外利用[20]。

而在 2016 年 10 月，FCC 頒布寬頻網路服務業隱私規則(Rules to Protect Broadband Consumer Privacy)[21]，其核心原則為選擇性、透明度和安全性。

選擇性指 ISP 業者必須獲得使用者許可後才能收集和使用客戶的網際網路瀏覽資訊，當使用或分享消費者之「敏感性資訊」，須事先取得消費者明確之同意。「敏感性資訊」包括精確的地理定位資訊、財務資訊、健康資訊、兒童資訊、社會安全碼(Social Security Number, SSN)、網站瀏覽與應用程式使用紀錄，以及通訊內容等。

透明度是指 ISP 業者必須說明收集哪些客戶資訊，以及如何利用乃至與第三方共享這些資訊。

安全性方面，ISP 業者必須採取合理的措施保護使用者的網際網路資訊等。一旦發生資料洩露，ISP 業者必須在發現後 7 日內通知聯邦通訊委員會，10 日內通知受影響的客戶。當受影響客戶超過 5000 人時，ISP 業者必須在 7 日內通知美國聯邦調查局(FBI)等相關聯邦執法機構。

本規則賦予網路用戶更多對個人資料的控制權。要求 ISP 業者在使用用戶的網路瀏覽、軟體使用、位置資訊及其他與個人資料相關的資料之前，必須徵得用戶同意；並就其收集資料的種類、使用方式、分享對象等事項，也需通知用戶。

然而，這項隱私保護規則受到大力抨擊，特別是網站瀏覽與軟體使用紀錄亦須取得消費者事先同意之部分，認為可能扼殺電子商務發展，消費者也可能被不必要的警示轟炸。同時反對者更批評此規則僅針對寬頻服務商加以監管，但對諸如 Facebook、Google 等大

[20] 47 U.S. Code § 222 - Privacy of customer information, https://www.law.cornell.edu/uscode/text/47/222 (last visited Oct. 26, 2017).

[21] FCC, FCC Releases Rules to Protect Broadband Consumer Privacy, https://www.huntonprivacyblog.com/2017/04/06/president-trump-nullifies-fcc-broadband-consumer-privacy-rules/ (last visited Oct. 26, 2017).

型網際網路公司獲取用戶資料的行為，由於網路服務則由 FTC 管轄，而 FTC 對隱私權之規範較為寬鬆，仍然是使用事後退出的機制[22]，可能發生提供不同服務的兩家業者使用同一份客戶資料，受到的管制程度卻不同，導致不公平競爭的情況。但反對廢除這項規則的主張者強調，用戶在使用搜尋引擎或影音串流服務時，若不同意其隱私規則，可以隨時選擇放棄瀏覽，但他們卻無法輕易放棄正在使用的寬頻服務。因為在美國，可供選擇的寬頻服務商十分有限。

最終，這個隱私規則先是在參議院，接著在 2017 年 3 月 28 日遭到眾議院表決廢除[23]。FCC 將不得再通過其他相同或實質上相同之規範，對 ISP 業者之管制回歸電信法第 222 條規定，亦即對於網站瀏覽與應用程式使用紀錄之使用或分享，不須取得客戶之事先同意。

（四） 小結

美國的開放資料源自於開放政府，透過開放政府資料來達到施政透明化，提升行政效能，其後才逐漸推展到民間業者的開放資料應用。相對於多數國家，美國政府對於民間的開放資料應用並未採取主動推動的態度，而是在隱私、公平競爭的框架下任其自由發展。主管機關 FCC 的作為也比較傾向是作為政府推動其智慧城市資料應用計畫的一環所配合的措施，FCC 本身並沒有實際投入推動通訊傳播產業開放資料的作為。然而就算沒有主管機關的推動，美國民間業者的蓬勃活力仍然將資料應用推到另一個高峰，伴隨著未來 IOT 等技術的活用，未來資料相當值得期待。

---

[22] Washington Bytes, We Should Welcome Trump's Reversal Of FCC Digital Privacy Rules, https://www.forbes.com/sites/washingtonbytes/2017/02/02/how-many-regulators-does-it-take-to-protect-our-digital-privacy/#fa043a1372a0 （last visited Oct. 26, 2017).

[23] Washington Post, The House just voted to wipe away the FCC's landmark Internet privacy protections, https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/ （last visited Oct. 26, 2017).

在法制方面，美國的個人資料保護並無統一適用的專法，而是依照各個領域分門別類制定相關個資保護規則。和通訊傳播產業相關的就是電信法、寬頻網路服務業隱私規則或有線電視隱私法等，特別是寬頻網路服務業隱私規則，對於電信業者影響甚鉅，在蒐集客戶資料前都必須要進行告知，雖然已經遭到廢除，但是從這個立法的攻防過程中也可以看出，傳統用行業別來規管的方式已經不適用於現在多元的通訊傳播環境。目前 FCC 的主席 Ajit Pai 就表示將與 FTC 就寬頻消費者隱私的事項進行合作，更表示應該要把相關的監理工作移到 FTC[24]。

第三節 英國

一、概說

英國資料加值與創新應用之緣起，可溯及至 2007 年「資訊力量審查報告」(The Power of Information: An Independent Review by Ed Mayo and Tom Steinberg)[25]，評估公部門資訊及其線上使用對於公眾生活之影響，包括公部門資訊如何再利用，政府如何投入參與及其對於公眾社群之效益。2009 年 6 月英國首相戈登・布朗（Gordon Brown）邀請全球資訊網發明人提姆・伯納－李爵士（Sir Tim-Berners Lee）擔任英國政府顧問，其對於全球「開放資料」具有重大貢獻，並曾於 2009 年 2 月即呼籲各國擁有資料之單位進行資料釋出[26]。英國之資料加值與創新應用係根據「促進政府及其服務之透明及可信度政策」來推動，英國政府於 2007 年至 2011 年陸續對資料加值與創新應用進行討論與評估，並於 2012 年「開放資料白皮書：釋出潛力」(Open Data White Paper: Unleashing the

[24] Ars Technica, ISPs and FCC Chair Ajit Pai celebrate death of online privacy rules, https://arstechnica.com/tech-policy/2017/03/isps-and-fcc-chair-ajit-pai-celebrate-death-of-online-privacy-rules/ (last visited Oct. 26, 2017).

[25] The Power of Information Review, OPSI, http://www.opsi.gov.uk/advice/poi/index (last visited Oct. 26, 2017).

[26] 行政院研究發展考核委員會，〈政府資料開放加值應用研究分析書面報告〉，頁 14 （2013）。

Potential） 提出具體作法，闡明資料加值與創新應用範圍定義、目標與作法[27]。

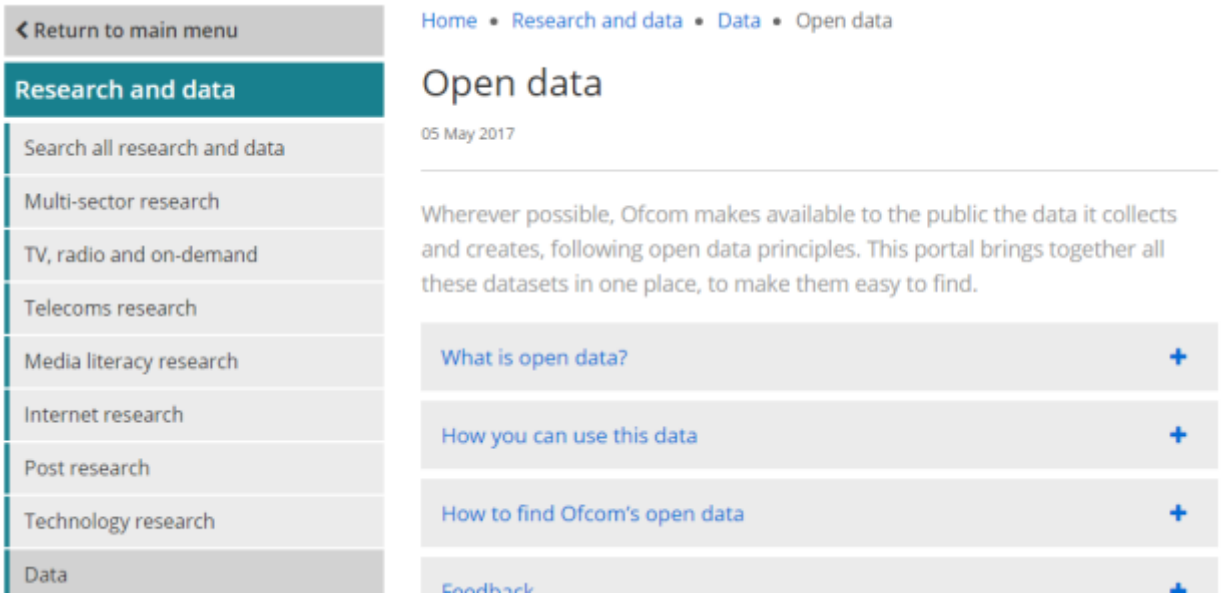
此外，開放資料研究所（Open Data Institute，簡稱 ODI）由提姆・伯納－李爵士創立，屬於獨立、非營利、無黨派之有限公司（limited by guarantee company)。ODI 催化「開放資料」文化演進，以創造經濟、環境及社會價值，同時協助開啟供給、產生需求、創造及散布知識以陳述地方及全球議題。召開世界級專家之合作、孵化、培養與指導新的創意，促進創新。ODI 使任何人皆可以學習及參與「開放資料」，並授權其團隊透過專業教練及指導來協助他人[28]，現今英國多數的民間私部門開放資料都是 ODI 輔導的成果。

二、應用案例

英國的通訊傳播監理機關通訊局(Office of Communications; OFCOM)本身就有各式各樣的資料加值與創新應用，包括費率資料、電信公司資料、市場調查資料、統計數據資料、研究報告資料等。這些資料都是來自於各個通訊業者，而有 Ofcom 放在網站的資料加值與創新應用專區公開。**該資料不含個人資料，且不分是否營利目的，沒有任何使用、分享限制，同時具有機器可判讀性(Machine readable)資料符合所謂開放資料的定義。**

[27] Open Data White Paper: Unleashing the Potential, GOV.UK, https://www.gov.uk/government/publications/open-data-white-paper-unleashing-the-potential (last visited Oct. 26, 2017).

[28] ODI, About the ODI, http://theodi.org/about-us (last visited Oct. 26, 2017).



資料來源：Office of Communications

圖 2-5 Ofcom 資料加值與創新應用網站

而像是電信比價網 Billmonitor，這個原先由牛津大學的資料分析家成立的網站就是利用電信業者和 Ofcom 的關於費率的資料加值與創新應用進行分析，甚至反過來幫助政府制訂政策。Ofcom 就是引用 Billmonitor 的分析資料，發現英國行動裝置用戶有 76%的用戶擁有長期合約，但是每月資料傳輸使用量遠不及應繳月費，導致一年平均浪費將近 200 歐元，所有用戶一年約浪費 50 億英鎊，當消費者更了解自己的使用習慣，將可以選擇更好的消費方案，而國家也能藉由這類的統計資訊，制定相關消費者保護法，維護消費者權益。Billmonitor 蒐集包括用戶的門號、姓名、密碼、通話資料以及 cookie[29]。為了克服個資法的議題，有使用去識別化的技術。

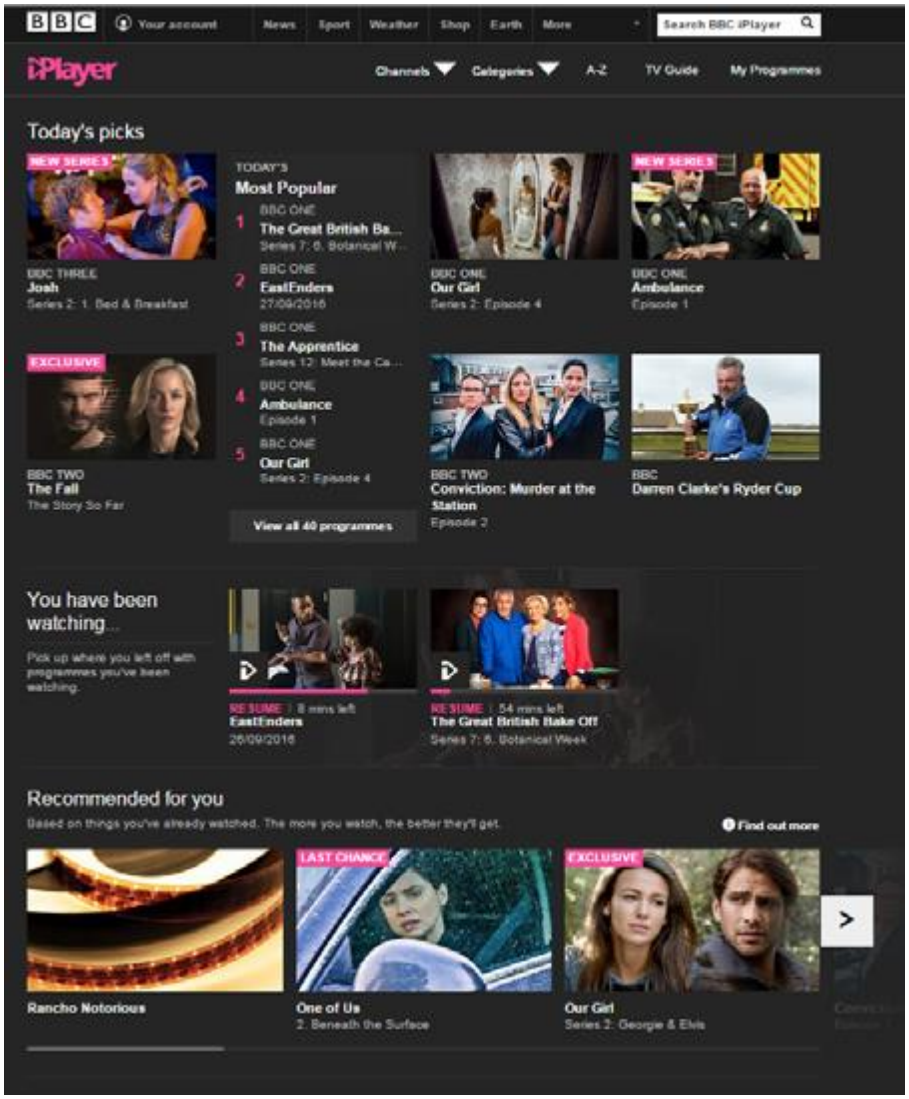
[29] Billmonitor, Privacy and Security Policy , hhttps://www.billmonitor.com/privacy (last visited Oct. 26, 2017).

資料來源：billmonitor

圖 2-6 Billmonitor 官方網站

英國廣播公司（British Broadcasting Corporation，簡稱 BBC)有一網路電視和廣播平台名為 iPlayer，能夠在這平台觀看 7 天內的 BBC 電視和廣播節目。從 2014 年 3 月 BBC 宣布將調整 iPlayer 介面設計，蒐集客戶的收視資料，建立起客製化的影片推薦系統，配合巨量資料運算，自動推薦使用者可能有興趣的片單。同時也建立搜尋引擎的預測系統，配合巨量資料運算，仿效 Google 搜尋引擎，在使用者鍵入關鍵字時，可事先預測使用者可能想要搜尋的片名。其主要蒐集的資料有個人資料，內容包括姓名、地址、電話外，也有 cookie、ip 位置及終端機器資訊[30]。BBC 對於個人資料有明示特定目的並有告知及請求同意。

[30] BBC, Your information & Privacy, http://www.bbc.com/privacy/ (last visited Oct. 26, 2017).



資料來源：iplayerhelp.external.bbc.co.uk/tv/personal_recs

圖 2-7 BBC iplayer

三、相關法規

（一） 個人資料定義

英國資料保護法中對個人資料（personal data）的定義， 指「有關能識別現存個人之資料」(relate to a living individual who can be identified)[31]。然而，因法條

[31] Data Protection Act 1998, Section 1(1), ‘“personal data” means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession

的文字過於抽象，在法條的操作上可能會因為解釋的不同，而造成一般大眾對於個人資料的定義有模糊不清的情形，故英國「資訊委員辦公室」（Information Commissioner’s Office, ICO）發佈了「界定個人資料指導手冊」（Determining What Is Personal Data）[32]，於其中針對資料是否屬於個人資料，做出共 8 項判斷標準。依指導手冊中的判斷標準為認定時，須從此 8 項判斷標準逐一判斷，如符合其中的判斷標準時，則該資料即為英國資料保護法所稱之個人資料。關於指導手冊中的 8 項判斷標準，詳細介紹如下：

1. 可識別性（Identifiability）

首先，第 1 項判斷標準為第 2 項至第 8 項判斷標準的先提要件，須先符合第 1 項的判斷標準後，始得進行下一步的判斷；如若不符合第 1 項的判斷標準，則無需進行下一步的判斷，因為該筆資料即非英國資料保護法所稱之個人資料。

第 1 項判斷標準說明，如果資料可以識別現存之個人，或者資料控制者（data controller）所保有（in the possession of），或可能即將保有（likely to come into the possession of）之資料及其他資訊（other information）可以識別現存之個人時，則符合第 1 項資料具可識別性之標準。

上述判斷標準即在說明若當資料可直接識別個人，或者當資料原先不可直接識別個人，但資料控制者如加上其他資訊而可間接識別個人時，該筆資料即具可識別性。此判斷標準也符合歐盟資料保護指令中對個人資料的判斷標準，亦即個人資料指資料是有關於被識別的（identified）或可被識別的（identifiable）個人[33]。

---

of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.’

[32] Information Commissioner’s Office, Determining What Is Personal Data (2012), https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf (last visited Oct. 26, 2017).

[33] Data Protection Directive, Article 2(a), ‘“personal data” shall mean any information

2.「關於」之定義（Meaning of ‘relates to’）

若資料是「關於」可被識別之個人時，該資料即為英國資料保護法所稱之個人資料。若不確定資料是否有關於可被識別之個人時，從後續第 3 項至第 8 項判斷標準繼續判斷。

3. 資料「顯然關於」特定個人（Data ‘obviously about’ a particular individual）

個人資料必須是具可識別性（第 1 項判斷標準）及關於個人（第 2 項判斷標準）之資料，然若不確定資料是否有關於個人時，第 3 項判斷標準說明，只要資料「顯然關於」特定之個人時，該資料即有關於個人，而為英國資料保護法所稱之個人資料。舉例來說，特定記錄記載個人的工作表現或運動狀況，皆是顯然關於個人之資料。

若資料非「顯然關於」特定個人時，則從後續判斷標準繼續判斷。

4. 資料可被連結至個人（Data linked to an individual）

若資料「可被連結」至個人而導致產生個人之特定資訊時，該資料即為英國資料保護法所稱之個人資料；若資料不可被連結至特定個人時，則從後續判斷標準繼續判斷。

5. 資料處理之目的（The purpose of the processing）

若資料用於或即將被用於影響（influence）一些行動或決定，而該行動或決定會影響可被識別之個人時，該資料即為英國資料保護法所稱之個人資料；若非如此，則從後續判斷標準繼續判斷。

6. 傳記重要性（Biographical significance）

若資料具有任何個人的傳記重要性時，該資料即為英國資料保護法所稱之個人資料；若資料不具傳記重要性時，則從後續判斷標準繼續判斷。

判斷傳記重要性即為考量資料是否有記錄個人之生活資料，並須考量資料的處理是否影響或可能影響個人。舉例而言，若當資料具有關於個人於特定時間點的行蹤或行為資訊，該資料即可能具傳記重要性。以更明確的例子舉例，若會議紀錄中有記載出席人員之資料

---

relating to an identified or identifiable natural person….’

時，因個人於特定時間之行蹤已被記錄於會議紀錄中，該紀錄即具有傳記重要性。

7. 資料是否集中在特定個人上（Does the information concentrate on the individual?）

若資料的核心主題專注集中在特定個人上時，則該資料即為英國資料保護法所稱之個人資料；若非如此，則從後續判斷標準繼續判斷。

8. 資料處理對個人產生巨大影響(Processing which has an impact on individuals)

若資料對於個人本身或其家庭、工作或專業能力造成重大影響或將可能造成重大影響時，該資料即為英國資料保護法所稱之個人資料；若資料不會造成巨大影響時，則該資料非為個人資料。

（二） 個人資料保護

為保護人民對其隱私所享有的權利，尤其當人民的個人資料被他人處理或利用時，歐盟於 1995 年 10 月通過歐盟「資料保護指令」(Data Protection Directive），該指令並於同年 12 月施行生效；身為歐盟會員國之一的英國，其國內的個人資料保護規定必須落實並符合歐盟對於個人資料保護所訂的相關規定，因此，英國為因應歐盟資料保護指令的施行，於 1998 年通過英國「1998 年資料保護法」(Data Protection Act 1998，本文以下簡稱「英國資料保護法」)，取代原先所制定的「1984 年資料保護法」(Data Protection Act 1984)。為使英國人民、企業及組織接受數位時代的變革，並確保英國做好脫離歐盟（European Union）的準備，英國數位文化媒體及運動部（Department for Digital, Culture Media & Sport）修正 1998 年的資料保護法（Data Protection Act 1998），於 2017 年 9 月 14 日，提交 2017 資料保護法草案（Data Protection Bill 2017）予上議院審議，以因應數位時代的來臨，法案內容配合即將於 2018 年 5 月施行的歐盟的一般資料保護規則（General Data Protection Regulation，簡稱 GDPR）有許多修正[34]。新法令將

[34] Data Protection Bill 2017, https://www.gov.uk/government/collections/data-protection-bill-2017 (last visited Oct.

讓英國民眾握有更大的資料控制權，諸如被遺忘的權利，或是要求業者移除他們的個人資料。這意味著人們可要求社交媒體刪除他們小時候所張貼的內容，企業也不得在未取得明確同意的情況下蒐集用戶資訊。同時，新版的英國資料保護法案的重點涵蓋了讓民眾更容易撤回業者對個人資料的使用；允許民眾要求企業刪除所保留的個資；家長與監護人得以決定兒童資料的使用；處理機密個人資料時必須取得明確的同意；將個人資料的範圍擴大到 IP 位址、cookie 與 DNA；讓民眾更容易要求企業揭露所持有的個人資料；讓客戶更容易在不同的服務供應商之間移轉資料。

（三） 數位經濟法案

英國商業、能源與產業策略部 BIS(Department for Business, Innovation & Skills，現已改為 Department for Business, Energy & Industrial Strategy)鑒於現在很多商業活動使用數位形式表現，但本身並不產生交易或是該活動本身僅透過網路使用，因而使這部分數據未被計算在數位經濟的經濟利益中，故政府為了蒐集真實世界的數據，希望透過提供標準及活動的代碼(coding)方式，以便於更準確量測政府數位化產品的分布以及政策決定的影響。除此之外，英國文化、媒體、體育部 DCMS(Department for Culture, Media & Sport)則是支持英國科技城市(Tech City)，為了幫助英國的數位化產業，DCMS 專注在數位技術、資本投資以及國際化發展等方面，希望數位化產業等。在這樣的背景之下，為了要讓英國成為數位化產業發展的引領者，DCMS 和 BIS 共同起草英國的數位經濟法案[35]。

透過本法，允許設計者採取新的方式(網址連結)進行智慧財產權的公告，而英國智慧財產權辦公室(Intellectual Property Office)也將確保英國數位企業能夠以簡易的方式獲取有關智慧財產權的相關建議。同時也明示通過通訊侵害著作權係屬犯罪，強化數位產業針對線上著作權侵權與法律上實體著作權侵權的罰則。對於通訊傳播產業在資料應用的

26, 2017).

[35] GOV.UK, Digital Economy Act 2017, https://www.gov.uk/government/collections/digital-economy-bill-2016 (last visited Oct. 26, 2017).

著作權議題上，提供一個充分的保護機制。

（四） 小結

英國是數位資料應用的大國，其開放資料程度在世界上也是名列前茅。其對於資料應用除了透過政府部分大量開放資料，使得像 Ofcom 這類監理機關擔任起推動開放資料的角色外，也透過像是 ODI 這種輔導資料應用產業的組織來促成資料應用的發展。

在法制方面，英國的個人資料保護法案因為進行脫歐準備，所以遵循歐盟的規範標準，是否對於資料應用造成阻礙仍有待觀察。而數位經濟法案對於線上著作權的規定，對於通訊傳播業者在釋出手上有著作權的資料(例如：資料的編輯方法)時能提供相當的保障，某種程度提升了民間業者資料應用的動機。

第四節 日本

一、概說

以 311 東日本大地震為契機，日本開始重視資料開放發展。日本政府於 2012 年 7 月公布「電子行政開放資料戰略（電子行政オープンデータ戦略）」，從那時資料加值與創新應用就成為日本重要的政策課題。但相較於其他國家，日本的資料加值與創新應用進度稍嫌緩慢，根據「開放知識基金會」(OKFN)資料開放國際評比，日本僅名列世界第 30 [36]。

2013 年 6 月發布了「世界最先端國家創造宣言(世界最先端 IT 国家創造宣言)」[37]，此篇宣言闡明了日本於 2013-2020 年期間將藉以開放公共資料與巨量資料為核心，達到「世界最高水準的廣泛運用資訊產業技術的社會」的目標，其主要的要點為(1)開放公共資料；(2)促進巨量資料之廣泛活用；(3)活用 ICT 技術的創新應用；在開放公資料數據方

[36] Open Knowledge Foundation, Global Open Data Index: Survey, http://global.census.okfn.org/ (last visited Oct. 26, 2017).

[37] 首相官邸，世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画について，http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20170530/siryou1.pdf（最後瀏覽日：2017 年 10 月 26 日）。

面，日本依據 IT 戰略本部所發布之電子政務開放資料戰略草案，建立可供居民瀏覽中央各部和地方省廳公開資料的網站，其內容包括各項統計資料、量測資料以及災害資訊等，並將這些資訊轉為標準化格式，使民眾在取得以及判讀上更為容易。

日本的資料開放以地方自治團體和民間企業合作型態為主，藉由開放自治團體的資料來舉辦各式各樣的競賽來創造資料加值與創新應用加值應用，目前共有 23 個道府縣，157 個市區村提供資料加值與創新應用，以總務省為中心的中央政府資料加值與創新應用推動也持續進行。

在 2015 年 10 月 23 日的電子行政實務者會議(電子行政オープンデータ実務者会議)中決定了今後日本資料加值與創新應用的發展。其訂立的未來主要目標包括：推動行政法人和公益事業（水、電、交通等事業體）資料釋出、提升開放資料的質與量、協助地方自治團體繼續發展資料加值與創新應用等。

二、應用案例

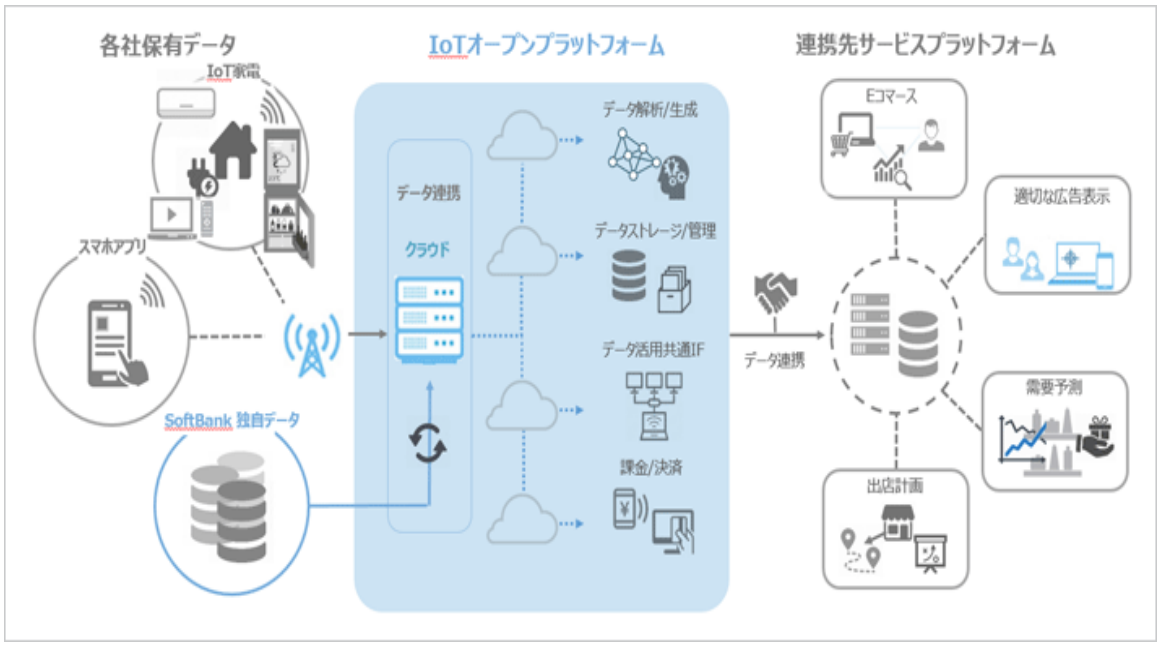
日本總務省、經產省也是在這個脈絡下推動資料加值與創新應用。其中像是經產省就訂出以推動資料交易為目的之契約指導方針(データに関する取引の推進を目的とした契約ガイドライン)[38]，將資料交換要締結契約所要注意的點都提示其中，以降低業者進行資料應用所面對的風險。

而在產業應用資料方面，日本電信商軟體銀行(Softbank)推出開放資料平台[39]。可提供資料加值與創新應用內容除了以軟體銀行本身保有的資料外，還匯集其他合作業者包括

[38] 経済産業省(2015 年 10 月 6 日)， データに関する取引の推進を目的とした契約ガイドライン ，http://www.meti.go.jp/press/2015/10/20151006004/20151006004.pdf（最後瀏覽日：2017 年 10 月 26 日)。

[39] ソフトバンク株式会社(2016 年 11 月 10 日)， IoT データをビジネスに活用するオープンプラットフォームの構築およびデータ価値化検証の PoC 実施について，http://www.softbank.jp/corp/group/sbm/news/press/2016/20161110_04/（最後瀏覽日：2017 年 10 月 26 日)。

Sony、電通、東芝等公司的資料，以創造新的應用程式和資料服務產業為目的。目前的資料來源以智慧行動電話和 IOT 為主，日後隨著智慧型家電日益普及，資料來源將會更為廣泛。而在 2017 年 9 月 26 日，軟體銀行的平台更達成與英國 Linaro 開發的 IOT 專用產品完成接續[40]，將平台的資料來源擴展到世界。軟體銀行平台蒐集的個資包括位置資訊、使用紀錄、裝置資訊等，其蒐集及處理的特定目的都依照軟體銀行的隱私權政策[41]



資料來源：Softbank

圖 2-8　Softbank 資料分享平台

日本電信商與地方自治團體合作，協助地方開放並且應用資料的例子所在多數。像是日本最大電信商 NTT 與日本札幌市政府的合作案，NTT 提供免費 wifi，藉由 wifi 來蒐集

[40]ソフトバンク ,ソフトバンクの IoT プラットフォームと英 Linaro の IoT 向けオープン規格「96Boards」シリーズ製品との相互接続を実現，https://www.softbank.jp/corp/group/sbm/news/press/2017/20170926_01/（最後瀏覽日：2017 年 10 月 26 日）。

[41]ソフトバンクグループ， 個人情報の取り扱いについて ,https://www.softbank.jp/help/privacy/（最後瀏覽日：2017 年 10 月 26 日）。

資料並且進行統計分析，之後將結果提供給札幌市政府作為發展觀光的依據，並且可以針對特定國家或是地區的觀光客進行特製化的服務。NTT 使用的個人資料種類甚多，包括郵件地址、位置資訊、行動軌跡等，除了有告知特定目的並且請求同意外(在使用 wifi 前)，同時也有經過去識別化程序，所公開並且據以利用的資料無法識別特定個人。

資料來源：2020.ntt/sousei/case_development/ict/

圖 2-9　NTTx 札幌市資料應用範例

日本第二大電信公司 KDDI 則是結合 IOT 技術與政府開放資料，製作出新的產品。在其附設購物網站 au WALLET Market 賣的傘架，連通智慧型手機的氣象資料後，就能依照天氣預報讓 LED 發出不同顏色的亮光，例如顯示橘色代表「不需要帶傘」、水藍色代表「必須帶傘等等」。由於該產品僅使用關於氣象的公開資料，故無蒐集處理個資議題。

資料來源：https://www.au.com/information/topic/auwallet/20150825-01/

圖 2-10　KDDI 傘架

丹南 CATV 是以福井縣越前市為中心的有線電視業者。丹南 CATV 和地方政府和業者合作，提供商店資料、地方政府資料、以及有線電視業者自己採訪的影像畫面，免費、不限使用目的供開放資料給程式開發者使用[42]。目前已經有利用這些開放資料開發出 APP 的案例。丹南 CATV 使用的資料都是不含有個人資料的公開資料，故無個資隱私的議題。

[42] TANNAN CATV Co.,LTD.（2017 年 3 月）， オープンデータについて ，http://miseban.com/opendata/（最後瀏覽日：2017 年 10 月 26 日）。

資料來源：丹南 CATV

圖 2-11　丹南 CATV 開放資料網站

三、相關法規

（一） 個人資料定義

修正前的日本個人資料保護法第 2 條第 1 項對於個人資料的定義為：「關於自然人的資料中包含姓名、出生年月日及其他得識別特定個人的資料(包含得容易與其他資訊比對，並藉而識別特定個人的資料)」因為規範過於簡單，許多資訊是否被納入規範迭有爭議。

為了避免產業界對使用個人資料卻步、也為了避免侵害到個人權益，因此要明確定義個人資料的範圍。本次修正條文第 2 條第 1 項第 2 款將「個人識別符號」納入規範[43]，即是將由個人身體特徵所轉換成得以識別個人的資訊，明確定義為受個資法保障的個人資料。在這樣的定義之下，包括指紋資料、臉部辨識資料、護照號碼、證書執照號碼、電話號碼

[43] 個人情報の保護に関する法律改正法，第二条第１項第二号 ，個人識別符号が含まれるもの。

以及個人編號都被明確納入規範對象[44]。

此外，修正條文第 2 條第 3 項新增「敏感性個人資料」的規定[45]，對於那些會造成本人受到歧視待遇的人種、信仰或是病歷等個人資料，除法律規定、保護他人生命財產而難以取得同意、維護兒童健全身心發展、或公務機關依法遂行職務而難以取得同意等情況外，應取得本人同意（第 17 條第 2 項）[46]，且禁止以事後退出的模式取代事前同意，而向第

---

[44] 個人情報の保護に関する法律改正法，第二条第２項，この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。

一 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの。

二 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの。

[45] 個人情報の保護に関する法律改正法，第二条第３項，この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

[46] 個人情報の保護に関する法律改正法，第十七条第２項， 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

一 法令に基づく場合。

二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

五 当該要配慮個人情報が、本人、国の機関、地方公共団体、第 76 条第１項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合。

三人提供資料（第 23 條第 2 項）[47]。

（二） 個人資料保護

日本個人資料保護法案中，不論是行政機關或是民間機構，只要有利用個人資料者，都受到此法之規範；因此，日本政府制定一般性規範，意即所謂的「基本原則」，作為各機構之標準。此外，特別是對於使用電腦或資料庫等儲存利用個人資料之相關單位(個人資料利用事業者)，亦設定「個人資料利用事業者之義務（個人情報取扱事業者の義務)」規定，訂立具體且明確之規範。以公務機關之個人資料處理而言，在昭和六十三年已制定「行政機關電腦處理個人資料保護法」(行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律)，然而為配合「個人資料保護法」之制定，除了將原先「行政機關之電腦處理個人資料保護法」修正為「行政機關個人資訊保護法」(行政機関の保有する個人情報の保護に関する法律)，另制定「獨立行政法人資料保護法」(独立行政法人等の保有する個人情報の保護に関する法律)、「資料公開與資料保護審查會設立法」(情報公開・個人情報保護審査会設置法)、「行政機關之個人資料保護法施行相關法律準備之法案」(行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律）等，以加強個人資料保護法之完整性，統稱為個人資料保護法關聯五

[47] 個人情報の保護に関する法律改正法，第二十三条第二項，個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一 第三者への提供を利用目的とすること。

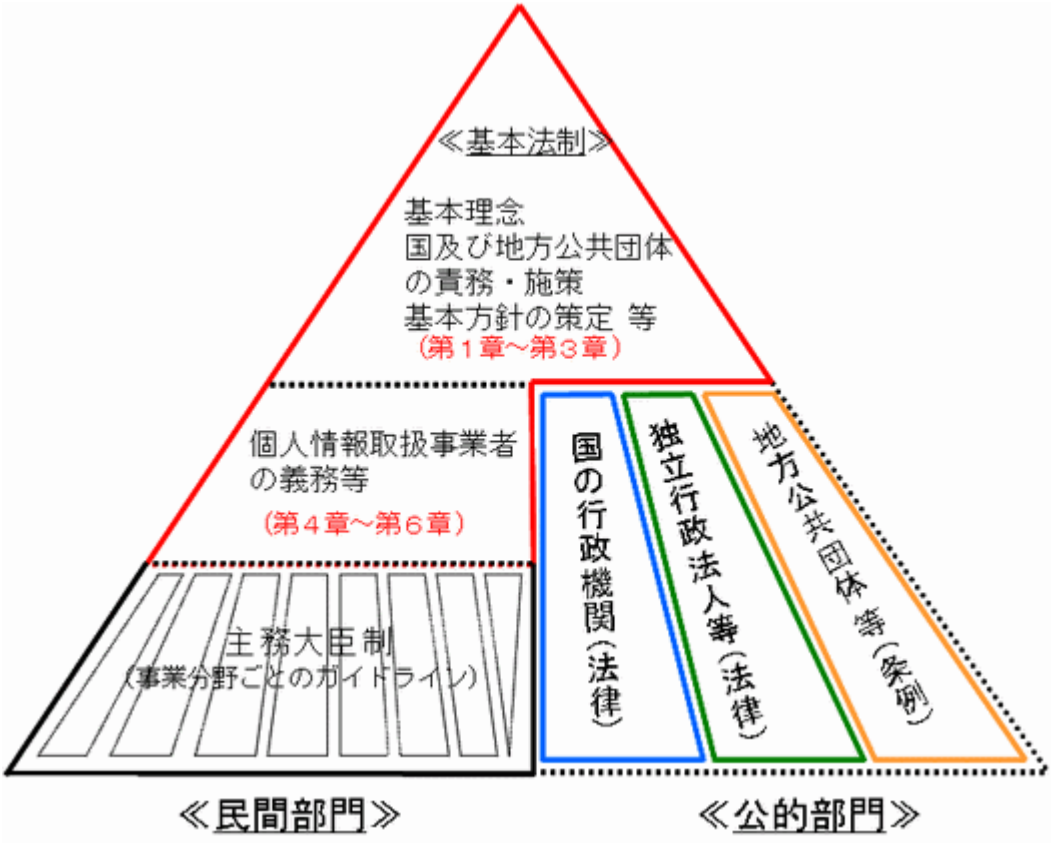
二 第三者に提供される個人データの項目

三 第三者への提供の方法

四 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

五 本人の求めを受け付ける方法

法（個人情報保護法関連五法）[48]。其法律體系如下所示：



資料來源：日本茨城縣政府網站

圖 2-12　日本個人資料保護法體系

但隨著大數據等技術科技對於個資使用的需求，舊的個人資料保護法僅著重於個資保護已不敷使用，因此在個資法通過 10 年後，日本再度展開新的修法工作。

日本內閣府於 2014 年 6 月的第 11 次「關於個人資料研討會（パーソナルデータに関する検討会）」中作成「有關個人資料利活用制度修正大綱（パーソナルデータの利活用に関する制度改正大綱）[49]」，並根據此大綱作成修正草案（個人情報保護法の改正案），

[48] 個人情報保護関連５法の概要 ，日本總務省行政管理局，http://www.city.yokohama.lg.jp/shimin/madoguchi/j-net/singikai/02/j-net2si3.pdf

[49] 内閣官房高度情報通信ネットワーク社会推進戦略本部，パーソナルデータの利活用に関する制度

於 2015 年 3 月經過閣議審定，終於在 2015 年 9 月 3 日眾議院通過修正草案審議，於 2017 年 9 月開始全面施行。其修正目標，是為加強個人資訊保護、促進個人資料利用、創造新產業、新服務、提升國民安全、同時期盼使日本成為歐盟所認可之個人資料保護程度充足的國家，進而成為歐盟所承認得為國際傳輸個人資料的對象國。

（三） 官民資料應用

為了擴大官方與民間的巨量資料應用，使得資料成為任何人都能自由使用的「開放資料」，日本自民、公明、民進、日本維新會四黨在 2016 年 11 月 1 日決議將「官民資料活用推進基本法」向本期臨時國會提出。希望藉由推動這個法案，來加速「第 4 次產業革命」核心的人工智慧產業，同時整備能趨使企業各式各樣資訊的環境，該法於 2016 年 12 月 7 日由參議院通過。

法案對於資訊的定義為：電磁紀錄或是以電磁方式記錄，受到因國家、地方公共團體或業者之事務或是遂行事務所管理、利用或是提供。另外對於「人工智慧（AI）」、「物聯網(IOT)」、和「雲端運算(クラウド)」在法律中都有明確定義。

法案的基本計畫，是藉由政府策定官民資料活用推進基本計畫、都府道縣策定都府道縣官民資料活用推進基本計畫、以及市町村策定市町村官民資料活用推進基本計畫，藉由分層負責來推動資料的運用。其基本的施政內容包括：(1) 行政程序線上辦理的原則化 (2) 促進民間業者工作程序線上辦理 (3) 推動國家、地方公共團體、業者保有的官民資料活用，以及相關制度的檢討 (4) 整備能夠適當使用關於個人的官民資料基礎環境 (5) 資訊系統的規格整備、確保資料交換性、業務的檢討、各式各樣領域的官民資料的合作、協調的基礎設施整備（服務平台）(6) 因為地理、年齡等因素導致資訊通信技術的使用機會落差的補正 (7) 國家與地方公共團體施政整合性的確保 (8) 其他議題，例如個人編號

改正大綱(平成 26 年 6 月 24 日),
http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf(最後瀏覽日 2017 年 10 月 26 日)。

卡(マイナンバーカード)的使用、研究開發的推動、人才育成和確保、教育普及等。此外，本法案也要求以首相為議長，開設「官民資料活用推進戰略會議」，會議負責(1) 依照各個領域整備官民資料活用的體制(由議長指定重要領域)(2) 由議長對相關行政首長進行業務推動的勸告 (3) 協助地方團體進行官民資料分享。

（四） 小結

日本雖然對於資料開放是處於較為落後的狀態，但由於安倍政權對於資料經濟的重視，這些年不管是在政策面與法律面都有急起直追的態勢。政策面來說，開放資料 2.0 的新政策指示總務省與經產省提供業界資料分享相當的協助，不管是提供契約範本還是與民間業者合作等等，而通訊傳播產業的民間發展也是相當活絡，尤其是因為日本為 ICT 產業大國，所以幾個大的通訊業者像是 Softbank 都開始往資料加值應用發展。而在法律面，日本這三年對於個人資料保護、或是資料應用的法制都有大幅度的修正，其修法方向都是更加促進資料流通，減少因為保護而造成的阻礙。由於安倍政權強調開放資料、資料經濟是未來日本面對 2020 奧運會對國際展現日本實力的核心價值，因此日本的開放資料發展值得觀察。

第三章　通訊傳播產業資料加值與創新應用相關法制研析

第一節　個人資料去識別化的標準與應用

一、概說

大數據（Big Data）應用下，資料就是最主要資源，同時資料得以充分流通，是促成大數據應用的最重要基礎。特別是客製化、訂製化服務這個領域，業者對於將個人資料為更進一步之利用都表現出相當強烈的意願。然而個人資料的應用與濫用只有一線之隔；個人資料涉及隱私保護，依法始得蒐集、處理、利用。各界普遍採取的因應之道，乃是將資料「去識別化」，無法直接或間接地識別個人而不再是個人資料（無涉個人隱私），與個人資料保護法等相關規定脫勾，藉以達成資料之開放及交流。

惟各方研究及實例陸續指出，大數據應用匯集多方資料，升高資料當事人被重行識別（re-identify）之可能，也因此導致公眾對於個人資料去識別化與否的檢視益發嚴格。然而，去識別化的要求越高，被要求移除的資訊細項越多，資料的可用性相形也就越加降低。因而，從去識別化等技術面切入，似陷入難以徹底維護個人隱私（大數據應用可能有辦法重行識別個人）、亦難以有效發揮資料價值的困境。

二、美國規範

（一） 背景介紹

在多樣 IT 服務急速普及化的美國，企業和政府積極促進各種電子資料的活用，而國民則是對於個人資料保護有疑慮，在這雙方價值觀已經產生相當衝突。而同時近年美國不斷發生資料洩漏與犯罪事件，導致個人資料保護受到威脅，因此對於各種關於個人資料保護的議題就開始不斷產生。美國的個人資料保護保護法律，是隨著科學技術開拓發展的同時，所制定出能順應時代潮流，因應領域別差異的法律。歐巴馬（Obama）政權致力於推動大數據科技應用和消費者隱私權保護，因為近年頻繁發生的資訊洩漏事件以及政府監聽

事實遭到暴露後，確立新的個人資料保護政策的呼聲逐漸變大。此外，美國各州也因應這樣的呼聲開始制定出屬於獨自的個人資料保護法。

美國並沒有像我國或是日本等國，對於個人資料並沒有法律明文的定義。在美國所指的個人資料，又稱為個人識別資訊(Personally Identifiable Information)，是指能成為識別特定個人線索可能性的各式資訊。包括姓名、出生地、出生時間、身體特徵紀錄、社會安全碼（Social Security Number）等。其他包括單獨無法識別個人，但和其他資訊組合比對足以識別個人的醫療紀錄、教育、財政狀態、雇用資訊等。

為深入研析美國的重行識別個人之規範，本章背景介紹先就美國的個人資料保護法規出發，再就美國的去識別化制度作初步介紹，以使後續討論得以順利開展。

（二） 美國去識別化規範

FTC 在 2012 年 3 月 26 日公布保護消費者隱私報告「在急速變化時代下的消費者隱私權保護（Protecting Consumer Privacy in an Era of Rapid Change）」[50]中，在第 20 頁以下針對個人資料的去識別化(de-identify)提供一個可資遵循的規定。在本報告中提到所謂美國係以「有無可合理連結(reasonable linkable)」做為判斷標準。而如何確保個人資料經過去識別化後無法合理連結到個人，就得符合下列三個標準：

一、 採行合理之去識別化措施；

第一個要件所謂「合理之去識別化」措施並沒有一定且一致的判斷標準，大致上是透過使用資料的目的、現時技術所以可能使用的技術來個案判斷。

二、 須公開（包括將合約公布等方式）約定不還原去識別化(re-identify)的資料：

如果企業嘗試去對資料進行重行識別(takes steps to re-identify such data)，FTC 得以聯邦交易委員會法（Federal Trade Commission Act）第 5 條認定其行為不公平、欺

[50] Protecting Consumer Privacy in an Era of Rapid Change, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last visited Oct. 26, 2017).

瞞，而得以採取行政或是司法的強制措施。

三、 提供去識別化的資料予第三人時，須訂立合約禁止接受者還原資料，若符合上開三個要件，則可認為並非可合理連結的資料：

對這些接受去識別化資料的第三人，要監視他們遵守合約禁止再行識別個人的約定，同時對於違反者也要採取適切的措施（should exercise reasonable oversight…），進行合理的監督。

此外 FTC 報告書也有揭示，若同時保有去識別化資料和未經去識別化資料，需要將這些資料分開保管。

美國對於去識別化資料，法律中還沒有明確細緻的標準。但 HIPPA 對去識別化(deidentification)作出了定義：通過處理使得資料不能識別特定個人，或者沒有合理的基礎能夠認為該資料可以被用來識別特定個人[51]。HIPAA 隱私規則，只規範「可識別個人之健康資訊」（individually identifiable health information）[52]。因此，該規則並沒有禁止受規範之機構（covered entities）揭露去識別之資料給第三人，包括揭露給研究者。

---

[51] 45 C.F.R. § 164.514(a) Standard: De-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

[52] 45 C.F.R. § 160.103. (“Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.”)

所謂的去識別化的判斷標準如下：(1) 一具有統計學與科學背景、且知道如何將資料去連結的專家認定，該資訊被取得者得到後，將其單獨或與其他合理方法可取得的資訊結合，只有非常小的風險，可以識別出該資訊所屬之個人，且(2)該專家提供他的書面分析[53]。這個判斷標準，被稱為 HIPAA 的資料分析標準（statistical standard）又稱為「專家判斷法」。而在 HIPAA 隱私規則中，也有另一種判斷資料是否去識別的安全港條款[54]，其規定若下述 18 種識別碼（identifiers）被移除，就可算是去識別資料：

---

[53] 45 C.F.R. § 164.514(b)(1). (“(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination…”)

[54] 45 C.F.R. § 164.514(b)(2)(i). In addition, information will not be considered de-identified if an entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." Id. § 164.514(b)(2)(ii).of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination…”).

A. 姓名（Names）；

B. 所有比州單位還要小的地理位置，包括街名、市、縣、選區、郵遞區號、以及相對應的地理編號。但是，若根據人口統計局現存公開資料中的計算，符合下述情況時，可公布其郵遞區號的前三碼(All geographic subdivisions smaller thana State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census):該郵遞區號前三碼涵蓋的人口,超過二萬人(The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people)；且若該郵遞區號前三碼所涵蓋人口為二萬以下，則需將前三碼改為 000（The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000）；

C. 所有與個人有直接連結的資料要素（除了年份），包括生日、入院日、出院日、死亡日；及所有 89 歲以上人的年紀，以及所有可推算出此年紀之日期（包括年），除非將這些年紀和元素,通通僅歸類於 90 歲以上者之單一類別(All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older)；

D. 電話號碼（Telephone numbers）；

E. 傳真號碼（Fax numbers）；

F. 電子郵件信箱（Electronic mail addresses）；

G. 社會安全號碼（Social security numbers）；

H. 醫療記錄編號（Medical record numbers）；

I. 健康照顧計畫受益人編號（Health plan beneficiary numbers）；

J. 帳戶號碼（Account numbers）；

K. 證書號碼（Certificate/license numbers）；

L. 車輛識別和序列編號，包括汽車牌照(Vehicle identifiers and serial numbers, including license plate numbers)；

M. 設備識別或序列編號 (Device identifiers and serial numbers)；

N. 網頁網址 (Web Universal Resource Locators (URLs))；

O. 通訊協定位置編號 (Internet Protocol (IP) address numbers)；

P. 生物識別，包括指紋和聲紋 (Biometric identifiers, including finger and voice prints)；

Q. 全臉照片或其他可比較影像(Full face photographic images and any comparable images)；及

R. 任何其他獨特可識別之號碼、特徵或編號(Any other unique identifying number, characteristic, or code)。

（三） 相關案例

FTC 2012 年的報告書中特別有提到 Netflix 的例子。當 Netflix 於 2006 年的 Netflix 舉辦競賽，在該場競賽公佈了大約來自 48 萬用戶的一億條租賃記錄，並且公開懸賞一百萬美金，獎勵工程師通過軟體設計來提高其電影推薦系統的精確度。為了將這個資料去識別化，Netflix 將評論者的姓名以一定有秩序的號碼替換，同時去除地址、電話等直接識別因子。然而不久之後，就有德州大學的學者能夠靠著這些資料推知出收視者為何人，最後還發表作為研究成果並公開在媒體上，其中有被識別的特定個人而因此起訴了 Netflix 公司。結果雖然 2009 年 7 月比賽如期順利完成，但當 Netflix 打算在 2009 年再度舉辦比賽，公布「宣稱已經去識別化的（purportedly anonymous）資料」，最後因為 FTC 感到有疑慮而宣布中止。

2009 年所要公布的資料比起 2006 年所要公布的資料具有更多識別因子，因此 FTC 在 2009 年 11 月所發的函[55]特別提到對於再識別化的風險疑慮，以及評估 Netflix 的公開資

[55] Closing Letter to Reed Freeman, Esq., Counsel for Netflix, Inc., https://www.ftc.gov/sites/default/files/documents/closing_letters/netflix-inc./100312netflixletter.pdf (last visited Oct. 26, 2017).

料行為違反聯邦交易委員會法第 5 條的可能性。FTC 認為 Netflix 宣稱資料經過「去識別化」，實際上卻仍然能被人透過比對分析再行識別這樣的行為，就足以該當聯邦交易委員會法第 5 條的「欺瞞手段(Deceptive acts or practices)」。

結論上，FTC 要求(1) Netflix 中止競賽和資料提供 (2) 該當資料以後要提供，只能依照一定使用目的提供給一部分的研究人員。(3) 對於防止該當資料被重行識別要以契約約束同時也要注意資料的運用手段。(4) 在公開資料前一定要經過 FTC 諮詢。

三、英國規範

英國資訊委員辦公室發佈的「去識別化：資料保護風險管理應用準則」(Anonymisation: Managing Data Protection Risk Code of Practice)[56]，本文以下簡稱「去識別化應用準則」) 提供一套準則供組織遵循，進行個人資料的去識別化。欲進行資料去識別化之組織須參考並遵守去識別化應用準則中的規定進行個人資料的去識別化，而資訊委員也將依本準則的規定，評量組織是否合理地進行個人資料的去識別化。

去識別化應用準則首先明定「去識別化資料」('anonymised data') 為資料本身無法識別任何個人之資料，以及透過與其他資料的組合 (combination)，無可能識別任何個人之資料[57]。而準則中也說明，英國資料保護法並沒有要求「去識別化」(anonymisation) 必須做到完全的 (completely) 沒有風險 (risk free)，任何欲進行資料去識別化之組織，僅需減低 (mitigate) 資料被識別的風險，直到其風險變得極微小 (remote) 即可[58]。當資料經去識別化後，因無法直接或間接識別個人，資料已不再被認為是英國資料保護法中的個人資料[59]。

---

[56] Information Commissioner's Office, Anonymisation: Managing Data Protection Risk Code of Practice (2012), https://ico.org.uk/media/1061/anonymisation-code.pdf (last visited Oct. 26, 2017).

[57] *Id.* at 6.

[58] *Id.*

[59] Information Commissioner's Office, Big Data and Data Protection (2014),

四、日本規範

（一） 背景介紹

在現今大數據（Big Data）或開放資料（Open Data）等新資料科技應用領域中，由於各種被使用的資料範圍開始擴大，社會也開始對個人資料及隱私安全產生疑慮。為了避免牴觸現今個人資料保護規制，往往這些個人資料在使用時必須配合去識別化，將這些個人資料以代碼、匿名、隱藏部分資料或其他方式，使之無從辨識該特定個人，以充分保障個人資料及隱私權、增進公眾互信的架構。

然而當越來越多個人資料以去識別化之方式向公眾提供時，一來因為資料數量增加，二來因為資料分析比對的技術提升，資料被重行識別出個人的機率也隨之變高，成為個人資料保護的另一漏洞。為了防止如此弊害，重新檢視並制定禁止重行識別個人規範，就成為個人資料保護的要務。

（二） 日本修法前規範

日本關於個人資料去識別化（匿名化）以及重新識別並沒有明文規定，2013 年 6 月 25 日總務省「關於個人資料利用、活用研討會（パーソナルデータ利用・活用に関する研究会）」的報告書中[60]中提到只要滿足下列的三個原則，即可被視為實質上無個人識別性，不屬於受法律保護的個人資料，能不得到本人同意即可利用。1.實施適當的去識別化措施。2.資訊接受方同意並且公告去識別化的資料將不再重新識別。3.將匿名化的資料向第三人提供時，提供資料的一方需以契約禁止資料重新識別。

對照同報告書第 58 頁「在急速變化時代下的消費者隱私權保護（急速に変化する時代における消費者プライバシーの保護）」章節提到美國聯邦交易委員會（Federal Trade

---

https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf (last visited Oct. 26, 2017), at 5.

[60] 総務省, パーソナルデータの利用・流通に関する研究会報告書～パーソナルデータの適正な利用・流通の促進に向けた方策～, http://www.soumu.go.jp/main_content/000231357.pdf(最後瀏覽日 2017 年 10 月 26 日)。

Commission ，FTC）頒布的三原則：1.採行合理的去識別化措施；2.受到不得還原去識別化資料的限制;3.提供去識別化的資料予第三人時,須訂立合約禁止資料收受者還原資料。違反時FTC將採取適當措施並合理性監視遵守情況。

可以發現兩者的相似度極高，但如果仔細比對可以發現，兩者仍有差異之處。以要件2來說，字面上FTC保留了介入執行的空間，得以聯邦交易委員會法（Federal Trade Commission Act）第五條採取強制措施，反觀總務省卻一開始就沒有要對業者監督管理的意思。而關於要件3，FTC多出了監督條款也是總務省所無。總括來看，總務省所定的三要件規制密度較FTC寬鬆。

因為沒有法律規制效果，實務上不遵守要件的案例層出不窮，例如發生在2013年的SUICA事件[61]。JR東日本在提供SUICA卡乘車紀錄給日立製作所進行大數據分析，資料包括車站使用人的性別、年齡分布、停留時間、上下車時間分布等。此舉當時引起社會一片撻伐，民眾認為自己有被監視的感覺，同時也質疑既然使用自己的個人資料為什麼沒有事先請求同意。對此，JR東日本卻只是表示「這些資料既然無法特定個人，則應該不算是個人資料。」強調所有資料都有經過去識別化，且在雙方契約中有約定禁止比對資料以及重新識別。然而當提及要將契約內容公開時，JR東日本卻以日立製作所是值得信賴的企業為由，而拒絕將契約內容公開。此一事件引起日本社會高度關注，最終成了個人資料保護法修正的關鍵。

（三） 日本修法後規範

日本舊個人資料保護法（個人情報保護法）對於匿名化及重新識別並沒有法規明文規定，但隨著大數據等技術科技對於個資使用的需求，舊的個人資料保護法僅著重於個資保護已不敷使用，因此在個資法通過10年後，日本再度展開新的修法工作，終於在2015年9月3日眾議院通過修正草案審議，於2017年9月開始全面施行。以下是這次修正，

[61] Business Joural, Suicaのデータ販売中止騒動、個人特定不可なのになぜ問題？ ビッグデータの難点, http://biz-journal.jp/2013/08/post_2760.html(最後瀏覽日2017年10月26日)。

關於去識別化的規範。

本次增修條文增加了「匿名處理資料」的概念。所謂「匿名處理資料」是指「對個人資料採取一定的匿名化措施處理，使其無法識別特定個人所得之關於個人的資料，且該個人資料無法復原。」（參照修正條文第 2 條第 9 項）[62]

而所謂的匿名化措施具體內容，是指將包含該個人資料等資訊的一部（若該資訊包含得以識別個人符號時則必須全部消除）消除，或是以不帶有可能復原個人資料規則性的方法替換成其他的記述。（參照修正條文第 2 條第 9 項）

因為「匿名處理資料」不屬於「個人資料」，因此一旦被視為是「匿名處理資料」，即不受目的外使用或是向第三人提供規定的限制。然而，這並不表示「匿名處理資料」完全不受限制，在本次修正考慮到資料有用性的同時，也設下的一定的規制，作成「匿名處理資料」的「個人資料處理業者」以及「匿名處理資料處理業者」等都課以相當的義務。

1. 作成「匿名處理資料」的「個人資料處理業者」的義務

關於作成「匿名處理資料」的「個人資料處理業者」的義務，規定如（修正條文第 36 條）[63]下：

---

[62]個人情報の保護に関する法律改正法，第二条第９項，この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。

一 第１項第１号に該当する個人情報 当該個人情報に含まれる記述等の一部を消除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）。

二 第１項第２号に該当する個人情報 当該個人情報に含まれる個人識別符号の全部を消除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）。

[63] 個人情報の保護に関する法律改正法，第三十六条 ，個人情報取扱事業者は、匿名加工情報（匿名加工情報データベース等を構成するものに限る。以下同じ。）を作成するときは、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするために必要

(1) 需要依照指定方法作成「匿名處理資料」。（修正條文第 36 條第 1 項）

(2) 作成過程中，應採取防止關於已消除記述、個人識別符號、以及處理方法等資訊洩漏的必要安全措施。（修正條文第 36 條第 2 項）

(3) 該「匿名處理資料」資訊作成時，應公開該「匿名處理資料」原所包含的個人資料項目。（修正條文第 36 條第 3 項）

(4) 向第三人提供該「匿名處理資料」資訊時，應公開所提供「匿名處理資料」的個人資料項目、提供方法，以及對該第三人明示該資料為「匿名處理資料」。（修正條文第 36 條第 4 項）

(5)「個人資料處理業者」在作成「匿名處理資料」時，需要對該「匿名處理資料」的安全管理作成必要且適當的處置，處理關於該「匿名處理資料」的申訴、以

なものとして個人情報保護委員会規則で定める基準に従い、当該個人情報を加工しなければならない。

2 個人情報取扱事業者は、匿名加工情報を作成したときは、その作成に用いた個人情報から消除した記述等及び個人識別符号並びに前項の規定により行った加工の方法に関する情報の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、これらの情報の安全管理のための措置を講じなければならない。

3 個人情報取扱事業者は、匿名加工情報を作成したときは、個人情報保護委員会規則で定めるところにより、当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならない。

4 個人情報取扱事業者は、匿名加工情報を作成して当該匿名加工情報を第三者に提供するときは、個人情報保護委員会規則で定めるところにより、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。

5 個人情報取扱事業者は、匿名加工情報を作成して自ら当該匿名加工情報を取り扱うに当たっては、当該匿名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該匿名加工情報を他の情報と照合してはならない。

6 個人情報取扱事業者は、匿名加工情報を作成したときは、当該匿名加工情報の安全管理のために必要かつ適切な措置、当該匿名加工情報の作成その他の取扱いに関する苦情の処理その他の当該匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

及確保該「匿名處理資料」的正當使用必要措施。上述具體作為必須要盡可能對外公開。（修正條文第 36 條第 6 項）

義務的具體內容將在未來由個人資訊委員會明定之。個人資訊委員會於 2016 年 10 月公布之指導方針[64]中具體指出：(1)將能識別特定個人的記述（例如：姓名）一部或全部消除。(2)將識別個人符號全數消除（包括護照號碼、健保號碼等）(3)個人資料與其他資料連結的符號（例如：存有個人資料壓縮檔的密碼等）(4)特別突出的記述（例如：年齡 116 歲）的消除。在指導方針中，則更是針對產業別提出具體的資訊消除方法，包括應該消除的項目、資料的平均化等，另外也具體指出何種資料不屬於去識別化資料，包括「統計資料」或是「做為安全管理措施的一環將個人資料一部去除」等情形。

2.「匿名處理資料處理業者」的義務：

(1) 關於處理已經作成之「匿名處理資料」業者（即「匿名處理資料處理業者」）義務，該「匿名處理資料」（自己加工作成的個人資料除外）資訊向第三人提供時，有公開該被提供「匿名處理資料」的個人資料項目的、提供方法，以及對第三人明示該資料為「匿名處理資料」的義務。（修正條文第 37 條）65

(2)「匿名資料處理業者」在處理「匿名處理資料」時，需要對該「匿名處理資料」進行必要且適當的安全管理、處理關於該「匿名處理資料」的申訴以及確保該「匿名處理資料」的正當使用必要措施。上述具體作為必須要盡可能對外公開。（修正條文第 39 條）66

---

[64] 個人情報保護委員会，個人情報の保護に関する法律についてのガイドライン（匿名加工情報編），http://www.ppc.go.jp/files/pdf/guidelines04.pdf（最後瀏覽日 2017 年 10 月 26 日）。

[65]個人情報の保護に関する法律改正法，第三十七条，匿名加工情報取扱事業者は、匿名加工情報（自ら個人情報を加工して作成したものを除く。以下この節において同じ。）を第三者に提供するときは、個人情報保護委員会規則で定めるところにより、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。

[66]個人情報の保護に関する法律改正法，第三十九条，匿名加工情報取扱事業者は、匿名加工情報の安

(3) 關於上開義務的具體內容將在未來將由個人資訊委員會明定之，詳細義務內容同前述。

3. 禁止重行識別規定

修正條文第 36 條第 5 項以及第 38 條[67]明文規定在處理「匿名處理資料」時，明文不得重新識別。

(1) 當處理「匿名處理資料」為「個人資料處理業者」時：業者自己處理該「匿名處理資料」時，不得為了識別本人而與其他資料相比對。（修正條文第 36 條第 5 項）

(2) 當處理「匿名處理資料」為「匿名處理資料處理業者」時：

(3) 處理該「匿名處理資料」時，不得為了識別本人而取得在處理過程中被消除了記述、或是個人識別符號、或是關於加工方法的資訊、而與其他資料相比對。（修正條文第 38 條）

(4) 對於違反第 36 條及第 38 條義務的業者，個人資訊保護委員會得施以中止該行為的勸告或採取必要導正措施。（修正條文第 42 條第 1 項、第 2 項）[68]

全管理のために必要かつ適切な措置、匿名加工情報の取扱いに関する苦情の処理その他の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

[67]個人情報の保護に関する法律改正法，第三十八条，匿名加工情報取扱事業者は、匿名加工情報を取り扱うに当たっては、当該匿名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該個人情報から消除された記述等若しくは個人識別符号若しくは第 36 条第１項の規定により行われた加工の方法に関する情報を取得し、又は当該匿名加工情報を他の情報と照合してはならない。

[68]個人情報の保護に関する法律改正法，第四十二条第１項、第２項，個人情報保護委員会は、個人情報取扱事業者が第 16 条から第 18 条まで、第 20 条から第 22 条まで、第 23 条（第４項を除く。）、第 24 条、第 25 条、第 26 条（第２項を除く。）、第 27 条、第 28 条（第１項を除く。）、第 29 条第２項若しくは第３項、第 30 条第２項、第４項若しくは第５項、第 33 条第２項若しくは第 36 条（第６項を除く。）の規定に違反した場合又は匿名加工情報取扱事業者が第 37 条若しくは第 38

第二節　資料應用分析產生的歧視議題

一、背景介紹

在大量資料得以高速分析的大數據時代。這樣的新科技不但能夠蒐集個人資料、分析個人的喜好和習慣，甚至可以預測未來的行動和一切行為的可能性。在這新科技帶來便利的同時，人性尊嚴和民主的基本價值將受到極大的挑戰。

2014 年 5 月 1 日，美國白宮發表了一篇長達 85 頁，內容在檢討大數據和隱私《大數據：抓住機會、保存價值》(Big Data: Seizing Opportunities, Preserving Values) 的報告，其中在大數據與差別待遇 (Big Data and Discrimination) 一章提到大數據技術可以劃“數位紅線”來區別人群，無論是客戶、受雇人、租戶等等，這份報告中明確發現大數據提供了歧視和掠奪的新形式。2016 年 1 月 6 日，美國聯邦交易委員會公布報告《大數據：吸納或排他的工具？》(Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues)中提到大數據分析是否會變成歧視和排他的工具，其實還有很多疑慮。2016 年 5 月 4 日，美國白宮再度發布《大數據：關於算法系統、機會、公民權利的報告》(Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights)，報告也提出大數據科技可能會帶有偏見，進而不經意造成差別待遇。

此外，美國哈佛大學教授 Latanya Sweeney 在運用 Google 搜尋時發現，只要輸入關

条の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者等に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

2 個人情報保護委員会は、前項の規定による勧告を受けた個人情報取扱事業者等が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者等に対し、その勧告に係る措置をとるべきことを命ずることができる。

連到非裔美人的關鍵字，其後被 Google 的分析預設有「逮捕」關鍵字的比例，比白人族裔高出百分之十八[69]。雖然後來 Google 公司道歉並且修正了這個問題，但是該公司從來沒有公開自己是如何修正這樣的問題。之後在 2015 年又發現如果在搜尋引擎輸入歧視非裔美人的字眼，同時在後面加上 House 時，會得到白宮的結果。Google 雖然再次道歉，但是從這些事情已經可以看出依靠大數據的養成的演算工具有製造歧視議題的危險。

而其他的歧視類型，像是量販店 Target 多年前便已開始收集消費者分析數據，依據龐大的消費紀錄，在某些情況下甚至可單純根據消費品項歷史，判斷該名女性顧客是否懷孕，準確度高達 87%。儘管該公司代表在報導內強調，這些資料是用來改善對準媽媽的行銷策略，可是這種手段很容易用於歧視，同時大大影響社會平等與隱私。

企業購買網路廣告宣傳信用卡時，可能依據家戶所得或信貸紀錄，挑選特定目標群眾，導致他人完全無從得知該項優惠。雇主們也傾向在人力資源方面運用大數據資料，完全透過分析電腦使用習慣，評估如何提高員工生產力，而員工可能對這些資料與用途毫不知情。上述都是法律所禁止的歧視行為，但是運用大數據分析可以讓受到歧視的人完全不知道自己受到歧視的理由，結果反而讓反歧視的相關法律變成具文。

而在亞洲國家像日本，伴隨著個人編號（マイナンバー）這個新制度運用於大數據分析，新的歧視議題也開始隱隱產生。日本的個人編號統合了個人戶頭資訊、醫療履歷、健康保險資料、納稅履歷、圖書館借閱資料等等，日本政府在宣導這個政策時強調要「擴大這些個人資料的應用範圍」，同時讓民間得以利用這些資料。這個也引起了許多日本法律學者的疑慮。雖然日本政府一直強調去識別化的作用，也在新修正的個人資料保護法（個人情報保護法）中加入禁止再識別的規定，但是透過資料的累積，就算不需要刻意比對分析，一樣可以還原資料的保有人。例如說單純看領取社會補助資料比例就能看出這個區域的族群分布狀況等。

---

[69] Latanya Sweeney, Discrimination in Online Ad Delivery (Jan 28, 2013), http://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf (last Visited: Oct 26, 2017).

二、爭議之處

（一） 不可探知性

現在的大數據分析的資料來源主要有兩個，其一是由當事人主動提供的「提供資料」(例如姓名、地址、電話等)，另一就是透過攝影機、感測儀器觀察個人所得的「觀察資料」(例如：個人的行動軌跡、購買紀錄、網頁的瀏覽紀錄等)。提供資料部分因為都是當事人有意識提供，尚不構成太大問題，但在觀察資料部分，因為現在感測儀器技術突飛猛進，往往可以在當事人不知情的情況下蒐集觀察資料。此外，當事人對於資料分析的結果也無法得知，往往造成因為這些分析資料造成對自己不利待遇卻不知道原因，進而無法主張救濟。

（二） 脫個人化

這種大數據分析資料往往是把人進行分類，把過去分析所得的特徵、行為模式去套用到被分析對象的身上。然而，個人的特徵、行為模式極為複雜，在進行大數據分析中往往會剃除細微的差異性，以求能將個人套入到既有公式中。本來人的社會或是法律評價應該是依照自己的行為來決定，現在因為大數據分析導致個人在行為以前就被評價，結果就是，如果個人的特徵、行為模式被歸入到負面的類型時，不管是不是真的有如此行為往往受到不應有的差別待遇。

（三） 難以避免的不確定性

所謂的大數據分析，終究只是一種根據過去的經驗，推論出未來可能發生的事，因此不管使用多麼複雜的演算方法，都不能避免不正確的結果。但是這個不正確的結果卻因為演算方法的不透明，導致當事人就算得知自己受到負面評價，無從舉證去主張自己的權利。

（四） 去脈絡化的分析結果

大數據分析使用的資料探勘技術，是從大量片段的資料中找到和日常生活或是私生活行為舉止的關係，例如從購買紀錄或許可以推導出性取向。但是因為資料之間關聯性有時候很薄弱，特別是想要從非敏感性資料去推導出敏感性資料，這中間往往會因為一兩個因

子的誤差，而導致完全不同的結果。這時出現欠缺連結的推斷，對當事人可能造成不利益。

（五） 應對規範

對於上開歧視問題，美國聯邦交易委員會 2016 年的報告就建議，在進行分析之前，首先要確保資料具有代表性；企業必須謹防資料模型中隱藏的偏差，釐清統計關聯性和因果性之間的區別；同時企業也需要詳盡審視相關模型所依賴的因子，把握好預測分析與公平性之間的平衡關係；在流程建構上，允許消費者能檢視自身資料並就錯誤或遺漏提出異議[70]。白宮 2016 年的報告則提出通過演算法和系統的設計來實現平等權利（a principle of 「equal opportunity by design」），並建議研究機構和業界一起開展演算法審計和對大數據系統的外部測試以保證人們被公平對待[71]。

歐洲則更進一步在 2016 年通過，預計於 2018 年 5 月 25 日正式生效的歐盟一般資料保護規則中，第 13 條和第 14 條明定不管是直接或間接蒐集個人資料，當使用這些個人資料進行側寫、分析時，都必須要讓個人資料被蒐集者得知自己的資料受到側寫、分析，同時也要告知進行這些活動的目的，同時必須具有法定依據或者獲得用戶明確同意；用戶必須是在充分知情下做出同意授權；不得針對敏感議題(例如：種族、政治立場、宗教信仰、性取向等)進行剖析。

在第 21 條賦予反對個人資料被側寫（Profiling）的權利，第 22 條明確規定了對於僅僅以自動化方式（包括側寫）做出的、對個人能夠產生法律效果的或其他類似的顯著影響的決定，個人有權免受這樣決定的制約。對於違反上開規定的，將會課處最高 2000 萬

[70] FTC REPORT, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (Jan 6, 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf (last visited Oct 26, 2017).

[71] The White House, Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights(May 4, 2016), https://www.whitehouse.gov/blog/2016/05/04/big-risks-big-opportunities-intersection-big-data-and-civil-rights (last visited Oct 26, 2017).

歐元，或是公司前一年度全球 4%的營業額。

第三節　資料跨境傳輸與在地化之資訊蒐集及監理趨勢

一、背景介紹

近數十年來，隨著網際網路的發展，國際合作越來越普遍，全球化的現象使得資料的跨境傳輸越發頻繁，創造出來的產值也相當驚人。單以電子商務的發展為例，美國國際貿易委員會（United States International Trade Commission）報告認為，由於全球消費者對於跨境連結越感舒適，跨境電子商務（cross-border e-commerce）預計將快速成長，自 2014 年的 800 億美元成長至 2025 年的 3500 億美元，占全球電子商務的百分之 10 至 15[72]。聯合國貿易暨發展會議（United Nations Conference on Trade and Development, UNCTAD)在 2016 年發表的報告也發現，就數位傳輸服務（digitally deliverable services）的產值而言，2012 年時由美國輸出至全球的數位傳輸服務就有 3837 億美元，由全球輸出至美國的則有 2336 億美元[73]。而同份報告也指出，全球範圍內跨境的產品、金融、服務的價值，在 2014 年時約有 30 兆美元的規模，而透過跨境電子商務完成的國際交易則大約佔了全部的百分之 12；全球 GDP 因跨境流通而於 2014 年時提高了百分之 10，而資料的流通（data flows）則佔了期中的百分之 35[74]。這些數據充分反應了資料的跨境流通對當今全球經濟發展的重要性。

---

[72] UNITED STATES INTERNATIONAL TRADE COMMISSION, *Recent Trends in U.S. Services Trade: 2015 Annual Report* 116 (2015), *available at* https://www.usitc.gov/publications/332/pub4526.pdf (last visited Oct. 17, 2017).

[73] United Nations Conference on Trade and Development [UNCTAD], *Data protection regulations and international data flows: Implications for trade and development* 4(2016), *available at* http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (last visited Oct. 17, 2017).

[74] *Id.*

然而，UNCTAD 的報告就指出，國際社會普遍的共識是資料跨境傳輸不能毫無限制，而是需要法令加以管制;不過當前階段國際間尚未有針對資料跨境傳輸建立一統一的全球模式[75]。這種管制的呼聲許多時候與個人資料的保護有關，在世界各國對於其國內個人資料之保護的態度不同，對於保護程度有寬嚴不同的設計，為使個人資料受到保護，因此有了管制的呼聲。大體而言，目前各國對於個人資料跨境傳輸之立場大致上可分為自由與限制兩種立場；採取自由立場的國家認為，如果從資訊自由及貿易自由的角度出發，應該鼓勵個人資料跨境傳輸與分享；而採取限制立場的國家，則可能有不同的立場，例如基於前述保護資料當事人隱私權的考量，或是為抵禦文化侵略、保障經濟利益或維護資訊主權等理由，而主張限制個人資料跨境傳輸[76]。在這樣的背景下，為使個人資料跨境傳輸能維持順暢，同時兼顧各國主權與資料自主權，透過國際規範或協議等方法以達成統一標準已經成為國際趨勢[77]。

目前國際間針對跨境傳輸的限制，廣泛而言，多半可以允許所謂「一次性例外情況」（one-off exceptional circumstances），意即雖然認為資料跨境傳輸應該以法令進行一定程度的限制，但應准許在特定情形下使資料進行跨境傳輸[78]。至於「持續性的例外情況」（Ongoing exceptions），目前在國際間則尚未達成一致共識[79]。常見的一次性例外情形包含：為履行契約所為之跨境傳輸（包含資料當事人與資料控制者間之契約、資料控制者與第三人間之契約等）；為法律程序、執法或獲得法律建議等目的而進行之跨境傳輸；為保護資料當事人之重大利益等情形[80]。至於持續性的例外情況，目前國際上一般使用的制度安排可以大致分為下列四種：

---

[75] *Id.* at 12.

[76] 陳榮傳，〈再論資料跨國流通〉，《月旦法學雜誌》，第 78 期，頁 166（2001）。

[77] 同前註。

[78] *Supra* note 73, at 13.

[79] *Id.*

[80] *Id.*

（一）「適當保護模式」（adequacy approach），又稱為「白名單模式」（whitelist approach）：

評估接收資料的第三國是否能提供個人資料足夠的保護程度，此方法為國際間廣泛採用之方法，包含歐盟、日本、以色列和瑞士等國家採取此一作法；

（二）「自我拘束規則模式」（binding rules approach）：

考慮進行跨境資料轉移的特定公司是否已經執行了足以保護個人資料安全的處理措施及獨立審查機制，這種方法可見於歐盟的「企業自我拘束規則」（Binding Corporate Rules system, BCRs）、亞太經濟合作組織（APEC）的「跨境隱私保護規則」（Cross Border Privacy Rules System, CBPRs）以及澳洲籍日本等國；

（三）「契約範本模式」（model contracts approach）：

此模式評估企業所使用的契約中之用詞是否已經提供個人資料轉移足夠的保護程度，此一方式目前僅有歐盟採用；

（四）「同意模式」（consent approach）：

此模式係檢驗個人是否同意將其資料進行跨境傳輸，但對於個人及企業而言，其同意可能難以證明，且難以保證獲得足夠之保護，此一模式可見於歐盟等地區[81]。

而從資料跨境傳輸衍生而來的，則是資料在地化的議題。資料在地化措施（data localization measure），指的是要求企業於儲存或處理「資料」（data）之伺服器必須設置在境內之法令或規範；因此，資料在地化措施亦可被稱為是「資料保護主義」（data protectionism）的現象之一[82]。一般來說，較少有國家係針對所有資料皆要求採取在地化措施，多半是針對特定領域的資料進行規範的情形，其中最常見的包含健康資料或金融

[81] *Id.*

[82] ALBRIGHT STONEBRIDGE GROUP, *Data Localization-A Challenge to Global Commerce and the Free Flow of Information* 3(2015).

服務領域之資料[83]。而之所以要求採取資料在地化措施的原因一般來說可能與下列動機有關：資料安全、海外監管可能性、透過網路提供之服務與政府監督需求[84]。

資料在地化措施的管制型態可能以法律、法規命令、行政規則等不同層級的規範出現；其所涉及的領域及主管機關也相當多樣，可能包含衛生機關、公共機關、稅務機關等等；正由於其管制型態及領域的多樣，使得要認定或完全盤點各國在地化措施變得相當困難[85]。不過，美國知名的全球戰略公司奧爾布萊特石橋集團（Albright Stonebridge Group）將資料在地化措施依其強度（strength）區分為下列6個等級，可以作為分析時的參考：

（一） 強烈（Strong）措施：指採取明確要求資料必須儲存在該國境內的伺服器上，採取此類作法的國家包含了中國大陸、印尼、俄羅斯、奈及利亞、越南與汶萊；

（二） 事實上（De Facto）措施：透過規範造成資料跨境傳輸的巨大阻礙，使其可以事實上達成資料在地化的效果，歐盟主要係採取這樣的作法；

（三） 部份（Partial）措施：指對跨境傳輸設下各種不同之條件，包含使用特定的網域名稱（domain name）、作跨境傳輸前須取得個資當事人之同意等，採用此種管制的國家包含印度、馬來西亞、南韓、白俄羅斯與哈薩克；

（四） 輕度（Mild）措施：僅於特定情況下限制資料的跨境傳輸，包含阿根廷、烏拉圭巴西、祕魯與哥倫比亞等國屬於此類；

（五） 特定部門（Sector Specific）措施：僅針對特定類別之資料採行在地化措施，例如針對健康照護（healthcare）、電信（telecom）、財政（finance）與國家安全（national security）等性質之資料，我國、澳洲、紐西蘭、加拿大、土耳其與委內瑞拉等國籍採取此種作法；

---

[83] *Id.*

[84] *Id.*

[85] EUROPEAN COMMISSION, *European free flow of data initiative within the Digital Single Market* 2(2016).

（六） 無措施（None）：無已知的資料在地化措施[86]。

然而，值得注意的是，由於實施資料在地化措施會影響資料跨境傳輸、影響全球供應鏈，對於電子通信、社群為體及製造業、服務業的資訊近用都會造成影響，因此會對全球經濟造成負面影響[87]。研究認為，資料在地化措施可能會對貿易、創新和競爭性帶來風險；同時，採行資料在地化的同時，會忽略近用資料時的真實狀況比起個人資料之濫用來得更為重要，影響資料之保護程度[88]。另外，UNCAD 研究發現，資料在地化措施之實施可能對於實施該措施的國家經濟造成負面影響，影響該國 GDP 的表現，根據該研究的預估，這類措施會使印度及巴西的 GDP 減少百分之 0.7 和百分之 0.8，而韓國更會減少百分之 1.1 的 GDP[89]。而從企業的角度來看，採行資料在地化措施，則可能使其增加百分之 30 至 60 的運算（computing）成本[90]。

二、各國資料在地化與跨境傳輸之規定

（一） 歐盟

歐盟於 1995 年頒布個人資料保護指令(95/46/EC)[91]，對於歐洲各國乃至全世界個人資料保護法制之發展，均有極重要影響。但 1995 年以來，資通訊技術發展變化迅速，網際網路與各項應用興起、近年來又有「巨量資料」與 IOT[92]概念之提出，既有歐盟個人資

[86] ALBRIGHT STONEBRIDGE GROUP, *Data Localization-A Challenge to Global Commerce and the Free Flow of Information* 5(2015).

[87] *Id.* at 7.

[88] *Id.* at 14.

[89] *Supra* note 73, at 4.

[90] *Id.*

[91] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.

[92] 物聯網時代資料保護的挑戰，可參考：徐彪豪，〈隱私與便捷的取捨——IoT時代下的資料分析利用 〉，《走入生活的智慧聯網——匯流科技、政策與產業》，財團法人資訊工業策進會科技法律研究所，頁 129-137（2013）。

料保護指令面對這些變化已經難以為繼，是以歐盟執委會於 2012 年宣布將要重新審視歐盟境內的資料保護法案，並提出新的資料保護規則草案，希望可以取代歐盟 1995 年通過之個人資料保護指令。該草案試圖整合過去三大資料保護指令[93]。同時由於 1995 年個人資料保護指令在規範形式上僅為「指令（directive)」，其執行必須透過各國立法轉化，自然免不了造成產生各國個人資料保護規範不一致之情形。這次歐盟以具有直接規範效力之「規則（regulation)」之制定，進一步統合各會員國間之個人資料保護標準，展現出落實資料保護的決心，減輕企業法規遵循的負擔，同時並強化個人對其個人資料的有效掌握(effective control)。

歐盟執委會(European Commission)於 2012 年初提出草案後[94]，原本希望能於 2014 年完成立法，2016 年正式施行。然而因為草案內容爭議頗大，各方意見紛歧，直至 2013 年底，歐洲議會公民自由、司法與內政委員會（European Parliament Committee on Civil Liberties, Justice and Home Affairs）才通過對於執委會版草案之修正意見；其後，歐盟執委會、議會（European Parliament）與理事會（European Council）持續進行三方協商討論，於 2015 年末終於獲致共識，於 2016 年 4 月 27 日通過，5 月 4 日公布，正式成為歐盟第 2016/679 號規則（Regulation (EU) 2016/679）[95]。原本依據歐盟一般資料保護規則第 99 條第 1 項，其將於公布後 20 天生效(2016 年 5 月 25 日)，但考量為達到歐

[93] Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final (Jan. 25, 2012), available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF (last visited Nov. 10, 2017).

[94] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited:Nov. 9, 2017).

[95] Reform of EU data protection rules, European Commission, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last visited Nov. 10, 2017).

盟個資保護規則所要求之水準，需要時間因應此一轉變，故在第 99 條第 2 項將生效日期延後 2 年，於 2018 年 5 月 25 日生效。此一新法在生效之後將會完全取代現行的個人資料保護指令，並且建立歐洲個資保護新秩序。

歐盟於 1995 年通過個人資料保護指令就有禁止會員國將個人資料跨境傳輸至對於資料保護不夠充足之國家[96]。依照指令的第 25 條，傳遞個人資料至第三國或國際組織，須在歐洲執委會認為該國或該組織具有充足的保護水準時始得為之。一般資料保護規則延續相同的規範，在第 45 條規定，除上述要求外，增加第三國須有獨立以及有效執法的主管機關，以及該第三國是否符合國際標準或簽訂其他現行有效之多邊或區域體系中保護個人資料之條款。

（二） 中國大陸

中國大陸是當前推行資料在地化措施最為積極，涉及層面最為廣泛的國家之一，其早至 2006 年起就針對銀行從事電子銀行業務要求實施資料在地化措施，近年來則不斷擴增要求實施在地化措施的範圍。以下將介紹目前已經施行的相關規定。

1. 金融領域

電子銀行業務管理辦法：金融領域是中國大陸最早要求實施資料在地化措施的領域。2006 年時，中國大陸的中國銀行業監督管理委員會通過《電子銀行業務管理辦法》，要求商業銀行等金融機構透過網路或通訊管道、自動服務設施等途徑向客戶提供銀行服務[97]時；如果是中資銀行業金融機構的話，其營運系統（运营系统）和業務處理伺服器（服务器）應設置在中國大陸境內[98]；若是外資銀行，則可以將其營運系統和業務處理伺服器設置在境內或境外，但設置在境外時，仍應在中國大陸境內設置可以紀錄和保存業務交易數據的

[96] Data Protection Directive, art. 45.

[97] 《电子银行业务管理办法》第 2 条（银监会令[2006]5 号）。

[98] 《电子银行业务管理办法》第 10 条第 4 款（银监会令[2006]5 号）。

設備，以滿足金融監管單位的現場監管及司法機關調查證據的需求[99]。

由此可見，中國大陸之所以要求銀行業者實施在地化措施，主要原因是為了確保其行政的監理及司法的調查可以順利落實。

人民銀行關於銀行業金融機構做好個人金融資訊保護工作的通知：2011 年，中國人民銀行針對銀行業金融機構蒐集、利用與對外提供個人金融資訊發布了《人民銀行關於銀行業金融機構做好個人金融資訊保護工作的通知》，要求各銀行在中國大陸境內蒐集的個人金融資料的儲存、處理和分析應於中國大陸境內進行，如無其他法律法規及中國人民銀行的規定，不得向境外提供個人金融資料[100]。

中國人民銀行金融消費者權益保護實施辦法：在 2011 年發布的通知基礎上，中國人民銀行於 2016 年底為進一步規範金融機構行為並確實保障金融消費者的權益[101]，制定了《中國人民銀行金融消費者權益保護實施辦法》。該辦法要求為金融消費者提供金融產品和服務的銀行業金融機構；提供跨市場、跨行業交叉性金融產品和服務的其他金融機構；以及非銀行支付機構等三類金融機構[102]，針對其在中國大陸境內蒐集的個人金融資訊（信息）的儲存、處理和分析應在中國大陸境內進行，且如無其他法律法規或中國人民銀行的規定，不得對境外提供個人金融資訊。[103]但同時，該辦法亦規定，如果中國大陸境內的金融機構在當事人同意（授权）的情況下，為了處理跨境業務，得向境外機構傳輸境內蒐集的個人金融資料，但應符合法律、行政法規和相關監管部門的規定，並簽訂協議、現場查

[99] 《电子银行业务管理办法》第 10 条第 4 款（银监会令[2006]5 号）。

[100] 《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第 6 条（银发〔2011〕17 号）。

[101] 《人民银行关于印发《中国人民银行金融消费者权益保护实施办法》的通知》(银发〔2016〕314 号)。

[102] 《中国人民银行金融消费者权益保护实施办法》第 2 条第 1 款（银发〔2016〕314 号）。

[103] 《中国人民银行金融消费者权益保护实施办法》第 6 条（银发〔2016〕314 号）。

核等，要求境外機構對個人金融資料保密[104]。

2. 徵信業

2013 年時，中國大陸針對徵信業制定《徵信業管理條例》。該條例第 24 條第 1 款規定，徵信機構在中國大陸境內蒐集到的資料之整理、保存和加工，應於中國大陸境內進行[105]。

3. 出版業

2016 年時，中國大陸的「國家新聞出版廣電總局」以及「工業和信息化部」公告，《網路出版服務管理規定》已經於 2015 年時經國家新聞出版廣電總局通過，並獲得工業和信息化部同意，於 2016 年 3 月 10 日起施行。

《網路出版服務管理規定》係依據《出版管理條例》及《互聯網資訊服務管理辦法》等法律之規定所制定的規定[106]。該規定第 8 條規定了圖書、音像、電子、報紙、期刊出版單位經營網路出版服務應具備的條件，其中要求上述出版單位應具備有從事網路出版服務所需的必要技術設備，且相關伺服器與儲存設備應存放於中國大陸境內[107]。

4. 健康資訊

2014 年時，中國大陸「國家衛生計生委」（相當於我國衛生福利部）為了規範人口健康資料的管理、促進共享利用，制定了《人口健康資訊管理辦法（試行）》，規範各級各類「醫療衛生計生服務機構」人口健康資料的蒐集、管理、利用、安全及隱私保護[108]。所謂人口健康資料係指前述機構在服務和管理過程中所產生的人口基本資料、醫療衛生服務資

---

[104] 《中国人民银行金融消费者权益保护实施办法》第 33 条（银发〔2016〕314 号）。

[105] 《征信业管理条例》第 24 条第 1 款（国务院令第 631 号 2013.01.21）。

[106] 《网络出版服务管理规定》第 1 条（国家新闻出版广电总局、工业和信息化部令第 5 号 2016.02.04）。

[107] 《网络出版服务管理规定》第 8 条第 3 款（国家新闻出版广电总局、工业和信息化部令第 5 号 2016.02.04）。

[108] 《人口健康信息管理办法（试行）》第 1 条、第 2 条（国卫规划发〔2014〕24 号）。

料等[109]。

該法要求醫療衛生計生服務機構不得將人口健康資料儲存於境外的伺服器之中，也不可託管、租賃境外伺服器[110]。

5. 地圖資訊

2015 年 11 月，中國大陸國務院公布《地圖管理條例》，該條例第 34 條中規定網路（互聯網）地圖服務單位需將儲存地圖資料（数据）的伺服器設置在中國大陸境內[111]。

6. 網路安全

中國大陸在 2016 年時制定了《網路安全法》，並於今年(2017 年)6 月 1 日正式施行。此一法律為中國大陸對資料在地化要求範圍最廣的法律規定。

該法第 37 條要求關鍵資訊（信息）基礎設施的營運者（运营者）將其在中國大陸境內蒐集和產生個個人資料（信息）及重要數據儲存於中國大陸境內，如果因業務需要而需向境外提供的話，則應依相關辦法進行安全評估[112]。

所謂關鍵基礎設施，其認定範圍相當廣，包含「公共通信和資訊服務、能源、交通、水利、金融、公共服務、電子政務等重要行業和領域」以及「其他一旦遭到破壞、喪失功能或者資料洩露，可能嚴重危害國家安全、國計民生、公共利益的關鍵資訊基礎設施」[113]。

（三） 香港

香港的個人資料的保護相關規定主要規定於香港的《個人資料（私隱）條例》，該條例係於 1995 年制定，並於 1996 年 12 月 20 日生效。該條例第 33 條規定，凡是其蒐集、

---

[109] 《人口健康信息管理办法（试行）》第 3 条第 1 款（国卫规划发〔2014〕24 号）。

[110] 《人口健康信息管理办法（试行）》第 10 条第 2 款（国卫规划发〔2014〕24 号）。

[111] 《地图管理条例》第 34 条第 1 款（国务院令第 664 号 2015.11.26）。

[112] 2016 年《网络安全法》第 37 条。

[113] 2016 年《网络安全法》第 31 条。

持有、處理或使用在香港進行，或是由主要業務地點是在香港的人所控制的個人資料，原則上資料使用者不得將個人資料轉移至香港以外的地區，但定有 6 種例外得轉移的情形。[114]

這六類例外包含：第一，「白名單模式」，可以向香港個人資料私隱專員指定之特定司法區傳輸個人資料，該司法區執行與香港相類似之個人資料隱私保護法律[115]。第二，若傳輸地並非白名單所列區域，但資料使用者有合理理由相信該地有與香港類似之各資料隱私保護法律生效，亦可以向該地傳輸個人資料[116]。第三則是獲得當事人書面同意進行移轉[117]。第四，若資料使用者有合理理由相信，跨境的傳輸是為了避免或減輕對當事人的不利行動，同時無法得當事人之同意，且當事人應會同意時，亦可以執行跨境傳輸[118]。第五，若資料屬於家庭用途[119]、防止犯罪[120]、保護當事人或他人身體精神健康[121]、依據法律規定或授權移轉[122]、因新聞[123]、統計、研究[124]或辨識生命急難之人[125]等香港個人資料（私隱）條例鎖定是由亦可執行跨境傳輸。最後則是所謂「克盡職責」的規定，若資料使用者已經近期所能確保個人資料之處理方式不會違反香港個人資料（私隱）條例規定時，則亦可進行跨境移轉[126]。

---

[114] 個人資料（私隱）條例第 33 條（香港）。

[115] 個人資料（私隱）條例第 32 條（香港）。

[116] 個人資料（私隱）條例第 32 條（香港）。

[117] 個人資料（私隱）條例第 32 條（香港）。

[118] 個人資料（私隱）條例第 32 條（香港）。

[119] 個人資料（私隱）條例第 52 條（香港）。

[120] 個人資料（私隱）條例第 58 條（香港）。

[121] 個人資料（私隱）條例第 59 條（香港）。

[122] 個人資料（私隱）條例第 60B 條（香港）。

[123] 個人資料（私隱）條例第 61 條（香港）。

[124] 個人資料（私隱）條例第 62 條（香港）。

[125] 個人資料（私隱）條例第 63C 條（香港）。

[126] 個人資料（私隱）條例第 32 條（香港）。

香港《個人資料（私隱）條例》第 33 條的規定目前尚未施行，但香港個人資料私隱專員公署仍鼓勵資料使用者採取符合該條的規定，作為企業管制責任的一部分。此外，香港立法會議員曾就多次該條之實行時間多次質詢政府，香港政府則以須考量個人資料私隱專員是否有制定、修訂及廢除「白名單」能力[127]；以及考量其對銀行業及電信業衝擊[128]；還有因應跨境資料流通之規模日漸增加、形式日漸多樣應審慎評估等為由，作為持續推遲該條施行的理由[129]。

（四） 俄羅斯

目前世界上採取強力的在地化措施的國家中，最有名的除了中國大陸以外，就屬俄羅斯了。近十年來，俄羅斯亦一步步的增強其資料在地化措施的要求。

俄羅斯個人資料保護法第 12 條規定，個人資料進行跨境傳輸原則上應確保目的地對當事人個資權利能提供充足的保護，但若有當事人書面同意、依據國際協定之法律程序、國安或國防目的、或未履行與當事人契約、保護當事人或他人生命健康或其他重要利益的情況下，亦可例外在未有充足保護時，傳輸至第三地。

此後，俄羅斯對於資料跨境的要求則逐漸增強。2014 年 7 月時，俄羅斯國會通過聯邦法規第 242 號，修正該國個資法，要求個人資料營運商應將處理及儲存俄羅斯公民個人資料的伺服器設於俄羅斯境內；並於營運前，向俄羅斯政府報備伺服器的地點，此部份規定已於 2015 年 9 月 1 日生效。

---

[127] （香港）政制及內地事務局，〈立法會十三題：個人資料移轉〉，（香港）政制及內地事務局，2007/03/07，http://www.cmab.gov.hk/tc/upload/lcq20070307person_c.pdf （最後瀏覽日：2017/02/10）。

[128] 同前註；（香港）政制及內地事務局，〈立法會政制事務委員會檢討《個人資料（私隱）條例》與相關事宜〉，立法會 CB(2)582/10-11(03)號文件，第 35 點，頁 11（2010/12），http://www.legco.gov.hk/yr10-11/chinese/panels/ca/papers/ca1220cb2-582-3-c.pdf （最後瀏覽日：2017/02/10）。

[129] （香港）政制及內地事務局，〈立法會十九題：《個人資料（私隱）條例》第 33 條的實施〉，（香港）政制及內地事務局，2007/03/07，http://www.cmab.gov.hk/tc/press/press_3611.htm （最後瀏覽日：2017/02/10）。

俄羅斯國會更進一步在 2016 年 7 月，通過聯邦法規第 374 號，修正反恐法，要求電信業者保留使用者通聯記錄 3 年，網路電信業者保留 1 年，且應保留其通訊的內容 6 個月，此部份規定將於 2018 年 7 月 1 日生效。綜合此次修法與前次修法的內容觀察，俄羅斯對於資料在地化的範圍及內容，都有相當多的規範。

這些資料在地化之措施已經對於跨國公司在俄羅斯展開相關服務造成影響，2016 年 11 月莫斯科市法院便以職業社交網站 LinkedIn 違反資料在地化措施規定，未將俄羅斯之使用者個人資料存放於俄羅斯境內為由，裁定禁止其餘俄羅斯境內營運[130]。

（五） 澳洲

一、 隱私權法

澳洲關於個人資料之規範，最主要係規範於《1988 年隱私權法》(Privacy Act 1988，以下簡稱《隱私權法》)之中。其中，隱私權法第 16C 條定義資料跨境揭露的意涵，而《隱私權法》授權訂定之《澳洲隱私權原則》(Australian Privacy Principles，以下簡稱 APPs、《隱私權原則》) 第 8 點則針對個人資料之跨境揭露（cross-border disclosure of personal information）有更詳細的規定。

根據《隱私權法》第 16C 條之規定，若「政府機關或私人組織」(即 APP entity，指受該法所規範之主體）揭露（disclose）個人資料給「海外資料接收者」(overseas recipient)，便屬於該法所定義的資料跨境揭露（資料跨境傳輸）[131]。

而澳洲對於資料跨境揭露的詳細規範，則在《隱私權原則》第 8 點「個人資料之跨境揭露」(cross-border disclosure of personal information）中有更詳細的規定。《隱私權原則》要求政府及私人組織應在跨境揭露前採取合理措施，以確保海外資料接收者不

---

[130] 端傳媒，〈因拒絕將用戶個人數據儲存在本地，LinkedIn 恐遭俄羅斯封殺〉，2016/11/11，https://theinitium.com/article/20161111-dailynews-russia-linkedin-blocked/ （最後瀏覽日：2017/10/27)。

[131] *Privacy Act 1988* (Cth) s16C (Austl.).

致違反《隱私權原則》的規定[132]，除非其能合理相信海外資料接收者接收個人資料時，將符合相關規範之規定，且其效力必須與《隱私權原則》保護個人資料之效力本質上相似，且有機制可以使該海外資料接收者採取法律保護個人資料[133]。或是若該政府或私人組織已經得到資料當事人告知後同意其進行跨境揭露;或未履行澳洲法律規定、法院命令(order)或履行國際條約義務、合理且必要之執法行為（且接收者有適當之職權）；或是在一般情形下，其所跨境揭露之資料屬於該政府或私人組織，亦可不採行前述之合理措施[134]。

《隱私權法》中關於跨境書的相關規定係於 2012 年時所修正，依照依照《2012 年隱私權法修正案（增強隱私保護）:解釋性備忘錄》(Privacy Amendment (Enhancing Privacy Protection) Bill 2012:Explanatory Memorandum）之記載澳洲本次修法係採取與《APEC 隱私保護綱領》(APEC Privacy Framework)類似之「課責模式」(accountability approach)，增加要求政府或私人組織於執行跨境傳輸前，應先採取合理措施，確保資料接收者能符合澳洲法律規定[135]。

二、　電子健康紀錄法

除了澳洲《隱私權法》對於個人資料的跨境運輸訂有規定外，澳洲尚有一被視為資料在地化措施規定於其《2012 年我的健康紀錄法》(My Health Records Act 2012，以下簡稱，《我的健康紀錄法》）之中。《我的健康紀錄法》原名《2012 年個人管理電子健康紀錄

---

[132] *Australian Privacy Principles* (Cth) 8.1 (Austl.).

[133] *Australian Privacy Principles* (Cth) 8.2 (Austl.).

[134] *Australian Privacy Principles* (Cth) 8.2 (Austl.).

[135] Privacy Amendment (Enhancing Privacy Protection) Bill 2012:Explanatory Memorandum, Parliament of Australia, http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728/upload_pdf/368711.pdf;fileType=application%2Fpdf (last visited Oct. 26, 2017).

法》(Personally Controlled Electronic Health Records Act 2012)，後於 2015 年更名為現名[136]。

根據《我的健康紀錄法》的規定，澳洲政府建立一全國性的健康資料庫「我的健康紀錄」(My Health Record)，其功能類似我國健康存摺與雲端藥歷，是一選擇性加入的健康資料庫[137]。該健康資料庫內記載的內容包含：處方藥物資訊、病歷、器官捐贈意願、出院資訊（Hospital discharge information)、醫學影像報告、病理學報告等，亦可增加依照個人意願過敏源或相關藥品副作用資訊以及預立醫療決策[138]。

原則上不允許於澳洲境外持有、處理「My Health Record」系統內之資料，或將該資料庫資料攜出澳洲境外，或使其他人於澳洲境外持有、處理「My Health Record」系統內之資料、或使其將「My Health Record」系統內之資料攜出澳洲[139]。

然而，若個人電子健康紀錄系統之營運機構澳洲衛生部（System Operator）在經過授權的情況下，基於個人電子健康紀錄系統之管理或營運之目的，可以允許其於澳洲境外持有、攜出或處理該系統之資料。但不包括關於系統中消費者或參與者之個人資料、任何可識別之個人或政府機構或私人組織之資料[140]。

---

[136] Series: C2012A00063 My Health Records Act 2012, Federal Register of Legislation, https://www.legislation.gov.au/Series/C2012A00063 (last visited Oct. 26, 2017).

[137] 陳誌雄、李崇僖、張照恬，〈105 年度政府健康資訊開放應用國際趨勢之法規推動計畫成果報告〉，衛生福利部中央健康保險署委託研究，頁 95（2016)。

[138] Managing your My Health Record, My Health Record, https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/managing-your-my-health-record (last visited Oct. 26, 2017).

[139] *Id.*

[140] *Id.*

第四章　我國通訊傳播產業資料加值與創新應用之法制盤點

第一節　個人資料去識別化之標準與應用相關議題

一、 國外重要國家作法

美國的個人資料保護制度上並沒有一個通用的法律來規範,只有一部分對於個人資料保護有高度需求的專門領域的有立法規範，像是針對生醫資訊的 HIPPA、或是針對兒童隱私保護的 COPPA 等。而對於個人資料保護負責單位是以 FTC 為中心，除了製作關於個人資料保護的報告書和指導方針外，也負責調查與強制執行。

關於去識別化和再行識別的規範也是如此,美國並沒有訂一個跨產業和領域別的法律來規範，而是透過像是 HIPPA 或是 FTC 報告書中所頒布的標準來規範。而其中 FTC 報告書中所訂的再行識別規定也被世界許多國家,像是日本等引用作為制定相關規範的依循標準。而對於違反規定者為再行識別行為者，FTC 是透過聯邦交易委員會法第五條規定，認定該行為屬於「不公平」，而得以起訴或是行政裁罰。而對於提供去識別化資料給第三人者，也要求要以契約約束，同時得有監督和違約處理的機制。

總結來說，美國現今的重新識別行為雖然沒有專門的法律規範，但是透過 FTC 頒布的標準，以及透過聯邦交易委員會法和契約的雙重運作，得以有強制力來確保重新識別行為規範的執行。

而英國資料保護法與對於個人資料及資料去識別化之規定為:個人資料皆指可直接或間接識別個人之資料;而對於去識別化之規定，只要資料經去識別化而無法直接或間接識別個人後，即非屬個人資料，而無英國資料保護法之適用餘地。

相對於歐盟對「去識別化資料」採取非常嚴格之門檻標準，甚至於中提到如果資料保有者在事件層次（event-level）並沒有刪除原始（可識別）資料（例如：在移除或摘蓋可識別資料之後)，即提供資料集的一部份，則所產生的資料集，仍然是個人資料。依英

國資訊保護官及英國法院之見解，則對於「去識別化資料」之範圍界定相對較為寬鬆，認為縱使係「可逆之擬匿名化資料」，只要原資料保有者並未將對照表或解密方法等連結工具提供給資料接收者，並且採取適當安全措施，使資料接收者無管道及機會重新識別資料當事人，則該釋出的資料也屬「去識別化資料」之一種。只是未來英國對於去識別化資料的認定是否會隨著歐盟個資新法規範進行調整，值得觀察。

日本的作法相較其他各國以更為直接的方式來規制，於 2015 年通過之個人資料保護法修正增訂「匿名處理資料」 概念，增設「個人資料保護委員會」此一專責機關，負責「匿名處理資料」相關督管理及配套規範之訂定。同時在管理「匿名處理資料」上，對「去識別化」資料作成方及接收方都有課以相當的義務，直接明文禁止將去識別化的資料進行比對還原。惟新修正的個人資料保護法條文對於違反規定重新識別個人，僅揭示「個人資料保護委員會」得採取勸告或必要措施，在規制力道上略有不足，是整個立法上最為可惜之處。

二、 我國對於去識別後資料之定性及其應用之限制

按我國個人資料保護法（以下簡稱個資法）第 2 條第 1 款對個人資料的定義，包含該款列舉之 19 種資料在內，所有得以直接或間接識別個人的資料極為個人資料。所謂直接識別，指的是只要單憑該資料，即可知悉資料當事人之身份；而間接識別，依據個人資料保護法施行細則（以下簡稱個資法施行細則）第.3 條的規定，指的是該資料不無法直接識別當事人，但在與其他資料對照、組合、連結之後，則可以識別特定個人的情形。舉例而言，若單純以代碼或編號取代當事人姓名（如員工編號等），則該比資料應仍可透過與其他筆資料的對照、組合，識別出該資料當事人的身份，因此仍屬於具有間接識別行之個人資料。

然而，若資料經去識別化，使其無法透過直接或間接的方式識別特定個人，則根據法務部103年11月17日法律字第10303513040號函的解釋，其以不具有直接及間接識別性，

「非屬個人資料，自非個資法之適用範圍」[141]。

至於對去識別化之資料重行識別的行為，目前個資法並無相關之規定。法務部則認為，對已經去識別化之資料重行識別，依照目前個資法之定義，應定性為資料的「蒐集」行為，需有個資法上合法之理由，期中個資法第 19 條第 1 項第 3 款「當事人自行公開或其他已合法公開之個人資料」及第 7 款「個人資料取自於一般可得之來源」兩項規範，其要件必須是該資料為「個人資料」才有適用，對於「去識別化資料」並無法適用[142]。而根據個資法之規定，非公務機關若違法蒐集個人資料，則可依據第 47 條之規定，處以行政裁罰。

綜上，依據目前實務上之解釋，個人資料經去識別化後，即非屬個資，不受個資法規範，但在未有個資法關於「蒐集」的合法要件下，不得對其進行再識別，否則可能被處以行政裁罰。

三、 我國對於「去識別化」行為之定性及其相關要求

此外，對於將個人資料「去識別化」之行為，究竟應屬個資法上何種性質之行為，亦值得討論。法務部認為，去識別化之行為應理解為對個人資料之處理行為[143]。

依據上述法務不知見解，依個人資料保護法之定義，「去識別化」此一處理行為原則上亦須有特定目的才可為之。然而，法務部同時認為「個人資料之『蒐集』大多緊密伴隨

---

[141] 法務部 103 年 11 月 17 日法律字第 10303513040 號函

[142] 〈規範重新識別行為〉，vTaiwan，https://talk.vtaiwan.tw/t/topic/566/4 （最後瀏覽日：2018/01/10）。

[143] 法務部，〈公務機關利用去識別化資料之合理風險控制及法律責任〉，頁 7，行政院國家發展委員會，https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjA__-Kj83YAhVGLpQKHXUQDsMQFggmMAA&url=https%3A%2F%2Ftraining.ndc.gov.tw%2Fupload%2Fofiles%2F20161021090832.pdf&usg=AOvVaw2DLH7s9UwTLEzgZ71LewIL （最後瀏覽日：2018/01/10）。

著『處理』行為，故個資法並未特別區隔兩者之行為要件」，同時「去識別化之加工處理並未增加對當事人權益之額外侵害」，因此如資料之蒐集具有個資法上合法之權源，「應可認為去識別化之處理並未逾越原先蒐集 之特定目的，而得依據原先蒐集時之同一合法事由為之」[144]。因此，依據法務部之解釋，若為何法蒐集之資料，原則上亦可合法的對齊進行「去識別化」之處理。

四、 我國對於去識別化之標準及規範

目前法務部對個資法之解釋，僅說明去識別化應達到無法識別特定當事人之程度，但做到什麼程度才符合法律規範，則並無明確說明，需要有另外的參考依據。

經濟部標準檢驗局在 2014 年 6 月 4 日公告 CNS 29100「資訊技術-安全技術-隱私權框架」國家標準，提供資通訊技術系統保護個人可識別資訊的高階框架，將組織、技術及程序各層面置於整體隱私權框架中。此一國家標準明確定義處理個人可識別資訊的行為者及其角色，描述隱私和保全的考量，以及對資訊技術已知隱私權原則提供參考資訊。

2015 年 6 月 10 日，經濟部標準檢驗局則公告 CNS 29191「資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項」國家標準，作為有關個資安全管理的重要規範。

然而，上述 CNS 標準僅為經濟部標檢局依據標準法所發布之國家標準，不一定能直接將經上述國家標準規範之架構與程序處理後之資料認為不具有個資法所定之直接或間接識別性。不過若遵循相關國家標準之程序，應可成為法官等解釋適用法律者在評斷機關、企業做個資保護是否善盡管理之責時或個資匿名化和去識別化是否合格時的重要參考指標。反面來說，只要個人資料去識別化的過程未遵守這樣的規定，則該資料則可能被視為未經足夠之去識別化，而仍屬於我國個資法定義之個人資料。

因此，將個人資料依據前述標準操作進行去識別化後再為其他之利用行為，由於已經依照經濟部標檢局所訂規範進行去識別化，應可認為其不具將個人為違法利用之故意性，

[144] 同前註。

而個資法目前並未以刑事處罰過失之行為，故應不需要負刑事責任[145]。

因此在結論上，本研究傾向建議業者若不欲受到個資法告知和請求同意的規範，特別是在實務運作上不可能向當事人個別徵求同意的狀況下，應提供 CNS 29100 及 CNS 29191 規定讓業者去遵循以踐行去識別化工作，消除識別因子以保護個資當事人，以及避免業者自身因為侵害個資而遭到民事求償或是行政處罰。同時對經過去識別化的資料也要審慎評估受到他人再識別化的可能性，目前初步研析比較可行的作法是以契約去約束資料的受傳輸方，要求不得以任何方法去比對、還原經去識別化資料的識別因子。

第二節　資料分析所產生的歧視議題

我國目前尚未針對資料分析可能後續引發的歧視議題有法律上的規範。我國個人資料保護法目前也未針對將資料匯集成立資料庫，或進一步對資料進行側寫等行為有特殊之規範。結論上來說，我國目前尚未針對此一議題有相關的規定。

不過值得注意的是大法官解釋釋字第 603 號曾明確要求政府大規模蒐集、錄存人民指紋並建立資料庫時，應以法律定之，並有特定重大公益之目的，同時其蒐集應與重大公益目的之達成具有密切之必要性與關聯性，且應明文禁止法定目的外之使用[146]。而林子儀大法官針對該號解釋所提出之協同意見書則認為，由於「隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化」，而當「看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出」，故其認為隱私權保障的範圍應擴張至非私密或非敏感性質的個人資料保護[147]。

除此之外，日前蔡季勳等台灣人權促進會成員就「健保資料庫訴訟案」確定終局判決

[145] 前揭註 143，頁 12。

[146] 大法官解釋釋字第 603 號。

[147] 大法官解釋釋字第 603 號林子儀大法官協同意見書。

[148]聲請大法官解釋，於聲請書中及主張：隨著巨量資料分析技術的發展，大規模的資料處理與解析，可以「從離散無意義之資料中，獲得對個體與群體額外的認識，而成為國家進一步實施社會控制的基礎」，因此大規模的蒐集、處理、利用個資，甚至建立資料庫的行為對於個人資訊自主有更強的限制，且對於人格自由發展有更大的威脅[149]。因此，該聲請書主張，對大規模蒐集、處理、利用及建立資料庫的行為，應以較嚴格的違憲審查基準檢驗，而目前個資法未區分小規模與大規模的個資蒐集、處理、利用行為，就大規模蒐集個資的部份，已經違反憲法規定[150]。

對於此一聲請，大法官目前尚未做出是否受理之決定，後續是否會針對我國「建立個資資料庫」的規範做出解釋，值得進一步追蹤。

第三節　資料跨境傳輸與在地化之資訊蒐集及監理

我國個人資料跨境傳輸與在地化之限制規定，除依個人資料保護法規定進行外，尚有因其他法令（或其他法令授權所定之法規命令）進行規範者。以下，將先從我國個資保護之主軸——個人資料保護法相關規定進行整理，再針對其他法律所為之限制，逐一盤點。

一、 個人資料保護法中對於資料跨境傳輸之規定

我國個資法對於公務機關資料之跨境傳輸，目前並無任何明文之限制。在非公務機關的部份，則根據個人資料保護法第 21 條的規定，原則上允許其進行跨境傳輸，然而也規

---

[148] 最高行政法院 106 年度判字第 54 號判決。

[149] 蔡季勳、邱伊翎、施逸翔、滕西華、黃淑英、劉怡顯、洪芳婷，〈憲法解釋聲請書（最高行政法院 106 年度判字第 54 號判決)〉，頁 36-38，台灣人權促進會，https://www.tahr.org.tw/sites/default/files/u5/shi_xian_sheng_qing_shu_20171204.pdf（最後瀏覽日：2018/1/9)。

[150] 同前註，頁 38。

定中央目的事業主管機關，可在有下列情形任一出現時，限制非公務機關個人資料的跨境傳輸：

（一） 涉及國家重大利益；

（二） 國際條約或協定有特別規定；

（三） 接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞；

（四） 以迂迴方法向第三國（地區）傳輸個人資料規避個人資料保護法之規定[151]。

我國目前唯一依據個資法規定，限制跨境傳輸者，係針對通訊傳播領域資料所為之限制。國家通訊傳播委員會在電腦處理個人資料保護法修正為個人資料保護法前，即於 2012 年 9 月 25 日時，因當時有效之電腦處理個人資料保護法第 24 條第 3 款之規定，以通傳通訊字第 10141050780 號令「限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區」[152]。根據此一法規命令之規定，之所以禁止通傳業者將個資傳遞至大陸，乃是因為「大陸地區之個人資料保護法令尚未完備」所致，係為保障個人資料保護所設之規定。

而除了個資法相關之規定外，我國人體生物資料庫管理條例，以及銀行法、信用合作設法所授權之法規命令，亦有針對個人資料之跨境傳輸有所限制，茲說明如下。

二、 人體生物資料庫管理條例之規定

我國對於人體生物資料之管理，定有「人體生物資料庫管理條例」進行特別規範。而人體生物資料庫管理條例第 15 條則對於人體生物資料庫之資料及檢體之跨境傳輸，定有限制。

根據人體生物資料庫管理條例第 15 條的規定，我國禁止生物資料庫中之生物檢體(不

[151] 個人資料保護法第 21 條

[152] 〈限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區〉，國家通訊傳播委員會網站，http://www.ncc.gov.tw/chinese/print.aspx?table_name=news&site_content_sn=538&sn_f=26302 （最後瀏覽日：2017/10/19）。

含其衍生物）輸出至境外，至於生物檢體之衍生物及生物資料庫中之資料，於輸出前則應經主管機關衛生福利部核准。所謂生物檢體之衍生物，指的是人體組織、血清、血漿或血球等生物檢體經生物科技程序操作後，產生之萃取物或研發物（但不含細胞株）[153]。

也就是說,儲存於人體生物資料庫內之資料,於輸出前應經衛生福利不許可方可進行,這是一種針對特定資料類別所為的資料跨境傳輸限制。但對於衛福部應如何審查，該條例並未明文規範。

衛生福利部於今年（2017 年）9 月 12 日依據人體生物資料庫管理條例第 15 條第 2 項、人體生物資料庫設置許可管理辦法第 9 條之規定，公告「人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準」[154]（以下簡稱審查基準），明確規定了人體生物資料庫資料跨境傳輸的審查程序及基準。

就跨境傳輸的目的限制而言,根據審查基準,人體生物資料庫資料要進行國際傳輸(即跨境傳輸)，其目的須限於資料庫設置者進行「跨國生物醫學研究或學術發表」所需才可向衛福部提出申請[155]。

而審查基準亦對輸出地有所限制。根據查基準，輸出地原則上限於該審查基準所匡列的「十大醫藥先進國家」，即美國、英國、日本、瑞士、加拿大、法國、澳洲、德國、比利時及瑞典等國[156]。

而對於輸出資料之種類及性質，則將其分為高風險、中風險及低風險三個等級，分別設有不同的審查程序；其中，屬於高風險等級的資料有：全基因體定序之序列資料、經全基因體定序所得之全基因體基因型定型資料、經微晶片陣列所得之全基因體基因型定型資料及親子鑑定或身份鑑定相關之基因定型圖譜資料等類別;屬於中風險的有部份基因體定

[153] 行政院衛生署衛署醫字第 0990069637 號，民國 99 年 5 月 28 日。

[154] 衛生福利部衛部醫字第 1061665812 號，民國 106 年 9 月 12 日。

[155] 人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準第 2 點。

[156] 人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準第 4 點。

序之序列資料或基因型定型資料、轉譯體定序之序列資料及外顯子全基因體定序之序列資料；至於原始參與者的相關臨床或流行病學資訊、原始參與者的相關統計資訊、蛋白質體實驗資料、代謝體實驗資料、基因表現微陣列晶片、染色體組型實驗、經統計後的全基因體定序資料、經統計後之全基因體定型資料以及經統計後之轉譯體分析資料等則屬於低風險[157]。

在實質審查的內容上，衛福部除審查其格式之正確、內容之完整及妥適性外，亦將下列四項與個人資料保護有關之事項列入審查的範圍：接受傳輸或輸出機構之性質及研究能力、接受傳輸或輸出機構對於參與者權益之保護、資料國際傳輸或生物檢體衍生物輸出後續處理方式之妥適性，以及是否訂有契約書或承諾書[158]。

至於審查程序，審查基準則將其分為行政審查及專業審查兩個部份，由申請人檢具申請書、計畫書及自評表後，先由衛生福利部進行行政審查，審查其資料是否完備，是否需要補正[159]。通過行政審查後，依照其所涉資料及衍生物的風險程度及輸出地的不同定有不同的專業審查程序：

（一） 其資料或衍生物風險程度屬於高風險或其輸出地非屬「十大醫藥先進國家」者，應經人體生物資料庫審查小組會議審議；

（二） 資料或衍生物風險屬於中風險極低風險，且其輸出地為「十大醫藥先進國家」者，由人體生物資料庫審查小組二位專家委員進行書面審查，若兩位專家意見一致，則將結果提報人體生物資料庫審查小組會議備查，若意見不一致，提交人體生物資料庫審查小組會議審議[160]。

---

[157] 人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準第 4 點及附件 2。

[158] 人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準第 3 點。

[159] 人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準第 5 點。

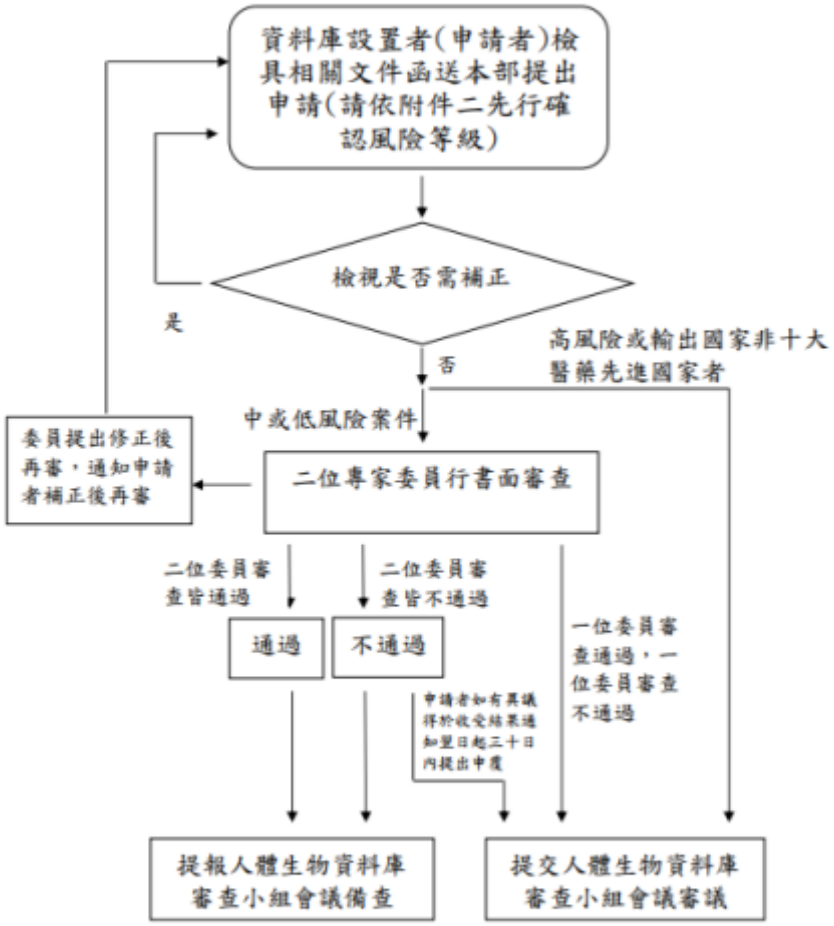
[160] 人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準第 5 點。

關於詳細的審查流程，請參考下圖。

附件三

人體生物資料庫

資料國際傳輸或生物檢體衍生物輸出審查作業流程圖



備註：

一、中或低風險案件由二位專家委員行書面審查，高風險或輸出國家非十大醫藥先進國家者，提交人體生物資料庫審查小組會議審議。

二、審查通過之資料國際傳輸或生物檢體衍生物輸出案，由原提出申請之人體生物資料庫進行案件追蹤管理，本部將依法對人體生物資料庫定期查核。

資料來源：人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準附件三

圖 4-1：人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查作業流程圖

三、 金融機構相關資料之規定

金融機構由於其所處理之資料相當敏感，為受到高度監理之行業，為確保資料之安全，金融監督管理委員會針對金融機構作業委託他人處理時的相關規定，依據銀行法及合作社法的授權定有「金融機構作業委託他人處理內部作業制度及程序辦法」[161]。

金融機構作業委託他人處理內部作業制度及程序辦法中對於金融機構將其作業委託至境外處理亦有相關規定。其中，金融監督管理委員會曾經於 2012 年 2 月時禁止國內銀行將消費金融業務相關資訊系統之資料登錄、處理、輸出等事項委託至境外辦理，但此一政策後來因我國積極參與國際區域整合的關係，於 2014 年 5 月時取消禁止規定，改為與其他委外事務相同的許可制[162]。

根據目前的金融機構作業委託他人處理內部作業制度及程序辦法規定，金融機構如擬將其作業項目（包含：資料處理、表單、憑證等資料保存之作業、代客開票作業、電子通路客戶服務業務等等[163]）委託至境外處理，應經主管機關的准許[164]。所謂的金融機構，包含外國銀行在台分行在內[165]，但金融機構將其國外分支機構之作業項目委外辦理或委託境外機構辦理位於境內資訊系統之開發及維護則不在此限[166]。

金融機構在申請主管機關核准時，應檢附下列文件：

（一） 受委託機構所在地金融主管機關書面確認文件（其內容應包含：該主管機關知悉並同意受委託機構執行受託事項、該主管機關同意我國主管機關得要求受委託機構提供受託事項相關資料、該主管機關允許我國主管機關及委託之金融機構得對受託事項進行必要之查核、該主管機關如有必要對受託事項進行查核，應事先通

---

[161] 金融機構作業委託他人處理內部作業制度及程序辦法第 1 條。

[162] 彭禎伶，〈外銀資訊委外禁令 重新打開〉，工商時報，2014/05/07，可參見 http://www.chinatimes.com/newspapers/20140507000135-260205 （最後瀏覽日：2017/10/19）。

[163] 金融機構作業委託他人處理內部作業制度及程序辦法第 3 條。

[164] 金融機構作業委託他人處理內部作業制度及程序辦法第 18 條第 1 項。

[165] 金融機構作業委託他人處理內部作業制度及程序辦法第 18 條第 3 項。

[166] 金融機構作業委託他人處理內部作業制度及程序辦法第 20 條。

知我國主管機關以及該主管機關同意不會取得我國客戶資訊，如為執行其監理職權而須取得時，應事先通知我國主管機關等事項）；

（二） 委外內部作業規範；

（三） 董（理）事會決議之議事錄（外國銀行在台分行得由總行授權人員出具同意書代替）；委外對營運之必要性及適法性分析（應包含對受委託機構遵守我國客戶資料保護相關規定之評估）；客戶資訊保護措施及是否已取得客戶同意[167]。

其中，外國銀行在台分行除了前述資料外，亦應取得總行或經總行授權之區域總部出具有關資料取用、安全控管及配合我國監理要求之承諾書[168]。而如果金融機構取得受委託機構所在地金融主管機關書面確認文件，則可以以下列資料代替：

（一） 受委託機構出具之同意函（其同意內容應包含：必要時得由金融機構指定之人，對受託事項進行查核，且指定之人得由主管機關指派）；

（二） 對受委託機構之內部控制制度及相關作業程序之審查情形；

（三） 受委託機構所在地對客戶資訊之保護不低於我國之法律意見書；

（四） 受委託機構最近期之經會計師查核簽證之財務報告；

（五） 受委託機構出具近三年內未發生造成客戶權益受損或影響機構健全營運之人員舞弊、資通安全及其他事件之聲明書[169]。

而如果該金融機構所欲委外之資料是屬於消費金融業務相關資訊系統之資料登錄、處

[167] 金融機構作業委託他人處理內部作業制度及程序辦法第 18 條第 1 項。

[168] 金融機構作業委託他人處理內部作業制度及程序辦法第 18 條第 1 項第 6 款。

[169] 金融機構作業委託他人處理內部作業制度及程序辦法第 18 條第 2 項。

理、輸出等事項的話，除了前述的所有資料外，金融機構尚應符合主管機關所定之條件[170]，並須提供下列資料：

（一） 海外資訊系統不低於我國資訊安全標準之查核報告（應委託具資訊專業之獨立第三人出具）；

（二） 針對海外資訊系統發生無法提供服務情事，建立營運備援計畫（由具資訊專業之獨立第三人出具評估報告，證明其可以符合主管機關的相關需求）；

（三） 日常監督機制之計畫書（包含設立專責監督管理單位，其參與人員應包含法律遵循、內部稽核、作業風險管理及資訊管理監督人員，以及日常委外作業機制）；

（四） 董事會通過之成本效益與集團內費用分攤合理性之評估報告[171]。

金融機構將其資料之處理委託至境外處理，除須經前述之申請程序外，主管機關亦要求金融機構應充分了解及掌握受委託機構對客戶資訊之使用、處理及控管情形[172]。且其提供之客戶資訊應僅限於受委託事項直接相關之必要資訊[173]。並要求受委託機構確實遵守主管機關所定之規範，同時應對其使用、處理及控管情形進行定期及不定期之查核與監督[174]。

而如果其所委託的是消費金融業務相關資訊系統之資料登錄、處理、輸出等事項的話，尚應確保受委託機構之使用、處理及控管符合我國個資法之規定，並留存完整稽核紀錄(且列為重點查核項目)[175]。同時，本國銀行應定期評估成本效益及集團內費用分攤之合理性，

---

[170] 金融機構作業委託他人處理內部作業制度及程序辦法第 18 條第 6 項。

[171] 金融機構作業委託他人處理內部作業制度及程序辦法第 18 條第 5 項。

[172] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 1 項第 1 款。

[173] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 1 項第 2 款。

[174] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 1 項第 3 款、第 4 款。

[175] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 2 項第 1 款。

報請董事會通過[176]。對其資訊系統安全性檢測應不低於主管機關或中華民國銀行商業同業公會全國聯合會之規範[177]。本國銀行每年應至少辦理一次一般性查核及一次專案查核[178]；且每年年度結束前應交當年度查核報告提報董事會並函報金管會[179]。而如果發生服務中斷情形，應盡快通知相關機構，且每年中斷長度有所限制[180]。

綜合上述可以發現，我國對於金融機構將資料處理委託境外處理的管理，係採取許可制之方式，其審查內容著重在主管機關對於委外作業查核權限之確保、個人資料安全及當事人同意權的確保、資訊安全的維持以及銀行本身成本效益之確認等，並針對不同類型之資料定有不同之要求。

四、 通訊傳播領域資料之規定

通訊傳播資料往往具有高度敏感性，因此國家通訊傳播委員會於 2012 年 9 月 25 日曾依據電腦處理個人資料保護法第 24 條第 3 款的授權，發布通傳通訊字第 10141050780 號命令，「限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區」。根據該命令，做出此一限制的主要考量係中國大陸地區對個資保護的法令建制較不完整，未保護個人資料，限制通訊傳播事業將個人資料傳遞至大陸地區[181]。這是我國目前有效唯一一個完全禁止將個人資料傳遞至特定區域的管理規定。

五、 小結

---

[176] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 2 項第 2 款。

[177] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 2 項第 3 款。

[178] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 2 項第 4 款。

[179] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 2 項第 5 款。

[180] 金融機構作業委託他人處理內部作業制度及程序辦法第 19 條第 2 項第 6 款、第 7 款。

[181] 〈限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區〉，國家通訊傳播委員會網站，http://www.ncc.gov.tw/chinese/print.aspx?table_name=news&site_content_sn=538&sn_f=26302 （最後瀏覽日：2017/10/19）。

我國資料在地化措施係採取「特定部門措施」的方式管制，也就是針對資料之類別，採取不同之在地化要求。而我國資料在地化之規定主要係集中於個人資料之保護上，因此本研究將集中於個人資料之相關規範上。

我國資料之跨境傳輸資料之限制目前主要出現在生物資料庫、金融業務及通訊傳播事業有關資料等三方面。其中，通訊傳播事業有關資料部份，我國採取禁止其傳輸至特定區域的方法。而其他兩類資料，則不分傳遞區域，皆要求欲傳遞資料者應先向主管機關取得許可。究其原因，無論那一類別的資料，之所以做出這類限制的原因，主要都是為維護個人資料之保護，可見保護個人資料之周全乃是目前政府思考是否限制資料跨境傳輸時的一個重要理由。

當前各國對於資料在地化措施或跨境流通限制之程度與作法各有不同，但常見的主要原因為個人資料之保護，尤其是特定類別個人資料之保護，係為確保個人資料不會因為跨境資料傳輸而無法得到保護。這種作法與我國目前之資料在地化措施之著眼基礎相類。而各國多以當事人同意、目的地個資保護程度等作為許可資料跨境傳輸之條件，則值得我國政府機關在研擬資料在地化措施時參考。

第五章　法制政策建議

為了促進通訊傳播資料應用，單由從主管機關透過政策推動是不夠的。除了法規調適、鬆綁之外，如何完善資料生態圈、促進良性互動與循環，本研究案提出下列建議供主管機關參考。

（一）　釐清個人資料定義，透過法院判決之累積來解決個資相關爭議問題

我國個人資料保護法在民國 99 年 5 月 26 日修正完成並且公布，於 101 年施行後至今也已五年。然而其中還是有許多規範讓業者不明瞭，例如說個人資料的定義，是否所有與個人有關之資訊皆屬值得保護之個資等出現疑義，而導致業者對於資料應用卻步。像是中華電信因為利用客戶個資催費被訴，或是之前 M+Messenger 的案子，都是這種情況的具體表現。

特別是「M+Messenger」事件。電信業者為提供號碼可攜服務（number portability service, NP），此共同建立「號碼可攜集中式資料庫管理中心」（Centralized Number Portability Database, CNPDB）並以此資料庫管理號碼可攜服務，其中台灣大哥大一家提供一項行動 app 名為「M+ Messenger」，其允許使用者得以知悉其手機通訊錄中之電話號碼所屬之行動電話業者別，藉以確認通訊錄中的朋友是否屬網內。然而，這項服務被認為違法蒐集個資而被請求損害賠償。事件經臺灣臺北地方法院審理，判決應給付新臺幣五百元（臺灣臺北地方法院 103 年度北小字第 1360 號），業者不服上訴仍然敗訴確定（臺灣臺北地方法院 103 年度小上字第 155 號）。理由就是認為電話號碼是一種個人資料，而「電話號碼所屬之電信業者別，乃個人電話號碼之附屬資料」，可以間接識別特定個人，而屬於個人資料。

這樣的判決結果當然對業者的資料應用產生阻礙，然而 NCC 在第 754 次委員會議認定：「台灣大哥大股份有限公司經由應用軟體提供其用戶檢視通訊錄中聯絡電話號碼之所屬電信業者，或變更檢視結果為「網內/網外」，均不足以直接或間接識別該等電話號碼之個

人身分，無個人資料保護法第 1 條所揭人格權受侵害之事實，自非同法所欲保護之標的及適用，爰不予裁罰。」是以在主管機關明確表示此等資料不屬於個人資料，業者就能放心針對資料進行應用。

我國沒有專責的隱私保護機關，仍有法務部擔當個資法法律解釋主管機關，同時各個目的事業主管機關為個資主管機關。因此雖然許多關於個資法的疑義需要由法務部解釋，但各主管機關由於有執行的權能，其解釋也有相同效力。因此當發現關於通訊傳播資料有個資疑義時，NCC 可以比照 M+Messenger 案提出解釋，讓業者有所遵循，降低其因為應用資料帶來的風險。

（二） 提供更精確的個資去識別化標準及禁止資料還原

我國個資法第 9 條、第 16 條、第 19 條及第 20 條皆有所謂「資料經過提供者處理後或依其揭露方式無從識別特定當事人」，係指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人（個資法施行細則第 17 條參照），此外，法務部法律字第 10303513040 號函也表示「個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍」。因此對許多業者來說，往往認為個資經過去識別化就能避免個資法規制而高枕無憂。

然而雖然有匿名化(anonymization)、加密(encryption)與轉換代碼(key-coding)等方法來讓資料避免連結到特定個人，要做到什麼程度卻是個問題。雖然現階段則採用經濟部標準檢驗局用我國與國際標準（ISO）調和之國家標準（CNS）之「資訊技術—安全技術—隱私權框架」國家標準 CNS29100，以及「資訊技術—安全技術—部分匿名及部分去除連結鑑別之要求事項」國家標準 CNS29191 作為現階段推動個人資料去識別化驗證標準，然而這個標準沒有強制力，同時這個作業流程標準其實對業者來說難以操作，而且過度去識別化也影響資料的用益價值。

NCC 作為主管機關可參考國外個資與隱私保護主管機關頒布「實務指引」或「準則」的方式，主動就去識別化的議題提出標準。目前委託財團法人電信技術中心就去識別化標

準的訂定進行研究，就是個很好的方向。由於目前研究內容尚未明朗，故不妨效法日本個人資料保護委員會的去識別化指導方針(個人情報の保護に関する法律についてのガイドライン（匿名加工情報編））[182]明確去識別化範例(包括移動資訊等)、列舉識別因子、提出關於個人識別與再識別的風險、提示去識別化的方法(特異值消除、匿名化等)等。

其中關於再識別的風險，由於去識別化資料隨時可能因被再識別而落入個資法的適用範圍，因此在鑑別去識別化的有效性上，應該是對去識別化進行風險評估。首應考慮去識別化資料之使用目的，或資料接收者有無利用個資之動機。由於企業對匿名資料的二次利用通常不同於資料初始之處理目的，因此從目的角度切入去識別化是否充分以及是否合乎「善意不知情」，可成為較為有效的判斷方式[183]。除此之外，參考日本個資法新修之規定，將禁止重行識別的規範納入未來個資修法的討論議題，也是可行之方式。

（三） 設立或協助第三方單位設立資料平台，以確保資料之利用具有品質效益

產業是否願意釋出自己所保有的資料進行應用全仰賴其意願，釋出資料所帶來的收益、法律或合規風險、執行的複雜程度等等因素都足以影響其意願。因此要促成這些產業釋出手上資料，必須要降低風險以及確保收益，而最有效達成的方式就是透過資料平台來協助業者釋出資料。

以前述介紹的日本軟體銀行資料平台為例，該資料平台除了提供資料存放外，更有資料分析、應用服務，以及法律、授權等文件的提供，資訊安全的控管等，能讓業者能在低風險環境下安心釋出資料。同時藉著平台能得到與其他同種、或是異種資料結合的機會，創造資料用益新價值。

作為主管機關的 NCC，可以選擇自行建構，類似美國 FCC 的開放資料平台，或是與業者合作，建構類似像日本軟體銀行的資料平台，由建構便利資料釋出的環境來提升產業資

[182] 個人情報保護委員会，個人情報の保護に関する法律についてのガイドライン（匿名加工情報編），https://www.ppc.go.jp/files/pdf/guidelines04.pdf（最後瀏覽日：2017/10/19)。

[183]葉志良，大數據應用下個人資料定義的檢討：以我國法院判決為例（最後瀏覽日：2017/10/19)。

料應用。

（四） 對於業者有跨境資料傳輸需求者，提供適當的法遵協助

面對各國資料在地化的趨勢，往往使得資料的跨境使用變得困難重重，甚至一不小心就會受到損害。為了避免這樣的狀況發生，短程仍建議 NCC 給予業者相關資訊，避免其因不知道規定而遭到損害。例如：提供關於歐盟或是中國大陸相關法規的資訊。

同時也提供協助民間業者在進行資料傳輸能夠符合傳輸國的法律規範。例如：協助業者符合 GDPR 認為有採取適當保護措施的要件。像是提供歐盟標準契約條款(SCC)，讓業者在進行資料處理時事先將這個條款置入契約內。或是協助業者建立企業自我約束規則(BCR)，並且向歐盟資料保護機關提出申請等。此外，若歐盟有提出關於 GDPR 的具體行動規範（Code of Conduct)，也可以提供業者尋找具有資格的認證機構請求認證。

由於我國並不被認可為資料保護充足的國家，因此要讓歐盟的個人資料能自由傳輸進我國境內，除了個別企業完成個資保護措施外，透過國際組織或協定讓歐盟許可個人資料跨境傳輸至我國才為長久之道。例如透過參加類似 APEC 體系的跨境隱私保護規則(CBPR)等方式，藉著調整隱私個資保護規範，透過與區域隱私權規範統合之方式，嘗試與歐盟甚至國際接軌以幫助業者順利接收來自國外的資料。

此一保護規則係 APEC 透過資料隱私開路者合作計畫（APEC Data Privacy Pathfinder Projects)，希望能達成：(1) 促成對於個人資料的適當隱私保護，避免惡意的入侵與對個人資料的濫用；(2) 使 APEC 各經濟體內的國際性組織能夠發展並致力於一個共通的個資保護制度；(3) 協助執法機關履行其保護隱私之職責；(4) 推動一個國際機制以促進與加強隱私的保護，同時保持資訊流動的持續性。其透過一連串的制度設計，提供企業經營者得以建立其內部之跨境資料傳輸規則，並且透過認證機構（Accountability Agents, AA）之建立，使企業得以提供消費者可信賴之標章[184]。

[184]法務部，法務部 99 年度公務機關個人資料保護方案計畫研究成果報告書，2012 年，頁 377。

CBPR 主要係基於 APEC「隱私保護綱領」及各經濟體之國內法所編寫，各組織可依其本身之情形彈性制定其內部之跨境個資隱私規則。CBPR 並不取代會員國之國內法。如果國內法之要求高於 CBPR 體系時，則企業所定之跨境隱私規則仍須遵循國內法之要求，但若該會員經濟體並無個人資料保護之國內法時，則 CBPR 則為最低之保護標準。基本上，CBPR 體系僅供於 APEC 會員國向其他 APEC 會員經濟體跨境蒐集或接受個人資料時使用。CBPR 要求組織發展其跨國隱私保護之企業內部規則，該規則必須透過公正的認證機構認證其符合 CBPR 之最低要求後，始可跨國傳輸個人資料。一旦企業內部所制定之跨境傳輸規則被認證後，將會約束企業本身，同時，該會員經濟體國內之管理者，例如隱私主管機關，也將要求企業執行該項隱私政策。藉由 CBPR 體系將有效鼓勵 CBPR 成員在此基礎下達成雙邊或多邊協議，從而對締約國產生約束力。

APEC 經濟體如欲加入 CBPR 體系，必須要有一個至少一個以上的隱私執法機關參與 CBPR，並由提報機關列名於「跨境隱私合作執行文件」(Cross-Border Privacy Enforcement Arrangement, CPEA)。在交付意向書（letter of intent）及聲明符合 CBPR 體系相關要求，並提供相關佐證後；由共同監督小組（JOP）進行申請案的審查，並出具審查報告，說明經濟體是否符合相關要求，若符合則於出具日正式加入 CBPR 體系。JOP 由三個 APEC 會員經濟體所組成，目前由美國、日本及澳洲的代表擔任。

我國要加入 CBPR 體系，除了具有 AEPC 經濟體會員資格外，同時需具有至少一個以上的隱私執法機關列名參與 CPEA。在 21 個 AEPC 經濟體會員中，僅有 16 個經濟體會員具有隱私保護的法律；而也僅有 14 個經濟體會員具有隱私保護之執行機關。由於有些國家係採取多重的個人資料保護主管機關之設計（如韓國及越南）。由於我國沒有專責的隱私保護執行機關，故現在參考韓國及越南模式，成立了由 15 個部會組成的專案小組，未來加入 CBPR 體系時，與 15 個部會將作為隱私執法機關，並由經濟部擔任專案小組的協調單位。相關程序正在進行中[185]。

[185]經濟部，APEC 跨境隱私保護規則體系能力建構國際研討會 10 月 2 日在臺北揭開序幕(2017 年 10 月 2

（五） 從資料經濟與國際貿易的層面切入，來思考資料在地化政策議題

在本次業者座談會中，多數業者反應認為自己受到個資隱私規範限制，不能任意使用個人資料。然而外國業者卻不受個資法的限制，導制雙方在資料應用上出現不公平的狀況。事實上，業者的意見並非完全正確，外國業者如果在我國境內進行個資的蒐集、處理、利用，一樣要受到個資法的規範。而就算在境外，也有個資法第 21 條國際傳輸來規範。但也不可否認，外國業者受到的管制確實比本國業者為少，個資法第 21 條在沒有主管機關明令禁止傳輸下，原則上仍為許可，而外國業者違法個資法時的執行也有相當疑問。更重要的是，外國業者挾著雄厚的資源，提供給本國人便捷的服務而得以輕易換取同意，故往往能通過個資法的檢視。因此，除了考慮對本國業者進行個資法規制鬆綁外，資料在地化政策就成為值得討論的議題。

資料在地化政策要施行並非難事，我國個資法第 21 條：「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。」亦即法律已經賦予主管機關限制的權利，而無需更複雜的修法工作，問題層次就變成是否要限制個資跨境傳輸。

事實上，世界各國確實常見以個人資料之保護為理由限制跨境傳輸，與我國目前之資料在地化措施之著眼基礎相類，目的地個資保護程度等作為許可資料跨境傳輸之條件是可行的。

但相對之下，以國家安全、反恐等理由，強制、大範圍的要求採取資料在地化措施並不多見，此類作法因為強烈限制了資料擁有者將資料跨境傳輸之可能，反而有可能遭到報

日），

https://www.moea.gov.tw/MNS/populace/news/News.aspx?kind=1&menu_id=40&news_id=72834，最後瀏覽日 2017 年 11 月 8 日。

復，對以國際貿易導向為主的我國經濟型態恐有不利影響。 此時反而可以反向思考，像是因為中國大陸的網路安全法通過，要求資料在地化的同時，香港和新加坡就藉著這個機會吸納不想把資料放在中國大陸境內的外商，如果同樣的思維放在我國，沒有強烈的在地化政策要求也能夠吸納外商的資料，甚至可作為外商的資料中心，一方面是繁榮我國的資通訊產業；另一方面如果我國有這麼多 Data center 的話，世界各國會想盡辦法保護我國的資訊安全。也就是說與努力說資料要在地化，所有的資料都放我國、不能放國外，倒不如用另外一種比較開放的方法能可以更增加價值跟資訊安全。

（六） 監理沙盒制度適用於通訊傳播資料加值應用的可行性低

英國開始，澳洲及新加坡等多國都相繼推出金融業的監理沙盒政策，企以更具彈性的方式來面對法規高度管制的金融產業，盼能減少創新技術應用的限制，帶動金融領域的另一波成長與翻轉。觀諸國際，如日本或新加坡，都已注意到並不是只有金融業有法規侷限新興科技應用的問題，在其他產業也有類似情況。使得監理沙盒的討論，從金融領域轉移到了非金融領域，不少人已在呼籲，非金融產業也需要監理沙盒機制，以用來測試新興產業發展。通訊傳播產業業者也常認為應當在通訊傳播資料應用領域導入監理沙盒，以監理沙盒的機制，政府給他們一個空間，讓他能排除個資法的適用，以安心運用所蒐集資料，但能否如此運用其實有待探討。

其實監理沙盒制度它不是一個監理的真空，也不是一個法規除外的空間，而是為了讓欠缺資源，難以達成特許要求而又想要投入特定領域的業者，透過一個很短暫的時間，給予一個暫時性、限制性，類似準特許的地位，給業者時間來發展取得資格。所以監理沙盒的主要功能，反而是透過那個實驗的期間，去強化這些業者機關的監理能力跟強化這些業者進行法律遵循能力。同時，監理沙盒制度還有一個很重要的設計，它希望在實驗的過程當中，讓這個實驗的業者跟主管機關在合作之下還是能夠做好三件事：第一件事情叫做消費者保護；第二件事情叫做風險管理；第三件事情，他必須發生爭議的時候，有一個爭議的解決途徑。

由上述監理沙盒的本質來看，因為每個業者要作的業務並不相同，因此要進入這個實驗場域往往需要建築在個案判斷的基礎上，這就與業者所期盼的功能有相當大的差距。此外，如果鬆綁個資規範，那麼監理沙盒制度在風險保障管理的那一環是否通過得了？新加坡的監理沙盒制度就很明確表示個資法的法律規範是不能夠被放寬的。同理在臺灣，如果要去做個資法的排除，或者是個人隱私保障密度的降低，會牽涉到基本權、憲法的問題，當個資法的規範就是確保當事人的資訊自主控制性時，監理沙盒就無法在這個地方進行讓步。

附錄

附錄一　通訊傳播產業資料加值與創新應用座談會及政策建議

第一場通訊傳播產業資料加值與創新應用業者座談會

（一）　參加名單：

1. 台灣電信發展協會 劉莉秋副祕書長
2. 台灣有限寬頻產業協會 彭淑芬理事長
3. 中華電信股份有限公司 闕仁斌科長
4. 中華電信股份有限公司 邱祥霖管理師
5. 台灣大哥大股份有限公司 張贏太經理
6. 台灣大哥大股份有限公司 曾志強副理
7. 聯禾有線電視(台灣大寬頻) 戴漢林專案副理
8. 遠傳電信股份有限公司 蕭景騰協理
9. 凱擘股份有限公司 鄭迪資深管理師
10. 資策會科法所 宋佩珊組長
11. 資策會科法所 吳柏凭研究員

（二）　討論議題：

1. 關於資料應用的現況。目前擁有的資料(包含但不限於個資)種類？、蒐集方式，以及可投入應用的方式？
2. 關於資料應用的困難對於無法應用手上有價值的資料的情形，評估認為主要的原因是什麼？
3. 目前業界是否有可用的資料共享應用平台？類似號碼可攜的資料分享模式是否可以投入應用？
4. 關於去識別化議題，現行的標準 CNS 29100 及 CNS 29191 是否提供可行的操作模式？又如日本由主管機關提供指引規範的模式是否比較容易操作？

5. 關於資料應用的解決方式，關於資料應用法規的具體調整建議方向。

（三） 時間：中華民國 106 年 10 月 27 日（星期五）下午 2 時

（四） 地點：台灣金融研訓 6 樓小會議室

（五） 發言內容：

業者代表	發言內容摘要
劉莉秋副祕書長	1. 關於物聯網，政府有個很有趣的邏輯，到現在還在把物聯網停留在賣設備的邏輯上面。這是非常可怕的，物聯網它代表的是龐大的資訊，當發展設備商的角度來看待物聯網的發展。結果就是，設備商會嘗試自己去做物聯網的資料收集者，但因為資料蒐集不易，最後還是會聯結 facebook、google、line 這些東西，讓更細微更精緻的資料往境外流。如果政府在政策上面沒有要鼓勵設備商跟電信業者的合作，未來的物聯網的發展也會出現類似同樣的問題。 2. Internet 在資料蒐集是全無國境的，境外的業者不需要但我們在座的所有業者都必須要符合要配合個資法的要求。facebook 跟 google 他們最近大肆的在做什麼事？其實

	也是我們所擔憂的，他們今天做到開放，他們 open id，open api，今天我們所有的消費也看在 line pay 也看在 facebook 的身分認證，也看在 google 的身分認證的眼裡。相對之下，我們的業者因為個資法規範被弄到寸步難行。今天創新應用如果臺灣業者要面對的是一個不需要綁手綁腳的敵人，那麼要我做創新應用的時候就必須要給我相對的自由的空間。如果今天創新應用真的造成困擾了，到時再來回收相對的權利都還來的及。 3. 希望把我們納入創新條例產創條例創新條例裡面的監理沙盒，放寬所有法規的限制在一個大的原則之下不再受這些限制，去做創新應用，我們才有那個一點點的機會去對抗我說的 facebook、google 跟 line 這些這麼大型的敵人，才能讓流到境外的資料再流回境內。 4. 現在的主管機關往往表示歡迎去做，但被告了就處罰你或者撤你。問題是我們沒有答案，去連結、去

	識別化等等，只要告訴我可以做的範圍在哪裡，說這個我能做我就去做，你說這個我不能做那我就不要做。這個也是一個很明確的方式。在未來政策規管上，希望能提供一個明確標準，不然就放手讓我們做。
彭淑芬理事長	1. 我們傳播行業的資料應用以所謂的智慧家庭為核心，可以發展的都是我們的未來希望發展的目標包括居家照顧、遠距醫療啊。還有那個保全等，保全就是我們基礎設施業者最能夠發揮的功能，用一個可以用很寬的頻寬然後看我們家裡的保全狀況，此外，像能源應用，節能的部分都可以跟電力來做結合。蒐集收視紀錄讓我能更精準掌握收視者的喜好也是很重要的應用方式。 2. 但是這些海闊天空服務，都牽涉到法律問題，沒有一樣例外，都被法規的嚴格限制而沒有辦法再發展。NCC 雖然很樂見發展，也一再問我們將來傳播全面數位化後能提供怎麼樣的創新應用服務。然後一方面又用法規把我們越綁越緊。比方說我們的定型化契約更加的嚴格，未來的新版的資料草案更加綁手綁腳。 3. 新版的有廣法相關法令也把我們的

	創新應用本來還有的模糊地帶鎖死。本來我們只要是屬於加值服務，加值服務以前的確是不管的，只要是加值的都不在基本服務裡面。現在卻又加了一條說必須依照其他相關法令去取得執照跟締造消費者同意，結果不但變得更加嚴格的，而且讓我們連怎麼去取得執照都不知道。 4. 截至今天我們仍沒有辦法用所謂的收視紀錄，就是我們機上盒所蒐集的所謂視聽消費收視戶行為的分析。首先收視紀錄是否為個資就吵不完，然後雖然有所謂的去識別化規範，但行政上並沒有落實，更沒有人能認可我去處理後產出的資料就符合去識別化定義。 5. 財團法人資訊技術中心他現在一個研究案就在訂所謂去識別化 sop，但就我的所知是否能成為可遵循的標準還是未知。
闕仁斌科長	1. 現在可以用的資料還是屬於政府機構的公開資料。像說經濟部的一些相關資料，NCC 有一些相關的 open data，大部分都是拿來做監聽用的，倒沒有到跟其他資料有交換。大致上所有的合作案因為法令限制大概都半途而廢，所以說沒有利用什麼大數據可以創造產值，頂多就是讓自己公

	司裡面一些行銷的提升，或者是基礎建設。 2. 現在最常做的資料應用還是屬於人潮分析，畢竟已經去識別化。那人潮分析是你就可以看看哪個地區的人潮分布嘛。可能在業者展店的時候也可以做個參考，什麼時段這人潮比較多什麼時段人潮比較少。 3. 共享應用平台倒是可行的方式。許多數位內容公司都有來找我們，表示說原來國內產業廣告已經被外商掠奪大半塊，只有電信公司還有這個資料量和外商一搏。而且，我覺得可以透過跨產業的討論會比較務實，透過討論就可以決定哪些資料能弄到分享平台去。
邱祥霖管理師	1. 目前垃圾郵件黑名單的資訊共享平台運作業是滿成功的，那不只有我國啦，應該說就電信業者資料互享平台這部分應該在防弊這一塊是可以切入的主題，比如說內政部警政署跟 whos call 做防詐騙的電話號碼這樣從維護消費者權益那防止詐騙這部分來著手是一個比較好的方向。
張贏太經理	1. 電信業者做的資料應用其實就是兩個方面，一個就是我們自己的用戶的服務，比如說我們按照他的消費行為去建議他你用什麼資費方案最好或

	者我要想辦法知道你會不會退出或其他的行銷，內部使用或者像台哥大我們有做一些音樂服務，根據你喜歡的音樂我們再去做推薦，我們需要很小心地在內部使用。而另一個外部的商業行為，如果不清楚那些事情事可以做，我們基本上是會很小心不碰觸的。 2. 目前資料共享的例子在電信業的典範真的是非常非常少。先不說更深層次的應用我們希望推動共同聯徵的機制這對我們就很重要，光是不要講更深層次的應用，因為每個電信業者幾乎都有自己的黑名單不管業務使用上的或是用小額支付上，那這些東西是沒有共享，不像金融機構可以有個聯徵中心，
曾志強副理	1. 對於資料應用的最大阻礙，除了法規以外，我更覺得是規管模式。現在的規管模式一直要求我們要消除分子，也就是說不能讓主管機關看到有任何檢舉客訴。我們常收到客訴件，任何資料我們都要花一大堆的人去處理客訴，而且客訴要在七天內完成。結果光處理客訴都已經筋疲力竭，哪有餘力再做資料應用？像之前中華電信因為客戶欠費 23 元，打電話去催費結果被告。判決雖然是客戶

	敗訴，但理由只是認為 23 元的損害對個人權益影響甚微，而非指利用客戶資料催費這件事是允許的，這讓我們對資料應用更加戒慎。因此，如果主管機關不能協助我們建立一個停損點，也就是只要風險在一定程度以下就可以容許做的話，產業資料應用還是推不起來。 2. 目前去識別化有幾個做法，那其實有應該有已經想了滿多，比方說有階段性的或是說有 Data laundering 這種資料庫把它洗過之後，或者是說建立一個新法讓他能夠排除適用或是加密、去連結性的等等。
蕭景騰協理	1. 從 DIGI+我們其實可以看到，2019 年 NCC 其實是有任務的，就是要訂一個在通傳市場大數據應用的去識別化要訂一個技術規範。在 2019 年要訂出來，所以這時間點來看還有明年一年的時間嘛，所以緊鑼密鼓去看我們要怎麼樣去識別化，這個技術規範他的標準在那裡現在正在訂， 2. 關於資料應用真的很困難，因為從頭到尾我們一直在被問說到底什麼樣叫做可以使用的資料。我們手機上跨機台收集到的資訊可能是全國最密的，連國安單位都想要跟我們要，但相對於 google、line，消費者甚少

	在意在使用這些軟體時的隱私問題，我們電信業者卻時常被嚴格檢視，這對我們資料應用造成阻礙。 3. 關於我們電信資料的應用，很多的車聯網物聯網都會用到這些資料，那我們怎樣極力的去識別化。當我們撈取資料時，為了要讓這資料不能回去回推到特定當事人或個人，只要少於一定數量，舉例來講當這基地台只有五個人的時候就會被濾掉，因為可能有機會回去推到這個人。或是在這個區塊裡面有多少個點那些點，然後他的活動範圍活動路線、甚或他的發話時間長短這些我們可能都我都可以掌握的到時，我們就必須把這個數量大到一個程度之後去把他模糊。這時候比較不會有隱私不會有個資的問題風險。 4. 我們電信業很需要這種資料交換的共同防堵機制，特別是針對洗手機的行為。我們很希望能有像是像 NP 這種電信法裡有規定，必須去成立一個 NPAC 資料庫去交換運用，這樣大家就敢放手去做。
鄭迪資深管理師	1. 個制度規範的管制實在太嚴，就是國內的業者實在很難跟境外的業者在不對等的狀況下去競爭。 2. 現在全數位化本來可以做的可以做

	的訂戶收視行為資料回傳，可是在這上面是在主管單位的態度還有民眾、一般民眾他們個資保護意識抬頭等，我們在收集資料都必須要有非常嚴謹的程序。這兩年我們被主管機關要求我們的定型化契約，裡面包含很多關於訂戶同意說他的資料收集的範圍我們是逐漸地被要求去限縮，因為我們以前的寫法可能比較像電信業者所說可能各項客戶服務管理或是比較行銷學術研究等對象都會被寫在同意範圍內，但大家現在可能去看電信業者的個資蒐集裡面這些條文都被刪掉，只能限縮在有線電視經營的範圍內才能使用訂戶的資料，所以如果要再去蒐集收視戶的收視行為的話我們還要再進一步去取得收視戶的同意，結果就是造成重重阻礙。

第二場通訊傳播產業資料加值與創新應用專家座談會

（一） 參加名單：

1. 元智大學資訊傳播學系 葉志良助理教授

2. 理律法律事務所 曾更瑩合夥律師

3. 輔仁大學財法系 翁清坤助理教授

4. 政治大學法律系 臧正運助理教授

5. 開南大學法律系 楊秋敏助理教授

6. 達文西個資暨高科技法律事務所 葉奇鑫所長

7. 資策會科法所 宋佩珊組長

8. 資策會科法所 吳柏凭研究員

（二） 時間：中華民國 106 年 11 月 10 日（星期五）下午 2 時

（三） 地點：台灣金融研訓 6 樓小會議室

（四） 討論議題：

1. 我國的個資法對於通訊傳播產業資料應用上造成阻礙，應該要進行什麼樣的調整？

2. 對於個人資料去識別化規範具體建議。是否要置入個資法明文規範？或是由主管機關頒布作業標準？

3. 監理沙盒制度適用於通訊傳播產業的可能性？

4. 通訊傳播資料應用下，個人資料保護與資料利用價值間該如何取得平衡？。

（五） 發言內容

學者專家	發言內容摘要
葉志良老師	1. 在討論資料應用發生的阻礙，其實講的就是同一件事情，因為目前個資的保護強度比較大，所以才會導致國內有些產業想要利用個人資料，發現個資法限制太多，有這樣的問題。 2. 對於個人資料上面的定義，其實從個資法上面提了很多例示、樣態，可是它最終還是要歸結到是不是可以識別該個人，那只是例示，單純一個名字，可是如果沒有辦法對

	到這個人，它只是一般的資訊，也不能算是個人資料，除非這個東西可以對到，譬如剛剛說的身份證字號，剛好就在你面前，可以對到他，不然我拿到一個身份證字號、車牌號碼、電話號碼，也沒有任何的意義。 3. M＋的案子也是一樣，如果我的個人資料未經他人許可，被人家拿去用，這樣就受害了嗎？我個人資料被拿去用，還是有其他的方法，譬如要求他不要用或者刪除，其實個人有很多的工具可以避免以後的事情發生。M＋這個案子，如果原告認為不妥，他可以要求資料庫或者是業者刪除你這個資料，都可以這樣做，他卻不做，去告了 M＋的服務，其他人都不要用，因為我受害了，它到底保護了誰？ 4. 告知同意如果碰到大數據，這都是一個最原始、每次都要拿來談的問題，因為很多的資料我們在蒐集的當下，其實你也沒有告知當事人。這個事情其實要回歸到業者，業者

	要創造一個服務，要蒐集你的個資，好比現在歐盟的 GDPR 一樣，他還是要取得當事人同意，這個是最原始，不能省掉的，。至於你要怎麼取得？業者要想辦法，現在業者都在喊很多的資料都沒辦法用，包括有線電視，現在都有機上盒，所有的資料其實有線電視端都有，可是他們覺得資料蒐集之後都不能用，真的都不能用嗎？有沒有認真的去推，我提供什麼樣的誘因讓用戶能夠乖乖簽寫同意書？不用全部都同意，只要少數同意，他還是可以部分做一些他們要做的加值應用，業者只要給他一個方向出來，能夠讓當事人取得一個明確的同意，當然就可以用，自己要想辦法讓用戶有這個誘因去簽這個同意書。 5. 談談去識別，去識別其實也是資料處理的一種，當我資料蒐集來之後，做一個去識別，它是一個資料處理過程，去識別根據個資法規定，還是要符合原先蒐集當時特定

	的目的，所以我們還是要回歸到一個宗旨，當我們蒐集個人資料的時候，這個特定目的是不可以被抹滅，即便是後續的處理、後續的利用，還是要根據原先的目的，你只要偏離這個目的，就要看有沒有符合目的外的利用，如果沒有，你就是違法利用。 6. 再識別問題，這其實是一個很明顯目的外利用，有提到要不要學日本，針對目的外利用用一個什麼樣的方式來禁止？其實也不用，因為它本來就是一個目的外利用，就要看那個目的外利用是不是符合法規的目的外利用、合法目的外利用？如果不是，就不是合法的。 7. 作為主管機關 NCC，其實應該要給與一個很明確的意見，什麼樣的情況下業者確實是可以利用這樣的資料，不用多，至少在業者碰到的例子裡面，要提出你們的見解。好比 M＋這個案子提出一個很明確的見解，他們認為「業者別」這件事情不能算是個人資料，非常清楚明

	白。 8. 臺灣個資法一直被業界認為它是一個限制很多的法律，問題在於我們各目的事業主管機關都沒有勇於跳出來說什麼樣的服務有問題來問我，我說這樣 OK，下一個很清楚的解釋；如果本身有異議，把各機關找來，大家尋求一個共同的見解。 9. 新的歐盟的 GDPR，我有一個新的想法，當資料主體很多工具可以主張你的權利，這件事情我反而是比較重要的，不管我個人資料當初到底有沒有被同意拿去用？可是事後我發現這個資料你用的不是很好，或者我不再願意讓你繼續使用，這時候你應該讓資料處理有一個很清楚、很容易的方式得知，行使他的權利，看是要移除或者是用什麼方式來做，不管現在業者提供什麼樣的資料，應該是一個經常性的提醒當事人你有這樣的權利。 10. 監理沙盒對於科技業來講沒有必要，我覺得金融機構可能非常需

	要，它的金融規範複雜很多，可是NCC 在現行的制度下，有實驗區，業主想要提供一個新的服務，或者NCC 推動某一個服務想要知道成效，他其實有實驗區的做法，這個實驗區就是排除目前現行的廣電三法，都是排除適用，在你的實驗區裡面要怎麼去定價，可以提一個Proposal 計畫，核可你就做了，其實已經有他的做法存在，只是NCC 這個角度，對於新的服務出來之後，還是要做一個 verify，到底對於消費者的權益有沒有損害？包括我們這個問題，個人資料保護上有沒有不周到的地方？其實 NCC 都可以做得到，他不是沒有方法可以做。
曾更瑩律師	1. 個資法剛出來的時候，許多專家學者都有提出一樣的評論，譬如在個資法第 6、19、20 條都有，關於學術研究機構基於公共利益為統計或學術研究而有必要的時候，他蒐集的資料其實在這個時候已經要求去識別化了，但是它還是入法。已經

	去識別化的資料在個資法第 6、19、20 條還是當作個人資料來管理它的蒐集跟利用，這點在邏輯上蠻奇怪的，也導致對於一般的業者來說，到底去識別化的資料是不是還是個資？也就一直存在著一個問題，我覺得這是我們法律體系一直都交代不太清楚的部分。不要管法條這樣寫，因為其實它是在規範學術研究機構，但是對一般的民間機構，不只是資通訊的產業，當一個律師要去跟業者說，你現在拿到的去識別化的資料到底是不是個資，對我們來說也是有相同程度的困難。 2. 法律文件來說，在去識別化的標準面，剛好關於全民健保的資料可不可以釋放出來給醫學界、學術界做研究，之前也有一個判決，判決已經經過最高行政法院裁判，但是法官在論理的時候，倒是有一點讓我覺得非常的有趣，因為在那個判決裡面健保局的主張，他的資料經過層層加密，一共加密了 6 次，所以他認為他的資料是去識別化的。我

	把一個東西放在盒子裡面，我包了 6 層，把它貼起來，所以它就去識別化，這件事我一直不懂。 3. 關於「資料在地化」的部分，我們要發展臺灣的資通訊產業的話，我們也許也可以往這個方向去思考，譬如明年 5 月 18 日 GDPR 就會生效了，如果我們能夠通過 GDPR 的認證，也許我們可以在臺灣做外商的 Date center，一方面是繁榮臺灣的資通訊產業；另一方面，如果臺灣有這麼多 Data center 的話，世界各國會想盡辦法保護臺灣的安全跟臺灣的資訊安全。這或許是一個想法，與其大家很努力說資料要在地化，所有的資料都放臺灣、不能放國外，要不要另外一種比較開放的方法？反過來也許可以更增加臺灣的價值跟資訊安全。
翁清坤老師	1. 普遍來說，個資到底要被應用還是不被應用？這就是一個難題，像個資法第 1 條立法宗旨就同時要保護這兩個，這兩個目標其實是衝突的，要怎麼樣來做調解？這是一個

	大難題，全世界應該都在尋找答案，從德國最早開始制定個資法之後，OECD、EU、APEC 等等，國際組織或各國大家的邏輯思維都差不多，包括個資法的結構（Fair Informantion Parctices/Principles）FIPP，所有個資法幾乎都是在這八、九大原則的這種結構下做討論，討論個資怎麼被蒐集、處理、利用。 2. 去識別化，是不是個資被去識別化就不算個資？表面上看起來確實是如此，個資的定義是直接或間接識別到特定。但是現在資料被大量的儲存跟蒐集之後，去識別化的定義譬如像英國的 ICO，針對什麼叫做「去識別化的個資或匿名的資料」，從資料本身無法連結到特定人或者結合其他資料無法識別到特定人。我們自己主觀上認為把一個資料某些點拿掉，可是接下來握有這個資料的人，他有可能從別的資料來源去做比對，這個時候它的資料其實還是會被再識別化。如果被

	去識別化之後不是個人資料，所以不受保護，隨便亂用，但是到最後的風險又要當事人承擔，他為什麼要來做這種承擔？其實是現行規範的困境，不是只有臺灣面對的困境，包括西方世界，歐洲或美國，這都是一個問題。 3. 對業者來說，希望對個資的定義更加具體，其實是蠻困難的，因為什麼狀況底下可以連結到一個人，它就變個資？什麼時候去識別化？什麼時候避免再識別化？這其實都是隨著科技的變遷，還有你掌握的資料量（尤其是大數據），越來越難以控制。所以有很多討論，過去 OECD 所建構的這些個資保護，是沒辦法應用電腦或網路大數據出現的時代。 4. 第一代個資的保護的規範，現在已經進入個一個新的時代，很多學者建議，應該要發展出第二代，但是第二代還沒有出來。GDPR 明年的 5 月要生效，但是美國有些學者是比較支持個資的利用，他們認為這個

	GDPR 不過是像他們立憲過程當中的某一個過渡文件，我們認為 GDPR 可能規範得好，在他們支持個資料要被大量利用的眼中看起來，這個既有的規範會面對大數據的大量挑戰，這個界限到底是什麼？我們如果堅守個資的保護、隱私的保護，會覺得大數據很多東西都侵犯隱私不能用。 5. 監理沙盒，金融業好像討論比較多，監理沙盒的精神我沒有去研究，不過看到報紙跟別人討論，以初淺來說，就是監理制度的放寬。如同先進剛剛所提到，這裡面會涉及到當事人隱私，監理沙盒放鬆的是監理面，可是當事人的隱私他如果不願意放鬆，一樣還是會面臨困境。 6. 針對剛剛機器產生的資料，就像網路上瀏覽的 cookie，這種也只有握有資料庫的人才有辦法比對，才知道收視行為，他是誰；或者像 cookie，也是 ADSL 提供業者或者是 ISP，網站可以知道，但是如果脫離

	這個資料庫的使用，它到底還是不是個資？是一個問題。如果有辦法連結到特定當事人，現行的個個資法體制，不管是國內或國外，經過當事人同意，而且是告知後的同意。我們看很多網頁，美國同意的方式或契約成立的方式有兩種：一種就是當事人點擊的同意方式；另中一種就是 browse 的同意方式，browse wrap contract 和 click wrap contract。 7. 對業者來說一個破解之道，就是你蒐集的特定目的是什麼？這個目的其實是一個很麻煩的事，美國偶然會討論這個特定目的，我們當然就是鎖定這個特定目的，可是這個特定目的具體內涵到底是什麼？個資法第 53 條授權法務部去制定特定目的，法務部制定 182 種，如果要傾向於業者的話，當然這個特定目的就放得很大。 8. 特定目的其實要符合當事人、消費者以及業者的隱私合理期待；下一

	步，隱私合理期待是什麼？這又是一個難題，要看社會通念，隨著時空的變遷，網路裸奔的年代，年輕人他們的隱私合理期待又變小，因為他已經做了很多公開。 9. 像位置資訊，早先美國人認為公開場合沒有隱私，可是慢慢又出現 privacy policy，1967 年 Alan F. Westin 在他的「Privacy and freedom」這本書裡面，為什麼要保護個資，有一種類型就是 Public privacy，公開場合我們也有隱私，除非你是公眾人物，不然你在公開場合不會被辨認出來，我看到美國文獻有提到「匿名的權利」，除非我是知名人物，我有保持不被人家辨認出來。
臧正運老師	11. 監理沙盒制度它不是一個監理的真空，也不是一個法規除外的空間，它在金融產業上面之所以會討論，是因為有一個很單純「雞生蛋、蛋生雞」的問題要解決。現在有很多業者，他看到某一些沒有被

	滿足的金融需求，他想要進入市場提供金融服務，但是那些業者只要那些提供金融服務，他就會違反涉及銀行法的吸收存款，譬如銷售保險業的產品、投信、投顧業務，他就會因為這些法律會有一些他必須取得執照，才能夠做這些業務的問題。所以這個雞生蛋、蛋生雞的問題在於，對於一個新創業者、不是金融業的業者，他沒有足夠的資源、沒有錢的情況之下，很難去取得特許跟執照，因為特許跟執照都會對業主有相當程度資本額的要求、法律遵循的要求，一連串的門檻，所以他沒有資本，就沒有辦法取得特許。可是另外一個問題，他沒有特許，他就無法在市場上募集資本，因為潛在的投資人就不覺得他是一個可能可以未來繼續發展的企業。所以才會有監理沙盒，透過一個很短暫的時間，讓你來試試看，我給你一個暫時性、限制性，類似準特許的地位，讓你利用那個階段找投資人，因為投資人就會對

	你有相當程度的信賴，覺得你有可能有機會正式成為金融產業的一份子。 12. 從這個角度來看，再回到這個提綱，就會變成通訊傳播產業在適用監理沙盒到底是要做什麼？如果我們今天討論的是通訊傳播產業有一個新的創新商業模式、新的服務模式要推動，他覺得這樣推動可能會因為適法的問題，所以他沒辦法解決，我們是不是要給他一個類似的空間？在這種情況之下，也許他會說，因為我無法處理個人的資料，會有一些相關的疑義，所以你應該要告訴我，個資法你可以怎麼樣放寬。但是在那個脈絡之下，顯然就是要個案處理，因為他的一個創新模式也有可能是單純牽涉到非敏感性的資訊，有可能是牽涉到極度敏感性的資訊，哪怕我們今天真的要有一個個資法的監理沙盒制度，去排除某些個資法的適用，我相信那也不可能是一體適用的排除，也一定是依據他這個資料的

	特性，做相當程度、暫時性的豁免或凍結。 13. 監理沙盒制度還有一個很重要的設計，它希望在實驗的過程當中，讓這個實驗的業者跟主管機關在合作之下還是能夠做好三件事：第一件事情叫做消費者保護；第二件事情叫做風險管理；第三件事情，他必須發生爭議的時候，有一個爭議的解決途徑。 14. 監理沙盒制度還有一個，在風險保障管理的那一環，資安的風險依然是非常重要的一環，如果去看新加坡的監理沙盒制度，他會跟你說我們新加坡的監理沙盒制度有幾種類型的法律規範是不能夠被放寬的，個資就是其中的一項。當然在臺灣，如果要去做個資法的排除，或者是個人隱私保障密度的降低，我覺得還會牽涉到基礎權、憲法的問題。 15. 嚴格說起來，我不覺得它是完全沒有空間去討論某一些條款的適度

	放寬，或者在執行上面，主管機關預先把他可能執法、行使他 description 的範圍先界定出來，我覺得這個是可能可以做到的，但是那個必須建立在 case by case 的基礎之下，因為每一個進來沙盒測試的業者他想做的事情都不一樣，所以不太可能那半年，像臺灣創新條例說最長可以到 3 年，不可能這 3 年的時間對於這些所有的業者都一體適用，排除個資法第 19、20、21、22 條，我覺得那個就會出很大的問題。
楊秋敏老師	1. 以美國現在主流來說，隱私權已經走向一個自主控制權的概念，所以其實我們的個資法只要 handle 到這個程度就好了。也就是說，我對於我的個資要流向到哪裡、給誰使用、它的範圍多大，我有一個自主控制性存在就夠了，並不是需要嚴格到別人完全都不能用，個資本身其實有一定的特殊性，因為它有價化以後，有一些美國的學者甚至討

	論到它是不是財產的一種？如果它不是財產的一種，一定要有公享性，你要分享出去跟人家一起用。我比較贊成的是，首先在個資法修法的時候，應該把那些矛盾點，甚至有些地方該鬆綁的還是要鬆綁，不必要的嚴苛應該要去除。 2. 有一些標準是國際面都有的，像現在國際上面對於物聯網其他這些個資的使用，國際標準三大組織早就做了，歐盟就是其中一個，對於個資法上面相關的規定，歐盟指令裡面他有八大原則，我們只要跟歐盟的指令一樣，抓一個大的原則性概念就夠了，不必一定要嚴苛到那種程度。另外，我們對於國際組織所訂出來的標準，如果今天要跟國際接軌，其實我們國家在修個資法的時候，是可以參考的。 3. 監理沙盒制度適用在資通訊產業，我個人是認為這個可能性不大，因為它的合法性基礎的問題之外，它其實也跟隱私權本身的本旨有矛

	盾，因為我剛才說，要讓這個人擁有他個資的自主控制權，照理說要經過他同意，也就是說他能夠對資訊的流向、誰可以來使用、範圍多大要有一定的控制權，如果越多人監理的制度都加進來，就等於是那個範圍無限的擴大之後，他其實就很容易失去這個自主控制性。 4. 美國有一個個案是這樣，我可以提供給大家等一下思考，因為有一州州法規定，他們懷疑消防隊員在救災的時候，可能把自己身上的傳染病傳染給已經受災的人，所有他就要求所有來擔任消防隊員的人，都要先經過抽血檢測，有一些消防隊員來告這個州的這個規定違反隱私權。之後美國的法院最終的判決認為，個人資料的保護，也就是隱私的保護跟國家公益對於公民健康權的保護來說，應該是以公益先於私益，就認為州法的規定並沒有違反到國家大方向的保護全體國民身體健康這樣的公益，在這種情況下，隱私權的這種私益應該退讓，所以

	在平衡點所取的標準是什麼？是公、私益萬一相衝突的時候，他要求私益要退讓。
葉奇鑫所長	1. 去識別化在法律上做原則性的規定OK，但是然後呢？它難是難在後面的實踐，CNS29100 出來了，可是其實它也沒有解決什麼問題，對於個人資料去識別化這件事情，我覺得這個是大議題。 2. 關於通訊傳播傳產業，我覺得他們是很特殊，我前一陣子看大數據國外一個很有名的學者，他說只有兩個行業不需要整併外面的資料，自己本身就足夠成為大數據，就是電信業跟金融業，就這兩個，其他的大部分都還要去外面找資料，去跟人家的資料做合併。所以通訊傳播業本身是有非常龐大的數據，中華電信現在有大數據辦公室，他們在成立之前是找我事務所做一個研究報告來做背書，意思是可以做，因為他們很怕，那全部都是個資。但是該怎麼用，是可以請客戶簽同意

	書，但是面對既有客戶該如何請他們簽，又是門學問。 3. 我最同意的是，在臺灣落實個資法但是管不了外國公司，所以其實是不非常不公平的競爭，對國內業者這個也不能用、那個也不能用，但是臉書跟Google什麼都可以用，臉書跟 Google 也沒有做個資法的告知，他的網站上有看過做個資法的告知嗎？他在那邊營業的很高興，這些其實都是一種很公平的應用。我覺得另外一個思維，我當然還是希望能夠放寬，讓個資能夠做更好的商業上運用，因為你不這樣做，「大數據」這三個字是沒有意義的；萬一不行的話，我會建議，要想想外國業者要怎麼做規範。 4. 我個人覺得，所有的個資法，不管產業或者實際上的那一些大部分都是 option out，如果大家都是 option in 的話，就不會有大數據出現，因為大家都不會願意去 in。所以原則上在蒐集以後，讓他能夠

	去主張個資法第 3 條的權利，其實那個是對當事人很重要的保障。我也建議通訊傳播業者自己不要太害怕，他們一聽到個資法，就是覺得很頭痛，很多煩惱其實是他們自己產生的，只要誠實告訴當事人，讓當事人能夠執行第 3 條的權利，其實也沒有這麼嚴重的法律問題。

會議結論

綜合業者與專家座談會，可以得到以下結論：

（一）現行個人資料及隱私保護規範確實對業者的資料應用造成影響，導致對資料應用雖有意願卻不敢著手進行。

（二）目前通訊傳播業者對於資料應用偏向提升內部行銷，對於外部使用或是資料交換持保守之態度。

（三）業者希望能從電信徵信這樣的模式開始發展資料應用，但對於資料交換平台仍有疑義，因為 NP 資料庫是有法源支持，在沒有法源支持的情況下，業者難以發展資料應用平台。

（四）業者普遍認為國外業者未受到國內個資法規範，導致雙方在資料應用上形成不公平競爭。業者並未要求主管機關針對國外業者進行規範，只希望鬆綁法規，讓他們有公平競爭的能力。

（五）業者期望的鬆綁法規方法主要為監理沙盒，或是主管機關能就個資法的執行範圍，能明確畫分出可從事應用的領域。

（六）學者專家對於是否要修個資法也持保留態度，一方面認為特定目的、告知及同意的要件不能隨意退讓，二方面也認為業者有時候是因為對個資法的誤解，導致自己選擇不進行資料應用。

（七）學者專家認為比起調整個資規範，主管機關就個資隱私規範的疑義進行解釋，畫清應用的界限更為重要。

（八）關於個資去識別化的問題，有學者就認為這個去識別的過程還是資料處理，仍然要受到特定目的的規範，並非一概去識別化後就能解決所有個資問題。至於去識別化的標準可以參考國際標準，或是由主管機關建立標準皆可，但重點仍在去識別化後的資料被重新識別特定個人的風險有多高，以風險來管控而非遵守標準作業流程就算是完成去識別化。

（九）監理沙盒並非創造法律真空地帶，而是讓特定業者能在未完全符合法律規範下進行實驗。也因為各個業者狀況不同，處理起來也是依照個案而定，若要以通案排除個資法的方法來處理，適用上恐有疑問。另外，監理沙盒也可能有使用的界限，像新加坡禁止用於排除隱私規範，在我國能否用來排除個資隱私規範也有疑問。

（十）也有學者認為 NCC 仍然有辦法做到類似監理沙盒的作法，像是實驗區或是實驗管理辦法。透過鬆綁部分通信、傳播法規的限制也可以達到類似監理沙盒的實驗作用。

（十一）　關於資料在地化政策，相對於業者齊聲認為政府需要重視資料外流的問題，部分學者專家也認為需要重視這個問題。但有專家卻也認為開放資料的流通，反而讓我國在世界資料在地化趨勢中有機會逆流找到新的定位。

附錄二　性別影響評估表

<table>
<tr><td>壹、計畫名稱</td><td colspan="3">通訊傳播產業資料加值與創新應用趨勢及法令研析委託研究案</td></tr>
<tr><td>貳、主管機關</td><td>國家通訊傳播委員會</td><td>承辦機關</td><td>資策會科法所</td></tr>
<tr><td colspan="3">參、計畫內容涉及領域</td><td>勾選（可複選）</td></tr>
<tr><td colspan="3">3-1 政治、社會、國際參與領域</td><td></td></tr>
<tr><td colspan="3">3-2 勞動、經濟領域</td><td></td></tr>
<tr><td colspan="3">3-3 福利、脫貧領域</td><td></td></tr>
<tr><td colspan="3">3-4 教育、文化、科技領域</td><td>V</td></tr>
<tr><td colspan="3">3-5 健康、醫療領域</td><td></td></tr>
<tr><td colspan="3">3-6 人身安全領域</td><td></td></tr>
<tr><td colspan="3">3-7 家庭、婚姻領域</td><td></td></tr>
<tr><td colspan="3">3-8 其他</td><td></td></tr>
<tr><td>肆、問題現況評析及需求評估概述</td><td colspan="3">歐美主要國家近年來大力倡議及推動「開放資料（Open Data)」做為國家發展之重要策略，在各國紛紛跟進推動開放資料的情況下，已逐漸形成一股資料應用革新的新浪潮。這股浪潮透過釋出各種全方位資料作為基礎，透過前端科技等工具，將資料附加價值最大化，以創造資料為導向的數位經濟(Digital Economy)。而作為推動數位經濟基礎的科技、媒體和通信（Technology，Media，Telecom，簡稱 TMT)產業，在現今開放資料的發展過程中自然應該扮演不可或缺的重要角色。透過其所保有大量資料為核心，以提供創新及加值服務為目的，其蘊藏的價值極具開發潛力，特別是通訊傳播產業所保有的個人資料，其未來潛在產值更是不可限量。

為了擘劃我國關於通訊傳播產業資料應用的發展架構，本計畫擬蒐集美國、英國及日本等國家之通訊傳播產業資料加值、資料保護及創新應用等之現況、案例及法制，同時分析、歸納及整理出通訊傳播產業或資料保護之主管機關所採取的相關政策或措施，並檢視於我國現行法令下，數位匯流產業於資料加值、資料保護與創新應用之際，可能面臨的法令議題，例如：個人資料保護、跨境傳輸、開放授權等議題，以作為我國未來政策與推動措施規劃之參考。</td></tr>
</table>

伍、計畫目標概述	本案所擬訂之目標內容，無涉及性別議題部分。

陸、受益對象(任一指標評定「是」者，請繼續填列「柒、評估內容」；如所有指標皆評定為「否」者，則免填「柒、評估內容」，逕填寫「捌、程序參與」及「玖、評估結果」)

項　目	評定結果（請勾選）		評定原因（請說明評定為「是」或「否」之原因）	備註
	是	否		
6-1 以特定性別、性傾向或性別認同者為受益對象		V	**本研究計畫係針對有關歐盟、德國、英國、美國、日本等國家之通訊傳播事業加值利用個人資料之規管方式進行分析，並提出開放個人資料加值運用之因應措施，以此產出可供我國參酌的通訊傳播事業的資料應用規管模式，並無以特定性別、性傾向或性別認同者為受益對象。**	如受益對象以男性或女性為主，或以同性戀、異性戀或雙性戀為主，或個人自認屬於男性或女性者，請評定為「是」。
6-2 受益對象無區別，但計畫內容涉及一般社會認知既存的性別偏見，或統計資料顯示性別比例差距過大者		V	**本研究計畫內容係以文獻分析及焦點座談討論等方法，探討有關通訊傳播事業個人資料保護之機制及管理模式，並無涉及一般社會認知既存的性別偏見，或統計資料顯示性別比例差距過大者。**	如受益對象雖未限於特定性別人口群，但計畫內容存有預防或消除性別偏見、縮小性別比例差距或隔離等之可能性者，請評定為「是」。

項　目	評定結果（請勾選）		評定原因（請說明評定為「是」或「否」之原因）	備註
	是	否		
6-3 公共建設之空間規劃與工程設計涉及對不同性別、性傾向或性別認同者權益相關者		V	**本研究計畫之研究面向與公共建設之空間規劃與工程設計無關，無涉不同性別、性傾向或性別認同者之權益。**	如公共建設之空間規劃與工程設計存有考量促進不同性別、性傾向或性別認同者使用便利及合理性、區位安全性，或消除空間死角，或考慮特殊使用需求者之可能性者，請評定為「是」。

柒、評估內容					
評估指標	**評定結果**（請勾選）			**評定原因**（請說明評定為「是」、「否」或「無涉及」之原因）	**備註**
	是	**否**	**無涉及**		
一、資源評估（4項資源評估全部評定為「無涉及」者，應重新檢討計畫案內容之妥適性。）					
7-1 經費需求與配置考量不同性別、性傾向或性別認同者之需求					如經費需求已就性別予以考量、或經評估已於額度內調整、新增費用等者，請評定為「是」。
7-2 分期(年)執行策略及步驟考慮到縮小不同性別、性傾向或性別認同者差異之迫切性與需求性					如有助消除、改善社會現有性別刻板印象、性別隔離、性別比例失衡、或提升弱勢性別者權益者，請評定為「是」。
7-3 宣導方式顧及不同性別、性傾向或性別認同者需求，避免歧視及協助弱勢性別獲取資訊					如宣導時間、文字或方式等已考量不同性別、性傾向或性別認同者資訊獲取能力與使用習慣之差異，請評定為「是」。
7-4 搭配其他對不同性別、性傾向或性別認同者之友善措施或方案					如有搭配其他性別友善措施或方案者，請評定為「是」。
二、效益評估（7-5至7-9中任一項評定為「否」者，應重新檢討計畫案內容之妥適性；公共建設計畫於7-10至7-12中任一項評定為「無涉及」者，應重新檢討計畫案內容之妥適性。）					
評估指標	**評定結果**（請勾選）			**評定原因**（請說明評定為「是」、「否」或	**備註**

	是	否	無涉及	「無涉及」之原因）	
7-5 受益人數或受益情形兼顧不同性別、性傾向或性別認同者之需求，及其在年齡及族群層面之需求					如有提出預期受益男女人數、男女比例、其占該性別總人數比率、或不同年齡、族群之性別需求者，請評定為「是」。
7-6 落實憲法、法律對於人民的基本保障					如經檢視計畫所依據之法規命令，未違反基本人權、婦女政策綱領或性別主流化政策之基本精神者，請評定為「是」；相關資料可至行政院婦權會網站參閱(http://cwrp.moi.gov.tw/index.asp)
7-7 符合相關條約、協定之規定或國際性別/婦女議題之發展趨勢					如符合世界人權公約、消除對婦女一切歧視公約、APEC、OECD 或 UN 等國際組織相關性別核心議題者，請評定為「是」；相關資料可至行政院婦權會網站參閱(http://cwrp.moi.gov.tw/index.asp)
7-8 預防或消除性別、性傾向或性別認同者刻板印象與性別隔離					如有助預防或消除傳統文化對男女角色、職業等之限制或僵化期待者，請評定為「是」。

7-9 提升不同性別、性傾向或性別認同者平等獲取社會資源機會，營造平等對待環境					如有提升不同性別、性傾向或性別認同者參與社會及公共事務之機會者，請評定為「是」。
評估指標	**評定結果**（請勾選）			**評定原因** （請說明評定為「是」、「否」或「無涉及」之原因）	**備註**
	是	**否**	**無涉及**		
7-10 公共建設（含軟硬體）之空間使用性：空間與設施設備之規劃，符合不同性別、性傾向或性別認同者使用上之便利與合理性					如空間與設施設備之規劃，已考量不同性別、性傾向或性別認同者使用便利及合理性者，請評定為「是」。
7-11 公共建設（含軟硬體）之空間安全性：建構安全無懼的空間與環境，消除潛在對不同性別、性傾向或性別認同者的威脅或不利影響					如空間規劃已考慮區位安全性或消除空間死角等對不同性別、性傾向或性別認同者之威脅或不利影響者，請評定為「是」。
7-12 公共建設（含軟硬體）之空間友善性：兼顧不同性別、性傾向或性傾向者對於空間使用的特殊需求與感受					如空間規劃已考慮不同性別、性傾向或性別認同者特殊使用需求者，請評定為「是」。

捌、程序參與 • 至少徵詢1位性別平等學者專家意見，並填寫參與者的姓名、職稱及服務單位；學者專家資料可至台灣國家婦女館網站參閱（http://www.taiwanwomencenter.org.tw/）。 • 參與方式包括提送性別平等專案小組討論，或以傳真、電郵、書面等方式諮詢專案小組民間委員、性別平等專家學者或婦女團體意見，可擇一辦理。 • 請以性別觀點提供意見。 • 如篇幅較多，可採附件方式呈現。	一、參與者： 二、參與方式： 三、主要意見：
玖、評估結果（請依據檢視結果提出綜合說明，包括對「捌、程序參與」主要意見參採情形、採納意見之計畫調整情形、無法採納意見之理由或替代規劃等）	

填表人姓名：吳柏凭　　職稱：法律研究員

電話：(02)6631-1153　　e-mail：ppwu@iii.org.tw

附錄三　期中報告審查意見修正對照表

委員	審查意見	修正情形
陳委員國龍	1、請受託單位，分析專家學者座談會意見，提出可供本會政策規劃可採納之意見。 2、針對本案請加強創新應用趨勢之實例。 3、請於期末報告提出建議，可供電信傳播業者可運用資料之免責條款。	1、遵示辦理。已經於P.111~P.112 分析整理出座談會的意見，並且綜合提出政策規畫意見於第四章。 2. 遵示辦理。已經完成補充美國、英國及日本應用案例於 P.11 、 P.22 、 及 P.30~P.31。 3、遵示辦理。
李委員文秀	1、本委託研究案期中報告就重要國家通訊傳播產業加值與創新相關法制彙整，業已兼顧消極面(個資保護法規)及積極面(大數據之運用)，及提出通訊傳播產業資料加值與創新應用議題之相關法制分析，架構完備，有引多國法制情況說明，亦多有實務案例說明，合乎本研究計畫需求。 2.惟為使本研究論述更加完整及切合本會所需，建議於期末報告補強如下： (1)有關美國立法例，列入及論述與收視行為有關之視	(1) 遵示辦理。已經補充於P.15~P.16 (2) 遵示辦理。已經補充論述於 P.16~P.18 (3) 遵示辦理。已經將部分第二章第二節移至第二章第一節，包括 P.11~P.12、P.22~P.25、P32~P.33

	訊隱私保護法(VideoPrivacy Protection Act)及有線電視隱私法(Cable TV Privacy Act)。 (2)美國FCC 於2016年所頒布之寬頻網路服務業隱私規則雖於川普上臺後遭廢除，但相關之政策及法理之爭議，可加強論述，或可考慮於第二章增加一議題係有關是否因資料蒐集者身分或業別不同區分保障或管制標準。 (3)章節內容可考慮調整，以使研究論述更嚴謹縝密，如第二章第二節所針對重要議題之分析，倘係與第一節外國法制(如美國)有關，可先於第一節略作完整概要說明。	
江委員耀國	1、本研究內容分為兩大部分，(1)資料加值與創新應用(事實、案例研究)；(2)資料加值應用法令(法規研究)。 目前期中報告中，第(2)部分比第(1)部分內容多，換言之，第(1)部分篇幅較少，若可行，請在期末報告補充第	1. 遵示辦理。已經完成補充美國、英國及日本應用案例於 P.11 、 P.22 、 及 P.30~P.31。 2. 遵示辦理。在案例部分都有分析各個個案是否有涉及個資的應用，並且提出關於業者解決個資議題的方

	(1)部分的內容。 2、在美國、英國、日本的案例部分，希望能夠區分為個資意涵及無個資意涵的部分，對於個資加值創用，產業如何進行去識別以不違反個資保護法，其產業作為及處理措施，可以值得介紹及建議的部分。	法。
卓委員政宏	1、列舉案例多為 Shared Data，是否有 Open Data 的實際案例可供參考。 2、是否可能建立資料去識別化規範，提供業者參考，並據以為究責之依據。	1. 遵示辦理。在案例部分都有補充關於 Open Data 的案例，包括 P.9、P.20、及 P.31。 2. 遵示辦理。關於去識別化規範的建議有提供於 P.113~P.114，惟宥於篇幅與研究時間，尚無法提供完整的去識別化規範供業者參考。
余委員啟民：	1、通訊傳播產業去識別化之技術面 建議可以透過業界訪談取得一些資料與經驗。 2、期中報告部分蒐集內容傾向醫療健康資訊之加值應用 建議結論章節能具體提出有關通訊傳播產業資料分類及加值類別後 再行針對創新應用機制提出可	1.遵示辦理。 2.3. 遵示辦理。綜合於第四章討論。 4. 遵示辦理。已經於 P.114~P.115 討論關於 CPBR 與 GDPR 的關聯與作為並提出建議。

	能因應作為。 3、有關法令鬆綁或具體法規解釋或建議部分 建議能於期末結論中提出。 4、跨境傳輸部分與目前的GDPR 與 CBPR 之關聯性與作為 建議於期末報告中略提建議。	
陳委員書銘	1.本案研究單位針對個人資料保護及使用有詳盡的研究，實屬不易；惟除了資料保護外，也希望研究單位對資料加值及創新應用的案例能有更多的著墨，以符合委託研究案的需求。 2.世界各國為發展數位經濟，均鼓勵創新應用服務。因此，除了個資保護去識別化以外，是否有其他針對通訊傳播創新應用服務的鼓勵機制(例如提供類似「金融監理沙盒」的作法) ？亦請補充。	1. 遵示辦理。已經完成補充美國、英國及日本應用案例於 P.11 、 P.22 、 及 P.30~P.31。 2. 關於監理沙盒應用於通信傳播資料應用領域補充說明於 P.117~P.118。
王委員伯珣	報告內之章節項次階層，建請依需求書附件 4(P.10~16)格式調整。	遵示辦理。
其他意見	有關「NCC」簡稱文字，建請於報告第 1 次出現時，以	遵示辦理。

	「國家通訊傳播委員會(以下簡稱 NCC)」，並請檢視後續簡稱文字，應於第 1 次出現時顯示全稱。	

附錄四　期末報告審查意見修正對照表

委員	審查意見	修正情形
陳委員國龍	有關提供業者資料加值之免責條款之指導方針，請受託單位考量相關法院之判例個案，提供允當建議供本會參考引用。	未來將於後續的研究持續擴充相關判決，並製作指導方針以引導業者。
李委員文秀	1、 本委託研究案期末報告業已多加補加值與創新應用案例，且已依委員期中意見加整合論述，並已提出具體政策建議，合乎本計畫需求。 2、 惟為更精進結論建議，可考量整合歸納簡報中各國立法例整理及相關考量因素，歸納出類似指針或指導原則之建議。 3、 報告中第 79 頁所提「數位通訊傳播法」草案第 21 條規定係針對數位跡證之規範，較無涉資料在地化具體規範，建議刪除較不相關論述，免引發誤解。	遵示辦理。
江委員耀國	1、 通訊傳播產業資料加值應用的研究結論，建議仍應區別個資 vs 非個資。 2、 在個資的部分，是否可能寫出給業者的初步指引(南)，包括個資的範圍(個資與非個資的辨別)，去識別的標準、去識別資料的使用措施(如以契約約定，不能重新再行識別)。 3、 第 112 頁的「第三節政策建議」建議加以修改，多加呼應前面各章的研究所得。	（一） 有鑑於與個資相關之資料為目前業者最關心的議題，也是爭議最大，尤其在於個資本身的定義仍有許多不同之見解，因此在本研究以個資相關之資料為優先研析對象；但在未來的相關研究中，將會對於非個資之資料，參酌歐盟之相關規範進行研析。

卓委員政宏	1、 本計畫之主要目的在增加資料加值與創新應用，對於哪些資料應 OPEN，希望能有建議。 2、 去識別化的技術很難有明確建議，希至少對於業者應盡責任的規範有所建議。	謝謝委員的建議，未來將在相關研究計畫中持續執行。
余委員啟民	1、 英文摘要第一段最後一字，建議 valuable 改為 invaluable。 2、 引註部分，英文結尾，請統一檢查，加上英文字的句點。 3、 P.106 第一行英文 description。 4、 期末報告綜整力度明顯加強，除上述小幅修改建議，應予建議審查通過，並將期末簡報綱要納入期末報告具體政策建議中。	遵示辦理。
王委員伯珣	1、 本案委託辦理工作項目共四項，第三項是檢視我國現行法令下，通訊傳播產業於資料加值、資料保護與創新應用可能作法及法令限制等議題，惟就目前初稿內容，這一工作項目的資料比較薄弱並且沒有統整，建議獨立一個章節並補強論述，以符合委託研究案需求。 2、 就初稿目錄架構觀之，第二章第一節與第二節分別為相關法制“彙整”、相關法制“研析”，惟視報告內容大都是蒐集彙整資料，第一節是著重在開放資料及個資保護，第二節是去識別化、跨境傳輸等議題。建議修正目錄及第二章之內容編排以前後一致，並請再加強	謝謝委員之提醒，已於第四章增加法令盤點之議題，並且調整第二章之結構以符合工作項目之要求。

	“研析”論述，以符合委託研究案需求。	
陳委員書銘	1、 期中審查建議事項已於期末報告補充。 2、 本研究目的在於如何減少法令阻礙以鼓勵通傳產業創新發展，並且就個人資料予以適度保護，保障消費者權益等項，提供主管機關政策參考。在業者座談會中，業者希望放寬法令限制以就蒐集的資料作分析運用，提供創新的服務。此部分政府應該如何處理，在期末報告似乎仍未見到具體明確的建議，例如政策建議中提到通訊傳播監理沙盒制度在台灣不適合，那是否有其他可行的具體政策建議？請研究團隊再予以補充。 3、 期末報告仍有一些錯漏字或重覆字，如 p5、p9、p27、p81、p83 等，請研究單位再行全盤檢視修正。	謝謝委員之建議與提醒，有鑑於資料加值創新應用的最大限制為個資法，所以本研究主要對於這個部份進行較多的研析，惟綜觀國際法制與我國相關人權團體之立場，目前短期內較可行之方式仍須透過去識別化或遵循個資法之相關規範，中長期則須透過修法來進行，未來在相關之研究案也會持續關注國際的法制趨勢與國內法院判決之走向，以提供業在資料加值利用的立基點。
工作小組	1、 報告內之章節項次階層，建請依需求書附件 4(P.10~16)格式調整，並建議每章及附件起始，應置於次頁第一行為宜。 2、 另完稿封面格式將以電子郵件寄予計畫主持人辦理。	遵示辦理。

附錄五　通訊傳播產業資料加值與創新應用座談會 DM

【通訊傳播產業資料加值與創新應用】
業者座談會

歐美主要國家近年來大力倡議及推動「開放資料（Open Data）」做為國家發展之重要策略，在各國紛紛跟進推動開放資料的情況下，已逐漸形成一股資料應用革新的新浪潮。透過釋出各種全方位資料作為基礎，透過前端科技等工具，將資料附加價值最大化，以創造資料為導向的數位經濟(Digital Economy)。

作為推動數位經濟基礎的通訊傳播產業，在現今開放資料的發展過程中自然應該扮演不可或缺的重要角色。透過其所保有大量資料為核心，以提供創新及加值服務為目的，其蘊藏的價值極具開發潛力，其能發展的創新應用模式更是充滿無限可能性。

資策會科技法律研究所特以「通訊傳播產業資料加值與創新應用」為題舉辦座談會，敬邀各位通訊傳播產業界先進蒞臨，藉由分享各業者資料應用的實際案例，進而深入討論關於資料應用的相關議題，包括運作面及法制面等並期望能經由這樣的討論能勾畫出目前通訊傳播產業資料分享應用的趨勢籃圖，進而制訂通訊傳播產業資料加值與創新應用新方針導引出可行的方向。

討論提綱

1、 資料應用的實務運作

（1） 目前業者對於資料的釋出與應用情形分享。

（2） 資料釋出與應用上所獲得的成果及遭遇的困難。

（3） 對於通訊傳播產業資料創新應用計畫的看法與參與意願。

2、 資料應用的法制議題

（1） 使用與個人相關資料法制面的議題。

（2） 其他關於資料應用的法制面議題。

（3） 於中介單位研擬相關原則與規範進行資料應用的需求？

3、 資料應用的需求與發展

（1） 由使用端來看還有哪些資料具有開發潛力。

（2） 關於資料應用上發展上除法制面外的顧慮。

（3） 關於資料應用的其他補充意見。

議　　程

下午	13:30-14:00	報　　到	
	14:00-14:20	引言簡報	資策會科法所價拓中心 吳柏凭 法律研究員
	14:20-16:00	與會業者綜合討論	
	16:00	會議結束	

指導單位：國家通訊傳播委員會
執行單位：資策會科技法律研究所
時　　間：2017 年 10 月 27 日下午 14:00-16:00
地　　點：台灣金融研訓院
(台北市中正區羅斯福路三段 62 號 6 樓小會議室)
聯 絡 人：

資策會科法所　　吳柏凭法律研究員
(02)6631-1153　　ppwu@iii.org.tw

業者名稱	與會代表
中華電信股份有限公司	闕仁斌 主任級工程師 邱祥霖 管理師
台灣大哥大股份有限公司	林雅雯 副處長 張贏太 經理
遠傳電信股份有限公司	蕭景騰 協理 廖鈺鳴 資專
凱擘股份有限公司	林雅惠 副處長 戴漢林 專案副理
台灣有線寬頻產業協會	彭淑芬 理事長
台灣電信產業發展協會	劉莉秋 副秘書長

交通資訊

◎地址：台北市中正區羅斯福路三段62號6樓小會議室

捷運站

捷運古亭站：2號出口 (往公館方向步行約5分鐘)

捷運台電大樓站：4號出口 (往古亭方向步行約3分鐘)

公車站

羅斯福路2段：[古 亭 站] 208 236 251 252 254 278 297 606 644 648 660 74 藍28 (步行約2-5分鐘)

羅斯福路3段：[埔城街站] 淡海2 606 644 648 藍28 252 254 236 251 74 278 208 1 (步行約1分鐘)

汀州路2段：[師大汀州街口] 673 671 297 藍28(步行約3-5分鐘)

和平東路一段：[師 大] 15 18 235 237 254 278 295 3 662 663 74 907 (步行約5-8分鐘)

停車資訊

北上行車：請沿汀州路二段至同安街右轉，約100公尺再右轉晉江街，直行約500公尺

南下行車：請沿羅斯福路三段至金門街或58巷右轉，約50公尺再左轉晉江街，直行約20公尺即抵本院地下停車場入口（本院大樓正後方位置）

※本院停車場容納數量有限，請多利用週遭停車場或大眾運輸工具。

【通訊傳播產業資料加值與創新應用】
專家座談會

歐美主要國家近年來大力倡議及推動「開放資料（Open Data）」做為國家發展之重要策略，在各國紛紛跟進推動開放資料的情況下，已逐漸形成一股資料應用革新的新浪潮。透過釋出各種全方位資料作為基礎，透過前端科技等工具，將資料附加價值最大化，以創造資料為導向的數位經濟(Digital Economy)。作為推動數位經濟基礎的通訊傳播產業，在現今開放資料的發展過程中自然應該扮演不可或缺的重要角色。透過其所保有大量資料為核心，以提供創新及加值服務為目的，其蘊藏的價值極具開發潛力，其能發展的創新應用模式更是充滿無限可能性。

然而部分資料加值運用方式所涉及個人資料法規之遵循、隱私保護以及資安議題等，稍一不慎就會造成當事人或是業者的損害，如何在資料應用與權益保護中取得衡平將會是通訊傳播產業未來提升競爭力的重要關鍵。

資策會科技法律研究所特以「通訊傳播產業資料加值與創新應用」為題舉辦座談會，敬邀各位產學研界專家先進蒞臨，共同討論上揭議題，並希望能獲得寶貴意見，俾為制訂通訊傳播產業資料加值與創新應用新方針導引出可行的方向。

討論提綱

1、 我國的個資法對於通訊傳播產業資料應用上造成阻礙，應該要進行什麼樣的調整？
2、 對於個人資料去識別化規範具體建議。是否要置入個資法明文規範？或是由主管機關頒布作業標準？
3、 監理沙盒制度適用於通訊傳播產業的可能性？
4、 通訊傳播資料應用下，個人資料保護與資料利用價值間該如何取得平衡？

議　　程

下午	13:30-14:00	報　　到
	14:00-14:10	開場致詞 資策會科法所價拓中心 顧振豪 主任
	14:10-14:30	引言簡報 資策會科法所價拓中心 宋佩珊 專案經理
	14:30-16:00	與會專家綜合討論
	16:00	會議結束

指導單位：國家通訊傳播委員會
執行單位：資策會科技法律研究所
時　　間：2017 年 11 月 10 日下午 14:00-16:00
地　　點：台灣金融研訓院
(台北市中正區羅斯福路三段 62 號 6 樓小會議室)
聯 絡 人：

資策會科法所	吳柏凭法律研究員
(02)6631-1153	ppwu@iii.org.tw

專家姓名	服務機關/單位/職稱
葉志良	元智大學資訊傳播學系助理教授
曾更瑩	理律法律事務所合夥律師
翁清坤	輔仁大學財法系助理教授
臧正運	政治大學法律系助理教授
葉奇鑫	達文西個資暨高科技法律事務所所長
楊秋敏	開南大學法律系助理教授

交通資訊

◎地址：台北市中正區羅斯福路三段62號6樓小會議室

捷運站

捷運古亭站：2號出口 (往公館方向步行約5分鐘)

捷運台電大樓站：4號出口 (往古亭方向步行約3分鐘)

公車站

羅斯福路2段：[古 亭 站] 208 236 251 252 254 278 297 606 644 648 660 74 藍28 (步行約2-5分鐘)

羅斯福路3段：[埔城街站] 淡海2 606 644 648 藍28 252 254 236 251 74 278 208 1 (步行約1分鐘)

汀州路2段：[師大汀州街口] 673 671 297 藍28(步行約3-5分鐘)

和平東路一段：[師 大] 15 18 235 237 254 278 295 3 662 663 74 907 (步行約5-8分鐘)

停車資訊

北上行車：請沿汀州路二段至同安街右轉，約100公尺再右轉晉江街，直行約500公尺

南下行車：請沿羅斯福路三段至金門街或58巷右轉，約50公尺再左轉晉江街，直行約20公尺即抵本院地下停車場入口（本院大樓正後方位置）

※本院停車場容納數量有限，請多利用週遭停車場或大眾運輸工具。

附錄六　通訊傳播產業資料加值與創新應用座談會照片

附錄七 期末報告審查會議簡報

通訊傳播產業資料加值與創新應用趨勢及法令研析 期末審查

財團法人資訊工業策進會
科技法律研究所
107.01.02

大綱

- 計畫說明
- 期中審查委員意見處理情形
- 計畫執行成果說明

計畫說明

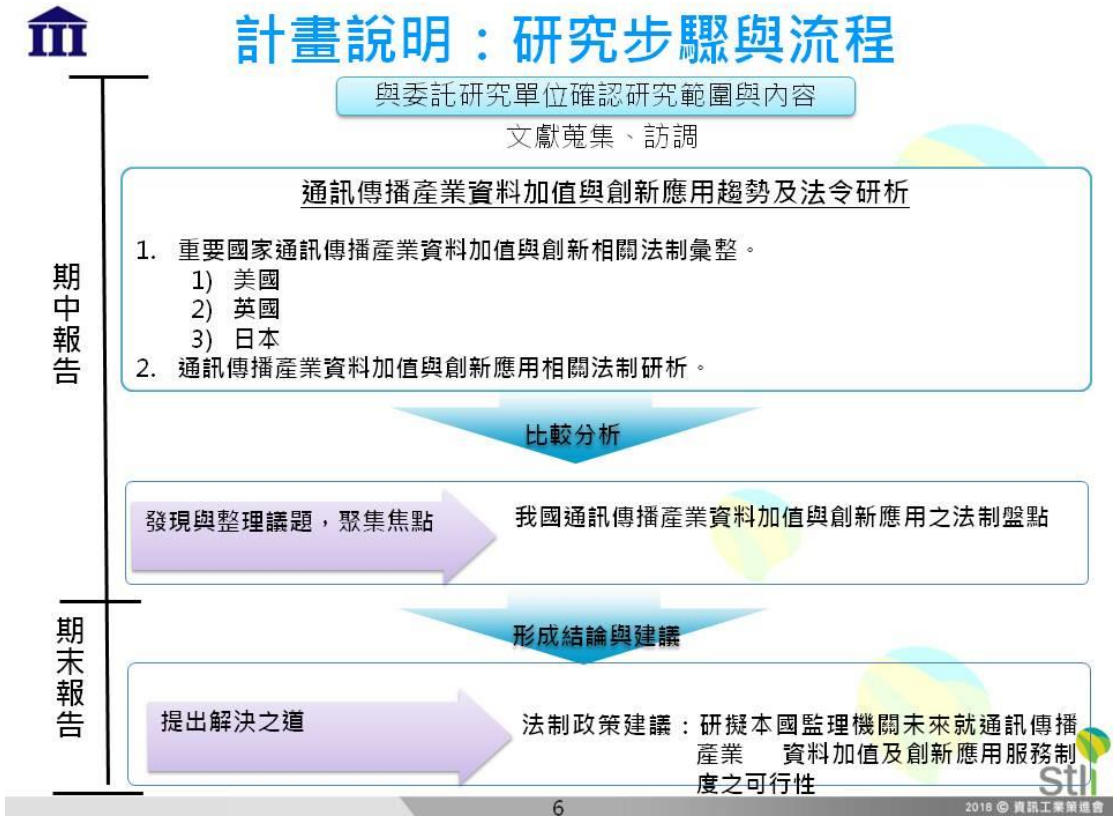
計畫說明：工作項目與執行進度

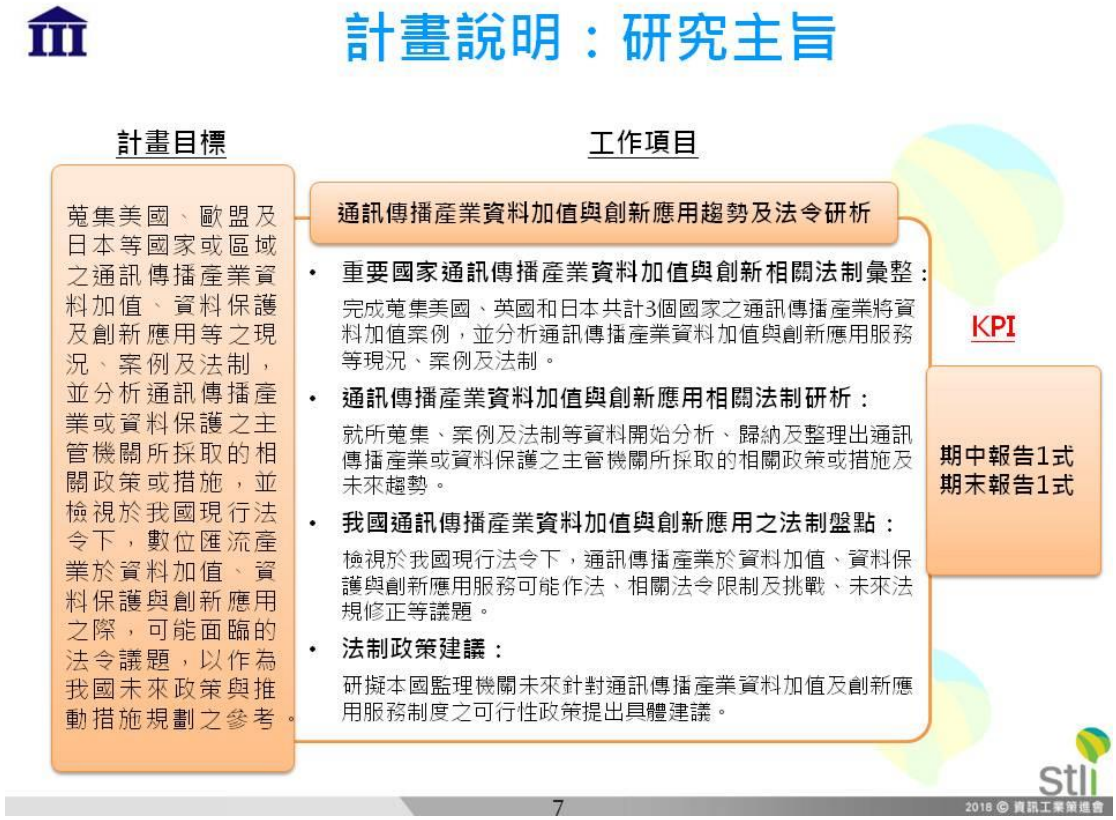
按照契約規定，分別於第四月及第六月完成期中與期末報告，如期如質完成研析。

工作項目	第一月	第二月	第三月	第四月	第五月	第六月	第七月	第八月	第九月	第十月	第十一月	第十二月
通訊傳播產業資料加值與創新應用趨勢及法令研析				期中報告▼		期末報告▼						
工作進度估計百分比（累積數）	10%	30%	50%	75%	90%	100%						

計畫說明：研究方法

研究方法論主要立基於比較法之研究，其實施步驟主要為(1) 確認施政需求(即研究議題)，(2) 國際相關政策、法規與措施研析，(3) 我國政策與法制現況檢視，(4) 研提相關之政策、推動措施或法規調適建議。





期中審查委員意見處理情形

期中審查委員意見處理情形(1/3)

委員	審查意見	修正情形
陳委員國龍	1、請受託單位，分析專家學者座談會意見，提出可供本會政策規劃可採納之意見。 2、針對本案請加強創新應用趨勢之實例。 3、請於期末報告提出建議，可供電信傳播業者可運用資料之免責條款。	1、遵示辦理。分析整理出座談會的意見，並且綜合提出政策規畫意見於第四章。 2. 遵示辦理。已經完成補充美國、英國及日本應用案例。 3、遵示辦理。
李委員文秀	1、本委託研究案期中報告就重要國家通訊傳播產業加值與創新相關法制彙整，業已兼顧消極面(個資保護法規)及積極面(大數據之運用)，及提出通訊傳播產業資料加值與創新應用議題之相關法制分析，架構完備，有引多國法制情況說明，亦多有實務案例說明，合乎本研究計畫需求。 2.惟為使本研究論述更加完整及切合本會所需，建議於期末報告補強如下： (1)有關美國立法例，列入及論述與收視行為有關之視訊隱私保護法(VideoPrivacy Protection Act)及有線電視隱私法(Cable TV Privacy Act)。 (2)美國FCC 於2016年所頒布之寬頻網路服務業隱私規則雖於川普上臺後遭廢除，但相關之政策及法理之爭議，可加強論述，或可考慮於第二章增加一議題係有關是否因資料蒐集者身分或業別不同區分保障或管制標準。 (3)章節內容可考慮調整，以使研究論述更嚴謹縝密，如第二章第二節所針對重要議題之分析，倘係與第一節外國法制(如美國)有關，可先於第一節略作完整概要說明。	(1) 遵示辦理，已經補充。 (2) 遵示辦理。已經補充論述。 (3) 遵示辦理。已經將部分第二章第二節移至第二章第一節。

期中審查委員意見處理情形(2/3)

委員	審查意見	修正情形
江委員耀國	1、本研究內容分為兩大部分，(1)資料加值與創新應用(事實、案例研究)；(2)資料加值應用法令(法規研究)。目前期中報告中，第(2)部分比第(1)部分內容多，換言之，第(1)部分篇幅較少，若可行，請在期末報告補充第(1)部分的內容。 2、在美國、英國、日本的案例部分，希望能夠區分為個資意涵及無個資意涵的部分，對於個資加值創用，產業如何進行去識別以不違反個資保護法，其產業作為及處理措施，可以值得介紹及建議的部分。	1. 遵示辦理。已經完成補充美國、英國及日本應用案例。 2. 遵示辦理。在案例部分都有分析各個個案是否有涉及個資的應用，並且提出關於業者解決個資議題的方法。
卓委員政宏	1、列舉案例多為Shared Data，是否有Open Data的實際案例可供參考。 2、是否可能建立資料去識別化規範，提供業者參考，並據以為究責之依據。	1. 遵示辦理。在案例部分都有補充關於Open Data的案例。 2. 遵示辦理。關於去識別化規範的建議已於報告提供，惟宥於篇幅與研究時間，尚無法提供完整的去識別化規範供業者參考。
余委員啟民	1、通訊傳播產業去識別化之技術面 建議可以透過業界訪談取得一些資料與經驗。 2、期中報告部分蒐集內容傾向醫療健康資訊之加值應用 建議結論章節能具體提出有關通訊傳播產業資料分類及加值類別後 再行針對創新應用機制提出可能因應作為。 3、有關法令鬆綁或具體法規解釋或建議部分 建議能於期末結論中提出。 4、跨境傳輸部分與目前的GDPR與CBPR之關聯性與作為建議於期末報告中略提建議。	1.遵示辦理。 2.3. 遵示辦理。綜合於第四章討論。 4.遵示辦理。已經於報告內討論關於CPBR與GDPR的關聯與作為並提出建議。

期中審查委員意見處理情形(3/3)

委員	審查意見	修正情形
陳委員書銘	1.本案研究單位針對個人資料保護及使用有詳盡的研究，實屬不易；惟除了資料保護外，也希望研究單位對資料加值及創新應用的案例能有更多的著墨，以符合委託研究案的需求。 2.世界各國為發展數位經濟，均鼓勵創新應用服務。因此，除了個資保護去識別化以外，是否有其他針對通訊傳播創新應用服務的鼓勵機制(例如提供類似「金融監理沙盒」的作法) ？亦請補充。	1. 遵示辦理。已經完成補充美國、英國及日本應用案例。 2. 關於監理沙盒應用於通信傳播資料應用領域補充說明於報告內。
王委員伯洵	報告內之章節項次階層，建請依需求書附件4(P.10~16)格式調整。	遵示辦理。
其他意見	有關「NCC」簡稱文字，建請於報告第1次出現時，以「國家通訊傳播委員會(以下簡稱NCC)」，並請檢視後續簡稱文字，應於第1次出現時顯示全稱。	遵示辦理。

計畫執行成果說明

計畫執行成果說明摘要

- ◆ 通訊傳播產業資料加值與創新應用趨勢及法令研析
  - ➢ 重要國家通訊傳播產業加值與創新應用案例
  - ➢ 重要國家通訊傳播產業加值與創新相關法制彙整
    - ✓ 美國 ✓ 英國 ✓ 日本
  - ➢ 通訊傳播產業資料加值與創新應用相關法制研析
    - ✓ 個人資料去識別化的標準與應用
    - ✓ 資料應用分析產生的歧視議題
    - ✓ 資料跨境傳輸與在地化之資訊蒐集及監理趨勢
- ◆ 通訊傳播產業資料加值與創新應用座談會
- ◆ 政策建議

重要國家通訊傳播產業加值與創新應用案例1/2

國別	主導者	參與者	內容
美國	Facebook 開放運算計畫 (OCP)	AT&T、Verizon	該計畫原聚焦於雲端供應商和大企業，現在邀請電信業者加入，將公開電信業用在全球通訊網路的強大交換器和其他設備的設計規格，以增加工作效率、彈性和客製化資料中心技術。
	AT&T	DirecTV	1. AT&T與運營商DirecTV合併後將DirecTV的電視定向功能與AT&T AdWorks資料驅動的TV Blueprint解決方案相結合。 2. DirecTV的定址廣告平台利用機上盒和第三方資料，以家庭為單位向付費電視用戶推送廣告活動。TV Blueprint則利用來自數百萬機上盒的匿名和總收視人群專有資料，開發訂製化的、最優化的媒體計劃，以便能更好地將廣告推送給廣告商的目標受眾群體。

重要國家通訊傳播產業加值與創新應用案例1/2

國別	主導者	參與者	內容
英國	英國廣播公司 (BBC)	iPlayer(免費在此平台觀看7天內的BBC電視和廣播節目)	2014年3月BBC宣布將調整iPlayer介面設計，蒐集客戶的收視資料，建立起客製化的影片推薦系統，配合巨量資料運算，自動推薦使用者可能有興趣的片單。

重要國家通訊傳播產業加值與創新應用案例2/2

國別	主導者	參與者	內容
日本	軟體銀行(SoftBank)	Sony、Toshiba、Linaro	1.以IOT的發展為主。 2.體銀行平台蒐集的個資包括位置資訊、使用紀錄、裝置資訊等，其蒐集及處理的特定目的都依照軟體銀行的隱私權政策
	NTT	札幌市	NTT提供免費wifi，藉由wifi來蒐集資料並且進行統計分析，之後將結果提供給札幌市政府作為發展觀光的依據，並且可以針對特定國家或是地區的觀光客進行特製化的服務。
	KDDI	政府開放資料與IOT技術	例如其附設購物網站au WALLET Market賣的傘架，連通智慧型手機的氣象資料

16

2018 © 資訊工業策進會

個人資料去識別化的標準與應用（1/2）

美國	重新識別並無專門法律規範，由FTC訂定相關標準，並以法（參考報告P.13-14）及契約的雙重運作確保重新識別行為規範的執行。
英國	對去識別化規定較歐盟寬鬆，可逆之擬匿名化資料，只要原資料保有者未將連結工具提供給資料接收者，並且採取適當安全措施，使資料接收者無管道及機會重新識別資料當事人，則也屬「去識別化資料」之一種。
日本	以更為直接的方式來規制，於個人資料保護法修正增訂「匿名處理資料」概念，增設「個人資料保護委員會」，負責匿名處理資料督管理及規範訂定。明文禁止將去識別化的資料進行比對還原。惟對於違反規定重新識別個人，在規制力道上略有不足。
我國	個資法中只規定去識別化要無法識別特定當事人，但做到什麼程度才符合法律規範，則需要有另外的參考依據。 透過CNS 29100、CNS 29191以及「個人資料去識別化過程驗證要求及控制措施」實作指引框架下，對於去識別化步驟中有要求評估重行識別的風險、制定對策。 2015年8月10日經濟部標準檢驗局的會議中，也與各法人機構取得關於「政府開放資料之個資不得被重行識別」的共識。 個資去識別化的過程未遵守上述規定，則應視為未經足夠之去識別化，而仍屬於我資法之個資。若違法蒐集個人資料時，將依我國個資法第47條之規定受行政裁罰。 法務部也是持樣見解，認為去識別化之資料若被重新識別應有法律責任。

17

2018 © 資訊工業策進會

個人資料去識別化的標準與應用（2/2）

- 本研究建議：
  - 業者若不欲告知和請求同意或是在實務上不可能向當事人個別徵求同意的時：
    - ✓ 應提供CNS 29100及CNS 29191規定讓業者去遵循以餞行去識別化工作。
  - 經去識別化的資料應審慎評估受到再識別化的可能性。
    - ✓ 較可行的作法：以契約去約束資料的受傳輸方，要求不得以任何方法去比對、還原經去識別化資料的識別因子。

資料應用分析產生的歧視議題

- 資料分析技術將人類型化、數據化，衝擊到既有對於人性尊嚴的基本價值觀。
- 現行個資法無法處理此問題：
  - 資料分析，特別是側寫（Profiling），係利用大量資訊來建立詳盡的機制進行分類和組織，**當事人會受到損害的原因並非個人資訊被蒐集，而是擔心被歸入錯誤或不利的類別**。我國的個資法的規範無法處理這個問題。
- 歐盟GDPR可資借鏡：
  - 賦予當事人拒絕被側寫及對側寫結果提出異議之權。
  - 細部規範仍待修正：
    - ✓ 如何確保被分析的人得知自己被側寫？
    - ✓ 透過什麼樣的機制可以保護自己的權利？

資料跨境傳輸與在地化之資訊蒐集及監理趨勢

- 我國：採取「特定部門措施」的方式管制
  - 生物資料庫、金融業務→不分區域，皆須主管機關許可
  - 通訊傳播事業→禁止其傳輸至特定區域
  - 原因：維護個人資料之保護
- 世界各國：程度與作法各有不同
  - 原因：個人資料之保護，尤其是特定類別個資保護（確保個人資料不會因為跨境資料傳輸而無法得到保護）
  - 例外：多以當事人同意、目的地個資保護程度等作為許可資料跨境傳輸之條件。
  - 亦有因國安或反恐需求，強制、大範圍要求在地化措施者。此類作法強烈限制擁有者跨境傳輸之可能，可能對該國之整體經濟及企業營運都產生負面影響，若要採取類似措施，宜慎重考慮。

資料跨境傳輸與在地化之資訊蒐集及監理趨勢

持續性的例外情況（Ongoing Exception）		
適當保護/白名單模式 (adequacy/whitelist approach)	評估接收資料的第三國是否能提供個人資料足夠的保護程度，此方法為國際間廣泛採用之方法	歐盟、日本、以色列和瑞士
自我拘束規則模式 (binding rules approach)	考慮進行跨境資料轉移的特定公司是否已經執行了足以保護個人資料安全的處理措施及獨立審查機制	歐盟的「企業自我拘束規則」、亞太經濟合作組織（APEC）的「跨境隱私保護規則」、澳洲、日本
契約範本模式 (model contracts approach)	此模式評估企業所使用的契約中的條款是否已經提供個人資料轉移足夠的保護程度	歐盟
同意模式 (approach)	此模式係檢驗個人是否同意將其資料進行跨境傳輸	歐盟

通訊傳播產業資料加值與創新應用座談會及政策建議

◆ 通訊傳播產業資料加值與創新應用業者座談會

- ➢ 現行規範影響業者資料應用，雖有意願卻難實行。
  - ✓ 應用偏向提升內部行銷，對外使用或交換持保守態度。
- ➢ 希望發展電信徵信，但對於交換平台疑義。
- ➢ 業者認為國外業者未受到國內個資法規範，形成不公平競爭。但並未要求針對國外業者進行規範，而是希望鬆綁法規。
  - ✓ 鬆綁方向：監理沙盒，或就個資法畫分出可應用的領域。

通訊傳播產業資料加值與創新應用座談會及政策建議

◆ 通訊傳播產業資料加值與創新應用專家座談會

- ➢ 修個資法：持保留態度
  - ✓ 特定目的、告知同意等不能隨意退讓，且有時是因業者對個資法的誤解
  - ✓ 就規範的疑義進行解釋，畫清應用界限更為重要。
- ➢ 去識別化
  - ✓ 去識別化還是資料處理，受特定目的的規範。標準可參考國際或由主管機關建立。重點在去識別化後的資料被重新識別的風險有多高，以非遵守標準作業流程就算是完成去識別化。
- ➢ 監理沙盒
  - ✓ 並非創造法律真空地帶。以通案排除個資法的方法來處理，適用上有疑問。另新加坡禁止監理沙盒排除隱私規範，能否排除個資法範也有疑問。
  - ✓ 有認為NCC有類似監理沙盒的作法，像是實驗區或是實驗管理辦法。
- ➢ 資料在地化政策
  - ✓ 部分學者專家也認為需要重視這個問題。
  - ✓ 有專家卻認為開放資料的流通，反而讓我國在世界資料在地化趨勢中有機會逆流找到新的定位。

通訊傳播產業資料加值與創新應用座談會及政策建議

- 通訊傳播產業資料加值與創新應用業者座談會
  - 現行規範影響業者資料應用，雖有意願卻難實行。
    - ✓ 應用偏向提升內部行銷，對外使用或交換持保守態度。
  - 希望發展電信徵信，但對於交換平台疑義。
  - 業者認為國外業者未受到國內個資法規範，形成不公平競爭。但並未要求針對國外業者進行規範，而是希望鬆綁法規。
    - ✓ 鬆綁方向：監理沙盒，或就個資法畫分出可應用的領域。

政策建議

- 釐清個人資料定義，解決爭議問題
- 提供更精確的個資去識別化標準
- 設立或協助設立資料平台
- 跨境資料傳輸議題的協助
- 資料在地化政策實施可行，但可思考開放帶來的正向利益
- 監理沙盒本質與業者所享有落差，個資保障牽涉當事人的資訊自主控制性，恐難開放

參考書目

中文部分

專書

陳儀、陳琇玲譯，《物聯網革命》，商周出版，2015年，台北。

期刊

陳榮傳，〈再論資料跨國流通〉，《月旦法學雜誌》，第 78 期，2001 年，頁 166。

研究報告

1. 行政院研究發展考核委員會，〈政府資料開放加值應用研究分析書面報告〉，2001 年，頁 14 。
2. 陳誌雄、李崇僖、張照恬，〈105 年度政府健康資訊開放應用國際趨勢之法規推動計畫成果報告〉，衛生福利部中央健康保險署委託研究，2016 年，頁 95。
3. 葉志良，大數據應用下個人資料定義的檢討：以我國法院判決為例，2016 年。
4. 鄭美華, 大數據分析與個人資料保護之衝突：從收視行為調查談起，2017 年 7 月。

我國法規

1. 個人資料保護法
2. 金融機構作業委託他人處理內部作業制度及程序辦法
3. 人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查基準

其他中文文獻

1. 中華民國法務部，〈電腦處理個人資料保護法修正草案總說明（行政院版）〉，http://www.moj.gov.tw/ct.asp?xItem=44566&ctNode=28007&mp=001
2. 行政院衛生署衛署醫字第 0990069637 號，2010 年 5 月 28 日。

3. 衛生福利部衛部醫字第 1061665812 號，2017 年 9 月 12 日。
4. 國家通訊傳播委員會，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區，2012 年 9 月 25 日，http://www.ncc.gov.tw/chinese/print.aspx?table_name=news&site_content_sn=538&sn_f=26302。
5. 公共政策網路參與平台，「數位通訊傳播法」草案意見徵詢，2017 年 1 月 4 日 https://join.gov.tw/policies/detail/6b949e24-0fe0-4f0a-b5d9-fb3b051de675。
6. （香港）政制及內地事務局，〈立法會十三題；個人資料移轉〉，（香港）政制及內地事務局，2007 年 3 月 7 日，http://www.cmab.gov.hk/tc/upload/lcq20070307person_c.pdf。
7. （香港）政制及內地事務局，〈立法會政制事務委員會檢討《個人資料（私隱）條例》與相關事宜〉，立法會 CB(2)582/10-11(03)號文件，第 35 點，頁 11，2010 年 12 月 http://www.legco.gov.hk/yr10-11/chinese/panels/ca/papers/ca1220cb2-582-3-c.pdf 。
8. （香港）政制及內地事務局，〈立法會十九題；《個人資料（私隱）條例》第 33 條的實施〉，（香港）政制及內地事務局，2007 年 3 月 7 日，http://www.cmab.gov.hk/tc/press/press_3611.htm。
9. 端傳媒，〈因拒絕將用戶個人數據儲存在本地，LinkedIn 恐遭俄羅斯封殺〉，2016 年 11 月 11 日，https://theinitium.com/article/20161111-dailynews-russia-linkedin-blocked/。
10. 法務部，法務部 99 年度公務機關個人資料保護方案計畫研究成果報告書，2012 年，

頁 377，http://www.moj.gov.tw/ct.asp?xItem=283487&ctNode=36912&mp=095。

11. 經濟部，APEC 跨境隱私保護規則體系能力建構國際研討會 10 月 2 日在臺北揭開序幕，2017 年 10 月 2 日，https://www.moea.gov.tw/MNS/populace/news/News.aspx?kind=1&menu_id=40&news_id=72834。

中國大陸法規

1. 电子银行业务管理办法
2. 人民银行关于银行业金融机构做好个人金融信息保护工作的通知
3. 中国人民银行金融消费者权益保护实施办法
4. 征信业管理条例
5. 网络出版服务管理规定
6. 人口健康信息管理办法（试行）
7. 地图管理条例》
8. 网络安全法

香港法規

個人資料（私隱）條例

英文部分

英文研究報告

1. Accenture strategy, DIGITAL DISRUPTION: THE GROWTH MULTIPLIER, May 2016 https://www.accenture.com/us-en/insight-digital-disruption-growth-multip

lier

2. FTC REPORT, Big Data: A Tool for Inclusion or Exclusion?Understanding the Issues, Jan 6, 2016, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf
3. The White House, Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights, May 4, 2016, https://www.whitehouse.gov/blog/2016/05/04/big-risks-big-opportunities-intersection-big-data-and-civil-rights.
4. UNITED STATES INTERNATIONAL TRADE COMMISSION, Recent Trends in U.S. Services Trade: 2015 Annual Report 116 ,May, 2015, https://www.usitc.gov/publications/332/pub4526.pdf
5. The White House,Fact Sheet: The White House Launches The Opportunity Project," Utilizing Open Data to Build Stronger Ladders of Opportunity for All, March 7, 2016 , https://www.whitehouse.gov/the-press-office/2016/03/07/fact-sheet-white-house-launches-opportunity-project-utilizing-open-data
6. DJ Solove, A Brief History of Information Privacy Law, 2016, http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications
7. Edward Snowden: the whistleblower behind the NSA surveillance revelations, Jun 9, 2013, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

8. Transcript of President Obama’s Jan. 17 speech on NSA reforms, Jan 17, 2014, https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsareforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.
9. The White House Big Data Report: The Good, The Bad, and The Missing, May, 2014, https://www.eff.org/deeplinks/2014/05/white-house-big-data-report-good-bad-and-missing.
10. The White House Office of the Press Secretary,FACT SHEET: Safeguarding American Consumers & Families(2015), Jan 12, 2015, http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.
11. Washington Post, The House just voted to wipe away the FCC’s landmark Internet privacy protections, March 28, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/.
12. OPSI, The Power of Information Review, May 20, 2010, http://www.opsi.gov.uk/advice/poi/index.
13. GOV.UK, Open Data White Paper: Unleashing the Potential, Jun 28, 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf
14. Information Commissioner’s Office, Determining What Is Personal Data (2012), Dec 12, 2012, https://ico.org.uk/media/for-organisations/documents/1554/determining-wh

at-is-personal-data.pdf.

15. Information Commissioner’s Office, Anonymisation: Managing Data Protection Risk Code of Practice (2012), Dec 12, 2012, https://ico.org.uk/media/1061/anonymisation-code.pdf.
16. Information Commissioner’s Office, Big Data and Data Protection (2014), Sep 4, 2017, https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf.
17. Latanya Sweeney, Discrimination in Online Ad Delivery, Jan 28, 2013, http://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf
18. BBC, Your information & Privacy, http://www.bbc.com/privacy/
19. Washington Post, The House just voted to wipe away the FCC’s landmark Internet privacy protections, March 28, 2017,https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/
20. FCC,FCC Releases Rules to Protect Broadband Consumer Privacy, April 28, 2017https://www.huntonprivacyblog.com/2017/04/06/president-trump-nullifies-fcc-broadband-consumer-privacy-rules/
21. Ars Technica, ISPs and FCC Chair Ajit Pai celebrate death of online privacy rules, March, 2017, https://arstechnica.com/tech-policy/2017/03/isps-and-fcc-chair-ajit-pai-celebrate-death-of-online-privacy-rules/

美國法規

1. Freedom of Information Act
2. Privacy Act of 1974
3. Right to financial privacy act
4. Telephone Consumer Protection Act
5. Health Insurance Portability and Accountability Act
6. Children’s Online Privacy Act，COPPA
7. USA PATRIOT Act
8. Homeland Security Act
9. Fair and Accurate Credit. Transaction Act
10. The Health Information Technology for Economic and Clinical Health Act
11. Consumer Privacy Bill of Rights
12. Video Privacy Protection Act
13. Cable TV Privacy Act

英國法規

1. Data Protection Act 1998
2. Data Protection Bill 2017
3. GOV.UK, Digital Economy Act 2017

澳洲法規

Privacy Act 1988

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

My Health Records Act 2012

歐盟法規

1. Data Protection Directive
2. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

其他英文文獻

1. Open Knowledge Foundation , Global Open Data Index, March, 2016 http://2015.index.okfn.org/place/.
2. Open Knowledge Foundation , Global Open Data Index, March, 2017 http://2016.index.okfn.org/place/.
3. Data.gov, http://catalog.data.gov/dataset.
4. ODI, About the ODI, http://theodi.org/about-us.

日文部分

日本法規

1. 個人情報の保護に関する法律改正法
2. 行政機関の保有する個人情報の保護に関する法律
3. 独立行政法人等の保有する個人情報の保護に関する法律
4. 情報公開・個人情報保護審査会設置法
5. 行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律（整備法）

其他日文文獻

1. 経済産業省， データに関する取引の推進を目的とした契約ガイドライン，
   2015 年 10 月 6 日
   http://www.meti.go.jp/press/2015/10/20151006004/20151006004.pdf
2. 首相官邸，世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画について，
   2017 年 5 月 30 日
   http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20170530/siryou1.pdf
3. ソフトバンク株式会社， IoT データをビジネスに活用するオープンプラットフォームの構築およびデータ価値化検証の PoC 実施について，
   2016 年 11 月 10 日
   http://www.softbank.jp/corp/group/sbm/news/press/2016/20161110_04/
4. TANNAN CATV Co.,LTD.， オープンデータについて，
   2016 年 11 月 10 日
   http://miseban.com/opendata/
5. 個人情報保護関連５法の概要 ，日本總務省行政管理局，
   2003 年 5 月
   http://www.city.yokohama.lg.jp/shimin/madoguchi/j-net/singikai/02/j-net2si3.pdf
6. 内閣官房高度情報通信ネットワーク社会推進戦略本部, パーソナルデータの利活用に関する制度改正大綱,
   2014 年 6 月 24 日
   http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf
7. 総務省, パーソナルデータの利用・流通に関する研究会報告書～パーソナルデータの適正な利用・流通の促進に向けた方策～,

2013 年 6 月

http://www.soumu.go.jp/main_content/000231357.pdf

8. Business Joural, Suica のデータ販売中止騒動、個人特定不可なのになぜ問題？ビッグデータの難点,

2013 年 8 月 23 日

http://biz-journal.jp/2013/08/post_2760.html

9. 個人情報保護委員会, 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）,

2016 年 11 月 30 日

http://www.ppc.go.jp/files/pdf/guidelines04.pdf

10. ソフトバンクグループ， 個人情報の取り扱いについて ，

https://www.softbank.jp/help/privacy/