104 年度委託研究案

「通訊傳播事業個人資料保護之機制及管理模式」
委託研究報告

The Research on The Regulatory Mechanism of Personal Data Protection on Communication Industries

計畫主持人：東吳大學法律學系余啟民教授
Project Coordinator：Prof.Yu Chi-Min
計畫執行單位：達文西個資暨高科技法律事務所
Executive Institution：Davinci Personal Data and High-Tech Law Firm
計畫執行期程：104 年 9 月 18 日至 105 年 4 月 16 日
Period of Project：September 18, 2015～April 16, 2016
計畫委託機關：國家通訊傳播委員會
Project DelegateInstitution：National Communications Commission
印製日期：中華民國 105 年 4 月 14 日
Date of Publication：April 14, 2016

「通訊傳播事業個人資料保護之機制及管理模式」

委託研究報告

(契約編號：NCCM104006-0724)

執行單位

達文西個資暨高科技法律事務所

主持人

余啟民

協同主持人

吳君婷

研究人員

王慕民、陳品安、吳彥欽、張又丹

GRB 計畫編號：NCC-46-104-01
GRB 系統編號：PG10409-0031
執行期程： 104 年 9 月 18 日至 105 年 4 月 16 日
委託機關：國家通訊傳播委員會
印製日期：中華民國 105 年 4 月 14 日

中文摘要

網路與通訊科技的發展及行動裝置的普及，為通訊傳播事業帶來革命性的發展，業者不再只是被動的提供電信、廣播服務，更能主動透過網路與用戶互動、提供客製化的服務及廣告資訊。同時，用戶在使用通訊傳播業者的各項服務時，將因此提供或產出許多與用戶個人相關的資料，例如身分基本資料、通信紀錄、網頁瀏覽紀錄、位置資訊、帳單明細、收視紀錄等，在大數據及智慧聯網的技術蓬勃發展的趨勢下，「資料加值運用」以達到「資料價值最大化」已成為國際潮流，用戶的資料對於通訊傳播業者無疑具有巨大的潛在商業價值。

然而，這些加值運用方式均涉及用戶對於其個人資料的「事前知情」、「事中控制」及「事後退出」等資訊隱私權、資訊自主權之憲法上基本權利，通訊傳播業者並不可漫無限制而在「服務契約」的必要範圍之外加值運用用戶資料。

本研究之目的在於參考國際上對於通訊傳播事業加值利用用戶個人資料的規範及管理方式進行分析，並提出開放個人資料加值運用的因應措施，例如要求通訊傳播業者加強事前對於用戶的個人資料蒐集、處理及利用之告知聲明（隱私權聲明）；以加強當事人的資料控制權取代當事人同意機制；建立用戶資料「去識別化」的參考標準或可行技術；要求業者設計讓用戶退出資料加值運用的機制。期從實體法律面及監管程序面借鏡國際實務作為，以此產出可供我國參酌的通訊傳播事業個人資料保護機制及管理模式。

關鍵詞：個人資料保護、隱私保護、通訊傳播事業、資料加值運用、大數據、智慧聯網

英文摘要

The rising development of internet, communication, and mobile device has brought the communication undertaking to a new era. Communication corporations now not only provide telecommunication and broadcast services, but also interact with their customers by internet and provide more customized service and targeted advertisement. In the meantime, corporations collect personal information, traffic data, location data, and itemised bill of their consumers while providing the service. Therefore, under the current trend of "Big Data" and "Internet of Things", these data are valuable to business enterprises.

However, value added service is related to the privacy and control of their personal data of data subjects. It should not be permitted without any regulations.

This research is to compare the regulation of other countries with the Personal Data Protection Act in Taiwan, and to address several suggestions of the protection of personal data while using those data for value added services, such as enhancing the regulation of privacy statement, enhance data owners’right of control of their personal data, establish the criteria of "Anynomisation", giving the "opt out" option to data owners.

Keywords：personal data protection, privacy, communication, value added service, big data, internet of things

目錄

表目錄

圖目錄

第一章 前言

第一節 背景說明與研究目的

一、個人資料的大數據分析應用具有誘因

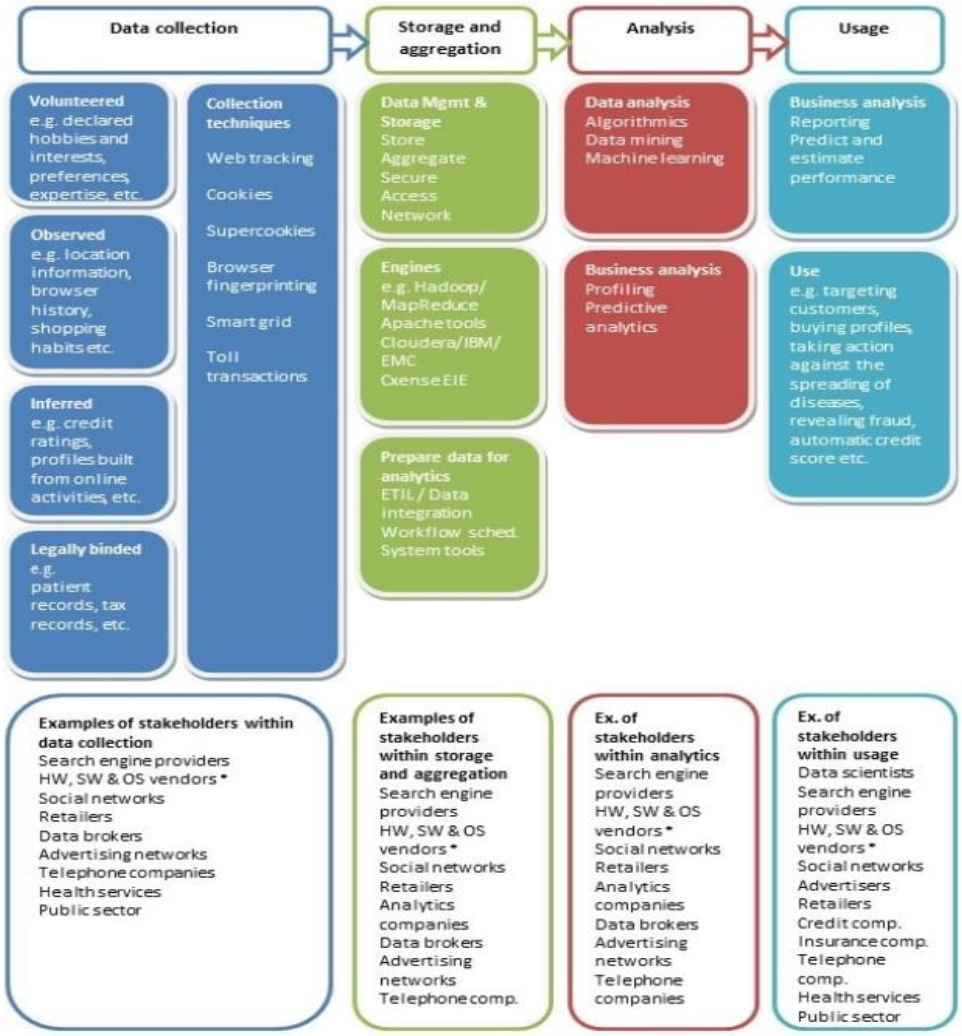
網路與通訊科技的變革及行動裝置的普及，使得通訊、傳播事業的界線已漸趨模糊，並且為通訊傳播事業帶來革命性發展。業者不再只是被動的提供電信、廣播服務，更能主動透過網路與用戶互動、提供客製化的服務及廣告資訊。同時，在大數據及智慧聯網的技術蓬勃發展的趨勢下，「資料加值運用」以達到「資料價值最大化」已成為國際潮流。用戶在使用通訊傳播業者的各項服務時，將因此提供或產出許多與用戶個人相關的資料，例如身分基本資料、通信紀錄、網頁瀏覽紀錄、位置資訊、帳單明細、收視紀錄等，對於通訊傳播業者無疑具有巨大的潛在商業價值。

舉例而言，日本電信業者 Wire and Wireless 推出分析服務平台（Analytics Services Platform ），協助客戶分析消費者洞察（Customer Insight）資訊，以精準鎖定行銷受眾；西班牙電信業者 Telefonica 也推出「Smart Steps」服務，以用戶的地理位置資訊為基礎，分析群眾行為以決定廣告投遞對象與區域。

國際上的個資與隱私保護組織觀察到此大數據與智慧聯網技術發展之勢，近年開始頻繁針對相關議題進行國際討論與頒布法令、指引以資因應。**國際電信個資保護工作小組（International Working Group on Data Protection in Telecommunications, IWGDPT）**於 2014 年 5 月召開的第 55

次會議中，即針對大數據時代下可能面臨的隱私爭議發布工作報告《Working Paper on Big Data and Privacy》[1]，將大數據價值鏈(Big data value chain)分為「資料蒐集」、「資料彙整」、「資料分析」、「資料運用」等四階段。

表 1 大數據價值鏈



（表來源：IWGDPT，《Working Paper on Big Data and Privacy》）

[1]IWGDPT, Working Paper on Big Data and Privacy, Privacy Principles under Pressure in the Age of Big Data Analytics (Skopje, 5./6. May 2014).

簡言之，通訊傳播業者對於用戶資料的加值運用至少有以下幾種方式：

1. 以瀏覽或收視紀錄分析用戶的喜好或關注商品、服務。
2. 以位置資訊分析用戶的足跡，辨別用戶的生活作息。
3. 以位置資訊鎖定用戶的地理位置進行廣告投遞。
4. 以帳單明細分析的使用習性及消費能力。
5. 將上述資訊與用戶之基本資料結合，加深用戶的屬性輪廓並標註用戶族群，並可進行精準廣告投遞。
6. 將大量用戶上述資訊串接統計，產出數據分析結果提供第三人（例如廣告商、廣告主）。
7. 將第三人（例如廣告商、廣告主）提供的個人資料與通訊傳播業者自己的用戶資料比對，回覆個別用戶的個人資料或群體用戶的統計資料。

然而，這些加值運用方式均涉及用戶對於其個人資料的「事前知情」、「事中控制」及「事後退出」等資訊隱私權、資訊自主權之憲法上基本權利，通訊傳播業者並不可漫無限制而在「服務契約」的必要範圍之外加值運用用戶資料。

二、個人資料保護法保障用戶的資訊隱私權及自主權

我國個人資料保護法於 2012 年 10 月施行，基於「保障當事人權利」並促進「個人資料合理利用」的立場，本法對於蒐集個資機關之蒐集、處理、利用個人資料等行為均設有規範，

且要求蒐集機關應針對所保有之個人資料檔案採取適當之安全措施，以確保不濫用、誤用個人資料，或發生其他個資侵害事故。例如個人資料保護法第 8 條、第 9 條要求蒐集機關須對資料當事人盡到「告知義務」，向資料當事人明確說明蒐集哪些個資、目的為何、利用方式為何、當事人權利為何，以此保障資料當事人的「知情權」；第 20 條規範蒐集機關受到「蒐集目的之限制」，僅能在原始蒐集個資之目的內利用資料當事人的個人資料；第 3 條及第 11 條賦予當事人可在特定情況下請求蒐集機關停止利用個人資料的權利。

凡此均影響通訊傳播業者在基於「契約關係」而合法蒐集用戶的個人資料後，可否及如何再合法「加值運用」用戶的個人資料，以發揮個人資料的最大商業價值。

三、法律的解釋空間讓業者難以因應

然而，個人資料保護法畢竟係針對各公務及非公務機關之規範，落實於各行各業對於執行職務或業務所涉及的個人資料時，法條的適用與解釋仍有爭議及窒礙之處，例如個人資料的定義、蒐集目的之範圍、書面同意的難以執行等，也因此本法在 2010 年修正後，為彙整業界意見並制定施行細則，遲至 2012 年方予施行，立法院又於 2015 年 12 月 15 日通過修正若干條文，包含刪除「當事人同意」的「書面」要式性，以因應網路時代的線上作業需求。

正由於個人資料保護法並非通訊傳播事業的特別法規定，在規範密度上自有不足之處，加上司法實務判決或主管機關的

解釋仍在少數，通訊傳播業者對於保有的用戶個人資料能否及如何加值運用實難以因應，一方面期望個人資料發揮最大價值，另一方面又顧忌動輒觸法，面臨高額的損害賠償或行政處罰，甚至是刑事責任，可謂「既期待又怕受傷害」。

四、主管機關應平衡保障用戶權利及業者利益

因此，通訊傳播事業應有契合於業務執行及法律規範的「個資保護機制及管理」準則以茲遵循，方可不致罔顧用戶的資訊隱私權及自主權，同時又可合法運用用戶之個人資料。

而就規管方式來看，我國目前尚未成立專責的「個資／隱私保護機關」，而是以法務部為個人資料保護法的主管機關，但針對各事業對於本法的因應則交由中央目的事業主管機關解釋、管理，並授權中央目的事業主管機關得指定蒐集機關「訂定個人資料檔案安全維護計畫」；而「資通安全管理法草案」第 22 條第 2 項同樣授權主管機關得指定蒐集機關訂定並實施「資通安全管理制度」，均是賦予主管機關強化管制的權限。

是以，國家通訊傳播委員會作為通訊傳播事業的主管機關，現階段亦肩負業者如何因應個人資料保護法的解釋、監督權限，如何對於業者採行適當監管以平衡保障用戶權利及個人資料的合理加值運用以達「資料效益最大化」，即有研究的必要。

五、研究目的

本研究之目的在於參考歐盟、德國、英國、美國及日本等國家或國際組織對於大數據與智慧聯網技術發展下的個資與隱私保護因應作為，特別對於通訊傳播事業加值利用用戶個人

資料的規範及管理方式進行分析，並提出可供我國參酌的因應措施，例如要求通訊傳播業者加強事前對於用戶的個人資料蒐集、處理及利用之告知聲明（隱私權聲明）；放寬業者取得用戶「同意」的合法方式，並搭配課以業者舉證責任；建立用戶資料「去識別化」的參考標準或可行技術；要求業者設計讓用戶退出資料加值運用的機制。是本研究期從實體法律面及監管程序面借鏡國際實務作為，以此產出可供我國參酌的通訊傳播事業個人資料保護機制及管理模式。

第二節　研究方法與進行步驟

本研究以「文獻比較分析」及「焦點座談」為主要研究方式，在 7 個月的計畫期間內，依序進行：

一、蒐集國內外法制與文獻資料

透過網路、圖書、期刊等管道蒐集國內外與通訊傳播事業個資保護規範管理機制相關之法制及文獻。

二、歸納各國個資保護機制與監理模式

彙整歐盟、英國、美國、德國、日本等國現行對通訊傳播事業個人資料保護之規範與監管模式。

三、分析通訊傳播事業面臨之個資保護衝擊

研究大數據及智慧聯網趨勢對於通訊傳播事業利用個資的衝擊及影響，包含個資保護重心的轉移、責任歸屬主體分析、開放資料及大數據（巨量資料）分析、智慧聯網等新型態觀念、技術與當事人隱私等權利的衝突、跨境傳輸的有關規定等。

四、研究各國因應措施

接續前章整理之議題，本章將產出國際實務對於大數據及智慧聯網趨勢下的個資/隱私保護之因應措施，包含法規（含修正草案）介紹、監理機制、去識別化要求、隱私衝擊評估、特定目的解釋範圍、第三方資料庫等。

五、整理我國個資法規範及業界因應現狀

分析我國個人資料保護法或相關法規（例如匯流五法草案）中關於本研究議題的規定，並依據我國通訊傳播事業涉及個人資料的特性，以及業者對於個資利用的需求（商業模式），分析業者對於用戶個資利用的法律問題點，同時整理業者的因應現況。

六、提出初步建議

綜整前述各章結論，提出通訊傳播事業合理利用個資之規管改革方向，包含增修法律、制定辦法、解釋實體要件等可資主管機關參考的方向。

七、廣徵學者專家意見

邀請學者專家及業界代表參與三次座談研討會及專家訪談，針對初步提出的規管方向提供意見。

八、彙整產出規管改革方向

依據研討座談會所得回饋增修研究報告，產出包含產、官、學三方的研究結論。

第二章 先進各國通訊傳播事業個人資料保護之機制

國際上對於個人資料與隱私的保護多分為基本法（例如個人資料保護法）與特別法（例如電信法）作為法律規範，並由主管機關針對該管事業制頒個資與隱私保護指引（例如隱私與電子通訊規則）。

以下將自歐盟的上位性規範起，就德國、英國、美國及日本等國家之基本法、特別法或相關指引中，與通訊傳播事業蒐集、處理、利用其用戶個人資料有關之規範臚列說明。

第一節 歐盟

一、個人資料保護指令（95/46/EC）[2]

(一) 背景

為保障歐盟境內自然人之基本權與自由，並建立會員國統一的隱私保護標準，歐盟於 1995 年制定《個人資料保護指令 95/46/EC》，要求會員國將其內涵修訂於內國法中，成為歐盟各國的一致性規範，以此衡平歐盟境內資料當事人的資訊隱私權（自主權）保障與個人資料的合理使用。

(二) 規範客體

本指令規範之客體為自然人之個人資料，其定義為「與可直接識別或經由身體、生理、精神、經濟、文化或社會身

[2]歐盟，《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》，見 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML，最後到訪日 105 年 4 月 14 日。

分等特徵而間接識別的自然人有關之資料」[3]，其客體範圍含括任何與可識別之自然人有關的資料，未區分該資料之內涵。惟針對「種族、道德背景、政治傾向、宗教、哲學信仰、所屬工會、健康紀錄、性生活」等更為敏感之特種個資則另有獨立規範之合法處理要件[4]。

值得注意的是，本指令特別在立法理由第 26 條指出，個資保護原則並不適用於「已無法辨識特定人的去識別化資料」，至於如何判斷該資料是否仍具識別性，則須依具體情況考量資料控制者或任何第三人所得採取的一切「合理、可能」之手段予以檢視[5]。

(三) 規範主體與行為

本指令適用之主體包含任何公、私部門之自然人及法人，（統稱為「資料控制者」）[6]，以及經資料控制者授權處理資

[3]歐盟，《Directive 95/46/EC》，Article 2（a），「'personal data' shall mean any information relating to an identified or identifiable natural person （'data subject'）; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity」。

[4]歐盟，《Directive 95/46/EC》，Article 8。

[5]歐盟，《Directive 95/46/EC》，Recital （26），「.....whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.....」。

[6]歐盟，《Directive 95/46/EC》，Article 2（d）。

料之人（稱為「資料處理者」）[7]。

規範行為則包含以自動化或非自動化方式對於資料之蒐集、記錄、組織、儲存、編輯、變更、檢索、諮詢、利用、傳輸、散佈、組合、封鎖、刪除及銷毀等行為[8]。

(四) 規範原則

1. 資料品質[9]

依本指令規範，資料控制者對於個人資料之處理必須公平且合法，須以明確之特定目的蒐集，且對於資料之處理必須適當、相關且不逾越蒐集目的，並應保持資料之完整與正確，亦須隨時更新當事人之個人資料。

2. 處理資料要件[10]

---

[7]歐盟，《Directive 95/46/EC》，Article 2（e）。

[8]歐盟，《Directive 95/46/EC》，Article 2（b）。

[9]歐盟，《Directive 95/46/EC》，Article 6。

[10]歐盟，《Directive 95/46/EC》，Article 7，「Member States shall provide that personal data may be processed only if：（a） the data subject has unambiguously given his consent; or（b） processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or（c） processing is necessary for compliance with a legal obligation to which the controller is subject; or（d） processing is necessary in order to protect the vital interests of the data subject; or（e） processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or（f） processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental

本指令於第 7 條規範資料控制者處理資料之要件，即僅在符合法定要件之一（例如為履行契約所必要、得到當事人同意、維護公益或合法利益等）時，始得合法處理當事人資料。

又本指令對於「當事人同意」特予定義為「資料當事人在被告知的前提下，依其自由意願所作出具體明確同意其資料被處裡的意思表示」[11]。

3. 告知義務[12]

本指令規定，資料控制者有義務向資料當事人告知其身分、蒐集個資的處理目的、對外提供個資的對象（或其類別）、強制性蒐集或自願性提供、當事人不提供資料的影響以及當事人權利等事項。

(五) 資料控制者責任[13]

本指令要求資料控制者須採取技術面及制度面之措施，以確保資料之機密與安全，並應約束受託之資料處理者亦遵守規範，且僅得於資料控制者指示之範圍內處理資料，以避免資料之洩漏、滅失、竄改或違法利用。

---

rights and freedoms of the data subject which require protection under Article 1 （1）.」。

[11]歐盟，《Directive 95/46/EC》，Article 2（h），「'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.」。

[12]歐盟，《Directive 95/46/EC》，Article 10、11。

[13]歐盟，《Directive 95/46/EC》，Article 16、17。

二、電子通訊隱私保護指令（2002/58/EC）[14]

(一) 背景

考量電子通訊事業在網路技術快速成長下所提供之科技服務發展，歐盟於 2002 年制定《電子通訊隱私保護指令 2002/58/EC》取代原 1997 年的《電信事業個資與隱私保護指令 1997/66/EC》，以符合電子通訊事業於網路時代所具備大量處理當事人資料並以此營利之能力所應有的規範。隨後亦因應發展而分別在 2006 年(Directive 2006/24/EC)及 2009 年（2009/136/EC）補充修正。

(二) 規範主體、行為與客體

本指令適用之主體為在歐盟境內提供公眾使用之電信服務業者；規範歐盟境內利用公共通訊網路、封包交換網路及網際網路中關於電子通訊服務之個人資料處理行為，客體包含訂戶與使用者之通訊資料、位置資訊等，並將法人的資料亦納入保護範圍。

1. 加值服務（Value added services）

本指令所稱之「加值服務」係指任何在通信服務之

[14]歐盟，《Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector （Directive on privacy and electronic communications）」，見 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML，最後到訪日 105 年 4 月 14 日。

外而須利用當事人的通信資訊或位置資訊的服務[15]。

2. 通訊資訊（Traffic data）

本指令所稱「通訊資料」係指任何基於在電子通訊網路中傳輸訊息之目的或為帳務計費之目的所處理產生之資料[16]。

而蒐集者原則上應於該此通信之目的完成或消失後，將通信資訊刪除或去識別化[17]，但如得到資料當事人的事先同意，則可保留通信資訊作為行銷產品或提供加值服務之用[18]。

3. 位置資訊（Location data）

本指令所稱之「位置資訊」係指在電子通訊網路中所處理產生，得以指示公眾電子通訊服務使用者所持終端設備之地理位置的任何資訊[19]。

而蒐集者僅能在將位置資訊去識別化或事先明確向

[15]歐盟，《Directive 2002/58/EC》，Article 2(f)。

[16]歐盟，《Directive 2002/58/EC》，Article 2（b），「"traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof」。

[17]歐盟，《Directive 2002/58/EC》，Article 6.1。

[18]歐盟，《Directive 2002/58/EC》，Article 6.3。

[19]歐盟，《Directive 2002/58/EC》，Article 2（c），「"location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service」。

資料當事人告知並取得同意的情況下，將位置資訊利用於提供加值服務；且資料當事人有權請求將特定時段連接網路的位置資訊納入資料利用的範圍[20]。

三、個資保護基礎規則（2012）

(一) 背景

自歐盟於 1995 年制定《個人資料保護指令 95/46/EC》以來已十餘年，為因應科技發展及隱私保障觀念的強化，歐盟擬增補對會員國關於個人資料保護的規範，遂於 2012 年提出《個資保護基礎規則 General Data Protection Regulation，GDPR》草案，加強對會員國處理當事人資料之約束，惟該規則仍強調僅為會員國基本法的規範，亦即如會員國本身對特定個人資料領域設有專法時，仍應優先適用該專法之特別規定。

本規則經過 3 年多的討論，終於在 2015 年 12 月 17 日由歐盟執委會、議會與理事會三方通過[21]。以下將介紹其中與本研究有關修正。

(二) GDPR 修正重點

1. 當事人同意

[20]歐盟，《Directive 2002/58/EC》，Article 9.1、9.2。

[21]見歐盟議會新聞稿，
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20151217IPR08112+0+DOC+XML+V0//EN，最後到訪日 105 年 4 月 14 日。

同意的「品質」應包含自由、特定、事前受告知以及具體透過聲明或行為實現來形成該意思表示，亦即排除擬制同意或選擇退出作為合法的同意方式。

2. 資料保護專員

對於主要業務即在大量、系統性蒐集、處理、利用個人資料之企業強制要求建置資料保護專員（Data Protection Officer）。

3. 隱私衝擊評估

如蒐集機關涉及高風險的資料蒐集，尤其是透過自動化方式處理個資的行為，即須強制要求於進行隱私衝擊評估。

4. 隱私保護內植設計及隱私保護預設

蒐集機關將有義務將隱私保護內植設計（Privacy by Design）及隱私保護預設（Privacy by Default）之原則落實於其產品或服務中。

5. 事故通知義務

個資侵害事故發生時，蒐集機關原則上應於 72 小時內通知個資保護的主管機關。

6. 可責性

蒐集機關有義務採取一切適當的技術面與管理面措施以符合本規則的要求。

7. 資訊告知

蒐集機關對當事人的通知須透明且易於取得。

8. 當事人側寫（Profiling）

當事人有權拒絕蒐集機關以其資料進行自動化側寫分析並以此對其作出決定。

9. 資料可攜

當事人有權要求蒐集機關交付可供其再利用之電子格式的個人資料檔案。

10. 請求刪除

在特定情形下，當事人有權要求蒐集機關即刻刪除其所有資料。

第二節　德國

一、聯邦個人資料保護法

(一) 背景

為保護個人免於因個人資料之流通而使其人格權受到損害，德國於 1977 年即制定《聯邦個人資料保護法》，最近期修正於 2009 年。

(二) 規範客體、主體與行為

本法保護之個人資料為「關於某特定或可得特定之人其個人或事物關係中的所有細節內容」，並將「種族、道德背

景、政治傾向、宗教或哲學信仰、所屬工會、健康紀錄及性生活」劃歸於「特種個資」範疇而有獨立規範要件。

適用主體包含所有公務機關與非公務機關，並規範其蒐集、處理及利用個人資料的行為。

(三) 規範原則：包含 1、資料縮減原則[22]；2、當事人同意原則[23]；3、透明原則[24]；4、目的限制原則；5、必要性原則。

(四) 資料當事人權利：包含 1、查詢權[25]；2、異議權[26]；3、更正、刪除與封鎖權[27]。

二、電信法

(一) 背景

德國於 2004 年制定電信法（Telecommunications Act，TKG），就國內電信事業作出規範，其中特於第 7 章第 2 節針對個人資料保護以專節規範。

(二) 重要內容

1. 當事人得以電子化方式表示同意[28]。

[22]德國，聯邦個人資料保護法，Section 3a。

[23]德國，聯邦個人資料保護法，Section 4a。

[24]德國，聯邦個人資料保護法，Section 4(3)。

[25]德國，聯邦個人資料保護法，Section 34。

[26]德國，聯邦個人資料保護法，Section 35。

[27]德國，聯邦個人資料保護法，Section 35。

[28]德國，電信法，Section 94。

2. 蒐集機關須事先取得當事人同意始得將其通信資訊用於行銷或提供加值服務之用[29]。

3. 蒐集機關須將當事人的位置資訊去識別化或事先取得其同意（當事人有權隨時撤回），始得將位置資訊利用於加值服務[30]。

三、電子媒體法

(一) 背景

德國電子媒體法（Telemedia Act，TMG）的適用範圍為電子資通訊服務，但排除電信法中的電信通訊及電信通訊支援服務[31]。

(二) 個資保護

依該法第 12 條規定，服務提供者僅得在本法或其他電子媒體相關法規的範圍及目的內蒐集、利用個人資料，或是取得當事人的同意[32]。

而該法亦規定，只要符合下列條件，則當事人的同意即得以電子方式為之[33]：

1、 當事人明確表示同意。

[29]德國，電信法，Section 96(3)。

[30]德國，電信法，Section 98(1)。

[31]德國，電子媒體法，Section 1(1)。

[32]德國，電子媒體法，Section 12。

[33]德國，電子媒體法，Section 13(2)。

2、該同意的紀錄能予以保存。

3、當事人可隨時存取該同意內容。

4、當事人得隨時撤回該同意。

四、邦際廣播電視條約

(一) 背景

德國對於廣播電視的監管係由各邦各自擁有管理權限，以個別的廣播電視法規範執照發放與其他管制措施。但為確保廣播電視規範的一致性，各邦之間亦協議批准邦際廣播電視條約（Interstate Broadcasting Treaty）

(二) 個資保護[34]

該條約雖於第 47 條針對個資保護制定規範，但係將經由廣播電視服務而蒐集、處理或利用的個資行為指回電子媒體法適用相關規範。

第三節　英國

一、個人資料保護法

(一) 背景

英國本於 1984 年及 1987 年即分別制定《個人資料保護法》與《個人檔案使用法》，惟在歐盟於 1995 年制定《個人資料保護指令 95/46/EC》後，英國為落實該指令意旨，遂於

[34]德國，邦際廣播電視條約，Article 47(1)。

1998 年制定現行之《個人資料保護法 Data Protection Act》，以規範國內所有涉及個人資料之蒐集、處理與利用行為。

(二) 規範原則

本法以附表 1 列舉之八大原則作為資料控制者應遵守之上位概念，任何涉及個資之行為皆應遵循下列原則[35]：

1. 合法且合理
2. 特定目的限制
3. 行為與目的間有充足關聯且不超過必要範圍
4. 資料正確與更新
5. 資料僅可於目的必要期間內保留
6. 尊重資料當事人權利
7. 採取適當措施防止個資事故
8. 除非符合要件，不得將國內當事人資料傳輸至歐盟經濟體以外之地區。

(三) 資料當事人權利：包含 1、資料查閱權[36]；2、停止利用權[37]；3、拒絕行銷權[38]；4、拒絕自動化決定權[39]；5、更正與

[35]英國，個人資料保護法，Schedule 1。

[36]英國，個人資料保護法，Section 7。

[37]英國，個人資料保護法，Section 10。

[38]英國，個人資料保護法，Section 11。

[39]英國，個人資料保護法，Section 12。

刪除權[40]。

(四) 資料控制者責任

資料控制者在本法規範下，有義務依照前述第 7 原則採取包括下列事項的適當措施以防止個資事故發生：

1. 對應個資性質與潛在威脅提供適當安全防護；
2. 採取必要措施以確保有權介接、存取、接觸個資之受雇人的可靠性；
3. 挑選對個資安全防護有足夠資格或能力的資料處理者以授權處理個資；
4. 在授權處理個資的情形中，資料控制者須與授權的資料處理者有書面協議，並使資料處理者僅能依照資料控制者的指示處理個資。

二、隱私與電子通訊規則

(一) 背景

除 1998 年的《個人資料保護法》外，英國又在 2003 年制定《隱私與電子通訊規則 The Privacy and Electronic Communications Regulations，PECR》，並於 2011 年修正。該規則將個人透過電信網路交換或傳輸之訊息納入保障，並針對行銷行為及各類電子通訊服務所產生之個人資料作出規範。

[40]英國，個人資料保護法，Section 14。

(二) 規範客體與行為

1. 行銷行為

本規則針對預錄訊息式電話行銷、真人對話式電話行銷、傳真行銷及電子郵件行銷定有規範。且英國電信事業主管機關 Office of Communications （OFCOM）亦設有「請勿來電名單」及「請勿傳真名單」，供民眾登記以拒絕接受行銷。

2. 瀏覽紀錄[41]

本規則規定，原則上不得於電信網路用戶或使用者之終端設備儲存或讀取資訊（例如利用 cookies 技術），除非符合例外的合法要件，例如在明確對用戶或使用者告知後取得其同意，而此「同意」可由用戶透過調整網頁瀏覽器的隱私設定或其他應用程式予以表示。

3. 通信資訊[42]

本規則定義之「通信資訊」係指「基於透過電信網路傳遞特定通訊之目的而處理的資料」，或「關於該特定通訊之計費而處理之資料」，包含通訊之線路、持續時間與通訊日期。

而電信業者除了為計費目的而處理用戶或使用者的流量資料外，僅得在「對用戶或使用者行銷其電信網路

[41]英國，隱私與電子通訊規則，Section 6。

[42]英國，隱私與電子通訊規則，Section 7。

服務或提供加值服務」或「事先取得用戶同意」等特定情況下使得處理流量資料。

4. 位置資訊[43]

本規則規範之「位置資訊」係指「任何透過電信網路處理，而能指出特定使用者所使用的終端設備所處之地理位置之資料」，包括該終端設備的經緯度與海拔高度、使用者行進軌跡，以及相關位置資訊被記錄的時間。

對於「位置資訊」僅在「用戶或使用者無法經由該資料被辨識」或「經用戶或使用者同意而為提供加值服務所必要」等特定情況下始得由電信業者處理。

第四節　美國

相較於歐盟傾向以「政府管制」之方式整體性的規範個資與隱私保護的框架，美國則奉行「自由市場」原則，將企業對於個資使用的議題交由資料當事人與資料蒐集者間基於契約自由原則自行協議解決，或由各產業自行訂定自律規範，僅在必要時以「部門立法」的方式針對不同產業制定個別的法律，並由主管機關頒布相關命令與規則。以下以與本研究相關法規舉例說明之。

一、電信法

(一) 背景

美國於 1996 年修正通過《電信法》(Telecommunication

[43]英國，隱私與電子通訊規則，Section 14。

Act），其中第 222 條規定「消費者的隱私保護」，針對電信事業使用用戶資訊的條件制定限制。

(二) 規範客體

本條規範的保護客體為「客戶專線資訊（Customer Proprietary Network Information，CPNI）」，包含「客戶基於與電信事業的電信服務契約關係而使電信事業取得之客戶的使用電信服務數量、技術規格、型態、目的地與總額之資訊」，以及「涉及客戶資訊的電話服務帳單資訊」，亦即電信事業在提供服務時所從客戶取得的資訊。

(三) 規範行為

依本條規定，電信事業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。然而，本條亦規定電信事業得在電信服務之目的外，利用「移除客戶識別資訊的複數客戶集合資訊」[44]。

二、消費者隱私權法草案

(一) 背景

美國於 2015 年提出的《消費者隱私權法》（Consumer Privacy Bill of Rights Act）草案，雖然主管機關為聯邦貿易委員會（FTC），但其規範內容卻有值得參考之處，如下述。

(二) 規範客體

[44]美國，電信法，Section 222(c)(3)。

草案所欲保護者為消費者之個人資料，在第 4 條 a 項第 1 款將「個人資料」定義為「在蒐集者控制下，且非一般合法公開來源可取得，而與特定個人連結或實際上可由蒐集者與特定個人連結，或與該個人有關或其經常使用之裝置連結的資料，包含但不限於 A 姓名；B 郵遞區號或電子郵件信箱；C 電話或傳真號碼；D 社會安全碼、稅籍號碼、護照號碼、駕照號碼或任何由政府編給之特殊編碼；E 生物特徵（例如指紋、聲紋）；F 永久識別碼，例如連網裝置號碼、金融帳戶號碼、信用卡號碼、健康照護帳號、消費帳號、車籍號碼、車牌號碼，以及用來存取個人帳號之安全碼、存取碼或密碼；G 與個人電腦或通訊裝置有關的特殊識別碼或描述資訊；H 由蒐集者蒐集、產生、處理、使用、揭露、儲存、維護而與特定個人連結或實際上可由蒐集者連結之資料」[45]。

然而，草案亦就前述個人資料定有例外，包含「A 去識別化資料，即蒐集者執行下列步驟：i 變更其內容使該資料具有合理基礎可期待不再與特定個人或裝置連結。ii 公開承諾不再企圖識別特定個人，並採取相關控制措施避免再識別。iii 以契約或其他具有法律強制力之方式規範揭露資料之對象不得企圖將資料連結至特定個人或裝置。iv 要求揭露資料之對象公開承諾不得企圖將資料連結至特定個人或裝置；B 已刪除之資料；C 員工資料；D 網路安全資料，即為了調查、

[45]美國，消費者隱私權法草案，2015，SEC 4(a)(1)。

降低或其他對應網路安全危險所須之個人資料」[46]。

(三) 規範行為

依草案規範，蒐集者原則上應於符合蒐集背景（reasonable in light of context）的情況下處理消費者個資[47]，如有超出蒐集背景時，則蒐集者應採取下列措施[48]：

1、 執行「隱私風險分析（privacy risk analysis）」，包含但不限於「審查個資來源、系統、資訊流、協力廠商等，並分析各種利用行為以檢視潛在的隱私風險。

2、 採行合理步驟降低已識別之隱私風險，包含但不限於「強化透明度及當事人控制」，即蒐集者應向當事人告知其超出蒐集背景外利用個資之情形，並規劃合理之方式使當事人得以決定是否降低在隱私風險中的曝險程度，以及規劃合理之控制機制使當事人得以執行降低曝險的選擇。而判斷告知與控制機制是否合理需考量：

(1) 告知置放的位置與能見度，需一併審酌展示告知的裝置的尺寸與容量。

(2) 告知出現的時機和頻率與個資被蒐集、使用、揭露之間的關聯。

(3) 蒐集者允許當事人行使控制權之方式與該告知之

[46]美國，消費者隱私權法草案，2015，SEC 4(a)(2)。

[47]美國，消費者隱私權法草案，2015，SEC 103(a)。

[48]美國，消費者隱私權法草案，2015，SEC 103(b)。

間的關聯。

然而上述措施亦有例外，依草案規範，當蒐集者在蒐集背景外「分析個人資料」時，如該行為是在（經 FTC 許可的）「隱私審查委員會（Privacy Review Board）」監督之下，並符合下列事項時，蒐集者將可無須採取額外措施[49]：

1、隱私審查委員會認定難以「強化透明度及當事人控制」。

2、隱私審查委員會認定蒐集者分析個資所生的潛在利益將不僅有利於蒐集者本身。

3、隱私審查委員會認定蒐集者已採取合理措施降低與該分析個資行為有關之隱私風險，包含「未強化透明度及當事人控制」之風險。

4、隱私審查委員會認定分析個資可能帶來的利益高於可能帶來的隱私風險。

三、寬頻網路服務業隱私規則

(一) 背景

美國聯邦通訊傳播委員會（FCC）在 2016 年 4 月 1 日公布一份「制定命令公告」（Notice of Proposed Rulemaking），針對「寬頻網路服務業（broadband internet service provider）」對於客戶的個資與隱私保護規範廣徵各界意見，其中若干具

[49]美國，消費者隱私權法草案，2015，SEC 103(c)。

有參考價值之規範內容臚列如下[50]。

(二) 定義

1、 客戶專線資訊

草案承接前述《電信法》第 222 條規定，將「客戶專線資訊（Customer Proprietary Network Information，CPNI）」作相同之定義，並舉例包含：服務方案資訊（服務類別，例如有線網路、光纖網路、行動網路；服務等級，例如網路速度；價格；流量，例如流量限制）、地理位置資訊、媒體存取控制（Media Access Control，MAC）位址或其他裝置識別碼、IP 位址及網域名稱資訊、流量資料。

2、 個人可識別資訊

考量各種個人資料相互關聯的本質，以及個資濫用或不當揭露的巨大風險，草案中刻意將「個人可識別資訊（Personal Identifiable Information，PII）」放寬定義為「與特定個人連結或得以連結之任何資訊」，亦即如果該資訊單獨或與他資料結合即可識別出特定個人，或該資訊合理的與特定個人的其他資訊有所關聯，則該資訊即屬草案定義的「個人可識別資訊」（...if it can be used on its own, in context, or in combination to identify an

[50]見 http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf，最後到訪為 105 年 4 月 13 日。

individual or to logically associate with other information about a specific individual.)。

在此定義下,草案中舉例個人可識別資訊至少包含:姓名、社會安全碼、生日及出生地、母親婚前姓名、政府編給的特別碼(例如駕照號碼、護照號碼、稅籍碼)、住址、電子郵件信箱或其他線上聯絡資訊、電話號碼、媒體存取控制(Media Access Control,MAC)位址或其他裝置識別碼、IP 位址、永久線上識別符(例如特殊的 cookies)、同名或非同名的網路身分、帳戶號碼及其他帳戶資訊、網路瀏覽紀錄、流量資訊、行動程式使用數據、當下與過往地理位置、財務資訊(例如金融帳戶號碼、信用卡或現金卡號碼、信用紀錄)、消費紀錄、醫療與健康紀錄、殘疾資訊、生物資訊、教育資訊、受雇資訊、與家人相關之資訊、種族、信仰、性取向、人口資訊以及可識別個人所屬財產之資訊(例如車牌號碼、裝置序號)。

3、 客戶專屬資訊

草案主要規範者為「客戶專屬資訊(Customer Proprietary Information,Customer PI)」,依草案定義,「客戶專屬資訊」即包含前述「客戶專線資訊」及「個人可識別資訊」。

4、 客戶聚合資訊

草案將「客戶聚合資訊(Aggregate Customer PI)」

定義為「與一群或一類服務或客戶相關，而已將個別客戶的身分與特徵移除的集合資訊（...collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.）」

(三) 行為規範

1、 事前告知

依草案規範，無論客戶透過親洽、線上、電話中或其他任何方式，業者均須在客戶訂購服務前，向客戶告知特定事項，該告知必須：

(1) 包含該寬頻服務須蒐集客戶專屬資訊之類別。

(2) 包含業者如何使用，以及在何種情況下將對外揭露何種類別的客戶專屬資訊。

(3) 包含業者將提供客戶專屬資訊之對象的類別，以及該接受資訊對象使用客戶專屬資訊之目的。

(4) 說明客戶在何種情況下可行使「選擇退出（Opt-Out）」或「選擇加入（Opt-In）」之權利。

(5) 向客戶解釋即便不同意業者在寬頻網路服務外使用、揭露或允許他人存取專屬資訊，亦不影響該服務的履行。但業者也可說明不同意存取專屬資訊對該客戶的影響。

(6) 向客戶說明任何同意（或撤回同意）、拒絕「業者

對於寬頻網路服務範圍外的專屬資訊之使用行為」均持續有效，直到客戶撤銷該次同意或拒絕為止。但業者亦須告知客戶，如有其他法律要求則不在此限。

(7) 易於理解且不可誤導。

(8) 清晰明確且須使用夠大的字體，同時須置放於客戶明顯可讀的位置。

(9) 如有必要須完整翻譯為他國語言。

除此之外，草案亦規範該告知必須經由業者的網站、行動裝置應用程式或其他與網站或應用程式相同功能的管道對客戶持續有效的揭露。

2、 隱私政策變更通知

依草案規範，業者在隱私權政策將有重大變更前，應事先向既有客戶通知特定事項，該通知必須：

(1) 經由「電子郵件或其他雙方同意的電子文件方式」、「客戶帳單」以及「業者的網站、行動裝置應用程式或其他與網站或應用程式相同功能的管道」向客戶明確通知。

(2) 向客戶以清楚、明確且易於閱讀的方式解釋：

A. 隱私權政策變更處，包含業者蒐集的客戶專屬資訊的變更，以及業者使用、揭露或允許他人存取該資訊的方式。

B. 客戶在何種程度內有權拒絕前述變更後的使用、揭露或允許他人存取，以及有權在任何時間拒絕或撤回對於存取專屬資訊之同意。

C. 客戶欲允許或拒絕存取專屬資訊之具體步驟。該通知必須明確讓客戶知悉任何拒絕之意均不影響客戶已訂購之服務。但業者也可說明不同意存取專屬資訊對該客戶的影響。如有必要，業者亦可向客戶說明如客戶允許使用專屬資訊，將可優化業者對客戶提供更多的精準行銷。

(3) 向客戶說明任何同意或拒絕「業者對於寬頻網路服務範圍外的專屬資訊之使用行為」均持續有效，直到客戶撤銷該次同意或拒絕為止。

(4) 易於理解且不可誤導。

(5) 清晰明確且須使用夠大的字體，同時須置放於客戶明顯可讀的位置。

(6) 如有必要，須將全部通知內容翻譯為他國語言。

3、利用客戶資訊之要件

草案將業者利用客戶資訊之行為區分不同類型，分別規範其合法要件：

(1) 無須當事人同意

依草案規範，業者在下列情況而使用或揭露客戶專屬資訊時，無須取得當事人同意：

A. 為提供寬頻網路接取服務所必要。

B. 為了與寬頻網路服務密切相關之行為，例如收費、技術支援等。

C. 為了保護業者或寬頻網路服務使用者免於詐欺、誹謗、或其他不法利用寬頻網路服務之行為。

D. 基於客戶主動要求並同意使用個資的自來行銷（inbound marketing）、轉介或行政服務。

E. 為避免客戶受到生命、身體等損害之緊急情況所須對有關單位提供支援。

F. 其他法律要求。

(2) 推定當事人同意

依草案規範，如客戶已向業者訂購某類服務（例如固網或行動上網），則業者可基於「行銷該類服務的額外服務」之目的利用客戶專屬資訊。

(3) 選擇退出或選擇加入之同意

依草案規範，在下列情況時，業者須取得客戶的「選擇退出（Opt-Out）」或「選擇加入（Opt-In）」之同意，始可利用客戶專屬資訊：

A. 利用客戶專屬資訊向該客戶行銷「與通訊業務相關之服務」。

B. 基於「行銷與通訊業務相關之服務」的目的，

使提供該相關服務之關係企業存取客戶專屬資訊，或將客戶專屬資訊揭露予提供該相關服務之關係企業。

(4) 選擇加入之同意

依草案規範,除前述條件之外,業者如欲使用、揭露或允許他人存取客戶專屬資訊時，均須事先取得當事人「選擇加入（Opt-In）」之同意。

(5) 同意之方式

依草案規範，業者須提供客戶簡單且便於執行的方式以隨時表達同意或撤回同意，而該方式必須向客戶明確揭露並永久可得，且客戶無須額外支付費用。

(6) 同意之前提—告知後同意

依草案規範,上述兩種同意方式的前提要件係業者的「合法告知」,告知內容包含：

A. 業者尋求客戶同意利用之專屬資訊的類別。

B. 利用專屬資訊之目的。

C. 業者欲揭露或提供存取客戶專屬資訊之對象或其類別。

(7) 客戶聚合資訊的使用與揭露

依草案規範，在符合下列條件時，業者可在提

供寬頻網路服務的必要範圍之外使用、揭露或允許他人存取客戶的聚合資訊，但須由業者負擔該聚合資訊中的客戶身分與特徵已被移除的舉證之責：

A. 確認該客戶聚合資訊無法以合理方式與特定個人連結。

B. 公開承諾保持並以非個人識別性的方式使用客戶聚合資訊，並承諾不以任何方式再識別該資訊。

C. 以契約方式禁止揭露或允許存取客戶聚合資訊的對象以任何方式再識別該資訊。

D. 以合理方式監督前述契約的有效遵循。

第五節　日本

一、個人資料保護法

日本對於非公務機關之個人資料保護重視業者的自律機制，其《個人資料保護法》僅於第四章規範非公務機關應遵循之個資保護最低義務，例如「目的限制原則」[51]、「誠實信用原則」[52]、「事前告知原則」[53]、「資料品質原則」[54]、「安全維護

[51]日本，個人資料保護法，Article 15、16。

[52]日本，個人資料保護法，Article 17。

[53]日本，個人資料保護法，Article 18。

[54]日本，個人資料保護法，Article19。

義務原則」[55]等。

至於各事業具體落實之個資保護規範面，則由內閣總理大臣於聽取消費者委員會之意見後，制定個資保護的「基本方針」[56]；再由各事業主管機關針對該管產業制定合於實際需求的個資保護指引（Guideline）[57]，由業者依其指引發展適宜的個資保護管理措施（例如下述之《電信事業個資保護指引》）。

二、電信事業個資保護指引

(一) 背景

日本對於電信事業蒐集、處理利用使用者資料的保護乃以《電信事業法》及《個人資料保護法》構成規範框架，但最重要的適用依據則為中央主管機關總務省於 1991 年制頒的《電信事業個資保護指引》，其後歷經諸次調整，最近一次修正則為 2015 年，由於此為目前國際上對於通訊傳播事業個資保護較新的實務規範，故本研究將其翻譯為中文，並臚列全文於附件 4。

(二) 規範客體與行為

本指引將個資區分為「一般個人資料」及「特殊個人資料」，針對前者參酌《個人資料保護法》的規定就「保存期限、目的限制、事先告知、對外提供個資、事故通報」等制

[55]日本，個人資料保護法，Article 20。

[56]日本，個人資料保護法，Article 7。

[57]日本，個人資料保護法，Article 8。

定要件；對於後者則為如下區分：

1. 通信履歷
2. 利用明細
3. 發信人資料
4. 位置資訊
5. 滯納支付費率者資料
6. 寄送垃圾郵件之用戶資料
7. 電話號碼資料

(三) 資料處理之共通原則

本指引於第二章規範個人資料的共通處理原則，例如：

1. 電信事業經營者取得之個人資料，原則上須以提供電信服務之必要時為限。
2. 電信事業經營者處理個人資料時，須儘可能限縮其使用目的；如欲變更使用目的時，不得逾越經認定與變更前使用目的之間具有一定關連性之合理範圍。
3. 電信事業經營者處理個人資料時，原則上不得在未經當事人事前同意下，逾越達成特定使用目的之必要範圍。
4. 電信事業經營者已變更使用目的時，須將變更後之使用目的告知當事人或公告週知。
5. 電信事業經營者處理個人資料時，原則上須在使用目的

之必要範圍內定出保存期間，在保存期間屆至後或達成使用目的後，須即刻刪除該個人資料。

(四) 特殊資料之處理原則

本指引於第三章針對特殊個人資料規範個別的處理原則，例如：

1. 電信事業經營者得記錄通信紀錄（使用者使用電信服務之日期時間、該通信之受信方及其他非屬通信內容而涉及該使用者通信之資訊）但原則上限用於收費、請款、處理客訴、防止非法使用及其他執行業務之必要範圍。

2. 電信事業經營者記載於使用明細（記載使用者使用電信服務之日期時間、該通信之受信方、對應之收費資訊及其他使用者使用電信服務相關資訊之書面）之範圍，不得逾越達成使用明細目的所需之必要限度。

3. 電信事業經營者除經使用者同意、根據法官核發之令狀或有其他阻卻違法事由外，不得將定位資訊（顯示行動終端設備持有者之資訊,而非發信方資訊)提供給他人。

(五) 資料控制者責任

1. 應公告事項

為確保資料當事人得以有效實行其資訊自主權，本指引規定電信業者應將下列事項置於當事人可得隨時得知之狀態：(1)電信業者名稱；(2)利用個資之目的；(3)當事人權利行使方式；(4)電信業者申訴窗口；(5)電信事

業如屬個資保護團體的事業時，該個資保護團體之名稱及申訴窗口。

2. 維護個人資料品質

本指引規定，電信事業經營者須在達成使用目的之必要範圍內，盡力維護個人資料之正確性及最新內容。

3. 安全維護

本指引規定，電信事業經營者須採行必要且適當之措施，以管理對個人資料之存取，限制攜出個人資料之方式，並防止來自外部之不法存取，同時避免個人資料外洩、滅失或毀損；而在採行安全管理措施時，須運用資訊通訊網路安全與信賴度標準等規範。

4. 委外監督

本指引規定，電信事業經營者將個人資料處理作業之全部或一部委外時，須對受託人採取必要且適當之監督措施，包含選擇經認定可妥適處理個人資料之受託人，並在委託契約中適度約定安全管理措施、保密、轉包之條件（是否允許轉包，以及如同意轉包時則要載明如何選擇轉包對象以及對轉包對象之監督等事項）、委託契約關係消滅時如何處理個人資料、未遵守契約內容時之處理方式及其他與個人資料處理相關之事項。

5. 管理與稽核

本指引規定，電信事業經營者須設置個人資料保護

管理人（該電信事業經營者下設個人資料處理之負責人員），由其擬定遵循本指導方針所需之內規，建立稽核機制並監督該電信事業經營者處理之個人資料。

6. 個資事故處理

本指引規定，如電信事業發生個資侵害事故時，應即時向受侵害的當事人通知，並基於避免侵害重覆發生，應將事故之資料公開，同時應向主管機關總務省報告。

第六節　本章結論

由本章所列國際實務可知，除德國於通訊傳播事業相關法律中設列個資保護章節，但仍以聯邦個人資料保護法作為基本規範外，英國在個人資料保護法外另有《隱私與電子通訊規則》，日本政府亦訂有《電信事業個資保護指引》，至於採部門式立法的美國則由各主管機關於所轄目的事業法律中針對個資或隱私保護訂有規範，自不待言。

我國現行仍以一部個人資料保護法但由各中央目的事業主管機關分別管理的模式執行監管，將來可參考國際先例，以通訊傳播事業個資保護專法或法規命令的方式，考量事業的特性及需求制訂規範。

第三章 先進各國通訊傳播事業個人資料保護之監理模式

第一節 歐盟

一、個人資料保護指令（95/46/EC）

歐盟個人資料保護指令於第 28 條第 1 項規定各成員國應定有一個以上公務機關，獨立監督個資保護法制之施行；其職權包含[58]：

1. 採取行政措施時，應與當事人進行協議。
2. 具有調查、監督職務而取得必要資料之權限。
3. 勸告、命令刪除或禁止處理個資檔案之權限；警告或懲戒管理者之權限。
4. 得提起訴訟或將其通知司法機關之權限。
5. 接受當事人請求調查之權限。

二、歐洲理事會

歐洲理事會（Council of Europe）第 108 號追加議定書第 1 條第 1 項中明訂締約國應設置一個或複數具有責任，確保履行為條約基本原則之國內法措施實行之機關。同條第 3 項規定獨立機關應完全獨立行使權限。而第 1 條第 2 項明定其權限為：具有調查、介入、訴訟程序之權力，同時應聽取任何人關於其

[58]歐盟，《Directive 95/46/EC》，Article 28。

個人資料之權利及基本自由之申訴。

在歐洲議會各成員國協議定立之保護個資國際協定，其中均有要求各會員國設置具有調查權限、仲裁權限等「監督機關」（Supervisory authorities）之專章，為依個資法設置獨立監督機關之法律依據，獨立監督機關已為歐洲各國建置個資法制時必要機關[59]。

三、資料保護及隱私委員會議

個資保護先進國間之資訊官員為交換各國執行個資與隱私保護法規之經驗及意見而召開之會議，限於設有獨立、自主個資或隱私保護監督機關國家之資訊官員始得參加每年所舉辦之國際會議（International Conference of Data Protection and Privacy Commissioners，ICDPPC）；在此會議上，各國討論並通過有關個資或隱私保護之國際基準、尋求隱私保護與經濟成長之衡平議題等，係國際間交換個資保護法制相關意見、建立合作關係之重要平台[60]。

四、小結

由上可知，在歐盟規範下，各會員國有義務設置個資或隱私保護的專責主管機關以負責國內個資與隱私保護法規的監管與落實。同時對歐盟而言，其他國家亦須具備個資或隱私保

[59]國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 189。

[60]國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，2015 年，頁 189。

護的專責主管機關，始符合歐盟認定「充足」個資與隱私保護的門檻，方得參加「資料保護及隱私委員會議」，甚至始符合歐盟對於跨境傳輸接受國的個資與隱私保護基本要求。

第二節　德國

依據聯邦個人資料保護法之規定，德國對於個資保護之監管係採立法建置中央的「聯邦資料保護與資訊自由監察官（Federal Commissioner for Data Protection and Freedom of Information）」[61]與各邦的「資料保護監察機構（Supervisory authority）」[62]之主管機關監管，以及要求非公務機關設置「資料保護監察人（Data protection official）」[63]之內部控管，並鼓勵非公務機關採行外部稽核取得個資或隱私保護驗證之自律機制[64]。

而就通訊傳播事業而言，以電信業者為例，德國電信法（TKG）第 115 條第 4 項即將電信業者蒐集、處理、利用個人資料之行為交由聯邦資料保護與資訊自由監察官依聯邦個人資料保護法之規定予以監管[65]。

一、主管機關監管

(一) 聯邦資料保護與資訊自由委員

德國聯邦個人資料保護法於第二部第三章規範設置

[61]德國，聯邦個人資料保護法，Part 2，Chapter 3。

[62]德國，聯邦個人資料保護法，Part 3，Chapter 3。

[63]德國，聯邦個人資料保護法，Section 4f。

[64]德國，聯邦個人資料保護法，Section 9a。

[65]德國，電信法，Section 115(4)。

「聯邦資料保護與資訊自由委員（聯邦委員）」，作為聯邦層級的獨立主管機關，主要職權在於監管德國公務機關的個資保護適法性遵循，包含下列項目：

1. 受理申訴[66]

依聯邦個人資料保護法規定，任何人如認為其權利因公務機關蒐集、處理或利用其個人資料而受到侵害時，均可向聯邦委員提出申訴。

2. 監察及提供建議[67]

聯邦個人資料保護法第24條授予聯邦委員對公務機關蒐集、處理、利用個人資料之監察權限，並明文規定其範圍包含公務機關所涉及關於人民的郵務與電信通訊之個人資料[68]。而各公務機關均有義務配合聯邦委員的監管調查行為[69]。

同時，聯邦委員對於公務機關之缺失選擇不提出糾正（見下述）而以提出改善建議的方式代替[70]。

3. 糾正[71]

[66]德國，聯邦個人資料保護法，Section 21。

[67]德國，聯邦個人資料保護法，Section 24。

[68]德國，聯邦個人資料保護法，Section 24 (2)1。

[69]德國，聯邦個人資料保護法，Section 24 (4)。

[70]德國，聯邦個人資料保護法，Section 24 (5)。

[71]德國，聯邦個人資料保護法，Section 25。

聯邦個人資料保護法第25條授權聯邦委員在發現公務機關違反相關個人資料保護法令時，有權對該機關提出糾正並限期改善。但如該公務機關在期限內改善並回覆其補救措施，或申訴告知該違反事實情節輕微時，聯邦委員亦有權撤銷該糾正[72]。

4. 提出報告[73]

聯邦個人資料保護法第 26 條第 1 項規定，聯邦委員應每兩年就個資保護領域的重要發展提出報告。

5. 專家意見與調查[74]

依聯邦個人資料保護法第 26 條第 2 項規定，聯邦委員有義務依聯邦眾議院或聯邦政府的要求，就個資保護事項提供專家意見，並依聯邦眾議院、請願委員會、內政委員會或聯邦政府之請求，對個資保護事務啟動調查。

6. 機關合作[75]

依聯邦個人資料保護法第 26 條第 4 項規定，聯邦委員有義務與各邦監管個資保護的公務機關合作，其中包含各邦的監管機關（見下述）。

[72]德國，聯邦個人資料保護法，Section 25 (2)、(3)。

[73]德國，聯邦個人資料保護法，Section 26 (1)。

[74]德國，聯邦個人資料保護法，Section 26 (2)。

[75]德國，聯邦個人資料保護法，Section 26 (4)。

(二) 各邦資料保護監管機關

德國聯邦個人資料保護法於第三部第三章規範各邦政府或其授權之機關設置「(資料保護)監管機關」,負責執行非公務機關之個人資料保護事項[76]。而監管機關之名稱及其設立依據則得因邦而異[77]。其主要職務如下:

1. 受理申訴[78]

與聯邦委員之職權相同,依聯邦個人資料保護法規定,任何人如認為其權利因非公務機關蒐集、處理或利用其個人資料而受到侵害時,均可向監管機關提出申訴。

2. 監察及提供建議[79]

監管機關亦有權監察非公務機關蒐集、處理、利用個人資料的合法性,並對非公務機關及其資料保護監察人(Data Protection Official)主動提供適法性建議或請求提供必要協助。

3. 侵害通知[80]

依聯邦個人資料保護法第 38 條第 1 項規定,監管

[76]德國,聯邦個人資料保護法,Section 38 (6)。

[77]科技部,《德國資訊監察制度之研究—兼論運用在我國之可行性》,103 年,頁 15。

[78]德國,聯邦個人資料保護法,Section 38 (1)。

[79]德國,聯邦個人資料保護法,Section 38 (1)。

[80]德國,聯邦個人資料保護法,Section 38 (1)。

機關如發現非公務機關有違反相關個資保護法令時，應通知侵害的當事人，並告知應承擔追訴或處罰責任的該等非公務機關。

4. 發布報告[81]

依聯邦個人資料保護法第 38 條第 1 項規定，監管機關應定期至少每兩年對其執行個資保護事項發布業務報告。

5. 糾正與免職[82]

為確保非公務機關落實個資保護，監管機關有權命令非公務機關採取適當的蒐集、處理、利用個資之程序，或是技術面、組織面之具體要求，以改善個資保護之缺失。而若非公務機關未於監管機關下達命令或處以罰鍰後於於期限內改善，則監管機關有權禁止其蒐集、處理或利用個人資料。另監管機關如認為非公務機關所選任之資料保護監察人不適任時，亦有權予以免職。

二、自律機制

(一) 資料保護監察人[83]

聯邦個人資料保護法第 4f 條規定，以自動化方式處

[81]德國，聯邦個人資料保護法，Section 38 (1)。

[82]德國，聯邦個人資料保護法，Section 38 (5)。

[83]德國，聯邦個人資料保護法，Section 4f。

理個人資料之公務或非公務機關，均應以書面指派資料保護監察人；以其他方式蒐集、處理、利用個人資料，但雇用至少 20 人執行該行為之機關亦同。但至多雇用不超過 9 人以負責自動化處理個人資料之非公務機關則不在此限[84]。惟此類無須指派資料保護監察人之機關則須由機關負責人以其他方式有效履行資料保護監察人之義務[85]。

資料保護監察人可以為機關外部之人，但須具備與該機關蒐集、處理、利用個人資料之程度、規模相稱之專業能力始得擔任[86]。又資料保護監察人應直屬於機關負責人，且有完整權限自由行使其職權，機關並應提供其必要之訓練與一切協助，以確保其專業能力[87]。

而資料保護監察人之職權在於監督機關蒐集、處理、利用個人資料的行為適法性，並採取適當之措施強化機關落實法令遵循。為達此目的，資料保護監察人有權向該管資料保護主管機關請求諮詢[88]。

此立法要求機關設置資料保護監察人之規定，可謂結合自律與他律之性質，論者即認為「資料保護監察人一方面似代監督機關之責，作為企業內部的『獨立單位』，管控企業內部在個人資料保護之運作情況，並與監督機關

[84]德國，聯邦個人資料保護法，Section 4f (1)。

[85]德國，聯邦個人資料保護法，Section 4g 2(a)。

[86]德國，聯邦個人資料保護法，Section 4f (2)。

[87]德國，聯邦個人資料保護法，Section 4f (3)、(5)。

[88]德國，聯邦個人資料保護法，Section 4g (1)。

保持密切的聯繫，提供一雙向溝通之管道；另一方面，其作為各企業對外在個人資料保護業務上的專責單位，擔負建立企業內部個人資料保護體系的重責大任，包括建立員工在個人資料保護領域應有之先備知識；處理因個人資料蒐集、處理、利用而生之事件並提供諮詢；配合科技與法律發展隨時確保企業個人資料保護之強度與密度等」[89]，對於個資保護之監管實具有重要功能。

(二) 外部稽核

除要求機關設置內部資料保護監察人外，德國聯邦個人資料保護法亦鼓勵機關導入外部稽核。第 9a 條規定「為強化資料之保護與資料之安全，資料處理系統或程式之提供者及資料處理單位，對於資料處理之概念及技術上之設備，得接受獨立及經驗證之專家進行檢驗及評價，並公開其檢驗結果（第 1 項）。檢驗及評價之詳細規定、程序及專家之選擇及驗證，另以法規定之（第 2 項）」[90]，亦即德國聯邦個人資料保護法鼓勵機關接受公正、專業之第三方機構執行個資保護之外部稽核，甚至取得國際認證標章。

[89]國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 193。

[90]國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 191。

三、小結

總體來看，德國對於公務及非公務機關的個資保護監管均以聯邦個人資料保護法做出規範，除設置「聯邦資料保護與資訊自由委員」及各邦「資料保護監管機關」之外，亦要求機關指派合格的內部「資料保護監察人」。在通訊傳播事業中，以電信業為例，亦是於電信法中將個資保護監管之權限授由聯邦個人資料保護法之規範處理，可謂是集中式的統一管理機制。另外，每兩年提出執行個資保護事項發布業務報告一節，亦有效對於個資保護執行成效給予定期檢視精進之機會。

第三節　英國

英國對於個人資料保護亦設置獨立之主管機關 Information Commissioner Office（ICO）監管，統一負責公務及非公務機關之個資保護因應，並依職權發布各領域、業務之個資保護準則（codes of practice）供機關自律遵守，且近年更研議推行 ICO 的個資及隱私保護認證標章。

一、主管機關監管

(一) 資訊委員辦公室（ICO）

英國於個人資料保護法（Data Protection Act）第 6 條創設「資訊委員（Information Commissioner）」一職，並於附表 5 中明訂其組織、人員與預算。其主要職權為：

1. 制定個資保護準則

依英國個人資料保護法第 51 條規定，資訊委員應

在徵詢商業公會或資料當事人(或其代表)之意見後，針對其認為適當之領域或業務制定「個資保護準則（codes of practice）[91]，或鼓勵商業公會推廣其自行制定之個資保護準則[92]。

2. 適法性評估

資訊委員亦可在得到蒐集機關同意的情況下，對該機關蒐集、處理、利用個人資料的行為評估其適法性，並將評估結果告知該機關[93]。

3. 發出執行通知、資訊請求通知或第三人資訊請求通知

依英國個人資料保護法第 40 條規定，如資訊委員認定蒐集機關有違反個人資料保護法之情事時，得對該機關發出「執行通知（Enforcement Notices）」，要求其於期限內採取特定之行為，或於期限屆滿後禁止進行特定之行為，甚至是在期限屆滿後禁止蒐集、處理、利用個人資料之（特定）行為[94]。該執行通知之內容應包含該機關違反之法律內容及資訊委員認定之理由，並須告示其救濟方式[95]。

此外，英國個人資料保護法第 43 條（經英國 2003

[91]英國，個人資料保護法，Section 51 (3)。

[92]英國，個人資料保護法，Section 51 (4)。

[93]英國，個人資料保護法，Section 51 (7)。

[94]英國，個人資料保護法，Section 40 (1)。

[95]英國，個人資料保護法，Section 40 (6)。

年隱私與電子通訊規則附表 1 第 4 條修正）亦規定，資訊委員可基於調查蒐集機關是否遵循個資保護法令要求之目的，對該機關發出「資訊請求通知（Information Notice）」，合理要求該機關提出必要之資料與證據[96]。

又英國 2011 年隱私與電子通訊規則第 12 條於 2003 年隱私與電子通訊規則中新增第 31A 條規定，資訊委員有權對通訊業者（communication provider）發出「第三人資訊請求通知（Third Party Information Notice）」，要求其提供第三人使用電子通訊網路或電子通訊服務的必要相關資料，以供資訊委員調查他人是否遵循該規則的規範[97]。

而若收受執行通知、資訊請求通知或第三人資訊請求通知之機關未遵守通知之要求，則將視為是犯罪行為[98]，但該機關得舉證證明已盡一切努力遵循通知之要求[99]；又該機關若對資訊委員的資訊請求或第三人資訊請求基於故意或重大過失而舊重要事項提出虛假資訊者，亦視為犯罪行為[100]。

4. 稽核安全措施

[96]英國，隱私與電子通訊規則 2003，Schedule1，Section 4(a)。

[97]英國，隱私與電子通訊規則 2011， Section 12。

[98]英國，個人資料保護法，Section 47 (1)。

[99]英國，個人資料保護法，Section 47 (3)。

[100]英國，個人資料保護法，Section 47 (2)。

依英國 2011 年隱私與電子通訊規則第 4 條第 2 項新增 2003 年隱私與電子通訊規則第 5 條第 6 項規定，資訊委員有權稽核電子通訊服務業者所採取的資料安全保護措施是否合於要求[101]。

5. 提出業務報告

依英國個人資料保護法第 52 條規定，資訊委員應每年定期向國會提出該年度之業務報告，或不定期在其認為適當時向國會提出執行報告[102]。資訊委員亦應在制定各項個資保護準則時向國會提出報告[103]。

(二) 通訊傳播辦公室（OFCOM）

英國的通訊傳播事業主管機關為依 2002 年《Office of Communications Act》設立的「通訊傳播辦公室（Office of Communications，OFCOM）」，負責執行監管英國的《通訊傳播法（Communication Act 2003）》。其主要職責在於「確保多種型態之電子通訊服務普及」、「確保高品質廣播電視服務普及，且符合大眾品味及興趣」、「確保廣播電視服務內容由不同機構提供」、「保護閱聽眾免於不當內容的侵犯與傷害」、「保護閱聽眾免於不公平或隱私被侵害」、「郵政服務普及化」，以及「無線頻譜使用效率極大化」

[101]英國，隱私與電子通訊規則 2011， Section 4 (2)。

[102]英國，個人資料保護法，Section 52 (1)、(2)。

[103]英國，個人資料保護法，Section 52 (3)

等 7 大任務[104]。

然而，雖然英國通訊傳播法第 14 條第 6 項第 e 款規範通訊傳播辦公室應針對避免當事人隱私遭不當侵害的事項進行研究[105]，但由於英國設有前述的個資與隱私保護主管機關資訊委員辦公室，且相關個資與隱私保護法令亦將監管權限劃為資訊委員辦公室之職權，是以對於通訊傳播事業於提供服務過程中涉及的個資與隱私保護事項，仍歸屬資訊委員辦公室管理。

二、自律機制

(一) 個資保護準則

如前所述，英國資訊委員辦公室除自行制定個資保護準則外，亦鼓勵各產業自行制定合於該產業之個資保護準則並積極推廣[106]。就《隱私與電子通訊規則》而言，資訊委員辦公室即曾發布《Guide to the Privacy and Electronic Communications Regulations》[107]及《Audit：a guide to ICO privacy and electronic communications regulations audits》[108]，供業者作為遵循與稽核之指引。

---

[104]國家通訊傳播委員會，《以英國通訊傳播法之研訂及推動為典範，研究我國匯流法制定與推動之可行方向》，104 年公務人員出國專題研究報告書，頁 18。

[105]英國，通訊傳播法，Section 14 (6) (e)。

[106]英國，個人資料保護法，Section 51 (4)。

[107]見 https://ico.org.uk/media/for-organisations/guide-to-pecr-2-1.pdf，最後到訪日 105 年 4 月 14 日。

[108]見 https://ico.org.uk/media/for-organisations/documents/2784/guide-to-ico-pecr-audits.pdf，最後到

(二) 隱私認證

除了積極發布個資保護準則之外，英國資訊委員辦公室亦於近年著手推動國家級的隱私認證標章（Privacy Seals），並鼓勵各機關導入認證取得該標章以建立市場信任。資訊委員辦公室預計將於 2016 年完成該認證標準並正式發布[109]。

三、小結

綜上所述，英國係以獨立組織「資訊委員辦公室」作為公務與公務機關的個資與隱私保護主管機關，統一規範個資保護法令的遵循事項。同時資訊委員辦公室亦就各產業發布個資保護準則，並鼓勵業界自行制定相關指引。

此外，資訊委員辦公室也定期舉辦個資保護遵循的推廣活動，本研究團隊成員即於 2015 年 3 月前往英國曼徹斯特參與資訊委員辦公室舉辦的「2015 年隱私保護實務研討會」，與會人員包含公務與非公務機關的個資及隱私保護實務工作者，內容則分為「專題演講」、「小組議題研討」及「展場攤位推廣」等，可供我國借鏡。

第四節　美國

以強調「市場機制」作為自律原則的美國，並未設置統一的

訪日 105 年 4 月 16 日。

[109]見 https://ico.org.uk/for-organisations/improve-your-practices/privacy-seals/，最後到訪日 105 年 4 月 14 日。

個資或隱私保護主管機關，而係由各目的事業主管機關依其所屬權責之法律而對該管事業進行監督。就通訊傳播事業而言，即由聯邦通訊傳播委員會（Federal Communications Commission ，FCC）與聯邦貿易委員會（Federal Trade Commission，FTC）為主管機關，以下分述之。

一、聯邦通訊傳播委員會

聯邦通訊傳播委員會係依美國 1934 年的《通訊傳播法（Communications Act of 1934）》所設立，其主要職權依據尚包含 1996 年的美國電信法（Telecommunications Act of 1996），負責規範美國州際及境內所有非政府使用之通訊，包括有線電、無線電、衛星通訊，電信頻率以及媒體業者的管理、電信執照的發放、電信資源之公平合理提供、電磁波使用之安全、通訊傳播產業競爭之監理等等[110]。主要職權為[111]：

(一) 規劃非聯邦政府使用之電波頻譜（Frequency Spectrum）及核配電台、轉播站頻率及執照。

(二) 制定相關法規以管理電波頻率，以避免干擾。

(三) 制定節目錄製、傳輸功率、聯播網等管理規則。

(四) 制訂法律、發放執照和執行法律。

(五) 要求電台應遵守國際法規。

[110]行政院研考會，《美、英、德、新獨立機關之研究》，98 年，頁 14。

[111]交通部電信總局，《電信資訊傳播協調工作小組出國考察》，90 年，頁 8。

(六) 以罰鍰（fine）、吊照（Suspending Licenses）、臨時照（TemporaryLicense）、及停播（Taking Station off Air）等行政罰，核處違反電信法者。

(七) 除了涉及猥褻（obscenity）、賭博（lotteries）、誇大不實廣告（Deceptive Commercials）及違反爭議性議題及公平播出原則之廣播內容外，基本上不管控傳播內容。

其中就「制定法規、行政命令」的過程來看，係由發布「制定命令公告」（Notice of Proposed Rulemaking ）或「諮詢公告」（Notice of Inquiry）開始。「制定命令公告」包括目標議題的討論、為解決該議題而提出的行政命令草案，以及通常包括該草案之基礎說明。利害當事人可在通知發布前與聯邦通訊傳播委員會進行溝通，以影響行政命令草案之內容，但「制定命令公告」發布後有法定的陳述意見期間，因此在任何行政命令生效前，縱非相關當事人亦有加以評論之機會[112]。

舉例而言，聯邦通訊傳播委員會即於 2015 年 5 月發布執行建議（FCC Enforcement Advisory），對提供寬頻服務的 ISP 業者提出保護用戶隱私的意見[113]，後又於同年 11 月表示將盡速針對寬頻業者保護用戶隱私制定規範並發布「制定命令公告」

[112]國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 225。

[113]見 https://apps.fcc.gov/edocs_public/attachmatch/DA-15-603A1.pdf，最後到訪日 105 年 4 月 14 日。

[114]。

二、聯邦貿易委員會

聯邦貿易委員會係依美國 1914 年《聯邦貿易委員會法（Federal Trade Commission Act）》所設立，目的在於防止商業活動競爭的不公平手段，以維持市場的公平運作及確保消費者權益，主要業務職掌包括執行反托拉斯法、保護消費者權益及報告與諮詢[115]。

聯邦貿易委員會於 1995 年開始處理消費者隱私議題，最初基於政府管制將限制自由市場發展，因此鼓勵產業自行訂定自律規範，但仍由聯邦貿易委員會執行。是以聯邦貿易委員會係具有「自律」機制之監管功能[116]。

目前聯邦貿易委員會主要係依《聯邦貿易委員會法》第 5 條「禁止商業中或影響商業進行的不公平或欺罔行為」為其處理消費者隱私保護議題之法源依據[117]。例如在 FTC v. Accusearch Inc.案中[118]，聯邦貿易委員會主張 Accusearch Inc. 以不實的偽裝、虛偽的陳述、欺騙的聲明、欺騙或偷來的文件、或其他不實的陳述之方法（包括偽裝為電信事業之用戶）而誘

[114]見 https://www.huntonprivacyblog.com/2015/11/09/fcc-to-tackle-issue-of-broadband-privacy/，最後到訪日 105 年 4 月 14 日。

[115]行政院研考會，《美、英、德、新獨立機關之研究》，98 年，頁 14。

[116]國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 227。

[117]美國，聯邦貿易委員會法，Section 5。

[118]2007 WL 4356786 （D. Wyo. Sept. 28, 2007）, aff'd, 570 F.3d 1187 （10th Cir. 2009）

使電信事業員工或代理人揭露應保守祕密的用戶電話紀錄，即未經用戶知悉及同意而取得「用戶專屬線路資訊」並將其販售與第三人。在該案審理中，第十巡迴法院亦認定以欺罔方式蒐集個人資料乃構成「不公平」交易慣例，即與聯邦貿易委員會之意見相符[119]。

三、小結

整體而言，美國對於個資與隱私保護係採分散式管理，由各主管機關依據主管之法規對所轄產業進行監管，此方式與我國目前由各中央目的事業主管機關各自監督該管事業的個人資料保護法令遵循性頗為類似。

第五節　日本

日本對於個人資料之保護重視各產業之自律，以個人資料保護法作為公務及非公務機關於蒐集、處理、利用個人資料均應適用之基本法，又兼採公務及非公務機關分別規範之立法方式，強調規範自主性、機制結構之雙層（或三層性）、個人資訊之透明性以及規範之必要最小限度等精神[120]，亦即主管機關得依民間產業之性質，制定合適的個人資料保護規範供業者遵循。

一、主管機關監管

日本個人資料保護法規定由各中央事業主管機關（主務大

[119]國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 231。

[120]林素鳳，《日本現行個人資訊保護法制初探》，94 年，警大法學論集，第十期，頁 46。

臣）監管其所轄事業的個資保護遵循，其主要職權包括：

(一) 要求提出報告[121]

在確保業者遵循個人資料保護法義務的必要範圍內，主管機關有權要求業者提出與此相關之報告。

(二) 提供建議[122]

在確保業者遵循個人資料保護法義務的必要範圍內，主管機關亦得對該業者提出適法性建議。

(三) 勸告及命令[123]

當業者違反個人資料保護法規範之義務時，主管機關有權對該業者提出勸告以採取適當措施停止該違反情形以保護當事人權益。

若該業者無合法理由不採納主管機關之勸告且主管機關認為當事人的權益即將遭受嚴重侵害時,便可命令業者遵循主管機關之要求。

(四) 緊急處分[124]

當主管機關認為當事人權益因業者違反個人資料保護法義務而有遭到侵害的急迫危險時,得不經勸告逕行命

[121] 日本，個人資料保護法，Article 32。

[122] 日本，個人資料保護法，Article 33。

[123] 日本，個人資料保護法，Article 34 (1)、(2)。

[124] 日本，個人資料保護法，Article 34 (3)。

令業者採取必要之措施以改正該違法行為。

二、自律機制

(一) 基本方針與個資保護指引（Guideline）

依日本個人資料保護法第 7 條規定，為達到個資保護整體發展之目的，內閣總理大臣應於聽取消費者委員會之意見後，制定個資保護的「基本方針」[125]；又依第 8 條規定各事業主管機關亦須針對該管產業制定合於實際需求的個資保護指引（Guideline）[126]，由業者依其指引發展事宜的個資保護管理措施。

(二) 個資保護團體

為推廣民間業者對於個資保護的自律機制，日本個人資料保護法於第四章第二節訂定「認定個資保護團體」制度[127]，由民間團體向主管機關申請取得認定後，便可以主管機關頒布之個資保護指引為基礎，依產業之特性訂立具體、適切之「個資保護指針」，以供團體成員共同遵守[128]。

而取得認定之個資保護團體亦可執行 1、處理有關其成員在處理個資上發生之申訴事件；2、提供有助於成員

[125] 日本，個人資料保護法，Article 7。

[126] 日本，個人資料保護法，Article 8。

[127] 日本，個人資料保護法，Article 37~49。

[128] 國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 212。

適當處理個資之相關資訊；3、其他協助成員適當處理個資之必要業務[129]。

(三) 隱私認證

除前述自律機制外，日本亦由財團法人日本資訊處理開發協會（JIPDEC）創設「Privacy mark（P-mark）」認證，由 JIPDEC 對於經評價符合日本工業規格 JIS2-500-1999 制定之「個人資訊保護之守法工作計畫（compliance program）」要求事項者，發給 P-mark 之認證標章供其使用於業務活動中，以取得消費者之信任[130]。

三、小結

總體而言，日本對於非公務機關之個資保護主要仍以業者自律為原則，鼓勵業者為維護其商譽與市場競爭性並強化消費者的信任，自行採取對其事業發展與消費者隱私保護最能達成平衡之個資保護措施。

第六節　本章結論

我國目前監管個資保護的方式應較近似美國的分散式管理模式，即由各中央目的事業主管機關對於所轄事業的個資保護予以管理。但與美國不同的是，我國僅有一部個人資料保護法規範所有公務與非公務機關的個人資料保護行為，此將難免造成規範上的漏洞（例如無法

[129] 日本，個人資料保護法，Article 37 (1)。

[130] 國家發展委員會，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，104 年，頁 215。

針對各別事業對於個人資料蒐集、處理、利用的特性與需求制訂切合該行業的規範內容）或不同主管機關間對於法律解釋的矛盾。將來即便仍維持由各主管機關分別管理，仍應考量以主管法規作為監理所轄事業個資保護的立足點。

第四章 大數據及智慧聯網對通訊傳播事業個資保護之衝擊

第一節 大數據與智慧聯網技術的崛起

美國資訊技術研究顧問公司 Gartner 的分析師 Doug Laney 於 2001 年發表《3D Data Management: Controlling Data Volume, Velocity, and Variety》文章[131]，對資料管理的發展提出三個構面的重要環節，分別為「資料量大（Volume）」、「處理速度快（Velocity）」以及「資料種類多（Variety）」，以此說明資料持有者在未來將面對的資料特性與潛在價值。

簡言之，隨著資料儲存、處理、分析的技術日趨發達，龐大的資料量對持有者而言再也不是用完即丟的「無價之物」，而是可用以創新加值的「無價之寶」。於是「資料探勘（Data Mining）」成為資料持有者傾力開發的領域，而「大數據（Big Data，又稱巨量資料）」一詞也應運而生。

國際電信聯盟（International Telecommunication Union, ITU）於 2005 年發表《The Internet of Things》報告[132]，正式宣告「智慧聯網（IoT，或稱物聯網）的時代來臨。簡單來說，智慧聯網係指透過網路技術的輔助，讓所有能獨立行使功能的物品實體連

[131]Doug Laney., 3D Data Management: Controlling Data Volume, Velocity, and Variety, http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf，最後到訪日 105 年 4 月 14 日。

[132]The-Internet-of-Things-2005.pdf - ITU, https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf，最後到訪日 105 年 4 月 14 日。

接網路，從而隨時蒐集、傳輸資料，並可偵測、定位、追蹤。

論者即謂「物聯網將透過一個高度整合的全球網路，把所有事物和每個人全部連結在一起。舉凡人、機器、天然資源、產品線、物流網路、消費習性、回收流程以及經濟和社會生活中的幾乎所有面向，都將透過感測器和軟體連接到物聯網平台，而且會持續不斷地對每個節點（node，包括企業、家庭、汽車等）提供巨量資料...」[133]。

第二節　大數據與智慧聯網帶來的隱私爭議

科技發展通常會帶來法律因應的挑戰，尤其涉及人民基本權利的限制或侵害疑慮時，更須透過法律檢驗來確保社會價值的衡平。大數據與智慧聯網的應用亦無可避免的引發了侵害權利的質疑，所指涉者即為人民的資訊隱私權與資訊自主權。

如前所述，大數據應用的特性在於「資料量大」及「資料種類多元」，因此對資料當事人而言，將面臨其個人資料被蒐集者大量取得、長期（甚至永久）保存、加值利用，更甚者將被透過與其公開資料互相彙整比對，而產出完整的人物側寫（Profile）。

而智慧聯網基於其「萬物皆與網路相連」的本質，蒐集者透過智慧聯網所取得的資料，除了機器（物品）運作自行產生之紀錄外，背後所隱含代表的極可能是「使用人」的行為模式或行動軌跡（例如智慧電表所回傳的用電時間及用電量，可以判斷使用人在家的時間、運動手環傳送的定位紀錄則可判斷穿戴人的地理

[133]Jeremy Rifkin 著，陳儀、陳琇玲譯，《物聯網革命》，商周出版，2015 年，頁 22。

位置足跡），對資料當事人的資訊自主控制權即有潛在損害的風險。

國際電信個資保護工作小組（International Working Group on Data Protection in Telecommunications, IWGDPT）於 2014 年 5 月召開的第 55 次會議中，即針對大數據分析時代下可能面臨的隱私爭議發布工作報告《Working Paper on Big Data and Privacy》[134]，並提出以下幾個面向的影響：

(一) 目的外利用個資

「目的限制原則」為國際上對於個資保護的重要原則，其意涵在於資料蒐集者對於個人資料的利用必須受到原始蒐集個資之目的限制，以此保障資料當事人對於個資的控制權利。

然而，大數據技術著重於資料的彙整與分析，依其性質必然將利用個資於原始蒐集目的之外，勢將衝擊「目的限制」此基本原則。

(二) 資料最大化

「資料最小化」及「必要保存期限」亦為個資保護的法律原則，強調蒐集者僅能在「達成目的之必要範圍內」取得及保存資料當事人的個人資料。

但大數據技術必須大量彙整資料以取得分析樣本，即蒐集者的期望在於最大範圍、最長時間內蒐集當事人的一切資訊作

[134] IWGDPT，Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics （Skopje, 5./6. May 2014）。

為分析依據，此亦與「資料最小化」、「必要保存期限」等原則相悖。

(三) 缺乏透明度

國際間對於個資保護多要求蒐集者於事前明確向資料當事人告知資料蒐集之目的、利用之方式與當事人權利等事項。然而在大數據趨勢下，蒐集者若未具體揭露其如何取得當事人資料，以及如何利用資料進行大數據分析，則當事人幾無可能理解其資料的來源與用途，使其資訊自主權將因缺乏透明度而受到侵害。

(四) 資料彙整可能揭露敏感資訊

大數據分析的技術之一在於資料的比對分析，因此對同一當事人而言，將有可能因為資料來源眾多，而使蒐集者在彙整不同管道取得的資料組後，因比對分析而產出對當事人而言屬於較敏感之資訊。

(五) 再識別的風險

雖然將當事人資料「去識別化」作為國際實務上肯認的大數據分析合法手段，但仍難以完全避免當事人基於不同資料群的彙整而被「再識別」的潛在風險。

實務上所稱之「馬賽克效應」即在說明同一當事人的各資料群雖以不同條件去識別化，但因仍存在某項可供勾稽的關鍵值，而使該當事人在多數資料群互相連結後仍能被重新識別。

(六) 資料不正確

「資料品質」同是個資保護的重要原則，強調蒐集者有義務保持當事人資料的即時與正確。但在大數據技術的發展下，一方面蒐集者可能並非從當事人直接取得其最新、最完整個人資料，二方面當事人可能因為不知悉蒐集者將以其資料作為大數據分析的基礎，而提供不正確的個人資料。此均將造成蒐集者對於當事人的資料分析結果產生錯誤或偏差，有違「資料品質」原則。

(七) 地位不平等

在缺乏透明度的情形下，由於當事人不知悉蒐集者將以其哪些個人資料作為哪些面向的大數據分析，以及將如何利用該等分析後之資料（例如提供第三者或以其分析結果對當事人做出何種決策），將使當事人處於資訊地位不平等的劣勢。

(八) 區別待遇

蒐集者將當事人資料彙整用於大數據分析，將有可能依其分析（預測）結果而對不同當事人間作成區別對待，此亦涉及國際實務上高度重視的平等與歧視問題。

(九) 國際傳輸

除上述國際電信個資保護工作小組提出之影響外，個人資料的「國際傳輸」亦為大數據技術發展下的重要個資保護議題。在網路技術精進時代，跨國企業在世界各地提供資訊服務，並將各地取得的個人資料互相跨境傳輸已是屢見不鮮。

然而各國對於個資保護的法規寬嚴不一，是否均對當事人

權利採取足夠保障仍有疑慮。歐盟的個資保護指令 95/46/EC 即對於個人資料的（歐盟）境外傳輸設有限制，僅在符合正面表列的前提或例外下始得將個人資料傳輸之歐盟境外：

1. 第 25 條原則規定

(1) 會員國應規定僅於他國能確保充足的保護（adequate level of protection）後，才能將個人資料傳輸至他國。

(2) 「適足」(adequacy)與否應考量所有關於該傳輸的情況，包括：

A、資料的特性。

B、傳輸之目的與期間。

C、資料輸出國與輸入國。

D、第三國的法律規範是否符合該國之專業規則與安全措施。

(3) 會員國與執委會若認為他國無法符合「適足」要件時，應互相通知。

(4) 若執委會認為他國不符合「適足」要件時，會員國應採取必要措施避免像同類型的資料傳送到該他國。

(5) 在適當時機，執委會應進行協商（negotiation）以補救第 4 項的審查結果。

(6) 執委會得依據國內法或是國際承諾，認為他國符合「適足」，特別是在依據第 5 項協商結果後，以保護私人生

活以及個人基本自由及權利。

(7) 會員國應採取必要措施以符合執委會的決定。

2. 第 26 條例外規定

(1) 會員國得在下列情況向未符合第 25 條第 2 項「適足」要件之他國傳輸個人資料：

A. 當事人明確同意。

B. 傳輸係為了實施資料當事人與資料控制者間契約之必要，或是因應當事人的要求為締結契約之準備行為。

C. 傳輸係為了締結或履行資料提供者與第三方間，對於資料當事人之第三方利益契約。

D. 傳輸係為了重大公共利益之必要或是法律要求，或以法律聲明之建立、實施或防禦為目的。

E. 傳輸係為了保護資料當事人之重大利益。

F. 傳輸係依據法規須提供給公眾之資訊，並公開給一般大眾或是有合法利益之人查詢，但僅及於該個案符合法定之查詢條件的範圍內。

(2) 若資料控制者舉證有適當的保護措施以保護隱私權與個人自由與實施基本權利時，會員國得授權傳輸個人資料到未符合第 25 條第 2 項「適足」要件之他國，此保護措施得由適當契約條款（contractual clauses）而生。

(3) 會員國應通知執委會與其他會員國其依照第 2 項所為之授權。

(4) 如執委會認定該特定契約條款符合第2項的保護措施，會員國應採取必要措施以符合執委會決定。

據此，大數據時代下對於跨國企業的資料蒐集與彙整分析行為，如何確保當事人權利在各國家的傳輸間仍能獲得足夠保障，亦是國際間刻正面臨的重要議題。

第三節　通訊傳播事業現況與面臨之衝擊

(一) 通訊傳播事業現況

通訊傳播事業在大數據與智慧聯網時代亦未缺席，尤其我國的智慧型手機、行動上網、無線寬頻、數位機上盒等科技普及率高，用戶的資料對通訊傳播業者而言可謂含量極豐的「資料金礦」。

在蒐集的資料類型方面，通訊傳播業者可以取得用戶的基本資料（姓名、地址、電話等）、通訊紀錄（發話時間、通話長短、受話對象等）、瀏覽紀錄（IP 位址、瀏覽時間、造訪網頁、收看之節目、影片或廣告、停留時間等）、位置紀錄（發收話基地台位置、行動上網位置等）；而就資料利用方式而言，通訊傳播業者可將上述所取得的資料透過創新發想而加值應用，例如：

1. 以網頁瀏覽紀錄或收視習慣分析用戶的喜好或關注商品、服務。

2. 以位置資訊分析用戶的足跡，辨別用戶的生活作息。

3. 以位置資訊鎖定用戶的地理位置進行廣告投遞。

4. 以帳單明細分析的使用習性及消費能力。

5. 將上述資訊與用戶之基本資料結合，加深用戶的屬性輪廓並標註用戶族群，並可進行精準廣告投遞。

6. 將大量用戶上述資訊串接統計，產出數據分析結果提供第三人（例如廣告商、廣告主）。

7. 將第三人（例如廣告商、廣告主）提供的個人資料與通訊傳播業者自己的用戶資料比對，回覆個別用戶的個人資料或群體用戶的統計資料。

上述行為僅為資料加值應用的冰山一角，在技術與發想不斷創新的趨勢下，必然會有更多的資料運用方式。然而，無論商業模式如何翻新，用戶的基本權利仍不可無端受損，根本之計，通訊傳播業者應遵守最上位的隱私與個資保護原則作為基本底線，方能以此開展其創新應用用戶資料的營利模式。

美國「數位權利評比（Ranking Digital Rights）計畫」依據各家公司對隱私權、言論自由、透明度和用戶個資保護的承諾，評比 8 家大型網路公司和 8 家大型電信供應商，並於 2015 年 11 月發布研究報告[135]，該研究以項目表評分 16 間公司，百分等級為 0 到 100，其中 Google 得分最高，達 65%，Yahoo 以

[135]https://rankingdigitalrights.org/index2015/，最後到訪日 105 年 4 月 14 日。

58%排名第二，接著是得到 56%的 Microsoft 與獲得 50%的 Twitter，得分最低的是俄羅斯網路公司 Mail.ru，為 13%；中國的騰訊則獲得 16%。而在電信公司方面，英國 Vodafone 表現最佳，得到 54%，其次是美國的 AT&T，有 50%，評分最低的是中東阿聯酋電信集團（Etisalat Group），得分為 14%。其中隱私項目表如下：

表 2 數位權利評比隱私項目評分表

隱私項目評分表		
1	隱私權政策可得性	
	1-1	隱私權政策是否免費取得且易於查閱，並無須註冊或訂閱
	1-2	隱私權政策是否以目標客群的主要語言撰寫
	1-3	隱私權政策內容是否以閱讀者易懂之文字撰寫
2	隱私權政策修訂、通知與紀錄	
	2-1	公司是否向使用者揭露隱私權政策修訂訊息通知之方式（例如簡訊或電子郵件）
	2-2	公司是否向使用者揭露通知隱私權修正訊息的時限（例如修正前 2 週通知）
	2-3	公司是否保存隱私權修訂的公開檔案或修訂紀錄
3	蒐集使用者資料	
	3-0	公司是否宣示不蒐集使用者資料，若否，則接下題
	3-1	公司是否承諾僅在達成蒐集目的之最小範圍內蒐集使用者的相關且必要之資料
	3-2	公司是否明確揭露將蒐集使用者的哪些資料
	3-3	公司是否明確揭露如何蒐集使用者之資料

	3-4	公司是否明確揭露為何目的而蒐集使用者之資料
4	與第三人分享使用者資料	
	4-0	公司是否宣示不與他人分享使用者資料，若否，則接下題
	4-1	公司是否明確揭露與第三人分享使用者的哪些資料
	4-2	公司是否明確揭露與第三人分享使用者之目的
	4-3	公司是否提供與其分享使用者資料的第三人類別之描述
	4-4	公司是否列舉所有與其分享使用者資料的第三人名稱，並逐一說明與個別第三人分享使用者的哪些資料
	4-5	如公司對使用者提供多元服務，是否明確揭露有無及如何在使用者使用各種服務時，將使用者資料與第三人分享
5	使用者控制權	
	5-1	公司是否讓使用者有權控制公司蒐集其資料
	5-2	公司是否讓使用者有權控制公司與第三人分享其資料
6	使用者資料存取	
	6-1	公司是否允許使用者查閱其資料
	6-2	公司是否對使用者提供其資料的複製本
	6-3	公司是否提供使用者以完整格式下載其資料
	6-4	公司提供使用者存取的資料是否包含公司所持有關於該使用者的公開與非公開資料
7	使用者資料保存	
	7-0	公司是否宣示不保存使用者資料，若否，則接下題
	7-1	除使用者交付資料供儲存或提供資料以公開外，公司是否主張以去識別化形式儲存使用者資料
	7-2	公司是否揭露其儲存使用者的資料類別

	7-3	公司是否揭露將在多長期間內保存使用者資料
	7-4	公司是否承諾將在使用者終止帳號後便刪除其所有資料
8	公司對第三人請求提供使用者資訊的回應程序	
	8-1	公司有無說明其對於無管轄權的政府機關請求提供使用者資訊的處理流程
	8-2	公司有無說明其對法院要求提供使用者資訊的處理程序
	8-3	公司有無說明其對第三人（非公務機關）請求提供使用者資訊的處理程序
	8-4	公司有無說明其對他國司法機關請求提供使用者資訊的處理程序
	8-5	公司的說明有無包含其所適用的法律依據
	8-6	公司是否承諾會在決定是否將使用者資訊對外提供前進行盡職調查
	8-7	公司是否承諾會拒絕非法的請求
	8-8	公司是否提供指引或範例以說明上述政策的執行
9	對使用者通知第三人請求提供使用者之資訊	
	9-1	公司是否承諾當政府機關請求提供使用者資訊時，將通知使用者該情事
	9-2	公司是否承諾當第三人（非公務機關）請求提供使用者資訊時，將通知使用者該情事
	9-3	公司有無揭露在何種情況下，將不向使用者通知第三人請求提供使用者資訊之情事，包含政府機關依法令禁止公司對使用者通知的情形
10	第三人請求提供使用者資訊	
	10-1	如國家機關要求提供使用者資訊，公司是否通知使用者

	10-2	公司是否列出受影響的使用者帳戶數量
	10-3	公司是否列出其對第三人提供的資料有無包含通信內容
	10-4	公司是否說明是由何政府機關或法律程序而要求提供使用者資訊
	10-5	公司是否將法院命令提交使用者資訊的情形向使用者告知
	10-6	公司是否說明其提供使用者資訊的對象包含非政府機關
	10-7	公司是否列出其對第三人提供使用者資訊的數量及類別
	10-8	公司是否列出在哪種情況下，政府機關要求提供資訊是依法不許的
	10-9	公司是否至少每年提出上述事項報告一次
	10-10	上述報告是否以完整的資料結構形式提出
11	安全防護標準	
	11-1	公司是否承諾隨時更新其加密與資安措施，並提出證明
	11-2	公司是否承諾一發現資安弱點便會公布其事實及原因
	11-3	公司是否說明其採取何種方案限制並監管員工對於使用者資訊的存取
	11-4	公司是否說明其定其執行資訊安全稽核
	11-5	公司是否將使用者資訊傳輸過程預設為加密方式
	11-6	公司是否採取先進的驗證方式預防不當的資料存取
12	潛在威脅提醒	
	12-1	公司是否承諾如有異常帳戶活動或疑似為授權存取資料時，將通知使用者
	12-2	公司是否向使用者發布關於避免網路資安威脅的說明

（來源自 https://rankingdigitalrights.org/index2015/，項目表由本研究團隊自行整理）

(二) 通訊傳播事業面臨之衝擊

具體而言，在大數據與智慧聯網技術發展的趨勢下，資料當事人隱私與個資保護的重心已由「安全防護以避免資料外洩」擴及「公開透明以尊重當事人自主控制」。因此，資料蒐集者將面臨以下幾點挑戰：

1. 事前告知，包含：

(1) 明確清晰的隱私權政策（個資蒐集告知聲明）。

(2) 具體描述蒐集資料之目的。

(3) 告知將透過何種方式蒐集哪些資料。

(4) 告知利用個資的方式。

2. 事中以去識別化方式保護當事人隱私，或強化資料安全的防護措施。

3. 事後給予當事人選擇退出（Opt-Out）以拒絕利用資料與大數據分析，甚至要求刪除資料的權利。

第四節　國外電信業隱私條款分析

(一) Telefonica，西班牙

西班牙電信商 Telefonica 在 2012 年 10 月與市場調查公司 GfK 合作推出 Smart Steps 商品，利用其電信用戶的行動位置資訊（時間及地點）結合個人屬性，為企業客戶產出「去識別化」的分析報告，供企業客戶判斷其場地客源特性，或決定最

佳開店地點。

1. 隱私權聲明

Telefonica Dynamic Insights 在其網站公布的隱私權聲明（Privacy Statement）中強調其商品僅利用去識別化的用戶匿名統計資料（anonymised and aggregated data）[136]。

2. 發展現況

Telefonica 在 2012 年 10 月宣布瞄準英國、德國及巴西推出該商品，卻於同年 11 月基於「消費者隱私疑慮」的考量，決定暫停進入德國市場[137]。

據悉 Telefonica 為提供 Smart Steps 商品，即便用戶將行動裝置的位置設定關閉，該公司仍能取得其位置資訊。亦即任何用戶皆無法選擇退出此項服務，而須強制成為分析報告的對象之一。但 Telefonica 同時也強調，所有用戶的資料都被匿名化處理，產出的報告均為去識別化的資料[138]。

[136]Privacy - Telefonica Dynamic Insights , http://dynamicinsights.telefonica.com/635/privacy，最後到訪日 105 年 4 月 14 日。

[137]Telefónica withdraws 'Big Data' service from German market, http://www.fiercewireless.com/europe/story/telef-nicas-big-data-plans-blocked-german-regulator/2012-11-02，最後到訪日 105 年 4 月 14 日。

[138]Telefónica to sell 'insights' gleaned from anonymised mobile phone location data, http://www.out-law.com/en/articles/2012/october/telefonica-to-sell-insights-gleaned-from-anonymised-mobile-phone-location-data/，最後到訪日 105 年 4 月 16 日。

據報導指出，德國官員認為依據德國聯邦個人資料保護法的相關規定，消費者位置資訊的加值應用只能以「去識別化」的方式為之，或是事先「取得當事人同意」，但卻又表示「銷售消費者的位置資訊是不被允許的」[139]，因此 Smart Steps 自始未進入德國市場，未能真正挑戰德國的個資保護相關規定。

然而，英國的隱私保護主管機關 ICO 於 2012 年 12 月發布的指引 Anonymisation：managing data protecting risk code of practice 則認為，蒐集機關如能確保產出的分析報告為完全去識別化（不可回復或藉由任何方式的資料比對而連結出特定人）的資料時，僅須於事前告知即可，無須取得當事人同意[140]。因此即便 Smart Steps 強制取得用戶的位置資訊，但如其能完全的去識別化處理用戶資訊，則並不違反英國的個人資料保護法。

(二) AT&T，美國

美國電信商 AT&T 在 2013 年 5 月推出 Blueprint 商品，透過行動用戶、網路用戶、電視用戶的匿名資料分析，以向企業

[139] German govt to limit Telefonica plans to sell customer data, http://www.telecompaper.com/news/german-govt-to-limit-telefonica-plans-to-sell-customer-data--905518，最後到訪日 105 年 4 月 14 日。

[140] Anonymisation - Information Commissioner's Office , http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf ，最後到訪日 105 年 4 月 14 日。

客戶銷售去識別化的精準行銷參考報告[141]。

1. 隱私權政策摘要

AT&T 在 2013 年 9 月版本的隱私權政策摘要中[142]，以具體、詳細方式「告知」用戶將以其各類資訊產出「去識別化」的分析報告銷售予企業客戶，預設用戶的同意，並提供用戶簡單操作的 opt-out 退出方式，節錄說明如下：

(1) 在所蒐集的資訊（Here's some of the information we collect）中明確記載：帳戶資訊（Account Information）、網路瀏覽及無線應用資訊（Web Browsing & Wireless Application Information）、位置資訊（Location Information）等。

(2) 在利用方式中（Here are just some of the way we use it）明確記載：產出外部行銷分析報告（Create External Marketing &Analytics Reports）等。

(3) 在當事人權利中（Your Choices & Controls）明確記載：您得選擇是否讓我們將您的匿名資訊使用於產出外部行銷分析報告中（You can control whether your anonymous information is used in our External Marketing

[141] AT&T rolls out multi-platform AdWorks Blueprint audience, http://www.fiercemobileit.com/story/att-rolls-out-multi-platform-adworks-blueprint-audience-targeting-effort/2013-05-22，最後到訪日 105 年 4 月 14 日。

[142] AT&T Privacy Policy, http://www.att.com/gen/privacy-policy?pid=2506，最後到訪日 105 年 4 月 14 日。

& Analytics Reports）。

(4) 在隱私權政策摘要中可點選「Visit our Privacy Policy for more information」連結至隱私權政策 FAQ[143]，並在隱私權 FAQ 的「QUESTIONS ABOUT EXTERNAL MARKETING AND ANALYTICS REPORTS」項目中詳細說明去識別化的分析報告的利用方式，如：

A、 我們以統計資訊的方式產出外部行銷分析報告，並可能銷售予企業客戶供其行銷、廣告或其他類似使用。（We use aggregate information to create External Marketing & Analytics Reports that we may sell to other companies for their own marketing, advertising or other similar uses.）

B、 報告包含如為零售商分析在特定時間內位於其店面之內或附近區域的無線裝置數量及使用者的屬性資料。（Reports for retail business that show the number of wireless devices in or near their store locations by time of day and day of week, together with demographic characteristics of the users （such as age and gender） in those groups.）

(5) 在隱私權 FAQ 的「QUESTIONS ABOUT LOCATION INFORMATION」項目中詳細說明：

[143]AT&T Privacy Policy FAQ | AT&T, http://www.att.com/gen/privacy-policy?pid=13692，最後到訪日 105 年 4 月 14 日。

A、 位置資訊服務（Location Based Services）：我們在使用或分享您的位置資訊前會向您事先告知並取得您的同意。（We'll give you prior notice and ask for your consent when your location is used or shared.）

B、 我們利用您的位置資訊進行廣告行銷。（We use if for Advertising.）

2. 發展現況

雖據報載該公司於同年 11 月大幅縮減 Blueprint 商品部門的人力[144]，但未有跡象顯示係因相關隱私法規的問題而導致該商品的阻礙。

(三) Verizon，美國

美國電信商 Verizon 成立精準行銷部門，其推出的 Precision Market Insights 商品可彙整特定場所內行動裝置用戶的屬性資訊提供予該場所的企業客戶；Precision Marketing 商品則為精準行銷服務。

1. 隱私權政策

Verizon 在 2014 年 8 月版本的隱私權政策中記載其所

[144] AT&T Is Ending Its 'AdWorks' Mobile Experiment And Laying Off Staff, http://www.businessinsider.com/att-is-ending-its-adworks-mobile-experiment-and-laying-off-staff-2013-10，最後到訪日 105 年 4 月 14 日。

蒐集的用戶資訊及利用方式[145]，節錄說明如下：

(1) 在所蒐集的資料（Information Collected When You Use Verizon Products and Services）中明確記載：通信紀錄、網頁瀏覽紀錄、無線位置資訊、應用程式紀錄、裝置序號、帳單資訊等。（call records, websites visited, wireless location, application and feature usage, other similar information may be used for billing purposes）

(2) 在 Verizon 網站資料蒐集（Information Collected on Verizon Websites）中亦說明：我們蒐集您的網頁瀏覽、搜尋、購買紀錄、IP 位置、裝置號碼、帳戶資訊、網頁到訪等資訊。（browsing, searching and buying activity , IP address, mobile telephone or device number, account information, web addresses of the sites you come from and go to next.）

(3) 在針對無線網路用戶的說明（Additional Information for Wireless Customers）中記載：您的行動裝置使用資訊及用戶資訊將用於商業及行銷報告，前者包含您瀏覽的網頁及位置和使用的應用程式等，後者包含您的性別、年紀等屬性。我們會將這些資訊結合以產出去識別化的商業行銷報告，除供自己使用外，也可能提供給企業客戶。（Verizon Wireless may use mobile usage information

[145]Privacy Policies | Verizon, http://www.verizon.com/about/privacy/policy/，最後到訪日 105 年 4 月 14 日。

and consumer information for certain business and marketing reports. Mobile usage information includes the addresses of websites you visit when you use our wireless services. These data strings （or URLs） may include search terms you have used. Mobile usage information also includes the location of your device and your use of applications and features. Consumer information includes information about your use of Verizon products and services （such as data and calling features, device type, and amount of use） as well as demographic and interest categories provided to us by other companies （such as gender, age range, sports fan, frequent diner, or pet owner）. We may combine this information in a manner that does not personally identify you and use it to prepare aggregated business and marketing reports that we may use ourselves or share with others for their use.）

2. 發展現況

美國聯邦通訊傳播委員會 FCC 在 2014 年 9 月 3 日公布一項調查結果[146]，內容為電信商 Verizon 違法對用戶行銷，經 FCC 調查後服從調查結果，提出約 740 萬美元（約新台幣 2.2 億元）與 FCC 達成和解。

[146]Verizon To Pay $7.4M To Settle Privacy Investigation, http://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation-0，最後到訪日 105 年 4 月 14 日。

據悉 Verizon 自 2006 年起疏於對大約 2 百萬名用戶提供拒絕行銷（opt-out）的方式，直至 2012 年 9 月始知此事，但卻在 2013 年 1 月才通知 FCC。案經 FCC 調查後，認定 Verizon 剝奪用戶請求蒐集者停止利用其個人資料的當事人權利，於法不合。

現 Verizon 除提出 740 萬美元與 FCC 和解之外，並同意未來在寄給用戶的「每一份」帳單中均載明 opt-out 拒絕行銷的方式。

(四) Wire and Wireless，日本

日本無線網路服務商 Wire and Wireless（Wi2）於 2013 年起與跨國管理顧問公司 Accenture 合作，利用用戶連接 Wi2 提供之無線網路所產生的各項資料進行分析，並以此產出可供 Wi2 的企業客戶加以利用的用戶足跡分析等加值數據。

1. 隱私權政策

依 Wi2 於網站上公告的隱私權政策可知，該公司事先即向用戶告知將以統計資料的方式利用用戶的個人資料，將分享給他人，節錄如下：

(1) 在 Tarvel Japan Wi-Fi 頁面的常見問題中，Wi2 告知用戶「由於相關資訊將被統計化，故無個人資訊（特定於個人的資料）的使用，洩漏等危險。為了提升服務品質

之目的，該統計資訊將會被分享給合作贊助企業」[147]。

(2) 在 Wi2 網頁的隱私政策中，Wi2 在「個人資訊之使用目的」告知用戶包含「基於市場調查及數據分析等提高及開發服務」、「針對資訊提供服務事業者，將年齡、性別等屬性資訊以及過去行動記錄資訊等加工成為無法指定個人身份的形式並進行提供。不提供用以指定個人身份之資訊（個人資訊）」[148]。

2. 發展現況

依報導所見，隨著日本觀光人數增加，旅客無線上網的便利性成為日本政府發展觀光的重點之一，Wi2 與 Accenture 合作的數據分析工具「以地圖形式將來日旅客動向可視化，並加入國籍、性別等條件篩選，作為店家開發新商業的參考」，可作為用戶大數據資料應用的參考案例[149]。

第五節　本章結論

綜上所述，通訊傳播事業在利用大數據與智慧聯網技術以加值分析運用使用者之個人資料時，仍須顧及「目的限制」、「具體告知」、「保障當事人控制權」、「安全維護」等個資與隱私保護之原則，始能符合以「誠實信用」之方式蒐集、處理、利用個人資料的法律規範，以避

[147] 見 http://wi2.co.jp/tjw/faq/faq_hantai.html，最後到訪日 105 年 4 月 14 日。

[148] 見 http://wi2.co.jp/tw/privacy/，最後到訪日 105 年 4 月 14 日。

[149] 見 http://www.digitimes.com.tw/tw/rpt/rpt_show.asp?cnlid=3&v=20160309-66&n=1，最後到訪日 105 年 4 月 14 日。

免觸法。本研究報告將於第五章介紹國際上對於大數據與智慧聯網技術發展在個資與隱私保護議題上的具體因應建議。

第五章 各國對通訊傳播事業因應大數據及智慧聯網時代個資保護之規管措施

如前章所述，大數據為資料蒐集與利用的創新發展，智慧聯網則是資料蒐集與利用新興科技模式，如回歸當事人個資與隱私保護本質，仍應遵守相關法律對於資訊隱私權與資訊自主權保護的規範。是以目前國際上尚未出現針對大數據與智慧聯網立法規管的實例，而多係就既存法律修正或加強解釋以供受規範者遵守，或由民間團體提出參考建議或準則。

例如國際電信個資保護工作小組（International Working Group on Data Protection in Telecommunications, IWGDPT）於 2014 年 5 月召開第 55 次會議針對大數據分析時代下可能面臨的隱私爭議發布工作報告《Working Paper on Big Data and Privacy》、歐盟在 2014 年由個人資料保護指令第 29 條工作小組提出《Opinion 8/2104 on the Recent Developments on the Internet of Things》、歐盟資料保護監督員（European Data Protection Supervisor）於 2015 年發布《Meeting the challenges of big data》、英國 ICO 在 2014 年提出《Big data and data protection》指引、美國白宮科技顧問委員會（President's Council of Advisors on Science and Technology，PCAST）於 2014 年提出《BIG DATA AND PRIVACY：A TECHNOLOGICAL PERSPECTIVE》報告、FTC 於 2015 年提出《internet of things, Privacy & Security in a Connected World 》工作報告等（見下述）。

是以下將以大數據與智慧聯網技術應適用之關鍵議題為架構，分析國際實務上現有的具體意見與規範，再就兩者於實務上的因應提出國際間的綜合建議。

第一節　大數據技術的個資保護議題

一、加強蒐集者責任

蒐集者在大數據技術發展下須擔負更大的責任以取得資料當事人的信任，因此蒐集者除須具體宣示其對當事人個資保護與隱私的重視之外，更須強化其資訊安全防護措施、個人資料管理機制以及持續性的風險評估與控管作為，同時要提高其透明性要求，必須確實將其大數據分析的個資來源、分析方式與結果利用方式明確向當事人揭露，並給予當事人便利自由選擇退出或加入的機會。

歐盟個資保護監察員更提出「道德委員會（Ethic Boards」的建議[150]，認為蒐集者應於機關內部設立類似組織，專責審視當事人資料再利用的合法、合適與合宜性。

二、目的限制原則的調整

蒐集個資須具有「特定目的」，此為國際實務上均無爭議的個資與隱私保護條件，其功能在於確認蒐集者取得個資的必要及關聯範圍，並劃清利用個資的界線，我國個人資料保護法第 15 條及第 19 條規定，蒐集個人資料須有「特定目的」，又第 5 條規定蒐集者的蒐集、處理、利用個資行為均須與「蒐集目的」有正當合理關聯。是以「目的限制」原則實為國際間個資與隱私保護的重要法律元素。

---

[150]歐盟個資保護監察員（European Data Protection Supervisor），《Meeting the challenges of big data》,2015。

歐盟個人資料保護指令第 29 條工作小組即於 2013 年提出《Opinion 03/2013 on the purpose limitation》討論「目的限制」原則的適用[151]，以下說明之：

(一) 蒐集個資之目的必須「特定」、「明確」及「正當」

1. 蒐集目的必須特定

即在個資的蒐集發生之前（最遲應於蒐集個資時），其目的必須精確且完全特定，以確定哪些處理及利用行為包含和不包含在特定目的中，並且允許資料當事人或主管機關評估對法律的遵守情況以及可資應用的資料保護措施。

因此，模糊或籠統的目的，例如「改善使用者體驗」、「行銷目的」、「資訊安全目的」或「將來的研究」等沒有更多細節的目的，通常無法符合「特定」之標準。即便如此，蒐集目的之詳細程度應當根據蒐集資料的背景以及涉及的個人資料來確定。

2. 蒐集目的必須明確

個人資料必須為明確的目的而蒐集，且蒐集目的不得僅僅在資料蒐集者的思想中明確特定，還必須以明確的方式提出。此要求係為確保特定目的在其含義或意圖上不存在含糊或歧義。

蒐集目的中的含義必須明確，不應當有任何理解上的疑

[151]歐盟，Article 219 Data Protection Working Party, WP203,《Opinion 03/2013 on the purpose limitation》,2013。

問或困難。目的特定的方式特別應當確保不僅資料蒐集者（包括所有相關工作人員）和任何第三方處理人員，而且主管機關以及相關資料當事人都能以相同的方式理解。

此要求有助於提高透明性和可預測性，使資料當事人與主管機關得以確定資料蒐集者能夠如何處理與利用所蒐集的個人資料，並著眼於保護資料當事人，同時亦說明所有代表資料蒐集者處理或利用資料的人員以及資料當事人、主管機關和其他利益相關人對於可如何處理或利用資料達成共識，進而降低資料當事人的預期與資料蒐集者的預期不相同的風險。

3. 蒐集目的必須正當

對正當性的要求意味著蒐集目的必須在最廣泛的意義上「與法律相符」，包括憲法、普通法、特別法、法規命令、司法判例等。在法律的限制範圍之內，考量蒐集目的是否正當時，也可以考慮其它要素，例如習慣、行為規範、道德規範、契約以及當時情況的整體背景和事實等，其中將包括資料蒐集者和資料當事人之間根本關係的性質，例如是否為商業性質。

但應注意的是，蒐集目的之正當性也可能隨著時間的推移而改變，視科學和技術的發展以及社會和文化態度的變化而定。

(二) 利用個資應與蒐集之特定目的「相符」（相容性）

如前所述，「特定目的」之功能其一在於劃清利用個資的

界線，是以當資料蒐集者須進一步利用所蒐集的個資時，其利用行為即應受到「相容性評估」的檢視：

1. 資料蒐集之目的和利用之目的之間的關係

由於實務上可能僅存在有限的（如有的話）的文字被用於表達蒐集之目的，因此本項因素應當不僅被視為一個文字性的問題，即蒐集目的之語言和利用目的之語言間有如何對比，焦點應在於蒐集目的和利用目的之間的關係。

其中可以包括利用行為已經或多或少在蒐集目的中被暗示的情況，或依照這些目的被假設為合乎邏輯的行為的情況，以及與蒐集目的只有部分不存在關聯的情況。在任何情況下，蒐集目的和利用目的之間的差距越大，相容性評估就越有可能發生問題。

2. 蒐集的背景以及資料當事人對於利用資料的合理期待

此處係指任何客觀理性的第三人在資料當事人所處的處境下，根據蒐集資料的背景將會對其資料的利用目的產生如何的預期。此不僅要求對已經提出的任何法律聲明進行審查，尚要求考慮在特定的背景下以及在特定的（商業性的或其它的）關係中存在哪些習慣性的和普遍預期的行為方式。大體而言，利用行為越超出預期或出人意料，其越有可能被視為不相容。

3. 資料的性質和利用行為對資料當事人的影響

為避免個人資料遭到不當或過度利用而對資料當事人

造成影響，被利用的資料之性質在此即有關鍵作用，例如對於生物特徵、基因、通訊資料、位置資訊以及其它類型的特殊個資，均應納入相容性評估的因素中。在一般情況下，涉及的資料敏感程度越高，相容利用的範圍就會越窄。

4. 資料蒐集者採取用於確保公平處理和防止對資料當事人產生任何不適當影響的保護措施

在某些情況下，相容性的不足可以透過其他措施進行彌補，因此「適當保護措施」可以作為「目的變更」或「目的未明確」的一種「補償」。

「適當保護措施」包含技術和/或組織的措施確保功能分離（例如部分或完全的匿名化、假名化和資料整合），而且還要求採取額外的措施保護資料當事人的利益，例如更高程度的透明性，並且可以提出異議或提供具體的同意，同時包含提供資料當事人選擇加入或退出的機制。

5. 相容性評估示例

舉例而言，如某國交通部詢問一家電信公司是否能夠提供公司的行動電話位置資訊以計算電話（以及由此推斷出電話所在車輛）在各種路線上移動的速度，藉此判斷哪些路段較易出現「超速行駛」的問題，並以該資料規劃車輛減速措施，而這些措施在後來顯示大大降低該地區的交通事故致死率。

在向交通部提供資料之前，這些行動電話資料已經經過有效的匿名處理，以確保將資料當事人被再次識別的風險降

至最低，並執行細緻的影響評估和滲透測試，並且與利益相關方進行磋商。在此情況下，可以認為所有事實都確認存在極低或最低的再次識別的風險和對資料當事人相對較低的影響（如果發生的話）。

如以此案例進行相容性評估，則電信資料最初為提供電信服務之目的被蒐集，而現在將用於不同的目的（道路交通相關的目的）。大部分人通常不會預期到其資料將以此方式被利用，且行動電話位置資訊也相對敏感即有可能表示此目的是不相容的。

但在本案例中，資料在被利用於其他目的之前，已經進行有效的匿名化。因此，儘管兩個目的並不相同，在充分執行匿名化的情況下（因此該資料也不再構成個人資料，或僅具有極低的再次識別的風險），任何與不相容利用相關的疑慮可以大大降低。惟儘管如此，電信公司仍然應採用額外的保護措施，例如使該利用行為具有完全的透明性，甚至事先取得資料當事人同意或給予資料當事人選擇退出的機會。

然如前章所述，「目的限制」原則在大數據趨勢下將面臨「目的變更」的衝擊，國際上例如歐盟提出的個資保護基礎規則草案即放寬目的限制原則而設例外規定。但由於此作法將形同侵蝕個資保護的基礎原則，是以德國個資保護主管機關即於 2015 年 8 月發布的意見中明確表示反對，認為應堅守目的限制原則以確保當事人對於其個人資料的基本自

主權利[152]。日本的消費者委員會亦於 2014 年發布的《對於「個人資料使用制度修正綱要」之意見》中對於「個人資料使用制度修正綱要」中關於「變更使用目的之程序」修正為「建立當事人可充分獲悉的程序，同時設定選擇退出機制（opt-out），供當事人表明不願意讓個人資料用於新的使用目的並將此告知當事人」之調整認為「應重視需當事人同意的原則，本會認為便宜行事而利用選擇退出（opt-out）機制做為同意得變更個人資料使用目的一節，非屬妥適」[153]。

三、當事人同意 v.當事人控制（被遺忘權）與利益分享

「當事人同意」本為當事人資訊自主權的基本條件，意涵在於當事人可透過自由意志決定其個人資料的蒐集、處理與利用。然而在網路時代下，「當事人同意」因為複雜繁瑣的服務條款或隱私權政策而趨向徒具形式，當事人多在未細閱讀艱澀文字的情況下直接於網頁中勾選「同意」；或是由蒐集者在相關條款中設計為當事人的「預設同意」，當事人必須另外採取行動已表示不同意；甚至當事人可能對蒐集者將所有蒐集資料目的及利用資料方式作出「綑綁式同意」。

---

[152]DER HESSISCHE DATENSCHUTZBEAUFTRAGTE,《Key data protection points for the trilogue on theGeneral Data Protection Regulation》,2015,"[a] strong guarantee of purpose limitation is essential to ensure that individuals have thegreatest possible transparency and freedom to decide. The conference therefore vehementlyopposes the Council's proposal to water down the purpose limitation principle and advocateson the basis of the Council's proposal, deleting Article 6（4） of the Regulation."

[153]日本消費者委員會，《「パーソナルデータの利活用に関する制度改正大綱」に関する意見》，2014。

此等「同意」行為均可能因為缺少「意思表示」、「自由性」、「具體性」、「明確性」、「清晰性」、「告知後同意（informed and consent）」等「同意品質」，而成為國際上認定的「無效同意」[154]。論者即謂在大數據技術下，「當事人同意」的要求恐怕難以發揮其功能[155]。

因此，國際上漸有傾向認為，在大數據技術時代，「當事人同意」將逐漸式微，取而代之的則是蒐集者的「透明性」提高與「當事人控制權」的保障，甚至是與當事人「分享大數據的利益」[156]，亦即：

(一)蒐集者於事前提高其透明性，詳盡且明確對當事人告知其蒐集資料目的包含大數據的分析，以及將如何取得其資料並如何進行大數據分析。

(二)蒐集者於事後對當事人提供完善的「無條件退出（opt-out）」機制，讓當事人可隨時不附理由、不受限制的行使其「請求停止利用個資」或「請求刪除個資（被遺忘權，the right to be forgotten）」等權利。

(三)強化當事人的資料近用與可攜權，亦即蒐集者應以最友善的方式提供當事人存取（access）其個人資料的機制，並且讓

[154]歐盟，Article 219 Data Protection Working Party, WP187,《Opinion 15/2011 on the definition of consent》, 2011。

[155] Fred H. Cate, Peter Cullen,and Viktor Mayer-Schönberger,《Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines》, 2013。

[156]歐盟個資保護監察員（European Data Protection Supervisor）,《Meeting the Challenges of Big Data,2015。

當事人得自由攜出其個人資料以再次利用，以此方式讓當事人亦能從對其個人資料進行的大數據分析中獲利，創造雙贏局面。應具備的面向包含：

1. 對當事人提供具備可攜出、可讀取、可電腦化利用之格式的個人資料。
2. 允許當事人自由修改、刪除、移轉或以其他方式利用其個人資料。
3. 讓當事人得自由更換服務提供商（例如變更其相簿、健身紀錄或電子郵件的服務提供商）。
4. 讓當事人得以允許第三人分析其個人資料，以此獲得利益（例如改變飲食習慣、選擇理財方案等）

四、第三方資料庫

承接前述「當事人控制權」與「大數據利益共享」等概念，國際上進一步提出在大數據技術下應可推廣「第三方資料庫（data spaces, data stores, data vaults」的發展[157]，強調大數據時代下的個資利用趨勢應由資料蒐集者大量追蹤當事人的線上（online）與線下（offline）行為，移轉至當事人自行管理其大數據個人資料將用於何種目的、提供給誰，以及如何使用。

亦即在強化資料可攜的前提下，大數據應用的光譜中應存在一介於蒐集者與當事人之間的具備安全性之第三方資料庫，讓當

[157]The European Commission,《Towards a thriving data-driven economy 》,2014。

事人得將其大數據個人資料儲存其中，並依其自由意願對外提供其個人資料，甚至以此賺取利益。

美國白宮科技顧問諮詢委員會（President's Council of Advisors on Science and Technology, PCAST）在 2014 年發布的《BIG DATA AND PRIVACY：A TECHNOLOGICAL PERSPECTIVE》報告中亦提到[158]，當事人可以在不同的第三方資料庫中設定不同的隱私偏好，而由該第三方資料庫機構協助確保當事人的隱私偏好執行，如此一來，將會自動產生隱私標準的協商市場。而為了吸引更多市場佔有，資料蒐集者（特別是小公司）會試圖將自己的隱私條款符合消費者的隱私偏好設定，該偏好設定是由不同的第三方資料庫機構提供，以此將資料的控制權交回資料當事人手中。

由於此因應方式尚涉及第三方資料庫的可靠性、可信任性、安全性與使用者友善性，在可預見的將來勢必將成為國際間探討的熱門議題。

五、去識別化（兼論法務部見解）

(一) 國際實務

資料蒐集者在將當事人資料用於大數據分析時，需決定將資料去識別化、匿名化，或保持其可識別性。國際上認為，個人資料在有效的「去識別化」後，將因無法以「合理可能」的方式識

[158]President's Council of Advisors on Science and Technology（PCAST）,《BIG DATA AND PRIVACY：A TECHNOLOGICAL PERSPECTIVE,2014.

別出特定當事人，因此該資料的利用即不違反個人資料保護法律（但將個人資料「去識別化」的行為仍構成個人資料的處理或利用行為，須受到蒐集目的限制原則的檢視）[159]。但「匿名化」的資料僅是蒐集者將當事人識別資訊暫時隱匿或以代號、假名取代，蒐集者而言仍能透過資料庫的勾稽識別出特定的當事人，因此並無法免除個人資料法律的適用。

實務上即有以「去識別化」資料作為蒐集者提供加值服務的合法要件，例如歐盟隱私與電子通訊指令（2002/58/EC）的立法前言第 26 條即規定「流量資料須將其去識別化後始可用於提供行銷通訊服務或提供加值服務」[160]。

然而，基於蒐集者對於個人資料利用的需求，其所採取的「去識別化」方式不盡然能完全達到避免「再識別」的風險，因此尚難有一致性的標準規範「去識別化」的條件，必須於具體個案中綜觀整體背景來檢視該等資料是否已達去識別化的效果。歐盟個人資保護指令第 29 條工作小組在 2014 年提出的《Opinion 05/2014 on Anonymisation Techniques》意見書中，列出三項判斷資料是否已達去識別化的基本要素：

1. 是否仍可能將特定當事人從資料群中單獨挑出；

[159]歐盟，Article 29 Data Protection Working Party, WP216,《Opinion 05/2014 on Anonymisation Techniques》, 2014。

[160]e-Privacy Directive （2002/58/EC）, Recital 26, "Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service."

2. 是否仍可能將特定當事人與其相關的紀錄作連結；

3. 既存資訊可否被推論與特定當事人有關。

若以此三項要素檢視現下實務上常見的去識別化技術，即能發現目前確實未有任何方式能達到百分百的去識別化。見下表：

表 3 各項技術之去識別化程度

	Is Singling out still a risk?	Is Linkability still a risk?	Is Inference still a risk?
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

（表來源：歐盟,《Opinion 05/2014 on Anonymisation Techniques》）

因此實務上即對蒐集者提出建議，認為對於所採取的去識別化技術仍可採取下列作為：

1. 持續評估風險與監控風險。

2. 持續評估去識別化的有效性與適當性。

3. 識別測試[161]，包含：

(1) 測試能否從資料群中識別特定當事人以及與其有關的私人屬性。

(2) 站在攻擊者的角度採取任何合理、可能的方式測試。

[161]英國 ICO,《Anonymisation：Managing Data Protection Risk》, 2012。

(3) 利用所有合法可取得的資料群（例如政府的開放資料）來比對測試可否識別特定當事人。

4. 蒐集者應揭露其所採取去識別化的技術為何。

5. 明確屬性（例如種族）或精準個人資訊（例如出生年月日）應從資料群中移除。

(二) 法務部見解

我國個人資料保護法之主管機關法務部亦同意「去識別化」作為因應個人資料保護的合理對策，其認為「個人資料運用技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料」[162]，是以雖然蒐集機關「所保有的整體資料仍然屬於個人資料，但其對外主動公開或被動提供去識別化後之資料並無違反個資法問題，因為當該資料對外公布釋出之時，其已不再是個人資料」[163]。

法務部並參考國外見解，將「去識別化」依其加工程度不同而區分為「匿名化資料」與「擬匿名化資料」[164]：

1. 匿名化資料（anonymised data）

匿名化資料必須對任何人(包含對原資料保有者)而言，均無法採取任何合理可能之方法識別特定個人，亦即資料經加工後，毫無保留連結之可能性；至於判斷資料是否已達匿

[162]法務部，103 年 11 月 17 日法律字第 10303513040 號函。

[163]法務部，105 年 1 月 22 日，《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 14。

[164]法務部，105 年 1 月 22 日，《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 8。

名化之程度，仍須評估各種情況而視個案而定，例如：即使在呈現聚集化統計或彙總資料時，樣本數是否超過足以識別特定個人之門檻。

2. 擬匿名化資料（pseudonymised data，假名化資料）

擬匿名化資料是以編碼或別名取代識別符（例如姓名、身分證號等），使研究或統計人員得以針對個體資訊進行分析而無須識別個體身分，可再分為兩種態樣：

(1) 不可逆（non-retraceable / irreversible）

此態樣欲使重新識別不具可能性，以非專屬代碼、單向加密或其他技術處理後，使任何人（包含原資料保有者）均無法透過資料比對或其他方式再直接或間接辨識出特定個人。

(2) 可逆（retraceable / reversible）

指以專屬代碼、雙向加密或其他技術處理後，編碼資料雖無從識別特定個人，惟原資料保有者仍得透過代碼與原始識別資料對照表或解密工具（鑰匙）還原為識別資料（例如：進行醫療實驗研究時，為能適時回溯追蹤調整對受試病患之醫療處置）。

對於原資料保有者而言，因其仍得透過對照表或解密工具等其他資料之對照、組合、連結而識別特定個人，該資料仍屬個人資料；而對資料接收者來說，如該擬匿名化資料之去連結程度性高，使資料接收者「運用一般知識

予以連結之再識別可能性甚小」，則可認為已非個人資料，而無個資法之適用。

此外，法務部認為，資料保有者可進行整體風險評估，綜合考量個人資料類型、敏感性程度、對外提供資料之方式、引發他人重新識別之意圖等因素，並根據風險評估之結果計算設定風險檻值[165]，依比例原則分級控管去識別化程度，例如[166]：

1. 供不特定人利用之開放資料，因並未限制資料提供之對象、使用目的或方法，而是以公開之方式提供，因此風險檻值相對較高，宜達「匿名化資料」或「不可逆之擬匿名化資料」之程度較為妥適。

2. 提供予特定人之資料，因提供對象有所限縮，除能對資料接收者之身分、使用目的、其他可能取得資料之管道、安全管理措施等先為必要之審查外，並得與資料使用者約定禁止重新識別資料之義務及其他資料利用之限制等，較有利風險的控管，因此風險檻值相對較低，去識別化之程度可相對放寬，可提供含有個體性、敏感性較為詳細之擬匿名化資料。

再就「無從識別的判斷標準」而言，法務部參酌國外實務之見，主張去識別化不可能毫無風險，僅能檢視其是否已排除「合理可能」識別特定個人之程度，是若釋出之資料本身雖不具有特定個人識別性，但如以此為線索，與「其他資訊」組合、比對下，亦得識別出特定個人時，則該資料將仍屬得間接識別之個人資料。

[165]風險檻值之概念應以資安風險管理理解，即針對風險評估後識別出的資安風險設定之標準值。

[166]法務部，105 年 1 月 22 日，《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 15。

從而，所謂「其他資訊」之範圍將會影響去識別化的判斷準據[167]。

對此，**法務部擬採「一般人基準說」為判斷依據，即所謂的「其他資訊」應限於已公開、被公知資訊，一般人於生活中如報章雜誌等媒體或圖書館等得輕易搜尋、獲得之資訊，以此作為基準，判斷有無「其他資訊」作組合、比對之可能**。蓋對於掌握「特殊（非一般）資訊」而有先前知識之人（例如同僚、親友、鄰居、醫師、律師等）而言，雖然其因具有先前知識而增加得以間接識別之可能性，但對於當事人所增加之隱私風險實際上很低（因為該人本即保有當事人之個資始有能力得以重新識別），因此重點並非其能否重新識別當事人，而應在於其透過釋出之資料能否取得當事人之新的個人資料。

六、隱私保護內植設計

加拿大隱私保護主管機關 Information Commissioner's Office of Canada 在 2008 年提出隱私保護內植設計（Privacy by Design）的觀念，強調蒐集者對於個人資料的隱私保護應從被動的「事後法規遵循」轉變為主動的「事前機制導入」，也就是讓「隱私保護」成為蒐集者推行各項政策、計畫、服務、產品、流程的「預設模式」，在規劃設計之初即納入隱私保護觀念，以強化對於當事人隱私的尊重

隱私保護內植設計（Privacy by Design）發展至今，已成為大數據技術下對於當事人個資與隱私保護的基本作為，其七大原則為：

[167]法務部，105 年 1 月 22 日，《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 16。

(一)Proactive not Reactive; Preventative not Remedial：強調隱私的保護應從事前即開始規劃設計，而非事後才來檢視適法差異或進行補救、賠償措施。

(二)Privacy as the Default Setting：將當事人的隱私保護設定為政策、計畫、作業、服務、產品等面向的預設模式。使當事人無須更改設定或行使權利，其隱私權便已獲得最大程度的保障。

(三)Privacy Embedded into Design：在設計中導入隱私觀念，即在每一流程均須考慮到對於當事人的隱私保障。

(四)Full Functionality-Positive Sum, no Zero-sum：透過每一環節均針對隱私保護進行考量，以此達到隱私保護與目的功能不相衝突的雙贏局面。

(五)End-to-End Security-Full Lifecycle Protection：以個人資料的生命週期為標的規劃完整的隱私保護機制。

(六)Visibility and Transparency-Keep it Open：保持開放與透明，讓當事人能隨時參與保護自己的隱私或行使權利。

(七)Respect for User Privacy-Keep it User-Centric：以當事人為中心，尊重當事人的隱私。

七、隱私衝擊評估

有鑑於大數據技術涉及大量、多元、長期的資料彙整與分析，蒐集者的隱私衝擊評估（Privacy Impact Assessment, PIA）將更顯重要。

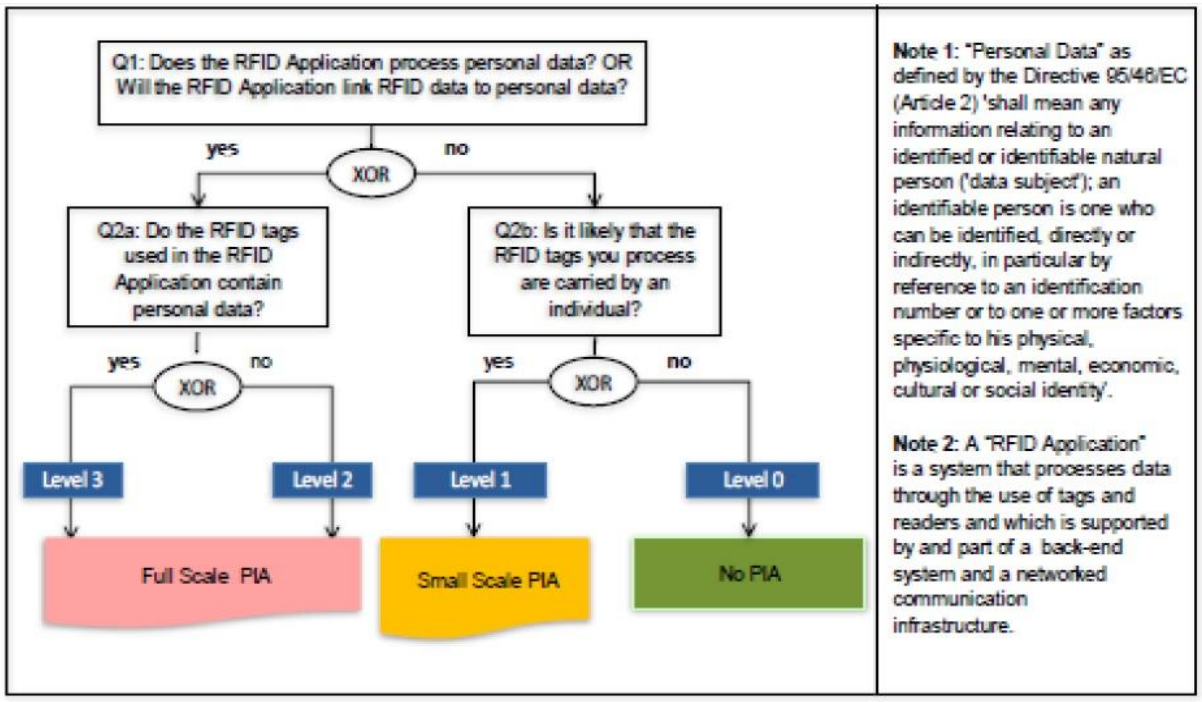
歐盟委員會（European Commission）於 2011 年針對 RFID 的智慧聯網技術提出《Privacy and Data Protection Impact Assessment Frameworkfor RFID Applications》，其中的隱私衝擊評估框架即可作為大數據分析的適用參考依據[168]：

(一) 框架評估階段

此階段之目的在於判斷目標產品或服務是否因涉及個人資料或隱私議題而須執行隱私衝擊評估，如有需要，應採取完整規模的評估(Full Scale)或簡易型的評估(Small Scale)即可，但簡易型評估的項目與完整型評估相同，僅在風險識別上判斷為較低程度的隱私衝擊。判斷流程見下圖：

圖 1 隱私衝擊框架評估

[168]The European Commission, 《Privacy and Data Protection Impact Assessment Frameworkfor RFID Applications》,2011。



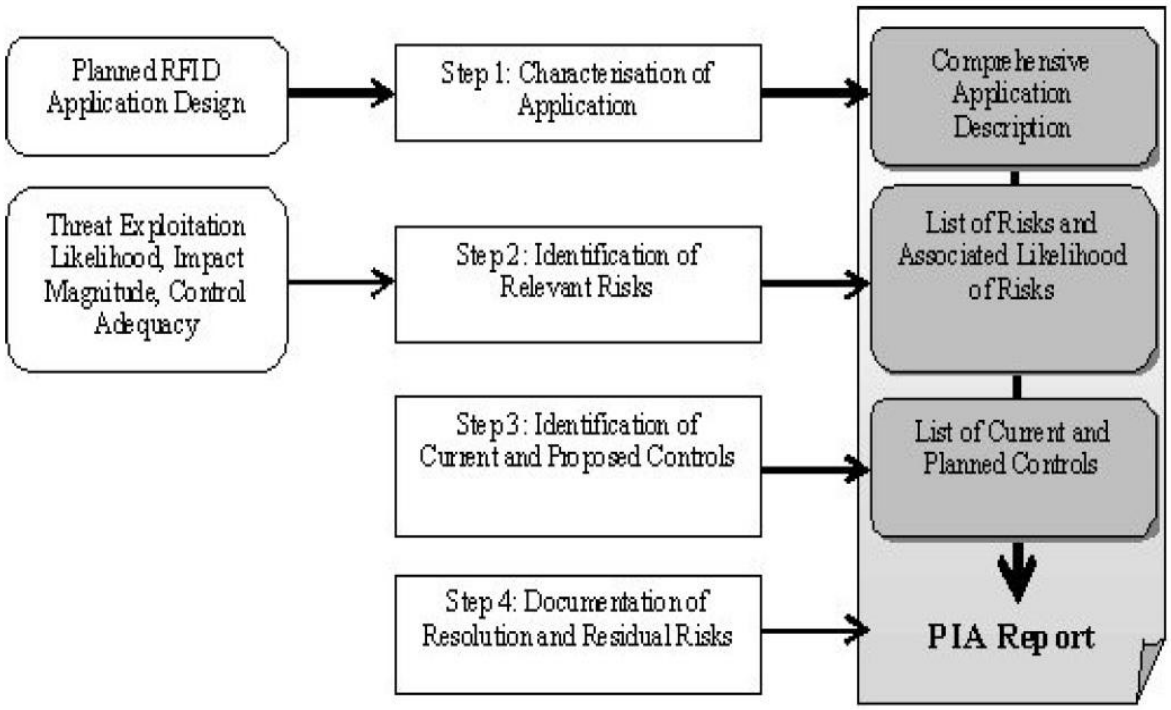
(圖來源：歐盟，《Privacy and Data Protection Impact Assessment Frameworkfor RFID Applications》)

(二) 風險評估階段

此階段即採下方四步驟執行隱私衝擊分析，詳見下圖：

1. 描述產品或服務。
2. 識別產品或服務可能造成的隱私威脅並評估風險發生的可能性。
3. 將已採行或將採行的管理面及技術面之風險控管方式列出。
4. 將各項風險對應之控管方式分析後產出評估報告。

圖 2 隱私衝擊評估流程



(圖來源：歐盟，《Privacy and Data Protection Impact Assessment Frameworkfor RFID Applications》)

八、著重資料利用而非資料蒐集與分析

由於大數據技術的最終目的並非在於大量彙整與分析資料（此為手段），而是看中資料彙整分析後的實際應用利益，因此國際上亦有提倡在大數據趨勢下，個資保護的重心應著重的資料分析後的利用方式，而非資料的蒐集與分析行為。

美國白宮科技顧問委員會（President's Council of Advisors on Science and Technology，PCAST）於 2014 年提出《BIG DATA AND PRIVACY：A TECHNOLOGICAL PERSPECTIVE》報告，從科技的角度解讀大數據時代下的隱私保護，便是從上述觀念提出建議[169]：

[169]President's Council of Advisors on Science and Technology（PCAST），《BIG DATA AND PRIVACY：

(一)政策不應聚焦於大數據資料的蒐集及分析：

在大數據的應用上，通常都是電腦程式或應用程式，與原始數據（raw data）或分析結果相互作用而成。在這個形式下，並不是資料本身造成損害，也不是電腦程式（在沒有資料的情況），而是兩者加在一起造成損害。因此，除非藉由嚴格且對經濟有損害的措施，否則限制蒐集及保存的行為將會愈來愈無法執行。

(二)政策應著眼於大數據的實際利用：

為了避免政策制定落後於科技，與個資或隱私保護有關的政策應該要處理目的（the “what”），而非機制為何（the “how”）。舉例來說，藉由要求去識別化技術的使用而規範關於健康資訊的揭露，則將漏未規範到資料融合的情況；藉由控制學校所持有學生紀錄的檢查而規範關於未成年人資訊的保護，則將漏未規範到學生資訊由線上學習系統所取得的情況。

正確的因應，應是不論資料如何取得，對不適當地揭露健康資訊或學生表現資訊的規範才是更健全的方法。

九、國際傳輸

如前章所述，大數據技術的發展將使當事人資料在各國各地流動，但由於各國對於個人資料保護的要求寬嚴不一，對於個人資料國際傳輸的限制條件也多有不同，因此目前如何因應國際間

A TECHNOLOGICAL PERSPECTIVE》,2014。

的大數據資料彙整分析仍是各國個資保護機關面臨的難題。

本研究團隊於 2015 年 12 月 2 日出席澳門個人資料保護辦公室舉辦的「大數據・大挑戰─私隱保護與合作」研討會，會中來自澳洲、紐西蘭、葡萄牙等國的個資保護專員即針對大數據時代的資料跨境傳輸因應發表意見，但仍多為探討國際間的行政、法律機關合作議題，亦即對於跨國企業的大數據資料蒐集彙整如涉侵害當事人權利時，各國個資保護機關應建立妥適的合作機制以共同行政稽查權利。

以下僅以歐盟對於國際傳輸個資之條件為例，提供我國可資參考的相應規範。

(一) 歐盟個資保護基礎規則

1、 傳輸（transfer）的定義

包括從第三國或國際組織轉送到另一個第三國或國際組織（第 40 條）。

2、 具備「適足（個資保護）」要件

經過執委會認定對於個人資料有充足保護（adequate level of protection）的國家/領土/第三國之處理部門（processing sector），可不須得到進一步的批准進行個人資料國際傳輸，考量因素如下：

(1) 依該國/國際組織之法律規範、專業規則與安全措施，當事人得要求行政或司法救濟之權利，特別針對居住在歐盟境內之個人。

(2) 設有確保遵循個資保護規則之獨立監督機關存在，以協助與提供諮詢讓當事人行使其權利。

(3) 該國/國際組織作出的國際承諾。

3、 執委會決定

執委會得作出資料接受國是否符合「適足(個資保護)」之決定，且應將決定結果列表公布（第 41 條)。

4、 資料提供者舉證

若執委會未依前項規定作出決定,則個人資料的提供者（控制者或處理者)得舉證已有適當的保護措施(appropriate safeguard),而能將個資移轉到第三國或國際組織(第 42 條)；適當的保護措施如下：

(1) 資料提供者與資料接受者間存有約束性企業規則（corporate rule)。

(2) 資料提供者與資料接受者間存有經執委會或是獨立監督機關接受的標準個資保護契約條款（standard data protection clauses)。

(3) 資料提供者與資料接受者間存有已被監督機關批准之契約條款。

5、 例外規定

即便未得到資料接收國具備「充足（個資保護)」要件之決定，亦無適當的保護措施，在符合與歐盟個人資料保護

指令第 26 條規範相仿的列舉情況下，個資仍能傳輸至第三國或國際組織：

(1) 會員國得在下列情況向未符合充足（個資保護）要件之第三國或國際組織傳輸個人資料：

A、 當事人明確同意。

B、 傳輸係為了實施資料當事人與資料控制者間契約之必要，或是因應當事人的要求為締結契約之準備行為。

C、 傳輸係為了締結或履行資料提供者與第三方間，對於資料當事人之第三方利益契約。

D、 傳輸係為了重大公共利益之必要或是法律要求，或以法律聲明之建立、實施或防禦為目的。

E、 傳輸係為了保護資料當事人之重大利益。

F、 傳輸係依據法規須提供給公眾之資訊，並公開給一般大眾或是有合法利益之人查詢，但僅及於該個案符合法定之查詢條件的範圍內。

(2) 適當契約條款（contractual clauses）

A、 若資料控制者舉證有適當的保護措施以保護隱私權與個人自由與實施基本權利時，會員國得允許資料控制者傳輸個人資料到未符合充足（個資保護）要件之他國，此保護措施得由適當「契約條款（contractual clauses）」而落實。

B、 會員國應通知執委會與其他會員國其依照前述規定所為之允許。

C、 如執委會以「標準契約條款」規範適當保護措施時，會員國應採取必要措施在其允許的適當契約條款中落實執委會的標準。

6、 主管機關合作

執委會與監督機關應採取適當行動合作保護個資，例如發展跨國合作機制來促使個資保護之執行等（第 45 條）。

(二) 歐盟—美國隱私防衛（EU-U.S. Privacy Shield）

歐盟與美國本於 2000 年起便以美國資料接受者遵守「安全港（Safe Harbor）隱私原則」作為歐盟許可的適足（個資保護）要件，而得由歐盟境內的資料提供者傳輸個資至該美國的資料接受者。然而，歐洲法院（European Court of Justice）在 2015 年 10 月的判決中宣告安全港隱私原則無效，造成歐盟資料提供者對美國資料接受者的個資傳輸要件失所附麗。有鑑於此，美國商業部遂於 2016 年 2 月制頒「New framework for transatlantic exchanges of personal data for commercial purposes：the EU-U.S. Privacy Shield」[170]，欲以此「隱私防衛框架」取代原安全港隱私

[170]Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework, https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework 最後到訪日 105 年 4 月 14 日。

原則。茲就其基本原則簡要介紹如下：

1、 告知義務

此原則規範機關的應告知事項及告知時機，包含蒐集的個資類別、蒐集目的、遵守隱私防衛原則的承諾、當事人權利及行使管道、擬揭露個資的對象及目的、當事人得限制資料使用或揭露的選擇權與行使方式、該機關受到美國相關主管機關管理等。

2、 當事人選擇權

此原則要求機關提供當事人選擇拒絕（Opt-Out）「資料被揭露予第三人」或「資料被用於與原始蒐集目的重大不符之新目的」的權利。

3、 傳輸資料者責任

(1) 如機關欲將個人資料傳輸予第三人，須遵守前述告知義務與當事人選擇權原則，並應以契約要求該第三人僅得於當事人同意的特定目的限制內使用當事人個資，且要求第三人以同樣程度遵守隱私防衛原則。

(2) 如機關欲將個人資料傳輸予受託處理個資者時，機關僅得在原始蒐集個資之目的限制內為之，且須確保受託者的個資保護措施應至少遵守隱私防衛原則，並應採取合理的適當措施監督受託者是否遵守該原則。

4、 安全維護

此原則要求機關採取合理而適當之安全維護措施以避

免個資侵害事故的發生。

5、 個資品質與目的限制

此原則要求機關僅得於蒐集個資之目的內使用當事人的個人資料，且機關應採取合理步驟確保當事人個資的完整、正確與即時。

6、 當事人近取權

此原則要求機關確保當事人得行使其更正、刪除個資等當事人權利。

7、 申訴、執行與義務

此原則規範機關落實個資保護應有的管理機制，以及主管機關的執行權力與機關應盡之義務。

十、開放資料

公部門的開放資料（Open Data）為國際趨勢，旨在促成政府資料的「創新應用」以達成「資料價值的最大化」，並同時建立政府行政的「透明性」及「歸責性」。

由於開放資料同樣須利用大數據分析技術，因此其適用原則亦可作為大數據分析之參考依據。

歐盟個人資保護指令第 29 條工作小組於 2003 年制定《公部門資訊再利用指令》（Re-use of Public sector information，PSI，2003/98/EC），並於 2013 年提出修正（PSI，2013/37/EU），其中說明資料再利用的原則為：

(一) 開放資料庫查閱。

(二) 提供標準電子格式。

(三) 任何人均可查閱，無需篩選。

(四) 免費或少許費用。

(五) 未限制商業或非商業用途（可採許可制）。

該指令雖未將資料開放與再利用規範為歐盟成員國政府的義務，但已允許並鼓勵成員國政府將公部門資料開放與再利用。

美國政府於 2009 年 12 月 8 日，在歐巴馬總統首度任命的聯邦資訊長和技術長領銜之下，在公眾諮詢的程序完成後，聯邦政府發佈《開放政府指令》（Open Government Directive），要求聯邦預算與管理局（Office of Management and Budget）針對聯邦各級單位明確訂定措施，以實現政務透明、公民參與以及協作政府的準則。

而我國政府自 101 年由行政院科技會報辦公室舉辦公開資料加值推動策略會議以來，已陸續建置各項政府資料開放平台，行政院更於 104 年啟動 Open Data 深化應用元年，加速釋出政府資料。凡此均在在顯示政府公部門的資料開放將是我國與國際接軌的重要指標，且是我國政府致力達成的目標。

然而，即便開放資料為政府致力目標，但開放之資料如涉及個人資料時，本質上極易與當事人的個資保護有所牴觸。102 年民眾控告健保署一案即為適例，該案緣起為民眾不滿健保署在欠缺法律授權又未得到當事人同意的情況下，將其健保就醫資料於

「全民健保財務之政策規劃、管理及監督」之「目的外」提供予國家衛生研究院建置的「全民健康保險研究資料庫」及衛生福利部的「健康資料加值應用協作中心」（以下簡稱協作中心）進行資料庫彙整及資料加值，並進而供第三人取得健康保險資料檔，因此循行政救濟途徑提起訴願，遭駁回後再向臺北高等行政法院提起行政訴訟。該案雖於 103 年 5 月遭臺北高等行政法院判決駁回原告之訴，但經上訴後，最高行政法院卻於同年 11 月以「新舊法適用錯誤」之理由予以廢棄發回，使得該案至本研究報告交付日（105 年 4 月 14 日）止仍未有定論。

簡繹臺北高等行政法院判決可知，法院一方面認定全民健保資料的加值統計應用有其公益目的，且經協作中心的匿名化處理後已無從自各項資料時別特定個人，對當事人資訊隱私權保障即屬無虞；另方面法院亦認為個人資料保護並非絕對權利，如法律已限制當事人的事前同意權，即應同時限制當事人的事後排除權，避免當事人的資訊自主權凌駕於公共利益之上，阻礙個人資料的合理利用。

但此見解應仍有探究空間，如前所述，「去識別化」的技術仍無法完全避免「再識別」技術的可能，當事人的資訊隱私權是否能徹底獲得保障尚有疑慮；「去識別化」亦為個人資料的處理或利用行為，仍須受到個人資料保護法律的規定，包含事前「向當事人告知」及事後「允許當事人退出」等機制，以此貫徹當事人的資訊自主權。

第二節　智慧聯網

與大數據分析的情況相似，智慧聯網技術的發展也面臨個資與隱私保護的議題，尤其在「智慧居家」市場熱絡的趨勢下，資料透過蒐集者透過穿戴裝置或家中的感應器、閘道器而長時間持續蒐集大量個資，更易觸及「居家活動」此隱私保護的核心價值。而隨著技術的發展，數位機上盒已是常見於家庭中的閘道器，有線電視業者可透過數位機上盒與網際網路的連結而發揮智慧聯網的功能，大量取得家庭成員的活動、作息、習性的個人資料。

一、歐盟個人資料保護指令第 29 條工作小組

有鑑於此，歐盟個人資料保護指令第 29 條工作小組在 2014 年頒布《Opinion 8/2104 on the Recent Developments on the Internet of Things》[171]，對於智慧聯網的發展提出關鍵議題觀察，例如：

(一) 資訊不對稱與缺乏控制權。

(二) 缺少同意之品質。

(三) 目的外利用個資。

(四) 未經告知的行為模式分析或側寫。

(五) 難以完全去識別化。

(六) 資料安全風險。

同時該意見書亦對利用智慧聯網蒐集使用者個資的業者提出具

[171]歐盟，Article 219 Data Protection Working Party, WP223,《Opinion 8/2104 on the Recent Developments on the Internet of Things》, 2014。

體建議，例如：

(一) 事先針對產品或服務進行隱私衝擊評估。

(二) 在將大量資料彙整成集合資訊(去識別化)後便應將原始資料(可識別個人)刪除。

(三) 落實隱私保護內植設計（Privacy by Design）及隱私保護預設（Privacy by Default）。

(四) 對使用者提供可隨時行使當事人權利之方式。

(五) 應以友善且便於閱讀之方式向使用者揭露隱私權政策，不可綑綁記載於蒐集者網站上的服務條款中。

(六) 任何重要事項皆應透過使用者的聯網裝置即時通知。

二、美國聯邦貿易委員會(FTC)

除歐盟提出意見之外，美國聯邦貿易委員會也在 2015 年 1 月發布《Internet of Things, Privacy & Security in a Connected World 》工作報告[172]，其中針對智慧聯網在資料安全部分建議業者：

(一) 落實資訊安全預設（Security by Design）。

(二) 提升內部開發智慧聯網產品或服務之同仁的資安能力。

(三) 確保自己或供應商有能力維持且確認智慧聯網產品或服務的資訊安全。

(四) 不可僅依賴使用者自身的資安防護（例如設定家中無線路由器密

[172] 美國，FTC，《Internet of Things, Privacy & Security in a Connected World 》,2015。

碼），而須深入強化產品或服務的每一層安全措施。

(五) 應考量可行的存取控管與驗證程序，以阻止任何未經授權而使用者的裝置、資料或網路之行為。

(六) 持續監控智慧聯網產品或服務的生命週期，並隨時修正脆弱點及其他經識別出的風險。

第三節　本章結論

綜上所述，「強化告知義務」、「加強保障當事人的資料控制權」、「加強資料蒐集者的遵法與安全維護責任」是目前國際上針對大數據與智慧聯網技術發展之個資與隱私保護議題的多數建議。本研究報告將於第六章將各項建議對應我國法律規範檢視，分析我國是否對於通訊傳播事業發展大數據與智慧聯網技術的個資與隱私保護均已含括於現有或將有之法律當中。

第六章 我國對於通訊傳播事業個人資料保護之規範

國際上對於個人資料與隱私保護的實體規範與監管方式，以及對大數據及智慧聯網技術蓬勃發展下的個資與隱私保護議題與建議已如前揭章節所述，以下將由我國相關法律及草案的角度，分析目前國內實務對於大數據與智慧聯網趨勢之個人資料蒐集、處理、利用及資料蒐集者責任的適用規範。

第一節　法律規範

一、個人資料保護法與民國 104 年 12 月最新修正

(一) 目的限制原則

如前所述，「目的限制」為國際上對於個人資料保護的重要原則，我國個人資料保護法亦將其納入立法精神之中，於第 15 條及第 19 條分別針對公務機關與非公務機關規定其蒐集個資應有「特定目的」；又針對公務機關與非公務機關利用個人資料的行為，在第 16 條及第 20 條規定原則上須與蒐集之特定目的相符。並更於總則第 5 條規定「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯」。

(二) 告知義務

個人資料保護法第 8 條第 1 項規定「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名

稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」；第 9 條第 1 項規定「公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。」

(三) 當事人同意

在立法院於 104 年 12 月 15 日新修正通過個人資料保護法若干條文前（見下述），本法所稱之「當事人同意」依第 7 條、第 15 條、第 16 條、第 19 條、第 20 條等規定係指在蒐集機關事先告知特定事項後，以「書面」作成之意思表示，且該書面要件僅在符合《電子簽章法》之規定時，始得以電子文件為之。

(四) 當事人權利

依個人資料保護法第 3 條規定，資料當事人原則上對其個人資料享有「查詢、閱覽、補充、更正、請求製給複製本、請求停止蒐集、處理、利用、請求刪除」等權利，不得預先拋棄或以特約限制。

(五) 資料保存

個人資料保護法第 11 條第 3 項本文規定「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料」。

(六) 國際傳輸

由個人資料保護法第 21 條規定「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。」可知，現階段我國對於個人資料的國際傳輸是採原則允許，例外得由中央目的事業主管機關予以限制的立法模式。

然而，在未有統一判斷標準的情況下，由於各中央目的事業主管機關對於個人資料保護法規的認知差異，難免造成各事業的管制落差，雖然法律立意或為使各中央目的事業主管機關針對所轄事業的特性而設定標準，但於實務執行上恐有窒礙難行之處。

另電子通訊傳播法草案第 21 條第 1 項規定「提供電子通訊服務傳播者或提供接取服務之使用人於我國境內者，不得以不合營業常規之方式規避經由我國境內通訊傳播設施傳輸、接取、處理或儲存與使用人相關之電子訊息」，亦是針對個人資料的國際傳輸設立規範。

惟與個人資料保護法第 21 條相同的是，所謂「不合營業常規」之標準為何並不明確，恐將造成適用上的爭議；且從體系解釋來看，本條既係存在於「個人資料之保護」章節，則立法考量即應由「個資保護」的角度開展，亦即縱使「合

於營業常規」，但若該行為將使當事人的個人資料有受侵害之虞時，仍不應貿然無條件允許個人資料的國際傳輸。是本條立法的構成要件恐將無法達成所欲保護之法益。

(七) 蒐集者責任

1. 安全維護義務

個人資料保護法第 18 條與第 27 條分別規定公務機關保有個人資料檔案者，應指定專人辦理安全維護事項；非公務機關保有個人資料檔案者，應採取適當之安全維護措施，以確保個人資料不受到侵害。

而所謂安全維護事項或適當之安全措施，依個人資料保護法施行細則第 12 條第 2 項規定，係由公務機關或非公務機關在符合比例原則的前提下採取包含風險評估、建立管理程序、安全稽核、紀錄保存等作為[173]。

2. 事故通知義務

依個人資料保護法第 12 條規定，公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

[173]個人資料保護法施行細則第 12 條第 2 款「前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善」。

值得注意的是，此處的事故通知對象並非如同其他國家較多規範為「個資保護主管機關」，而是要求蒐集機關逕行通知當事人，應是考量我國並無個資保護專責機關之故。但發生事故的蒐集機關在實務上是否以及如何對當事人通知，則有待持續觀察。

(八) 105 年 3 月 15 日施行之新個資法

個人資料保護法自 101 年施行以來，難免遭遇窒礙難行或有發現缺漏之處，是以立法院在 104 年 12 月 15 日通過修正若干條文，並依行政院公布於 105 年 3 月 15 日施行，其中與本研究之通訊傳播事業有關者為：

1. 同意方式放寬

新修正之個人資料保護法於第 15 條、第 16 條、第 19 條及第 20 條中將原本規定當事人「書面」同意之要件刪除，不再要求資料蒐集者取得當事人同意的要式性。

更在第 7 條第 3 項增加「公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意」的「推定同意」；同時在第 7 條第 4 項將「當事人同意之事實」交由蒐集機關承擔舉證責任。

2. 以契約關係為由蒐集個資的要件限制

新修正之個人資料保護法將第 19 條第 1 項第 2 款增

修為「與當事人有契約或類似契約之關係，且已採取適當之安全措施」，亦即要求蒐集機關即便基於與當事人間的契約關係，為履行該契約而須蒐集個人資料，但仍須以針對所擬蒐集之資料採取適當之安全措施為前提，否則依條文文意觀之，似無法認定為合法蒐集。

二、電信法

(一) 背景

我國現行電信法所規範的「電信」依第 2 條第 1 款係指「利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息」;「電信事業」依同條第 5 款指「經營電信服務供公眾使用之事業」;而「通信紀錄」依同條第 8 款則為「電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則。電信號碼係指電話號碼或用戶識別碼」。

(二) 通信秘密

1. 第 6 條第 2 項規定「電信事業應採適當並必要之措施，以保障其處理通信之秘密」。

2. 第 7 條第 1 項規定「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同」。

三、通訊保障及監察法

(一) 背景

我國通訊保障及監察法於 103 年新增第 3 條之 1 及第 11 條之 1，將通信紀錄（見下述）及通訊使用者資料（見下述）規定為原則上須有法院核發之調取票始得取得。

(二) 通信紀錄與通訊使用者資料

第 3 條之 1 規定「本法所稱通信紀錄者，謂電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄（第 1 項）。本法所稱之通訊使用者資料，謂電信使用者姓名或名稱、身分證明文件字號、地址、電信號碼及申請各項電信服務所填列之資料（第 2 項）」。

四、資通安全管理法草案

(一) 背景

有鑑於資通科技之應用已普及至公、私部門，相對應之資通安全風險議題已引發各界之注意。為有效規劃我國之資通安全管理政策及其策略，並落實於公、私部門，以建構一個安心與安全之資通使用環境，進而確保民眾數位生活福祉、資安產業發展及數位國土國家安全[174]，我國遂於近年推動「資通安全管理法」之制定。

(二) 資通安全維護計畫

第 16 條第 2 項規定「中央目的事業主管機關得指定非

[174]資通安全管理法草案，2015 年 10 月 2 日版，第一條立法理由。

公務機關所提供之產品或服務，制定及實施資通安全維護計畫」；第 4 項規定「第二項計畫之標準、內容與其他遵循事項，由中央目的事業主管機關定之」。

(三) 資通安全標準

第 20 條規定「中央目的事業主管機關得協助未受指定之事業，發展或遵循相關產品或服務之資通安全標準」。

五、電子通訊傳播法草案[175]

(一)背景

鑒於科技匯流業已逐漸弭除傳統通訊傳播產業間壁壘分明之界線，跨媒體之經營亦影響新世代通訊傳播技術及服務發展模式，曩昔依業別不同，而循個別管制政策目的分別立法規管之垂直管制模式，實有重新檢視正當性而進行調整之必要[176]。是我國考量傳統分流之電信、廣播電視與電腦網路已藉由網際網路高度匯流，遂意以電子通訊傳播為規範主體，以民事權利義務關係為主軸，制定電子通訊傳播行為的一般性規範。其中關於使用人個人資料之規範如下所述。

(二) 告知事項

第 12 條第 1 項第 1 款規定，提供電子通訊傳播服務者應依其服務性質，以得清楚辨識之方式公告其服務使用條款，

[175]電子通訊傳播法草案，105 年 5 月版。

[176]電子通訊傳播法草案，105 年 5 月版，總說明。

包含「隱私權與資訊政策，包括下列事項：1.適用之範圍與例外。2.蒐集之資訊類型與蒐集理由。3.使用資訊之方式。4.提供使用人存取、使用及更新資訊之服務方式」。

(三) 資訊安全防護機制

第 17 條規定「提供電子通訊傳播服務者應建立符合其服務所需之資通安全防護機制」。

六、無線廣播電視事業與頻道事業管理條例草案[177]

(一) 背景

有鑑於數位匯流下，考量廣播電視產業變化仍有異於通訊產業，且其使用公共之無線電波頻率，肩負有促進多元文化、維護本國文化及保障兒少等弱勢權益之社會責任，復基於廣播電視產業於內容製作、營運方式及網路設置之要求，均有其特殊之歷史背景與需求，因此，以漸進匯流方式，維持現行垂直式整合型態，內容部分則予以調和管制程度，並因應現階段就專門性、特殊性或臨時性事項之需求，分就不同類型之廣電事業之營運，予以專章規範[178]。

(二) 服務契約

第 65 條第 2 項第 5 款規定事業在與用戶訂定之服務契約中應載明「用戶個人資料蒐集、處理、利用之範圍」。

[177]無線廣播電視事業與頻道事業管理條例草案，105 年 5 月版。

[178]無線廣播電視事業與頻道事業管理條例草案，105 年 5 月版，總說明。

七、有線多頻道平臺服務管理條例草案[179]

(一) 背景

鑑於民眾透過纜線收視多頻道節目方式已日趨多元，固網及有線電視系統互跨經營亦蔚為常態，過去依業別管制環境下所制定或修正之規範或管理措施，形成繁複且落差之監理架構，有需要重新調整之必要。而現行電信法將電信定義為「利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息」，內容實與有線廣播電視法「以設置纜線方式傳播影像、聲音，供公眾直接視、聽」之有線廣播電視定義相近[180]，因此我國擬統合以往區分為不同平臺分別管理的有線多頻道平臺服務，並視其為電信事業所提供的一種特殊服務樣態予以管制，始推動本條例之制定。

(二) 用戶資料及收視紀錄

第 34 條第 2 項 5 款規定提供有線多頻道平臺服務之電信事業在與用戶訂立之服務契約中應記載「用戶資料與收視紀錄之蒐集、處理、利用之方式及限制」。

第二節　國家標準

為建立個人資料去識別化的標準供資料蒐集機關依循，我國行政院近來規劃透過第三方驗證機制以提供專業意見，並指示經濟部標準

[179]有線多頻道平臺服務管理條例草案，105 年 5 月版。

[180]有線多頻道平臺服務管理條例草案，105 年 5 月版，總說明。

檢驗局參考國際標準（ISO）調和制定國家標準 CNS 29100 及 CNS 29191，並訂定「個人資料去識別化過程驗證要求及控制措施」，內容包含：「用語及定義」、「隱私權政策」、「PII（個人可識別資訊）隱私風險管理過程」、「PII 之隱私權原則」、「PII 去識別化過程」、「重新識別 PII 之要求（此為選項，僅適用於允許重新識別之情形）。

目前（105 年 4 月）已有財團法人台灣電子檢驗中心提供驗證服務，並提出「個人資料去識別化過程控制措施對照自評表」供申請驗證者預先自評，內容如下[181]：

表 4 財團法人台灣電子檢驗中心「個人資料去識別化過程控制措施對照自評表」

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
參、隱私權政策			
要求事項 (3.1)	涉及 PII 處理之組織的高階管理階層，應依營運要求及相關法律與法規，建立隱私權政策，提供隱私權保護之管理指導方針及支持。		☐符合 ☐不符合 ☐部分符合 ☐不適用

[181]見財團法人台灣電子檢驗中心網站，http://www.etc.org.tw/驗證服務/個人資料去識別化過程驗證.aspx，最後到訪日 105 年 4 月 14 日。

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 3.1.1	隱私權政策應如下： －合於組織目的。 －提供設定目標之框架(包含管理委員會之組成、職掌、召開時機；各工作小組之組成、任務；反應及溝通管道；員工教育訓練之要求等)。 －包括滿足適用之隱私保全要求事項的承諾。 －包括持續改善之承諾。 －於組織內傳達。 －公眾(或相關各方)可適時且容易取得。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3. 1.2	組織應以書面載明其隱私權政策。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.3	隱私權政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.4	隱私權政策應依不同隱私權利害相關者，補充更詳細之 PII 處理規則及義務(例：特定部門或員工之程序)。		☐符合 ☐不符合 ☐部分符合

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
			☐不適用
控制措施 3.1.5	隱私權政策應載明，用以增強隱私權政策之存取控制、告知條款、稽核等特殊設置。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.6	內部隱私權政策應載明組織採用之目標、規則、義務、懲處規定、限制及/或控制措施，以滿足與其 PII 處理生命週期各階段有關之隱私保全要求事項。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 3.1.7	組織應傳達予隱私權利害相關者下列資訊： －PII 控制者及所有相關之 PII 處理者的身分。 －關於移轉 PII 至 PII 處理者之政策。 －蒐集 PII 之目的。 －識別將蒐集之 PII。 －加強隱私權保護之作為及其目的。 －PII 當事人對其被蒐集之 PII 的法律權利。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施	外部隱私權政策應提供外部人員對組織隱私權實務作法聲明，以及其他		☐符合

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
3.1.8	相關資訊，如 PII 控制者之身分及辦公室地址、PII 當事人可能取得額外資訊之連絡窗口等。		☐不符合 ☐部分符合 ☐不適用
控制措施 **3.1.9**	組織應具備正式懲處過程，並傳達予員工及約用人員，以對違反隱私權者採取行動。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **3.1.10**	(告知之透明性)**若** PII 處理者非 PII 控制者，則 PII 處理者之隱私權政策應依循 PII 控制者之隱私權訂定。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **3.1.11**	組織若進行 PII 去識別化過程，則隱私權政策應包含下列項目，並應對外公布適宜之內容： －敘明組織之去識別化作法，並以一般用語描述將使用何種去識別化技術。 －敘明備妥何種保護措施，以盡量減少可能之相關風險。尤其是，應敘明去識別化資訊是否會對外公開或僅有限揭露，及其公開原則(例：離群值之處理、K-匿名性之使用時機)。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
	－敘明對公眾開放去識別化資料之相關風險。 －敘明關於公布已去識別化資訊之推理過程，說明如何衡量及取捨、考量或未考量哪些因素、原因為何。		
控制措施 3.1.12	組織若開放 PII 去識別化資料，應對資料開放對象敘明使用去識別化資料之相關風險，以及不當使用去識別化資料應負之責任。		☐符合 ☐不符合 ☐部分符合 ☐不適用
肆、PII 隱私風險管理過程			
要求事項(4.1)	組織應定期執行廣泛之 PII 風險管理活動並發展與其隱私保護有關的風險剖繪。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 4.1.1	組織應建立 PII 處理生命週期各階段之風險管理過程。各階段之風險管理應包含下列子過程： －建立全景過程：藉瞭解組織(例：PII 處理、職責)、技術環境及影響隱私風險管理之因素(亦即法規因素、契約因素、營運因素與其他因素)達成。 －風險評鑑過程：藉識別、分析及		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
	評估 PII 隱私權原則之風險(可能有負面影響之風險)達成。 — 風險處理過程：藉定義隱私保全要求事項、識別及實作隱私控制措施以避免或減少 PII 隱私權原則之風險達成。 — 溝通及諮詢過程：藉從利益相關者得到資訊、對每一風險管理過程獲得共識，以及通知 PII 當事人與溝通風險及控制措施達成。 — 監視及審查過程：藉追查風險及控制措施，以及改善過程達成。		
陸、PII 去識別化過程			
要求事項(6.1)	組織應建立有效且周延之 PII 去識別化過程的治理結構		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 **6.1.1**	組織應指定足夠數量具技術與法律知識之員工或約用人員進行 PII 去識別化。並應指定資深員工，負責授權及監督 PII 去識別化過程。 此負責人員應有能力負責 PII 去識別化主要決策、宣達及協調組織之 PII 去識別化作法、召集組織內部及外部相關專家，並應能協助高階管理階層決定已去識別化資料之適當揭露形式(亦即公開或有限存取)。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.1.2**	應經由人員訓練，使 PII 去識別化工作人員清楚認識 PII 去識別化技術、所涉及之所有風險及減輕此等風險之措施。尤其是，各工作人員應了解其於確保安全進行去識別化之特定角色。	抽問	☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.1.3**	應提供獨立及隔離(無法連線)空間(及系統)進行 PII 去識別化工作，並管制及記錄人員與資料之進出(及存取)，且人員不得攜帶任何具照像及記錄功能之設備進入工作區域。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.1.4**	應備妥以文件記錄之程序，識別判定是否對資料進行 PII 去識別化、其實施方法、產生之資料是否需揭露、揭露原則及揭露方式等之準則。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 **6.1.5**	組織應備妥以文件記錄之程序，用以識別於實務上去識別化可能是有問題或難以達成之情況。例：難以評估重新識別之風險，或是對某些個人之風險太高。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.1.6**	組織應依據法律規定、組織任務、營運要求、資料使用對象及目的、所持有包含 PII 之資料內容、型式及數量、資料揭露範圍、處理成本及風險評鑑結果等因素，選擇適宜之去識別化方法，並經管理階層核准，且以文件記錄。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.1.7**	資料去識別化過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改，並定期稽核。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.1.8**	委外處理 PII 去識別化時，組織應監督及監視委外處理活動。原始資料以不攜出組織場域為原則。含有 PII 之資料應經組織之高階管理階層核准方可攜出場域外，而受委託單位須依組織之隱私權政策及隱私權原則妥善並安全保存原始資料，並於完成 PII 去識別化後，立即歸還組織或安全銷毀。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
要求事項 (6.2)	組織之高階管理階層應監督及審查 PII 去識別化過程之治理的安排。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.1	組織應管理，關於 PII 去識別化之任何新指引、法規、法律、裁判、行政解釋、可用技術或威脅之相關知識，並據以評估風險。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.2	組織應與同行業或從事類似工作之其他組織分享並交流關於 PII 去識別化之知識。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.2.3	組織應定期進行隱私衝擊評鑑(PIA)，並應公布其 PIA 報告，顯示如何處理風險評鑑過程。PIA 應包含所採用去識別化技術之有效性，以及評估重新識別風險，以制定風險緩解措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 **6.2.4**	組織之高階管理階層應決定已移除 PII 之資料之可接受剩餘風險。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.2.5**	組織之高階管理階層應依規劃之期間或發生重大變更時審查去識別化過程。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.2.6**	**控制措施**：告知之透明性，同控制措施(3.1.11)。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.2.7**	組織應依據對來自利害相關者之回饋的分析，持續且及時審查 PII 去識別化過程。審查時應使用〝重新識別測試〞技術，評鑑重新識別風險及降低風險之措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 **6.2.8**	組織應對已移除 PII 之所有資料，進行獨立(非原 PII 去識別化工作人員)之系統化(自動或人工)檢查，確保其中未包含直接識別資訊，以及非必要保留之間接識別資訊。並確保必要保留之間接識別資訊皆已(經由匿名化、擬匿名化或其他方法)合理去除與 PII 當事人之連結。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項(6.3)	組織應訂定 PII 去識別化過程之標準作業程序，並依此進行 PII 去識別化。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.3.1**	應對待移除 PII 之資料集，先行備份，必要時應依隱私權原則進行前置處理，抽出最少需處理之資料、欄位或其部分。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.3.2**	應依待移除 PII 之資料型式(例：書面文字資料、書面圖片、文字檔、資料庫、圖片檔等)，選擇適當去識別作法及工具。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 **6.3.3**	組織應依資料揭露(公布)對象及資料敏感性，設定推論控制之檻值(例：K-匿名性之最小 K 值、揭露筆數占整體筆數之最小百分比)。不得揭露超過檻值之資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.3.4**	各項欲 PII 去識別化資料，應由領域專家(或有經驗人員)判定資料集之中的直接識別資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.3.5**	應對已 PII 去識別化資料建立威脅模型。分析可能使用額外資訊或間接識別資料進行重新識別攻擊之各種情境，判定各種“可能威脅”，並分析其風險，以及可能降低風險之各項控制措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 **6.3.6**	應使用所建立之威脅模型，對已去識別化資料之使用，訂定重新識別攻擊之可接受風險。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 6.3.7	PII 去識別化工作人員於完成去識別化操作後，應於管制之環境中，測試所有已去識別化之資料，確認合理之重新識別攻擊不可能成功。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.3.8	應對各項經 PII 去識別化資料，將所採用之 PII 去識別化技術、參數、威脅模型、風險值、控制措施、可接受風險及各項相關資料，以書面記錄。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項 (6. 4)：	組織應對 PII 遭非預期揭露備妥災難復原計畫。		
控制措施 6.4.1	應及時回應來自自認為個人資料遭揭露民眾之申述及查詢，並依已建立之程序採取因應措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.4.2	應備妥程序，因應公開資料遭重新識別而揭露個人隱私之情況，包含：移除可能揭露個人隱私之資料，重新處理；停止或修改(採取更嚴格之)去識別化過程。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 6.4.3	當公開資料遭重新識別而揭露個人隱私時，應告知隱私遭揭露之個人，並協助其採取必要之彌補措施。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項 (6.5)	組織應備妥程序，對已移除 PII 之資料，依可接受風險，定期進行〝重新識別測試〞。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.5.1	應對已移除 PII 之資料進行〝重新識別測試〞，包含： －搜尋網頁，嘗試連結 PII 當事人。 －搜尋全國或地方新聞資料庫，嘗試連結 PII 當事人。 －搜尋政府單位或其他組織之開放資料，嘗試連結 PII 當事人。 －以社群網路嘗試連結 PII 當事人。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 6.5.2	因公眾可用之資料庫，隨時會增長，故應定期重新對已移除 PII 之資料進行〝重新識別測試〞，以重新評鑑其風險。		☐符合 ☐不符合 ☐部分符合 ☐不適用
柒、重新識別 PII 之要求 (此部分為選項)			

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
要求事項(7.1)：	經匿名(或擬匿名)處理後資料之接收者應僅能鑑別 PII 當事人之資料屬性，而無法識別出 PII 當事人。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.1.1	經匿名(或擬匿名)處理後之資料，不得提供任何可用以識別出 PII 當事人之資料，但必要時可允許資料接收者查證經匿名(或擬匿名)處理後之資料(或其屬性)是否真實。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項(7.2)	同一 PII 當事人之經匿名(或擬匿名)處理後之不同資料，不得提供具有聚合後能連結至該 PII 當事人之資訊。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.2.1	資料接收者取得之經匿名(或擬匿名)處理資料，不得包含可據以連結 PII 當事人之間接識別資料。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項(7.3)	資料經可逆之擬匿名處理後，應可由 PII 控制者重新識別 PII 當事人。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 7.3.1	PII 控制者應備有重新識別 PII 之程序，規定所使用方法、所需資訊、授權及啟動流程。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.3.2	應定期審查重新識別 PII 之程序的有效性。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.3.3	為使 PII 控制者之後能重新識別 PII 當事人，將資料經可逆之擬匿名處理後產生之紀錄單，應提供足以識別 PII 當事人之必要資訊。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.3.4	PII 控制者對將 PII 資料經可逆之擬匿名處理所產生之紀錄單及重新識別所需之必要資料，應妥善加密，持續保存。		☐符合 ☐不符合 ☐部分符合 ☐不適用
要求事項(7.4)	PII控制者應提供能正確重新識別PII當事人之證據。		☐符合 ☐不符合 ☐部分符合 ☐不適用

項目	控制措施	文件名稱、章節出處或紀錄名稱	自評結果
控制措施 7.4.1	為避免PII控制者之不誠實宣稱，PII控制者應提供正確履行重新識別 PII當事人之程序的證據。		☐符合 ☐不符合 ☐部分符合 ☐不適用
控制措施 7.4.2	重新識別 PII 當事人資料之過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改。		☐符合 ☐不符合 ☐部分符合 ☐不適用

第三節　本章結論

一、我國法律規範範圍

由前述個別法律與草案可知，《個人資料保護法》已將個資與隱私保護的「目的限制」、「當事人權利」、「資料保存期限」、「蒐集者責任」等重要原則納入規範，而《資通安全管理法草案》參酌個資法的立法模式，亦授權中央目的事業主管機關針對事業制定資通安全維護計畫辦法或輔導導入資通安全標準。

此外，有鑑於電信法之規範不足而刻正熱烈討論中的匯流五法亦將個資與隱私保護之意旨訂於規範之中，惟依前列《電子通訊傳播法草案》、《無線廣播電視事業與頻道事業管理條例草案》、《有線多頻道平臺服務管理條例草案》觀之，除強調事前告知(隱

私權政策、服務契約)之管制外，對於通訊傳播事業蒐集、處理、利用個人資料及其安全維護措施，皆僅及於以條文指回到《個人資料保護法》，以期回歸該法規範之權利義務要件適用。

至通訊保障及監察法第 3 條之 1 與第 11 條之 1 的規範自施行以來爭議不斷，且主要係針對國家機關的調取行為，是否適用於非公務機關仍未屬定論，故本研究報告暫此尚不納入範圍。

二、我國法律不足之處

(一) 我國法律目前缺少對於通訊傳播事業所涉及特殊個資類別（例如通信資訊、位置資訊）之個別定義與利用規範。此將影響通傳會對於通訊傳播事業在告知義務的強化、透明度的提高、當事人的資料控制權行使標的等面向之規範效力。

(二) 無論在《個人資料保護法》或匯流五法目前公布的草案中，均缺少當事人請求資料可攜之權利。此權利涉及當事人控制權的完整性，若缺少讓當事人可以特定格式攜出資料並便於再次利用之權利，則將難以保障當事人居於個資主體的地位，亦難令當事人與資料蒐集者共享其個人資料帶來的經濟利益。

第七章 焦點座談討論會

第一節　會議內容

一、第一次焦點座談討論會議

- 時間：105 年 1 月 15 日上午 10:30-12:30
- 地點：東吳大學城中校區 R5215 會議室
- 專家學者：(依發言順序)

1. 臺灣科技大學—方修忠教授
2. 輔仁大學—翁清坤教授
3. 財團法人資訊工業策進會—戴豪君資訊長
4. 元智大學—葉志良教授
5. 中央研究院—邱文聰副研究員

- 研究團隊：

1. 余啟民教授
2. 王慕民研究員
3. 陳品安研究員
4. 張又丹研究員

- 討論議題：

一、 NCC 對大數據的監管範圍

二、 我國應否成立個資/隱私保護專責主管機關

三、 我國應否就通訊傳播事業的個資保護制定專法

四、 承三，如制定專法，下列方法是否可行：

(一) 強化告知義務(包含告知資料來源類型、去識別化利用方式)

(二) 保障當事人退出(分析)及刪除(資料庫)資料權利

(三) 增加當事人資料可攜權利

（四）加強蒐集者責任：隱私衝擊評估、資料稽核制度、導入國際標準等

五、 若不制定專法，是否須修訂現行法律以授權 NCC 執行權力

六、 若不修法，就現行法規授予 NCC 的監管權限是否足夠，例如：

（一）制定通訊傳播事業個資安全維護計畫辦法

（二）行政函釋

（三）行政指導

（四）行政檢查(稽核)

七、 綜合討論

➢ 專家學者發言

表 5 第一次焦點座談討論會內容

專家學者	發言內容整理
方修忠老師	1. 首先研究資料都很新，大家都可以參照歐盟、美國的資料，所以我首先對研究資料表達感謝，讓我可以很快進入狀況。 2. 修法這件事我個人覺得不好談，不管是修個資法，但委託機關不是個資法的主管機關，再來修電信法或是新的法，新的法不知道是不是送到行政院了，就算送到行政院，目前狀況比較尷尬，新的國會產生了，所以沒有意義，但是 NCC 很努力把匯流法送出去了，算是一個進度，我個人是比較傾向就修電信法，這是目前 NCC 比較能夠主控的，因為現任 NCC 七個的委員並不受新

	的政府影響，因為本身是獨立機關，還有委員的任期，所以在可行性跟操作上應該就電信法本身。 3. 有關於個資的保護跟大數據，因為我看不出來這個題目是不是要討論到大數據，但是這個議題肯定是要談到的，剛剛看了王律師的簡報談到其他國家的大數據，跟甚至很多產業資料，這點也表達感謝，特別是在通訊傳播行業不可能不談大數據，不管是手機或其他裝置來上網，我是說廣義的上網，也包含 OTT，我最近也跟一些 OTT 的業者談過，他們覺得他們不需要網路就可以運作，這也是匪夷所思，沒有網路他們怎麼跑，但也透過這個機會跟他們交流一下，特別在大陸的研究上，像是騰訊或是阿里巴巴他的支付，還有叫車或外賣，都是走大陸的網路，也不需要拆帳，不用跟提供網路業者拆帳，這個地方王律師有點到 OTT，不去談 OTT 的個資的保護也脫離現實，所以建議從 OTT 要不要納管這件事已經討論很多了，要不要管制或特許，但從個資法的角度，有拿執照的不管是一類二類，都要納入個資法的保護的話，那 OTT 如果沒有納入保護的話好像不太行，特別是 OTT 使用者很多，又是免費的，使用者對於個資保護的期待可能性很低，按照現行的通訊保障及監察法，所謂電信事業或郵政

	事業，協助通訊監察，是不包含 OTT 的，這是當初立法漏洞。 4. 回到剛剛修正電信法，現行電信事業去保護個資，不管個資還是通保法，以我的了解，葉老師也知道電信事業在保護個人資料，最低就是符合法律的標準，各個業者都有找標準機關在做個人資料保護，但是怎麼讓個資保護跟資料有效利用達到衡平，我個人覺得可以從銀行法第 47-3 條(104 年 6 月 24 日修正)，47-3 第三項，應該要通過金管會的許可，所以要訂一個辦法，這個辦法本身就是跟著 47-3 在走，要跨出大數據的話，因為電信相關的資料太多筆，使用者自己都不知道，除了申裝書密密麻麻的，有更多資料，還有銀行開戶，現在已經不用臨櫃辦理，從跨出這步，現在也有金管會銀行法相關條文的修正是不是給我們 NCC 作為修正的參考 5. 巨量數據(big data)是沒辦法拒絕的，全世界每個國家政府、行業都在運用跟管理，open data 不管現在未來也是政府要推動的，例如保險費率計算，如果沒有經過人口壽命歲數計算的基礎就不會有壽險，沒有出意外的數據基礎，怎麼會有意外險，這些早就是 open data 了，只是之前不是系統，所以我支持 open data 跟 big data，否則不會有創新，因為如果開放給第三公正機關，他們相對也可以去治理管理他的政府機關。

	6. 這個草案，找電信跟傳播來開會，我認為應該整合，也應該要有個資保護以外的譬如說巨量資料的管理，不過應該要花很多時間管理。
翁清坤老師	1. 就我國是否該成立個資跟隱私的主管機關，你們剛好有參考文獻有提到國家發展委員會有關電信法跟電信加值網路個資保護跟監管機制的研究，其中我們處理到這個問題，像歐盟的會員國或先進國家東亞日本或香港澳門，都有個資的專責機關，我國長遠來看也要有，可是我們當初的研究，我們有中央組織基準法之類的，所以如果要成立一個中央部會組織是有相當困難性，另外，在法務部個資諮詢小組，他們只是一個法律事務司裡面只是科室，負責的人只有三個，很難負荷，所以我覺得還是要成立專責機關，但是現行難度要克服。 2. 法務部目前是個資法的專責機關，但實際上，各目的事業主關機關他們的領域內也有做管轄，像金控法，在金管會的部份算是走得比較前面，金控公司他們是彼此分享資料，所以對他們來說，個資可以不用經過當事人同意就可以分享，他們有制定特別法規命令來授權，可以在子公司分享，這部分可以拿來給電信領域參考，各個領域都有遇到困難，因為個資法太抽象，下一步的落實及施行起來有困難，譬如說去圖書館借閱書籍有借書資料，螢幕會秀出來所有的資料，但是萬

	一後面的人看到怎麼辦，還有另外我們之前還有受臺北市法務局的委託處理一個委託研究案，要我們去訪談五個單位，警察局、教育局、衛生局、民政局、社會局等等，結果發現他們都沒有一個專法或法規命令來指導他們怎麼做，法務部先天有人員的困擾，法務部是一個一般性、準則性的規定，沒辦法針對各個產業來規範，所以就可以參考金管會的金控法，這也衍生到美國有部門式的法律有各個不同的法律，大概有十幾二十個產業受到規範，其他的就放任不管，所以美國的做法他們金融服務法案針對這個領域規定的很仔細，這樣的方式就可以滿足不同領域。 3. 像強化告知義務，我們的個資法對告知義務就有蠻多規定，所以如果說通訊傳播領域如果沒有比較特別的地方新訂條文內容不用特別強調，包括還有退出的部分，嚴格講起來個資法第三條及第二十條，有關不要再行銷，刪除個資，這些都是可以運用的空間，但是我們不知道怎麼使用，因為各個產業也還沒有落實實際使用的地方，所以通訊傳播業要制定特別的法條可以參考這些法規要怎麼用。 4. 當初我們在做有關電信法跟電信加值網路個資保護跟監管機制的研究時就有遇到很大的困擾，電信加值網路業(第二類電信)到底是甚麼？後來電信業跟通信業我們就避開，因為這樣太包

	山包海，那貴研究案針對通訊跟傳播是指網際網路的話這樣就包山包海了，但是傳播會涉及到個資相對其實少很多(譬如機上盒)，但他所蒐集的東西透過網路的話就會蒐集到很多，所以甚麼都包的話挑戰就會很大，像美國對於大數據也還沒找到解決方案，當然我們也希望看到這個報告對這部分有個方向。 我看過一些文獻，過去資料庫的處理已經沒辦法涵蓋大數據，美國對於這個議題也很分歧，應該全世界都還在思考，所以要在法規上有個區別，挑戰蠻大的。 個資法最大挑戰是甚麼是特定目的，還有可不可以分享，如果超出特定目的就不能使用，所以這個範圍到底多大?如果引進大數據，個資法現在是以去識別化之後可以使用，去識別化的話就不算是個資，這個可以滿足大數據的要求，如果不去識別化的話，就回到美國規範的模式，但是目前應該不被人接受，所以要找出一個方式，譬如說放寬解釋，但是對隱私的合理期待能不能到達這個程度，這是我的見解。 5. 制定專法方面我覺得有必要，各行各業其實面對很多問題，但都要等主管機關，第一線的公務人員他們面對很多個資問題也不敢做決定，所以像金管會的金控法就可以做參考，或者 NCC 可能要制訂一個詳細程度比個資法更為詳細的專

	法，我們發現電信業，除了可攜式號碼有些可以做加值的利用，像美國就有業者，將看球賽的球迷的資料做分析，譬如說球迷的年齡大概是在25-45 歲、還有如果有小孩的話看球賽時多少人會將交給保母照顧、如果比賽前或是開賽前 24 小時如果有打廣告，會不會增加來客數，但是臺灣是沒有這樣，美國這樣的運用就是因為他們去識別化，所以沒有受到爭議，以上是我的淺見。
戴豪君資訊長	1. 研究報告資料分析清楚用心，解說清楚，尤其是歐盟最新法規解說，給予肯定。 2. 通訊傳播事業的範圍,NCC 認為管轄的範圍是通訊傳播的業者，但是個資是不是只管業者就能處理。例如手機 app 通傳會堅持管理內建軟體，對於內建 app 需要預查管理，OTT 也是一樣。但是下載使用其他 APP，卻無法分別資訊產品還是通訊產品，所以只管業者是不是在設備端、應用服務端是不是會有問題，這是 NCC 需要審酌的。 3. 資策會目前進行研究有些新的課題，舉例：最近提個 IOT 的問題，每個物件都會有個 chip，每個 chip 都可以發出訊號，那這個訊號有可能是 realtime 的有些是很久才一次(ex.森林的監控)的。但有些是需要即時回應的，像我們最近在龍門國中附近有做一個視障者的導航，會告訴你哪邊有障礙物，或是階梯，讓視障者可以順利到達目的地，所以未來 IOT 會是一個混和網路，不管

	是透過藍牙、WI-FI、4G，但是問題是我們如果走 3G、4G 然後每天需要回覆的資料很小一天可能一次，但是對於電信業者來說這就是一個門號要收月租費，這樣收費的模式不知道能不能改變，這種衝突會不斷產生。或是說像 BSD，譬如說用裝置來監控你開車的行為與習慣，來訂出你需要繳的保費，這樣每個人的保險費用都不一樣，所以議題一是很重要的，只用這個想法來做是有問題的，第一個討論議題很重要，如果用這個思維去做，其實實際是有困難的。 4. 以目前來說二級機關部會不太可能，至少要修兩個法，中央機關基準法跟行政院組織法，這兩個法要修都是很困難的。如果是三級機關，目前法律規定是 70 個，已經額滿，除非廢掉其中一個，或是修法讓上限提升，但就目前接觸到的都希望可以把數量下修，為了精簡政府組織機關，就算刪除其中一個單位也有困難，單獨立法目前幾乎沒有成功，除了廣電之外，所以我贊同方教授，立在電信法裡面規範。 5. 大數據最麻煩的就是越發達，間接識別的範圍就越大，施行細則修法歷程裡面我本來希望可以加入一些文字，像消保法第七條那樣，「當時科技或專業水準可合理期待之安全性」，但是我們的個資法沒有註明到這塊，只有寫到對照組合連結，各位知道像美國做過一個 test，把所有的 data

	打上，他們可以很精準的組合出一組名單大概 20 個人，裡面包含所有 911 去撞飛機的那些名單，是可以找到的，所以如果沒有加上剛剛那句「當前可得的科技」，把間接識別的範圍擴大，NCC 管制的範圍就會越沉重，舉例來說人體生物資料庫法中，文字寫編碼加密去連結，但是這很矛盾，編碼加密去連結是不是就能夠對照組合連結，要討論大數據就要先處理間接識別，如果間接識別沒有處理，那坦白說大數據你能想像到的數據以目前技術來說不可能不與個人發生連結，我想這可能是需要處理的。 6. 通傳會也要關心跨機關的資料流通，NCC 的監管單位去管民間的話，但是會面臨到一個挑戰是，但是機關之間需要跟 NCC 拿資料，最近中國大陸大陸公布一個第三方支付電子帳戶認證的標準，在臺灣第三方支付專法對於認證有分三種，第一是出生年月日還有身分證是補發還是換發，第二是綁定銀行帳戶，第三就是要電子簽章加密認證。大陸現在只要你提供三個可信賴來源，來做交互認證，其實就是大數據去對比，對於可信任的來源，譬如稅捐單位、教育機構、車輛機構、甚至 pchome 的帳戶，其實你只要有三個可信賴的來源去對照，電信公司相信也是一個非常重要的依據。但倒覺得不需要在這個專案處理，如果是要提供可信賴來源，電信業者會是有

	很多資料的蒐集的，所以將來要怎麼樣去應付科技的需求，需要處理這些問題。 7. 最後，將來的管理機制，應該要有幾個層次： (1) 譬如業者的自律，配套應該在個資法上有幾個管制的機制，譬如說業者管理好了，可以取得某個認證，這個認證可以在不管是責任也好能夠有個保護，這樣才會鼓勵大家(業者)去實踐，歐盟跟美國的 safe harbor 也是同樣的例子。因為歐盟認為美國不是個資保護適當的國家，所以理論上不能做跨國傳輸，那時候差點形成貿易大戰，後來才想出這個 safe harbor，企業來通過他的認證，就認為是可以做國際傳輸的企業，只是說這個最近又被法院否定，被一個法學院的學生去告臉書，所以 safe harbor 可能之後又要再訂定另外一個標準，歐盟不可能要求美國去修改法律，但是企業自己知道要去做這個認證，才能符合市場的需求，所以不管是共管或是公司自己先管理，NCC 要去考慮業者自律這部分。 (2) NCC 的監管機制，是不是都要自己來，應該要有個民間組織以公私協力方式的幫助，應該要有幾個層次。 (3) 最後才是政府透過行政裁量來處理，如果可以盡到某些責任上的保障，民事責任上的豁

	免跟保障，這樣會有誘因會讓業者來自律，所以比較不建議僅從行政法上的規管來做，而且電信業變化很快，其實是很難。
葉志良老師	1. 匯流事業怎麼定範圍，這應該是 NCC 很困擾的，可以從他現在草擬的匯流五法看出端倪，想要規範出管制匯流產業的問題，尤其是想要把一二類的消除，最困擾的就是執照的問題，是說不要用強制的管制方式來發執照，過去他們針對業者來管拿執照，我認定你是要來這個市場，就必須要有執照，過去是這樣的方式，但是當初這個一二類的分類非常不妥，因為二類在做一類的事，應該管到服務的本質，如果服務本質是通訊傳播，那 NCC 就應該要插手管，看是要用執照或是登記甚麼的，那是主管機關要決定的，那麼在匯流五法裡面的電信事業法或是其他的傳播法裡面，有這樣的調整。 2. 接下來是範圍的部分，到底要不要管網路的部分，其實立場已經講的很清楚，是傾向不管理網路部分，但是如果管制的本質是傳播服務的話 NCC 應該是要插手，像是 OTT 要不要管，一開始是說不管，但是 OTT 的內容跟大家看電視一樣的，所以主管機關要自己決定，現行只要是通傳服務的話是不是都要納管包括牽涉到個資的部分。 3. 到底要不要成立隱私或個資的主管機關，剛好是

	個前提，目前個資法立法方式是參考歐盟，是單一立法方式，所以如果是用這個方式的話，要成立專責機關我覺得是指日可待，當然法制上還有要克服的問題應該都可以在翁老師的報告看見，那 NCC 以通傳的主管機關在個資保護方面該怎麼著力，到底要不要修法或設立專法，應該這樣講如果前提個資法是集中式單一法典的話，NCC 其實不需要再立專法，不用跟法務部搶生意，而是說以目前單一法來看，以個資法 27 條來看，NCC 自己很清楚它可以管也有一個方向，只是要不要在層次上立法，但是通常 NCC 在政策措施前想要一個有利的法源依據來保護，在他們現行的法律中應該要加入一些文字，譬如說現行電信法第七條，有講到通訊秘密，但又不是很清楚，在電信事業法中有兩條跟個資有關的內容，某種程度來看有表達出針對通訊傳播業者的個人資料保護來補足跟管理，另外，更有趣的還有電子通訊傳播法草案有專章保護個資，一條要處理國際傳輸，其中第 21 條就是個資法 27 條的內容，所以其實這個可以刪掉，可以發現 NCC 對於網路這塊很徬徨，但在時間這麼短的狀況下有一個初步的內容對於團隊很佩服。 4. 再來要不要立專法這個問題，我個人認為修既有的法律就好，那要修現在的電信法或是廣電三法

	困難度頗高，但他不會是非常優先的東西，不過個資的東西反而比較容易凸顯，因為跟社會大眾有關，如果 NCC 扣住這點即便不立新法或是修法，起碼這個安全維護計畫可以彌補規範既有對業者的指引。 5. 在這幾個議題之外，資料可攜，把資料視為一個財產，在美國有一個專門機構(data broker)，但是這些行業沒辦法可以管，他們在蒐集的過程沒有進行一些蒐集的程序，甚至沒有告知使用者等等，主管機關其實想要管理，但是現階段是業者自律，所以回到研究案來講，戴資訊長有提到到底規範的範圍層次要到甚麼程度，要用法律或是共管，不需要把所有事情攬在自己身上，某種程度來講業者之間會達成一種默契，業者如果達到一定的水準，主管機關的重擔會比較小，自律或是共管在這份草案應該加入。
邱文聰老師	1. 針對到底 NCC 要處理的範圍，也就是通訊傳播事業的範圍，我的想法也是應該不是只管業者，而是應該以服務為管制對象，因為同樣是電信業者，不是所以東西都歸 NCC 管，譬如說雇用勞工就不規 NCC 管，所以如果以業別來管絕對是 over inclusive，那麼 under inclusive 就是就算不是電信業者，但是牽涉通訊傳播事業，應該都受到 NCC 管，但 NCC 卻不管，其實有點奇怪。衍伸各位的剛剛提到 OTT 的問題，我實在不太容易

	理解要嘗試迴避網路的管制如何能夠達到這樣一個管制的方式。 2. 再來，立專法或是修法的部分，倘若用目前以事業別來做為管制標的的話，不立專法有沒有辦法去擴張成是以服務來當做他的管制標的，我覺得也可以來思考一下這個可行性在哪裡。 3. 聯結到要不要成立專責機關的問題，如果要成立的話，剛剛的討論都是多餘的，因為只要是個資就歸個資主管機關，也不用去討論到通訊傳播事業是不是他的業務，反正只要是個資都歸個資主管機關管理，但這個問題剛剛前面幾位也有提到，好多部會都提到要成立一個主管機關，才能去參加國際部會，所以我想政府應該慢慢會朝這個方向也知道這個的必要性。 不過在成立專責機關之前，還是由各部會管理的情況下，去立一個個資法以外的特別法來處理各個不同領域的個資問題還是有必要，即便不是用專法而是在既有的法律來修法去加入一個個資的保護條款，我想這個可能是有其必要的，這個必要性是建立在第一個現在個資法理面雖然有一些蠻原則性的規定，包括也有退出權，但實際上在現在個資法的操作底下，現在這些退出權的機制都沒有辦法用在我們現在實際面臨到的大數據底下的研究上或著應用上，前面幾位有提到公務機關所適用的 16 條以及非公務機關適用的

	20 條裡面，對於已經蒐集來的資料要做目的外利用的時候，只要宣稱他是某種程度的去識別化，就可以不需要當事人同意的情況下，就拿來做研究，但前提是說這些所謂的商業也好，要拿這些資料來做研究有沒有辦法去 qualify 這個學術研究案，或許有些理論，不過可能很容易就 by pass，只要名義上找一個學術研究單位來幫他當白手套，其實就可以解決這樣的問題，或甚至是他在部門底下設立一個學術單位都有辦法去 by pass 這樣的困境，所以很容易就可以透過 16 條及 20 條的方式就直接進入到不需要當事人同意就可以來利用，而且按照現在法務部的一個函示的說法，個資只要經過去識別之後，就可以不適用個資法，邏輯上是一個奇怪的說法，如果你的去識別化，本身不是符合個資法的去識別化，那怎麼可以說去識別化之後就不適用個資法，所以去識別化本身有沒有符合個資法還是要看個資法本身的到底有沒有符合的問題，現在的個資法在法務部的操作底下，是有一些問題的，要去克服這樣的問題，然後在各自的領域裡頭去解決大數據研究下所產生的爭議或是挑戰，比較快的方式可能是在各該領域裡面去立一些特別法來解決，那當然前面幾位有提到幾個概念的區分，我想也需要在這個特別法裡頭來澄清，包括所謂的 aggregate data 跟 anonymous data 兩個應該是不一

	樣的。 資訊長剛提到編碼就是我給他一個 code，不是那個人的身分證字號或是不是那個人的名字，我只是給他一個 code，這就是所謂的假名化，這個方式的處理可以某個程度達到資訊安全不會外洩，但是對於個人的資訊隱私的自主權仍然沒有達到完全斷開連結，所以其實在大數據的研究，大數據的整個趨勢對個資最大的挑戰是在於說，傳統的個資態樣，都是在講說我只要跟個人好像沒有識別性之後就沒有個資保護的必要，可是其實剛剛的報告提到，有沒有可能再識別的可能是永遠沒有辦法除掉的，所以如果我們再用原來的情況去想像只要跟個人沒有識別可能性的話，就沒有個資保護的必要，那其實在這個大數據時代，個資法乾脆丟掉，因為完全沒有保護的必要性，所以他引發出來的問題是，可識別性是一件事，但是自主控制是例外，我們要如何在大數據年代底下去談說識別性跟不識別性是要考慮到的問題，在個人的自主控制底下這是不可能完全的放棄，只說自主控制可以讓他到甚麼程度的問題，不同類型承認他的退出權，在大多數商業應用底下，不用事前同意事後也不用，從識別與否的角度下去設計不同的模式，大數據的利用，可能要朝這個方向幾種不同模式，才能因應大數據的挑戰。

二、第二次焦點座談討論會議

- 時間：105 年 3 月 4 日上午 10:00-12:00
- 地點：東吳大學城中校區 R1106 會議室
- 專家學者：(依發言順序)

1. 寬頻產業協會—彭淑芬理事長
2. 凱擘—林雅惠副處長
3. 台灣之星—丁憲文副總
4. 遠傳電信—陳麗玲律師
5. 政治大學—劉定基教授

- 研究團隊：

1. 余啟民教授
2. 王慕民研究員
3. 陳品安研究員
4. 張又丹研究員

- 討論議題：

一、 通訊傳播事業的範圍？以行業或服務內容決定？

二、 我國應否成立個資/隱私保護專責主管機關

三、 我國應否就通訊傳播事業的個資保護制定專法

四、 承三，如制定專法，下列方法是否可行：

(一) 強化告知義務(包含告知資料來源類型、去識別化利用方式)

(二) 保障當事人退出(分析)及刪除(資料庫)資料權利

(三) 增加當事人資料可攜權利

(四) 加強蒐集者責任：隱私衝擊評估、資料稽核制度、導入國際

標準等

五、 若不制定專法，是否須修訂現行法律以授權 NCC 執行權力

六、 若不修法，就現行法規授予 NCC 的監管權限是否足夠，例如：

(一)制定通訊傳播事業個資安全維護計畫辦法

(二)行政函釋

(三)行政指導

(四)行政檢查(稽核)

七、 綜合討論

- 業界專家發言

表 6 第二次焦點座談討論會內容

業界專家	發言內容整理
寬頻產業協會 彭淑芬理事長	1. 這議題兩難，很有挑戰，如果可以做到十全十美是最好，但是如果完美的話業界就不用做了，現在業界很多都已經在做資料蒐集的動作了，為什麼我們在執行網路的時候很放心、很習以為常，但是來到通傳產業就變得躊躇不前，這是一個很嚴重的事情，用顯微鏡特別來看。第一段我要說現在是網路化的時代很多行為其實已經發生，今天我們也很難不得不用網路的思維也就是平常心來看這件事，我覺得研究團隊所擬的大方向我都是同意的，問題在於怎麼做，這是一個很大的挑戰，事情總是要往前推動，新的媒體、新的網路商業模式一直

	來，不往前就會錯失機會，本土的業者不趕快做這一塊，其實國際的業者早就在做了，機會稍縱即逝，所以不能等到完美之後再來做，這是一個前提。我個人覺得，OTT 是個重大的議題沒錯，視訊主流產業其實幾乎以 OTT 來說已經囊括很多收訊行為，已經是不可忽視的主流力量，所以主管機關不能再用工業化的思維來說：對不起網路我不管，因為所有的媒體都是新媒體，只管 4G、3G 業者系統業者是不可能的，所有媒體都是新媒體了。這個跟我們匯流法的問題是一樣的，現在匯流法也是傾向只要是 OTT 他就不管，我們很強烈建議主管機關這點必須要修正，因為這是網路媒體的時代，不論是個資的管理、個資法的修訂去連結到匯流法的部分，OTT 這塊都必須納入思考怎麼去 manage 它，我們建議的前提是相同服務相同管制的方式較好，產業的界線已經模糊化，我們只能去看服務型態是不是相同的，如果是的話就要用一致的標準來看他，包括個資管理的範圍也是一樣，確立這個前提以後就可以去看哪些是相同服務做相同管制，現在其實應該注意的是廣大的視頻網站視頻媒體的部分，這塊就像大海一樣比傳統視訊服務大好多倍的，只要他要來台灣做服務與消費者產生關係，就應該要 follow 我們公佈的個資的準則，

	就看他的服務是甚麼來思考，不應該停留在網路以前的時代。怎麼管在機制上非常重要，現行個資法最大的原則就是用戶同意，我們在網路上下的每個指令都很稀鬆平常，但是我們在實體做的時候就覺得是大事情，實務上大數據已經發生，但是我們產業要去做用戶同意時門檻很高，既然是網路化的時代，過去我們都用紙本規定，其實應該考慮電子的可行性，當然我們也不是要便宜行事，因為用戶所有權或變更或主張的一些權利也是重要的。 2. 研究團隊其實有考量到除事前同意外在過程中的控制權，當我們是網路化的思維，過程中的機制就很重要，永遠要讓消費者有他的控制權存在，那對產業端來說，剛說的可行性都牽涉到幾個面向，就是未來這個機制必須是效率化，因為商業變動太快速了，如果要做，很多流程或成本太高昂的都應該要改革，所以效率化、快速化而且是可負擔的成本是必要的，其實我們現在所有被高度規管的產業，我們資安都是用高規格的成本在被要求，成本也是非常高昂的，就是被高度管制的行業責任義務很高、成本被大幅墊高，卻要去面對 OTT 行業不受規管的情況，這種不對等的競爭應該要被檢討，看有什麼方法可以讓這個競爭更加公平。

	3. 剛有提到這整個環節最困難的還是在機制的部分，我們協會在 2011、2012 年就探討這個問題，我記得當時新聞局曾經有提議想要做一個收視率稽核組織的單位，後來不了了之。有幾個觀點，其實是不是都由政府來做是最好的方法，可能未必是，因為政府一般而言效率比較低、彈性比較低、比較僵化，加上這些資訊的確擁有在各個產業的系統裡面，他們是資訊的產出與維運者，如果什麼事情都交給政府去做可能不見得有效率或有其困難度在，如果去承襲當初那個收視率稽核組織的這種精神，我們就想到說有沒有可能做一個民間的具公信力的中立第三方的相關機構，去維繫這個 DATA，因為畢竟每個人都是 stakeholder，所以有沒有可能讓大家共管，像現在所謂 NP 資料庫一樣，放在中立第三者的資料平台上，他是一個維運單位，產出這樣的 data，產出是一個單位，但分析是另一個單位。那時候我們的想法是分開兩個單位，比較不容易，安全性被全盤壟斷或被控制，很重要的一定要有稽核的單位，定期稽核這個機制是不是安全的，當然政府在這個環節是一個 regulator，一個制定遊戲規則或是一個稽核組織的角色也說不定，如果可以用制度上的設計，擁有資料庫的跟去 process 資料庫的跟去 audit 整個流程的是一個

	比較有規劃的機制，或者可以讓所有的用戶、所有消費者可信賴的，也真正可以達到安全控管，去稽核整個流程不被駭，或是有什麼資料缺失去傷害到個人隱私的風險存在，所以結論是全部讓政府規管未必是很有效率的方法，有沒有可能引進一個公民共同協力共管的機制，或許是一個可以考慮的方向。 4. 另外，就是除了 procedure 以外，所謂的資料類別也應該會被分級，安全等級不一樣處理的方式不一樣，比方說如果屬於去識別化後整體的消費型態研究或統計，應用方式與有個別資料的資料方式自然不一樣，很多環節部分都有賴事前嚴謹小心的設計規劃，想清楚之後再來執行會比較妥善。
凱擘 林雅惠副處長	1. 從產業面在訂戶之個人資料處理利用的一些困難進行說明：以我們公司來說，所經營的服務包括有線電視視訊服務及寬頻上網服務，在所蒐集訂戶個資的部分，包括訂戶在營業處簽約、電話撥打至客服續約或透過官網網站於網路上進行續約，而現在用戶也可以透過數位機上盒(STB)訂購加值服務，再者，我們規劃未來下半年將推出 OTT 服務，所以手機上也是我們個資蒐集的來源。以個資法施行到現在，為因應個資法第八條目前在蒐集個資前段，需依法提供訂戶義務告知書，但是我們蒐集的方

	式有很多，假設我們可以 access 到客戶的情況，的確可以做到告知，但如果是在締約中間階段，譬如我們最近被要求清查一些資料，這些用戶實際上可能沒有跟我們締約，但是我們還是有他的資料，經過我們清查後大約有數十萬筆，也就是說可能消費者曾經打電話進來約裝但沒有約裝成功，或者消費者曾經約裝但是之後可能因為商業條件或是鑑賞期間過後申請退租，所以除了真正是我們的訂戶以外，我們常常會保留這些非有效訂戶之個人資料，但是這些資料對我們來說最大的問題是要怎麼取得當事人的同意以及這個同意是可以事後被檢驗的。目前我們的作法是在電視機使訂戶透過機上盒訂購加值服務，顯示個人資料保護法第八條個資蒐集義務告知書條款並讓訂戶在電視機畫面上勾選同意，這些都是未來如果對個資蒐集範圍發生爭議的時候我們必須要舉證出來並做說明的。 2. 但是在施行這麼多年以後，我們發現自己履行蒐集的特定目的範圍跟 NCC 監管的想像是有很大差距的。NCC 從 97 年、98 年以後對於電信或有線電視傳播業確實在個資上面有非常多要求，譬如說要求我們訂定個人資料安全維護計畫並每季申報執行狀況等，且近日我們收到 NCC 來文函文告知其認為有線電視基本頻

	道服務定型化契約對於用戶資料保密、利用條款、授權對象、授權範圍、授權內容均過於廣泛寬鬆並要求系統業者改正，經與主管機關溝通後瞭解，主管機關認為，系統業者目前蒐集個人資料範圍除經營有線電視業務外，還及於電信加值服務譬如寬頻上網，客戶管理服務、關係企業行銷、合作廠商市調和共同行銷需要還有學術研究等等，當然包括還有一些優惠措施和活動訊息等等，但主管機關希望系統業者將蒐集個資的特定目的範圍限縮在有線廣播電視業務項目內。我們在營運面上對於訂戶個資之蒐集、處理、利用各方面，跟 NCC 有很大差距，主管機關在相關法令或匯流五法還沒修訂前用行政指導的方式來要求我們修改定型化契約，對系統業者來說其實很困擾，若按照 NCC 要求只把個資特定目的範圍只限縮在有線電視跟寬頻服務那麼狹隘的範圍，會嚴重影響到未來其他加值服務的應用與發展。 3. 以收視率調查分析為例，因為目前數位機上盒具有雙向收視功能，可蒐集每個訂戶在特定時段之基本頻道、付費頻道或隨選視訊(VOD)等頻道節目之收視行為等。這些資訊我們蒐集進來之後，在本業來說可以提供消費者更精準的節目推薦或是訂購服務的推薦等，或作為未來發展電視上面的精準行銷或是購物服務，這些

	蒐集我們遇到最大的困難是如何更容易地得到當事人的同意。之前在新聞局時代，曾有希望成立一個第三方機關稽核的機制，把這些資料交給第三方，但是顯示出通訊傳播產業在個資法遇到的困境，這個資訊是不是可以把它當成一個有價的資訊還是傳統的隱私權，中間如何取得調和，因為科技的發展，這些資訊透過加工我們可得到更多用戶的資料，在未來的加值服務上做一些有效的利用，設立保護個人資料的專法我覺得這是有必要的，一般的個資法他是比較 general 的規範概念，但是針對通訊傳播事業，他可能去蒐集這些資料，他的特性是不是應該在個資法以外立專法去做些放寬解釋的適用，這對未來產業發展是很有幫助的。
台灣之星 丁憲文副總	1. 台灣之星是個新的業者，我們現在還在生存的階段，過去十幾年來我也在其他通訊傳播事業待過，從產業的軌跡來看，台灣大哥大也有過 OTT 的想法，在剛才王律師提到大數據跟物聯網，事實上從以前到現在這個新經濟，至少就電信也者來說，十年前行動通訊的產值大概是兩千兩百億，通訊業者現在不管是資訊的蒐集是不是非常有潛力的，就我對這個產業的理解並不是，這些 OTT 業者不會跟我們分享策略，舉例來說去 GOOGLE 搜尋東西，之後會有廣

	告出現在你的頁面上，網路廣告上市占率很高，電信業者也是一樣，以前在 2G 時代，電信業者的市佔率是很高的，但是現在電信業者佔有率不比 OTT 的萬分之一，這是真實的市場狀況，也就是說將個資跟隱私發揮比較大的商業價值不是電信業者，要有商業價值他必須要有成功的商業模式，像 APPLE 不是一個服務，從這個角度來看不管這個管制要怎麼做，中央是不是要有機關，是不是要做專法，先要搞清楚要管甚麼，大部分我們都管不到，台灣現在也是在新經濟缺席的國家，我不知道我的想法跟其他先進是不是一樣，我是從電信業者在這方面創造多少錢，未來還有多少可能，如果要管應該是要以已經創造價值跟未來還會創造更多價值的資料跟資料的擷取者來講。 2. 機上盒做收視率調查是有這個潛力，這部分是蠻有經濟價值的，電信業經手很多資料的傳遞，電信業者要來跟他們競爭是很困難的，台哥大也曾經試著做，這個產業能不能產生那樣的商業化價值，要加強怎麼樣的管制，我抱持懷疑的態度。
遠傳電信 陳麗玲律師	1. 從電信業者的角度，確實以電信業的特性看起來我們好像會產出客戶的 LBS、上網瀏覽網路的紀錄、通話行為，電信業不管在台灣還是全世界是一個受到高度管制的產業，王律師有提

	到要用行業還是服務內容來管制，剛丁副總也有提到，很多 OTT 業者都在做，如果回過頭看台灣，我們還是用行業來做管制的話，會限制我們在這個產業跟國外業者或者跟相同類似內容的服務提供者的競爭力，電信業者反而是弱勢，因為受到主管機關太多限制，我們有很多看起來有價值的數據，可是我們在執行的時候受到這些限制，到底要怎麼發揮效益，然後要怎麼跟消費者個人的資料保護做一個平衡，如果透過這個研究案，讓政府機關知道，或透過這個研究案，我們參考國外的做法，因為很多不管是 OTT 業者、APP 服務業者他們都是在國外發想這樣的服務，那國外的主管機關又是怎麼管制的，除了看到管制面，他們怎麼樣有這樣的空間取得個人的資料或隱私，發展出一個很貼近用戶的制度，不只在他們當地的市場，他們還可以達到海外全球市場，所以有這些東西怎麼樣發揮最大值，我覺得是政府應該很 overall 去考量的，不是只是看到一個點說我們應該怎麼去保護消費者權益，我知道這個也是非常非常重要，但是一個全盤的產業考量應該不亞於對消費者權益的保護。 2. OTT 業者到台灣後，不管是愛奇藝還是 Netflix，還是會回到他們進來以後他們也有很多機會可以得到消費者的資料，那這些資料可

	不可以真的利用或是有產值，那對於電信業者來說，雖然都是適用同一個個資法，但是主管機關不同，密度不一樣，嚴謹的程度不一樣，立基點就不同，這樣管制的方式在國外的環境是不是有類似這樣的規範，如果有的話，台灣當然有可能可以這樣做，可是如果沒有的話，會不會被說台灣對外資不友善或限制太多，反而限制了台灣在這個產業的活水，不活的話，電信業者我們想要去推這樣的 content，想要把餅做大的機會就被限縮了，我自己觀察不代表公司意見，對 OTT 又愛又恨的感覺，他刺激了我們這個產業，但同時也佔了我們相當程度頻寬，我們希望政府介入，可是又不希望以單一管制電信業者的角度來介入。
政治大學 劉定基教授	1. 從學術的角度來想，因為行業別的關係，所以某些行業的目的事業主管機關是 NCC，某些是經濟部，大家受到管制的程度跟密度因此不一樣，但是大家使用的是同一部個資法，這樣實在有點奇怪。譬如剛提到 OTT 業者，以 Netflix 來講，他在台灣進行服務，在台灣經營實體的公司，當然受到台灣個資法的拘束，那 Netflix 可以在台灣做的任何個人資料蒐集、處理或利用行為，理論上其他的通訊傳播事業，按照同一部個資法，我很難想像是不可以做的。當然我剛強調管制上的差別最大原因是目

	前主管機關不同，我的理解 Netflix 的目的事業主管機關應該是在經濟部，原因是 NCC 對於網際網路的個人資料保護應該是不(想)管的，剛一開始報告時提到 NCC 對智慧聯網想管，我很訝異，因為智慧聯網本質上就是 internet。 2. 看起來研究團隊目前短期的建議之一是要強化蒐集者的告知義務，這個建議在大數據時代要怎麼落實，我蠻懷疑的。個別蒐集者的資料用途在蒐集時可能可以告知一些，像剛剛有些業者提到他們有具體的做法，但是在之後資料處理、利用中間就可能已經有些改變，所以事前的告知要怎麼落實，如果蒐集者根本不知道後續資料經過比對、分析會產出什麼結果，怎麼可能在蒐集時就事先告知？建議研究團隊可以再思考。 3. 當事人同意的問題，大概百分之五十（以上）業者蒐集的資料或他們要做的應用，依據現行法的規定根本不需要得到當事人同意，因為法律上已經有契約關係的存在(ex.幾十萬筆原本要裝機沒有裝機的客戶資料)，那些資料的蒐集或處理，法律應該沒有任何問題，唯一的問題是原來有類似契約關係之後，當這些關係消滅，但業者仍然無限期繼續保留資料才會有問題，但是當初取得個人資料（甚至為了預備裝

	機而利用）不會有任何問題。 現在要減少當事人同意的研究建議，如果起因只是因為技術上要怎麼保留同意的（證明）有困難（或是成本很大），我覺得這不是個大問題，如果 Netflix 可以因為點選同意之後就做這麼多事，那現在應該只是技術的問題，Netflix 可以做，其他通訊傳播業者認為有困難，似乎不太合理。除了這個以外，在現行個資法架構下要減少當事人同意我覺得有困難，個資法沒有額外空間，我也很難想像當事人同意會是一個很困難的問題，因為不管是電信或有線電視一開始一定要簽紙本契約，契約裡面如果已經規範好了，不會是太大的問題，問題反而是因為這些契約是主管機關管制的契約，所以內容不見得是業者想要放甚麼就放甚麼，反而是這個地方研究團隊可以有些空間。在定型化契約內容上，有關個人資料利用的部分，是不是應該可以放寬，但如果超出履行契約必要範圍的利用，一定要明確告知並依法取得有效的當事人同意。 4. 研究團隊還有另一個建議是，強化蒐集者責任，看起來方式是透過 27 條第二項跟第三項，這邊我覺得 27 條第二項跟第三項空間有限，因為法務部的函釋沒有辦法透過該條去增加個資法沒有的規定，尤其是有處罰的規定。

	舉例來說，個資法說資料發生外洩的時候，必須要通知資料當事人，但是沒有說要通知主管機關，這是立法上的一個疏漏。現在許多行政機關訂的辦法，都規定不管業者發生任何資料外洩都必須要通知主管機關，這個有點迂迴，因為母法沒有規定。法務部目前的見解是認為如果目的事業主管機關要用有辦法增加規定這個義務，是可以的，所以包括金管會的辦法就有類似規定；但是法務部有一點抓得很嚴，就是這種超出個資法規定的義務不能有罰則，換句話說，這個規定就是沒有牙齒的規定，如何落實，完全看各個目的事業主管機關的「功力」。當然就通傳事業來說或許不是太大的問題，因為這種特許的行業，主管機關不一定要用罰則來處理，會有很多迂迴的方式。但至少在法理上可能要小心，強化可責性不能超過現行個資法，短期內想用安全維護辦法強化可責性空間恐怕是很有限的，可以有義務的規定，但是不能有處罰的規定。 5. 至於要不要訂專門的法律，跟剛剛第一個問題是一樣的，重點是在專門的法律裡面想要訂的是什麼，如果是說要全面放寬個資法的標準，我覺得這個在現在的氣氛下有困難，特別是通訊傳播業者所擁有的個資可能相對敏感（雖然不一定是個資法上的特種個資）。但如果放鬆

	某些管制，在比較法上，是有立法例可以參照的，比如說歐盟對於電信在行銷方面有不同於其他行業的規定，例如可以先讓你行銷第一次，拒絕之後才不能再行銷，這個在台灣現行個資法上是沒有空間的，第一次行銷就已經要有合法事由，例如履行契約必要範圍內的行銷。類似這種微調或許可以考慮，但我還蠻難想像通訊事業個人資料保護的專法裡面額外可以再放寬什麼。

三、第三次焦點座談討論會議（業界訪談）

- 時間：105 年 3 月 24 日下午 16:00-17:00
- 地點：中華電信法務處會議室
- 業界專家：鍾國強科長及法務處代表
- 研究團隊：

1. 余啟民教授
2. 王慕民研究員
3. 陳品安研究員

- 訪談紀錄：

表 7 第三次焦點座談討論會內容

發言人	發言內容整理
余啟民教授	本次訪談希望中華電信能就本研究案初步研究方向給予寶貴意見。據我所知，中華電信的 emome

	帳單是採取整合的模式，整合很多不同的服務類項，而這些不同的服務類項未來即可進行大數據分析。剛剛王律師有提到定址化鎖定，電信業者可能針對特定的時間、區域的消費者從事行銷活動、訊息推送，就這個部分來講，有沒有尺度？主管機關應該著力的是甚麼地方？目前行政院資通安全會報針對 165 反詐騙的問題責成經濟部來監督電商業者，因此電商業者就由經濟部負責，經濟部只好用個資法的行政檢查權去要求電商業者改進，若沒有改進就裁罰，所以未來在 NCC 會不會也用經濟部這套發動行政檢查權的模式，來針對電信公司要求你們來說明？這或許是未來的方向之一。
中華電信 鍾國強科長	NCC 為電信事業的主管機關，可以本於職權，執行公權力。惟就電信業者而言，使用大數據，涉及個資的去識別化，但業者不清楚去識別化的認定標準？要去識別化到那個程度才沒有侵犯個資？ 現在大家都在討論收視率的調查，有線電視數位化後，透過機上盒可以知道客戶收視的時間、頻道等，這部分有沒有違反個資？可不可以做為收視率調查？業者並不清楚。 建議政府機關應公布去識別化的判定準則(guideline)，讓業者明瞭何種情況會涉及個資？何種情況不會涉及個資？政府正在推動大數據，希

	望產業界藉由大數據創造更多的經濟活力，那麼這些準則必須趕快明訂出來，否則大家有很多創意，但沒有人敢做。
余啟民教授	所以第一個意見是傾向主管機關應先提出guideline（指引）給大家遵循。
中華電信代表	就我的看法，台灣是法律規定的才可以做；可是國外，法律沒規定的就可以做。做了，如果侵害到國家或其他人的權利，法律才會介入規範。最明顯的就是行動支付和第三方支付，像衣索比亞，好幾年前就發展得非常蓬勃，並沒有以法律規範，也沒有出現大問題。但國內金管會認為要有法律規範才可以做，沒有法律規管，這種商業行為不能做。就法治面而言，如果主管機關認為任何新服務，都要用特別法來管，我個人覺得對產業不利，主管機關管太多，對產業發展反而有害。
王慕民律師	業界目前會有兩種極端，一個是法律沒說可以的就不能做，一個是法律沒有說不行的就先做，各行各業的態度都不太一樣，不知道中華電信就這部分的態度為何？
中華電信 鍾國強科長	中華電信遵循法律，依法辦理。
王慕民律師	我們猜想主管機關可能有困境，如果可以做的話，他可能會頒布一個，無論是不是以行政函釋的方式，頒布一個 guideline，但我猜他們無法幻

	想出一個創新方式，畢竟他們是行政機關，他們做的是法規制定和法規遵循，可能無法了解業界實際上怎麼去創新和應用。如果可以的話，主管機關會有意願請業界提供各種情境（scenario）給主管機關參考，我個人認為主管機關應可以接受業界先彙整需求後再做出指引。
中華電信 鍾國強科長	推動產業發展是經濟部的職掌，而法務部是依法行政，各部會執掌不同。個資法的解釋機關是法務部，法務部函釋台電帳單夾寄廣告之內容應與契約有正當合理關聯，使得業者沒有什麼行銷空間。
中華電信代表	針對大數據的應用，各業者最需要的是行銷方面的運用。法務部的函釋，使得行銷的空間非常狹窄。如果依據用戶契約關係蒐集的客戶資料，縱使已告知用戶蒐集的特定目的包括行銷，但行銷的內容必須限定在與契約內容有正當關聯的才能做。在法務部的函釋未被法院的見解推翻以前，我們就只能依照這個函釋去做。但這個函釋，跟大數據的應用相互矛盾，因為大數據的應用就是要活用這些數據資料，開創商機，但是這個函釋造成很多阻礙，這是我個人的淺見。
余啟民教授	所以這也是個具體建議事項，建議這個函釋本身應該重新思考。
王慕民律師	其實這個函釋已經有一陣子了，應該可以再重新挑戰，只是要看誰去挑戰。

余啟民教授	如果我們有具體建議事項時，搞不好長官會願意採納。
中華電信代表	法務部開座談會時，如果老師或教授去表達意見，他們會願意接受；如果業界發表意見，他們會認為業界是為了自己的利益發言。
余啟民教授	法務部可能較不願意聽，政委可能比較容易聽進去。
中華電信代表 鍾國強科長	政府要帶動產業，如果個資法的條文是從嚴解釋，甚而，函釋比條文更嚴格，這樣大數據就很難推動。
中華電信代表	還有一個觀點我想提出來。去年或前年，法務部針對個資法的修正召開座談會，其中有個議題，就是討論配合大數據，個資法應該怎麼修。看到這次新修的個資法，好像沒有看到有配合大數據的修正條文，這跟大家的期待有落差。
王慕民律師	修法這部分可能還要分很多階段去補上。
余啟民教授	因為這次能夠過的個資法條文，是上次通過後馬上又去協調的內容，所以有關大數據的議題，可能是下一個階段。
王慕民律師	現在政委在推 CNS29191 的去識別化標準，目前只有財政資訊中心通過，所以也不知道未來國內大家買不買帳。因為上次在開虛擬座談會時，法務部的科長也有明講說，這個標準不是做了就一定達到去識別化，法院仍會就事實認定，所以便有人提出問題，如果這個標章如果通過，對事業

	會有什麼用處？科長當時回答，這是個業者自律的展現，所以他在法律上的效力也不見得百分之百。因此，這個標準到底能不能推動，也是需要觀察的地方。
中華電信 鍾國強科長	這是目前最大的問題。業者做了去識別化的認證，但認證通過不代表沒有觸法疑慮。若是這樣，做這個認證也沒什麼意義。
余啟民教授	請問中華電信提供的產品或服務，目前而言，對個資的揭示或告知，不知有無標準？其實電信業在舊個資法已被列為八大行業，因此電信業都會做告知事項，只是就其他產品或服務，有沒有做這樣的設計或聲明？或許我們也可以將這種 practice 作為參考。不知道中華電信從舊個資法、新個資法到現在，就個資告知部分，有無任何的 policy？
中華電信代表 鍾國強科長	在個資法公布後，我們公司成立工作小組以符合個資法規定，因此個資法要求的事項我們都有在做。
中華電信代表	在舊個資法時代，我們被要求要用登記公告的方式公告我們特定目的。新個資法實施後，法規要求告知。就我所知，營業窗口在客戶新申請時，都會出示告知條款，請客戶審閱並簽名，證明我們有進行告知。
余啟民教授：	你們所有的服務都是臨櫃的嗎？
中華電信代表	我們的服務都是必須核對證件才能申辦，要臨櫃

	才能核證。
余啟民教授	請問如果後續的加值服務需要臨櫃辦理嗎？例如我簽了一個電信服務，然後在這個電信服務的內容中再加載服務，也會需要臨櫃辦理嗎？或是電話通知即可？
中華電信代表	客戶臨櫃申請時需要簽署服務契約。服務契約所定之服務內容包括加值服務，且告知聲明中的特定目的也涵蓋電信加值服務，所以客戶申請加值服務，如以電話申請，並沒有超過當初申請的範圍。
余啟民教授：	因為我最近去看醫生發現衛福部最近在蒐集一些資料，因此醫院在病患臨櫃繳錢之前，要填寫另外一個聲明，這可能會衍生其他產業在適應新法時所要面臨的問題。
中華電信代表	醫療資料依法不能蒐集，如果要蒐集，需要被搜集者填同意書。早年電腦處理個人資料保護法，現在改成個人資料保護法，早年都有告知，且需要取得主管機關的執照，才可以對個資做處理和蒐集。本公司在實施個資法後，有全面盤點檢討，不管是申請書或告知，要依照個資法第 8 點告知消費者我們蒐集個資的利用範圍，我們是比較守法的。
王慕民律師	在國外的研究上有發現，大數據的發展之下，容易出現問題是後續的應用服務，就是商用化服務，都會超出當初蒐集的目的，所以原本告訴他

	用來申請手機門號或寬頻，本來只是享受契約範圍內的通話服務，但後來為活化大數據資料，國外都有注意到，後來都會構成目的外利用的狀況。所以這段要怎麼處理，可能會是以後不管主管機關要表示也好，或業界可以提出想法讓主管機關參考。因為 NCC 當初在委託案中，有特別要求我們就「特定目的」範圍的放寬機制去研究，NCC 是沒有解釋放寬機制，但我猜測是不是有可能要替業者鬆綁，只要用個很模糊的字眼框下去，只要可以講得通的目的都可以包含，而不認為是目的外利用，所以我當初只要告知一個比較上位且模糊的概念，然後我用放寬解釋的方式把行為全部劃進去。坦白說我看國外的文獻，國外是不採這種說法，尤其是德國，剛好去年底歐盟的個資保護法也修法，德國的個資保護主管機關有針對這個表示意見，再次重申特定目的是個資保護的重要原則，無論如何不能放寬，所以如果我們主管機關要採前開放鬆的趨勢，可能會跟國際上的趨勢背道而馳。所以也想看看長官這邊有沒有什麼想法？可能想要詢問各位長官，對現有的個資法，長官是覺得管太多或管太少？密度太緊什麼都不能做，還管太鬆，很多都沒有講到，害我都不知道能不能做？
中華電信代表	講得不清楚，不知道那些能做，那些不能做。像個資法第 20 條規定，非公務機關利用個資應在蒐

	集之特定目的範圍內，但有下列情形得為特定目的外之利用，這次修法特別加了第七款，我在想是不是為了大數據利用，所以增加第七款「有利於當事人權益，可以做目的外利用」。我覺得這款有解釋空間，今天我蒐集的個資，在我的業務範圍內去做分析應用。法務部一直講，業者可以做大數據分析應用，但是要去識別化。是不是去識別化就不會侵害到個資法? 剛剛提到的李科長，我們在研討會遇到過，他表示雖然是消極不違法，但有沒有侵害隱私部分，應該要另外考慮。這次修法增訂有利於當事人權益，這部分有很大的解釋空間。所以業界就是摸石頭過河，先做做看，再看法院的見解。我認為「目的外利用」應該要有些彈性。
余啟民教授：	假設我的 Call Call 卡，幫我做食衣住行的分類，是不是有利於當事人權益，事實上連我都不知道我有這種食衣住行的分類，雖然他已經去識別化，但也已經做了分類，這種就一體兩面可以去做，這也是一種數據分析。
中華電信代表	所以業者可以做到什麼地步，我們真的不知道。例如剛提到的台電帳單夾寄，將一個好的優惠服務訊息通知你，我認為是有利於當事人權益，但法務部就不這麼認為，我就不懂。法條這樣寫，但業者可以做到什麼地步，我們不知道，這是我們現在最大的問題。或像百貨業，客戶走到

	SOGO，SOGO 就可以推播客戶說他們有什麼產品促銷，聽說這也違反個資，我也不懂這為什麼違反個資。LBS 服務，全世界不知道用了多少，國外實施了很久，民眾在 SOGO 附近就會收到推播的訊息，這應該是一個很有利消費者的資訊，為什麼違反個資? 業者到底可不可以做? 這是我們的困擾。
中華電信代表	雖然現在有制定「有利當事人權益」可以特定目的外利用的要件，但它畢竟還是不確定的法律概念，所以還是要回歸到法務部解釋。如果法務部採取嚴格解釋，縱使法律鬆綁，對業者一樣沒有助益。
中華電信代表	對於 LBS，我們早年曾考慮提供服務。LBS 雖是暴露個人隱私，但在刑事案件和緊急救援的運用上，對當事人有利，應該可以去做。又例如若有人在中橫開車墜落懸崖,可以用 LBS 去尋找。LBS 的應用是一體兩面，看你要怎麼看，可能對消費者有利，但反面來看，消費者開啟地圖定位，車子開到什麼地方，或消費者走到什麼地方，行蹤都會暴露。
王慕民律師	行銷資訊的提供，是不是被認為一定有利於當事人權益，我們認為還是有風險，因為實務上還是有因為寄行銷信結果被告的案例。不確定法律概念到最後就會變成，如果當事人一方覺得不是有利，另一方覺得有利，雙方就上法院。不過因為

	現在新法增訂「推定當事人同意」，這點或許是業者可以採用，指業者如果已經告知應告知事項，當事人看到也沒有表示拒絕並提供資料，就表示同意，這某種程度應該可以表示鬆綁嚴格的蒐集條件，這或許是業者可以走的一條路。
中華電信代表	雖然新法增訂推定同意的條款，但並沒有在利用行為那邊增訂。
王慕民律師	所以我的解讀是一種鬆綁，然後業者可以將未來可能利用的方式都放在告知裡面，消費者看到後仍舊交出資料，就會還屬於目的內利用，不會走到目的外利用。我們的解釋是立法者要刻意開個門讓業者方便做事，另類的特定目的鬆綁。
中華電信代表	您剛提到的部分，因為我們沒有在立法理由看到，所以解釋上仍會擔心。
余啟民教授	剛剛這段討論，或許可以列入未來可能的 guideline 裡面，就法條的層次解讀裡面，就蒐集面如能解決利用方式以及揭露的話，可不可以解決個資法第 20 條目的外利用的問題。
中華電信代表	這樣對我們來說可能會較好。
中華電信代表	未來如果消費者否認，說其實他當時沒有要同意。怎麼辦？
王慕民律師	這就是舉證的問題，變成還是要從技術上看你們事前有多明確，到底怎麼去呈現。雖然新法刪除書面，但書面還是免不了，不過是線上的話，可以寄電子文件。我們也有討論到是不是要用定型

	化契約，因為電信業並不像有線電視有定型化契約應記載及不得記載事項。
中華電信代表	現在正在推。
余啟民教授	有線電視的定型化契約因為有些問題，所以現在是退回去重審。但他過去一直以來都有應記載及不得記載事項，且會被列為評鑑的標準。
王慕民律師	所以電信業未來可能可以用定型化契約同意用電子化文件表示，就可以用電子文件表示同意，可能就比較容易處理書面要簽名的狀況。
中華電信代表	如果用電子記錄保存的話，還是會有點風險。
王慕民律師	對於我們前兩天寄出的討論問題，其實都有詢問到，例如個資法會不會太嚴格，公司現在運用客戶資料時，又特別導入什麼安全維護措施嗎？
中華電信 鍾國強科長	我們對於客戶的個資是非常重視，所以對個資的保護都會遵守主管機關的要求。
王慕民律師	針對之前 NCC 依據個資法第 27 條研擬電信業的通訊傳播事業個資安全維護計畫辦法，公司有沒有想要提出的意見和辦法，可以反映給主管機關知悉？
中華電信代表	先前 NCC 召開過會議跟各業者討論，我們表示過意見，業界也有達成共識。
王慕民律師	之前有學者專家提出，由主管機關一肩扛起監管的責任負擔太大了，有學者提出由民間第三方機構來共管，或是交由業者自律，請問各位覺得這幾種方式，及其控管密度有甚麼想法？

中華電信 鍾國強科長	法律依循就是業者依照法律來遵循，如果每個法規都要有第三方機關來控管法規依循，我認為是疊床架屋，增加大家困擾。個資法已有明訂，就由業者自己依照個資法來遵循就可以了。
余啟民老師	不過像第三方支付的跨境匯付，經濟部也有發執照，期限是一年或兩年，包含法律及會計層面的遵循，每次更新時都要再做一次檢驗。電信的監理或許也可以這樣處理。有線電視的執照是九年，每三年評鑑一次，以電信業者來說，是否有固定時間來做評鑑或查檢，這部分能否加入個資的查檢？
中華電信 鍾國強科長	站在業者立場，我們很不希望增加這些程序。我們會依照法律規定辦理，如果三不五時要來評鑑或查檢，確會增加大家的困擾。若真的有違法事證，主管機關來檢查當然是沒問題。若無違法事證，就不需要來檢查。
中華電信代表	如果再有第三方機構的介入，而主管機關和第三方機構意見不一致時，我們要遵示哪一個單位意見？我們會無所適從。
中華電信 鍾國強科長	主管機關可能會想請第三方機構來協助，委託第三方機構來檢查。但這是主管機關的權責，主管機關才有公權力可以進行檢查。
王慕民律師：	如果今天為了要讓主管機關能夠針對特定的大數據應用來頒布指引，若我們請業界一起來匯整未來可能可以推行的有關大數據的加值服務，讓主

	管機關統一表示意見，您覺得可行嗎？
中華電信 鍾國強科長	行政院應該先成立一個組織來做這件事。業者的要求提出後，究竟誰說了算？通傳會或法務部？我們希望經濟部也能表示意見。如果政府沒有成立一個跨部會的組織，做這件事就沒有意義了。我們很希望政府趕快告訴我們那些可以做，那些不能做，政府應該是跨部會來決定這件事，而非由單一部會決定。以現況而言，是由法務部來解釋，若從嚴解釋，可能還是沒有辦法解決問題。目前經濟部在推大數據，應該由經濟部跟法務部一起決定那些可以做，那些不能做，給業者一條明路。否則經濟部要推大數據，但法務部要維護個資權益，兩邊的立場沒有交集。 另請問數位電視盒上做的收視率調查究竟有無違反個資法？
余啟民老師	以現在還沒修訂的應記載不得記載事項來看，可能會有問題。因為我之前審客服時，他們大多還是用舊的條文，但有些業者的條文有一些更動，可以從寬解釋。我們查驗客服的時候，如有聲明，我們就會打勾，但我會給一些建議給委員會作參考。若將利用方式明載於契約上，會比較妥適。
中華電信 鍾國強科長	當然能在合約上記載清楚是好事，但新的應用不斷推出，可能無法在原合約中事先完備記載，這樣新的應用服務出來，到底可不可做，仍舊會是困擾。就我個人想法，收視率調查就是統計資料，

	這算不算是去識別化？如果大家都認為統計資料是去識別化的資料，講清楚，大家都可以做，那就很簡單了。
余啟民老師	您提出很棒的意見，所以如果能在應記載及不得記載事項中寫清楚去識別化之統計資料可以利用的話，我們就可以依循這個去做應用。請問還有沒有其他建議？
中華電信代表	請問單獨一個電話號碼算不算個資？單獨一個 E-mail 算不算個資？
王慕民律師	這要看下一個動作是甚麼？要怎麼用這個電話或 E-mail？
中華電信代表	若我把單一的電話號碼給你，讓你做行銷呢？
王慕民律師	若後面搭配的是行銷，有可能會被認定是利用個資的行為。
中華電信代表	但這個電話號碼其實不知道是誰所有？不知道他的姓名、性別、地址等資料？我單純給你一個電話號碼，你去寄一個行銷廣告，這樣有違反個資法嗎？
王慕民律師	台灣目前還沒有法院對這個表示意見，但從國際上來看，澳門曾經討論過這個議題，那個案子的行銷人員說我隨機抽的號碼，不帶姓名、性別，只隨機抽出號碼就寄廣告給他，市民收到之後就去檢舉，後來澳門個資保護的主管機關就認定這樣的行為違反個資法，因為他們認為即便你不知道我的姓名等其他資料，但這個號碼還是可以連

	結到我，而你可以利用這個號碼，針對我來對我投遞廣告訊息，這是對於資訊自主控制權益的侵害，因此認定這樣的行為是違法的。
中華電信代表	其實這應該有兩派見解，一派認為侵害個資，因為對電信業者而言，號碼在電信業者是可以間接識別到特定人，所以屬於個資。但若在外面，隨便一個電話號碼，應該不構成個資。這就很奇怪，在電信業者內部算，在電信業者以外不算，很矛盾。
王慕民律師	一個資料在不同的脈絡下，確實可能會有不同的認定。
余啟民老師	問題是，這個門號當初在臨櫃申請時，有沒有說明可用於行銷目的？假設沒有事先說明，可能就會有問題，但若當初有一些文字說明，例如「本公司會提供更好的服務」等等，這部分可能就比較沒有問題。我們希望能透過這次訪談蒐集到大家的建議，看有沒有甚麼類別或文字，未來放在契約裡面，可以幫助消費者比較清楚了解，這也是對消費者隱私的尊重。
中華電信代表	我們公司的號碼一定是用在我們公司內部的行銷，只會做我們業務範圍內的行銷，不會交給外面的人去行銷。如果是隨機抽取出的號碼，不應該認定違反個資法。
余啟民老師	中華電信的帳單應該都是制式格式。假設你發現我常常打國際電話，便對我做 Special Promotion，

	或是你知道我有申請過數據漫遊，你便常常遞送數據漫遊的推廣訊息給我，這也是一種大數據的利用，這樣您們怎麼看呢？未來你們會考慮做這樣的服務嗎？或者已經這樣做了？
中華電信代表	您說的是客戶分析，但這又回到個資法的問題，有沒有超出特定目的利用？如果當初申請時，已經告知會對你做一些分析及行銷，你也同意，這樣就沒有爭議。例如我對你個人消費行為作分析，你常打國際電話，如果某一段時間有國際電話優惠時，我會事先通知你。另外，有關這次修法「特定目的外利用」第七款「有利於當事人權益」的修訂，如果在特定目的內利用是沒問題，但若超出原來的特定目的，可不可以認定是第七款的「有利於當事人權益」？如果可以這樣認定，應該就不算違法了。
余啟民老師	如果以其他業者的範例，你們在合約上寫我們會就 emome 的各項服務下做行銷推播，如果客戶簽字同意了，就比較沒有爭議。因為 emome 是整合式的服務，也包括小額付費服務，這樣對於　貴公司或許更好。
中華電信	這也涉及到告知的範圍，要不要比較具體？或是範圍要大一點？當然有一些是列舉的規定，最後應該有一個概括的條款，在解釋上，未來若有新的服務，可以納入概括條款。
王慕民律師	國際上討論告知條款也有這樣的問題，我不可能

	在一開始的告知條款告訴你我未來所有的創新服務，因此他們反而把重心往後移，移到事後，看有沒有給當事人一個退出的機制？將來可能會要求你在事前大略告訴我你要做什麼，例如你把我的資料拿去做統計分析，這樣就可以了，但是我事後有一個權利，就是我可以拒絕你繼續用。如果我事後想想覺得不妥，我就可以要求你只在契約範圍內提供我服務就好了，不要把我的資料拿去資料庫作統計分析。這也是未來可能可以去調和資料蒐集者和資料提供者之間武器平等的方式，也或許是　貴公司可以考慮的模式。
中華電信代表	這也是法務部科長曾提及的「當事人退出機制」。實務上來說，消費者可能很難瞭解業者究竟拿資料做了甚麼統計分析，但業者提供這樣的退出機制給消費者選擇，消費者會比較放心。主管機關也會認為這樣比較好，讓當事人有自由選擇的機會和權利。

四、第四次焦點座談討論會議

- 時間：105 年 3 月 25 日上午 10:00-12:00
- 地點：東吳大學城中校區 R110 會議室
- 業界專家（依發言順序）：

1. 台灣大哥大—簡肇盈律師
2. 台灣雅虎—林煒鎔總監

3. 中嘉網路—趙培培資深副總、游博治主任

4. 中天電視—蔡玟瑛經理

➢ 研究團隊：

1. 余啟民教授

2. 王慕民研究員

3. 陳品安研究員

4. 張又丹研究員

➢ 討論議題：

一、 就用戶資料的加值運用或大數據利用而言，現行個資法對業者有無窒礙難行之處？有何認為規範不夠詳盡或過於嚴格之處？

二、 如將用戶資料加值運用或大數據利用時，是否採取特定措施確保個資安全或當事人權利保障，例如去識別化技術？

三、 有無提供用戶拒絕公司以其資料加值運用、分析的管道？

四、 我國應否就通訊傳播事業的個資保護制定專法

五、 現行法規授予 NCC 的監管權限是否適宜：

(一) 制定通訊傳播事業個資安全維護計畫辦法

(二) 行政函釋

(三) 行政指導

(四) 行政檢查(稽核)

六、 若 NCC 將通訊傳播事業利用用戶資料進行大數據應用的監管採取與民間第三方機構共管方式是否可行？交由業者以自律機制自行管理是否可行？

七、 綜合討論

➢ 業界專家發言：

表 8 第四次焦點座談討論會內容

業界專家	發言內容整理
台灣大哥大 簡肇盈律師	1. 有關大數據的定義可能要釐清，每個人對大數據的理解可能會不同，確定大數據的定義之後才有後面修法的問題，大數據未來的發展如果到時候要因應這個發展，要怎麼樣在法條裡面呈現，那首先就必須要對大數據有明確的定義，不然在後面的討論會很容易分歧。從另一個角度，大數據到時候在法條的規管要怎麼呈現，其實在規管上要有價值的判斷不只有技術，怎麼樣才算明確的大數據，這個部分可能還要再討論。 我看了個資法裡面，第 20 條裡面有提到學術統計分析，必須基於公共利益，但是這跟我們討論的大數據是不是完全的 match 還是有點落差這樣我不曉得，但如果他指的就是我們說的大數據的話，那針對這個條文就可以進一步探討，例如說是不是限縮在公共利益還是說商業使用也可以去做這樣的處理，但如果這條本身不能涵蓋大數據，那在個資法裡面可能就要有專章或增加條文來針對大數據有些修正會比較明確，否則個資法整個法條裡面，規定都散落在各個地方而且有點複雜。 2. 剛余老師講到用戶同意用帳單的方式，聽起來好像很簡單，實際上運作的話，如果用戶他們

	沒有誘因，他們是不會做這件事的，就好像我們在簽信用卡，銀行問我們資料可不可以給其他公司使用，基本上都是否定的，大數據的利用基本上要量夠大，如果說必須要取得用戶同意，可能一成兩成都不到，如果兩成的話對數據的應用本身統計上就會失真，所以其實是有個盲點在，幾百萬的用戶能夠大家都同意這其實是很困難的。 3. 其實本身個資法緊箍咒就在那邊，NCC 不可能去超越個資法，基本上不會有創新的解套方式所以幫助不大，舉個例子，台灣大哥大有推出 M+，會顯示你的通訊錄裡面的人是使用哪個電信，有受到一些反彈跟介入來進行行政指導，他們的原則還是依據個資法，只希望你不要惹麻煩，不會去想說這樣的服務對客戶有甚麼幫助，可是討論到後來我們退一步，本來是我們 M+裡面的通訊錄顯示各業者，後來變成通訊錄裡面的人會顯示網內還是網外，NCC 來函回覆說這其實是符合個資法，但是還是得到法院去，法院還是判定違反個資法，所以從這裡可以知道說業者的創新服務風險非常大，這個用戶到底有沒有同意對我們來說有討論空間，在業者的角度來看當你推出一個服務，到時候會有違反的風險，那個後面的整個處分的影響跟損害賠償是非常大的，所以基本上會造成業者

	很多創新服務是不敢貿然去做的，所以這個部分基本上是在個資法那邊就應該做一些相關明確的界定，政府對創新產業沒有勇氣去面對，所以很多業者已經錯失先機，所以對於第五題我們是認為到底的實益在哪邊，有的話指是在個資法框架下做更多的規管，你所謂的同意的怎樣的同意反而對業者來說沒有彈性。 4. 匯流五法專章研擬我們是非常同意的，但是會有個大問題，專責研究個資法的一直都是法務部，法務部訂定個資法但是不想要自己當主管機關，如果匯流五法放進去，NCC 在面對個資法解釋，內部在處理個資法專精的人其實不多，要怎麼樣在匯流法裡面做一個比較前進的個資條文，其實難度很高，要制定專法效益不大，應該說要有個專責機關，國內需要一個專責機關，非常了解個資法，跟 TIPO 一樣他們對智慧財產權很清楚，知道未來的方向趨勢，才能制定一個跨時代的個資法，但是現在如果要求 NCC 做一個對未來有創意跨時代的想法的個資法，其實難度是非常高的，他會面對很多問題，所以我們應該要設立一個專責機關，確實我們個資法的問題太多了，而且阻礙到各個產業的發展。 5. 我們是認為說，剛老師有提到匯流，基本上未來通訊傳播的各個業務其實會很模糊，個人資

	料的運用會很流通，公司跟公司之間的業務，資料流通的需求會越來越多，金控法裡面，各個公司可以共同行銷，基本上在我們這邊沒有這樣條文的 support，業者跟業者間做的事已經越來越接近，但是因為個資條文的限制，很難做些突破，是不是能夠像金控法一樣可以流通，打開這個大門，讓同集團內的相關資料可以流通，然後可以做共同的行銷，我想這樣比較明確一點。 6. 根據客戶的習性和消費習慣，去整理出一個資料已經去識別化，那我把這些資料賣給其他產業這樣會有問題嗎？從蒐集、處理、分析到利用，利用的話已經去識別化，會有問題的應該就是在前面的告知。我的意思是說其實對用戶的保障應該是有分層次的，他個人的資料我拿去賣這個一定要充分的告知，但是如果我只是把大數據的資料整理之後再賣出，其實對個人的影響應該就不是這麼明顯，所以對告知的部分應該要降低他的同意權，如果是這樣的話是不是要告知，可能就要在前階段有些修正。
台灣雅虎 林煒鎔總監	1. 前面先進提及個資法，現行個資法的問題，是規範架構的疊床架屋。一個公司如果有經營通訊傳播事業、電子商務、代收付、以及其他資訊服務業等等的話，會有多個主管機關（包括 ncc、商業司、工業局等等），而現行每個主管

	機關都有不一樣的安全維護計畫辦法（可能多達五六個，而每套條文都不一致），重點是，每一個主管機關都有權來公司行政檢查，此種規範架構，其實是個很不健康的個資法規範方式，也不是解決問題的辦法。因此，我們不希望再多訂一套安全維護計畫辦法、行政函釋之類的。我們公司有完整的隱私權政策（privacy policy），整個公司遵循一套完整的隱私政策，針對同服務有不同對外說明（比方說電子商務服務的隱私權範疇跟廣告服務可能不太一樣），建議我們個資法考慮調整規範架構，不建議執意採行造成一個公司可能必須遵守多套安全維護計畫辦法這種規範方式。 2. 另外，不希望有國家標準，沒有意義，因為我們遵守的規範不是只有台灣，隱私權政策是全球的（只是語言不一），過去的經驗是台灣喜歡訂一套只適用在台灣的標準，箝制境內業者但對境外業者卻鞭長莫及，這種規範方式毫無意義可言。 3. 我們不管做任何的資料處理或利用，是否去識別化，都一定會告訴使用者經過使用者同意。比方說，我們必須明確的告訴使用者 IP 位址只留六個月，六個月後就去識別化等等，這些我們都會很明確的告訴使用者。另外，現在科技跟過去不同，比方說個人化廣告，不同使用者

	開了我們的影音服務，每人看到的廣告內容不一樣（ad targeting），假設我是 50 歲女性，我不想看到一般這個年齡層女性會看到的廣告，我可以自己更動設定或選擇退出，我們在使用者註冊時就明確告訴使用者他的個資將怎麼被利用。我們隱私政策針對不同服務而撰寫，是要讓使用者看懂，或許跟個資法現在針對目的事業主管機關或是項目的分類有點不同，但那是若按照個資法照本宣科分類，使用者看不懂，我們隱私權政策是用白話的告訴使用者他們的資料是怎麼被利用的，也跟使用者很明確的說他可以選擇退出，「如果」有任何個人資料會分享給第三方廠商，也一定要跟使用者講我們跟廣告商分享資源，使用者不同意的話當然可以選擇退出，也隨時可以修改個人資料或是行銷偏好。因此，不是只針對通訊傳播事業，對我來說，e-commerce 也是我們的服務，我也用一樣的方式處理。但實際上我們要遵守不同主管機關規範，如果不同主管機關規範不一致，對我們來說會有困擾。主管機關對科技沒有足夠的認知，訂出來的辦法會很可怕，對我們這樣的公司來說非常困擾，尤其是當政府技術能力追不上業界，規範方式值得考慮。 4. 另外，電子通訊傳播法有個章節是個人資料保護，一樣有個問題就是主管機關是誰、誰來執

	行、罰則是甚麼，疊床架屋的規範恐怕跟個資法一樣的問題，但這種規範方式是沒辦法解決問題的。我猜主管機關的想法恐怕偏向要「監管」，但監管想要監管什麼，就我的認知今天是講「監管」「個人資料蒐集處理利用」，但既然是個人資料保護這個問題，應該回頭討論個人資料保護法規範的架構。如：分散給各目的事業主管機關管理是不是好方式，以通訊傳播事業為例，甚麼是通訊傳播？舉個例子，比方說我播網路的節目，使用者點下主播穿的衣服他就可以直接買，或是看做菜節目，點擊材料或食譜久直接連到超市買，這些買東西的個人資料，在台灣要遵循電子商務還是所謂的通訊傳播事業規範？還是所有規範通通都要遵守（然後就得遵守越來越多規範)。我舉這個例子就是說如果要用這個方式去限縮通訊傳播事業的話，聽起來很合理，這樣跟不上實際趨勢的發展，這個是通訊事業還是影音，政府不管是擴張或是限縮自己管的範圍，都不是健全的政府管制方式，因此這套管制規範是否能跟上科技發展很值得被討論的。
中嘉網路 趙培培資深副總	1. 有線電視以往還沒數位化前對客戶資訊的應用只 for 一般的帳單，或是一些服務的告知，所以以前並沒有什麼問題，隨著數位化服務，個資法其實對於事業的轉型是造成困擾的。

	有線電視登記的用戶資料可能是父親，但是使用的人不一定是註冊的人，所以我們在研發數位加值服務的時候，因為本身我們不一定會跟個資作連結，例如用機上盒（set-up box）點 VOD（Video-On-Demand），我們在乎的不是用戶登記的資料，我們會分析的是說假設 VOD 的存續期間是三天，但是他是一次看完還是分次看完，我們在這樣的所謂視訊應用上面，幾乎沒有跟個資畫上等號，我的理解在用戶資料的加值應用上一定要有事前告知且事後用戶可以自行退出，可是我覺得在大數據利用上有些跟用戶資料有連結，但是其實很多都是 by box 的行為，這塊其實才是不應該被管制的，隨著整個傳播產業更進一步可能跟電信有跨業結合，以後要處理的問題是因為多螢的關係，對於家庭戶跟個人資料連結的部分，也就是今天假設父親訂了一個機上盒，但是有可能是他的兒子使用 iphone 或平板去訂閱視訊服務，對我而言他只是收視行為的分析而已，隨著我們的認知，以後家庭化要延伸到個人，或是家庭外面走出去連結電信業者的網路然後收看機上盒的東西，那個的個資就跟當初註冊的用戶不一樣，到底什麼時候要取得哪個用戶的同意，到底是機上盒的用戶同意還是末端使用者的同意，那個才是未來一定要去思考的，不管是個資法要

	修正也好，或是說主管機關在訂定安全維護的時候應該要與時俱進，否則會因為他的限制影響到我們對用戶提供一些比較 fancy 的服務。所有只要沒有去識別化的 data，商業上我們覺得有利用價值的，是不是都要允許我們可以做，這才是一個服務，如果在家裡他就是有看電影的需求，有點選的話，那我們是不是透過一些訊息跟優惠的寄送這塊的利用。 2. 特別收視率調查的部分，目前我們是做內部使用，原則上我們都是全部去識別化技術，也就是說我們是 by box，不跟開博的用戶系統連結，我會很純粹的看到這個時間全省的用戶目前在收看哪個頻道，所以對我們而言跟個資的部分是沒有連結的，我們現在也不敢連結的原因是通常用戶的申請都是很早以前，可能是 10 幾年前所訂的用戶同意合約，以前完全沒有想到未來會有這麼多不一樣的數位影音的利用，先前的個資法希望我們在目的內使用，那到底以前的目的就只有收視，也不知道以後會跟廣告商合作插播廣告，因為數位時代而帶來的便利性，然後提供給用戶符合他們需求的頻道，其實我們都面臨很大的困難是，沒辦法重新取得用戶的書面同意。 3. 我們現在的問題在於機上盒跳出來同意的不一定是當初的註冊人，其實我們是希望在技術上

	克服這點，可是因為遙控器不是像手機或平板電腦這麼好操作、書寫，如果註冊人不是使用者，這樣使用者是不是又要再填其他資料？在技術上跟修法後允許的方式是不是雷同？這階段我們還在克服中。 4. 我也是比較建議看中長期，就像剛余老師講的，現在匯流五法我們都覺得 NCC 所提的這個包括通訊傳播跟 data 這塊，譬如說通訊傳播、資訊事業跟個資，其實這三個他的定義跟資訊，到底是什麼？另外，OTT（Over-The-Top）應該被規管，目前第一版的匯流五法他是希望有做頻寬保證的，那如果基於這個匯流五法裡面要再訂立專法，那能不能對超越規管範圍以外的產業去做個資法的放寬，也是說主管機關現在鼓勵我們如果不想被管，那你 MSO 就轉型，你以後做開放平台，也不要做頻寬保證。但是現在的過渡期，我在我既有客戶裡面一定是一個封閉型網路，那我為了要做更多的客戶服務，可能是往外 OTT 的這塊，最終大家的商轉模式其實大概都會跟 Doris 講的一樣，所以我還是要跟電子商務這塊一定要連結，但是這塊可能在這個專法裡面事實上就沒有保護傘，就會變成你的營業範圍要被切割，你在這塊有這個專法可以保護，可是最終商轉模式的部分是沒有開發的，尤其是現在數位匯流五法裡面我

	覺得他還沒有到達一個比較定性或共識的階段，我覺得是以中長期看起來是可以去研究，那個專法是在做很多解套，這塊目前在匯流五法裡面 draft 的階段好像看不到，就是希望他能夠好好把我們擔心的問題一次在這個專法裡頭做解決。
中天電視 蔡玟瑛經理	1. 就電視台來講，他的屬性比較特別，就個資利用的這部份，我們應該是還在小朋友剛在學走路的階段，我在電視台待比較久的時間，我記得以前在新聞局時代電腦處理個人資料保護法是給我們一個證書，以前八大行業必須要申報後會發一張執照，個資法從 99 年到現在一直再改，我們總公司也因為這個內部有很多調整，國外的看法跟國內的看法都不太一樣，如果 OTT 要進來，政府對於個資法要做規管，定義很重要，雖然有點難，個資法現在所有行業都被納入，不是以前那個時代，我覺得法務部很不錯，最新修正的版本有幫我們很大的忙，就是把書面同意這部分拿掉，當初因為這個我們還跟國外討論，我們算是間接拿到這些資料，拿到資料之後怎麼去處理跟利用還有怎麼樣取得事前的告知，所以我們之前很緊張，NCC 很認真他跟我們開很多會，當初這個辦法已經擬了草案跟罰則，我們也很緊張，一個行為到底要有多少人管。

	2. 對我來說最好的是行政指導，就是有事情發生的話，事後處理或是有救濟，回歸到王律師講的，我們現在到底是要訂一個法律沒有禁止我們做的，就像一般的商業條件有個帝王條款，只要法律不是限制我就可以做，這樣可能比較適用各行業，現在不像以前八大要被規管，是每個行業都要被管，如果每個各目的事業主關機關都管一套，所以回歸到這次，我覺得法務部這次蠻體恤我們的，至於 NCC 我們比較喜歡行政指導，然後不要再立專法了，這次的廣電三法我們也很困擾，他太多授權命令，我們可不可以穿著衣服改衣服。 3. 另外，共管我反對，我覺得還是自律，既然資料比較需要被保護的話，那如果又找了一個民間機關然後再來共管，這樣就像保險之後又在保險，我覺得沒有甚麼必要，我覺得還是回歸自律，或者是說可以比照當初有證書，只要你是大量使用個資的，就可以有個免死金牌，就是我的注意義務沒有這麼高，因為我的業務往返的關係，我覺得這樣做一些輕度的規管，當初為了以前那張證書也是搞了很久，我是建議也許可以這樣，這只是一個粗淺的想法。 4. 雖然現在個資法好像每個行業都要被管，其實我覺得對業者來講不管是討論甚麼法規，每次去討論最好都是 deregulation，我們都是希望不

	要被管，像支付寶的事情，我們台灣真的很可惜，你的利益是好的但是有時候實際變成害了我們，就是你阻礙了這個產業的發展，就像簡律師說的，一些創新的想法是沒有人敢做的。

第二節　學者業界意見整理

一、以專法或法規命令管制的必要性

由於我國目前採取「一部個人資料保護法」由各中央目的事業主管機關「分別管理」的監管方式，對通訊傳播業者而言，若在實務上未獲得主管機關國家通訊傳播委員會的明確表達立場，而僅依法務部少量的函釋或是少數司法判決作為用戶資料加值運用的準據，恐將因擔心違法受罰或涉訟而踟躕不前。且依通訊傳播事業之特性，若完全依現行個人資料保護法操作，亦有解釋模糊或規範不足的疑慮，例如：

1、 有線電視系統業者透過機上盒(未針對該家戶內的特定收視人）取得的收視行為，是否屬於個人資料？
2、 行動電話號碼、IP 位址是否屬於「可識別特定人」之個人資料？
3、 業者對於用戶基本資料、流量資訊與位置資訊之加值利用是否需要獨立明確向用戶事前告知，以確保用戶得以行使其「拒絕利用個資」之權利？
4、 業者將用戶資料加值分析利用，須否取得用戶同意？或僅事先告知即為合法？
5、 業者可否對用戶行銷異業合作對象之商品或服務？是否構成目的外利用而須事先取得用戶同意？

以上示例均為通訊傳播業者在現行個人資料保護法規範下將面臨的難題，仍有賴主管機關進一步說明立場。是以在本研究的歷次學者、業界代表會議中，與會專家或有認為應以專法針對通訊傳播事業之特性與以管制者[182]，亦有認為可從現行法律著手（例如電信法）修正[183]，在小幅度調整範圍內針對用戶大數據資料的加值運用作出規範，甚或於法律中制定授權條款，由主管機關針對業者的相關行為制定管理辦法[184]，例如銀行法第 47-3 條[185]或金融控股公司法第 43 條第 3 項[186]。

此外，專家也從個人資料保護法的角度出發，認為業者以

[182]見第一次焦點座談討論會議，翁清坤教授、邱文聰老師發言；第二次焦點座談討論會議，凱擘林雅惠副處長發言；第四次焦點座談討論會議，中嘉趙培培副總發言。

[183]見第一次焦點座談討論會議，方修忠教授、戴豪君資訊長、葉志良教授發言。

[184]見第一次焦點座談討論會議，方修忠教授發言；第四次焦點座談討論會議，台灣大哥大簡肇盈律師發言。

[185]銀行法第 47-3 條：「經營銀行間資金移轉帳務清算之金融資訊服務事業，應經主管機關許可。但涉及大額資金移轉帳務清算之業務，並應經中央銀行許可；其許可及管理辦法，由主管機關洽商中央銀行定之。（第一項）經營銀行間徵信資料處理交換之服務事業，應經主管機關許可；其許可及管理辦法，由主管機關定之。（第二項）」。

[186]金融控股公司法第 43 條：「金融控股公司之子公司間進行共同行銷，應由金融控股公司事先向主管機關申請核准，且不得有損害其客戶權益之行為。（第一項）金融控股公司之子公司間進行共同行銷，其營業、業務人員及服務項目應使客戶易於識別。除姓名及地址外，共同蒐集、處理及利用客戶其他個人基本資料、往來交易資料等相關資料，應依個人資料保護法相關規定辦理（第二項）。依第一項規定申請核准應具備之條件、應檢附之書件、申請程序、可從事之業務範圍、資訊交互運用、共用設備、場所或人員之管理及其他應遵行事項之辦法，由主管機關定之。（第三項）金融控股公司之子公司與客戶簽訂商品或服務契約時，應向客戶明確揭露契約之重要內容及交易風險，並依該商品或服務之性質，註明有無受存款保險、保險安定基金或其他相關保護機制之保障。上述契約並需向主管機關或其指定之機構報備，並責成於各金融機構之網站公告。但其他法律另有規定者，從其規定。（第四項）」。

現行法「與當事人有契約或類似契約關係」要件，再搭配告知義務的踐行，即可合法運用用戶的大數據資料，並提出主管機關可由「定型化契約應記載及不得記載事項」著手納入個資法遵循相關規範之建議[187]。

二、與民間第三方共同管理

相較於由主管機關國家通訊傳播委員會一肩扛起管理之責，亦有專家提出與民間第三方共同管理用戶大數據資料加值應用的因應對策，並以「號碼可攜服務管理辦法」為例，認為或可區分「資料產出機關（通訊傳播業者）」與「資料分析機關（第三方」分別處理用戶大數據資料的分析利用，再搭配「資料稽核機關」執行稽核以確保用戶資料的安全性[188]。

然而亦有專家主張此舉恐有疊床架屋之困擾，徒增資料傳遞之複雜與安全性疑慮[189]。

三、業者自律並由市場機制管理

除了上述措施之外，亦有與會專家認為站在用戶大數據資料創新應用的立場，對於個資保護的遵循應交由業者自律，以市場機制管理即可，避免業者疲於應對不同業務之不同中央目的事業主管機關各自的個資安全維護計畫或其他管理辦法(例如人事、電商、通訊傳播)，造成業務的僵化或阻礙發展，對業者的負擔實將過苛[190]。

---

[187]見第二次焦點討論會議，劉定基教授發言。

[188]見第一次焦點座談討論會議，資策會戴豪君資訊長發言；第二次焦點座談討論會議，寬頻協會彭淑芬理事長發言。

[189]見第三次焦點座談討論會議，中華電信鍾國強科長發言。

[190]見第四次焦點座談討論會議，雅虎林煒鎔總監、中天電視蔡玟瑛經理發言。

第八章 結論—通訊傳播事業利用個資規管改革方向

綜合以上研究及專家學者意見，以下將由通訊傳播事業主管機關國家通訊傳播委員會的管制手段出發，提出在現有法規架構下的短期建議以及制訂專法與增補個人資料保護法的長期建議，作為本報告的結論。

第一節 管制手段

一、行政檢查

依個人資料保護法第 22 條第 1 項規定「中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。」亦即賦予中央目的事業主管機關對於主管事業的行政檢查權限，得以稽核其個資安全性與適法性。

我國實務上已有經濟部於 104 年 5 月針對較常發生個資外洩之資安事故的網際網路零售業者組成「個資保護行政檢查小組」進行實地查訪，稽核其技術面的安全防護措施，並限期提出改善[191]。

通傳會為通訊傳播事業之中央目的事業主管機關，亦可依法律授權之行政檢查權對於通訊傳播業者執行稽核，尤其在大數據技術下，

[191]經濟部即時新聞，2015 年 4 月 24 日，見 http://gcis.nat.gov.tw/main/publicContentAction.do?method=showPublic&pkGcisPublicContent=4025 ，最後到訪日 105 年 4 月 14 日。

通訊傳播事業將保存極大量的使用者資料以資利用，因此無論在適法性與安全性層面均應負擔更重的法律遵循與安全維護義務，主管機關的稽核將有助於業者責任的落實。

二、行政指導

依行政程序法第 165 條第 1 項規定，行政機關在其職權或所掌事務範圍內，為實現一定之行政目的，得以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人為一定作為或不作為之行為。據此，通傳會亦可以行政指導（例如發布行政函釋）之方式，輔導或建議通訊傳播業者採取適當之作為，以因應大數據技術下的用戶個人資料應用行為。

三、訂定個人資料檔案安全維護計畫辦法

依個人資料保護法第 27 條第 2 項及第 3 項規定「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」、「前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之」。

通傳會為通訊傳播事業的中央目的事業主管機關，即可在現行法的授權下依職權訂定「通訊傳播事業個人資料檔案安全維護計畫辦法」，並在其中納入要求通訊傳播事業在大數據及智慧聯網技術下應遵循之規範。

四、修訂定型化契約應記載及不得記載事項

由於通訊傳播業者蒐集用戶資料之合法要件多為個人資料保護法第 19 條第 1 項第 2 款「與當事人有契約或類似契約之關係，且已

採取適當之安全措施」，是以由主管機關制訂「定型化契約應記載及不得記載事項」亦可作為用戶資料大數據應用的規管方式。

五、制定專法

通傳會為通訊傳播事業之主管機關，為監管業者對於用戶個人資料的蒐集、處理與利用，亦可考慮制定專法作為各項管制手段的法律依據。

第二節　短期建議（在現有法規架構下）

一、區分各類個人資料管理

在不修法的前提下，通傳會可依美國聯邦通訊傳播委員會對於寬頻服務提供者隱私保護規則制定命令公告的方式，並參考歐盟、英國、日本等國的管制作法，先將通訊傳播事業所涉及的用戶個人資料予以區分並定義，例如個人資料的範圍、來源、基本資料、流量資訊、通信紀錄、位置資訊、瀏覽紀錄、收視紀錄、帳單明細等，邀集通訊傳播業者提出對各類資訊的管理及運用之反饋意見，經充分討論思辯後，以彼此共識作為將來修訂法律、制定行政規則、制定個人資料檔案安全維護計畫管理辦法、修訂定型化契約應記載及不得記載事項，或執行行政檢查或行政指導的依據，以各項強制或自律手段達成保護或管理之目的。

二、訂定通訊傳播事業國際傳輸個人資料之限制標準

個人資料保護法於第 21 條規定在有特定情況（涉及國家重大利益；國際條約或協定有特別規定；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；以迂迴方法向第三國或第三地區

傳輸個人資料規避個資法）時，中央目的事業主管機關得限制該國際傳輸。

考量通訊傳播事業將用戶資料國際傳輸至第三國或第三地區漸成通傳會的管理重點，通傳會即可參酌本研究報告第五章第一節第九項「國際傳輸」所列歐盟作法，就通訊傳播事業將用戶個人資料國際傳輸之限制訂定標準，除載明具備完善個資保護法規之國家外，可考量正面表列符合何等條件者始為個資保護完善，或負面表列若有何等情況即視為個資保護並不完善，以此作為通訊傳播業者一致性的因應準據。

三、訂定個資檔案安全維護計畫管理辦法

在個人資料保護法第 27 條第 3 項的授權下，通傳會可以制定個資檔案安全維護計畫管理辦法的方式，將大數據技術下通訊傳播事業用戶的個資保護管制納入規範。

(一) 規範限制

應留意的是，由於該辦法之規範內容不得超出個人資料保護法之授權，不可增加法律所無之限制或責任，因此該辦法僅能在個人資料保護法第 27 條所謂「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏（第 1 項）。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法（第 2 項）。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之（第 3 項）。」之範圍內，就「防止個人資料被竊取、

竄改、毀損、滅失或洩漏」的「安全維護」及「業務終止後的個人資料處理」制定規範。

(二) 草案內容檢視

檢視本研究委託機關國家通訊傳播委員會提出之「電信事業訂定個人資料檔案安全維護計畫標準辦法草案」及「廣播電視事業訂定個人資料檔案安全維護計畫標準辦法草案」可見，內容多係依個人資料保護法施行細則第 12 條第 2 項所列 11 款安全維護措施，並導入資訊安全管理系統之因應作為規範依據，尚未針對用戶大數據資料應用涉及面向（例如目的外利用、蒐集目的消失後之資料保存、個資去識別化應用等）制定管理辦法。

(三) 規範內容建議

據此，本研究擬在符合個人資料保護法的授權範圍內，建議增加下列項目作為安全維護計畫標準辦法之規範：

1、 特定目的消失或期限屆滿後的資料處理

由於大數據應用的特性之一在於資料的龐大性，因此對通訊傳播業者而言，即便蒐集用戶資料的特定目的已消失或期限屆滿，但歷來取得之用戶各項資料或仍具有分析應用之價值，加以依本研究團隊執行個資法稽核實務之經驗，業者多以「資料庫內的用戶資料無法完全刪除，否則將造成系統運作障礙」為由，主張符合個人資料保護法施行細則第 21 條第 3 款「其他不能刪除（個資）之正當事由」而拒絕刪除當事人之個人資料。

是以本研究參酌美國消費者隱私權法草案規定，建議於標準辦法中增加**「電信/廣播電視事業於蒐集個人資料之特定目的消失或期限屆滿後，應依本法第 11 條第 3 項規定，以不可回復之方式刪除個人資料。如因正當事由而不能刪除者，應在合理範圍內以無法再識別特定當事人之去識別化方式保存資料」**。

2、 導入去識別化概念作為用戶資料大數據應用之基礎

考量我國目前著重「去識別化」標準的發展趨勢，本研究亦建議將「去識別化」納入標準辦法中，作為業者應用用戶大數據資料之依據，例如**「電信/廣播電視事業利用個人資料時，應建立相關程序確實遵守本法第 20 條規定，或以無法再識別特定當事人之方式對第三人提供去識別化之資料或將去識別化之資料公開」。**

四、修訂定型化契約應記載及不得記載事項

依現有的「有線廣播電視系統經營者／有線播送系統定型化契約應記載及不得記載事項」來看，目前僅在第 10 條對於訂戶資料之保密及利用設有規範，且依條文內容**「甲方僅得於履行契約之目的範圍內，使用乙方提供之各項基本資料。非經乙方書面同意，不得為目的範圍外之利用或洩露（第 1 項）。甲方如以電腦處理前項個人基本資料，應依『電腦處理個人資料保護法』相關規定辦理（第 2 項）。」**可知，該定型化契約應記載及不得記載事項尚未依據個人資料保護法之施行予以修訂。

據此，本研究建議應可考量以下列事項作為通訊傳播事業之定型

化契約應記載及不得記載事項的規範內容：

(一) 應記載事項

1、 法定應告知事項

甲方應依個人資料保護法第 8 條規定，向乙方告知下列事項：(1)甲方名稱；(2)蒐集個資之目的；(3)蒐集個資之類別；(4)個資利用之期間、地區、對象及方式；(5)乙方依個人資料保護法第 3 條規定得行使之權利及方式；(6)乙方得自由選擇提供個人資料時，不提供將對其權益之影響。

2、 個人資料之利用

甲方僅得於履行契約給付義務或附隨義務之目的必要範圍內利用乙方因本契約而提供或產出之個人資料。甲方如欲於契約目的必要範圍外利用乙方之個人資料時，應事先告知乙方利用該資料之目的、方式（包含利用之期間、地區及對象）及乙方可表示拒絕之管道，並遵守個人資料保護法第 20 條相關規範，或以無法再識別特定當事人之方式對第三人提供去識別化之資料或將去識別化之資料公開。

(二) 不得記載事項

1、 個人資料權利之行使

不得記載乙方預先拋棄或限制下列個人資料權利之行使：(1)查詢及請求閱覽；(2)請求製給複製本；(3)

請求補充或更正；(4)請求停止蒐集、處理或利用；(5)請求刪除。

2、特定目的外利用個人資料

不得記載甲方得單方決定於契約目的之必要範圍外利用乙方之個人資料。

五、執行稽核

依前述行政檢查之管制手段，通傳會除可以制訂之個資檔案安全維護計畫管理辦法或定型化契約應記載及不得記載事項作為稽核依據之外，亦可先行參考下列不同密度之稽核方式執行行政檢查。

(一) 執行方式

1. 低度執行

要求通訊傳播業者自行提出說明，告知目前如何利用用戶之個人資料（尤其針對目的外利用或加值服務），以及採取如何之管理上或技術上措施以保障用戶權利。

2. 中度執行

以調查表要求通訊傳播業者針對如何利用用戶資料的現狀作出說明，由主管機關依其說明內容檢視是否與該業者向用戶揭露之「個人資料蒐集告知」或「隱私權政策」等聲明相符。本研究團隊試擬調查表內容如下：

表 9 通訊傳播事業利用用戶資料方式調查表

通訊傳播事業利用用戶資料方式調查表		
項次	內容	業者說明
(1)	公司有無或擬將不同管道來源取得之同一用戶個資（例如同一用戶分別申請手機門號租用、行動上網及室內寬頻，而可取得其基本資料、帳單明細、位置資訊、網路行為等）彙整併入資料庫？	
(2)	公司有無或擬將利用用戶之各項個資針對該用戶進行分析以描繪其輪廓屬性（Profiling）？	
(3)	承上，如有，公司有無或擬將利用個別用戶之屬性採取特定行為（例如精準行銷）？	
(4)	公司有無或擬將利用多數用戶之各項個資進行分析以產出不含可識別個別用戶之統計分析結果？	
(5)	承上，如有，公司有無或擬將該不含可識別個別用戶之統計分析結果提供予第三人？	
(6)	公司有無或擬將提供第三人「可識別個別用戶」之用戶個資？	
(7)	公司有無或擬將接受第三人給予條件（例如居住台北市內湖區的 30-40 歲男性最常瀏覽的網頁或收視喜好，或特定	

	時間出沒於特定場所之消費者性別比例與年齡層），再依該條件於資料庫中篩選，並提供不含可識別個別用戶之統計分析結果提供予該第三人？	
(8)	公司有無或擬將接受第三人給予條件（例如居住台北市內湖區的 30-40 歲男性最常瀏覽的網頁或收視喜好，或特定時間出沒於特定場所之消費者性別比例與年齡層），再依該條件於資料庫中篩選出特定用戶，並對用戶行銷該第三人之商品或服務（例如帳單夾寄廣告或簡訊廣告投遞）？	
(9)	公司有無或擬將接受第三人提供特定消費者之條件（例如行動電話號碼、地址），由公司以該條件於資料庫中比對，再將對應用戶的個資（包含公司對該用戶之分析）提供予該第三人。	
(10)	用戶可否拒絕公司彙整其各項資料以描繪屬性（Profiling）？	
(11)	用戶可否拒絕公司利用其資料加值運用，包含拒絕公司以去識別化方式統計分析？	

（表來源：本研究自行整理）

3. 高度執行

將上述調查表轉為稽核項目表，由主管機關執行實地稽核。

六、發布行政函釋

如前述行政指導之管制手段，通傳會亦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，主動或被動針對關鍵議題公開解釋，以行政函釋向通訊傳播事業說明正確適用法律的因應作為與具體措施。以下以我國政府目前大力推廣之個人資料去識別化措施為例，提出行政指導的參考。

(一) 去識別化

以我國政府目前致力推廣的「個人資料去識別化」為例，即可參考前述法務部的見解作為去識別化的判斷標準。研究團隊嘗試將不同需求情境下的個資去識別化可行方式整理如下：

表 10 去識別化情境示例

利用方式	需求條件	去識別化方式	情境示例
群體分析	不需要區分個別當事人，僅需知悉統計數據或趨勢。	以聚合資訊方式呈現	將符合一定條件下的多數當事人以聚合方式呈現資訊。 例：20-30 歲使用行動上網服務之男性於假日白天多於台北市信義區活動。

<table>
<tr>
<td>個別分析</td>
<td>有區分個別資料當事人的必要，不適合聚集資訊，且注重各欄位資訊的精確。</td>
<td>識別符置換（擬匿名化）加密、索引</td>
<td>業者欲針對個別行動電話號碼持有人在特定時間的位置軌跡進行足跡分析。
原始欄位
<table>
<tr><td>號碼</td><td>時間</td><td>位置</td></tr>
<tr><td>0912345678</td><td>105.1.1</td><td>台北車站</td></tr>
</table>
識別符置換後欄位
<table>
<tr><td>號碼</td><td>時間</td><td>位置</td></tr>
<tr><td>ASDF543</td><td>105.1.1</td><td>台北車站</td></tr>
</table>
</td>
</tr>
<tr>
<td>個別分析</td>
<td>有區分個別資料當事人的必要，不適合聚集資訊，但不強調各欄位資訊的精確。</td>
<td>識別符置換＋模糊資料</td>
<td>業者透過機上盒分析個別年齡收視戶對特定節目的停駐時間
原始欄位
<table>
<tr><td>機上盒號碼</td><td>生日</td><td>觀賞時間</td></tr>
<tr><td>S12345</td><td>60.2.2</td><td>20 分鐘</td></tr>
</table>
識別符置換+資料模糊後欄位
<table>
<tr><td>機上盒號碼</td><td>年齡</td><td>觀賞時間</td></tr>
<tr><td>2T5DS41</td><td>40-50</td><td>20 分鐘</td></tr>
</table>
</td>
</tr>
</table>

（表來源：本研究自行整理）

雖然我國政府刻正推動 CNS29191 之個人資料去識別化國家標準，然該標準並非法律要求，且即便業者通過認證，亦不必然代表在實際情形中確實將個人資料去識別化，仍應就事實予以檢視，如再考量取得驗證所需花費之成本，該認證在推廣上或將缺少誘因。

是以本研究認為，除通傳會搭配獎勵措施作為輔導或鼓勵通訊傳播業者取得認證，並逐步形成同業共識以成為市場自律機制之外，通傳會初步應將重點置於宣導去識別化之合理措施，並稽核業者是否確實以去識別化方式利用用戶之個人資料。

第三節　長期建議（法律修正）

一、修訂法律以符合通訊傳播事業之個資保護管制

我國現行法律缺少對於通訊傳播事業所涉及特殊個資類別（例如通信資訊、位置資訊）之個別定義與利用規範，以及缺少當事人請求資料可攜之權利已如前述，據此，長期目標應可考量推動個人資料保護法的修訂，或針對通訊傳播事業的個資保護事項制定專法，內容可包含：

(一) 強化資料蒐集者的告知義務與行為規範（專法）

如前揭章節所述，加強保障當事人對其個人資料的控制權將為國際上因應大數據與智慧聯網技術發展的規範趨勢，而當事人控制權的保障前提在於要求資料蒐集者提高其資訊透明度，亦即強化執行現行個人資料保護法對資料蒐集者應踐行之告知義務的要求。

據此，通傳會即可於專法中區分各項資料類別（例如基本資料、通信資訊、位置資訊、瀏覽紀錄、帳單明細、收視紀錄等），並分列業者利用不同類別資料的行為規範，同時要求通訊傳播事業於事前明確向使用者告知：

１、 蒐集各種個人資料之類別。

2、各種個人資料類別對應之目的與利用方式、提供對象（例如作為大數據分析以優化服務或對第三人提供分析報告等）。

3、明確向使用者告知其拒絕、退出資料分析之權利及行使方式。

(二) 以提高當事人控制權取代當事人同意

強化保障當事人控制權成為國際間因應大數據與智慧聯網技術發展的規範趨勢，以此彰顯資料當事人作為資料主體的地位，並可依其意願形塑其經資料分析後產出的屬性輪廓，避免大數據分析造成的偏頗或不利益。

是以通傳會應可在個人資料保護法第 3 條賦予資料當事人「請求停止利用」及「請求刪除」等權利之基礎下，推動個人資料保護法的修正，或於專法中規範業者尊重使用者「選擇退出（Opt-out）」的權利以及「被遺忘權」並建立行使權利之機制，讓使用者得以不具理由、不附條件、自由且便利的執行其權利，甚至讓使用者可單獨要求業者（暫時）停止利用或刪除某特定類別（例如某時段的位置資訊或瀏覽紀錄）之個人資料作為大數據分析之標的。

(三) 以不可識別之方式保存資料，取代刪除

考量前述用戶各項資料之「分析應用之價值」，以及「資料庫內的用戶資料無法完全刪除，否則將造成系統運作障礙」之事由，應可考量於個人資料保護法或專法中規範業者在蒐集個資之特定目的消失或期限屆滿後，以「**在合理範圍內以**

無法再識別特定當事人之去識別化方式保存資料」代替嚴格的刪除個資規範。

(四) 強化蒐集者責任

1、隱私保護內植設計、隱私保護預設及資安預設

參酌前揭章節所述之國際實務建議，於個人資料保護法或專法中可要求業者將隱私保護內植設計（Privacy by Design）、隱私保護預設（Privacy by Default）及資訊安全預設（Security by Default）等觀念納入其產品及服務當中，即讓使用者的隱私與資料安全保障成為預設值（default），由使用者自行選擇是否退讓其資料隱私或安全保護以換取進階服務或功能。

2、事先執行隱私衝擊評估

於個人資料保護法或專法中亦可規定業者應於推出以智慧聯網技術取得使用者個人資料或涉及將使用者資料進行大數據分析之產品或服務前，先予執行隱私衝擊評估，且該評估應包含法律面及技術面之項目，以此同時確保該產品或服務的適法性與安全性。

3、強化可責性

依個人資料保護法施行細則第12條第2項第9款、第 10 款規定，資料蒐集者對於個人資料檔案所須採取的適當之安全措施可包含「資料安全稽核機制」與「使用紀錄、軌跡資料及證據保存」。

是以即可於個人資料保護法或專法中據以參考，明確要求業者強化其「可責性」，具體落實安全稽核與資料紀錄（例如存取 log），以求降低使用者個人資料遭受濫用或其他侵害的風險，並確保個資事故發生的可追溯性（Traceability）。

4、納入國際標準規範

國際上不乏針對個資與隱私保護或資訊安全等技術面與管理面制度制定的標準，例如針對資訊安全管理系統的 ISO 27001、針對個資保護的 ISO 29100、針對個資管理系統的 BS 10012，乃至於近年的雲端個資保護 ISO 27018 與雲端安全 ISO 27017、ITU 於 2015 年 11 月針對大數據下的雲端運算頒布之 Y.3600 ITU-T 等標準。是以於個人資料保護法或專法中亦可考慮將各項國際標準的條文內涵納入，以此作為對業者蒐集、處理、利用與保護使用者資料的具體規範。

二、成立隱私與個資保護的專責主管機關

我國現行以法務部為個人資料保護法的主管機關，但在該法中將個別事業的監督權限交由各中央目的事業主管機關負責，造成各事業對於相同的個資與隱私保護爭議恐有適用原則相異的潛在風險。

由於大數據與智慧聯網發展帶來的個資與隱私保護議題將不只衝擊通訊傳播事業，因此如為在法規解釋與適用上有一致性之標準，長遠之計應可參考如英、德、加、澳、紐等國，乃至於鄰近國家如香港、澳門、新加坡等，設立個資或隱私保護的專責機關，給予獨立的

編制、人員及經費，始能有足夠的人員及資源負責處理全國各事業涉及個資或隱私保護有關的法規事項。

三、推廣個資第三方資料庫的發展

在「與當事人共享資料利益」的趨勢下，尊重當事人控制其個人資料的權利將越顯重要，尤其對通訊傳播事業而言，其蒐集、保有大量多樣性來源的使用者個人資料作為分析依據，實應讓使用者有更強的制衡以促使業者落實個資與隱私保護。

為使該權利能有效執行，我國應可考量於商業市場中推廣「個資第三方資料庫」的發展，該機制可提高通訊傳播使用者對其資料的控制，搭配資料可攜的要求，使用者不僅可透過攜出其個資以儲存於第三方資料庫中，藉此完善其個人資料內容，並可進一步自由選擇服務提供者並交付其個人資料，而無須擔心其個資遭原服務提供者「綁架」，更可藉此達到「以市場篩選未能滿足使用者對於個資或隱私保護之期待」的通訊傳播事業之淘汰功能。

第九章 參考文獻

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

林素鳳，〈日本現行個人資訊保護法制初探〉，《警大法學論集》，第十期，2005 年，頁 46。

研究報告

1. 交通部電信總局，《電信資訊傳播協調工作小組出國考察》，90 年 5 月 26 日。
2. 李寧修，《德國資訊監察制度之研究─兼論運用在我國之可行性》，科技部補助專題研究計畫成果報告期末報告，2014 年 10 月 31 日。
3. 范姜真嫩，《我國電信業及電信加值網路業個人資料保護與監管機制之研究》，國家發展委員會編印，2015 年 4 月。
4. 廖雪君，《以英國通訊傳播法之研訂及推動為典範，研究我國匯流法制定與推動之可行方向》，104 年公務人員出國專題研究報告書，2015 年 11 月 25 日。
5. 劉孔中，《美、英、德、新獨立機關之研究》，行政院研究發展考核委員會委託研究，2009 年 4 月。

6. 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》，105 年 1 月 22 日。

我國法規

1. 個人資料保護法
2. 個人資料保護法施行細則。
3. 電信法
4. 通訊保障及監察法

其他中文文獻

1. 立法院三讀通過修正「個人資料保護法」。2015 年 12 月 16 日，取自 http://www.lawbank.com.tw/news/NewsContent_print.aspx?NID=132849.00。
2. 有線多頻道平臺服務管理條例草案。20115 年 11 月 4 日版，取自 http://www.ncc.gov.tw/chinese/files/15111/8_34527_151112_1.pdf。
3. 無線廣播電視事業與頻道事業管理條例草案。2015 年 10 月 15 日版，取自 http://www.ncc.gov.tw/chinese/files/15101/8_34409_151015_2.pdf。
4. 經濟部成立網際網路零售商品之公司行號個資保護行政檢查小組，促使業者改善個資外洩。2015 年 4 月 24 日，取自

http://gcis.nat.gov.tw/main/publicContentAction.do?method=showPublic&pkGcisPublicContent=4025

5. 資通安全管理法草案。2015 年 10 月 2 日版。
6. 電子通訊傳播法草案。2015 年 10 月 21 日版，取自 http://www.ncc.gov.tw/chinese/files/15102/8_34444_151026_1.pdf 。

英文部分

研討會論文

1. IWGDPT, Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics (Skopje, 5./6. May 2014).

歐盟法規

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the

protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

英國法規

1. Communications Act 2003
2. Data Protection Act 1998
3. The Privacy and Electronic Communications (EC Directive) Regulations 2003

美國法規

1. Federal Trade Commission Act
2. Telecommunications Act of 1996
3. Consumer Privacy Bill of Rights Act Draft
4. Notice of Proposed Rulemaking on broadband internet service provider

判決

1. Federal Trade Commission v Accusearch Inc., No. 08-8003, United States Court of Appeals Tenth Circuit (June 29, 2009)

Available at http://www.ca10.uscourts.gov/opinions/08/08-8003.pdf

研究報告

1. Article 219 Data Protection Working Party, Opinion 03/2013 on the purpose limitation, April 2, 2013.
   Available at
   http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
2. Article 219 Data Protection Working Party, Opinion 15/2011 on the definition of consent, July 3, 2011
   Available
   athttp://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf
3. Article 219 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, September 16, 2013.
   Available at
   http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
4. Der Hessische Datenschutzbeauftragte, Key data protection points for the trilogue on the General Data Protection Regulation, August 14, 2015.
   Available at
   https://datenschutz-berlin.de/attachments/1137/Kernpunktepapier.EN.pdf?1440511241

5. European Commission, Privacy and Data Protection Impact Assessment Framework for RFID Applications, January 12, 2011. Available at http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
6. European Data Protection Supervisor, Meeting the challenges of big data, November 19, 2015. Available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf
7. European Economic and Social Committee, Towards a thriving data-driven economy, January 21, 2015. Available at http://toad.eesc.europa.eu/viewdoc.aspx?doc=ces/ten/ten557/en/EESC-2014-05300-00-00-AC-TRA-en.doc
8. Federal Trade Commission, internet of things, Privacy & Security in a Connected World, January, 2015. Available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
9. Fred H. Cate, Peter Cullen and Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines, March 2014. Available at

http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf

10. International Telecommunications Union, The Internet of Things, November 2005.
Available at https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf
11. President's Council of Advisors on Science and Technology, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE, May 2014.
Available at https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

其他英文文獻

1. Ankeny, Jason, AT&T rolls out multi-platform AdWorks Blueprint audience, May 22, 2013.
http://www.fiercemobileit.com/story/att-rolls-out-multi-platform-adworks-blueprint-audience-targeting-effort/2013-05-22
2. AT&T, AT&T Privacy Policy FAQ.
Available at http://www.att.com/gen/privacy-policy?pid=13692
3. AT&T, AT&T Privacy Policy.
Available at https://www.att.com/gen/privacy-policy?pid=2506
4. Edwards, Jim, AT&T Is Ending Its 'AdWorks' Mobile Experiment

And Laying Off Staff, October 11, 2013.
Available at
http://www.businessinsider.com/att-is-ending-its-adworks-mobile-experiment-and-laying-off-staff-2013-10

5. European Parliament, New EU rules on data protection put the citizen back in the driving seat, December 17, 2015.
Available at
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20151217IPR08112+0+DOC+XML+V0//EN
6. Federal Communications Commission, FCC ENFORCEMENT ADVISORY, ENFORCEMENT BUREAU GUIDANCE: BROADBAND PROVIDERS SHOULD TAKE REASONABLE, GOOD FAITH STEPS TO PROTECT CONSUMER PRIVACY, May 20, 2015.
Available at
https://apps.fcc.gov/edocs_public/attachmatch/DA-15-603A1.pdf
7. Federal Communications Commission, Verizon To Pay $7.4 Million To Settle Consumer Privacy Investigation, September 3, 2014
Available at
https://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation-0
8. Hunton & Williams LLP, FCC to Tackle Issue of Broadband Privacy, November 9, 2015.
Available at
https://www.huntonprivacyblog.com/2015/11/09/fcc-to-tackle-issue-o

f-broadband-privacy/

9. Information Commissioner's Office, Anonymisation: managing data protection risk code of practice.
   Available at https://ico.org.uk/media/1061/anonymisation-code.pdf
10. Information Commissioner's Office, Audit: a guide to ICO privacy and electronic communications regulations audits.
    Available at
    https://ico.org.uk/media/for-organisations/documents/2784/guide-to-ico-pecr-audits.pdf
11. Information Commissioner's Office, Guide to the Privacy and Electronic Communications Regulations.
    Available at
    https://ico.org.uk/media/for-organisations/guide-to-pecr-2-1.pdf
12. Information Commissioner's Office, Privacy Seals.
    Available at
    https://ico.org.uk/for-organisations/improve-your-practices/privacy-seals/
13. Laney, Doug, 3D Data Management: Controlling Data Volume, Velocity, and Variety, February 6, 2001.
    Available at
    http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf
14. Out-Law, Telefónica to sell 'insights' gleaned from anonymised mobile phone location data, October 11, 2012.
    Available at

http://www.out-law.com/en/articles/2012/october/telefonica-to-sell-insights-gleaned-from-anonymised-mobile-phone-location-data/

15. Ranking Digital Rights, 2015 Ranking Digital Rights Corporate Accountability Index.
    Available at https://rankingdigitalrights.org/index2015/
16. Rasmussen, Paul, Telefónica withdraws 'Big Data' service from German market, November 2, 2012.
    Available at
    http://www.fiercewireless.com/europe/story/telef-nicas-big-data-plans-blocked-german-regulator/2012-11-02
17. Telecompaper, German govt to limit Telefonica plans to sell customer data, November 1, 2012.
    Available at
    http://www.telecompaper.com/news/german-govt-to-limit-telefonica-plans-to-sell-customer-data--905518
18. Telefónica Dynamic Insights, Privacy.
    Available at http://dynamicinsights.telefonica.com/blog/635/privacy
19. Verizon, Privacy Policies.
    Available at http://www.verizon.com/about/privacy/policy/

德文部分

德國法規

1. Federal Data Protection Act

2. Telecommunications Act

3. Telemedia Act

4. Interstate Broadcasting Treaty

日文部分

日本法規

1. 個人情報の保護に關する法律

2. 電信事業個資保護指引

其他日文文獻

日本消費者委員會，「パーソナルデータの利活用に関する制度改正大綱」に関する意見，2014 年 7 月 15 日。
Available at http://www.cao.go.jp/consumer/iinkaikouhyou/2014/0715_iken.html

附件

附件 1：性別影響評估表

壹、計畫名稱	**通訊傳播事業個人資料保護之機制及管理模式委託研究案**		
貳、主管機關	**國家通訊傳播委員會**	**承辦機關**	**達文西個資暨高科技法律事務所**
參、計畫內容涉及領域			**勾選（可複選）**
3-1 政治、社會、國際參與領域			
3-2 勞動、經濟領域			
3-3 福利、脫貧領域			
3-4 教育、文化、科技領域			V
3-5 健康、醫療領域			
3-6 人身安全領域			
3-7 家庭、婚姻領域			
3-8 其他			
肆、問題現況評析及需求評估概述	網路與通訊科技的發展及行動裝置的普及，為通訊傳播事業帶來革命性的發展，業者不再只是被動的提供電信、廣播服務，更能主動透過網路與用戶互動、提供客製化的服務及廣告資訊。同時，用戶在使用通訊傳播業者的各項服務時，將因此提供或產出許多與用戶個人相關的資料，例如身分基本資料、通信紀錄、網頁瀏覽紀錄、位置資訊、帳單明細、收視紀錄等，在大數據及智慧聯網的技術蓬勃發展的趨勢下，「資料加值運用」以達到「資料價值最大化」已成為國際潮流，用戶的資料對於通訊傳播業者無疑具有巨大的潛在商		

	業價值。 然而，這些加值運用方式均涉及用戶對於其個人資料的「事前知情」、「事中控制」及「事後退出」等資訊隱私權、資訊自主權之憲法上基本權利，通訊傳播業者並不可漫無限制而在「服務契約」的必要範圍之外加值運用用戶資料。 本研究之目的在於參考國際上對於通訊傳播事業加值利用用戶個人資料的規範及管理方式進行分析，並提出開放個人資料加值運用的因應措施，例如要求通訊傳播業者加強事前對於用戶的個人資料蒐集、處理及利用之告知聲明（隱私權聲明）；以加強當事人的資料控制權取代當事人同意機制；建立用戶資料「去識別化」的參考標準或可行技術；要求業者設計讓用戶退出資料加值運用的機制。期從實體法律面及監管程序面借鏡國際實務作為，以此產出可供我國參酌的通訊傳播事業個人資料保護機制及管理模式。
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個人資料保護機制及管理模式，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「無涉及」之原因）	備註
	是	否	無涉及		
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：陳品安 **職稱：律師**

電話：(02)2367-0902 e-mail：pinan@davinci.idv.tw

附件 2：期中報告審查意見修正對照表

委員	審查意見	修訂情形
葉處長	1. 本研究計畫的目的是希望以通訊傳播事業為主，對於個人資料保護建立一個保護機制，而國家通訊傳播委員會又該如何管理及建置規範。因此，本研究案所稱「通訊傳播事業」所關切的並不與「網路」畫上等號，就像個人資料與網路或是大數據也不能畫上等號，彼此間有關連但不盡然相同。 2. 從本會的角度，我們最關切的是我們現在所監管的事業，跟一般的事業有差別，因為這些個人資料時時刻刻都處於流動的狀態。因此，在這樣的特性	遵示辦理。

	之下，我們要建立怎麼樣的規範？我們不是沒有工具(不缺法律，ex 電信法…)，但問題是這些工具要如何用？用在甚麼地方？我們訂得過猶不及都不好，希望透過這個研究案能進一步了解我們針對這個產業可以創造出甚麼樣的機制。	
黃副處長	1. 就報告而言，因為現在數據交換的節點很清楚，透過穿戴裝置、冰箱等上傳資料，但是未來數據交換的節點很模糊，因此本研究案短中長期的建議重點應該放在要怎麼規範。 2. 我們主要的問題不是怎麼管理，例如：「金融控股公司子公司間共同行銷管理辦法」只限	1. 遵示辦理。 2. 依委員意見修正報告之建議。 3. 參酌《大數據時代下通訊傳播領域消費者保護議題之法律研究》之內容並納入期末報告。 4. 已修訂期中報告之

	定事業間靜態個人資料的流動，但我們所監管的產業並不是這麼狹隘的靜態個人資料使用，而我國法規不足之處其實就是我們要問的部分 3. 就現行個資法的規定，現在業界有很多大數據的資訊，但是他們都不敢用，所以限制太多而沒有辦法發展大數據跟智慧聯網。就個資保護這部分的討論不應只限於電信事業，其實隨著科技發展，已經完全超過電信事業的範疇，所謂通訊傳播事業的概念並不是只有電信業者，但又還不及於網路遊戲業者，因此，現在研究的方向應該針對提供公眾通訊服務業	錯別字。

	者(ex. Skype)，就應該算是所謂的「通訊傳播」服務而受管控，未來就沒有事業的概念，只有通訊傳播服務的概念。 4. 報告中提出我國法規不足的部分與研究案所提出的建議不相搭配，應再修正。 5. 請修改錯字。	
詹委員	1. 電子通訊傳播法修正草案§21-§23 有關跨境傳輸之規定應納入報告中討論。 2. 有關去年歐盟法院認定個資跨境運輸至美國的安全港協議無效，本研究案若涉及到國際傳輸的部分應如何發展？希望納入期末報告。	1. 遵示辦理。 2. 有關電子通訊傳播法修正草案§21-§23 有關跨境傳輸之規定及安全港協議無效等將持續追蹤歐盟最新動態於期末報告中呈現。

謝委員	1. 本研究案期中報告蒐集國外文獻相當有份量，平台處有實際執行消費者申訴，前年底有訂定出電信事業及廣播電視事業訂定個人資料檔案安全維護計畫標準辦法草案，希望研究團隊將此草案納入在期末報告中，並提出建議。 2. 第二章德國及美國的資料較少，希望可以補充。 3. 請調整頁碼。 4. 第四章第四節除了提到西班牙及美國案例外，希望還有其他國家案例可以參考。 5. 請修改錯漏字。	1. 遵示辦理。 2. 針對「電信事業及廣播電視事業訂定個人資料檔案安全維護計畫標準辦法草案」之建議將於期末報告中呈現。 3. 有關外國文獻（德國及美國）及案例將於期末報告中補充。 4. 已調整期中報告頁碼。 5. 已修訂期中報告之錯漏字。
吳委員	1. 第二章結構上論述歐盟部分沒有小結。	1. 遵示辦理。 2. 已於第二章論述歐

	2. 第二章針對歐盟電子通訊隱私保護指令規定位置資訊，只要去識別化或得事先同意即可將位置資訊利用於加值服務，但第四章則提及西班牙電信商 Smart Steps 商品要推到德國，就算位置資訊去識別化後，德國認為未得同意仍不得利用於加值服務，請說明德國是否有特別規定。 3. 第七章提及以行政指導方式建立準則，請提出如何建立去識別化的判斷標準。	盟部分補上小結，詳參本文第 42 頁以下。 3. 有關「西班牙電信商 Smart Steps 商品於德國發展受限事件及相關資料」及「去識別化之判斷標準」將於期末報告中呈現。

附件 3：期末報告審查意見修正對照表

委員	審查意見	修訂情形
葉處長	1. 有關個人資料之保護，如採取行為管理模式，即可為跨業別管理，解決在數位匯流趨勢下，通訊傳播產業界線模糊之問題，然而產業特性因而模糊；而若本會基於通訊傳播事業主管機關，就通訊傳播事業重要個資事項特別立法，較能解決通訊傳播產業真正面對的問題，但受到權責限制，無法解決跨業的問題。另個資法固然賦予目的事業主管機關權責，然不能忽視個資法框架限制，本會等目的事業主管機關只能進行檢查或指定事業訂定	1. 遵示辦理。

	維護計畫，基本上是消極防弊，無法針對個別產業情形詮釋個資法之適用（例如 IP 位址是不是個資；或通訊傳播資料如何去識別化），第 27 條第 3 項之辦法也無罰則，更不具有規管個別產業效力，法務部仍為個資法主管機關，對個資法通常傾向統一解釋。 2. 研究報告之短期建議，如果是從軟法著手引導產業共識，比較可行，但效果有限；中期建議從定型化契約應記載及不得記載事項著手，是從軟法轉變為法規範值得思考的方法，也符合數位匯流以民事平等關係取代統治關係的方向，且軟法	2. 遵示辦理，列於報告第 220 頁至 222 頁。

	先行可降低消費者保護團體及學者疑慮。然而如何擬定可行條文，例如如何利用契約條文解決去識別化爭議，難度不低，可請研究團隊研提具體條文參考。 3. 長期建議專法或專章一事，恐難一步到位全盤處理多面向問題，以點到面由個別條文重點突破或較可行，也能承接短期軟法、中期契約成果。	3. 遵示辦理，綜合修正於報告第八章結論，第 215 頁至 231 頁。
黃副處長	有關結論部分其旨在對於通傳事業利用個資之改革，爰建議酌作修正如下： 4. 有關短期建議，所列(一)行政檢查及行政指導；(二)行政函釋等二項所列方法似僅為執行	遵示辦理，綜合修正於報告第八章結論，第 215 頁至 231 頁。

	方法且無具體指明針對個資保護機制或管理給予具體改良建議。 5. 為此建議，將短期建議與中期建議合併，並與長期建議整併，區分為修法及不修法二項。 6. 不修法律部分，參採美國制度，將各類資訊（包含個資等）重新歸類，再分別其特性透過訂定行政規則、定型化契約或其他行政指導等之強制或自律手段，達成保護或管理各類資訊之目的。 7. 由於個資法之框架限制，即便修正通傳法規也不能違反個資法，因此個資法如何修正以符合通傳事業所需，建請併予補	

	述。	
詹委員	1. 期末報告已針對國際傳輸部分進行增補。 2. 專家學者座談沒有本會代表參與，不能當場與各專家學者討論，甚為可惜。	遵示辦理。
謝委員	1. 在國際傳輸部分，個資法目前是原則許可，例外禁止，與本研究報告提及之各國須「充足」條件後才可傳遞恰好相反，且在目前僅限制電信事業傳遞個資到大陸地區，有無相關建議？ 2. 在通傳定型化契約中納入去識別化之規定，對業者有相當大的助益，但在消保會審查可能會引起相當討論。	1. 遵示辦理，增補於報告第 217 頁至 218 頁。 2. 遵示辦理。

	3. CNS29191 標章對業者無助益，可能需有更有效方式推動，有無建議？ 4. 第 36 頁第一段倒數第 2 行「事宜」應為「適宜」。 5. 第 38 頁日本指引部分請摘錄重點，另全文列為附件。	3. 遵示辦理，增補於報告第 226 至 227 頁。 4. 遵示辦理。 5. 遵示辦理，請參見附件 4。
吳委員	1. 希望未來可再跟邱文聰老師討論，就行為面來規管應是未來方向，亦為大數據發展應強化的重心。 2. 有關國際傳輸部分，仍待法務部對此議題表示意見。	遵示辦理。

附件 4：日本電信事業個資保護指引（2015）

電信事業個資保護指引	
第一章總則	
第一條	鑑於個人資料之使用層面隨著電信事業之公共性及高度資訊通訊社會發展而明顯擴大，為保護使用者之權益並提升電信服務之便利性，本指導方針爰就屬於通訊秘密之事項及其他適當處理個人資料之事宜，明定電信事業應遵守之基本事項。
第二條	除個人資料保護法（2003 年法律第 57 號）第 2 條之用詞定義外，本指導方針使用之名詞定義如下： 一、電信事業經營者：指經營電信事業（(1984 年法律第 86 號）第 2 條第 4 款規定之電信事業）者。 二、電信服務：由電信事業經營者提供之電信服務（電信事業法第 2 條第 3 款規定之電信服務）及其附隨之服務。 三、使用者：使用電信服務之人。 四、用戶：與電信事業經營者簽訂契約以享有電信服務之人。
第三條	本指導方針係就適當處理個人資料事宜，明定電信事業經營者應遵守之基本事項，及應遵行事項之解釋與運用。 電信事業經營者除遵守個人資料保護法之規定，以及涉及通訊秘密之電信事業法第 4 條與其他相關規定外，亦須遵示本指導方針適當處理個人資料。

	電信事業經營者針對第 3 章規定之各種資料，除遵守第 2 章規定之個人資料處理共通原則外，尚須遵示第 3 章規定予以適當處理。
第二章個人資料處理之共通原則	
第四條	電信事業經營者取得個人資料，須以提供電信服務之必要時為限。 電信事業經營者不得取得下列各款個人資料。但為保護自身或第三人之權利而有必要，或其他一般交易觀念認為適當之情形，不在此限： 一、有關思想、信仰及宗教相關事項。 二、人種、出身背景、身體與精神障礙、犯罪前科、病歷及其他恐引發社會歧視之事項。
第五條	電信事業經營者處理個人資料時，須儘可能限縮其使用目的（以下稱「使用目的」）。 電信事業經營者變更使用目的時，不得逾越經認定與變更前使用目的之間具有一定關連性之合理範圍。 依前二項規定而限縮之使用目的，不得逾越提供電信服務之必要範圍。
第六條	電信事業經營者處理個人資料時，不得未經當事人事前同意下，逾越前條達成特定使用目的之必要範圍。 電信事業經營者因合併及其他事由而繼受其他電信事業經營者之業務，進而取得個人資料時，電信事業經營者使用前揭個人資料時，不得未經當事人事前同意而逾越達成使用目的之必要範圍。 下列情形不適用前二項規定：

	一、有法令為依據時。 二、為保護人之生命、身體或財產，且難以取得當事人同意時。 三、基於提升公共衛生且或兒童健全成長而有特殊必要，且難以取得當事人同意時。 四、需配合國家、地方政府或前兩者之受託人執行法令規定事務，而取得當事人同意恐妨礙前揭事務之執行時。 如有前項各款規定之情形，除經使用者同意或有其他阻卻違法事由外，電信事業經營者仍不得逾越前條達成使用目的所必要之範圍，處理涉及通訊秘密之個人資料，不受前項規定之拘束。
第七條	電信事業經營者不得以虛偽不實或其他不法手段取得個人資料。
第八條	電信事業經營者已取得個人資料時，除已事先公布其使用目的外，須儘速將使用目的通知當事人，或將使用目的公告週知。 電信事業經營者因與當事人之間簽訂契約而取得契約或其他文件（含電磁形式及其他無法從人類感官辨識之方式所製成之紀錄。以下於本項同之。）所記載之當事人個人資料，或取得由當事人直接記載於書面之個人資料時，須事先向當事人明示其使用目的，不受前項規定之拘束。但為保護人之生命、身體或財產而有緊急必要時，不在此限。 電信事業經營者已變更使用目的時，須將變更後之使

	用目的告知當事人或公告週知。 下列情形不適用前三項規定： 一、將使用目的通知本人或公告週知將有危害當事人或第三人之生命、身體、財產及其他權益之虞。 二、通知當事人使用其個人資料之目的或將使用目的公告週知，恐將危害該電信事業經營者之權利或正當利益。 三、需配合國家、地方政府或前兩者之受託人執行法令規定事務，而取得當事人同意恐妨礙前揭事務之執行時。 四、從取得個人資料之情形觀之，足已認定個人資料之使用目的既已明確。
第九條	電信事業經營者須在達成使用目的之必要範圍內，盡力維護個人資料之正確性以及最新內容。
第十條	電信事業經營者處理個人資料時，原則上須在使用目的之必要範圍內定出保存期間，在保存期間屆至後或達成使用目的後，須即刻刪除該個人資料。 電信事業經營者經認定符合下列各款情形之一時，得允許其無須在保存期間屆至後或使用目的達成後刪去該個人資料： 一、根據法令規定應保存個人資料時。 二、經當事人同意。 三、電信事業經營者在執行本身業務之必要限度內保存個人資料，並有相當理由無須刪除該個人資料。 四、除前三款規定外，尚有特殊事由無須刪除該個人

	資料。
第十一條	電信事業經營者須採行必要且適當之措施，以管理對個人資料之存取，限制攜出個人資料之方式，並防止來自外部之不法存取，同時避免個人資料外洩、滅失或毀損（以下稱「外洩等情形」）。 電信事業經營者採行安全管理措施時，須運用資訊通訊網路安全與信賴度標準（1987 年郵政省公告第 73 號）等規範。
第十二條	電信事業經營者命其員工（含派遣人員，以下亦同。）處理個人資料時，須對員工採行必要且適當之監督措施，以安全管理該個人資料。 電信事業經營者基於實施個人資料之安全管理措施及其他確保個人資料獲妥適處理之目的，須令員工接受必要之教育訓練。 電信事業經營者將個人資料處理作業之全部或一部委外時，須對受託人採取必要且適當之監督措施。 如有前項情形，電信事業經營者須選擇經認定可妥適處理個人資料之受託人，並在委託契約中適度約定安全管理措施、保密、轉包之條件（是否允許轉包，以及如同意轉包時則要載明如何選擇轉包對象以及對轉包對象之監督等事項）、委託契約關係消滅時如何處理個人資料、未遵守契約內容時之處理方式及其他與個人資料處理相關之事項。 從事電信事業經營者及接受電信事業經營者委託而從事與個人資料處理相關業務之人，不得將執行業務所

	知悉之個人資料內容告知他人，亦不得用於不法目的。其離職後亦同。
第十三條	電信事業經營者須設置個人資料保護管理人（該電信事業經營者下設個人資料處理之負責人），由其擬定遵循本指導方針所需之內規，建立稽核機制並監督該電信事業經營者處理之個人資料。
第十四條	電信事業經營者須公布其隱私權政策（該電信事業經營者推動個人資料保護所秉持之精神與原則），同時遵守其所公布之隱私權政策。
第十五條	除有下列各款情形之一，電信事業經營者不得未經當事人之事前同意，而將個人資料提供給他人： 一、有法令為依據時。 二、為保護人之生命、身體或財產，且難以取得當事人同意時。 三、基於提升公共衛生且或兒童健全成長而有特殊必要，且難以取得當事人同意時。 四、需配合國家、地方政府或前兩者之受託人執行法令規定事務，而取得當事人同意恐妨礙前揭事務之執行時。 電信事業經營者依當事人之請求，停止將得識別當事人之個人資料提供給他人時，如有下列事項，得事先通知當事人或方便當事人知悉之狀態下，將該個人資料提供給他人，不受前項規定之拘束： 一、電信事業為達成使用目的而在必要範圍內，將個人資料之全部或一部委外處理。

	二、因合併及其他事由而繼受業務，因而取得個人資料。 三、個人資料係由特定人間共用時，已事先將此情況及共用之個人資料項目、共用個人資料之人之範圍、使用個人資料者之使用目的及負責管理該個人資料者之姓名或名稱，告知當事人或方便當事人知悉。 電信事業經營者變更前項第三款規定之使用個人資料者之使用目的或負責管理該個人資料者之姓名或名稱，告知當事人或方便當事人知悉。 電信事業經營者將個人資料提供給他人時，須遵守涉及保障通訊秘密之電信事業法及其他相關規定。
第十六條	電信事業經營者於處理個人資料時，須將下列事項置於當事人可得知悉之狀態（含即刻回覆當事人之請求。）： 一、電信事業經營者之姓名或名稱。 二、所有個人資料之使用目的（除符合第八條第四項第一款至第三款之情形外） 三、符合下一項或下一條第一項或第三項規定要求之程序（依第二十條第二項規定明定手續費時，含該手續費金額。） 四、電信事業受理個人資料處理相關客訴之窗口。 五、電信事業為經認可之個人資料保護團體（依個人資料保護法第 37 條第 1 項規定獲得認可之組織，以下亦同）列管之業者時，則須標示該個人資料

	保護團體之名稱及受理客訴之窗口。 電信事業經營者接獲當事人要求告知使用足以識別其個人之個人資料之目的時，須即刻告知。但有下列各款情形之一時，不在此限： 一、依前項規定，使用足以辨識人別之個人資料其使用目的已明確時。 二、符合第八條第一款至第三款規定。 電信事業經營者依前項規定，決定不將個人資料之使用目的通知當事人時，須立即將此決定告知該當事人。
第十七條	電信事業經營者接獲當事人要求揭示識別其個人之個人資料（當識別該當事人之個人資料不存在時，告知不存在亦含在其中。以下亦同）時，須儘速以書面（請求揭示資料之當事人另同意使用其他方法時，則使用該方法）揭示該當事人之個人資料。但因揭示個人資料而有下列各款情形之一時，得不予揭示該當事人之個人資料之一部或全部： 一、對本人或第三人之生命、身體、財產及其他權益有危害之虞時。 二、對該電信事業執行業務有危害之虞時。 三、違反其他法令時。 電信事業經營者依前項規定決定不予揭示個人資料之全部或一部時，須儘速將此決定告知當事人。 電信事業接獲當事人要求更正其個人資料時（指更正、追加、刪除、停止使用或停止提供給他人。以下亦同。）時，須儘速進行調查。此時若認定前述要求

	涉及之個人資料內容不屬實、已逾保存期間或該個人資料處理不適切時，須儘速更正。 電信事業經營者根據前揭規定更正系爭個人資料內容之全部或一部，或決定不予更正時，須儘速通知該當事人（含更正個人資料時，通知更正內容。）。
第十八條	電信事業經營者依第十六條第三項或前條第二項或第四項規定，通知當事人不採行其所要求之措施全部或一部時，須盡力向當事人說明決定之理由。
第十九條	電信事業經營者對於依第十六條第二項、第十七條第一項或第三項規定之請求（在以下各條稱為「揭示等請求」)，得明定下列各款事項，做為受理請求之方式。此時，當事人須依電信事業經營者規定之方式提出揭示等請求： 一、受理揭示等請求之窗口。 二、提出請求時應提交之文件（含電磁方式或其他人類感官無法辨識之方法所製成之紀錄。）規格及其他提出揭示等請求之方式。 三、確認提出揭示等請求者為當事人本人或第三項規定之代理人之方式。 四、次條第一項手續費之收取方式。 電信事業經營者得要求當事人提供足以識別其要求之個人資料之事項。此時，電信事業經營者得提供足以特定該當事人之個人資料或其他考量當事人便利之適當措施，讓當事人能提出簡單又明確之請求。 揭示等請求可由下列代理人提出。但第十七條第一項

	規定請求揭示係由無當事人具體委任之代理人提出，將侵害當事人之通訊秘密而符合該條項各款情形之一時，不在此限： 一、未成年人或受監護宣告之成年人之法定代理人。 二、受當事人委任提出揭示等請求之代理人。 電信事業經營者明定處理前三項之揭示等請求之程序時，須避免課予當事人過大之負擔。
第二十條	電信事業經營者依第十六條第二項規定通知使用目的，或接獲第十七條第二項規定之揭示請求時，得收取相關手續費。 電信事業經營者依前項規定收取手續費時，須依實際支出費用在足認合理範圍內決定手續費金額。
第二十一條	電信事業經營者須迅速並適當處理使用、提供、揭示或更正個人資料等行為所引發之客訴及其他處理個人資料引發之客訴。 電信事業經營者須建立處理前揭目的所需之機制。
第二十二條	電信事業經營者於個人資料外洩時，須儘速將外洩情況通知相關當事人。但該個人資料之外洩原因為筆記型電腦遺失或遭竊，但已採行避免對當事人造成二次傷害之適當技術防護措施時，不在此限。 電信事業經營者於個人資料外洩時，須從防止二次傷害、避免類似事件再次發生等觀點，防範與外洩相關之事實與其他二次傷害發生，並公布有助於避免類似事件發生之資訊。但該個人資料之外洩原因為筆記型電腦遺失或遭竊，但已採行避免對當事人造成二次傷

	害之適當技術防護措施時，不在此限。 電信事業經營者於個人資料外洩時，須立即將外洩相關事態向總務省報告。但該個人資料之外洩原因為筆記型電腦遺失或遭竊，但已採行避免對當事人造成二次傷害之適當技術防護措施時，得改在一季過後儘速向總務省報告上一季發生之個人資料外洩相關事態。
第三章各種資料之處理	
第二十三條	電信事業經營者得記錄通信紀錄（使用者使用電信服務之日期時間、該通信之受信方及其他非屬通信內容而涉及該使用者通信之資訊，以下亦同。）但限用於收費、請款、處理客訴、防止非法使用及其他執行業務之必要範圍。 電信事業經營者除經使用者同意、根據法官核發之令狀、符合正當防衛或緊急避難之情形及其他有阻卻違法事由之情形外，不得提供通信紀錄給第三人。
第二十四條	電信事業經營者記載於使用明細（記載使用者使用電信服務之日期時間、該通信之受信方、對應之收費資訊及其他使用者使用電信服務相關資訊之書面。以下亦同。）之範圍，不得逾越達成使用明細目的所需之必要限度。 電信事業將使用明細交付或供用戶或其他可得閱覽者閱覽時，須採行必要措施以防止使用者之通訊秘密及個人資料不受不法侵害。
第二十五條	電信事業經營者提供發信方資訊通知服務（將顯示發信方電話號碼、發信方所在位置等有關發信方之資

	訊，以電話通知受信方，簡稱「發信方資訊」，以下亦同）時，須在每次通信設定阻止發送發信方資訊通知之功能。 電信事業經營者提供發信方資訊通知服務時，須採行保障發信方權利所需之措施。 電信事業經營者除需提供發信方資訊通知服務及其他服務外，不得將發信方資訊提供給他人。但經使用者同意、根據法官核發之令狀、出現使用電話為強暴脅迫行為之現行犯而應受害人及搜索機關之請求進行反向偵測時、接獲緊急通報表示發生危害人之生命、身體等危險時應通報者之請求進行反向偵測時，或有其他阻卻違法事由時，不在此限。
第二十六條	電信事業經營者除經使用者同意、根據法官核發之令狀或有其他阻卻違法事由外，不得將定位資訊（顯示行動終端設備持有者之資訊，而非發信方資訊。以下亦同。）提供給他人。 電信事業經營者將定位資訊提供給用戶或用戶指示之人，抑或被要求提供給第三人時，須採行必要措施避免使用者權利受到不法侵害。 電信事業經營者接獲搜索機關之請求，要求提供定位資訊時，須有法官核發之令狀為憑，始得取得定位資訊，不受第四條之限制。 除前項規定外，電信事業經營者接獲執行搜救之警察、海上保安廳、消防機關或其他類似機關之請求，要求提供搜救對象之定位資訊時，須在重大危及救助

	對象之生命或身體且定位資訊是儘早發現搜救對象所不可或缺之資料時，始得取得該定位資訊。
第二十七條	電信事業經營者為防範不繳電信服務費用或非法使用行動語音通訊服務而有特殊必要並經認定為適當時，得與其他電信事業經營者交換欠費者資訊（不論是否逾越繳費日期，舉凡 2005 年法律第 31 號防止欠繳電信服務資費及非法使用行動語音通訊服務法第九條規定之未回應用戶確認者之姓名、住址、欠費金額、電話號碼或其他相關資訊皆屬欠費者資訊，以下亦同。)。但經認定恐不當侵害用於交換之欠費者資訊當事人之權益時，不在此限。 電信事業經營者與其他電信事業經營者交換欠費者資訊時，須事先將交換資訊事宜、交換之資訊項目、交換之電信事業範圍及負責管理供交換之欠費者資訊之人員姓名或名稱通知當事人，或便於當事人知悉。 電信事業經營者變更前項負責管理交換資訊之人員時，須事先通知當事人，或便於當事人知悉。 已交換欠費者資訊之電信事業經營者不得將該資訊用於申辦服務審核以外之用途。 提供欠費者資訊或接獲欠費者資訊之電信事業經營者，須充分管理該欠費者資訊。
第二十八條	電信事業經營者為暫時避免多數人遭遇收發電子郵件之障礙，於必要時得適度與其他電信事業經營者交換用戶資訊（違反 2002 年法律第 26 號濫發電子郵件管理法之電子郵件發送行為，或發送電子郵件而有妨礙

	收發電子郵件之虞時，電信事業經營者得以此為由採取停止提供電信服務之措施或解約，並將被停用或解約之用戶姓名、地址及其他相關資訊與其他電信事業經營者交換，以下亦同。)。但經認定恐不當侵害被解約或被停用之當事人權益時，不在此限。 電信事業經營者將用戶資料與其他電信事業經營者交換時，須事先將將交換資訊事宜、交換之資訊項目、交換之電信事業範圍及負責管理供交換資訊之人員姓名或名稱通知當事人，或便於當事人知悉。 電信事業經營者變更前項負責管理交換資訊之人員時，須事先通知當事人，或便於當事人知悉。 已交換用戶資訊之電信事業經營者不得將該資訊用於申辦服務審核以外之用途。 提供用戶資訊或接獲用戶資訊之電信事業經營者，須充分管理該用戶資訊。
第二十九條	電信事業經營者使用電話號碼資訊（電信事業經營者與使用者簽訂使用電話之契約時，所獲知之用戶姓名，或用戶希望刊登在電話簿、電話簿索引使用之名稱及相對應之電話號碼與其他有關用戶之資訊。以下亦同。）發行電話簿或提供電話號碼索引服務時，須給予用戶選擇是否刊登於電話簿或是否省略電話簿索引之機會。於用戶選擇省略索引時，應儘速將該用戶之資料從電話簿或索引服務中排除。 電信事業經營者發行電話簿或提供電話號碼索引服務時，其所提供之電話號碼資訊之範圍，不得逾越達成

	各該業務之必要限度。但經用戶同意時，不在此限。 電信事業經營者發行電話簿或提供電話號碼索引服務時，其所提供之電話號碼資訊之型態，不得不當侵害當事人之權益。 除發行電話簿或提供電話號碼索引服務外，電信事業不得對他人提供電話號碼資訊。但有下列情形，不在此限： 一、將發行電話簿或提供電話號碼索引之服務委外。 二、發行電話簿或提供給從事電話號碼索引服務者。 三、其他符合第六條第三項之情形。 電信事業經營者將電話號碼資訊提供給發行電話簿或提供電話號碼索引服務者時，須在該提供契約中載明比照前述各項規定之條款。
第四章附則	
第三十條	主管機關須根據社會情勢變動、國民觀念之變化、技術動向之變動等各種環境變化，於必要時修正本指導方針。