NDC-DSD-103-014(委託研究報告)

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

中華民國 **104** 年 **4** 月

NDC-DSD-103-014(委託研究報告)

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

受委託單位：東海大學法律學系
研究主持人：范姜副教授真媺
協同主持人：高副教授啟中
協同主持人：翁助理教授清坤
協同主持人：李助理教授寧修

國家發展委員會編印
中華民國 **104** 年 **4** 月

提要

關鍵詞：個人資料保護、專責監督機關、電信業監管機制、通訊秘密、電信法
Keywords: personal data protection, regulatory mechanism regarding telecommunications enterprise, supervisory authority, privacy of correspondence, Telecommunications Act

壹、研究緣起與背景

民國 100 年 10 月開始施行之個人資料保護法（下稱:個資法），已立法明確規範個資之蒐集、處理及利用者應遵守之要件與義務，更進一步落實個人資料之自主控制權。對提供通訊服務之業者而言，不僅應有保護使用其服務者通訊秘密之義務，關於提供電信服務所蒐集、儲存之其他個資，亦不得違反個資法之規範。

查我國電信法對電信事業雖於第 6 條、第 7 條定有保護通訊秘密，及電信服務使用者查詢通訊紀錄等規定，然其保護電信服務使用者個資之範圍、及課予電信事業之義務，顯有未符合個資法要求；且於電腦處理個人資料保護法時期所定之「電信事業及傳播業電腦處理個人資料管理辦法」,亦因個資法之施行而被廢止，我國主管機關迄今對電信事業亦未訂出最低限度之安全維護計畫標準，以上問題均使我國在電信通訊部分之個資保護法制上有嚴重缺失;因此如何彌補以上缺失，針對電信事業蒐集、處理及利用個資之特性及應特別加重義務部分，建立較高密度之規範,及完整健全電信使用者個資之保護,並確立監督電信事業遵法之機制，確實保障電信服務使用者之權益，實為我國當務之急。

貳、研究主題

一、電信加值網路業務與第二類電信事業之由來

所謂「電信加值網路業務」則係民國 85 年之前因電腦處理資料技術及網際網路逐漸商業化普及化，在傳統電信傳送語音之線纜及機房交換設備，附加電腦及相關應用系統之軟體設備，而提供資料之儲存、檢索、處理及轉存等新型態之服

務業務方興未艾，其發展帶來新的商機及市場經濟利益，為扶植其正當發展，且又因此類電信服務不須建置線路及機房等硬體設施其獨占性與公共性並不顯著，實不宜與傳統電信事業務置於相同規範下管理。基此，我國於民國 85 年之前即由交通部頒定「電信加值網路業務管理規則」，對經營電信加值網路服務之業者加以管理。此為電信加值網路業務之由來。

故，嚴格來說，第二類電信事業應以電信法及「第二類電信事業管理規則」之相關定義為準。「加值網路服務」定義上容易引起爭議，建議以「電信加值服務」為之較為清楚。

二、研究範疇

本研究計畫探究各研究國家（歐盟、德國、英國、日本、韓國以及美國）關於其蒐集、處理或利用之合法要件，如何定立、檢討電信事業應遵守之規範為何。因現今全球有關個資保護規範大至分為兩大派，一為以歐盟為首所定立之對公務機關與非公務機關全面性規範個人資料保護指令，另一則為以僅對公務機關及特定領域(如金融、教育、醫療保險等)蒐集、處理或利用個資予以立法規範之美國，而英國、德國為歐盟中之重要國家，故本研究以歐盟、德國、英國、美國為對象，另加上日本及韓國之亞洲近鄰國家，因其國情與我國接近，故立法規範方式亦應有值得參考之處。

再者，設置獨立監督機關以監督個資法之施行，已為歐洲各國建置個資法制時被要求之必要裝備 。而美國及日本亦有監督機制，我國個資法關於此部分並未有任何規定,故對電信事業有無嘗試循國外之立法例建立適用於我國之監督機制、及如何設置，亦為本研究計畫探究之範疇。

參、研究方法與步驟

本研究計畫執行期間為八個月，大致分為以下階段完成；

第一階段：蒐集文獻期間，蒐集歐盟、德國、英國、日本、韓國以及美國電信事業及電信加值網路業個人資料保護與監管機制相關法規，以及學者之相關論述。

第二個階段：撰寫及提出期中報告。

第三個階段：舉辦焦點座談、深度訪談。

第四個階段：彙整焦點座談、深度訪談之資料並進行我國與外國相關法制之比較

研究與撰寫期末報告，擬具建議。

肆、問題之發現

一、法律面

本研究團隊綜合分析電信法等法律或釋憲實務有關電信事業提供電信服務，對個人資料之蒐集、處理或利用所揭示之規範後，得有以下之發現：

(一) 法律之適用關係複雜

1、 保護客體之不一致

2、 規範位階之疑慮

3、 相關法令分散繁多

(二) 個人資料保護法之欠缺

1、資料共同利用之疑慮

2、關於個資之蒐集、處理或利用之委外〈outsourcing〉欠缺實效性規範

3、目的外利用之寬泛

4、不完備之事故通知規定

(三) 空白之領域

藉由加值網路擴展至電子郵件傳送，電子公告欄、網路電話、上網查詢資料等服務，可明確察知；但也因此使電信事業面臨新的挑戰，如惡意散播病毒郵件或垃圾郵件等，致使網路通信發生障礙甚至癱瘓，造成經營網路電信事業者損失，或濫發廣告簡訊至使電信用戶困擾等事件；而提供電信通信服務之業者依現行個資法似亦無任何條文得援用以檢閱電子郵件加以攔阻。立法院曾於 101 年 4 月審議通過二讀卻未完成立法之「濫發商業電子郵件管理條例草案」，試圖解決問題。亦足證我國有關法律對此部分之規範，顯有不足。

二、實務面

(一) 隱私政策之公告有欠完善

(二) 業務服務契約中個資蒐集告知條款有所不足

(三) 監管法令分割零碎，缺乏統一規劃

(四) 認證標章之取得有太偏重資安部分之疑慮

伍、建議

本研究團隊探討之我國問題，及在對各國相關法制作綜合分析後，試圖對我國有關電信事業對個人資料之保護及其監管機制，依其實現所需時間之長短，提出以下短期得施行、中期得施行及長期可實現之建議。

一、短期得實施之建議（主辦機關：通傳會）

(一) 統整相關法規命令與明確化秘密通訊範圍。

(二) 通訊秘密範圍之重新訂明。

(三) 檢視各大電信公司隱私政策。

(四) 業者委外處理個資之輔導。

(五) 明訂個資保護認證標章獎勵措施。

二、中期得施行之建議（共同主辦機關：通傳會、法務部）

(一)法規命令之訂立：電信事業主管機關與法律主管機關會商，參酌外國有關規範電信事業蒐集、處理或利用個資之法令，依法規命令(如:電信事業個人資料保護辦法)先將電信事業蒐集、處理或利用之個資類型化。對通信紀錄、用戶或使用者資料等之蒐集，應採事前同意之 Opt-in 制，不應採事後選擇退出之 Opt-out 制。

(二)電信法相關規定之修正:電信法第 7 條第一項所訂電信業及其服務人員應保密之「電信之有無」與「內容」之用詞，建議修正為「通信紀錄」與「通信內容」。如此亦與通訊保障暨監察法之用詞一致，亦較原「通訊之有無」之定義清楚。

目的外利用要件之明訂：提供第三人其通信服務時所取得之個資，係屬典型之目的外利用，因涉及權利、及義務規定，故建議修正電信法第 7 條，將電信事業處理其提供第三人調閱、查詢通信內容、通信紀錄及使用者資料之事，配合通

保法相關規定，明訂要件。現行之「電信事業處理有關機關查詢通信紀錄實施辦法」及「電信事業處理有關機關(構)查詢使用者資料實施辦法」，留存申請程序及費用徵收方法即可。

(三)共同利用個資之規定。

(四)名單查詢機制之建立。

三、長期得實施之建議（主辦機關：行政院人事總處；協辦機關：通傳會）

(一)電信通訊與網路通訊是否應依同一法規規範？此為國家在思考IT(InformationTechnology)產業發展策略時，必須全面考量之課題。但不問是否整合由同一法律規範，對利用者個資之保護則仍應依現行個資法採一致之標準。

(二)獨立監督機關設置之建議

基於國家長遠發展之觀點，本研究報告最終之建議，則仍以設置個資保護之獨立監督機關為最佳之選擇方向。

1、 設置專責監督機關之理由

綜觀本研究計畫所調查研究之德國、英國、日本、韓國等四國，雖可能個資執行監督機關設置層級或其組織方式及掌有職權容有不同，惟至少是設有一專責機關在負責。

(1) 法律解釋與適用上統一之必要

個資法適用範圍廣泛，為橫跨各領域包括公務機關與非公務機關、個人均受其規範之法律，所定之條文難免有概括難以理解之處，易於在適用上造成爭議；應統一由專責機關監督執行，才可避免法解釋與適用之混亂，及安全維護標準之不一致之問題，且執法成本亦較低。

(2) 公正、中立執法之必要

有一獨立於政府機關外之監督機關以中立立場，在不受政治等外力干涉下，得監督政府機關或大企業依法蒐集、處理或利用個資，讓個資法之規範落實，以保障人民權益，或得對政府保護個資之政策或相關法令之修正提出建議。

(3) 跨國合作窗口單一化之必要

設置一個監督個資法執行之專責機關，其除為 APEC 之事務外，更能代表國家參加其他國際重要之有關個資保護會議，與各國交換個資保護之最新資訊、執法經驗，並得為國家與外國進行侵害個資法事件之共同調查或司法合作執行之聯絡、談判窗口，此較之由各機關各自進行所轄事務之國際合作，將更能代表國家表達政策或意見且具有效率。

2、 組織方式

委員制之方式，遴選能代表社會各領域專家(包括業界及消費者)及法律、資訊技術之學者組成委員會負責監督個資法之施行，應較能作出公正、不偏頗之決定。

3、 獨立監督機關之職權

對監督對象機關等蒐集處理或利用個資之事務，得對政府提出有關個資保護政策、修法建議，對監督對象進行檢查及聽取報告並給予建議、命令改善，得代表國家參加國際會議，與外國商談個資法執行之合作，應為基本得行使之職權。

4、 設置獨立監督機關之缺點及在我國將面臨之困難與可能之選擇

(1) 難以了解各行業或領域個資利用之實際狀況

(2) 中央政府組織基準法之限制

我國現今設立之二級獨立機關則已有中央選舉委員會、公平交易委員會、國家通訊傳播委員會，換言之，在法律上已無再新設二級獨立機關之空間，勢必須要修改中央政府組織基準法始有可能性，而修法即可能引起各機關間權力之分配及政治上之角力，確有相當之難度。

(3) 現行可能之選擇

行政院為積極推動國家資訊通信安全政策,加速建構國家資訊通訊安全環境，提升國家競爭力，特設「國家資通安全會報」。雖依其組成方式各委員能否獨立行使職權，不受任何外力介入，尚非無疑慮。但行政院下既有此專責單位之存在，在設置獨立監督機關有困難之情形下，退而求其次，可以其為基礎，先建構公務機關個資保護施行之監督機制。亦即，增設體系，將原網際犯罪偵防體系下之個資保護及法制推動組，改為監督個資保護施行體系。

目次

提要.....I

目次.....VII

表次.....XI

第一章 前言.....1

第一節 研究緣起與背景.....1

第二節 研究主題.....2

第三節 研究方法與步驟.....6

第二章 我國個人資料保護法制與業者因應現況.....11

第一節 由基本權利保障出發之憲法層次觀察.....11

第二節 個人資料保護法概觀.....14

第三節 電信法及相關法規範.....23

第四節 我國現況.....35

第五節 小結.....42

第三章 歐盟、德國、英國、日本、韓國及美國電信事業個人資料保護法制.....49

第一節 歐盟.....49

第二節 德國.....81

第三節 英國.....109

第四節 日本..... 131
第五節 韓國..... 148
第六節 美國..... 159
第四章　電信事業監管機制之介紹..... 187
第一節 概述..... 187
第二節 德國..... 191
第三節 英國..... 202
第四節 日本.....211
第五節 韓國..... 221
第六節　美國..... 225
第七節 我國現行制度..... 233
第五章 結論與建議..... 239
第一節　法律規範面..... 239
第二節　監管機制面..... 245
第三節　實務面..... 246
第四節　外國法制之借鏡..... 249
第五節　建議..... 252
參考文獻..... 261
附錄一 第一類電信事業經營者名單暨其業務項目 276
附錄二 第二類電信業者名單及其營業項目..... 280
附錄三 第一場焦點座談紀錄..... 301
附錄四 第二場焦點座談紀錄..... 305

附錄五 第二場焦點座談會 法務部書面意見.....310
附錄六 第三場焦點座談紀錄.....312
附錄七 第四場焦點座談會紀錄.....318
附錄八 第三場焦點座談會 法務部書面意見.....322
附錄九 隱私權協會深度訪談紀錄.....327
附錄十 瑪凱電信公司深度訪談紀錄.....329
附錄十一 通傳會深度訪談紀錄.....334
附錄十二 台灣大哥大電信公司深度訪談紀錄.....338
附錄十三 資策會深度訪談紀錄.....343
附錄十四 法務部法律事務司深度訪談紀錄.....346
附錄十五 中華電信公司深度訪談紀錄.....350
附錄十六 期中審查意見回應表.....354
附錄十七 期末審查意見回應表.....360

表次

表 2-1 電信法及通保法中相關個人資料類型之界分及其運用要件……..……..46
表 3-1 歐盟個人資料保護指令(95/46/EC)……..…….77
表 3-2 歐盟個資保護基礎規則草案之相關規範……..……...78
表 3-3 歐盟電子通訊個資保護指令(2002/58/EG)特別規範……..……79
表 3-4 德國聯邦個人資料保護法……..……106
表 3-5 德國電信通訊法（TKG）……106
表 3-6 德國電子媒體法（TMG）……107
表 3-7 電信通訊法及電子媒體法之特別運用要件……..……107
表 3-8 DPA 1998 對個資之基本規範……..……129
表 3-9 2003Regulations 與 2011 Regulations 對電信個資之特別規範……130
表 3-10 一般性個資之要件……146
表 3-11 特別規定之要件……147
表 3-12 韓國有關個資蒐集、處理及利用之要件……154
表 3-13 韓國個人資料保護相關法律……155
表 3-14 美國個資要件整理……184
表 4-1 聯邦資料保護與資訊自由監察機構之組織與職權 201
表 4-2 特定個人資料保護委員會……..……220
表 4-3 韓國個人資料保護委員會之層級、組織方式及職權……..……224

第一章 前言

第一節 研究緣起與背景

憲法第 12 條規定：人民有秘密通訊之自由，其為憲法所保障之基本權利，旨在確保人民就通訊之有無、對象、方式、及內容等事項，有不受國家及其他人任意侵擾之權利。此自由權利亦為憲法保障個人隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利[1]。

民國 100 年 10 月開始施行之個人資料保護法（下稱：個資法），已立法明確規範個資之蒐集、處理及利用者應遵守之要件與義務，更進一步落實個人資料之自主控制權。對提供通訊服務之業者而言，不僅應有保護使用其服務者通訊秘密之義務，關於提供電信服務所蒐集、儲存之其他個資，亦不得違反個資法之規範。

隨近年數位科技之快速發展，與電腦網路之普及，人與人間之通信早已不限於利用纜線作一對一之雙向語音交換方式，而是以無線、衛星或其他電磁系統等傳輸文字、聲音或影像等訊息[2]；尤其智慧型手機(smart-phone)被普遍使用之今日，經常隨身攜帶、保持通信狀態之手機，不僅被用來通話、傳簡訊、瀏覽網站、操作 APP(application server)、檢索店鋪等，除通訊內容外，通信之日時、場所、種類、通話時間、網站瀏覽履歷(cookie)等之電信服務使用者各種個資(CDR：Call Detail Record(下稱個資))，提供通訊服務業者均得輕易大量蒐集、儲存，甚至在未得電信服務使用者同意下加以利用、或提供給第三人，勢必造成通訊當事人隱私權益等受損。

查我國電信法對電信事業雖於第 6 條、第 7 條訂有保護通訊秘密，及電信服務使用者查詢通訊紀錄等規定，然其保護電信服務使用者個資之範圍、及課予電信事業之義務，顯有未符合個資法要求；且於電腦處理個人資料保護法時期所定

1 參見司法院釋字第 603 號、631 號解釋理由書。
2 參見電信法第 2 條第 1 項第 2 款「電信」之定義。

之「電信事業及傳播業電腦處理個人資料管理辦法」,亦因個資法之施行而被廢止，我國主管機關迄今對電信事業亦未訂出最低限度之安全維護計畫標準，以上問題均使我國在電信通訊部分之個資保護法制上有嚴重缺失;因此如何彌補以上缺失，針對電信事業蒐集、處理及利用個資之特性及應特別加重義務部分，建立較高密度之規範,及完整健全電信使用者個資之保護,並確立監督電信事業遵法之機制，確實保障電信服務使用者之權益，實為我國當務之急。

第二節 研究主題

一、電信加值網路業務與第二類電信事業之由來

首先,電信事業之分類依我國電信法第 2 條之定義規定「電信」: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。而「電信服務」指：利用電信設備所提供之通信服務;「電信事業」,則為經營電信服務供公眾使用之事業。再電信事業依電信法第 11 條又得分為「第一類電信事業[3]」及「第二類電信事業[4]」;第一類電信事業：為設置電信機線設備，提供電信服務之事業，其事業經營者以依公司法設立之股份有限公司為限，且須經交通特許並發給執照後，始得營業。而第一類電信事業以外之電信事業通稱為第二類電信事業。第一類電信事業與第二類電信事業最大區別在於硬體設施之有無及資本額之限制；換言之，第一類電信事業者，可建設基地台、電話傳輸設備、機房等，並銷售自家門號，其所需投資資本額龐大，如中華電信、遠傳、台灣大哥大等屬之；而第二類電信事業者，則無法投資設置基地台、電話傳輸設備等硬體設備，其主要業務係向第一類電信事業者或國際電信事業者批發電話語音頻號，再轉售，如瑪凱、統一超商等。

而所謂「電信加值網路業務」則係民國 85 年之前因電腦處理資料技術及網際網路逐漸商業化普及化，在傳統電信傳送語音之線纜及機房交換設備，附加電腦及相關應用系統之軟體設備，而提供資料之儲存、檢索、處理及轉存等新型態之服務業務方興未艾，其發展帶來新的商機及市場經濟利益，為扶植其正當發展，

[3] 第一類電信事業經營者名單暨其業務項目，請參見附錄一。
[4] 第二類電信業者名單及其營業項目，請參見附錄二。

且又因此類電信服務不須建置線路及機房等硬體設施，其獨占性與公共性並不顯著，實不宜與傳統電信事業務置於相同規範下管理[5]。

基此，我國於民國 85 年之前即由交通部頒定「電信加值網路業務管理規則」，對經營電信加值網路服務之業者加以管理。此為電信加值網路業務之由來。之後，於民國 85 年 2 月交通部修正電信法將電信事業分為「第一類電信事業」及「第二類電信事業」，並將前開「電信加值網路業務管理規則」廢止，再於 86 年 2 月訂定發布「第二類電信事業管理規則」。

二、第二類電信事業之營業項目

依電信法第 17 條規定，經營第二類電信事業，應向 NCC 申請許可，經依法辦理公司或商業登記後，發給許可執照，始得營業。第二類電信事業營業項目、技術規範與審驗項目、許可之方式、條件與程序、許可執照有效期間、營運之監督與管理及其他應遵行事項之管理規則，由 NCC 訂定之。

再依「第二類電信事業管理規則」第 2 條第 4 款，其得經營之「特殊業務」為：

1、單純語音轉售服務：指經營者以租用電信事業之電路或頻寬連接公眾交換電信網路，提供國際或長途語音服務，或話務轉接服務。

2、E.164 用戶號碼網路電話服務：此為經營者利用國際電信聯合會（ITU）制定之電信號碼規格 E.164 提供網路電話服務。

3、非 E.164 用戶號碼網路電話服務：此指經營者未利用國際電信聯合會制定之電信號碼規格提供網路電話服務。

4、租用國際電路提供不特定用戶國際之電信服務或其他主管機關公告之業務項目。

應注意的是，現在流行之 Line 因其為利用網路之通訊軟體，為不帶門號之網路電話，目前仍不被認為屬於電信服務。

另外，前開管理規則同條第 9 款則訂有第二類電信事業「一般業務」之營業項目，則有批發轉售如門號、電話卡、公用電話等服務，公司內部網路通信服務，語音會議服務，網際網路接取服務，頻寬轉售服務，存轉網路服務(如傳真存轉、

[5]參閱陳銘祥，電信加值網路業務規範對策之比較研究，經社法制論叢，第 5 期，頁 266，79 年。

交易服務、數據網路服務)，存取網路服務(如電話秘書、線上資訊接取、電子布告告欄(BBS)、電子資料交換、電子文件服務、語音訊息、語音信箱服務)，視訊會議服務，數據分封交換服務，負費語音資訊服務，行動轉售服務，行動轉售及加值服務等 12 項業務。

故，嚴格來說，第二類電信事業應以電信法及「第二類電信事業管理規則」之相關定義為準。「加值網路服務」定義上容易引起爭議，建議以「電信加值服務」為之較為清楚。

再查，第一類電信事業所經營之業務為：一、電信(無線)行動業者經營之 1、語音服務(行動電話)，2、數據服務，如 sms、content、E-Mail 及數據加值服務，如定位追蹤、企業應用、國際漫遊、無線上網；二、有線(固網)業者經營之 1、網路出租業務，包括國際網路、撥接上網、ADSL、及數據網路出租，2、電話業務，包括室內電話、長途電話、國際電話、智慧加值服務，如 0800、0809 受話對方付費電話、電話投票等。

綜上，所謂「電信」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；「電信服務」係指利用電信設備所提供之通信服務。不論第一類電信事業或第二類電信事業，皆需依電信相關法規申請特許執照，以提供相關法規所規定之營業項目，並受 NCC 之監督管理。於數位匯流之環境下，各種技術與服務推陳出新，是否需要受主管機關所監管則需要持續滾動式之研議，以及相關主管機關依職權、或訂定、或修正相關法規予以認定。

三、研究範疇

上開資料大致上可再分為三種類型，一為有關第三人之資料，其二為有關使用者識別資料，及第三為有關通信服務上之行動履歷或利用狀態之資料。本研究計畫主要即以上開個資為對象，依其性質之不同，亦即是屬通訊秘密或屬單純具有特定個人識別性之個資，探究各研究國家等關於其蒐集、處理或利用上之合法要件，如何定立。

又因為國際間有關個資保護法制，大至分為兩大類型，一為「全方位式」(comprehensive)的立法（如「歐盟資料保護指令」，the EU Data Protection Directive），所有處理個資活動皆受一定的拘束，而非放任資料蒐集者恣意為之。另一為美國，

其選擇 「市場機制」模式，將個人資料的蒐集、使用或分享問題委由當事人個人與資料蒐集者雙方自行透過自由市場的機制協商，政府於必要時再輔以產業界自訂的自治、自律規範(self-regulation)。在某些特定產業的領域，個人資料遭濫用問題嚴重，形成隱私保護的危機，美國政府乃特別訂立僅適用於該特定「部門」(sector)的法令，以謀有效規範。

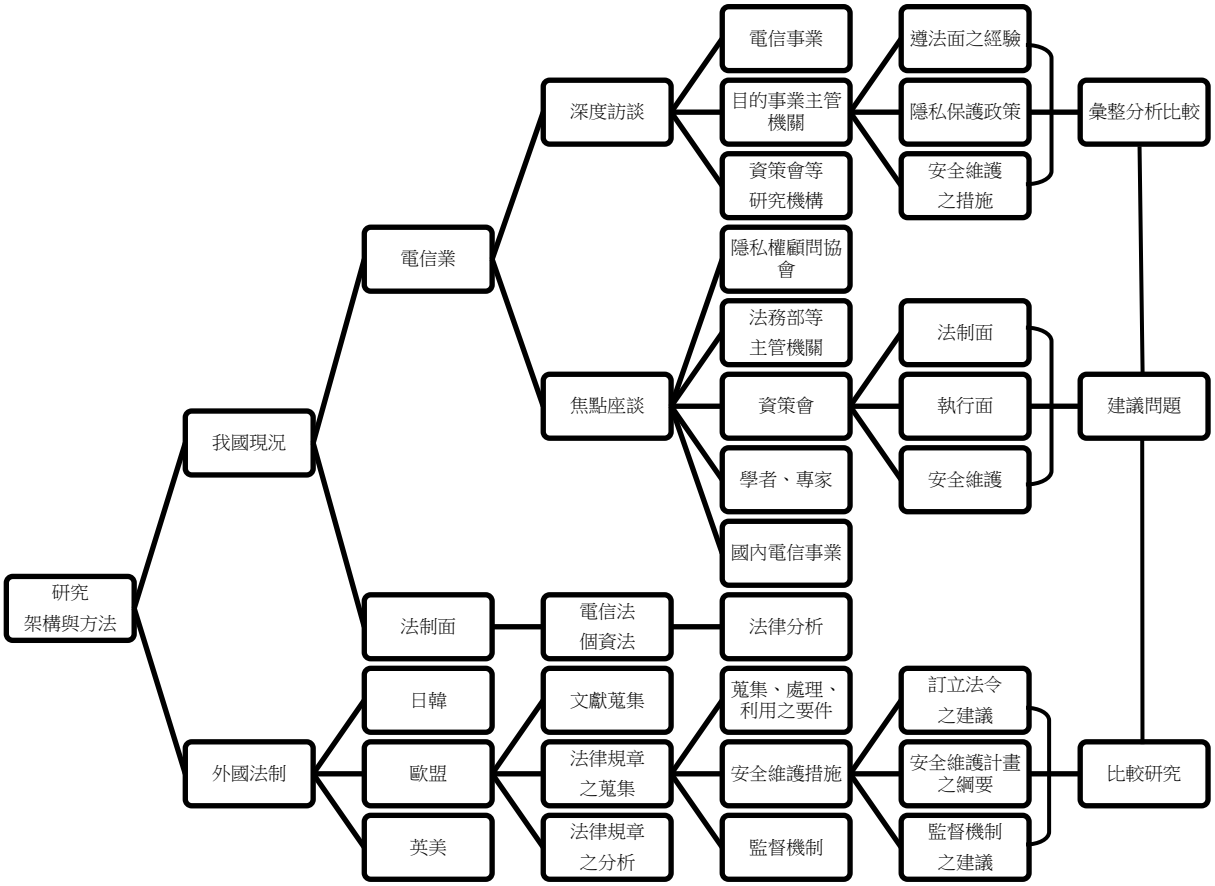
換言之，因全球有關個人資料保護規範大至分為兩大派，一為以歐盟為首所定立之對公務機關與非公務機關全面性規範個人資料保護指令，另一則為以僅對公務機關及特定領域(如金融、教育、醫療保險等)蒐集、處理或利用個資予以立法規範之美國，而英國、德國為歐盟中之重要國家，故本研究以歐盟、德國、英國、美國為對象，另加上日本及韓國之亞洲近鄰國家，因國情與我國接近，其立法規範方式應有值得參考之處。

簡言之，本研究以現行個資法所規定之法定要件，並參照歐盟、德國、英國、日本、韓國以及美國等國家所定規範，檢討電信事業者應遵守之規範為何。

再者，依我國個資法第 27 條之規定，無論公務機關或非公務機關皆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。也就是說電信事業者依前述個資法規定應建立個資檔案安全維護計畫，所以本研究亦將參酌日本、歐盟、德國等國家之立法例和該國主要電信事業者之作法，檢討我國電信事業者在維護個資檔案安全上，於軟體、硬體及人員組織面應具備之條件。

最後，查歐盟指令（Directive 95/46/EC）第 6 章第 28 條第 1 項 即規定各加盟國應定有一個以上公務機關，專責監督個資保護法制之施行；此機關行使法定職務時，應完全獨立。在歐洲理事會（Council of Europe, CoE）各加盟國協議訂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裝備 。而美國及日本亦有監督機制，我國個資法關於此部分並未有任何規定，但有無可能對電信事業嘗試循國外之立法例建立適用於我國之監督機制，亦為本研究計畫探究之範疇。

第三節 研究方法與步驟



一、研究進度及完成之工作項目

本研究計畫執行期間總計8個月，大致分為；

第一階段(1至3個月)：蒐集法規和期刊等相關文獻期間，包括歐盟、德國、英國、日本、韓國以及美國電信事業及電信加值網路業個人資料保護與監管機制相關法

規，以及學者之相關論述和司法判決。惟各國個資保護法制各有其特色，因此部分國家尚未見有指標性意義的司法判決，因此本研究在撰寫上係以該研究對象之法規和行政規範為重心。

第二個階段(1至2個月)：撰寫及提出期中報告。

第三個階段(3至4個月)：舉辦焦點座談、深度訪談。

第四個階段(2至3個月)，彙整焦點座談、深度訪談之資料並進行我國與外國相關法制之比較研究與撰寫期末報告，擬具建議。

第五個階段(1個月)，修改期末報告。

執行研究進度甘特圖

工作項目	第一個月	第二個月	第三個月	第四個月	第五個月	第六個月	第七個月	第八個月
蒐集文獻期間	■	■	■					
個資保護立法模式、監督管理機制與發展趨勢編譯		■	■	■				
撰寫期中報告				■				
舉辦焦點座談會				■	■	■	■	
進行深度訪談						■	■	
撰寫期末報告							■	■
修改期末報告								■

二、完成之工作項目

整體而言，本研究團隊召開多次小組會議進行計畫事務討論、學術意見交流，依循上開進度執行計畫。本研究已完成我國和歐盟、德國、英國、日本、韓國以及美國等國家規範電信事業者的個資保護與監督機制相關法規之蒐集與整理、分析，詳細內容請參見第二、三、四章，並在第五章說明發現之問題與提出建議。

本研究團隊人員在蒐集關於我國主要電信事業者個資保護現況的過程中，除了造訪各家電信事業者官方網站蒐集書面文獻並實際走訪店家臨櫃探詢外，已在

103 年 06 月 24 日借用文化大新館教室場地舉辦業者焦點座談會，和中華電信、遠傳、亞太、威寶[6]等業者針對下列三大主題「遵法義務之實踐」、「安全維護機制」和「監督機制之設立」之實際執行面和法制面進行交流。此外，為徵集更多學者專家對於我國電信事業及電信加值網路業之個資保護機制和個資法相關規範之意見，本研究團隊在同前述地點於 103 年 06 月 25 日舉辦學者專家焦點座談會，邀請專研憲法、電信法和個資法領域的數位學者、專家、律師和個資法主管機關法務部代表與會交流，針對「現行法規之檢討」和「監督機制之設立」等議題進行討論。十分感謝與會學者專家們，踴躍提出寶貴意見與建議讓本研究團隊獲益良多。

計畫中期依照預定執行事項進行深度訪談，可分作電信事業、主管機關以及民間機構等三部分；第一部分受訪單位為中華電信、台灣大哥大以及國內較具規模的第二類電信事業者瑪凱電信，由本研究團隊主持人偕同助理至各家公司進行訪談；第二部分則有國家通訊傳播委員會以及法務部法律事務司，由本研究團隊主持人偕同助理至各該機關訪問；第三部分依序是台灣隱私權顧問協會以及財團法人資訊工業策進會科技法律研究所科技應用法制中心，後者訪談內容係針對臺灣個人資料保護與管理制度規範(Taiwan Personal Information Protection and Administration System, TPIPAS)和核發「資料隱私保護標章」(Data Privacy Protection Mark, DP Mark)事務進行對談；共計七個受訪對象，深度訪談紀錄亦已併入報告作為附錄。

此外，本研究團隊亦嘗試研擬題目並公開放置於「公共政策大家談 粉絲頁」讓民眾上網點閱留言表達意見。事實上，本研究團隊意圖藉此舉觀察我國民眾對於電信事業個資保護與監管機制之現況的觀感和發現問題，以及透過此管道聆聽公眾提供的建議，然截至 11 月底為止皆未見有任何值得本研究團隊寫入報告並加以討論的建議，本研究團隊對此甚感遺憾。

進入計畫後期，本研究團隊再次召開兩場焦點座談會，邀請學者專家、主管機關，包含法規與目的事業主管機關，和我國第一類和第二類電信事業之代表性公司，針對「傳統電信通訊與網路通信之分與合」和「監管機制建立模式與方法

6 台灣大哥大公司因當日適逢國家通訊傳播委員會進行行政檢查而不克出席;原定與會的大眾電信公司代表因臨時有緊急事務，故而未參與。

之探討」兩大議題進行討論。有關兩場座談會之細部問題與討論，請參閱佐附作為附錄的第三場和第四場座談會紀錄，在此不予以贅述。

第二章 我國個人資料保護法制與業者因應現況

本研究主題聚焦於我國電信事業及電信加值網路業，就現行個人資料保護之相關規範與實踐進行探究，並針對監管機制之設計是否得適當發揮應有功能，提供外國法之比較觀點作為參考。以下將透過憲法（第一節）、個人資料保護法（第二節）與電信法及相關法規範（第三節）探究我國個人資料保護法制之框架，並就我國電信事業因應現況（第四節），予以介紹。

第一節 由基本權利保障出發之憲法層次觀察

個人資料保護議題之討論上，在憲法層次所涉及之基本權利應有二，即憲法第 12 條所明文列舉之秘密通訊自由；以及透過大法官相關解釋予以確證之資訊隱私權。

一、秘密通訊自由

秘密通訊自由立於憲法明文列舉之基本權利清單中，其保障基本權利主體於採取積極或消極之通訊行為及與其連動之整個通訊溝通過程中，皆享有不受國家權力干涉之自由，即「確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利」[7]。

司法院釋字第 631 號解釋理由書，其中援引司法院釋字第 603 號解釋將秘密通訊自由界定為「憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利」，隨著科技不斷進步，通訊的方式由傳統之通訊方式如郵信、電話，發展成相當多元之型態，例如近年發展之新興通訊方式 SkypeOut 與 Line；但亦促成監控技術與設備的同步精進，對人民得主張秘密通訊之空間帶來極大的威脅[8]，且此一監控的力量似乎逐漸有由作為「老大哥」

[7]參照司法院釋字第 631 號解釋文。

[8]由史諾登所揭發之「美國稜鏡計畫」與「英國皇家禮賓部」，即突顯此一合作趨勢：前者，係美國國家安全局(NSA)自 2007 年開始，所實行的電子監聽計畫，該計劃之內容，主要是針對即時通訊

的國家，拉攏「小老弟」電信事業共同合作之趨勢[9]，秘密通訊自由之保障內涵是否得隨之與時俱進，提供相應之保護水準，極具重要性。

二、資訊隱私權

秘密通訊自由保障於通訊之過程中不受干擾的權利，但就期間所產生之個人資料，卻非僅有在通訊的過程中方有其保護之必要，因此，如何勾勒出完整個人資料保護的憲法保障內涵，即有必要進一步探究資訊隱私權之概念。觀諸我國基本權利清單，雖未明文規範隱私權之類型，但隨著大法官解釋之發展[10]，大法官明確承認隱私權受憲法所保障，並闡明：「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障[11]。」隱私權在大法官解釋的脈絡下，包括兩個面向：個人生活私密空間之維護與個人資料自主控制權利之確保。資訊隱私權之保障內涵，若由權利主體-人民的角度觀察，其包括每個人對於其本身或與其本身相關之資訊，無論

之內容與既存之資料進行深度監聽，而其監聽對象包括與外國人士通訊之美國公民與在美國境外地區使用參與此計畫公司之服務客戶；後者，係依據德國明鏡周刊(Der Spiegel)之報導所指，英國政府通訊總部(GCHQ) 自 2010 年開始，為了監控外國的外交官及政府官員，設立一個自由監控系統，將全球至少三百五十間之豪華飯店的訂房系統列入目標，並輔以監控電子郵件與情報人員之分析，達到提早掌握其下榻之飯店，開始監控飯店內的電話通訊與網路。

[9]以「交通資訊服務雲基礎建設與應用計畫」與「國道行車資訊查詢系統」兩者為例，前者之內容，即是以掌握即時路況為目的，透過監視器、閉路電視、etag 紀錄、民間車隊、導航業者與手機 GPS 定位，蒐集全國高速公路、快速道路、主要省道與縣道與連絡道等路交通資訊；後者之內容，即是警政署要求遠通電收及高公局提供全天候的行車記錄。因此項行為等同可全天候監控全國所有車輛的行蹤，引發用路人反彈，故立法院經過朝野協商後，要求高公局不得提供 ETC 交通資料給警政署進行犯罪偵查。事後警政署亦表態原意僅針對犯罪車輛且尚未收取任何資料。本研究計畫所欲探討之電信事業個人資料保護亦有類似的情況，電信事業藉由大量掌握個人資料及數位資訊，能夠提高透過分析或比對，得出電信事業所需或可以轉售給其他業者之個人資料，提高人民個人資料被侵害的風險。當電信事業持有前述之資料時，若與國家或公權力機關合作，提供國家相關資料進行處理、利用，不僅可能造成個人資料之侵害，更引發導致人民基本權利侵害之疑慮。

[10]隱私權在司法院釋字第 293 號解釋中首次提及：「保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權」；大法官更在司法院釋字第 509 號與 535 號將之視為現代民主國家不可或缺之權利；續於司法院釋字第 585 號解釋理由書中確認，「基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利」，將之納入憲法第 22 條保障，從私法上的權利提升為憲法上的基本權利，司法院釋字第 603 號解釋，更將有關個人資料從隱私權中具體化為資訊隱私權，並進一步於司法院釋字第 689 號解釋中強調個人擁有資料自主權。隱私權在司法院大法官釋憲實務中之發展，詳見王勁力，新版個資法的衝擊與影響：論我國公務機關對特種個資的管控與監督，科技法律評析第 4 期，2011 年 12 月，頁 76-78。黃昭元，無指紋則無身份證？換發國民身份證與強制全民捺指紋的憲法爭議分析，收錄於民主、人權、正義：蘇俊雄教授七秩華誕祝壽論文集，國際刑法學會台灣分會編，2005 年 9 月，頁 468-469。

[11]參照司法院釋字第 603 號解釋文。

是否涉及私密資訊[12]，皆應得依其個人意志，為消極不提供或是積極公開之行為決定；對於被揭露之資訊，有權知悉並掌握其使用的歷程，即便是已獲同意並公開之資訊亦同[13]；進而，對於資料的完整與正確性，人民得要求更正或更新；若國家運用個人資料的行為致生人民損害，則應設計相應之救濟途徑[14]；國家僅得於目的範圍內利用該資料並應建置相關管道讓資訊主體得知悉資訊之使用及處理情形等。

資訊隱私權與秘密通訊自由在不同之情境下皆賦予基本權利主體掌握其個人資訊之權利；但秘密通訊自由僅及於與通訊連動相關過程中之積極或消極通訊行為，確保其不受干擾，惟隱私權之保障內涵卻無法僅以秘密通訊自由完整涵蓋，因而，仍有援引資訊隱私權作為保障個人資料基礎之必要[15]。故若由憲法基本權利保障之觀點出發，憲法第 12 條之秘密通訊自由與透過憲法第 22 條演繹出之資訊隱私權，共同構築出一憲法層次之個人資料保障體系。

惟上述基本權利之類型均非不得予以限制：針對秘密通訊自由，「國家採取限制手段時，除應有法律依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當，方符憲法保護人民秘密通訊自由之意旨」[16]；「憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第 23 條規定意旨之範圍內，

[12]司法院釋字第 603 號解釋林大法官子儀於其所提出協同意見書中，就資訊隱私權保障範圍之論述：「將資訊隱私權所欲保護之對象限於個人私密之資訊，毋寧過分限縮，而不能因應現今資訊科技發展所可能對個人造成之侵害。蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。司法院釋字第 585 號解釋亦係有鑑於此，而將個人資訊之自主控制權納入隱私權保障範圍內，不限於個人秘密不受揭露的自由。」值得贊同。同樣見解得見李惠宗，憲法要義，2009 年，元照，頁 373-374。李震山，論資訊自決權，收錄於人性尊嚴與人權保障，2011 年，頁 233-234。

[13]因此，即便是已經公開之資訊，其再次進行處理或利用，仍會涉及個人資料自主控制權之干預。相關論述詳見李惠宗，裁判書上網公開與個人資訊自決權的衝突，月旦法學雜誌第 154 期，2008 年 3 月，頁 23。司法院釋字第 603 號解釋林大法官子儀於其所提出之協同意見書，亦有相同見解。

[14]黃昭元，前揭註 10，頁 471-472。

[15]德國聯邦憲法法院指出，秘密通訊自由僅能在法律授權範圍內，就進行中之通訊活動予以基本權保護功能。蔡宗珍，憲法人格權之保障及其界限─兼論網路人格權保護之憲法挑戰，中研院法律學研究所憲法解釋理論與實務學術研討會，2013 年 6 月，頁 19。

[16]參照司法院釋字第 631 號解釋文。我國目前限制秘密通訊自由之法律，包括有關刑事目的者，有通訊保障及監察法之規定；國家安全目的者，有國家安全法之規定；行政管理目的種類甚多，以監獄行政而言，監獄行刑法第 66 條採行檢閱強制即屬一例；保障私人權益目的而言，破產法第 67 條規定，破產管理人即取得開拆權以便防止脫產，保障債權人之權益。陳新民，憲法學釋論，2008 年 9 月，三民，頁 279-282。

以法律明確規定對之予以適當之限制」[17]，故在符合法律保留原則、法律明確性原則以及比例原則之前提下，秘密通訊自由與資訊隱私權之行使乃得予以適當限制。

第二節 個人資料保護法概觀

我國個人資料保護法於 2012 年 10 月正式上路，該法以保護人格權為目的，就公務機關及非公務機關針對個人資料蒐集、處理和利用之行為予以規範，以促進個人資料之合理利用。

一、個人資料之定義

個人資料保護法將個人資料定義為：自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料[18]。而所謂間接識別方式，係指該資料須與其他資料對照、組合、連結等，始能識別該特定之個人之情況[19]，將得間接識別出特定人之資料亦列屬於個人資料之範疇，乃考量「因社會態樣複雜，有些資料雖未直接指名道姓，但一經揭露仍足以識別為某一特定人，對個人隱私仍會造成侵害」，故亦應予以相應之保障[20]。關於間接識別性之認定，近日 M+Messenger 通訊軟體案[21]中「從使用者電話號碼所識別出之電信業別是否屬個人資料」爭議，歷審判決皆肯認「如任令第三人得以任意蒐集、處理、利用自然人電話號碼所屬電信業者

[17]參照司法院釋字第 603 號解釋文。

[18]參照個人資料保護法第 2 條。就此條文之細密釋義者，如劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外─以監視錄影為例(上)，月旦法學教室第 115 期，2012 年 5 月，頁 43-49。

[19]個人資料保護法法施行細則第 3 條就所謂「間接方式識別」，乃指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。有關間接識別性之認定操作，及因科技時代進步，其所叢生問題研究，詳見郭戎晉，論數位環境下個人資料保護法制之發展與難題─以「數位足跡」之評價為核心，科技法律透析第 24 卷第 4 期，2012 年 4 月，頁 18-39。

[20]個人資料保護法第 2 條立法理由一，個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

[21]M+Messenger 通訊軟體案之歷審裁判為台北地方法院 103 年北小字第 1360 號與台北地方法院 103 年小上字第 155 號。

別之資料，藉拼湊、比對、組合、連結其他當事人之社會活動資料，據以間接識別特定自然人後，將使當事人陷於遭不當之窺探、侵擾或行銷之危險中，自與個人資料保護法之立法意旨有違。」或許提供了一判斷間接識別性之標準。

此外，個人資料保護法於第 6 條第 1 項就性質較為特殊或具敏感性之特種個人資料類型另有規範，包括有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料[22]，惟因其性質較一般性個人資料更為敏感，故該法明定，此種類型之個人資料以不得蒐集、處理或利用為原則，「避免造成社會不安或對當事人造成難以彌補之傷害」，但同時列明四種得例外情形[23]，惟其迄今尚未施行[24]。而為周延人民於上述規範尚未施行前之特種個人資料保護，法務部就蒐集、處理與利用規範原則，認「於第 6 條尚未施行前，其蒐集、處理與利用仍應適用個人資料保護法有關一般個人資料之規定」補充規定之（法務部法律字第 10100211340 號），且除「已合法公開之個人資料」得為蒐集、處理或利用外，其餘皆須於法律有明文規定時方得行之」（法務部法律字第 10100095060 與 10103103240 號），以避免立法目的落空。

特種資料在目前個人資料保護法第 6 條尚未施行之狀況下，究竟應當如何適用之，學說及實務尚有爭論。以全民健康保險資料庫案之爭議為例[25]，我國全民健

[22]個人資料保護法法施行細則第 4 條就特種個人資料有定義性之規定：「醫療之個人資料」係指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料（第 2 項）；「基因之個人資料」係指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息（第 3 項）；「性生活之個人資料」係指性取向或性慣行之個人資料（第 4 項）；「健康檢查之個人資料」係指指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料（第 5 項）；「犯罪前科之個人資料」係指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄（第 6 項）。值得注意的是在歐盟個人資料保護指令(Directive 95/46/EC)第 8 條第 1 項，所指摘敏感性個人資料尚包含：種族背景、政治意向、宗教信仰與哲學信仰、工會會員身分。(Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.)

[23]參照個人資料保護法第 6 條立法理由第 1 點。有關例外情形中以編碼(coded)與永久去連結(delinked)之方式處理特種資料之可能性及其後續帶來影響，詳見邱文聰，從資訊自決與資訊隱私的概念區分─評「電腦處理個人資料保護法修正草案」的結構性問題，月旦法學雜誌第 168 期，2009 年 5 月，頁 185-186；有關犯罪前科之評析，詳見蕭奕弘，論個人資料保護法的法制性問題，成大法學第 23 期，2012 年 6 月，頁 168-171。

[24]現行個人資料保護法乃由行政院令於 2012 年 10 月 1 日起施行，但排除第 6、54 條。另，亦有認給予此一緩衝空間實將導致人民基本權利之侵害，詳見李建良，科技部「醫療人權的憲法基礎與保障體系」成果發表記者會，http://news.ltn.com.tw/news/politics/breakingnews/1102859(最後瀏覽日期 2015 年 2 月 5 日)。

[25]全民健康保險資料庫案目前之歷審裁判為臺北高等行政法院 102 年訴字第 36 號、最高行政法院 103 年判字第 600 號。目前全案已發回台北高等行政法院重審中，截至本研究計畫結案前，尚未作

康保險制度基於健保申報制度所需要，各大醫療院所必須蒐集全體納保人之醫療紀錄，例如醫囑檔、費用檔及個人基本資料檔，以利中央健康保險署（即本案之被告，下稱健保署）核定相關給付金額，故全國民眾之納保及就醫資料皆會由健保署進行建檔及保存，是為全民健康保險資料庫。自 1998 年起，健保署為促進國內全民健康保險相關研究，以提升醫療衛生之發展，即委託國家衛生研究院建置全民健康保險資料庫;並於 2000 年起開放研究單位或生物技術產業付費使用;2009 年起，為求能夠更有效地利用健康保險資料庫，被告另外建置健康資料加值服務中心。此舉即引發侵害人民資訊隱私權及個人資料保護法等疑慮。此一爭議於第一審台北高等行政法院之判決中，就健保署蒐集、處理及利用之「特種資料」及其法律適用之判斷上，據法務部函釋[26]認為，在個人資料保護法第 6 條尚未施行之情況下，第 6 條之規範目前應暫時不予適用，故醫療記錄等特種資料應將其視為一般個人資料來作判斷及處理[27]；惟全案上訴至最高行政法院卻針對此一見解，認為雖然個人資料保護第 6 條尚未施行，但是醫療等特種個人資料蒐集、處理及利用仍應適用該條文，不應將其視為一般個人資料處理之；否則個人資料保護法對於特種資料保護之條文，將有被行政機關以消極不作為或不施行方式來架空之疑慮[28]。

電信事業與電信加值網路業於提供服務的過程中所蒐集、處理獲利用之資料，若符合上述定義，其蒐集、處理及利用之行為即應受個人資料保護法之拘束。為就敏感性個人資料的部分，有鑑於法律規範之效力尚未明確，電信事業目前並未進行蒐集、處理或利用。

二、立法之基本原則

個人資料保護法係參考經濟合作暨開發組織（Organization for Economic Co-operation and Development，OECD)於 1980 年隱私保護與個人資料跨境流動準則(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)所揭示之八大原則分別為：蒐集限制原則(Collection Limitation Principle)、目的特定

成判決。

[26]參照法務部法律字第 10100211340 號函。

[27]參照台北高等行政法院 102 年度訴字第 36 號判決中，七、本院之判斷(一)的第 3 點部分。

[28]參照最高行政法院 103 年度判字第 600 號判決中，八、本院按之(二)部分。

原則(Purpose Specification Principle)、資料關聯性及正確原則(Data Quality Principle)、使用限制原則(Use Limitation Principle)、個人參與原則(Individual Participation Principle)、公開透明原則(Openness Principle)、安全維護原則(Security Safeguards Principle)以及課責原則(Accountability Principle)而訂定[29]。

(一) 蒐集限制原則

蒐集限制原則係指經當事人同意或於具有其他法律所允許之事由時，才得以合法、公正手段於適當場所蒐集個人資料，基於對合法、公正手段之要求，即便資料蒐集者已經獲得當事人之同意，其蒐集之手法上仍受有一定之限制。此項原則落實於我國個人資料保護法第 5、6、8、9、15 以及 19 條。

(二) 目的特定原則

此原則要求資料蒐集者應於蒐集當下，即向當事人明確闡述蒐集的目的，或依法令另為告知；爾後亦須在符合當初蒐集的目的範圍內使用，不得作為其他目的使用[30]。此項原則落實於我國個人資料保護法第 5、8 以及 11 條第 3 項。

然而蒐集資料之特定目的應當如何確認，以及特定目的外之使用是否一律禁止，即具重要性。以前述全民健康保險資料庫案為例，該案原告主張被告機關蒐集、處理健保個人資料之特定目的，應係為了確保健保申報金額正確等特定目的，應不包含將其釋出給第三人使用，故被告機關違反目的特定原則之規定；惟被告機關則認為，依據中央健康保險署組織法第 2 條第 5 款及第 8 款之規定可知，被告之職掌範圍除全民健康保險事項外，另有就國內醫療品質提升之研究、規畫及執行等事務。故其蒐集健保個人資料之特定目的應有包含所謂將其提供給第三人進行學術研究等。且即便上述運用個資之行為未與目的相符，仍得透過個人資料保護法第 16 條第 5 款之例外事由，得將健保個人資料釋出給第三人作特定目的外之利用。就此爭議，台北高等行政法院雖認為健保署蒐集健保個人資料之特定目

[29]劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外─以監視錄影為例(下)，月旦法學教室第 119 期，2012 年 9 月，頁 39-43；邱伊翎，OECD 關於個人資料保護的八大原則，TAHRPAS 報，2008 年 7 月，頁 6。

[30]李婉萍，歐盟個資小組對「目的拘束原則」之詮釋及該詮釋對界定個資法上「特定目的」之啟發，科技法律透析第 25 卷 9 期，2013 年 5 月，頁 19-22；該原則運用在新聞報導與犯罪偵查上之研究，可參考田炎欣，個人資料保護法「目的拘束原則」對新聞報導的限制，中央警察大學犯罪防治學報第 18 期，2013 年 12 月，頁 77-96；田炎欣，警察偵查犯罪侵害個人資料保護法「目的拘束原則」之探討(上)(下)，台灣法學雜誌第 256 期、257 期，2014 年 9 月、10 月。

的應僅係為了確保健保申報金額正確等行政業務，而未包含將個人資料作學術研究，然而，肯認其符合個人資料保護法特定目的外使用之例外事由。最高行政法院則未就此爭議再為闡釋，誠屬可惜。觀察現行個人資料保護法第 6 條及第 16 條之例外條款規定，只要係為了學術研究之必要，不論是一般資料或特種資料，皆可以為特定目的外之使用，似乎大幅擴張學術自由或所謂公共利益等不確定法律概念之適用範圍，對於人民資訊隱私權之保障是否屬正向，容有疑義[31]。

(三) 資料關聯性及正確原則

係指蒐集資料除需符合前述蒐集之特定目的外，另外課予資料蒐集者必須確保相關資料之正確性、完整性適時更新。此項原則落實於個人資料保護法第 5 條以及 11 條。

(四) 使用限制原則

本原則係指除非有經過當事人之同意或法令之許可，否則相關個人資料不得予以洩漏、販售或提供作為當初蒐集之特定目的外之使用[32]。此項原則落實於我國個人資料保護法第 5、16、20 條。

(五) 個人參與原則

每個人都有向資料蒐集者確認對方是否擁有自己的個人資料的權利。若確實負有提供個人資料供蒐集、處理及利用之義務，當事人也都有在合理的時間內、以不貴的價格、合理且明確的方式，獲得通知的權利。若前述二項權利遭到拒絕，當事人也有對此拒絕提出異議的權利，並可以在異議成立時，要求消除、修改、完善或補充資料。此項原則落實於我國個人資料保護法第 3、10、11、13 以及 14 條。

隨著近年台灣個人資料保護意識抬頭，不僅提升人民對於個人資料重視程度，更強化其透過司法途徑主張權利之行動力，以捍衛處在資訊時代下自身個人資料權益，例如：士林地方法院 103 年湖小字第 537 號判決即肯認個人資料主體享有

[31]劉靜怡，不算進步之立法:個人資料保護法初評，月旦法學雜誌，183 期， 2010 年 8 月，頁 154。

[32]通常資料蒐集者會透過定型化契約之方式，要求當事人事先同意為特定目的外之使用，然後才肯提供相對應的服務，此種方法被稱為綑綁式同意。此種作法導致實務上經常濫用當事人同意，來將個人資料為特定目的外之使用。有關綑綁式同意的利弊，請參照李婉萍，個人資料保護脈絡下的「綑綁式同意」，科技法律透析第 24 卷第 1 期，2012 年 1 月，頁 18-41。

主張刪除其過去留於店家個資的權利；以及台北地方法院 103 年訴字 2976 號判決之原告，援引歐洲法院判決之「被遺忘權(right to be forgotten)」[33]，要求 Google 台灣分公司將 Google 網站上，有侵害其人格權之虞所有資料全數刪除之主張，均可見個人資料保護意識之抬頭，並得一窺個人參與原則在司法實務之實踐現況。

(六) 公開透明原則

公開透明原則要求國家必須公開個人資料保護之法規，不得予以隱瞞或拒絕制訂相關規範。僅有如此，人民才能知悉或瞭解如何行使相關權利；並且藉此使資料蒐集者知悉其所應負之義務。此項原則落實於我國個人資料保護法第 8、17 條，惟第 17 條僅限於公務機關，非公務機關並不在此限。

(七) 安全維護原則

透過安全維護原則，資料蒐集者被要求必須採取足夠的安全保護措施來確保相關個人資料不會被遺失、盜用、竄改、毀損或洩漏。根據此一原則，資料蒐集者必須要制定相關保護措施或限制資料存取之方法。此項原則落實於我國個人資料保護法第 18 條以及 27 條。

(八) 課責原則

本原則課與資料蒐集者必須對其所蒐集、處理及利用的資料負責，並需確保其使用者或其自身皆有遵守前述七大原則之要求或限制，若有違反者須負擔一定責任。此項原則落實於我國個人資料保護法第四章(損害賠償)以及第五章(罰則)。

三、蒐集、處理或利用個人資料

(一) 蒐集、處理與利用之行為

所謂蒐集、處理與利用個人資料，蒐集係指「為建立個人資料檔案取得個人資料而言，以任何方式取得個人資料，故不論是直接由當事人交付提供所取得之直接蒐集，或由第三人處取得之間接蒐集」皆屬之；又「為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送，蓋資料經蒐集取得後，須建立成檔案才能利用以發揮其功效，在建立檔案或準備利用之過程中，所為上述紀錄、輸入等行為，因未達於利用之階段」

[33]有關此一資訊時代下新興權利之介紹與限制，詳見第三章第一節。

是謂處理；而利用可依其行為區分為單純利用與共同利用，前者，係指「資料蒐集取得建立檔案後，其最終目的就是利用，以發揮工作之效率，但何謂利用，實難用文字明確定義，故現行個人資料保護法將其定義為『將蒐集之個人資料為處理以外之使用』，以避免疏漏。」[34]；後者，乃指不同蒐集資料主體間之傳遞，如不同層級公務機關間傳送，或總公司與子公司、事業集團內各公司間共同利用等情形。[35]

(二) 蒐集、處理或利用之機關

個人資料保護法就個人資料之蒐集、處理或利用依行為主體區分為之公務機關及非公務機關，前者乃指依法行使公權力之中央或地方機關或行政法人（個人資料保護法第 2 條第 7 款）；而後者則是排除前者以外之自然人、法人或其他團體（個人資料保護法第 2 條第 8 款）。

另外，受公務機關或非公務機關委託蒐集、處理或利用個人資料之本國或外國之法人、團體或自然人，於本法適用範圍內，視同委託機關（個人資料保護法第 4 條），依委託機關應適用之規定為之[36]。惟為確保委託處理個人資料之安全管理，委託機關應對受託者為適當之監督，而監督之方法應涵蓋締約前至契約終止後：締約前，明確預定委託契約內容，包含蒐集、處理與利用之範圍、類別、特定目的及期間，俾保障日後委託者權益受損時，得據此主張損害賠償，捍衛其所持有之個人資料，複委託者之約定受託者，亦同；契約執行期間，定期確認受託者之執行情況並紀錄確認結果，如受託者或其受僱人有違反個人資料保護法或其他相關法規命令時，應向委託機關通報，並採行補救措施；契約終止後，受委託者應將契約期間所儲存之個人資料刪除(個人資料保護法施行細則第 8 條)。

(三) 要件

個人資料保護法分別就公務及非公務機關定有蒐集、處理或利用個人資料之要件，以下僅以非公務機關之部分為重心予以引介說明。

---

[34] 關於蒐集、處理及利用個人資料之定義，台北高等行政法院 102 年訴字第 36 號判決七、本院判斷(二)中，有值得參考之闡述。

[35]綜合觀察個人資料保護法第 2 條第 4 款，以及個人資料保護法施行細則第 6 條第 2 項規定及其立法理由，可知內部傳送定義為同一主體內部間之資料傳遞。

[36]參照法務部法律決字第 10300570190 號函釋：「如委託境外協力廠商代為蒐集、處理及利用客戶個人資料，該受託境外協力廠商即視為委託機關。」

1、特定目的之確認

個人資料保護法第 5 條揭示個人資料蒐集、處理或利用必須以誠實信用方法為之；蒐集不得逾越特定目的之必要範圍及蒐集之範圍必須和目的具有正當合理之關連性等原則，「避免資料蒐集者巧立名目或理由，任意的蒐集、處理或利用個人資料」[37]。個人資料保護法進一步於第 19、20 條要求非公務機關蒐集、處理或利用個人資料應具備特定目的。但為促進資料之合理利用，個人資料保護法第 20 條第 1 項中定有得為特定目的外利用之 6 種情形，包括法律明文規定；為增進公共利益；為免除當事人之生命、身體、自由或財產上之危險；為防止他人權益之重大危害；公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人；經當事人書面同意等六種情形。

以非公務機關之電信事業為例，依據精神衛生法第 33 條第 1 項規定：「為利提供緊急處置，以維護民眾生命、財產安全，主管機關、警察機關、消防機關設置特定之對外服務專線，得要求各電信事業配合提供來電自動顯示號碼及其所在地」以及第 2 項：「前項機關對來電者知有傷害他人或自己或有傷害之虞，得洽請電信事業提供該人所在地地址及其他救護所需相關資訊，電信事業不得拒絕。」電信事業於此即負有配合提供相關個人資料作為特定目的外利用之義務[38]。

2、告知義務

個人資料之蒐集、處理除需符合特定目的之要求外，為了確保人民知悉其個人資料被蒐集、處理及利用之情況，個人資料保護法第 8 條同時要求蒐集機關必須告知被蒐集人包括：蒐集機關名稱、蒐集目的、個人資料類別、利用期間、地區、對象及方式；被蒐集人得主張之權利以及選擇不提供資料對其權益之影響。而蒐集個人資料除向當事人直接蒐集外，亦得自第三人取得之，此等間接蒐集個人資料，蒐集機關依據個人資料保護法第 9 條第 1 項之規定，尤需告知當事人資料來源及其相關事項，俾使當事人明瞭其個人資料被蒐集情形，並得以判斷提供該個人資料之來源是否合法，並及早採取救濟措施，避免其個人資料遭不法濫用

[37]個人資料保護法第 5 條立法理由，其內涵即為不當聯結禁止與筆例原則等法律原則，李婉萍，前揭註 32，頁 23。另，亦有論者認為所謂特定目的，應具正當性，詳見李惠宗，個人資料保護法上的帝王條款—目的拘束原則，法令月刊，64 卷 1 期，2013 年 1 月，頁 50-51。

[38]參照法務部法律字第 1000012630 號。

而損害其權益[39]。此種告知義務之課予乃係為了落實人民憲法上之資訊隱私權，「保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權」[40]。惟個人資料保護法第 8 條第 2 項及第 9 條第 2 項亦分別定有 5 款例外不需踐行告知程序事由。

3、國際傳輸之規範

個人資料保護法第 21 條就非公務機關為國際傳輸個人資料之行為，授權中央目的事業主管機關得限制之[41]，其理由包括[42]：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或是以迂迴方法向第三國（地區）傳輸個人資料規避個人資料保護法等情形。以電信事業為例，主管機關國家通訊傳播委員會(NCC)即於 2012 年依當時電腦處理個人資料保護法第 24 條第 3 款（現行個人資料保護法第 21 條第 3 款）規定，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區[43]。此一由通傳會依據法律授權所發布之命令，應屬行政程序法第 150 條第 1 項所稱：「…行政機關基於法律授權，對多數不特定人民就一般事項所作抽象之對外發生法律效果之規定」，而屬法規命令之性質。

(四) 個人資料之保護義務

個人資料保護法第 27 條要求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。是以，中央目的事業主管機關得訂定「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」，規範其所管制事業於事故發生後，除應即時通報主管機關

[39]參照個人資料保護法第 9 條立法理由。

[40]參照司法院釋字第 603 號解釋文。

[41]中央主管機關目前限制國際傳輸個人資料之形態，大致上分為：國家通訊傳播委員會針對電信事業國際傳輸個人資料以及金融管理監督委員會對金融機構國際傳輸客戶個人資料之限制等兩大種類。陳秭璇，我國個資法對於國際傳輸之限制，科技法律透析第 25 卷 12 期，2013 年 12 月，頁 23；另，有關個人資料國際傳輸之規範模式，詳見張乃文，解析個人資料國際傳輸之法規範趨勢，萬國法律第 181 期，2012 年 2 月，頁 37-41。

[42]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傳輸個人資料規避本法。

[43]國家通訊傳播委員會令通傳通訊字第 10141050780 號「衡酌大陸地區之個人資料保護法令尚未完備，通訊傳播事業於國際傳遞及利用個人資料時，應考量接受國家或地區對個人資料有完善之保護法令，爰依『電腦處理個人資料保護法』第 24 條第 3 款規定，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。」

外，並據個人資料保護法第 12 條規定，於查明後負有以適當方式通知當事人之義務，若經查明後有隱匿不為通知情形，按個人資料保護法第 47 條第 2 款之規定，主管機關得命其限期改正，屆期仍不改正者，得按次處以行政罰鍰。

基此，國家通訊傳播委員會定電信事業資訊通訊安全管理作業要點，並據此製作電信事業資通安全管理手冊，其目的在於保障通訊安全及維護使用者權益原則，確保電信事業資料、系統、設備及網路安全，故其規範電信事業須通過以下標準：資訊安全管理系統要求事項(ISO27)、資訊安全管理之作業規範(ISO27002)、資訊安全管理風險管理(ISO27005)以及電信產業資訊安全管理指引(ISO27011)，當發生資通安全事件時，應立即填具「國家通訊傳播委員會資通安全事件通報單」，向國家通訊傳播委員會通報，並採取應變措施[44]。

第三節 電信法及相關法規範

一、電信法

電信法以「健全電信發展，增進公共福利，保障通信安全及維護使用者權益」為目的，其所稱「電信」乃指利用有線、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（電信法第 2 條第 1 款），電信法就經營電信服務[45]提供民眾使用之電信事業，其事業經營（第一章）；建設與管理電信經營，包括取得與使用土地、維護及管理電信設備（第二章）；以及電信監理（第三章）定有相關規範。

觀察電信法之規範內容，可得知其並未針對電信事業提供電信服務過程中可能涉及之個人資料進行類型化之區分，僅於電信法第 2 條第 8 款中界定通信紀錄之概念：「指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」[46]，而電信號碼係指電話號碼或用戶識別碼。然究應給予通信紀錄何種保護，

[44]由於該管理手冊僅為行政機關之行政指導，並不具有強制拘束力，多由業者自主採行相關資通安全之認證。詳細內容詳見本章第四節之說明。

[45]電信法第 2 條第 4 項定義電信服務為「利用電信設備所提供之通信服務」。

[46]電信法及其相關法令所稱之「通信紀錄」，即慣稱之「通聯紀錄」，在通訊保障及監察法尚未增訂第 3 條之 1 將其明確定義前，我國實務上對通信紀錄所指涉對象相當混亂，或為通訊內容譯文，或

電信法第 6 條針對提供電信服務之過程中電信事業及專用電信處理之通信，基於秘密通訊自由之保障，明訂「他人不得盜接、盜錄或以其他非法之方法侵犯其秘密」，並要求電信事業應就此採行適當並必要之措施；另外，電信事業或其服務人員對於電信之有無及其內容，即便退職，亦負有保密義務（電信法第 7 條第 1 項）。惟受理依法查詢之申請者，即得免除上述義務[47]。

二、第一類電信事業相關管理規則

電信法將電信事業區分為第一類電信事業與第二類電信事業[48]，又，第一類電信事業根據傳送訊息的方式與手段的不同，得再區分為依線纜傳送之固定通信、以電波傳送之行動通信與依電波定位傳送之衛星通信等三大業務類別，以下將就國家通訊傳播委員會依據電信法第 14 條第 6 項授權制定之管理規則中，涉及個人資料類型及其相關規範為說明[49]。

(一) 依線纜傳送之固定通信業務

經主管機關特許並發給執照經營之固定通信業務經營者，乃利用有線或其他經主管機關核准之傳輸方式連接固定發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備，以及二者之附屬設備組成通信系統，並利用此一系統所組成之通信網路，提供網路發送、傳輸或接收語音、數據、影像、視訊、多媒體或其他性質訊息之服務。國家通訊傳播委員會作為固定通信業務之主管機關，依據電信法第 14 條第 6 項之授權，制定固定通信業務管理規則，就固定

為僅含一定門號的通話對象門號、通話時間長短及所使用的基地台位置資料，相關論述詳見，李榮耕，論偵察機關對通信紀錄的調取，政大法學評論第 115 期，2009 年 10 月，頁 8。最高法院 97 年台上字第 505 號與 508 號刑事判決。

[47]基於電信之國家安全性之考量，國家通訊傳播委員會依此授權訂定電信事業處理有關機關 (構) 查詢使用者資料實施辦法、電信事業處理有關機關查詢電信通信紀錄實施辦法以及電信事業用戶查詢通信紀錄作業辦法，詳見第三節、四之說明。另，有關電信具備之特性，請參閱陳銘祥，電信規範體制之探討，經社法制論叢第 23 期，1999 年 1 月，頁 69-70。

[48]觀諸我國電信法第 11 條之規定：「（第 1 項）電信事業分為第一類電信事業及第二類電信事業。（第 2 項）第一類電信事業指設置電信機線設備，提供電信服務之事業。（第 3 項）前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。（第 4 項）第二類電信事業指第一類電信事業以外之電信事業。」可得知我國對於第一類電信事業與第二類電信事業之區分基準，係以通信機線設備之有無區分，詳細論述詳見前述第一章第二節就本研究計畫研究對項及範圍界定之說明；惟此種將兩者以同一市場作為管制範疇，恐難以達到相同服務相同對待之規範效果，王郁琦、林雅惠，我國電信事業分類規範之探討─以網路電話為例，月旦法學雜誌第 102 期，2003 年 11 月，頁 128-132。

[49]陳銘祥，前揭註 47，頁 70。

通信業務之經營特許及其營運管理加以規範[50]。

固定通信業務經營者於提供固定通信服務的過程中可能涉及之個人資料類型，首先即為與固定通信業務經營者訂定契約以使用其所提供服務之用戶[51]相關資料，包括姓名、國民身分證統一編號及國民身分證外之其他足資辨認身分之證明文件證號[52]、地址及所指配號碼等資料。就此，經營者應核對及登錄用戶資料，並於受理申請 2 日內將其載入系統資料檔存查後開通使用，用戶資料至少保存至服務契約終止後 1 年；有關機關依法查詢時，經營者應提供之。

另外，就電信之有無及其內容，固定通信業務管理規則第 49 條之 1 第 2 項規定，就用戶本人查詢之申請，經營者自應提供其所保存之通信紀錄；進一步針對基於調查或蒐集證據之需要，依法申請之查詢，同規則第 49 條明文課予經營者提供相關資料之義務，然若涉及電信內容之監察事項，則應依通訊保障及監察法規定辦理。而通信紀錄之保存，固定通信業務管理規則第 49-1 條第 1 項明訂：市內通信紀錄應至少保存 3 個月；國際及國內長途通信之通信紀錄，應至少保存 6 個月。

(二) 依電波傳送之行動通信業務

行動通信，根據基礎建設[53]與所配電波頻率[54]不同，發展出：

1. 行動通信，即利用無線電終端設備經由行動臺、基地臺、交換設備、網路管理及帳務管理等設備及電信機線設備所構成之行動通信網路，進行語音或非語音之通信，即一般所稱之 2G；

---

[50]有關電信特許制及營運管理之相關探討，詳見劉孔中，關於電信管制政策與法規的一些檢討意見，萬國法律第 114 期，2000 年 12 月，頁 12-24。

[51]「用戶」與「使用者」之概念於固定通信業務管理規則第 2 條第 8 款及第 9 款中有分予定義：用戶乃指與經營者訂定契約，使用該經營者提供之固定通信服務者；使用者係指用戶及其他使用經營者提供之固定通信服務者。由此可知，用戶和使用者未必為同一人，例如：父母申辦門號給未成年之子女使用時，即會發生使用者和用戶事實上屬不同人之狀況。

[52]固定通信業務管理規則第 49-2 條第 3 項就用戶資料中所指證件號碼，於外國人申請時，指護照號碼及護照外之其他足資辨認身分之證明文件證號；於法人申請時，指公司登記統一編號及代表人國民身分證統一編號。

[53]行動通信之基礎建設為行動臺與基地臺，但其於不同電信技術上之定義稍有差異，關於行動臺與基地臺於各行動通信業務規則中之定義請參考行動通信業務管理規則第 2 條第 5 及 6 款、第三代行動通信業務管理規則第 2 條第 5 及 6 款、無線寬頻接取業務管理規則第 2 條第 6 及 7 款、行動寬頻業務管理規則第 2 條第 3、4 及 5 款。

[54]綜合觀察我國第三代行動通信業務管理規則第 7 條、行動寬頻業務管理規則第 7 條以及無線寬頻接取業務管理規則第 6 條之規定，可得知三者所配電波頻率有所差異。

2. 第三代行動通信，指利用指配之頻率以及國際電信聯合會公布 IMT-2000 所定之技術標準，透過行動臺、基地臺、交換設備、網路管理及帳務管理等設備所構成之通信網路，達成語音及非語音通信，即一般所稱之 3G；

3. 無限寬頻接取技術，係指經營者利用所核配頻率，採取無線寬頻接取技術，透過行動臺、基地臺、交換設備、網路管理及帳務管理等設備構成之通信系統，提供使用者發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息。符合該技術之規格分別為 WiMax 以及 LTE，惟其技術仍未達 4G 標準，故電信業界稱其為 3.9G[55]；

4. 行動寬頻，指利用指配之頻率以及國際電信聯合會公布之行動通訊技術標準，透過行動通信之行動臺、基地臺、高速基地臺、交換設備、傳輸機線設備、網路管理設備及帳務管理設備等設備，構成通信系統，提供服務。

而國家通訊傳播委員會作為上述通信業務之主管機關，依據電信法第 14 條第 6 項之授權，就此等所生之行動通信業務，分別制定行動通信業務管理規則、第三代行動通信業務管理規則、無線寬頻接取業務管理規則以及行動寬頻業務管理規則，規範其經營特許、技術及業務監理。

據行動通信業務管理規則第 73 條、第三代行動業務管理規則第 77 條、行動寬頻業務管理規則第 77 條以及無線寬頻接取業務管理規則第 75 條之規定，各業務之經營者於受理行動通信服務申請 2 日內，應完成核對及登錄使用者之資料，包含使用者姓名、身分證或護照之證號、身分證或護照外之其他足資辨識身分之證明文件證號、住址及所指配號碼等資料，並載入系統資料檔存查後開通，至少保存至服務契約終止後 1 年，若有關機關依法查詢時，應提供之。

惟針對以預付卡或其他預付資費方式經營業務之經營者，除同受上述規範拘束外，按行動通信業務管理規則第 74 條、第三代行動業務管理規則第 78 條、行動寬頻業務管理規則第 78 條以及無線寬頻接取業務管理規則第 76 條之規定，要求此類業務經營者應於其營業規章及服務契約範本內明訂，每週複查其使用者資料，如有使用者已經啟用服務而無使用者資料之情事，應通知使用者於 1 週內補具，逾期未補具者，經營者應暫停其通信。

[55]江耀國，無限寬頻接取應用服務之電信監理分析，科技法律透析第 24 卷第 1 期，2012 年 1 月，頁 28。

行動通信業務經營者提供電信服務時，不可避免地持有電信通信紀錄，而其內容包括使用行動通信網路所建立之發信方、受信方電信號碼、通信日期以及通信起訖時間等紀錄，此等個人資料依據行動通信業務管理規則第 72 條之 1、第三代行動業務管理規則第 76 條第 1 項、行動寬頻業務管理規則第 76 條第 1 項以及無線寬頻接取業務管理規則第 74 條第 5 項規定，至少保存 6 個月。而經營者僅得基於調查或蒐集證據之目的依法提供查詢(行動通信業務管理規則第72條第1項、第三代行動業務管理規則第 75 條第 1 項、行動寬頻業務管理規則第 75 條第 1 項以及無線寬頻接取業務管理規則第 74 條第 1 項之規定)，或是應使用者本人申請提供查詢（行動通信業務管理規則第 72 條之 1 第 2 項、第三代行動業務管理規則第 76 條第 2 項、行動寬頻業務管理規則第 76 條第 2 項以及無線寬頻接取業務管理規則第 74 條第 6 項)。

惟若查詢之範圍不僅及於「通信之有無」，進一步及於「通訊之內容」時，因涉及電信內容之監察事項，則應循通訊保障及監察法之相關規定辦理之。(行動通信業務管理規則第 72 條第 2 項、第三代行動業務管理規則第 75 條第 2 項、行動寬頻業務管理規則第 75 條第 2 項以及無線寬頻接取業務管理規則第 74 條第 2 項）

(三) 依電波定位傳送之衛星通信業務

衛星通信業務係由經主管機關特許並發給執照經營衛星通信業務者，利用衛星系統[56]與地球電臺[57]組成之衛星通信網路，提供無線電通信服務之業務，國家通訊傳播委員會作為衛星通信業務之主管機關，依據電信法第 14 條第 6 項之授權，制定衛星通信業務管理規則，就衛星固定通信業務與衛星行動通信業務之經營特許及營運管理加以規範[58]。

[56]衛星通信業務管理規則第 2 條第 1 款：「衛星系統：指由一枚或數枚人造衛星及控制該衛星之設備所組成之系統。」

[57]衛星通信業務管理規則第 2 條第 2 款:「地球電臺:指在地球上與衛星系統間做無線電信號接收、處理、發射之電信設備。」。地球電台又可區分為第 3 款:「固定地球電臺：指須架設於地球表面固定地點，始可進行通信之地球電臺。」第 4 款:「行動地球電臺：指可移動之衛星行動終端設備或非架設於固定地點，可於行動中通信之地球電臺。」

[58]「在其他國家衛星通信事業業者主要有兩種：衛星傳輸業者與衛星傳輸分租業者，前者，係指根據各國國內法律規定，取得擁有或經營衛星通信業務知業者，依我國電信法之分類，屬於第一類電信事業；後者，則是指長期向衛星傳輸業者租用衛星之地面和太空設施，再作短期性之分租，依照我國電信法之分類，應屬於第二類電信事業。惟在我國電信法與電信政策下，一向不傾向容許單純電信傳輸能力之分租，以其可能和第一類電信事業競爭，有害於電信市場秩序故也，衛星通信業務亦不例外，因此在其他國家盛行之衛星傳輸分租業者，我國現制並不認之。因此，衛星通信業務僅限於第一類電信事業，下再分為衛星固定通信業務與衛星行動通信業務。」陳銘祥，衛星通信法律

衛星通信業務之經營者於受理服務申請 2 日內，應完成核對及登錄使用者之資料，其包含使用者姓名、身分證或護照之證號、身分證或護照外之其他足資辨識身分之證明文件證號、住址及所指配號碼等資料[59]，並載入系統資料存查後開通，至少保存至服務契約終止後 1 年；有關機關依法查詢時應提供之。針對以預付卡或其他預付資費方式經營衛星通信業務者，除應於預付卡售出時即將購買者資料記存，並應於每週複查其使用者資料，如有使用者已經啟用服務而無使用資料者資料之情事，應通知其於 1 週內補具，逾期未補具者，應暫停其通信衛星。前述規定，應由預付卡或其他預付資費之衛星通信業務經營者明訂於其營業規章及服務契約範本內。而就電信之有無及其內容，衛星通信經營者對基於調查或蒐集證據之目的依法查詢者，應提供之，惟若涉及電信內容之監察事項，即應依通訊保障及監察法之相關規定辦理（衛星通信業務管理規則第 52 條）。

惟衛星通信業務管理規則並未就用戶本人查詢之情況加以規範，亦未說明經營者經營衛星通信業務過程中所蒐集相關個人資料之保存期間。前者應可適用電信法第 7 條第 3 項授權制定之電信用戶查詢通信紀錄作業辦法，提供用戶相關通信紀錄；使用期間的部分或可參考行動通信業務管理規則之規定予以增定。

三、第二類電信事業管理規則

依據電信法對於電信事業之區分，第二類電信事業依據電信法第 17 條第 1 項規定，應向電信總局申請許可，經依法辦理公司或商業登記後，發給許可執照，始得營業。而就其營業項目、技術規範與審驗項目、許可之方式、條件與程序、許可執照有效期間、營運之監督與管理及其他應遵行事項之管理規則，立法者透過電信法第 17 條第 2 項授權由主管機關訂定之。國家通訊傳播委員會作為第二類電信事業之主管機關，即依上述授權制定第二類電信事業管理規則，就第二類電信事業之經營許可、營運管理、通信設備維運之管理加以規範，並於 2014 年 8 月修正時新增資通安全管理之相關規定[60]。

規範之研究，經社法制論叢第 26 期，2000 年 7 月，頁 50-51。

[59]衛星通信業務管理規則第 53 條第 3 項規定就外國人申請時，其證件號碼乃指護照號碼及護照外之其他足資辨認身分之證明文件證號；於法人申請時，指公司登記統一編號及代表人國民身分證統一編號。另就申請用戶為政府機關、公立學校及公營事業機構之情形，經營者核對及登錄其用戶資料，得以該機關(構)公文書為證明文件。

[60]有關資訊安全管理之概念，詳見財團法人資訊工業策進會，公務機關個人資料保護方案計畫研究成果報告書，行政院法務部委託研究，2012 年 5 月，頁 15-67。顏婉旬，資訊安全與電子商務─談資訊安全通報機制，科技法律透析第 23 卷第 11 期，2011 年 11 月，頁 43-63。顏婉旬，防災應變

第二類電信事業經營一般及特殊業務[61]時，均應核對及登錄其用戶[62]之資料，包括使用者姓名、國民身分證統一編號、第二證件號碼[63]及住址等資料：若屬虛擬行動網路服務經營者或 E.164 用戶號碼網路電話服務經營者[64]，則應另載入所指配號碼，並於受理申請二日內完成使用者資料載入其系統資料檔存查，方得開通。以預付卡或其他預付資費方式經營虛擬行動網路服務者或 E.164 用戶號碼網路電話服務者，亦同，但其應於營業規章及服務契約內明定每週複查其用戶資料，如有使用者已經啟用服務而無使用者資料之情事，經營者應暫停其通信。

前項規定，經營者應於其之。用戶資料至少保存至服務契約終止後 1 年，於有關機關依法查詢時，經營者應提供之。

另外，就電信之有無及其內容之電信通信紀錄查詢，若是基於調查或蒐集證據之目的，並依法律程序申請者，第二類電信事業經營者應提供之。惟若涉及電信內容之監察事項，則應遵循通訊保障及監察法規定。而就電信通信紀錄保存期間之規定，第二類電信事業管理規則第 27 條第 3 項將通信紀錄分為四種類型，其至少應保存之期間由 3 至 6 個月不等[65]：

1、語音單純轉售服務通信紀錄應保存 6 個月。

之挑戰─談關鍵基礎設施保護，科技法律透析第 23 卷第 8 期，2011 年 8 月，頁 13-18。

[61]第二類電信事業管理規則第 2 條第 4 款：「第二類電信事業特殊業務：指經營語音單純轉售服務、E.164 用戶號碼網路電話服務、非 E.164 用戶號碼網路電話服務、租用國際電路提供不特定用戶國際間之通信服務或其他經主管機關公告之營業項目者。」第 9 款：「第二類電信事業一般業務：指第 4 款以外之第二類電信事業業務。」綜上，第二類電信特殊業務之意義，在於讓沒有網路的業者也能加入市場服務，提供與既有業者同等的服務給消費者，詳見王郁綺、林雅惠，前揭註 48，頁 133。王廷俊，國內第二類電信事業經營現況與問題探討，通訊雜誌第 59 期，1998 年 12 月，頁 76-77；另有論者認為，該業務分類方式恐有違法律保留原則，王郁綺、張家慧，網路語音服務在現代電信管制架構下的政策與法律爭議，萬國法律第 114 期，2001 年 12 月，頁 25-37。

[62]第二類電信事業管理規則就用戶與使用者之定義與固定通信業務管理規則相同。針對用戶為政府機關、公立學校及公營事業機構之情況，第二類電信事業管理規則第 27 條第 5 項規定得以該機關（構）公文書作為識別用戶身分之證明文件。

[63]證件號碼於外國人申請時，指護照號碼及護照外之其他足資辨認身分之證明文件證號；於法人申請時，指公司登記統一編號及代表人國民身分證統一編號；於自然人申請時，指身分證號及足資辨識身分之證明文件證號，參照第二類電信事業管理規則第 27 條第 6 項。

[64]「網路電話服務可分為：電腦對電腦(PC to PC)、電腦對電話(PC to Phone)、電話對電腦(Phone to PC)或電話對電話(Phone to Phone)，但不論何種形式網路電話，主要都是透過網際網路，並以分封交換(packet switching)方式，將資料或語音訊號分割成許多封包(packet)同時附加標頭(header)，該封包標頭會註明發話端與受話端之 IP 位址(非電話號碼)，再藉由 IP 位址與許多可行之路徑並配合『儲存並輸送』(store&forward)，將封包由發話端傳送給受信端。」王郁綺、林雅惠，前揭註 48，頁 134-135。

[65]周慧蓮，電信法中關於網際網路服務提供者權義規範簡析，科技法律透析第 16 卷第 8 期，2004 年 8 月，頁 14。

2、網路電話服務通信紀錄應保存 6 個月。

3、網際網路接取服務：

（1）撥接用戶識別帳號、通信日期及上、下網時間等紀錄應保存 6 個月。

（2）非固接式非對稱性數位用戶迴路（ADSL）用戶識別帳號、通信日期及上、下網時間等紀錄應保存 3 個月。

（3）纜線數據機用戶識別帳號、通信日期及上、下網時間等紀錄應保存 3 個月。

（4）張貼於留言版、貼圖區或新聞討論群之內容來源 IP 位址與當時系統時間應保存 3 個月。

（5）免費電子郵件信箱及網頁空間線上申請帳號時之來源 IP 位址及當時系統時間應保存 6 個月。

（6）電子郵件通信紀錄應保存 1 個月。

4、虛擬行動網路服務通信紀錄應保存 6 個月

第二類電信事業管理規則第 27 條第 7 項賦予主管機關限制經營者受理民眾以同一身分證統一編號申請電信服務之用戶號碼數之權限。經營者應依主管機關公告之限制條件及執行方式辦理[66]。

2014 年第二類電信事業管理規則新增之第四章之一資通安全管理之規定，第 31 條之 1 要求經營者有「系統發生資通安全事件達國家資通安全通報應變作業綱要規定之影響等級第三級以上」、「有危害國家安全或資通安全之虞，經有關機關知會」或「經主管機關考量經營業務與設施之關鍵性、用戶數或網路規模、經營控制權等因素認定有必要」的情形時，經主管機關通知，應於 1 年內建立資通安全防護及偵測設施，並定期進行滲透測試、弱點掃描及修補作業，並通過 ISO/IEC27001 國際標準及主管機關公告之電信事業資通安全管理手冊 ISO/IEC27011 增項稽核表之資通安全管理驗證。並分別於第 31 條之 2 及第 31 條之 3 就硬體設備與人員之管理及維護予以規範。另外，要求第二類電信事業經營

[66]國家通訊傳播委員會所公告之申購行動電話預付卡門號辦法中，定有「一證一號」，即每一個身分證號在同一電信事業只能申辦一個門號；以及「雙證查核」，即申辦手機時必須以雙份證件辦理。

者應依主管機關公告之資通安全應變作業程序，建立資通安全事件之通報、處理、回報等聯防應變措施[67]。若發生資通安全事件，經營者應依主管機關通報之資安事件，辦理緊急應變措施並保存紀錄，回報主管機關備查，該紀錄應至少保存 6 個月（第二類電信事業管理規則第 31 條之 1 第 4、5 項）。

四、提供第三人資料之相關規範[68]

(一) 電信事業處理有關機關（構）查詢電信使用者資料實施辦法

國家通訊傳傳播委員會依電信法第 7 條第 2 項規定訂定之電信事業處理有關機關（構）查詢電信使用者資料實施辦法，使用者資料指電信使用者姓名或名稱、身分證統一編號、地址、電信號碼（指電話號碼或用戶識別碼）等資料，並以用戶申請各項電信事業業務所填列之資料為限。

電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 3 條規定得依法向電信事業查詢使用者資料之情形包括：司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者；其他政府機關因執行公權力所需者；與公眾生命安全有關之機關（構）為緊急救助所需者[69]。

有關機關（構）查詢使用者資料應備正式公文或電信使用者資料查詢單；對於案由特殊、情況緊急之查詢，得由法官、檢察官或查詢機關（構）之首長或經其授權之主管署名並加蓋職章及連絡人之資料，視同機關（構）正式公文書先傳真之，並經回叫確認為之，並於查詢後 3 個工作日內補具正式公文或加蓋印信之電信使用者資料查詢單正本。（電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 5 條）

---

[67]此新增章節之規範與個人資料保護法之重疊處，約略可分為以下四大點：實體環境安全、機關安全、資訊系統安全與人員安全，而此與行政院研究發展考核委員會(現國家發展委員會)之「個人資料保護參考指引」導入尚未通過 ISO/IEC27001 之機關，所為之檢視控制措施四大層面，並無二致，故針對已取得 ISO/IEC27001 驗證之資訊安全管理系統(Information Security Management Systems，ISMS)之第二類電信事業，為避免產生制度上多頭馬車，其可參酌將該 ISMS，融入個人資料保護法之規範，藉由 P D C A (Plan – Do – Check –Action)循環強化個資保護工作。財團法人資訊工業策進會，前揭註 60，頁 48-51；另有關資安政策與個人資料保護法之契合，詳見廖緯民，資安政策與法律課責─兼論我國 2010 年個人資料保護法中的資安政策管理體制，前瞻科技與管理第 2 卷第 2 期，2012 年 11 月，頁 37-51。

[68]相關研究內容，詳見潘維大、余啟民、黃心怡、張錕盛，資訊服務業者配合政府公權力提供客戶資料之法制研究，行政院經濟建設委員會委託研究，2006 年 12 月，頁 74-77。

[69]電信事業原則上不負向受侵權人提供使用者資料之義務，但卻負有保存使用者資料之義務，以利受侵權人提起訴訟時，檢調單位得調取之。周慧蓮，前揭註 65，頁 14。

查詢單中若有不屬受理查詢之電信事業之使用者或逾電信事業資料保存期限，致無法提供者，該電信事業應於查詢單加註明「無資料」答覆之（電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 7 條）。有關機關（構）申請查詢之公文或查詢單，各電信事業受理單位應以專冊登記列管，並保存 1 年（電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 10 條）。經辦查詢作業之人員，對於查詢作業之過程及所查得資料之內容等，應予保密（電信事業處理有關機關（構）查詢電信使用者資料實施辦法第 11 條）。

(二) 電信事業處理有關機關查詢電信通信記錄實施辦法

國家通訊傳播委員會依電信法第 7 條第 2 項規定訂定之電信事業處理有關機關查詢電信通信記錄實施辦法，本辦法所稱通信紀錄，指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（包括電話號碼或用戶識別碼）、通信日期、通信起迄時間等紀錄，並以電信系統設備性能可予提供者為原則（電信事業處理有關機關查詢電信通信記錄實施辦法第 2 條）。

電信事業處理有關機關查詢電信通信記錄實施辦法第 3 條要求有關機關查詢通信紀錄應先考量其必要性、合理性及比例相當原則[70]，並應符合相關法律程序後，再備正式公文或附上電信通信紀錄查詢單，載明需查詢之電信號碼、通信紀錄種類、起迄時間、查詢依據或案號、資料用途、連絡人、連絡電話或傳真機號碼、及指定之列帳相關資料等，送該電話用戶所屬電信事業指定之受理單位辦理[71]。但若遇案情特殊、情況緊急之查詢，得由法官、軍事審判官、檢察官、軍事檢察官、查詢機關首長或其書面指定人先以電話或公文傳真，並經回叫確認為之，並應於查詢後 3 個工作日內補具正式公文或加蓋印信之電信通信紀錄查詢單正本。經辦查詢作業之人員，對於查詢作業之過程及所查得資料之內容等，負有保密之義務（電信事業處理有關機關查詢電信通信記錄實施辦法第 10 條）。

電信事業提供有關機關查詢之通信紀錄，應僅於該通信紀錄之保存期限以內者，

[70]有關行政機關及偵查機關對必要性、合理性及比例相當性原則認定標準之設定，將對通訊隱私保障造成顯著影響，詳見林三欽，通訊監察與秘密通訊自由，憲政時代第 23 卷第 2 期，1997 年 3 月，頁 8 以下；有關行政機關之行政行為，於行政法上一般容許性與合法性之審查步驟，詳見潘維大、余啟民、黃心怡、張錕盛，前揭註 68，頁 83-106。

[71]事實上，電信事業並無決定是否同意的實質審查權限，歷次修法所增訂之條件與程序要件，僅是就電信事業及其所屬人員依辦法提供通信紀錄，因而未履行電信法第 7 條第 1 項所課予之保密義務，阻卻其不法性。石世豪，電信自由化下通訊安全規範的轉型趨勢─通信秘密、個人資料保護與電信事業的管制變革，全國律師，第 9 卷第 5 期，2005 年 5 月，頁 46-48。

始予受理，該期限之計算乃由受理查詢日回溯起算，市內通信紀錄，最近 3 個月以內；國際、國內長途通信紀錄，最近 6 個月以內；行動通信通信紀錄，最近 6 個月以內。若因逾此保存期限，致無法提供者，電信事業應書面回覆說明之。

有關機關申請查詢之公文，各電信事業受理單位應以專冊登記列管，並通信紀錄保存 2 年，逾期予以銷毀。另外，經辦查詢作業之人員，對於查詢作業之過程及所查得資料之內容等，應予保密，不得外洩。

(三) 通訊保障及監察法

我國個人資料保護之規範中就提供第三人通訊相關資料，包括通信內容、使用者資料或通信紀錄，於通訊保障及監察法中亦有相關規範，且因其相較於個人資料保護法具有特別法之地位而往往優先適用[72]。通訊保障及監察法第 1 條開宗明義表示其立法目的乃係為了保障人民秘密通訊自由及隱私權不受非法侵害，除了呼應憲法第 12 條保障人民通訊秘密自由之意旨，亦配合條文之增訂，納入隱私權之保障。通訊保障及監察法發展至此，與個人資料保護之聯繫逐趨緊密，故接續擬就通訊保障及監察法中有關個人資料保護之規定進行介紹說明[73]。

1、 涉及個人資料之類型

觀諸通訊保障及監察法之客體，可歸類為第 3 條所稱「通訊」，以及第 3-1 條之「通訊使用者資料」及「通信紀錄」。依據通訊保障及監察法第 3 條之規定，所謂「通訊」係指郵件及書信、言論及談話和其他利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信，惟其須以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限[74]。

又依據通訊保障及監察法第 3 條之 1 之規定，所謂「使用者資料」係指電信

[72]參照法務部法律字第 10303506200 號要旨：「個人資料保護法第 15、16 條、電信法第 7 條、通訊保障及監察法第 11-1 條規定，個人資料保護法屬普通法性質，個別法律如對個人資料蒐集、處理或利用另有特別規定，應優先適用，故電信公司是否應為個人資料提供，因有上述特別規定，該等規定應優先適用」。

[73]關於具電信事業身分之網路提供者，個人資料保護法與電信法及其相關法規範下，在面對通訊保障及監察法之衝擊，應具有之義務與責任，詳見吳兆琰，網路環境下的監察法制，科技法律透析第 17 卷第 2 期，2005 年 2 月，頁 61；關於網際網路通訊之特色與爭議，詳見蔡美智，「通訊保障及監察法」關於網路監聽的相關爭議，資訊法務透析第 11 卷第 12 期，1999 年 12 月，頁 35-45。

[74]由此可知，昔日通訊保障及監察法所規範者，應是以監察特定人間所交換的訊息內容時，所應遵循的相關程序規定，並不及於非內容性通訊資料；屬於非通訊資料之電信紀錄及用戶資料，則須循通訊保障及監察法第 11-1 條所規範之要件以及電信法第 7 條第 2 項授權訂定之有關機關（構）查詢通信紀錄及使用者資料之作業程序為之。李榮耕，前揭註 46，頁 19。

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；而「通信紀錄」，係指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、位置、服務型態、信箱或位置資訊等紀錄，突破電信法第 2 條第 8 款對於通信紀錄之界定，將「信箱」及「位置資訊」定位為通信紀錄之類型之一[75]，惟目前電信事業所蒐集、處理及利用之位置資料乃為使用者收發話之基地台位置資料；相關 GPS 全球定位系統資料部分，受限於資料過於龐大之故，目前電信事業並未就此進行蒐集、處理及利用[76]。

2、 相關規範部分

通訊保障及監察法中對人民秘密通訊自由與隱私權之限制，可分為通訊內容之監察及通信資料之調取兩大型態：

(1)通訊內容之監察

目前我國通訊保障及監察法中，針對通訊內容之監察，在符合通訊保障及監察法第 5 條之規定下，檢察官或司法警察官報請檢察官同意後，得聲請法院核發通訊監察書；通訊監察之方法依據同法第 13 條之規定，僅得以以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。

(2)使用者資料與通信紀錄之調取[77]

---

[75]法務部法檢字第10300162120號函中，對於使用者IP位址及電子郵件是否適用通訊保障及監察法之疑義，認：IP位址若屬電信使用人使用IASP之電信服務後，電信系統所產生之紀錄，即屬通訊保障及監察法第3條之1第1項所稱之通信紀錄，調取時應依通保法相關規定為之。至網際網路平臺提供者（Internet Platform Provider，IPP）網際網路內容提供者（Internet Content Provider，ICP）、網際應用服務提供者（Application Service Provider，ASP），因非屬電信法第2條第5款所稱之電信事業，無通訊保障及監察法之適用，故無須遵循該法所定之調取程序；而電子郵件若為針對特定帳號，預定一定期間攔截、過濾將寄發或收受之郵件者，應遵守通訊保障及監察法規範要件，然若係調取某特定帳號內業已寄發或收受之郵件情形，則非適用通保法而應依刑事訴訟法為之。

[76]有關位置資料與資訊隱私權之關係，詳見周慧蓮，論行動化生活之資訊隱私侵害─以定位服務為例，月旦法學雜誌第 99 期，2003 年 8 月，頁 152-165。洪聖濠，行動定位服務中的位置資料隱私保護，科技法律透析第 17 卷第 1 期，2005 年 1 月，頁 8-13。林達峰，行動生活之隱私爭議─現行法制能否妥善處理位置資訊衍生問題，科技法律透析第 18 卷第 6 期，2006 年 6 月。

[77]根據行政院 2014 年 10 月 16 日會議通過之通訊保障及監察法草案總說明第 1 點「通信紀錄及通訊使用者資料對人民隱私權影響較為輕微，應無採法官保留之必要，爰刪除相關規定」，甫實行不久之第 11 條第 1 項，若日後送進立法院審議通過，該法條恐將走入歷史。而對現行法之評析，詳見李榮耕，現行通訊保障監察法制的困境及去路，司法改革雜誌第 99 期，2013 年 12 月，頁 22-25、劉靜怡，通保法究竟保障了誰？，司法改革雜誌第 99 期，2013 年 12 月，頁 30-33、劉孔中、趙晞華，通訊保障及監察法修正意旨之辯證與再修正方向之檢視，軍法專刊第 60 卷第 3 期，2014 年 6 月，頁 38-48。

2014年1月修正之通訊保障及監察法新增使用者資料與通信紀錄調閱等規定，依據通訊保障及監察法第11條之1第1項之規定，檢察官偵查最重本刑3年以上有期徒刑之罪；且有事實足認其使用者資料對案件偵查有必要及關連性時，除有急迫事由外，皆應向法院聲請核發調取票；縱使有急迫之情事，依據同條第 5 項之規定，於急迫原因消滅後，應向法院補行聲請調取票。惟當檢察官偵查最輕本刑10年以上有期徒刑之罪等相關罪名時，依據同條第3項之規定，例外得依職權直接調閱相關使用者資料。

司法警察官依據同條第2項之規定，因調查犯罪嫌疑人犯罪情形及蒐集證據，認有調取通信紀錄之必要時，必須報請檢察官許可後，才能向法院聲請核發調取票。惟若偵查最輕本刑10年以上有期徒刑之罪等相關罪名時，則可向檢察官聲請同意後，直接調閱通信紀錄，不須再向法院聲請調取票。

另外，依據通訊保障及監察法第11條之1第8項之規定，為避免國家安全遭受危害，必須蒐集外國勢力或境外敵對勢力情報之必要者，由綜理國家情報工作機關向電信或郵政事業調取相關使用者資料或通信紀錄時，不須受到同條前七項之限制。

第四節 我國現況

一、概述

我國電信事業者個資保護現況大致可分作兩方面加以觀察，其一是遵法義務，亦即根據個資法蒐集、處理、利用電信服務使用者和契約用戶的個資，進一步而言，涉及特定目的外利用、資訊分享第三人、如何監督受委託處理個資者，以及是否擬定和公告電信服務使用者和契約用戶主張資訊自主權之處理流程等問題；其二是各該電信者對其保有之電信服務使用者和契約用戶的個人資料檔案，所採行之適當安全維護機制，此範疇包含有無事先進行隱私影響之評估、發生個資外洩事故通報之流程以及個資資料庫之管理規範、流程。

關於安全維護機制方面，目的事業主管機關國家通訊傳播委員會，據其組織法

第 3 條第 8 款所定「資通安全之技術規範及管制」職權，制訂電信事業資訊通訊安全管理作業要點；並再就該作業要點之第 2 點訂定了「電信事業資通安全管理手冊[78]」，輔導業者落實並通過 ISO/IEC27001 與 ISO/IEC27011，以達個人資料保護與自我檢視資訊安全等級。簡言之，我國電信事業者主要是依據前述資通安全手冊建構各該業者的個資安全維護機制。

至於遵法義務方面，首先特定目的之告知方式，主要有兩大途徑，一是公告於各家官方網站，二則記載於契約條款當中。其次，資訊分享第三人方面，各家業者皆在營業規章中載明，其對因業務上所掌握之用戶相關資料負有保密義務。除當事人要求查閱本身資料，或符合個人資料保護法及相關法令規定外，其不得以任何方式將當事人之個人資料對第三人(含與本公司合作之內容服務提供者)揭露。

目前達成共識一致的資訊分享第三人事由則是：一、司法機關、監察機關或治安機關因偵查犯罪或調查證據所需者；二、其他政府機關因執行公權力並有正當理由所需者；三、與公眾生命安全有關之機關(構)為緊急救助所需者。若有前述情形者，有權機關(構)得依法以正式公文載明理由及相關法令依據查詢。甚且如情況緊急，得先為查詢，再以正式公文後補之。

此外，關於各家電信事業者與子公司、關係企業間，抑或是受各該業者委託或與其有合作或業務往來合作廠商之資訊分享，各家業者僅說明是符合法令規定範圍之利用，但卻未告知公眾哪些是必要範圍內的資料，且即便允許客戶得自由選擇提供資料，但業者通常會表示若不提供將影響服務申辦或其完整性，致使電信服務使用者或契約用戶心生不安，從而懼於主張權利。

綜言之，或因各家業者能以「電信事業資通安全管理手冊」為據，且可透過下一節所述認證方式達成有形的檢測，所以個資安全維護機制方面尚謂無嚴重缺失。然相較之下，遵法義務方面則有多處待改進之處，比如如何監督受託處理個資者、個資保存期限、蒐集個資內容等事項的資訊之公告說明。

[78]電信事業資通安全管理手冊，
http://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=261&law_sn=1535&sn_f=1790&is_history=0

二、第一類電信事業者個人資料保護政策比較

	中華電信	台灣大哥大	遠傳電信	威寶電信	亞太電信
法源	個人資料保護法	個人資料保護法	個人資料保護法	個人資料保護法	個人資料保護法
原則	-依據契約及當事人同意 -妥善保護個人資料	-依據契約及當事人同意 -妥善保護個人資料	依據契約及當事人同意 -妥善保護個人資料	-依據契約及當事人同意 -妥善保護個人資料	尊重顧客之個人隱私權 遵循個資法、亞太電信個人資料保護管理政策
目的	-行銷 -提供電子票證、契約或類似契約、經營電信事業務與電信加值網路業務等服務 -遵守通訊傳播監理、司法或其他公務機關之命令或查核 -於業務範圍內蒐集個人資料	-行銷 -提供電子票證、契約或類似契約、經營電信事業務與電信加值網路業務等服務 -遵守通訊傳播監理、司法或其他公務機關之命令或查核 -於業務範圍內蒐集個人資料	-行銷 -提供電子票證、契約或類似契約、經營電信事業務與電信加值網路業務等服務 -於業務範圍內蒐集個人資料	-履行法定及契約義務 -提供或辦理電信商品或服務 -遵守通訊傳播監理、司法或其他公務機關之命令或查核 -於業務範圍內蒐集個人資料	因經營電信事業務及其他合於營業登記項目或組織章程所定業務等等之特定目的，因作業需求將蒐集、處理或利用您的識別類、特徵類、社會情況類、財務細節等類別之個人資料。
個資類別	-主管機關公告之個人資料類別及電信事業或電信加值網路業務執行所必要之個人資料 -各項申請文件之客戶本人及法定代理人之姓名及身分證字號等足資辨識身分之個人資料	-主管機關公告之個人資料類別及電信事業或電信加值網路業務執行所必要之個人資料 -各項申請文件之客戶本人及法定代理人之姓名及身分證字號等足資辨識身分之個人資料	-主管機關公告之個人資料類別及電信事業或電信加值網路業務執行所必要之個人資料 -各項申請文件之客戶本人及法定代理人之姓名及身分證字號等足資辨識身分之個人資料	-辨識個人資料、辨識財務者、政府資料中之辨識者、個人描述及其他依主管機關公告之個人資料類別	本政策所稱之個人資料，係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

	中華電信	台灣大哥大	遠傳電信	威寶電信	亞太電信
利用範圍	-中華民國所轄境內 -供母公司及母公司關係企業及合作廠商 -利用期間為契約成立前階段及契約存續期間(其他法規另有規定者，從其規定)	-中華民國所轄境內 -供母公司及母公司關係企業及合作廠商 -於網站上說明其相關資料處理系統已受妥善保護 -利用期間為契約成立前階段及契約存續期間(其他法規另有規定者，從其規定)	-中華民國所轄境內 -供母公司、子公司及母公司委外之廠商 -利用期間為契約成立前階段及契約存續期間(其他法規另有規定者，從其規定)	-中華民國所轄境內 -供母公司及母公司關係企業及合作廠商 -保證其相關資料處理系統已受妥善保護，如有必要委託第三者時，會嚴格遵守保密義務、並採取必要檢查程序確保個人資料之保障	亞太電信所蒐集之個人資料僅供蒐集時所符合之目的和範圍加以運用，除在下列情況下，不會將個人資料提供予第三人或移作其他目的使用： 1.事前取得您的同意。 2.需要與第三人共用您的資料，方能提供您所要求的產品或 服務。 遵守法令或政府機關的要求。 3.您的使用行為違反本公司服務約定或其他產品、服務特定 使用規定。
權利告知	-告知當事人依據個人資料保護法得請求查詢或閱覽、製給複本、補充或更正、停止蒐集處理及利用相關個人資料 -行使前述權利必須提供相關個人資料以供辨識	-告知當事人依據個人資料保護法得請求查詢或閱覽、製給複本、補充或更正、停止蒐集處理及利用相關個人資料 -行使前述權利必須提供相關個人資料以供辨識	-告知當事人依據個人資料保護法得請求查詢或閱覽、製給複本、補充或更正、停止蒐集處理及利用相關個人資料 -行使前述權利必須提供相關個人資料以供辨識	-告知當事人依據個人資料保護法得請求查詢或閱覽、製給複本、補充或更正、停止蒐集處理及利用相關個人資料	可依個人資料保護法第三條之規定，請求停止蒐集、處理及利用個人資料
監督機制	無	無	無	-有提及資料提供給第三人時會有保護監督機制，但卻未明文表示	無
事故通知	無	無	無	無	無

	中華電信	台灣大哥大	遠傳電信	威寶電信	亞太電信
受理客訴窗口	門市、客服專線及 EMAIL	客服專線及 EMAIL	客服專線及 EMAIL	客服專線及 EMAIL	客服專線及 EMAIL
個資保護期限	未載明銷毀期限及銷毀期限	未載明銷毀期限	未載明銷毀期限	未載明資料保存及銷毀期限	未載明資料保存及銷毀期限
疑問洽詢方式	客服專線及 EMAIL	客服專線及 EMAIL	客服專線及 EMAIL	客服專線及 EMAIL	客服專線及 EMAIL

三、第二類電信事業者個人資料保護政策比較

	家樂福電信	瑪凱電信	7 mobile	連科通訊 (pchome&talk)
法源依據	個人資料保護法	個人資料保護法	個人資料保護法	個人資料保護法
原則	個人資料之蒐集、處理或利用之原則	個人資料之蒐集、處理或利用之原則	個人資料之蒐集、處理或利用之原則	個人資料之蒐集、處理或利用之原則
目的	係為確認在本公司網站（下稱本網站）上取得資訊的使用者身份及提供有關行動電話各項服務之用	為確認在MKY上取得資訊的使用者身份確認及提供有關加值服務之用	為確認在本公司網站上取得資訊的使用者身份及提供有關行動電話各項服務之用	行銷、客戶管理與服務、售後服務、提供電子商務服務、履行法定或合約義務、保護當事人及相關利害關係人之權益、以及經營合於營業登記項目或組織章程所定之業務
個資類別	行動電話門號、身分證字號、行動電話SIM卡號碼、姓名、電子郵件地址、職業或行業別、教育程度、婚姻、個人收入或營業額、興趣 上網瀏覽或查詢時，在系統上產生的相關記錄：IP位址、使用時間、瀏覽器、瀏覽及點選紀錄	門號、身份證字號或統一編號、電子郵件、教育程度、婚姻 使用MKY任何服務時，在系統上產生的相關記錄，包括：IP位址、使用時間、瀏覽器、瀏覽及點選紀錄等。	行動電話門號、身分證字號、行動電話、SIM卡號碼、姓名、電子郵件地址 上網瀏覽或查詢時，在系統上產生的相關記錄，包括IP位址、使用時間、瀏覽器、瀏覽及點選紀錄	-姓名 -連絡方式(包括但不限於電話、E-MAIL及地址等) -為完成收款或付款所需之資料 -IP位址 -其他得以直接或間接識別使用者身分之個人資料 -在PChomeTalk相關網站內的瀏覽活動等資料
使用範圍	與家樂福電信連結的網站，各自廣告主或連結網站，應有個別的隱私權保護政策。 -使用Cookie以紀錄及分析使用者行為。	-網路活動：可能會請使用者提供姓名或公司名稱、身份證字號或統一編號、電話號碼、email及住址等 -廣告連結服務：各自廣告主或連結網站，應有個別的隱私權保護政策。 -線上購物：在MKY官網進行線上購物，使用者仍受	-在活動時提供充分說明，自由選擇是否提供個人資料提供予本公司之優良商業夥伴或合作廠商 -可能提供其他網站的網路連結。 -使用Cookie以紀錄及分析使用者行為。	-僅供內部 -除非事先說明、或為完成提供服務或履行合約義務之必要、或依照相關法令規定或有權主管機關之命令或要求，否則不會將足以識別使用者身分的個人資料提供給第三人（包括境內及境外）、或移作蒐

		MKY 隱私權保護。 -為了提供其他服務或優惠權益，需要與第三者共用資料時，可以自由選擇 -為了讓系統能夠辨識使用者的資料，系統將以 Cookie 方式記錄使用者行為，並統計分析瀏覽模式		集目的以外之使用。 -PChomeTalk 網站也會讀取儲存在使用者電腦中的 cookie 資料
權利告知	-發現個人資料須修改時，經過身分確認無誤後，可透過本網站提供之服務管道來修改、更正	-隨時利用您的帳號和密碼更改您所輸入的任何個人或公司資料，惟，過往使用服務內容紀錄、交易資料等不在此更改範圍內	-發現個人資料須修改時，經過身分確認無誤後，您可透過本網站提供之服務管道來修改、更正	資料當事人可以請求查詢、閱覽本人的個人資料或要求給予複本。若發現資料不正確，可要求修改或更正。當蒐集之目的消失或期限屆滿時，可要求刪除、停止處理或利用。但執行職務或業務所必須者，不在此限。
業者義務	-因業務需要有必要委託第三者提供服務時，嚴格要求其遵守保密義務，並且採取必要檢查程序以確定其將確實遵守 -保存資料處理系統均已接受妥善的維護，並符合相關主管機關之要求並以保護措施防止未經授權人員之接觸。 -公司人員均接受過完整之資訊保密教育，如有違反保密義務者，將受相關法律及公司內部規定之處分。	-與客戶或交易有關的頁面均採用 https 加密方式進行，防制任何資料竊取行為。 -網路設有多層防火牆，可實質保護主機安全	-因業務需要有必要委託第三者提供服務時，嚴格要求其遵守保密義務，並且採取必要檢查程序以確定其將確實遵守 -保存資料處理系統均已接受妥善的維護，並符合相關主管機關之要求並以保護措施防止未經授權人員之接觸。 -公司人員均接受過完整之資訊保密教育，如有違反保密義務者，將受相關法律及公司內部規定之處分。	-以合於產業標準之合理技術及程序，維護個人資料之安全

第五節小結

我國目前個人資料保護之規範主要由憲法保障秘密通訊自由及隱私權之框架下，由立法者所制定之個人資料保護法加以規範之，惟考量電信事業與電信加值網路業所具備之特性，國家通訊傳播委員會依據電信法之授權，訂定法規命令以求規範之具體明確；同時亦不乏以行政指導之方式，提供業者在個人資料保護之領域作為之建議，期得同時兼顧產業發展之彈性與空間。

一、釋憲實務

依司法院釋字第 631 號解釋，通訊秘密在確保人民就通信之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵害之權利。而於同號解釋理由書更敘明：秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人私生活領域之免於國家、他人侵擾，及維護個人資料之自主控制，所不可或缺之基本權利。基此，通訊秘密內涵：通訊之有無、對象、時間、方式及內容等事項，應得先確認，且此所稱亦為維護個人資料之自主控制，得解釋為通訊秘密之保護同為個人資料之保護。

二、個人資料保護法

個人資料保護法屬我國個人資料保護法制之普通法，規範公務機關與非公務機關蒐集、處理及利用個人資料之程序與要件，令合理使用的同時兼顧個人資料之保護。

（一）個人資料之定義

個人資料保護法第 2 條第 1 款所定義之個人資料係指具備得直接或間接識別特定個人之資料皆屬之，其中又可再區分為一般個人資料，包括：姓名、出生年月日、職業等；以及特種個人資料，如：醫療、基因、前科紀錄等資料。就電信事業於營運過程中可能涉及之資料，若具備有上述所稱之直接或間接識別性，則當屬個人資料之類型，而應受個人資料保護法相關規範之拘束。然而，由於個人資料保護法第 6 條關於特種個人資料蒐集、處理及利用之規範至今尚未施行，亦導致在觸及特種資料運用時，其要件不甚明確之困境。

（二）蒐集、處理及利用之要件

我國個人資料保護法係參考經濟合作暨開發組織（OECD)所揭示之八大原則訂定個人資料蒐集、處理及利用之要件。個人資料保護法第 5 條揭示個人資料蒐集、處理或利用必須以誠實信用方法為之，且蒐集不得逾越特定目的之必要範圍及蒐集之範圍必須和目的具有正當合理之關連性，但為促進資料之合理利用，同時定有得為特定目的外利用之 6 種情形（個人資料保護法第 16 條及第 20 條第 1 項)。個人資料之蒐集、處理除需符合特定目的之要求外，為了確保人民知悉其個人資料被蒐集、處理及利用之情況（個人資料保護法第 8 條)，落實人民憲法上之資訊隱私權，「保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權」。

個人資料保護法第 21 條就非公務機關為國際傳輸個人資料之行為，授權中央目的事業主管機關得於涉及國家重大利益。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法規，致有損當事人權益之虞或是以迂迴方法向第三國（地區）傳輸個人資料規避個人資料保護法等情形時，限制國際傳輸個人資料，國家通訊傳播委員會即於 2012 年依當時電腦處理個人資料保護法第 24 條第 3 款（現行個人資料保護法第 21 條第 3 款）規定，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。另外，個人資料保護法第 27 條要求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，國家通訊傳播委員會即據此制定電信事業資訊通訊安全管理作業要點與電信事業資通安全管理手冊，確保電信事業資料、系統、設備及網路安全。

三、電信法及其相關法規

(一) 保護之個人資料

依電信法第 7 條規定：「電信事業或其服務人員、退職人員，對於電信之有無及其內容，應嚴守秘密。並授權主管機關訂定行政規則或作業程序，以保障通信祕密及規範當事人查詢相關個人通訊資料之程序。」此外通信紀錄依電信法第 2 條第 8 項規定係指: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(電話號碼或用戶識別碼)、通信日期、通信起訖時間等紀錄。

又，所謂「使用者資料」依電信事業處理有關機關(構)查詢電信使用者資料實

施辦法第 4 條訂為：電信使用者姓名.名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信事業務所填列之資料為限。

(二) 利用之要件

對「通信內容」除通信雙方當事人同意外，電信事業者應不得蒐集、處理之。而「通信紀錄」為通信時電信系統自動留存之資料，係將來用以計算電信費率之重要根據，為電信事業營運業務之目的而正當合法所蒐集、處理、利用之資料。應注意者為應第三人要求而提供之目的外利用，對此電信法本身並未為規定，而係依電信事業處理有關機關查詢電信通信紀錄實施辦法為規範。而依前開辦法第 3 條之規定，得要求提供之第三人為「有關機關」，然其與個人資料保護法中所稱公務機關或非公務機關間似缺乏明確區分；且其需符合法律程序，載明法訂定應記載事項，送該電話用戶所屬電信事業所指定之受理單位辦理。「使用者資料」依電信事業處理有關機關(構)查詢電信使用者資料實施辦法第 3 條，得要求提供之第三人為：司法機關、監察機關或治安機關；其他政府機關；以及與公眾生命安全有關之機關(構)。查詢要件則明訂為：(1)因偵查犯罪或調查證據所需，(2)因執行公權力所需，(3)為緊急救助所需；如為前(2)及(3)之請求者須敘明法律依據外，並備妥正式公文或電信使用者資料查詢單，載明應記明資料事項，送該電信使用者所屬電信事業指定之受理單位辦理。

(三) 資料之保存期限

通信紀錄依據行動通訊管理規則第 72 條之 1 之規定，相關通信紀錄應至少保存 6 個月以上。固定通信(俗稱之市內電話)紀錄之部分，依據固定通信業務管理規則第 49 條之 1 之規定，將其分為一般室內電話及長途電話等作不同之規範；前者依法至少必須保存 3 個月，後者則必須至少保存 6 個月以上。

網路通信紀錄之部分，依據第二類電信事業管理規則第 27 條之規定，將其分為語音單純轉售服務通信紀錄、網路電話服務通信紀錄、網際網路接取服務和虛擬行動網路服務通信紀錄等四大類型，各類型之保存期限皆有所不同，最長為 6 個月，最短則為 1 個月。

使用者資料保存期限，電信法對此並無明確之規範，惟依據國家通訊傳播委員會頒布之行動通訊業務管理規則第 73 條及固定通信業務管理規則第 49 條之 2 規定，電信事業經營者應核對及登錄使用者資料，並至少保存至服務契約終止後 1

年。

四、通訊保障及監察法

通保法保護之客體分作以下三類，一為通訊內容；其二為同法第 3 條之 1 規定之「通信紀錄」即電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電話號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄；另一則為通訊使用者資料。

關於通訊內容之監聽，其對象須為同法第 5 條第 1 項所訂各款犯罪之被告或嫌疑人，或同法第 7 條第 1 項之外國勢力、境外敵對勢力其工作人員之通訊。而對通信紀錄及通訊使用者資料之調取，則須為同法第 11 條第 1 項或第 2 項或第 3 項所訂之犯罪偵查。再得為蒐集或利用者限定為檢察官或司法警察，且須事前或事後依書面申請法院核發或補核發通訊監察書或調取票。而該當資訊之利用依同法第 2 條、第 10 條僅限於確保國家安全，維持社會秩序而調查犯罪證據之用，或國家安全預警情報之用。而依同法第 17 條，就通信監察之內容，除已供案件證據之用留存於該卷宗或為監察目的有必要長期留存外，由執行機關於監察通訊結束後，保存 5 年。

而就通信紀錄與使用者資料之調取，檢察官或司法警察原則上還是須向法院申請調取票，原則上亦採「令狀主義」，同樣限於特定犯罪調查之需（通訊保障及監察法第 11 條之 1）。另外同法第 11 條之 1 第 8 款是有關國家安全之必要調取外國勢力或境外敵對勢力之情報之例外。

觀察上述各個法規之規範內容，不難發現我國現行之個人資料法制乃以個人資料保護法作為普通法，而就電信事業可能涉及個人資料之類型及其運用要件，則以電信法及電信法所授權之相關法規中之相關規範作為特別規定，共同構築個人資料保護之法制框架。而就個人資料之界定與分類，除於個人資料保護法中得見個人資料之一般性定義外，電信法所授權訂定之第一類與第二類電信之相關業務管理規則中，則就其電信事業涉及之個人資料類型予以區分，其大致可區分為兩大類：其一為「使用者資料」（行動通訊業務管理規則、衛星通信業務管理規則）

或「用戶資料」(固定通信業務管理規則、第二類電信事業管理規則)[79]；另一則為「通信紀錄」，其蒐集、處理、利用之要件除應遵循個人資料保護法對於非公務機關之要求外，另外於電信法授權制定之各個法規命令中，再依據該等資料之特性分別予以規範，包括儲存、保存期限、提供第三人查詢之要件等。而 2014 年 1 月修正之通訊保障及監察法，於第 3 條之 1 定義通信紀錄與通訊使用者資料，並將通信紀錄之範圍予以擴充，納入「信箱」、「位置資料」等，與電信法第 2 條第 8 款所定義之通信紀錄有所差異，亦顯現出配合科技發展而蓬勃之位置資料的高度利用價值。觀察上述規範可知，我國目前個人資料法制就電信業及電信加值網路業涉及個人資料類型之用語與定義皆不甚一致，首先應配合科技發展，釐清可能涉及之個人資料類型，續就其名稱與定義制定一致性與明確性的規範，避免在蒐集、處理與利用要件判斷上可能產生之爭議，以及在適用法律解釋上有所出入之困境。

表 2-1 電信法及通保法中相關個人資料類型之界分及其運用要件

	電信法						通訊保障及監察法
	固定通信業務管理規則	行動通訊業務管理規則	無線寬頻接取業務管理規則	第三代行動通信業務管理規則	行動寬頻業務管理規則	衛星通信業務管理規則	

[79]「用戶資料」之用語為固定通信業務管理規則及第二類電信事業管理規則所採用，其包括姓名、國民身分證統一編號及國民身分證外之其他足資辨認身分之證明文件證號、地址及所指配號碼等資料；於外國人申請時，指護照號碼及護照外之其他足資辨認身分之證明文件證號；於法人申請時，指公司登記統一編號及代表人國民身分證統一編號。「使用者資料」則為行動通訊業務管理規則及衛星通信業務管理規則所使用之用語，其包括使用者、姓名、國民身分證統一編號及國民身分證外之其他足資辨認身分之證明文件證號、地址及所指配號碼等資料；於外國人申請時，指護照號碼及護照外之其他足資辨認身分之證明文件證號；於法人申請時，指公司登記統一編號及代表人國民身分證統一編號。自其內容觀之，似無太大之差異。

使用者資料/用戶資料	**第 49 條之 2** - 定義「用戶資料」 - 核對及登陸使用者資料，並載入系統資料檔。 - 至少保存至契約終止後 1 年 - 依法提供有關機關查詢	**第 73 條** - 定義「使用者資料」 - 核對及登陸使用者資料，並載入系統資料檔。 - 至少保存至契約終止後 1 年 - 依法提供有關機關查詢	**第 75 條** - 定義「使用者資料」 - 核對及登陸使用者資料，並載入系統資料檔 - 至少保存至契約終止後 1 年 - 依法提供有關機關查詢	**第 77 條** -定義「使用者資料」 -核對及登陸使用者資料，並載入系統資料檔 -至少保存至契約終止後 1 年 - 依法提供有關機關查詢	**第 77 條** --定義「使用者資料」 -核對及登陸使用者資料，並載入系統資料檔 -至少保存至契約終止 1 年 - 依法提供有關機關查詢	**第 53 條** -- 定義「使用者資料」 -核對及登陸使用者資料，並載入系統資料檔 -至少保存至契約終止 1 年 - 依法提供有關機關查詢	**第 3 條之 1** -定義：「通訊使用者資料」（第 2 項） **第 11 條之 1** -主體：檢、警、調 - 調取要件：最重本刑 3 年以上、與本案偵查有必要性與關連性、書面聲請該管法院核發調取票 -例外無須調取票之情形（第 3、8 項） -調取期間由法官酌定，但調取之資料未有保存期間規定(第 5 項)
通信紀錄	**第 49 條** -基於調查或蒐集證據之目的，依法提供查詢（適用通保	**第 72 條第 1 項** - 基於調查或蒐集證據之目的，依法提供查詢（適用	**第 74 條第 1 項** - 基於調查或蒐集證據之目的，依法提供查詢（適用	**第 75 條第 1 項** -基於調查或蒐集證據之目的，	**第 75 條第 1 項** - 基於調查或蒐集證據之目的，依法提	**第 52 條** -基於調查或蒐集證據之目的，依法提供查詢（適用通保法）	**第 3 條之 1** -定義：「通信紀錄」(第 1 項) **第 11 條之 1** -主體：檢、警、調 -調取要件：最重本刑 3 年以

	法） **第 49 條之 1** - 室內通信至少保存 3 個月；國際或國內長途通信至少保存 6 個月 - 應用戶本人申請提供查詢	通保法） **第 72 條之 1 第 2 項** - 至少保存 6 個月 - 應使用者本人申請提供查詢	通保法） **第 74 條第 5 項-**至少保存 6 個月 **第 74 條第 6 項** - 應使用者本人申請提供查詢	依法提供查詢（適用通保法） **第 76 條第 2 項** -至少保存 6 個月 - 應使用者本人申請提供查詢	供查詢（適用通保法） **第 76 條第 2 項** - 至少保存 6 個月 - 應使用者本人申請提供查詢	*未有保存期間規定	上、與本案偵查有必要性與關連性、書面聲請該管法院核發調取票 -例外無須調取票之情形（第 3、8 項） -調取期間由法官酌定，但調取之資料未有保存期間規定(第 5 項)
位置資料	無	無	無	無	無	無	**第 3 條之 1** -「位置資訊」:屬通信紀錄之類型（第 1 項） **第 11 條之 1** 主體、要件及其例外與通信紀錄相同

資料來源：本研究自行整理。

第三章　歐盟、德國、英國、日本、韓國及美國電信事業個人資料保護法制

第一節 歐盟

(一) 歐盟基本權利憲章

歐盟基本權利憲章（Charter of Fundamental Rights of the European Union）乃於2000年12月7日由歐洲聯盟(European Union，簡稱歐盟)各國元首於尼斯(Nizza)歐洲高峰會議中公布，分為前言及以下七章，共計54條條文，其延續歐盟憲法草案第二編第61-114條之內容，除得見生命、身體、尊嚴、平等、工作、財產、言論、集會、結社、居住、遷徙等廣受肯認之基本權利類型外，亦納入一些新興的基本權利類型。2009年12月1日里斯本條約生效，透過其中第6條第1項之規定，使歐盟基本權利憲章取得歐盟主要法源之地位，除了歐盟各公權力機關外，亦對於各會員國產生法的拘束力[80]。

綜觀歐盟基本權利憲章所明文規範之基本權利類型，其中第7條「尊重私人與家庭生活（Respect for private and family life）」與第8條「個人資料的保護（Protection of personal data）」應屬與本研究密切相關[81]。歐盟基本權利憲章第7條：「人人均有權要求尊重其私人與家庭生活、住居及通訊。」[82]被視為是實現人格自由發展下的重要權利樣態，其中對於通訊的尊重，狹義可理解為通訊過程中

[80]但英國及波蘭行使了條約中所賦予的退出選擇權，致使歐盟基本權利憲章在該國境內無拘束力。關於歐盟基本權利憲章的發展的階段歷程，請參考王服清，里斯本條約對歐盟組織與法律架構之影響與調整，憲政時代38卷2期，2012年10月，頁184-185。陳麗娟，里斯本條約後歐洲聯盟新面貌，五南，二版，2013年3月，頁18-20。黃舒芃，歐盟基本權利憲章對各會員國之拘束：由新近實務發展與理論爭議反思基本權利保障在歐盟的實踐途徑，歐洲聯盟法律專書研討會，臺灣歐洲聯盟中心，臺灣大學社會科學院第一會議室，2014年5月17日，頁27-28。Stein, Torsten/ von Buttlar, Christian, Völkerrecht, 12. Auflage, Köln 2009, Rn. 1065-1067.

[81]歐盟基本權利憲章第8條：「（第1項）所有人皆享有主張其個人資料保護之權利。（第2項）該個人資料之處理應本於誠信，在當事人同意或以法律作為正當基礎之情況下，作合於目的之使用，人人皆有權知悉關於其個人資料蒐集之情況，並得要求更正。（第3項）上述規範之遵循，應由獨立機構進行監督。」

[82]歐盟基本權利憲章第7條。

不被干擾的自由，即所謂秘密通訊自由；若進一步結合私人生活領域，則應可理解為隱私權之保障，而其保護範圍亦不僅侷限於通訊過程，甚至得擴張至家庭生活。承接此一尊重私人與家庭生活權利之揭示，歐盟基本權利憲章第 8 條開宗明義地明確賦予所有人皆享有主張其個人資料保護之基本權利；並針對個人資料之處理，要求應本於誠信，且僅有在獲得當事人同意或是法律有明確規範之情況下，方得為之，並不得逾越其目的，個人資料之主體就與其相關個人資料得主張之權利包括：知悉其被蒐集之相關資料，並得要求更正，而上述個人資料保護之規範是否確實踐履，歐盟基本權利憲章第 8 條第 3 項明訂應交由獨立機構進行監督[83]。

(二) 歐盟個人資料保護指令（95/46/EC）[84]

1、 規範架構

歐盟個人資料保護法制之濫觴，乃於 1995 年制定，1998 年末生效之「歐盟促進個人資料處理之自然人保護與資料流通指令（Directive 1995/46/EC of 24 October 1995 on protection of individuals with regard to the processing of personal data and on the free movement of such data）」，簡稱為「歐盟個人資料保護指令(95/46/EC)」[85]，其採框架式立法模式，要求歐盟各會員國應以其為基礎，修訂其個人資料保護立法，將相關規定內國法化（第 32 條），故觀諸現今歐盟各會員國中所適用之個人資料保護法制，皆為同中求異之續造結果。

歐盟個人資料保護指令共計七章 34 個條文，其規範架構為：一般性條款（第一章）；個人資料處理之一般性原則（第二章）；救濟、責任與制裁（第三章）；傳遞個人資料至第三國（第四章）；行為準則（第五章）；監督機構和工作小組對於個人資料處理過程中對個人之保障（第六章）；歐洲共同體實施措施（Community Implementing Measures)（第七章）。

2、 一般性規定

---

[83]Stein, Torsten/ von Buttlar, Christian, a.a.O.Fn80, Rn. 1065.歐盟基本權利憲章之中譯，請參考東吳人權教育網，歐洲聯盟基本權利憲章，http://www.hrp.scu.edu.tw/library/literature/entry.jsp?id=1236571265852-bdbe8a11-3085-4049-8168-2129a906421b（最後瀏覽日：2015 年 2 月 5 日）。

[84] Directive 1995/46/EC of 24 October 1995 on protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23/11/1995, 31-50)

[85]關於歐盟現行之個人資料保護指令(95/46/EC)之沿革與介紹，請參考許文義，個人資料保護法，三民，2001 年，頁 163-165。

歐盟個人資料保護指令第 1 條揭櫫其立法目的係為保障自然人之基本權與自由，建立一致性之隱私保護標準，調和各會員國關於隱私保護立法之分歧，一方面保障歐盟各會員國境內之個人資訊隱私權；另一方面，則致力於防止他人假借隱私保護之名妨害資料流通，一般性條款中同時就保護客體、適用主體及相關名詞定義等加以說明，其保護客體包括以自動化或非自動化方式處理之個人資料，且適用主體及於公、私部門，即歐盟個人資料保護指令之適用對象除了歐盟各會員國外，實際上資料控管者(Data Controller)亦同受其拘束。

歐盟個人資料保護指令於第 2 條中將「個人資料」與「處理個人資料」予以定義：所謂個人資料 (Personal Data)乃指可識別或足以識別個人相關之任何資訊，其中關於足以識別個人之資訊是指可以直接、間接透過該個人資料，特別是身體、生理、精神、經濟、文化或社會身份等特徵識別個人（第 2 條 2 段 A 項）；而個人資料之處理(Processing Personal Data)指對於個人資料之操作，不論是否以自動化的方式，包括蒐集、記錄、組織、儲存、改編、變更、檢索、諮詢、利用、傳輸的揭露、散佈、或使用之組合、封鎖、刪除或銷毀等（第 2 條 2 段Ｂ項）。

除此之外，歐盟個人資料保護指令對於個資處理過程中所涉及之相關人亦詳細條列，例如：資料控管者指自然人或法人、公家機關或機構、任何經控制者授權處理個人資料之人; 當處理個人資料的目的與意義是由國家或區域 (community)法律或法規決定者，資料控管者或提名資料控管者的特定條件可由國家或區域法律指定[86] ;資料處理者(Processor)指為資料控管者處理個人資料之自然人或法人、公家機關或機構以及任何其他組織[87];第三方(Third Party)指除了資料當事人、資料控管者、資料處理者跟受資料控管者與資料處理者直接管轄之人以外，任何自然人或法人、公家機關或機構、任何其他組織，經授權處理資料者[88];接收方(Recipient)指資料被揭露給一自然人或法人、公家機關或機構、任何其他組織，不管是否為第三方，不過，行政機關於受託進行個別調查獲得資訊之情況，非屬此處所界定之接收方[89]。但歐盟個人資料保護指令對於通聯記錄、位置資料、帳單資料等資訊，其並未多做著墨（主要規範於 2002 年歐盟電子通訊個資保護指令中）。

[86]Directive 1995/46/EC, Art.2(d).
[87]Directive 1995/46/EC, Art.2(e).
[88]Directive 1995/46/EC, Art.2(f).
[89]Directive 1995/46/EC, Art.2(g).

3、 處理個人資料之一般性原則

歐盟個人資料保護指令之基本原則規定於第二章中，大致可分為資料處理原則、資料當事人之權利和資料控管者之責任三大部分[90]。

(1) 資料處理相關原則[91]

資料處理原則方面，包括限制蒐集、資料內容完整、目的明確、限制利用等諸原則，另有敏感性資料妥善處理原則。

A. 資料品質原則

會員國必須立法規範關於個人資料之原則，以公平及合法地處理、以特定、明確且合法之目的蒐集，其處理必須適當、相關連且不超越目的範圍、該等資料必須確保正確且隨時更新以及以該個人資料所有人允許之形式保存（第 6 條）。

B. 依法處理資料原則

個人資料之處理時必須先符合特定要件，始得視為為合法，歐盟個人資料保護指令第 7 條以得個人明確同意、為履行契約之需要、為保護個人之重大利益、為維護公益或或為合法之利益，作為合法資料處理之前提設定。

C. 特殊種類個人資料的處理原則

歐盟個人資料保護指令第 8 條第 1 項規定有關種族及道德背景、政治意向、宗教或哲學信仰、工會歸屬、健康或性生活等皆屬於敏感資料，原則上禁止處理，例外僅得於第 8 條第 2 項所列舉之五種情形始得為之，包括資料當事人已明確同意對這些資料的處理，除非會員國的國內法規定在第 8 條第 1 項提及的禁止因素不因資料當事人之同意而有例外；為資料控管者行使或履行其在雇佣法規之權利或義務之必要；當資料當事人因實體或法律原因無法表示同意時，而為保護資料當事人或他人重大利益之必要者；資料處理是進行合法活動由基金會、協會或其他非營利組織為適當擔保，並以政治、哲學、宗教或工會為目標，且如資料處理僅僅與成員或與之目標相關有接觸的人，而該資料在未經資料當事人同意的情況

[90]蘇文萱、李科逸，產業研發投入智慧能源於隱私保護與資安因應建議-以歐盟動法制政策為研析，科技法律透析第 24 卷 12 期，2012 年 12 月，頁 48~62。

[91]European Union Agency for Fundamental Rights, *Handbook on European data protection law,* 61-101 (Jan. 2014).

下不向第三人揭露；資訊已經資料當事人公開或為對請求權（legal claims）建立、行使或抗辯之必要者。其第 2 項之例外為預防醫學、醫學診斷、照護之提供、健康服務之管理以及醫護從業人員（health professional）而依法有守密義務者。第 4 項規定會員國得於第 2 項以外，基於重要公共利益，以法律或主管機關之規則，增加豁免之規定。第 5 項規定犯罪，刑事處分或安全措施、行政罰、民事案件之判決等資訊之處理限於官方為之[92]。第 6 項規定依第 4、5 項而不適用第一項之情形應通知執委會。第 7 項規定會員國有權決定在何種條件下得允許就國民身分號碼（National Identification Number）或其他一般辨識方式（identifier ）進行處理[93]。

D. 告知當事人原則[94]

資料控管者應將資料控管人之身份、資料處理之目的、資料傳送之收受者、當事人不提供資料之後果及當事人查詢或更正資料之權利等，告知當事人[95]。第 11 條第 1 項規定，如果資料非當事人所提供而被資料控管者所使用，各會員國應告知當事人間接蒐集之情況，並確保公正的處理資料，除非當事人已知悉資料控制者身份、處理的目的或接收方身份等。但是，如果基於統計之目的; 歷史、科學研究之目的; 無法提供控管者資料; 提供該資料所須耗費之作業程序不符比例; 或已有法律明文規定須公開資料時，則上述第 1 項規定不適用[96]。

E. 其他

資料控管者應回應使用者對於違反個資保護規定之情形之投訴，並且與各國個人資料保護監督機構(National Data Protection Supervisory Authorities)合作[97]。

(2) 當事人之權利

---

[92] Foreign surveillance: law and practice in a global digital environment E.H.R.L.R. 2014, 3, 243-251, 244 -245.

[93]大法官釋字第 603 號解釋解釋文參照。

[94] Richard Jones&DalalTahri, An overview of EU data protection rules on use of data collected online, 27 Computer Law & Security Review 630, 632(2011), available at: http://ac.els-cdn.com/S0267364911001488/1-s2.0-S0267364911001488-main.pdf?_tid=5760a6ca-6356-11e4-9337-00000aacb35f&acdnat=1415018501_a2526288692b4593166b3136bd95a175 (last visited: Feb. 5, 2015).

[95]Directive 1995/46/EC, Art. 10

[96]Directive 1995/46/EC, Art. 11.

[97]歐盟執委會網頁公布資料控管者應盡之義務，請參見 http://ec.europa.eu/justice/data-protection/data-collection/obligations/index_en.htm（最後瀏覽日：2015 年 2 月 5 日）。

資料當事人之權利則包含明定資料處理者須向資料當事人提供資料控管者身份和處理目的等相關資訊 （第 10 條），資料當事人亦有取得個人資料之相關權利（第 12 條），並定有例外及限制之情況（第 13 條）。資料當事人對於自己個人資料之處理方式得提出異議，當事人得基於特殊情況之重大正當理由提出異議，異議有理由時，資料控管人應除去相關資料（第 14 條）。並賦予當事人得拒絕僅以自動化處理資料之方式，評定與其個別人格相關之事項，如工作表現、信用、可靠度、品行等，並據其做成對其具有法律效果或重大影響之決定（第 15 條）。

歐洲法院針對各會員國之政府機構提供個人資料查詢並收取費用之規範，認為 歐盟個人資料保護指令第 12 條第 a 項並未排除政府機構收取手續費用之可能性，但其不應收取超過此條款目的與所必要之費用[98]。因此，就其所受理當事人 X 因主張交通罰鍰寄送地址寄送錯誤而向政府機構請求將他於 2008 年到 2009 年的個人資料揭露，政府機構將經認證的謄本給予當事人 X 後，向其要求 12.5 歐費用之作為，認為並未違反歐盟個人資料保護指令之規範。

於 2013 年關於 歐盟個人資料保護指令第 13 條之爭議案件中，比利時房地產機構(Belgian Institute of Estate Agents) 依據私人偵探所提供之資料，主張停止有違法行為之房地產經紀人 Mr. Englebert 執行業務之權利，歐洲法院認為各會員國得選擇將第 13 條第 1 項所定之例外情況納入國內法中，限制當事人權利之行使，而比利時房地產機構聘請私人偵探調查房地產經紀人之行為，即可歸屬於歐盟個人資料保護指令第 13 條第 1 項所規定之例外情況之一[99]。

(3) 資料控管者之責任[100]

[98]C-486/12, Judgment of the Court Eighth Chamber (12 December 2012), available at: http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0486&lang1=en&type=TXT&ancre= (last visited: Feb. 5,. 2015).

[99]Institutprofessionnel des agentsimmobiliers (IPI) v Geoffrey Englebert, Case C‑473/12, Judgment of the Court Third Chamber (7 November 2013), available at: http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0473&lang1=en&type=TXT&ancre= (last visited: Feb. 5, 2015).

[100] Rebecca Wong, *Data protection: The future of privacy*, 27 Computer Law & Security Review 53, 56 (2011), available at: http://ac.els-cdn.com/S0267364910001718/1-s2.0-S0267364910001718-main.pdf?_tid=639d78dc-6356-11e4-b82f-00000aab0f02&acdnat=1415018521_bdd95424794e5baf446c9508d6d1e205 (last visited: Feb.

歐盟個人資料保護指令要求資料控管者須確保個人資料之機密性及安全性，要求受託處理資料者未經資料控制者指示，不得處理資料，法律有明定者不在此限（第 16 條）。資料控管者必須選任受託處理資料者，以確保資料處理的技術層面跟組織層面的執行，足以防範各種違法處理個人資料之情況發生。受託處理資料者必須受契約拘束，契約中須記載受託處理資料者僅在資料控管者指示下處理資料（第 17 條）。且為避免資料受到非法破獲、或偶然喪失、揭露、篡改、利用。資料控管者在對於個人資料進行自動化處理前亦須通知主管機關（第 18 條）。

(三) 歐盟電信通訊個資保護指令（2002/58/EG）[101]

1、 發展沿革

歐盟於 1997 年「電信事業處理個人資料及隱私保護指令」[102]中即已納入歐盟個人資料保護規範，然而，隨著科技的發展日新月異，歐盟個人資料保護之立法政策中，就網際網路之發展亦予以高度關注，其中就新興的科技服務，如：社群網站、雲端計算或手機位置等，應如何納入個人資料保護之體系中，即備受重視。故歐盟於 2002 年制頒「歐盟電信通訊中關於個人資料處理與隱私保護指令（Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector）」，簡稱「歐盟電信個資保護指令（Directive on Privacy and Electronic Communications ）」，取代「電信事業處理個人資料及隱私保護指令」，以因應電子通訊一日千里的發展趨勢[103]。其於制定理由中明確指出，現代資訊社會中所不可或缺的通訊網絡，帶來了個人資料與隱私權保護之難題，數位網絡提升了取得龐大數量個人資訊之能力以及利用這些資料的絕佳機會[104]，但這些數位服務之成功，卻必須取決於使用者的信賴[105]。

5, 2015).

[101]Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector (OJ L 201, 31/07/2002, 37-47).

[102]Directive 1997/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30/01/1998, 1-8).

[103]VagelisPapakonstantinou& Paul de Hert, *The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implentation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights*, 29 J. Marshall J. Computer & Info. L. 29 (2011), available at: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1698&context=jitpl.(last visited: Feb. 5, 2015)

[104] Emily Steel, *WPP's digital ad arm pushes into China*, Financial Times (last visited: Feb. 5, 2015). "Mobile phones send location information to network providers to enable calls to be forwarded, and to

因此，如何在當代科技不斷發展的同時，相應完善個人資料及隱私權之保障，乃為當前重要課題。

2、 規範架構

歐盟電信個資保護指令共計 21 個條文，歐盟電信個資保護指令著眼於基本權利之保護，特別是隱私權的保障，提供各會員國在規範電子通訊領域之個人資料保護時一致性之基礎，並期待藉此得達成資料有效、合理運用及流通之目的[106]。只要是在歐盟公開的通訊網路中以公開可近用的電子通訊服務處理個人資料的行為，應即遵循電信個資保護指令之規範[107]。提供公開可用之電信服務業者，負有採行技術及組織上之措施以維護其服務安全之義務[108]。會員國必須透過內國法確保利用公開通訊網路和公開可近用的電信服務所傳遞之訊息及與其相關交易資料的機密性[109]。

保障範圍含括歐盟境內利用公共通訊網路、封包交換網路與網際網路有關電子通訊服務之個人資料處理。保護客體及於自然人、法人之資料[110]，包含業者保留使用者連線紀錄檔(log files)的時間及使用限制、通訊資料、位置資料、帳單明細表、利用通訊設備濫發廣告(如電子郵件、行動簡訊等)的規範、來電顯示的規範、網路瀏覽歷程記錄（cookies）的合法用途等。歐盟電信個資保護指令適度補充 1995 年歐盟個人資料保護指令使其更為明確和完整，確保電信資料、設備、服務在歐盟自由流通，並將法人用戶(subscriber) 的合法利益涵括於保護範圍內（第 1 條第 2 項)。

歐盟電子通訊個資保護指令就電子通訊服務中之交易紀錄（第 6 條）、分項列舉帳單（第 7 條）、發話與受話者之來電顯示及拒示（第 8 條）、來電拒示之例外(第

enable location-based "value-added" services such as mapping and advertising. Social media apps running on these smartphones allow users to both explicitly and implicitly share information about themselves and those around them. Behavioral advertising companies track individuals across websites to show adverts targeted to their profiles. WPP already has built such profiles on 500 million individuals in North America, Europe and Australia".

[105] Directive 2002/58/EC，立法理由第 5 條。

[106]Directive 2002/58/EC，立法理由第 1 條。

[107]Directive 2002/58/EC，立法理由第 3 條 1 項。

[108]Directive 2002/58/EC，立法理由第 4 條第 1 項第 1 句。

[109]Directive 2002/58/EC，立法理由第 5 條第 1 項第 1 句。

[110]蘇三榮，網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，2009 年 6 月，頁 85 。

10 條)、定位資料（第 9 條）、自動轉接（第 11 條）、用戶名錄（第 12 條）以及未經請求之訊息（第 13 條）等事項予以規範，希望能讓使用者在享受電子通訊服務時，得免於隱私權受到侵犯之恐懼，確保其個人資料得以獲致充分的保障。

關於用戶名錄，歐洲法院認為，歐盟電子通訊個資保護指令第12條應該被解釋為國內立法須保證電信公司所出版之紙本或電子用戶名錄，在通知但未取得同意之情況下傳輸至其他第三方電信公司時，電信公司應保證如資料再經轉手，個人資料之用途不得超過當初第一次將用戶資料蒐集納入用戶目錄時之目的[111]。

3、 個人資料蒐集、處理、利用要件

(1) 使用者資料

歐盟電信個資保護指令第 2 條第 2 項中，將使用者(user)定義為任何使用公共可用之電子通訊服務於私人或商務用途之自然人，且並不以訂購該服務為必要。關於使用者的權益規範散見於歐盟電信通訊個資保護指令條文間，包括第 5 條 3 項（電子通訊網路資料存取使用）、第 9 條（位置資料）、第 10 條（終端機的設備必須在保護使用者資料下建構）。

另外，針對加值服務(value added service) 定義為除了通訊或帳單傳送需要以外，需要用到通訊資料或位置資料[112]的服務者[113]，其可能包含促銷方案、交通資訊、天氣預報或旅遊資訊等[114]。而究竟提供加值服務是否需要取得使用者之同意，依其被提供之服務性質是否能技術上、程序上、契約上判斷使用該服務之使用者而

[111]Deutsche Telekom AG v Bundesrepublik Deutschland, Case C-543/09, Judgment of the Court Third Chamber, (5 May 2011), available at: http://curia.europa.eu/juris/celex.jsf?celex=62009CJ0543&lang1=en&type=TXT&ancre=（last visited: Feb. 5, 2015）.

[112] Ian Brown, *The challenges to European data protection laws and principles, Working Paper No.1 for a "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, European Commission, 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_1_en.pdf. (last visited: Feb. 5, 2015) “The mobile phone sends location information to its network provider so that calls may be forwarded to the correct cell, and more recently to enable location-based services such as contextual advertising and mapping. Debit and credit card payment systems record amounts spent and stores visited… Even where users are not required to provide identifying information to services, logs can be linked to individuals through the Internet Protocol (IP) address of their computer, and often through digital “cookies” or electronic identifiers left on their browser by Web sites. Telephony and Internet Service Providers are required to retain some of this data for periods of up to two years for law enforcement access under the EU Data Retention Directive.”.

[113]Directive 2002/58/EC,Art. 2 (g).

[114] Directive 2002/58/EC，立法理由第 18 條。

定[115]。來電顯示與拒示的規定 (Presentation and restriction of calling and connected line identification)在第 8 條中規範，服務提供者(service provider)必須提供發話方使用者(calling users)與接話方之用戶(called subscribers) 選擇不顯示電話號碼的機會。除非有第 10 條例外之情況，例如：用戶申請追蹤惡意騷擾電話時，或在符合內國法情況下，業者為追蹤緊急求助電話時得在未取得用戶同意取得位置資料。

通訊的機密性規範在第 5 條，會員國應透過國內立法確保通訊跟有關的位置資料在公共通訊網絡的機密性。且應特別禁止在未經使用者同意，為監聽、監視、儲存或攔截使用者的通訊資料或位置資料的行為。除非在第 15 條 1 項合法授權的情況下始得為之。但如果為提供從事合法商業行為交易的證據時，則不在此限。另惟有在符合歐盟個人資料保護指令規定關於使用者明確取得處理資料的目的，且被提供拒絕的機會時才得儲存資料或取得終端設備裡的資訊。

於歐盟電信通訊個資保護指令(2002/58/EG)雖未明文對網路瀏覽歷程記錄規範，但於第5條3項中規定所有電子通訊網路在儲存或取得資料時，使用者或用戶必須被告知明確資料、瞭解個資處理目的和資料控管者須給予該用戶拒絕的權利要件下方得使用。垃圾電子郵件受歐盟電信通訊個資保護指令第13條1項規範，必須事先取得使用者同意。在同條4項中，則禁止在用電子郵件行銷時隱藏發信方資訊，使收件者無法提出停止寄送資訊的要求。如果自然人或法人已從顧客手上取得電子信箱聯絡資訊，則允許使用該電子信箱行銷相關產品或服務。

業者(provider)義務包括其提供的服務必須有適當的技術層面跟組織層面的保護，如果由危害網絡安全之風險存在時，業者應通知用戶說明該風險以及可能的救濟[116]。

(2) 通訊資料(Traffic Data)

歐盟電信個資保護指令就通訊資料予以規範[117]，第 2 條 2 項第 B 款定義其為：

---

115 Directive 2002/58/EC，立法理由第 31 條。

116 Directive 2002/58/EC,Art. 4.

117 Directive 2002/58/EC,Art. 6; Article 29 Data Protection Working Party, *Working Party 29 Opinion on the Use of Location Data with a View to Providing Value-Added Services*, 2005 2130/05 (WP 115) (EN), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf (last visited: Feb. 5, 2015); Raffaele Zallone, *Here, There and Everywhere: Mobility Data in the EU (Help Needed: Where is Privacy?)*, 30 Santa Clara High Tech.L.J. 57 (2014), available at: http://digitalcommons.law.scu.edu/chtlj/vol30/iss1/3(last visited: Feb. 5, 2015).

指以在電子通訊網路中通訊傳輸為目的、或為帳務目的而處理的資料而言，例如通話對象、持續時間、費率、經過的中繼點等。除了做為計費（billing）的依據外，通訊業者亦可藉由蒐集此類資料，分析個別使用者的使用習慣、偏好，供行銷之用[118]。當通訊傳輸的目的不再存續時，必須被刪除或匿名化處理。另為使用者帳務及互連費用所需的通訊資料，必須是在得對帳單提出異議或得為付款請求之期間內為限處理之。此外，為行銷電子通訊服務或提供加值服務之目的，若取得用或使用者的同意，通訊業者得在目的之必要範圍及期間內處理通訊資料，且亦應提供用或使用者撤銷同意之機會[119]。同時服務提供者須遵守規範告知之義務，告知用戶或使用者所處理的通訊資料之類型、為用戶帳務及互連費用之目的資料處理期間、及為行銷或加值服務目的，在取的同意前告知行銷必要的期間。此外，上述所為之處理，必須限制是公共通訊網路服務（或公共電子通訊服務）提供者所授權之人員，且為處理帳務、流量管理、客戶查詢、詐欺偵查、行銷電子通訊服務或提供加值服務目的之必要範圍內始得為之[120]。

關於通訊資料，歐洲法院於 2012 年 Josef Probst v. Mr.Nexnet GmbH 一案中[121], 援引歐盟電信個資保護指令第 6 條 2 項跟第 5 項規定，認為公共通信網絡(provider of public communications networks)與公共電子通傳服務提供者(publicly‑accessible electronic communications services)，應得將通訊資料傳遞給其代理人(assignee)以利其取得費用，且授權給代理人於特定情況下處理資料。但通訊資料必須經服務提供者授權後方得處理，且須於為取得費用目的之範圍內為之。代理人必須在服務提供者的指示與控制下處理通訊資料，而服務提供者應隨時確保代理人依據契約合法處理通訊資料。

(3) 位置資料(Location Data)

指在電子通訊網路中處理、得以表明公共電子通訊服務使用者的終端設備所在地理位置之資料而言（第 2 條 2 項第 C 款）。所謂的地理位置，除了包括精確的地

[118]章毓群，服務業科技應用之個人隱私權保護相關法制之研究，行政院經濟建設委員會，2004 年 12 月，頁 23。
[119]郭戎晉，前揭註 19，頁 34。
[120]章毓群，前揭註 118，頁 32.
[121]Josef Probst v mr.nexnet GmbH, Case C-119/12, Judgment of the Court Third Chamber (22 November 2012), available at: http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0119&lang1=en&type=TXT&ancre= (last visited: Feb, 5, 2015).

表經度、緯度之外，尚包括終端設備於特定時點所連接的基地台（network cell）。位置資料並不必準確地指出終端設備於特定時點所在的精確位置，即使僅能說明終端設備於特定時點的位置的大概範圍者亦屬之[122]。

而第 9 條另外指出「非通訊資料之位置資料」，針對公共通訊網路或公共電子通訊服務業者處理這類位置資料，要求僅得於匿名化後始得為之；或須取得使用者或用戶的同意[123]，在提供加值服務之必要範圍及期間內始得為之，且服務業者必須在取得同意前，告知用戶或使用者以下事項：將處理的位置資料種類、處理的用途及期間、為提供該加值服務，該資料是否會傳輸至第三者（第 9 條 1 項）。此外，在取得使用者或用戶處理位置資料之同意時，必須讓使用者及用戶有機會能隨時撤銷其先前之同意[124]，並得繼續以簡單且免費的方式，在每一網路連結或每一通訊傳輸時，暫時地拒絕位置資料的處理（第 9 條 2 項）。同樣地，第 9 條亦限制只有經通訊業者授權之人員，且必須為提供加值服務的必要範圍內，才能處理位置資料（第 9 條 3 項）[125]。

(4) 計費明細(Itemised Billing)[126]

計費明細為個人資料保護的一環，消費者因為確保其電話費用，往往可要求電信事業者在帳單上詳列其通訊明細；但也有消費者也會基於維護其通聯紀錄之隱私不被他人知情，而不希望帳單上有詳細的紀錄。由於目前電話通訊仍是基於線路交換（circuit-switch）技術，依單次連線時間計費；而在封包交換（packet-switch）

[122]Federal Trade Commission [FTC], Protecting Consumer Privacy in an Era of Rapid Change-Recommendations for Businesses and Policymakers (March 2012), p.33. “Data collection and Disposal Case Study: Mobile.”

[123] Anne S.Y. Cheung, *Location privacy: The challenges of mobile service devices*, 30 Computer Law & Security Review 41, 50 (2014), available at: http://ac.els-cdn.com/S026736491300201X/1-s2.0-S026736491300201X-main.pdf?_tid=2727ac60-6360-11e4-9833-00000aacb361&acdnat=1415022715_3fd722847fd921b0e23b554f406be0fe(last visited: Feb. 5, 2015)

[124] Nancy J. King &Pernille Wegener Jessen, *Profiling the mobile customer e Privacy concerns when behavioural advertisers target mobile phones e Part I*, 26 Computer Law & Security Review 455 (2010), available at: http://ac.els-cdn.com/S0267364910001044/1-s2.0-S0267364910001044-main.pdf?_tid=e0757a10-635d-11e4-9ce4-00000aab0f27&acdnat=1415021737_c4e551fcf9b821cbe9fa67b9d25c04cf (last visited: last visited: Feb. 5, 2015).

[125]章毓群，前揭註 118，頁 33。廖淑君，智慧聯網之發展與個人資訊隱私保護課題：以歐盟之因應為例，科技法律透析 23 卷 11 期，2011 年 11 月，頁 31。

[126]Directive 2002/58/EC,Art.7.

的通訊網路，其計費基準則是以資料傳輸量計算，或是以定期不限時間連線之方式計費，後者並無產出詳細通聯紀錄。於歐盟電信個資保護指令第 7 條中規定可見，用戶應有收到非計費明細帳單（non-itemised bills）的權利，且為了保護發話方使用者與接話方之用戶隱私權和取得條目化帳單的用戶的權利的一致，會員國必須適用國內法規定。例如確保有充足加強隱私權之通訊或繳費替代方案可供使用者與用戶選擇[127]。

(四) 歐盟個人資料保護基礎規則[128]

1、規範架構

為使歐盟各會員國能適用一致性之個人資料保護法規，歐盟執行委員會（European Commission）針對 1995 年之歐盟個人資料保護指令之基礎原則進行增修、調整，並因應現代科技發展推出「保護個人處理其個人資料及資料自由流通規則（Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data），簡稱「歐盟個資保護基礎規則」（General Data Protection Regulation)）草案，總共有 11 章 91 個條文，並於 2012 年 1 月正式向理事會提出；歐洲議會於 2013 年 10 月表決通過[129]，其若施行則將取代僅 34 條之歐盟個人資料保護指令[130]，其主要之革新包括：超過 250 人之公司必須設置資料監察人（Data Protection Officer); 拒絕人物側寫(Profiling)的權利; 被遺忘的權利 (The Right to be Forgotten); 資料使用之明示同意(Consent); 小孩的個人資料保護（Personal Data of Children)等。

歐盟個人資料保護基礎規則中規範包括基礎規則(第一章)；原則(第二章)、資料當事人之權利(第三章)；資料控管者與資料處理者之義務（第四章）; 個資傳輸

[127]Directive 2002/58/EC, Art.7(2).

[128]歐盟個資保護基礎規則之草案，請參見 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF（最後瀏覽日：2015 年 2 月 5 日）。

[129]歐盟個資保護基礎規則於歐洲議會通過之相關報導，請參見 http://www.heise.de/newsticker/meldung/EU-Parlament-gibt-gruenes-Licht-fuer-Datenschutzreform-1983124.html（最後瀏覽日：2015 年 2 月 5 日）。

[130] Paul M. Schwartz and Danie J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877, 885 (2014), available at: http://scholarship.law.berkeley.edu/californialawreview/vol102/iss4/7 (last visited: Feb. 5, 2015).

至第三國或組織之規定（第五章）；獨立監督機構(第六章)；合作與持續維護之機制（第七章）；救濟、責任與制裁（第八章）；有關於特種個資處理的規範（第九章）;授權條款與執行條款（第十章）；最終條款（第十一章）。

歐盟個人資料保護基礎規則之適用，在有專法另定時，則優先適用特別規定[131]。公務機關依本規則處理個人資料，若係以預防犯罪為目的，仍應受特別規定之拘束。

歐盟個人資料保護基礎規則之重要革新，包括確認資料保護為歐盟之基本權利類型; 當事人之權利特別是刪除權應予強化; 廣泛地禁止在未有法令基礎之情況下進行資料傳遞（尤其是國際傳輸）; 計費明細僅於獲得當事人明確同意時始得使用; 提高違反資料保護之罰責至公司營業額 5%（過昔: 2%); 非公務機關負有任命資料監察人之義務。

歐盟個人資料保護指令與個資保護基礎規則所保護之個人資料類別雖無太大的差異，但在個資保護基礎規則草案中有更詳盡、一致地規範下，各會員國的立法形成空間將受到限縮，在個人資料處理與資料自由流通之法制規範上，皆須受歐盟個資保護基礎規則之拘束，其對於歐盟個人資料保護法制之發展與革新，實具有里程碑之意義。而歐盟個人資料保護指令則將被歐盟個人資料保護基礎規則所取代(repealed)。但是歐盟執委會根據歐盟個人資料保護指令所做成的決定或是監督機關(supervisory authorities)根據歐盟個人資料保護指令所做出之授權則仍維持其效力[132]。

而歐盟個人資料保護基礎規則主要在規範處理個人資料時產生權利與自由保障的問題，而歐盟電信通訊個資保護指令則被賦予特定處理事項[133]，即歐盟個人資料保護指令主要是就歐盟個人資料保護為基礎性之規範；而歐盟電信通訊個資保護指令則是關注電信業之特性，將其適用範圍限於電信通訊領域之個資保護。一旦歐盟個人資料保護基礎規則通過，歐盟電信通訊個資保護指令即應做相應之修正與調整。

2、一般性規定

[131]歐盟個資保護基礎規則之草案立法理由，第 16 段。
[132]歐盟個資保護基礎規則之草案立法理由，第 134 段。
[133]歐盟個資保護基礎規則之草案立法理由，第 135 段。

第一條規定指出該規則的主旨跟歐盟個人資料保護指令相同，但是另外加上（a)小段。此規則確立有關於個人資料自由移動(free movement)的規範。在第 2、3 條更進一步的去規定該規則的實質範圍（material scope)跟地域性範圍（territorial scope）[134]。第 4 條則包含規則內術語的名詞定義。雖然有些定義和歐盟個人資料保護指令相同，但部分有變更、新增要件或是術語定義，例如基因相關資料(genetic data)、健康相關之資料、共同約束條款(binding corporate rules)、小孩(child)、監督機構等[135]。

3、處理個人資料之一般性原則

(1) 原則

歐盟個人資料保護基礎規則原則出現在第二章，從第 5 條到第 10 條詳細規範出原則大綱。歐盟個人資料保護基礎規則第五條列出處理個人資料有關且符合歐盟個人資料保護指令第 6 條的原則。新增加的原則為透明化原則(transparency principle)[136], 闡明資料最小化原則(data minimization principle)跟建立資料控管者的綜合的義務與責任。歐盟個人資料保護基礎規則第 6 條根據歐盟個人資料保護指令第 7 條的原則，列出合法處理資料的要件，並且更進一步規定利益衡量的要件與法律義務跟公共利益的遵循。第 7 條則闡明何時同意的要件被認為有效，而得取得合法原因(legal ground)進行合法資料處理。第 8 條更是進一步規範合法處理兒童個人資料的要件，在該資料得直接提供給兒童的社會的資訊服務時（information society services）。第九條也規範出何為一般禁止特別分類處理的個人資料跟一般禁止原則的例外，此條規定建立在歐盟個人資料保護指令第 8 條上。第 10 條闡明控管者沒有義務為了符合基礎規則的任何條款而取得額外的資訊。

(2) 當事人權利

---

[134] New EU data protection laws: European Parliament proposes restrictive data protection laws in Europe C.T.L.R. 2014, 20(2), 64.

[135] Paul De Hert&VagelisPapakonstantinou, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, 28 Computer Law & Security Review 130,132-33(2012), available at: http://ac.els-cdn.com/S0267364912000295/1-s2.0-S0267364912000295-main.pdf?_tid=9ff91b70-6355-11e4-9ce4-00000aab0f27&acdnat=1415018193_f63edad57f238d77af4e84aadc6edd02（last visited: Feb. 5, 2015).

[136]Federal Trade Commission [FTC], *supra* note122, p.60-67.

當事人的權利規範在歐盟個人資料保護基礎規則第三章，從第 11 條到第 21 條，分別分成五大類別，透明性與形態(Transparency and Modalities)、資訊與資料取得(Information and access to data)、更正與刪去(Rectification and Erasure)、反對的權利與分析(Right to Object and Profiling)、原則的限制(Restriction)。

第 11 條介紹控管者提供透明化、易取得並容易理解資料的義務，此條受到馬德里決議(Madrid Resolution on International Standards on the Protection of Personal Data and Privacy)[137]的影響。第 12 條規定控管者有義務提供實行個資主體權利的程序與機制，包括電子申請的方法、要求個資主體的請求必須於一定期間內回應與告知拒絕的原因。第 13 條規定提供接收方有關之權利，基於歐盟個人資料保護指令第 12 條 (c)項，此擴張到所有的接收方，包括合併的控管者(joint controllers)和處理者(processors)。

第二節資訊與資料取得中，第 14 條更進一步特定控管者對於個資主體的資料義務，建立於歐盟個人資料保護指令第 10 條和第 11 條上，要求提供關於個資主體的額外資料，包括儲存期間、提出申訴的權利和有關於國際移轉資料到最初的來源（in relation to international transfers and to the source from which the data are originating)，並亦保留在歐盟個人資料保護指令中克減(derogation)的可能性，例如：如果錄音或公開資料是法律所明示允許，則不會有任何義務。第 15 條提供個資主體取得個人資料權利，以歐盟個人資料保護指令第 12 條(a)項為基礎再加上新要件，例如通知個資主體儲存期間、更正與刪去資料、提出申訴的權利。

第三節規範更正與刪去的權利。第 16 條規定個資主體更正的權利，根據歐盟個人資料保護指令第 12 條(b)項。第 17 條提供個資主體被遺忘或刪去的權利[138]，包括使資料公開控管者的義務，在個資主體的請求下通知第三方刪去任何相關個人資料的資料本身、影本或複本。本條也整合了在特定情況下禁止處理資料的權

[137] International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy-The Madrid Solution* (Nov. 5, 2009), available at: http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf (last visited: Feb. 5, 2015)

[138] JefAusloos, *The 'Right to be Forgotten' e Worth remembering?*, 28 Computer Law & Security Review 143 (2012), available at: http://ac.els-cdn.com/S0267364912000246/1-s2.0-S0267364912000246-main.pdf?_tid=f6c43e6c-635f-11e4-97bb-00000aacb35d&acdnat=1415022636_861e31ad49273ad17f8e7d4e274b1e12 (last visited: Feb. 5, 2015).

利，且避免使用「阻擋(blocking)」等模糊不清的用語。第 18 條介紹了個資主體移轉資料的權利(right to data portability)，例如：將資料從一個資料處理系統移動到另一個系統，而不會被資料控管者阻止。做為一個前提，並且為了更加增進個體取得個人資料，本條提供個資主體有權利從資料控管者用有結構和普遍的電子格式取得資料。

第四節是反對的權利跟分析，主要規範為第 19、20 條。其提供個資主體反對的權利，建構在歐盟個人資料保護指令第 14 條上，但有些微的變更，包括舉證責任。第 20 條提到關於個資主體不被側寫的權利。此條將歐盟個人資料保護指令第 15 條第 1 項改變與增加保護，並受歐盟執委會對於人物側寫的建議。

第五節，最後一章則闡明歐盟或其會員被授權維持在第 5 條的限制原則跟個資主體權利，見於第 11、20 及 32 條。

(3) 資料控管者及受託處理資料者之責任

資料控管者的責任被規範在第四章，從第 22 條到第 34 條為範圍。主要分為控管者一般義務、資料安全、資料安全影響評估與授權（Data protection impact assessment and prior authorization）、資料監察人、行為準則與認證(Codes of conduct and certification)。

第 22 條主要描述控管者遵循個人資料保護基礎規則的責任義務，包括將基礎規則納入控管者內部政策跟機制，以確保有遵循基礎規則[139]。第 23 條點出控管者須透過制度設計或確保無違反達成資料保護原則的義務。例如：不論是被處理的資料量或是資料儲存時間，都必須透過機制確保只在有必要為特定目的的個人資料被處理，而且處理的資料沒有超過最小限度的必要或目的，被搜集或保留[140]。第 24 條討論共同控管人有關於內部關係跟個資主體關係人的義務。第 25 條規定非在歐盟成立的控管者但本基礎規則得適用控管者所為之活動時，在特定情況下得強制控管者在歐盟指定代表者。第 26 條澄清處理者的工作跟義務，並且增加新元素，如處理者處理超出控管者指示的資料時，可被認為是共同控管者。第 27 條

[139]Federal Trade Commission [FTC], *supra* note122, p.15, 22, 30. “privacy by design includes the collection limitation, data quality, and security principles.”

[140]Federal Trade Commission [FTC], *supra* note122, p.23, 26, 29. “Framework’s simplified choice and transparency components, discussed below, encompass…the purpose specification, use limitation, individual participation and openness.

討論處理者或任何聽從於控管者職權的人，除非有控管者指示不得處理資料，例外在非歐盟或其他會員國內國法要求下得處理。第 28 條介紹控管者跟處理者維持正在進行活動文件資料的義務，而非僅依歐盟個人資料保護指令第 18 條跟 19 條，一般的通知監督機關。第 29 條闡明控管者跟處理者在跟監督機關共同合作時的義務。包括在合理時間內回報監督機關，回報內容須包括施行的措施跟成效。

第二節則規範資料安全。第 30 條為給予控管者跟處理者義務執行適當的安全措施[141]。相較於歐盟個人資料保護指令，更多出當處理者跟控管者為契約無關事務時，處理者之義務。第 31 跟 32 條提出個人資料違反時之通知，此條亦可見於歐盟電信通訊個資保護指令第 4 條 3 項中。

第三節為資料保護影響評估跟事前授權，主要分為兩個部分：第 33 條介紹控管者跟處理者有義務在進行有風險操作前為資料保護影響評估義務；第 34 條則是在特定情況下控管者在執行操作前必須取得監督機關授權或向其咨詢，已確保有符合本基礎規則並減少對個資主體的傷害。例如將資料傳輸至第三國或國際組織時。

第四節包括第 35 條到第 37 條，其要求公務單位及大型私人企業應僱用資料監察人專責個人資料保護之事務，其具有獨立性[142]。第五節主要包括對於認證的規範，會員國與歐盟執委會應鼓勵個資認證機制的建立，以維持基礎規則的適用[143]。

資料傳輸至第三國或國際傳輸規定在在第 40 條到 45 條。個人資料傳輸僅得在歐盟執委會決定第三國有適當的保護時，方得進行。歐盟執委會考量的要件包括該國的法律或是否有監督機構的設置等。如歐盟執委會未作出決定時，資料控管者傳輸資料至第三國至少要有適當的防護(Transfers by way of appropriate safeguards)，包括共同約束條款或監督機關所立的標準個資保護條款。只有在第 44 條所列的情況下才得在沒有歐盟執委會確定有適當保護，或沒有適當防護的情況下免除義務，例外得傳輸資料至第三國。

[141]Federal Trade Commission [FTC], *supra* note122, p.24. “Data Security: Companies Must Provide Reasonable Security for Consumer Data.”
[142]歐盟個資保護基礎規則之草案，第 36 條第 2 段。
[143]歐盟個資保護基礎規則，第 39 條。

(五) 由新近歐洲法院判決觀察歐盟個人資料保護趨勢

1、 2014 年歐洲法院 C-293/12 與 C-594/12 判決

1. 背景

歐盟在歐盟第 2006/24/EG 指令制定前，並未針對通信資料之蒐集、處理與利用明文課與相關業者預先存取的義務，業者多是基於計算及收取費用之目的，依據契約蒐集並儲存用戶或使用者之個人資料與通信紀錄，同時受限於法律所定之保存期限，必須於目的消失後一定期間內予以銷毀。但隨著科技進步與網際網路之興起，通信資料成為掌握及分析人民行為的有效材料，尤其面對激進份子劇烈的攻擊行為，各國皆致力於尋找得避免類似事件再次發生的方法與措施，而主張以監控通信資料「預防」其成真的討論，亦在歐盟逐步地開展。

有鑑於自 2001 年起相繼於紐約、馬德里與倫敦發生激進份子攻擊而引發之緊張局勢[144]，歐洲議會於 2005 年底通過歐盟執委會提出之歐盟第 2006/24/EG 指令草案，作為對抗當前此情勢所必要之措施；歐洲理事會接續於隔年 2 月通過，並訂於 2006 年 3 月 15 日生效，並於指令第 15 條明訂各會員國至遲於 2007 年 9 月 15 日將其轉化為內國法令之義務，引發高度議論，當時歐盟 25 個會員國中，一共有 16 個會員國依據該指令第 15 條第 3 項聲明延遲執行。[145]

針對歐盟 2006/24/EG 指令之爭議，愛爾蘭高等法院（Irischer High Court）就愛爾蘭之公民團體-數位權利協會（IrischeGesellschaft Digital Rights）與其內國行政機關間，對於適用其國內預先存取資料規範產生之合法性爭議問題；另，奧地利憲法法院（Ö sterreichischerVerfassungsgerichtshof）亦合併受理多起憲法訴願，包括分別由 Kärntner 邦政府及由 Seitlinger 先生、Tschohl 先生與另外 11128 位聲請人共同提出，主張宣告其國內轉化歐盟 2006/24/EG 指令而制定之 2003 年奧地利電信法（Telekommunikationsgesetz 2003）第 102 條 a 無效之聲請，由於兩案涉及爭議均以釐清歐盟 2006/24/EG 指令之效力為先決條件，故皆裁定停止訴訟程序，送請歐

[144]西班牙馬德里於 2004 年 3 月 11 日發生一系列的火車炸彈攻擊事件，多輛開往馬德里之列車上被引爆炸彈，一共造成 191 人死亡，逾 2 千人受傷，此一事件發生後，歐洲理事會隨即委託歐盟執委會起草關於預先儲備通信資料（Vorratsdatenspeicherung）之法令。而 2005 年 7 月 7 日，於英國倫敦之地鐵再次發生連續多達 7 起的爆炸事件，由於正值早上交通尖峰時間，共造成 56 人死亡，傷者逾百，成為該指令通過、施行時程之助力。Vgl. Westphal, Dietrich, KommentarzuEuGH,Vorratsdatenspeicherung, Kommunikation&Recht 6（2014）, S.410-411.

[145]聲明延遲執行之國家分別為荷蘭、奧地利、愛沙尼亞、英國、賽普勒斯、希臘、盧森堡、斯洛文尼亞、瑞士、立陶宛、拉脫維亞、捷克、比利時、波蘭、芬蘭及德國。

洲法院為先決裁判（Vorabentscheidung），分別編列為 C-293/12 及 C-594/12 案，歐洲法院裁定將其合併審理，共同舉行言詞審理程序，並於 2014 年 4 月 8 日作成 C-293/12 及 C-594/12 判決[146] 。

2.法規架構

歐盟 2006/24/EG 指令共計 17 個條文，以下僅就其立法目的、會員國相應而生之義務與權力、預先存取資料之類型及其保存期間與監督機制等相關規範進行說明。觀諸歐盟 2006/24/EG 指令之立法理由及立法目的，其首先要求各會員國就其內國法規中關於課予公共電子通信服務提供者或公共通訊網路經營者（ AnbieteröffentlichzugänglicherelektronischerKommunikationsdiensteoderBetreibereinesöffentlichenKommunikationsnetzes，以下簡稱電信或網路業者）預先存取特定資料義務之規範，需與歐盟 2006/24/EG 指令取得一致性，以確保該特定資料得基於預防（Verhütung）、偵查（Ermittlung）、確認（Feststellung）及追訴（Verfolgung）重大犯罪，例如組織犯罪或恐怖主義（organisierteKriminalität und Terrorismus）時得提供運用。[147]

存取資料之類型依據歐盟 2006/24/EG 指令第 5 條第 1 項規定，包括以下 6 類：追蹤或辨別訊息來源之必要資料；確認受信方之必要資料；確認訊息傳遞之日期、時間與期間之必要資料；確認訊息傳遞類型之必要資料；確認終端或使用者預定終端的必要資料及確認行動通信設備位置所必要的資料，[148]基本上涵蓋所有有助

[146]Durner, Wolfgang, Anmerkung zu EuGH, Urteil vom 08. 04. 2014- C-293/12 und C-594/12, Deutsches Verwaltungsblatt 11 (2014), S.713-714.

[147]歐盟 2006/24/EG 指令第 1 條：「（第 1 項）本指令的目標在於使各會員國關於公眾電信服務業者及關於公眾通訊網路產生或傳輸的資料保存義務之規範一致化，以確保資料可供各國國內法定義下的重大犯罪偵查、確認及追訴目的之利用。（第 2 項）本指令適用在法人及自然人的通信資料與位置資料(Verkehrs- und Standortdaten)，並包括與之相關而為辨識使用者或用戶所必要的資料。但不適用於電子訊息交換之實質內容，包括藉由電子通訊網路所獲取之資訊。」及立法理由第 4、5、7 至 11、21、22 參照。

[148]歐盟 2006/24/EG 指令第 5 條：「(1) 在本指令下，會員國應確保下列目錄所列資料之保存：

a. 屬追蹤或辨別通訊來源必要的資料：

1. 固定通信或行動通信：

（i）電話號碼。（ii）用戶或使用者之姓名及地址。

2.網路、電子郵件及網路電話：

（i）登入之使用者身份。（ii）使用者身分及任何登入公共電話網路的號碼。（iii）用戶即使用者之姓名及 IP 位址，同時間通訊的使用者身分或電話號碼。

b. 確認受信方之必要資料：

1. 固定通信或行動通信：

於判斷誰、於何時、與誰進行通訊之資料，均列屬於應蒐集並存取之資料範圍，但於第 2 項中明文排除通信之內容及其衍伸之資訊。而被預先存取之資料，其保存期間依歐盟第 2006/24/EG 指令第 6 條之規定，自存取之時起算，至少 6 個月，最長 2 年。

為達成對抗重大犯罪之公益目的，歐盟 2006/24/EG 指令明確要求各會員國應採行相應措施，一方面確保業者依據本指令將相關資料預先存取，但以該資料乃於其職權範圍內透過電信或網路業者所提供通訊服務而產生或處理者為限，其存取應以得立即應申請將該資料及所有與其相關之必要資訊傳遞給專責機關之形式為之；[149]同時，歐盟第 2006/24/EG 指令第 4 條針對各會員國近用該預先存取資料之權力，規定「會員國應採取必要措施確保依據本指令預先存取之資料僅於特定情況且與內國法令相合致之情況下方得傳遞給各國專責機關。各會員國在同時關注歐盟相關法令或國際法規之決議，特別是歐洲人權法院（European Court of

---

（i）撥號號碼，使用加值服務，如轉接，其轉接之號碼。（ii）用戶或使用者之姓名及地址。

2.網路、電子郵件及網路電話：

（i）預期接收網路電話的使用者身分及電話號碼。（ii）用戶或使用者之姓名、地址及預期接收通訊的使用者身分。

c. 確認訊息傳遞之日期、時間與期間之必要資料：

1. 固定通信或行動通信：日期、通訊開始與結束時間。

2. 網路、電子郵件及網路電話：

（i）特定時區下登入登出網路之日期、時間、浮動或固定 IP 位址、登記用戶身分。（ii）特定時區下登入登出電子郵件或網路電話服務日期、時間。

d. 確認訊息傳遞類型之必要資料：

1. 固定通信或行動通信：使用的電話服務。

2. 網路、電子郵件及網路電話：使用的網路服務。

e.確認終端或使用者預定終端的必要資料：

1. 固定通信：電話號碼。

2. 行動通信：

（i）電話號碼。（ii）撥號方國際行動用戶識別碼（IMSI）。（iii）撥號方國際行動設備識別碼（IMEI）。（iv）接收方國際行動用戶識別碼（IMSI）。（v）接收方國際行動設備識別碼（IMEI）。（vi）在預付匿名服務情況：日期、第一次使用時間、方位。

3. 網路、電子郵件及網路電話：

（i）撥號方數據機之電話號碼。（ii）數位用戶迴路（DSL）或其它原始通訊終端。

f.確認行動通信設備位置所必要的資料：

1. 通訊開始的方位標籤（Cell ID）。

2. 通訊期間參考方位標籤（Cell ID）辨別地理位置的資料。

（2）涉及通訊內容的資料不能根據此指令保存。」中譯請參考蘇三榮，前揭註 110，頁 86-87。

[149]歐盟 2006/24/EG 指令第 3 條及第 8 條參照。

Human Rights, 簡稱 ECHR）對於歐洲人權公約（EMRK）所為解釋之情況下，可自行以內國法規範近用預先存取資料之程序與要件，但必須遵守必要性與比例原則之要求。」

歐盟第 2006/24/EG 指令第 7 條要求各會員國在不違背轉化歐盟 95/46/EG 指令與歐盟 2002/58/EG 指令所制定規範之情況下，應確保電信及網路業者至少應遵守下列資料安全原則：維持預先存取資料原有之品質並確保其與在網路上的資料受到同等安全與保護；應採行適當之技術與組織防免資料遭受意外或非法破壞、意外損失或改變、未經授權或非法之儲存、處理、揭露或散佈；應採行適當之技術與組織確保僅有被授權之人得近用；資料於保存期間經過後應銷毀，曾被檢索並保全的資料不在此限。並要求各會員國就維護資料安全所制定之法令，應設立一個或多個公法機構監督其於內國適用之狀況。上述監督權限得同時由歐盟 95/46/EG 指令第 28 條之監督機構行使，其監督應於全然之獨立（in völligerUnabhängigkeit）之情況下為之。[150]

3.歐洲法院之見解

歐洲法院於 C-293/12 及 C-594/12 判決[151]中指出透過歐盟 2006/24/EG 指令所定應預先存取之資料,將得以推估使用者或是當事人與誰透過何種方式進行通訊；通訊持續的時間及發訊地點；使用者或是當事人於特定期間內與特定人通訊之頻率。而上述資料經整合，將不難獲悉個人隱私生活之關鍵。歐洲法院因而認定，歐盟 2006/24/EG 指令所規範預先存取資料之義務及國家機關享有得近用上述資料之權力，對於歐盟基本權利憲章所保障之隱私權尊重及個人資料保護之基本權利確實帶來特別重大的侵害，且由於使用者或是當事人對此預先存取與後續之利用渾然不知，其很有可能引發私生活暴露在持續性監控之下的恐懼，因此歐盟立法者於此所享有之形成空間（Gestaltungsspielraum）應受到限縮，受到嚴格審查。

惟其亦認同基本權利並非不得以限制，歐盟 2006/24/EG 指令對於國家機關得以運用電信或網路業者預先存取之資料，其目的亦僅限於公益，即對抗重大犯罪及與其相關之公共安全之情況，應屬適當，且歐盟 2006/24/EG 指令實際上亦未允許存取通訊之相關內容，且亦要求電信及網路業者必須遵循資料保護及資料安全

[150]歐盟第 2006/24/EG 指令第 9 條參照。

[151]EuGH C-293/12 und C-594/12 vom 08.04.2014, Europäische Zeitschrift für Wirtschaftsrecht 12 (2014), S.459-464.

之特定原則。

然其對於可能招致系爭基本權利大規模且特別嚴重之侵害，卻缺乏將其範圍限縮於絕對必要情況（das absolutNotwendige）之相關規定：首先，歐盟 2006/24/EG 指令一體適用於所有人、所有通訊方式及所有通訊資料，並未依據其要對抗之重大犯罪目的作任何區別、限制或例外之規定；其次，其並未提供客觀之基準（objektivesKriterium），藉以衡平內國專責機關取得並利用該等資料之權力，反而是概括授權予各會員國自行界定「重大犯罪」之類型，且在內國權責機關近用該等資料及其後續利用之實質或程序之前提要件上留白，更缺乏透過法院或獨立機關建立事前審查之機制[152]；最後，歐盟 2006/24/EG 指令對於預先存取資料之保存期限，由 6 個月至 2 年不等，然卻未依據涉及之當事人或為達成目的可能使用之資料進一步區分資料類別，而定其保存期限。

另外，其允許電信事業者得依其基於經濟上考量所適用之安全水準，特別是針對執行安全措施所需費用，斟酌預先存取資料於保存期限過後是否採行不可回復之刪除。基此，歐洲法院認為，歐盟電信資料保存指令雖實際上符合客觀公益目的，但歐盟立法者並未提供充分的保證，該等資料得有效地排除被濫用的風險以及任何未經授權之近用，亦未提供客觀之理由，說明預先存取該等資料確實具有絕對的必要性，因而違反比例原則，而逾越了立法的界限，認定其違反歐盟基本權利憲章第 7 條之隱私權與第 8 條之個人資料保護之規定而屬無效。

（二）被遺忘權之行使：Google 搜尋引擎案

1. 概說

人民作為個人資料之主體，其所得主張傳統權利的類型，伴隨科技的發展與進步，其內涵應如何相應演進，透過歐洲法院於 2014 年 5 月 13 作成之 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González 案[153]判決，探討其中提出之「被遺忘權」在個資保護上的發展及其意涵。此判決

[152]歐盟基本權利憲章第 8 條第 3 項明文規定：「本條規定之遵行應由一獨立單位負責監督。」

[153]ECJGoogle Spain SL, Google Inc.vAgencia Española de Protección de Datos (AEPD), C-131/12, (13 May 2014), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN (last

認為搜尋引擎網路服務提供者須對其搜尋結果涉及由第三方發布於網路的個人資料負起責任，亦即歐盟民眾有權要求網路搜尋引擎業者封鎖該特定資料。

2. 歐洲法院 C-131/12 判決之見解

歐洲法院解釋，搜尋引擎網路服務自動、不斷且有系統地搜尋網路公開之資料，已屬歐盟個人資料保護指令[154]中「蒐集」之範圍[155]。法院認為搜尋引擎網路服務業者，有記錄、組織資料且儲存在伺服器裡，在此案以搜尋結果的方式公佈且使其它用戶得取得資料。這樣的行為在指令中被歸為明確地(expressly)和無條件(unconditionally)運作方式(operation)，必須歸類為“處理”(processing)資料的範圍內，因搜尋引擎網路服務業者處理個資與其他種類資料方式並無不同。歐盟個人資料保護指令提到運作的方式必須分類為處理，即使該資料已經在媒體中發行。如果在現行情況下普遍免除指令的適用，將會導致指令喪失其成立效果。

法院再進一步提出在指令中，搜尋引擎網路服務業者在“處理”的情況下，即屬控管者[156]。因搜尋引擎網路服務業者可以決定處理的目的與方式。法院認為，因為搜尋引擎的活動是網頁發行者所附加的，而且會重大影響基本隱私權和個人資料保護，搜尋引擎網路服務業者必須確保，在他責任、權力和能力下，他的活動符合指令的要件。這樣才能確保指令能夠發揮其效用，且達到個資主體隱私權的完整保護。

再討論搜尋引擎服務業的責任範圍，當連結是透過搜尋特定人名字所產生的搜尋結果時，法院認為業者在特定情況下有義務去移除第三方發佈之網頁連結。法院清楚指出這樣移除的義務在該名字或資料沒有事前或同時被消除，或即使該資料在網路發佈是合法的情況下亦可能存在。

法院認為如果不是透過搜尋引擎，個人資料在網路上無法或至少會非常困難取得，網路使用者也只能取得較不詳盡的個人簡歷。再者，因搜尋引擎在現代社

visited: Feb. 5, 2015).

[154] 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 (OJ 1995 L 281, p. 31).

[155] The right to privacy catches up with search engines: the unforgettable decision in Google Spain v AEPD C.T.L.R. 2014, 20(5), 131.

[156] To strive, to seek, to Google, to forget E.L. Rev. 2014, 39(3), 293

會中的重要性跟普遍性，個人權利侵害也會升高。這樣的干預，法院認為不能只因未搜尋引擎業者的資料處理有經濟利益而被正當化[157]。

但法院也認為在業者利益跟個資主體基本權利間應取的平衡，特別是隱私權和個人資料被保護的權利。雖然個資主體的利益在普遍原則下優於網路使用者的利益，但此平衡亦須考量公眾知的權利，此權利可能因個資主體在公眾的角色而有所不同。

法院最終回應如果在個資主體的請求下，發現包含個資主體資料的連結，在當下不符合指令規範，該聯結跟資訊必須被移除。即使該資料一開始符合法律被處理且為真實資訊，該比資料仍有可能因為時間使該資料處理方式不符合指令規範，或使該筆資訊不再適當、相關或超越原來目的。法院認為應檢驗，個資主體在請求當時，是否擁有權利請求跟他相關之資料不應在搜尋該名字時跟他名字有連結而出現在搜尋結果上。除非有特殊情況，例如因個資主體在公眾的角色可能會正當化大眾知的權利。

個資主體得對搜尋引擎網路服務業者請求移除連結，而業者收到請求後必須檢驗移除是否適當。如果業者拒絕移除其連結，個資主體得將該爭端提至監督機關或法院，針對爭端為必要的審查或命業者遵循特定措施。

因此在該案判決後,如果搜索人名而出現的搜尋結果包含被搜索人的個資時，個資主體(data subject)可以向搜尋引擎網路服務提供者請求移除該資料，且如服務提供者拒絕移除時，個資主體得在特定情況下向告知主管機關，以從網路搜尋結果中移除連結。

違反基礎規則基礎規則更包含了罰金[158]、罰鍰[159]相關規定。公司不遵守新的規則，可能會有大量的金錢損失並且造成市場競爭上的劣勢。因此想要在歐洲市場做生意的公司必須改善公司的規定以符合基礎規則。

3. 判決後之後續發展

[157]Google Spain and Google v AEPD (C-131/12) [2014] E.C.D.R. 16.at [80].
[158]歐盟個資保護基礎規則之草案，第 77、78 條。
[159]歐盟個資保護基礎規則之草案，第 79 條。

在判決出來後，有報導指出 Google 每天都會收到高達一萬封去除搜尋結果的要求[160]。在申請去除搜尋結果的網站上，Google 即表示：「當你做出移除搜尋結果的請求時，我們會考量到隱私權、大眾知的權利與散播資訊的權利。當我們在審核你的資料時，我們會看包含你過往資料的搜尋結果，包括是否有公共利益相關的資訊在內，例如我們會拒絕刪除金融詐騙、瀆職、刑事定罪等有關的資訊[161]」

從中可以看出被遺忘的權利，並非得漫無目的的主張。而 Google 也因為想配合判決、大眾知的權利跟眾多的申請中取得平衡，而成立了「專家委員會（expert advisory committee) ）」，成員包含了 Google 本身的執行長、法務長，聯合國特別報告員，維基百科共同創辦人等組成[162]。此委員會在資料被移除後再決定移除是否適當。資料只會在歐盟會員國家的 Google 網站上移除，因此與其說是完全被遺忘，真正的權利只是用戶在搜尋引擎搜尋時該筆資料不會再出現。但實際上該網頁在網路上仍然能夠被取得或找到。而歐洲法院也留給各會員國法院決定，究竟搜尋引擎是否能將足夠辨識某個體的方法，以結構化的(structured)資料呈現。此案的判決展開了大眾對隱私權、知的權利與表達權利的辯論。Google 主張他們用戶使用搜尋引擎只是運用他們在歐洲人權公約（European Convention on Human Rights）第 10 條言論自由，取得資料的權利。但歐洲法院在此案對此並無太多著墨。也無針對歐洲人權公約第 10 條和第 8 條隱私權適用的解釋。

而 Google 案判決出來的時間點與基礎規則草案修改的時間接近。基礎規則草案在第 17 條規範了具爭議的遺忘跟刪去的權利，雖大抵上與歐洲法院於本案的判決相同，但未來如果通過，如何在歐盟適用仍有許多探討空間。

六、小結

歐盟從 1995 年之歐盟個人資料保護指令便已開始對於個人資料保護採取積極

---

[160] A decision to quickly forget: Google Spain and Google on the right to be forgotten Ent. L.R. 2014, 25(7), 234.

[161] *SeeSearch removal request under data protection law in Europe*, Google, available at: https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en (last visited: Feb. 5, 2015) .

[162] Danny Sullivan, *How Google's New "Right To Be Forgotten" Form Works: An Explainer*, Search Engine Land (May 30, 2014), available at: http://searchengineland.com/google-right-to-be-forgotten-form-192837 ; James Vincent, *Google begins implementation of 'right to be forgotten' ruling with online takedown form*, The Independent (May 30, 2014), available at: http://www.independent.co.uk/life-style/gadgets-and-tech/google-begins-implementation-of-right-to-be-forgotten-ruling-with-online-takedown-form-9459209.html (last visited: Feb. 5, 2015).

的態度。更隨著時代的演進，確立個人資料保護作為歐盟基本權利之地位，並訂立新的指令，強化個人資料的保護。近年來對於歐盟資料保護基礎規則草案的熱切討論，即展現出歐盟對於個人資料法規在各會員國更全面化執行的目標，更與時俱進地發展出有別於 20 年前的歐盟個人資料保護指令的新原則與特色。

歐盟個人資料保護指令(95/46/EC)，其採框架式立法模式，要求歐盟各會員國應以其為基礎，修訂其個人資料保護立法，將相關規定內國法化。歐盟個人資料保護指令將個人資料 (Personal Data)定義為，可識別或足以識別個人相關之任何資訊。而個人資料之處理(Processing Personal Data)指對於個人資料之操作，不論是否以自動化的方式，廣泛的包括蒐集、記錄、組織、儲存、改編、變更、檢索、諮詢、利用、傳輸的揭露、散佈、或使用之組合、封鎖、刪除或銷毀等…。規範的主體包括資料處理者、第三方、接收方。

歐盟個人資料保護指令中主要可區分為基本的資料處理原則、當事人權利和資料控管者之責任三大部分。資料處理原則方面，包括限制蒐集、資料內容完整、目的明確、限制利用與告知當事人等諸原則。另有關於敏感性資料妥善處理原則，於指令第 8 條第 1 項規定有關種族及道德背景、政治意向、宗教或哲學信仰、工會歸屬、健康或性生活等皆屬於敏感資料，原則上禁止處理，例外僅得於第 8 條第 2 項所列舉之五種情形始得為之。資料當事人之權利則包含明定資料處理者須向資料當事人提供資料控管者身份和處理目的等相關資訊（第 10 條），資料當事人亦有取得個人資料之相關權利(第 12 條)，並定有例外及限制之情況(第 13 條)。資料當事人對於自己個人之資料處理方式得提出異議，當事人得基於特殊情況之重大正當理由提出異議，異議有理由時，資料控管人應除去相關資料（第 14 條）。歐盟個人資料保護指令要求資料控管者須確保個人資料之機密性及安全性，要求受託處理資料者未經資料控制者指示，不得處理資料，但法律有明定者不在此限（第 16 條）。

2002 年訂定之歐盟電信通訊個資保護指令中關於個人資料處理與隱私保護，相較於歐盟個人資料保護指令與歐盟個人資料保護基礎規則對於電信事業者的規範較為詳盡。歐盟電信個資保護指令適度補充 1995 年歐盟個人資料保護指令使其更為明確和完整。為確保電信資料、設備、服務在歐盟自由流通，該指令將法人用戶的合法利益涵括於保護範圍內（第 1 條第 2 項)。指令特別就電子通訊服務中之交易紀錄（第 6 條）、計費明細（第 7 條）、發話與受話者之來電顯示及拒示（第

8 條）、來電拒示之例外(第 10 條)、定位資料（第 9 條）、自動轉接（第 11 條）、用戶名錄（第 12 條）以及未經請求之訊息（第 13 條）等事項予以規範，希望能讓使用者在享受電子通訊服務時，得免於隱私權受到侵犯之恐懼，確保其個人資料得以獲致充分的保障。

另外，歐盟電信通訊個資保護指令亦特別針對加值服務做出定義，除了通訊或帳單傳送需要以外，需要用到通訊資料或位置資料的服務者，其可能包含促銷方案、交通資訊、天氣預報或旅遊資訊等情況皆可視為加值服務。而究竟提供加值服務是否需要取得使用者之同意，依其被提供之服務性質是否能技術上、程序上、契約上判斷使用該服務之使用者而定。來電顯示與拒示的規定在第 8 條中規範，服務提供者必須提供發話方使用者與接話方之用戶選擇不顯示電話號碼的機會。

歐盟電子通訊個資保護指令中對於通聯記錄、位置資料、帳單資料等予以定義。通訊資料，指以在電子通訊網路中通訊傳輸為目的、或為帳務目的而處理的資料而言，例如通話對象、持續時間、費率、經過的中繼點等。當通訊傳輸的目的不再存續時，必須被刪除或匿名化處理。另為使用者帳務及互連費用所需的通訊資料，必須是在得對帳單提出異議或得為付款請求之期間內為限處理之。此外，為行銷電子通訊服務或提供加值服務之目的，若取得用或使用者的同意，通訊業者得在目的之必要範圍及期間內處理通訊資料，且亦應提供用或使用者撤銷同意之機會。位置資料指在電子通訊網路中處理、得以表明公共電子通訊服務使用者的終端設備所在地理位置之資料而言。要求僅得於匿名化後始得為之；或須取得使用者或用戶的同意，在提供加值服務之必要範圍及期間內始得為之，且服務業者必須在取得同意前。除非有第 10 條例外之情況，例如：用戶申請追蹤惡意騷擾電話時，或在符合內國法情況下，業者為追蹤緊急求助電話時得在未取得用戶同意取得位置資料。但如果為提供從事合法商業行為交易的證據時，則不在此限。而在歐盟電信通訊個資保護指令第 7 條中可見計費明細之規定，用戶應有收到非計費明細帳單的權利，且為了保護發話方使用者與接話方之用戶隱私權和取得條目化帳單的用戶的權利的一致，會員國必須適用國內法規定。例如確保有充足加強隱私權之通訊或繳費替代方案可供使用者與用戶選擇。歐盟電信通訊個資保護指令雖未明文對網路瀏覽歷程記錄規範，但於第 5 條 3 項中規定所有電子通訊網路在儲存或取得資料時，使用者或用戶必須被告知明確資料、瞭解個資處理目的和資料控管者須給予該用戶拒絕的權利要件下方得使用。

為使歐盟各會員國能適用一致性之個人資料保護法規，歐盟刻正積極推動歐盟個人資料保護基礎規則完成立法程序。歐盟個人資料保護指令與個資保護基礎規則草案所保護之個人資料類別雖無太大的差異，但在個資保護基礎規則草案中有更詳盡、一致地規範下，各會員國的立法形成空間將受到限縮，在個人資料處理與資料自由流通之法制規範上，皆須受歐盟個資保護基礎規則之拘束，其對於歐盟個人資料保護法制之發展與革新，實具有里程碑之意義。歐盟個人資料保護基礎規則之重要革新，包括確認資料保護為歐盟之基本權利類型; 當事人之權利特別是刪除權應予強化;廣泛地禁止在未有法令基礎之情況下進行資料傳遞（尤其是國際傳輸）;提高違反資料保護之罰鍰上限; 非公務機關負有任命資料監察人之義務等。並於處理個人資料之一般性原則中新增透明化原則、闡明資料最小化原則跟建立資料控管者的綜合義務與責任。其中當事人權利可以分成下列類別：第一節，介紹控管者提供透明化、易取得並容易理解資料的義務。第二節資訊與資料取得中，第 14 條更進一步特定控管者對於個資主體的資料義務，要求提供關於個資主體的額外資料，包括儲存期間、提出申訴的權利和有關於國際移轉資料到最初的來源。第三節規範更正與刪去的權利。第 17 條提供個資主體被遺忘或刪去的權利，包括使資料公開控管者的義務，在個資主體的請求下通知第三方刪去任何相關個人資料的資料本身、影本或複本。第四節是反對的權利跟分析。資料控管者及受託處理資料者之責任，主要分為控管者一般義務、資料安全、資料安全影響評估與授權、資料監察人、行為準則與認證。包括第 35 條到第 37 條，其要求公務單位及大型私人企業應僱用資料監察人專責個人資料保護之事務，其具有獨立性。且會員國與歐盟執委會應鼓勵個資認證機制的建立，以維持基礎規則的適用。

歐盟對於個人資料之保護，其創新的規則與詳細的規定，對各國個資保障皆產生重大影響。透過本節對歐盟個人資料保護的概述，希望能供作我國個資保護規範參考。

表 3-1 歐盟個人資料保護指令(95/46/EC)

	個資處理之條件	利用目的之告知	利用目的之限制	個資分享
依據	第.7 條	第 10 條	第 6 條	第 14 條

一般個資	1.個資主體明確同意 2.或指令第 7 條(b)-(f)項規定之情況(e.g.公家機關賦予控制者的情況、控制者有法律上正當化利益處理資料)	控制者須提供個資主體: 控制者身分、利用目的告知或其他任何有必要之資訊(necessary), e.g.個資接收方身分、取得或改正個資的權利	明確、特定、合法的目的蒐集資料，並根據此目的處理資料	個資主體在個資被公開給第三方前，應被通知，且通知後有拒絕的權利
特殊種類個人資料	除非會員國法令禁止公布，處理個資須取得個資主體的明確同意	無	必要性, 指令第 8 條(a)-(e)項規定之情況 e.g.當個資主體無法給予同意時，為保護個資主體的重要利益	無

資料來源：本研究自行整理。

表 3-2 歐盟個資保護基礎規則草案之相關規範

	個資處理之條件	利用目的之告知	利用目的之限制	個資分享
依據	第 6 條	第 14 條	第 5 條	第 10 條
一般個資	1.個資主體明確同意 2.或指令第 6 條(b)-(f)項規定之情況(e.g.公家機關賦予控制者的情況、控制者有法律上正當化利益處理資料)	控制者須提供個資主體: 控制者身分、利用目的與個資被儲存時間之告知或其他任何有必要之資訊(necessary), e.g.個資接收方身分、取得或改正個資的權利	明確、特定、合法的目的蒐集資料，並根據此目的處理資料	個資主體在個資被公開給第三方前，應被通知
特殊種類個人資料	除非會員國法令禁止公布，處理	無特殊種類個人資料利用目的之告	第 9 條(a)-(j)事由	無特殊種類個人資料分享之

	個資須取得個資主體的明確同意	知		規定

資料來源：本研究自行整理。

表 3-3 歐盟電子通訊個資保護指令(2002/58/EG)特別規範

	電話行銷	電話號碼顯示	傳真行銷	電子郵件
依據	第 13 條	第 8 條	第 13 條	第 13 條
利用要件	預錄式行銷:須使用者事先同意(prior consent) 對話式行銷:須使用者事先同意	須提供用戶或使用者簡易且免費的方式取消顯示電話號碼之功能	須使用者事先同意	須使用者事先同意
利用目的	直接行銷(direct marketing)	無利用目的之規範	直接行銷	直接行銷
個資分享	未有個資分享相關規範	無個資分享相關規範	無個資分享相關規範	無個資分享相關規範
	計費明細	流量資料	位置資料	加值服務
依據	第 7 條	第 6 條	第 9 條	立法理由第 33 段
利用要件	1.使用者有權利收到沒有通訊履歷的帳單 2.會員國須確保國內法法規保障使用者收到通訊履歷有保障通話者隱私權，e.g.有增強隱私權保障或替代繳費方式	1.服務提供者必須告知使用者或用戶，流量資料的種類與使用期間 2. 流量資料作為行銷用途前，必須在取得使用者同意前告知資料的種類與使用期間	1. 位置資料限於匿名且取得使用者或用戶同意時，並符合提供加值服務的期間始得處理位置資料 2.服務提供者必須在取得使用者同意前告知，處理資料的種類、使用期間等。	1. 是否需要取得使用者之同意，依其被提供之服務性質是否能技術上、程序上、契約上判斷使用該服務之使用者而定 2. 加值服務的流量資料作為行銷用途時須事先取得同意
利用目的	無利用目的之規範	在計算使用者帳單資料允許處理流量資料，但限於繳費前或帳單可能有異議的期間內	限於提供加值服務的範圍內	加值服務於必要期間(necessary)得使用流量資料
個資	無個資分享相關	資料於必要範圍	資料於必要範圍	無個資分享相關

分享	規範	內，限於使用目相關之人始得處理之	內，限於使用目的相關之人始得處理之。且須於使用者同意前，事前告知是否分享資料給第三人	規範

資料來源：本研究自行整理。

第二節 德國

一、德國個人資料保護之法制基礎

德國個人資料保護法制實以德國基本法（Grundgesetz）所保障之秘密通訊自由與資訊自決權（Grundrecht auf informationelle Selbstbestimmung）為中心開展，並於法律位階尋求基本法中所揭示相關基本權保障之具體實踐：首先，制定德國聯邦個人資料保護法（Bundesdatenschutzgesetz,BDSG）作為個人資料保護之基準法[163]；另，重新整合或修訂特別法以因應特定領域個人資料保護之需求，包括：面對網路世代來臨，於 2007 年整併昔日電子媒體法（Teledienstegesetz）、電子服務個人資料保護法（Teledienstedatenschutzgesetz）以及關於媒體服務國家契約（Mediendienste- Staatsvertrag）之相關規範，制定現行之電子媒體法（Telemediengesetz, TMG）[164]；以及 2012 年就電信通訊法（Telekommunikationsgesetz，TKG）進行相關革新，一方面達成將歐盟相關指令轉換為內國法規範之要求；另一方面，藉此提供人民不落科技發展之後的個人資料保護[165]。以下即依據法位階之順序，由上而下依次介紹德國個人資料保護法制之框架。

(一)德國基本法

德國基本法中與個人資料之蒐集、處理、利用行為相關之基本權類型，首先，應得列出德國基本法第 10 條第 1 項所明訂之秘密通訊自由（Fernmeldegeheimnis），秘密通訊自由係保障通訊各方藉由通訊管道無形傳輸資訊之過程及其內容得免於公權力之干預，人民在通訊活動中的意見表達或資訊傳遞應得在不受公權力知悉之情況下進行，且其保障範圍亦應及於資訊或資料之處理程序，而得拘束任何公

[163]德國聯邦個人資料保護法最近一次的修正為 2009 年 8 月 14 日，並於同年 9 月 1 日起施行。關於德國聯邦個人資料保護法之沿革及其所揭示之重要個人資料保護原則，請參考許文義，前揭註 85，頁 171-176。

[164]Vgl. Tinnenfeld, Marie-Theres/ Buchner, Benedikt/ Petri, Thomas, Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Auflage, Oldenbourg Verlag München, 2012, S.387.Wolff, Heinrich Amadeus/ Brink, Stefan, Datenschutzrecht in Bund und die Ländern, 2013, S.202.

[165]Vgl. Simits, Spiros(Hrsg.), Bundesdatenschutzgesetz, 6. Auflage, Nomos Verlag, 2006, Einleitung Rn.93-102 . Tinnenfeld, Marie-Theres/ Buchner, Benedikt/ Petri, Thomas, a.a.O.Fn164, S.212-213.

權力對於因通訊而生資料或資訊之閱覽、紀錄與利用行為，其對於表意自由與人格發展具有重要的意涵。[166]

但秘密通訊自由之保障範圍並未及於所有與通訊行為相牽連之資料，例如電信事業以簽訂契約為目的所需之資料，此種配合電信服務所形成之用戶相關資料，即有進一步討論資訊自決權（informationelle Selbstbestimmung）於此適用之可能性[167]。資訊自決權之概念於 1983 年透過德國聯邦憲法法院於「人口普查判決（Volkszählungsurteil）」[168]加以確認，透過聯邦憲法法院的判決實務，以德國基本法第 2 條第 1 項之一般人格權，結合第 1 條第 1 項之人性尊嚴規定，[169]引導出資訊自決權之保障內涵：「自決權的概念乃是賦予個人就何時、於何種界限內公開其個人生活的內涵（Lebenssachverhalte），享有自我決定的權限。」[170]資訊自決權確保人民有權知悉關於國家如何以及蒐集了哪些個人資料與其利用的方式，其一方面乃作為國家蒐集與利用個人資料的權力的抗衡，更進一步要求國家應積極保護個人資料，防免其遭到他人不當利用，藉此維護個人人格得以自由型塑發展、意見得以充分表達發揮[171]。

而隨著科技的發展與進步，資料之蒐集與傳遞不再侷限於特定形式，在現代化資料處理模式下，個人資料被儲存及利用之型態更為多元，國家於此應加倍關

---

[166]Pieroth, Bodo/ Schlink, Bernhard, Grundrechte, Staatsrecht II, 24. Aufl., 2008, S.196-197. Manssen, Gerrit, Staatsrecht II Grundrechte, 5.Aufl., 2007, S.160.

[167]蔡宗珍，通信記錄強制提供義務之基本權關聯性：BVerfGE 125, 260 與 BVerfGE 130, 151 判決評析，第二屆翁岳生教授公法研討會：德國聯邦憲法法院 2010-2013 年重要判決之研究，臺灣大學法律學院公法研究中心主辦，2014 年 6 月 14 日，頁 12-14。謝碩駿譯，「預防性電信監察」判決（BVerfGE 113, 348），德國聯邦憲法法院裁判選輯（十四），司法院，2013 年 4 月，頁 12-14。

[168] BVerfGE 65, 1. Vgl. Bull, Hans-Peter, Informationelle Selbstbestimmung- Version oder Illusion, 2. Auflage, 2011, S.29-34. Bumke, Christian/Voßkuhle, Andreas, Casebook Verfassungsrecht, 5.Auflage, 2008, S.78-81. Pieroth, Bodo/ Schlink, Bernhard, a.a.O.Fn166, Rn.377b. 該判決之中譯請參考蕭文生譯，關於「1983 年人口普查法判決」，西德聯邦憲法法院裁判選輯（一），司法週刊雜誌社印，1990 年 10 月，頁 288-348。

[169]德國基本法第 2 條第 1 項：「每個人於不侵害他人權利或不抵觸憲政秩序或道德規範之範圍內，享有自由發展其人格的權利。」德國基本法第 1 條第 1 項：「人性尊嚴不得侵犯，尊重及保護此項尊嚴為所有國家權利之義務。」德國基本法翻譯請參考司法院大法官書記處編，德國聯邦憲法法院裁判選輯（十三），頁 381-435。

[170] BVerfGE 65, 1, 42. Vgl. Bull, Hans-Peter,a.a.O.Fn168, S.22-29. Bumke, Christian/Voßkuhle, Andreas, a.a.O.Fn168 , S.34. Pieroth, Bodo/ Schlink, Bernhard,a.a.O.Fn166, Rn.377b.

[171]德國聯邦憲法法院於 1983 年之「人口普查法判決」（BVerfGE 65, 1, 43）中指出：「在一個法律秩序中，人民若無法知道其個人資料被和人所知悉、何以被知悉、為何被知悉、以及在何種機會下被知悉，則此一社會秩序及其所賴以存在之法律秩序，將與資訊自決權之意旨未盡合致。」上述中譯請參考克理斯提安・史塔克（Christian Starck）著，楊子慧、林三欽、陳愛娥、張嫻安、李建良、許宗力、陳英鈐譯，法學、憲法法院審判權與基本權利，2006 年，元照，頁 425-426。

注「人民有權決定其個人資料之公開與運用」此一受基本法所捍衛之核心價值[172]，因此，當國家基於對其他法益的維護而需限制人民資訊自決權時，應具備重大公益（das überwiegende Allgemeininteresse）之考量，並以法律明確規範其限制之要件、範圍與方式，使人民充分瞭解，更應注意謹守比例原則[173]。

依據德國聯邦憲法法院於相關判決中所表示之見解[174]，電信相關資料所涉及之基本權保護領域，原則上可大致區分如下：電信事業者以建立、變更或終止契約為目的，或是契約內容之需所建立之主資料（Bestandsdaten）應屬資訊自決權之範疇；電信服務之基本資料，包括動態 IP 位址及其所屬使用者連結資料，乃資訊自決權之保障範圍，但排除浮動 IP 及其所分配之使用者連結資料；而通信資料則應受秘密通訊自由之保障[175]。

但德國聯邦憲法法院在秘密通訊自由與資訊自決權之選擇上，秘密通訊自由因相較於資訊自決權屬特別保障規定而往往得出應優先適用之結果，惟兩種基本權保障範圍之區劃界限並非十分清楚明確，也因此往往招致標準不一之批評[176]。

近年德國聯邦憲法法院更於判決中，針對網際網路的崛起與相應科技設備之發展，自一般人格權導出一新興之基本權類型：「保障資訊科技系統之秘密性與完整不可侵犯性之基本權（Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme）」，一般簡稱為「電腦基本權(Grundrecht auf Computerschutz)」，其保障範圍擴及使用所有資訊科技系統而產生、分析及儲存的所有資料，而並不僅侷限於個別的網路通訊過程，就基本權利主體因信任該系統之秘密性而交付資料，卻因系統遭第三人侵入或非法利用，致使資訊系統所承載之資訊、資料與應具備之功能受損，導致其完整性受到干預，將關注重心置於

[172]程明修，政府資訊蒐集與隱私權-以德國聯邦憲法法院「儲備性資料存取案」判決之發展為中心，「憲法解釋與隱私權之保障」司法院大法官一百年度學術研討會，司法院主辦，國立政治大學公共行政及企業管理教育中心協辦，2011 年 12 月 3 日，頁 22-24。

[173]Bumke, Christian/ Voßkuhle, Andreas, Casebook Verfassungsrecht, 5.Auflage, 2008, S. 80. Sodan, Helge(Hrsg.) , Grundgesetz Kommentar, S. 40.

[174] BVerfGE 113, 348; 125, 260; 130, 151. 相關判決之中譯請參考程明修，前揭註 172，頁 1-30。詹鎮榮譯，「電信通信記錄」判決，德國聯邦憲法法院裁判選輯（十一），司法院，2004 年 10 月，頁 247-271。蔡宗珍，前揭註 167，頁 1-25。

[175]德國聯邦憲法法院對於電信相關資料與基本權之對應關係，相關整理節錄自蔡宗珍，前揭註 167，頁 15。

[176] Vgl. Roßnagel, Alexander/ Moser-Knierim, Antonie/ Schweda, Sebastiasn, Interessenausgleich im Rahmen der Vorratsdatenspeicherung, 2013, S.100-104.

資訊系統使用過程不受干擾及該系統不被任意擷取之面向，應與資訊自決權之保障內涵有所不同，而特別予以保障[177]。

(二)德國聯邦個人資料保護法

為保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損，德國於 1977 年 1 月 27 日即制定「資料處理個人資料濫用防制法」(Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung)，簡稱「聯邦個人資料保護法」(Bundesdatenschutzgesetz)，並行之有年，最近一次修正日期為 2009 年 8 月 14 日。

1、 相關概念之界定

德國聯邦個人資料保護法第 1 條第 1 項明文揭示其立法目的「在於保護個人免於因個人資料之流通致其人格權（Persönlichkeitsrecht）遭受侵害」[178]，其同時拘束公務單位（öffentliche Stelle）與非公務單位（nicht-öffentliche Stelle）蒐集（Erhebung）、處理（Verarbeitung）與利用（Nutzung）[179]個人資料之行為，德國聯邦個人資料保護法將個人資料區分為一般個人資料（personenbezogene Daten）及特殊種類之個人資料（besondere Arten personenbezogene Daten），並分別予以界定：第 3 條第 1 項稱個人資料為關於一特定或可得特定人（即所謂當事人）其個人或事物關係中的所有細節內容（Einzelangaben über persönliche oder sachliche Verhältnisse）；同條第 9 項稱特殊種類之個人資料乃指與種族及道德出身背景、政治見解、宗教或哲學信仰、所屬工會、健康或性生活有關之內容，並就此種特殊類型個人資料之蒐集、處理、利用，於後續規範中設定較為嚴格之要件[180]。

---

[177]關於此一新興之「電腦基本權」之介紹與討論，Vgl. Jotzo,Florian, Der Schutz personenbezogener Daten in der Cloud, 2013, S.41-43.Wolff, Heinrich Amadeus/ Brink, Stefan, a.a.O.Fn164,S. 88-89.程明修，前揭註 172，頁 24。蔡宗珍，憲法人格權之保障及其界限-兼論網路人格權保護之憲法挑戰，第 9 屆憲法解釋之理論與實務學術研討會，中央研究院法律學研究所，2013 年 6 月 21、22 日，頁 21-23。

[178]相較於我國個人資料保護法第 1 條：「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」德國聯邦個人資料保護法之出發點相當明確地以「保障人格權」為主軸，與德國聯邦憲法法院在人口普查案判決中之觀點相互呼應，因此，即便後續之條文規範中，亦不乏「促進個人資料合理利用」之相關規定，但在解釋論上皆不應忘其所本，時時檢證是否屬符合「保障當事人人格權」宗旨之「合理利用」。

[179]蒐集，指取得當事人之資料；處理，至個人資料之儲存、變更、傳遞、封鎖與消除；利用，指與處理無關之任一使用個人資料之方式。上述定義請參見德國聯邦個人資料保護法第 3 條第 3 項第 4 項及第 5 項規定。

[180]例如：聯邦個人資料保護法第 4a 條第 3 項就涉及特種資料之蒐集、處理、利用，應明確告知其內容，並就此取得當事人同意；第 4d 條第 5 項第 1 款要求針對特種資料之自動化處理應於處理個

就個人資料之判斷標準，須具有得連結至特定人之特性時方屬個人資料，因此各式資料包括代替姓名之檔案號碼、E-Mail 地址、車牌號碼、地理資料（如 Google 街景拍攝）、IP 位址等，均須就個案情況為個別認定[181]。以 IP 位址以及浮動 IP 位址為例，德國聯邦憲法法院即於判決中強調隨著網際網路技術之發展，IP 位址能夠連結至使用者相關資訊之潛力亦不斷提升，與特定人連結之可能性亦大幅提升，而應認定屬個人資料之類型，而就個人資料之保護，立法者即負有持續關注並於必要時立法改善之義務。[182]

除了公務與非公務單位外，受託蒐集、處理、利用個人資料之個人或團體，同受德國聯邦個人資料保護法之拘束，並承擔該法所定之相關責任。而在選擇受託單位時，應特別注意其就個人資料保護所採行相應之技術與組織上防範措施。（德國聯邦個人資料保護法第 11 條第 1 項）其委託應以書面載明相關內容，[183]受託單位僅得於委託之範圍內蒐集、處理、利用個人資料，如認為有抵觸該法或其他個人資料保護相關法令之情況時，應立即通知委託人。（德國聯邦個人資料保護法第 11 條第 3 項）

2、 個人資料保護之基本原則

(1) 當事人同意原則（Verbot mit Erlaubnisvorbehalt）

蒐集、處理及利用個人資料之行為屬於原則上禁止，例外許可之情況必須以「本法或其他法令有明文規定」或是取得「當事人同意」為前提，此為德國聯邦個人資料保護法第 4 條第 1 項所明文揭示；基於當事人同意得進行資料蒐集，而有效之同意必須出自於當事人之自由決定，其知悉蒐集、處理、利用之目的，並於必要之個別情況或是應當事人要求，告知拒絕提供之結果，原則上同意以書面形式為之。（第 4 條 a）

個人資料之蒐集若非向當事人為之，如當事人未經其他方式獲知時，負責單位應告知當事人關於負責單位之身分；蒐集、處理、利用之目的；收受者之類型（Kategorien von Empfängern），但以當事人依個案情況無法確知者為限。

人資料前採行事先控管（Vorabkontrolle）程序。

[181]Plath, Kai-Uwe(Hrsg.), Bundesdatenschutzgesetz Kommentar zum BDSG sowie den Datenschutzbestimmungen des TMG und TKG, 2013, S.49-50.

[182]BVerfGE 130, 151, 199.

[183]聯邦個人資料保護法第 11 條第 2 項規定應記載之 10 款事項。

(2) 直接（向當事人）蒐集原則（Direkterhebung）

德國聯邦個人資料保護法第 4 條第 2 項規範資料以向當事人本人直接蒐集為原則，亦及個人資料之蒐集必須在當事人之協力（Mitwirkung）下為之，然而，在未有妨害當事人更高保護法益之論據存在時，得無須當事人同意，向其以外之人或單位進行資料蒐集，此特定情況包括：法令已為預先規範或是強行規定；欲達成之行政任務依其性質或目的而有向他人或單位蒐集資料之必要；向當事人蒐集將需耗費不合比例之費用。

(3) 資料節約原則（Datensparsamkeit）

針對資料之利用，應於必要範圍內為之，因此，資料不得作無限期之保存，亦及當其無留存之必要時，應即予刪除。[184]由於針對不同之資料類型往往訂有不同之保存時限，但其均應儘可能縮短於必要之時限內為保存。

(4) 資料縮減原則（Datenvermeidbarkeit）

個人資料之處理應隨時校準其目的，處理資料之範圍應儘可能縮減，而不應就所有能取得之資料一概為廣泛地蒐集與利用。

(5) 目的拘束原則（Zweckbindung）

資料之蒐集、處理、利用均應立基於特定目的，且該目的應於行為發動前即已確認，甚至予以記錄，而個人資料之蒐集、處理、利用之行為僅得於此事前所設定之原始目的下進行，例外情況下-即若事前取得當事人同意-則得為目的外之蒐集、處理、利用。

(6) 透明原則（Transparenz）

透明原則要求所有當事人均有權知悉其相關個人資料被蒐集之情況，包括：哪些資料、基於何種目的、被哪些單位、基於何種理由、將被儲存多長之時間，秘密的資料蒐集僅得於符合嚴格的例外要件下方被允許。該原則於德國聯邦個人資料保護法中透過資訊請求權之設計付諸具體實踐，例如：當事人得主張之查詢權、蒐集單位之告知義務等。[185]

[184]Jotzo,Florian, a.a.O.Fn177, S.45.
[185]Wolff, Heinrich Amadeus/ Brink, Stefan, a.a.O.Fn164, S.9-10.

(7) 必要性原則（Erforderlichkeit）

個人資料之蒐集需具有必要性，其判斷上主要要求蒐集之目的與手段間的平衡，亦即採行得達成目的中侵害最小之手段[186]。德國聯邦個人資料保護法將必要性原則作為限縮合法及合目的之資料處理範圍的要件，例如第 28 條第 1 項第 1 款所定基於履行民法上契約之義務；或是第 13 條第 1 項針對行政機關履行法定任務之規定，皆僅得於該具體處理資料屬達成目的之必要範圍內為之。[187]

3、 當事人之權利

面對資訊時代中個人資料被廣泛的蒐集，作為資料之主體，德國聯邦個人資料保護法相對賦予當事人得透過相關權利之主張，以求其平。

(1) 查詢權（Auskunftrecht）

當事人依據德國聯邦個人資料保護法第 34 條之規定，得向負責單位查詢下列資訊：已儲存關於其個人之資料，包括與該資料之來源相關者；資料傳遞對象（收受者）之類型；儲存之目的；並課予非公務單位應當事人之請求負有提供之義務，其答覆應以書面為之（第 6 項），且原則上無須付費（unentgeltlich），個人資料基於傳遞目的而為儲存時，例如相關單位為了信用調查業務而為之個資儲存，當事人一年內得為一次無償之查詢（第 8 項）。在特定情況下，通常是該答覆涉及保密法益之保護時，當事人之查詢權於此將被排除（第 7 項）。

(2) 異議權（Widerspruchrecht）

當事人在資料處理時應被告知享有異議權，一般情況下，當事人若有特別值得保護之利益，且其超越個人資料蒐集、處理、利用之利益時，則得行使異議權（德國聯邦個人資料保護法第 35 條第 5 項），而在市場、意見調查或是廣告之特殊情形，當事人之異議權無須具備理由（德國聯邦個人資料保護法第 28 條第 4 項）。蒐集、處理、利用個人資料之行為均應在事前有取得當事人明確同意之情況下為之，並應於一開始即告知當事人得隨時行使異議權。

(3) 更正、刪除及封鎖之權利（Anspruch auf Berichtigung, Löschung und Sperrung）

[186]必要性之判斷在德國聯邦個人資料保護法中亦多有標準上仍多有爭論，其往往會同時與資料縮減原則共同應用。Vgl.Jotzo,Florian, a.a.O.Fn177, 2013, S.45-46.

[187]Wolff, Heinrich Amadeus/ Brink, Stefan, a.a.O.Fn164, S.5-8.

德國聯邦個人資料保護法分別針對公務單位（第 20 條）與非公務單位（第 35 條）之蒐集、處理、利用個人資料行為，賦予當事人得主張更正（Berichtigung）、刪除（Löschung）或封鎖（Sperrung）之權利，德國聯邦個人資料保護法第 6 條並明文規定，此一權利之行使不得以法律行為排除或限制之。更正之要求乃針對儲存資料有瑕疵、過於陳舊、或是有誤的情形。而在面對個人資料被非法儲存；專責單位無法證明特種資料之正確性；資料已符合處理要件，因而無儲存之必要：以傳遞為目的而儲存之個人資料無繼續延長儲存之必要時，當事人得為刪除之請求（第 35 條第 2 項）。而雖未有上述情形，資料仍有可能於下列情況下被封鎖：包括與法令或是契約所定訂之保存期限不符之情況；刪除資料有可能造成當事人值得保護之法益受到侵害；或是消除資料可能需耗費不合比例之費用（第 35 條第 3 項）。

(4) 向監督機關申訴之權利（Anrufung der Aussichtsbehörden）

當事人若認定相關單位就其個人資料所採行之蒐集、處理、利用行為，已導致其人格權之侵害時，即得向個人資料保護之監督機關提出申訴。針對公務機關，其應向聯邦個人資料與資訊自由監察官提出（Bundesbeauftragte für Datenschutz und Informationsfreiheit）；而非公務機關則是向各邦之個人資料保護監察官（Landesdatenschutzbeauftragte）提出。

(5) 損害賠償請求權（Anspruch auf Schadenersatz）

德國聯邦個人資料保護法第 7 條[188]就不法或是不當之個人資料蒐集、處理、利用行為，賦予當事人得就其所造成之損害提請賠償，而專責單位亦應負損害賠償責任。

二、電信事業及網路業之個人資料保護規範

(一)電子媒體法（TMG）

1、 規範架構

電子媒體法（TMG）關注之焦點置於電子資訊與通訊服務，包括網路供應者

[188]德國聯邦個人資料保護法第 7 條：「專責單位為本法或其他資料保護法所不許可或不正確之個人資料蒐集、處理與利用而損害當事人者，該單位或其負責人對當事人應負損害賠償責任，但專責單位已依其情事盡必要之注意義務者，免賠償義務。」

的責任、商業電子郵件之一般性資訊義務以及在網際網路之個人資料保護，皆屬電信通訊法所含括之規範內容[189]。其適用於所有電子的資訊或是通訊服務，例如：部落格、搜尋引擎、電子報、房地產線上仲介服務及線上遊戲等，但排除電信法（TKG）第 3 條第 24 款所稱之「電信通訊（Telekommunikation）」、同條第 25 款所稱之「電信通訊之支援服務（telekommunikationsgestützte Dienste）」以及廣播國家契約（Rundfunkstaatsvertrag）第 2 條所稱之廣播（Rundfunk），因而排除例如網路電話、網路廣播或是特殊付費電話之適用。惟隨著智慧型手機逐漸普及，許多透過網路進行的活動，已難以清楚劃分，致生區分其適用範圍的困境[190]。

網路中之個人資料保護乃電子媒體法（TMG）中不可或缺之一環，其於第 4 節明確規範，開宗明義界定提供者與使用者[191]的關係（第 11 條），對職務或是工作關係中專門基於職業或是業務目的蒐集與利用電子媒體使用者之個人資料；以及公務單位或及非公務單位之間，或是其各自所屬內部單位專門為了工作或業務程序之控管而蒐集與利用電子媒體使用者之個人資料，均不適用電子媒體法第 4 節之相關規範。

電子媒體法第 6 條第 2 項針對垃圾電子郵件（Spam）規定：「如透過電子郵件寄發商業通信，信首及主旨不得掩飾或隱瞞寄件人及郵件訊息之商業本質。掩飾或隱瞞之行為尤指信首及主旨足使收件人於閱讀郵件內容前無法得知或被誤導寄件人之真實身分或信件訊息之商業本質。」並於同法第 16 條第 1 項明訂違反上述規定者，最高可處 5 萬歐元罰鍰。

電子媒體法第 12 條揭示服務提供者蒐集、處理與利用個人資料之基本原則[192]：強調服務提供者蒐集及利用個人資料或是變更利用個人資料之目的，僅得於本法或其他與電子媒體明確相關之法令所允許，或是使用者同意之情況下，方得為之。網路上之使用者同意亦應循聯邦個人資料保護法第 4 條 a 之規定行之，即：當事

[189]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.1066ff. Tinnenfeld, Marie-Theres/ Buchner, Benedikt/ Petri, Thomas, a.a.O.Fn164, S.403.

[190]Hoeren, Thomas, Das Telemediengesetz, NJW 12/2007, S. 802-803.

[191]使用者之定義，得見電信媒體法第 11 條第 2 項：「本節所稱使用者，乃指所有使用電信媒體之自然人，特別是為了獲取資訊或得近用之。」

[192]電子媒體法第 12 條：「服務提供者僅得於本法或其他與電信媒體明確相關之法令所允許，或是使用者同意之情況下，方得蒐集及利用個人資料（第 1 項）。變更目的使用個人資料，僅得於法律或其他與電信媒體明確相關之規範所允許或是使用者同意之情況下為之（第 2 項）。電信媒體法中之個人資料保護規範僅於無其他特定規範時方有其適用，即便資料非以自動化處理亦同（第 3 項）。」

人需出於自由意志；充分瞭解蒐集、處理及利用之目的與其拒絕同意之後果；依據書面形式，但亦得依電子媒體法第 13 條第 2、3 項之規定以電子形式為之。若電子媒體法中欠缺相關之個人資料保護規範，則將回歸適用聯邦個人資料保護法之規定。

承接上述原則之揭示，明定業者之義務於電子媒體法第 13 條，要求於蒐集及利用個人資料前，應以一般易懂之形式，告知當事人其方式、範圍與目的，以及有關其於歐盟 95/46/EG 指令適用範圍外之其他國家處理之情況；而較晚啟動使用者身份識別與個人資料蒐集與利用之自動化程序中，則應於程序開始前為告知，使用者對於告知之內容，必須得隨時調回查閱（第 1 項）。但隨著蒐集媒介之不同，告知之方式往往其區別，例如以網路為媒介者，多運用個人資料保護聲明（Datenschutzerklärung）為告知。

當事人之同意得以電子形式為之，當服務提供者確認：1. 使用者知悉其同意且明確表示者；2. 該同意有紀錄者；3. 使用者得隨時調整（abrufbar）同意之內容；4. 使用者未來得隨時使其同意發生撤回效力（第 2 項）。業者應於使用者同意前告知其依據第 13 條第 2 項第 4 款所享有之權利，第 1 項第 3 句準用之（第 3 項）。

業者應透過技術與組織之預防措施，確保：1. 使用者得隨時終止使用其服務；2. 開啟或其他使用過程中牽涉之個人資料，於使用結束後直接刪除或是於第 2 句之情況下封鎖；3.使用者得要求受到不被第三人辨識之保護；4.同一使用者透過使用不同電信媒體所涉及之個人資料得分開利用；5.第 15 條第 2 項所稱資料僅得基於帳單目的彙整；6. 第 15 條第 3 項所稱使用履歷不得與匿名主體之辨識說明進行彙整。第 1 句第 2 款所稱刪除之情況，在其與法令或契約所定訂之保存時限不符時，改以封鎖取代之（第 4 項）。轉遞予其他服務提供者之行為應像使用者揭示（第 5 項）。在技術可能或可期待之範圍內，服務提供者對於電信媒體之使用與其付款應以匿名或假名之方式為之。使用者應被告知此種可能性（第 6 項）。服務提供者依德國聯邦個人資料保護法第 34 條之規定，應使用者之請求，提供與其個人相關或儲存於其假名之下的資料之答覆。其答覆得據使用者要求以電子形式提供之。（第 7 項）

接續區分電子媒體服務中可能會涉及之個人資料類型，並進一步區分其蒐集、處理、利用之要件。電子媒體法於第 5 節定有罰責，對於違反相關個人資料保護

規範之行為，最高得處以 5 萬歐元之罰金（第 16 條第 3 項）。[193]

2、 涉及個人資料之類型

得見諸於電子媒體法之個人資料類別包括：主資料（Bestandsdaten）、使用資料（Nutzungsdaten）及帳單資料（Abrechnungsdaten）[194]。

(1) 主資料（電子媒體法第 14 條）

主資料乃指提供服務者和使用者間為了契約之成立、內容或是變更所需，且為使用電子媒體所必要之使用者個人資料，主資料之蒐集亦僅得基於此目的進行蒐集與利用（電子媒體法第 14 條第 1 項），主資料之處理強調必要性原則，電子媒體服務提供者必須是在提供其服務所必須之情況下方得進行主資料之處理[195]。但在例外的情況下，業者得應專責單位之要求，於各別情況下分別提供關於主資料之查詢，包括：為了犯罪追溯之目的；透過各邦警察機關達成危害防止；聯邦及各邦憲法保護機關法定任務之完成；聯邦情報機關、軍事防衛機構、聯邦犯罪防治局於其防禦國際恐怖主義之危害或是為確保智慧財產權所必要者（電子媒體法第 14 條第 2 項）。

(2) 使用資料（電子媒體法第 15 條第 1-3 項）

電子媒體法第 15 條第 1 項規範業者對於使用資料之蒐集與利用，僅得於為了使用或阻斷電子媒體所必要時為之，其包括：識別使用者身份之特；每次使用之始、終及其範圍之說明；關於使用者所使用之電子媒體之內容。為了計算帳單之目的所必要，業者得將同一使用者使用不同電子媒體之資料進行彙整（電子媒體法第 15 條第 2 項）。業者得基於廣告、市場調查或是形成電子媒體所需之目的，使用假名（Pseudonymen）製作使用履歷（Nutzungsprofil），透過使用履歷將彰顯使用者之各別資料，例如：IP 位址、使用特定服務之時間及期間等，並將此等資料共同彙整建立其彼此之間的關連性，[196]其必須以使用者未表達異議者為限方得為之，業者並應依第 13 條第 1 項向使用者傳達其享有之異議權。使用履歷不得與

[193]Tinnenfeld, Marie-Theres/ Buchner, Benedikt/ Petri, Thomas, a.a.O.Fn164 , S.391-396.

[194]電子媒體法並未明文規範位置資料之類型，電子媒體服務提供者若有蒐集與處理的情況，則應另依特別法，即電信法第 98 條之規定行之。Wolff, Heinrich Amadeus/ Brink, Stefan, a.a.O.Fn164, S. 202-203.

[195]Wolff, Heinrich Amadeus/ Brink, Stefan, a.a.O.Fn164, S. 207.

[196]Wolff, Heinrich Amadeus/ Brink, Stefan, a.a.O.Fn164, S. 208.

該假名所代表本人之個人資料進行整合。

(3) 帳單資料（電子媒體法第 15 條第 4-8 項）

電子媒體法第 15 條第 4 項明文規定，業者在使用過程終結後，僅得基於向使用者收取費用之目的，於必要範圍內利用使用資料，此即為帳單資料。為遵循現行法令或契約所規範之保存時限，服務提供者得封鎖資料。業者在告知費用及向使用者收取費用之必要範圍內，得將帳單資料傳遞予其他業者或第三人。業者若與第三人簽訂繳交費用之契約，則於達成此一目的之必要範圍內，其得將帳單資料傳遞予此第三人。基於其他業者市場調查目的而提供使用資料，僅得以匿名之方式為之（第 5 項）。

帳單中不得顯示使用者所選用特定電子媒體之提供者、時點、時程、方式、內容及頻率，除非使用者要求提供個別證明明細（Einzelnachweis）（第 6 項）。因此而進行處理之帳單資料，得自帳單寄送後保存至多 6 個月，若於此期限內對於帳單內容有異議或是未繳納費用，則其保存時限得延長至異議釐清或帳單繳納為止（第 7 項）。若業者透過事實上記錄之證據，認為特定使用者就其所提供之服務意圖規避費用或未完整繳納時，得再延長第 7 項所定處理期間，但以達成法律上追訴目的所必要者為限。且一旦上述延長之要件消滅或是該資料不再為法律追訴所需要，應即刻刪除該資料。在確知不會危及該措施所欲達成目的時，即應儘速告知所涉及之使用者（第 8 項）。

(二)電信通訊法（TKG）

1、 規範架構

電信通訊法（Telekommunikationsgesetz, TKG）第 7 章第 2 節（第 91-107 條）針對電信事業之個人資料保護予以專章規範。

電信服務業者之告知義務（Informationspflichten）明訂於電信通訊法第 93 條，要求電信服務業者應於契約結束時，告知其用戶（Teilnehmer）關於其個人資料蒐集與利用之形式、範圍、地點與目的，以一般可理解之形式使用戶知悉基本的資料處理要件，並同時告知用戶其享有之選擇或形成的可能性（Wahl- und Gestaltungsmöglichkeit）。使用者（Nutzer）應得自電信服務業者透過一般可近用之資訊得知個人資料蒐集與利用之狀況。德國聯邦個人資料保護法所規範查詢權之

行使不受影響。（第 1 項）電信服務業者在第 1 項所規範之告知義務外，對於有危及網絡安全風險存在之特殊情況時，應告知用戶此一風險，當該風險超越電信服務業者所得採取措施效力所及範圍時，應告知可能的協助包括可能因此而生之費用。（第 2 項）

以電子形式表達同意之要件與程序訂於電信通訊法第 94 條：同意得以電子形式為之，當服務提供者確認：1. 用戶或使用者知悉其同意且明確表示者；2. 該同意有紀錄者；3. 用戶或使用者得隨時取消（abrufbar）同意之內容；4. 用戶或使用者未來得隨時使其同意發生撤回效力。

在用戶不同意即無法或無其他可推知之方法可取得此電信服務時，不得藉由電信服務之提供連帶要求用戶同意將其資料轉作其他目的之利用，於此種情況下之同意屬無效（電信通訊法第 95 條第 4 項）。

2、 涉及個人資料之類型

得見諸於電信通訊法之個人資料類別應得大致區分為：主資料（Bestandsdaten）、通信資料（Verkehrsdaten）、位址資料（Standortdaten）與帳單資料（Abrechnungsdaten）等類型。

(1) 主資料（電信通訊法第 95 條）

電信通訊法第 3 條第 3 款所界定之「主資料」與電信通訊法之定義相同，乃指所有電信服務契約關係之成立、內容架構、變更或終止而予以蒐集之使用者資料。同法第 95 條第 1 項授權電信服務業者為達上述目的所必要之範圍內，得就主資料進行蒐集與利用。電信服務業者除自身用戶外，若與其他電信事業者存有契約關係，而為履約所必要時，其蒐集與利用之範圍得及於他電信服務業者所屬用戶之主資料。

電信通訊法第 95 條對於電信服務業者就主資料之運用加以規範，電信服務業者基於達成同法第 3 條第 3 項所稱目的所必要之範圍內，得蒐集與利用主資料。電信事業者與其他電信事業者簽訂契約之範圍內，得於履行契約所必要之範圍內，蒐集與利用其用戶或其他電信服務業者所屬用戶之主資料。將主資料轉遞與第三人僅得於用戶同意下行之（第 1 項）。

電信服務者僅得基於用戶諮詢、其自身優惠方案之廣告、市場調查及告知關

於其他使用者個別通話意願等目的之必要範圍內利用前項第 2 句所稱用戶之主資料，且需經用戶同意。電信服務業者基於存續中之顧客關係合法得知用戶之電話號碼或地址，包括電子的，其得依據第 1 句所稱目的利用該電話或地址，向其傳送文字或圖畫之通知，除非用戶對於此種利用已予拒絕。第 2 句中所規定利用電話號碼或地址之情況，僅得於符合下列要求時行之：用戶於其電話號碼或地址被蒐集或第一次儲存以及每次基於第 1 句所稱目的寄送訊息至該電話號碼或地址時，電信服務業者皆以明確可見且易於閱讀地方式提示，其得隨時以書面或電子之形式拒絕此一利用（第 2 項）。

電信服務業者應於契約關係結束之次曆年刪除主資料。德國聯邦個人資料保護法第 35 條第 3 項準用之（第 3 項）。

電信服務業者得附具理由於契約成立、變更或提供服務時，得於確認用戶所提供資料之必要範圍內，要求用戶人出具身份證明文件，並得影印留存，該影本應於確認用戶所提供資料後由電信服務業者立即銷毀（第 4 項）。

當用戶無其他或無可得預測之方式得以近用該電信服務時，電信服務業者即不得以用戶同意其資料得作為其他目的使用作為提供電信服務之前提。於此情況下所為之同意，無效（第 5 項）。

但應注意的是，透過德國聯邦憲法法院 1 BvR 1299/05 裁定[197]，確認了「雙門模式（Doppeltuerenmodell）」於電信通信法主資料查詢程序（Bestanddatenauskunftverfahren）中之應用，意即，電信通信法中規範電信服務業者蒐集、處理或利用個人資料之權限，並不當然代表其負有提供第三人查詢該資料之義務。上述資料之運用，均應由立法者明確立法訂定傳遞、提供查詢等之目的、要件及程序，作為請求之基礎。德國聯邦憲法法院透過此一判決強化個人資料傳遞之要件，資料之傳遞猶如穿越一道道門欄，每一次的穿越，皆應有其相應的「通關密語」，而此一通關密語，應由立法者加以把關，確保個人資料每一次的傳遞，皆受到充分之保障[198]。

(2) 通信資料（Verkehrsdaten）

[197]BVerfGE, 1 BvR 1299/05, vom 24. 1. 2012, http://www.bundesverfassungsgericht.de/entscheidungen/rs20120124_1bvr129905.html(最後瀏覽日期：2015 年 2 月 5 日)

[198]蔡宗珍，前揭註 167，頁 17-19。

電信通訊法第 96 條第 1 項授權電信服務業者得於達成電信通訊法本節規範目的所必要之範圍內，蒐集與利用下列 5 種通信資料：所涉連線與終端設備之號碼與識別碼、個人識別碼、使用客戶卡之卡號、通信卡號碼、行動裝置之通訊地點資料（第 1 款）；所有連線起迄日期與時間、與連線費用之結算相關之傳輸資料流量（第 2 款）；使用者所使用之電信服務（第 3 款）；固網連線之終端點、其起迄日期與時間、與連線費用之結算有關之傳輸資料流量（第 4 款）；其他為建立或維護通訊以及為結算費用所必要之通信資料（第 5 款）。

原則上電信服務業者應於連線結束後，立即依據第 96 條第 1 項第 3 句銷毀儲存之通信資料。惟有當該通信資料乃為達成同條項第 1 句所稱或其他法令所定目的或為建立其他連線必要者，不在此限。上述目的包括：結算用戶連線費用[199]；辨識、限定或排除通信設施之干擾或錯誤所必要[200]；答覆相關機關對撥打威脅或騷擾電話之電信使用者資料之查詢[201]等。電信服務業者僅得於達成其所定目的而必要之情況下，蒐集電信通訊法第 96 條第 1 項之下列通信資料：各種通訊設備之號碼與識別碼、通訊卡號碼、行動裝置之通訊地點資料；所有連線起迄日期與時間、與結算連線費用有關之傳輸資料流量；使用者所使用之電信服務；固網連線之終端點、起迄日期與時間、與結算連線費用有關之傳輸資料流量；其他為建立或維護通訊以為結算費用所必要之通信資料。

惟電信通訊法第 96 條第 1 項第 3 句所稱「立即」銷毀通信資料之期限判斷，目前實務上乃以「事實上的 7 天（de Facto sieben Tage）」為度，若非同法第 96 條第 1 項第 1 句所稱或其他法令所定目的或為建立其他連線必要者，應即於 7 天內銷毀，此一原則目前亦為德國聯邦最高法院所採[202]。

(3) 帳單資料

即電信服務業者基於估算與結清費用（Entgeltermittlung und Entgeltabrechnung）目的所需之資料，其並非全然獨立之資料類型，而實由上述主資料與通信資料交互組成，但考量其目的不同，故於蒐集、處理、利用之要件與保存時限上之規範

[199]電信通訊法第 97 條第 1 項第 1 句參照。
[200]電信通訊法第 100 條第 1 項參照。
[201]電信通訊法第 101 條第 1 項第 1 句參照。
[202]BGH- Entscheidung vom 13. Jan. 2011, III ZR 146/10.

亦為進一步之區別。[203]

電信通訊法第 97 條明文揭示:「電信服務業者得基於費用估計與結算之目的，利用其所需之通信資料。若電信服務業者將其服務委託給他公開電信網絡經營者時，其得傳遞於受託範圍內所蒐集之通信資料予電信服務業者。電信服務業者與第三人簽訂收款業務委託契約，則得於收款或建立詳細帳單所必要範圍內，將第 2 項所稱資料轉遞予該第三人（第 1 項）。

電信服務業者得基於違反秩序之調查及結算電信通訊服務費用之目的，以及為了證明其正確性，依據第 3 至 6 項之規定蒐集與利用下列個人資料：1. 第 96 條第 1 項所稱通信資料；2. 用戶或帳單收受人之地址、連線類型、在計畫費用結清之計費期間所產生之費用一致性、被通報之資料短缺、應繳納之所有費用；3. 其他對於費用結清具有重要性之狀態，如預先付款、於預定日付款、欠款、警告、已執行或延後斷線、已提出或處理中之賠償要求、已申請及經許可之延期附款、分期付款及提供擔保（第 2 項）。

電信服務業者於連線結束後即刻查明結清費用所需之第 96 條第 1 項第 1-3 及 5 款之通信資料。其得保存至帳單寄送後 6 個月。非結算費用所必要之資料應即刻刪除。若在第 2 句所規定之期限前，用戶對其帳單中所示連線費用提出異議者，則其保存期限得延長至該異議處理終結（第 3 項）。因此，帳單資料保存期限長短之判斷，仍應視其是否屬「結算費用所必要之資料」而定，若觀察德國電信服務業者所定一般服務條款中，多要求用戶需於收到帳單後 8 週內提出申訴，則上述資料是否有保存到「帳單寄送後 6 個月」之必要，即容有疑義。

若為了電信服務業者與其他電信服務業者或其用戶間，以及其他電信服務業者與其用戶間結清費用所必要之範圍內，電信使用者得利用通信資料（第 4 項）。

電信服務業者於帳單中收取第三人代收電信服務費用時，其得將主資料與通信資料傳遞予第三人，若在個別情況中第三人對用戶進行費用收繳所其必要者（第 5 項）。」

電信通訊法第 99 條第 1 項則讓用戶得要求提供其應付費之各筆通話明細，但僅有用戶在繳費期間以書面方式提出此一申請，電信服務業者方需告知其所儲存

[203]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S. 1140-1141.

之個別通話明細（Einzelverbingdungsnachweis），亦可依其請求一次告知選定通話之資料。其並進一步區分用戶申請提供之明細若及於整個家計單位、營業處所、機關及公法宗教團體時，必須以告知該明細涉及之所有相關人作為提供之前提要件。第 2 項規定通信明細中不得顯示匿名提供精神上或是社會緊急救助之人、機關或團體，或是其本身或其工作人員負有保密義務者。

(4) 位置資料（Standortdaten）

位置資料（Standortdaten）之相關規範見諸電信通訊法第 98 條，第 1 項中就位置資料之處理訂有一定要件，使用者透過公共電信網絡或是公開可近用之電信服務所產生之位置資料，僅得於準備加值服務（Diensten mit Zusatznutzen）所必要之範圍內，並於其所必要之時段內處理之，並以其為匿名顯示或使用者已對服務提供者就此加值服務予以同意時方得為之。於此所含括之資料並未限制其定位之型態或方式，因而透過行動網路進行登錄（Anmeldung）或是 GPS 定位及 WLAN 認證等所相應產生之位置資料，皆屬電信通訊法第 98 條所規範之對象。[204]

於此情況下，加值服務業者在每一次鎖定使用者位置之定位時，皆應發送電子訊息至該被鎖定之終端設備通知使用者，以避免有使用者與用戶並非同一人之情況。若該位置資料僅會於該終端機內顯示者則不在此限。位置資料之處理若涉及將手機之位址資料傳輸與使用者或非屬加值服務業者之第三人，則需依據同法第 94 條取得使用者對於加值服務業者明確、特別及書面之同意。第 2 句對於加值服務業者所課予之義務準用之。加值服務業者為履行第 2 句之義務，得利用於此範圍內必要之主資料。使用者就其同意應通知其他共用者。該同意得隨時撤回。

使用者已同意其位置資料之處理，必須繼續給予其得以簡易且不需付費之暫時拒絕於處理該資料時，對任意網路連結或任意轉遞訊息之機會（第 2 項）。

在連接撥打緊急電話 112 或 110，或是電話號碼 124 124 或 116 117 時，業者應確保位置資訊在個別情況或是經常性轉遞之可能性（第 3 項）。

依據第 1 項及第 2 項處理位置資料時必須限於準備加值服務所必要之範圍與人，即公共電信網絡或是公開可近用之電信服務經營者所授權之人，或是提供電信加值服務之第三人（第 4 項）。

[204]Wolff, Heinrich Amadeus/ Brink, Stefan, a.a.O.Fn164, S. 216-217.

3、 個人資料之蒐集、處理、利用要件

(1)辨識、限定或排除通信設施之干擾

電信通訊法第 100 條電信服務業者為辨識、限定或排除電信通訊設施之干擾或錯誤所必要，得蒐集與利用主資料與用戶及使用者之通信資料（第 1 項）。電信通訊設施之經營者或是其監察人在為了執行開閉，以及辨識及限定網絡中的干擾在其企業所必要之範圍內，得侵入現有之通訊連結。在此過程中所產生之記錄應即刻銷毀並必須透過聲音或其他符號之顯示,明確通知該通訊連結之所有使用者。若技術上不可行者，應立即通知該企業之資料保護監察人關於程序與其採行之各個個別措施情況的細節，該資訊將由資料保護監察人保存兩年（第 2 項）。

當已有記錄之事實上證據顯示該情況涉及電信通訊網絡或服務之不法利用時，特別是迂迴線路（Leistungserschleichung）或是詐欺（Betrug）的情形，電信服務業者為確保其費用之請求，得利用主資料與通信資料，但限於揭露或防範電信通訊網絡或服務之不法利用所必要之範內為之（第 3 項）。

在第 3 項第 1 句之前提下，電信服務業者得於個別情況中蒐集與利用控制信號（Steuersignal），若其對於釐清與防範其中所表示之行為有迫切性者。但不得蒐集與利用其他訊息內容。其依第 1 句所採行之各個措施應知會聯邦網路局（Bundesnetzagentur）。一旦無危及該措施欲達成目的之可能性時，應通知相關人（第 4 項）。

(2)威脅或騷擾電話之揭露

電信通訊法第 101 條規定，若用戶於一文件程序中確鑿地（schlüssig）聲明於其線路中有接獲威脅或騷擾電話（bedrohende oder belästigende Anrufe）之情況，電信服務業者應據書面申請或跨網訊息（netzübergreifende Auskunft）告知其該線路之持有者，即撥話發送方。該答覆僅限於申請後所進行之撥話。其得蒐集與利用線路持有者之姓名、住址及電話號碼；連結或嘗試連結之日期、時間，並得將此資訊告知其用戶。但對於僅針對特定使用者提供封閉式服務之電信服務業者不在此限（第 1 項）。

電信通訊法第 101 條第 3 項說明所謂跨網絡訊息之情況，乃指於連結中協力之其他電信服務業者，當其掌握有相關資料時，負有告知被威脅或騷擾之用戶所

屬電信服務業者必要信息之義務。

電信服務提供者對於其用戶所擁有之線路被作為發送威脅或騷擾電話者，若已將相關訊息提供予他用戶時，即應予以通知[205]。惟若經申請人書面確切地說明，將可能因此受有極大之不利益，且經衡量後認為其較值得保護者，則不予通知。對於持有發送威脅或騷擾電話線路之用戶，若經由其他方式得知此訊息，則即應據其請求告知（第 4 項）。

(3)來電顯示與拒示（Rufnummeranzeige und-unterdrückung）

電信通訊法第 102 條，電信服務業者得提供來電號碼之顯示，但應給予收發話之雙方皆有以簡易之方式免費選擇持續性或個別性拒絕顯示號碼之機會。收話者必須有以簡易且免費之方式拒絕由發話者設定為拒示號碼來電之機會(第 1 項)。但廣告電話之發話方不得隱藏來電號碼，且應確保告知收話方其來電號碼（第 2 項)。上述兩項不適用於僅提供屬封閉式使用群體之用戶服務之電信事業者。只要收、發話之一方在國內，即有第 1-3 項之適用（第 7 項)。電信服務業者在緊急電話 112 或 110 或 124 124 撥號之連接應確保發話方無論是持續性或個別性拒示號碼功能之關閉（第 8 項)。

(4)自動來電轉接（Automatische Anrufweiterschaltung）

電信通訊法第 103 條課予電信服務業者義務，給予其用戶以簡易且免費之方式關閉由第三人設定自動轉接至其終端機之機會，但僅提供封閉式使用族群之用戶服務的業者不在此限。

(5) 用戶名冊之登錄（Teilnehmerverzeichnisse）

電信通訊法第 104 條，用戶得申請將其姓名、住址及其他附加說明如：職業、行業、及連線型態，登錄於公開之電子或紙本之使用者名冊。用戶得自行決定於此名冊中公開哪些說明。應用戶之請求得將共用者一同登錄，但須取得其同意。

(6) 答覆查詢（Auskunfterteilung）

電信通訊法第 105 條，關於用戶名冊中登錄之電話號碼得於遵守第 104 條及第 105 條第、3 項之限制下提供查詢（第 1 項)。答覆關於用戶號碼之查詢僅得以

[205]電信法第 101 條第 4 項第 1 句:「就已提供之訊息內容，應通知線路之持有者，即撥話發送方。」

適當之方式為告知，即用戶得撤回其號碼之轉遞。針對已依第 104 條公開資料之查詢，需取得用戶對於查詢回覆中轉遞其資料之同意。（第 2 項）電話告知僅得辨識電話號碼之用戶姓名，或是姓名與住址，僅有當用戶已申請登錄用戶名冊，且未行使異議權者始得為之（第 3 項）。

(6) 電報業務（Telegrammdienst）

電信通訊法第 106 條就電報業務予以規範：「關於電報業務處理與遞交之資料及憑據得於依據契約收繳相關服務費用所必要之範圍內儲存之，其保存期限至長為 6 個月，期限屆滿應由電信服務業者刪除之（第 1 項）。

電信事業者就電報業務內容之資料及憑據，得於傳送後繼續保存，但僅限於電信服務業者依據與用戶所簽訂之契約之範圍內，釐清傳送錯誤責任之用。其若為國內電報業務保存期限至長為 3 個月，國外則為 6 個月，期限屆滿應由電信服務業者刪除之（第 2 項）。

銷毀期限之計算始於電報發送該月的第 1 天，其期限得例外因追訴之請求或國際協定而延長（第 3 項）。」

(7) 資料傳遞系統中之暫存（Nachrichtenübermittlungssysteme mit Zwischenspeicherung）

電信通訊法第 107 條規定；「電信服務業者於提供有執行暫存必要之服務時，得處理訊息內容、特別是用戶的語言、聲音、文字、圖像傳遞，基此提供之服務應遵守下列前提：專由提供此暫存服務業者之電子通訊設施負責處理，但若其將此業務轉由其他服務業者時不在此限；透過用戶之指示決定處理之內容、範圍及形式；由用戶決定接收與存取訊息之對象；電信服務業者得告知用戶其訊息已被存取；電信服務業者僅得於符合其與用戶簽訂契約之情況下刪除訊息內容（第 1 項）。

電信服務業者應採行必要之技術性與組織性措施，防免錯誤傳遞及訊息內容在未授權之情況下於公司內或向第三人公開。必要性措施乃指，其花費成本與保障目的符合適當比例者而言。若對於追求之保護目的屬必要者，則其相應措施應配合現有技術之狀態，與時俱進（第 2 項）。」

4、 公共安全之考量（Öffentliche Sicherheit）

電信服務業者所蒐集、處理之資料，往往在面對特殊情況下時，有提供與第三人利用之義務。電信通訊法接續於第七部分第三節，第 108 條至第 115 條之規範中，專就涉及公共安全之情況，規範電信服務業者包括蒐集、儲存電信基本資料之義務（電信通訊法第 111 條）[206]；自動查詢程序之建置（電信通訊法第 112 條）[207]；人工查詢程序之建置（電信通訊法第 113 條）[208]；強制儲存通信資料之義務(電信通訊法第 113 條 a)；強制儲存通信資料之利用(電信通訊法第 113 條 b）等。

其中，德國於 2007 年底制訂「電信監察及其他隱藏性偵查措施及轉化歐盟 2006/24/EG 指令修正法（Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG ）」，增修電信通訊法第 113 條 a 及第 113 條 b，以及刑事訴訟法第 100 條 g 等規定，引發德國各界質疑違憲之聲浪，並接濟串連向德國聯邦憲法法院提起憲法訴訟，共計 3 組聲請被受理，併案進行審查。

2008 年 3 月 11 日德國聯邦憲法法院作成定暫時處分（einstweilige Anordnung）之裁定，[209]僅允許電信法第 113 條 b 就追訴德國刑事訴訟法第 100 條 a 所定重大犯

---

[206]依據電信通訊法第 111 條規定，凡因提供電信服務或參與該等服務而分配電信號碼或其他通訊識別碼、為接收其他電信號碼或通訊識別碼而配置電信連線之業者，為提供第 112 條與第 113 條所定資料查詢程序之用，應於服務啟用前，就下列資料予以蒐集並及時儲存，即便該等資料對於業者之經營非屬必要者一同；契約終結之日其亦應於知悉時予以儲存。1.電話號碼與其他通訊識別碼；2.電信使用者之姓名與地址；3.電信使用者為自然人時，其出生日期；4.屬固網連線者，其連線所在地址；5.於行動網路連線外同時提供行動終端機之情形，其行動終端機之號碼；6.契約起使日期。上述儲存資料應於契約關係消滅後次曆年終了時予以刪除。

[207]電信通訊法第 112 條針對自動查詢系統調取資料規定：凡對不特定人提供電信服務者，應及時儲存第 111 條第 1 項第 1、3、4 句與第 2 項所定資料，其中包括為後續行銷行為或其他使用目的而提供給其他電信服務業者之電話號碼與電話號碼配額之資料，以及可攜式電話號碼之識別碼。負有儲存義務之電信服務業者應確保：聯邦民生網路署（Bundesnetzagentur）隨時得於國內應第 2 項所列機關之查詢，而由該資料庫中以自動查詢方式調取資料；資料之調取可得使用不完整之搜尋字串或可藉助類似功能進行檢索。

[208]電信通訊法第 113 條規定：「電信服務業者或參與電信服務之業者，應依有權機關之個案查詢需求，及時提供其依第 95 條與第 111 條所蒐集之資料，若其乃為追訴犯罪行為或違反秩序之行為、為排除公共安全或秩序之危險、或聯邦與各邦之憲法保護機關、聯邦情報工作、軍事反情報工作為履行其法定任務所必要者。對於用以防戶終端設備、社置於終端設備中或網路中之資料儲存裝置之登入連結資料，特別是個人識別碼（PIN）或解除所定密碼（PUK），第 1 段所定義務人應有權機關依刑事訴訟法第 161 條第 1 項第 1 段、第 163 條第 1 項、聯邦或各邦警察法中除公共安全或秩序之危險所為之資料調取規定、聯邦憲法保護法第 8 條第 1 項或各邦憲法保護法語此相當之規定、聯邦情報工作法第 2 條第 1 項獲第 4 條第 1 項、聯邦軍事反情報工作法第 4 條第 1 項等規定之查詢請求，應予以提供；該等資料不得傳遞與其他公務或非公務單位。對於受通訊秘密所保護之資料的調取，僅得於符合相關法律規定之前提下使得為之。義務人就其所提供之資料，不得告知其客戶與第三人。」

[209]BVerfG, 1 BvR 256/08 vom 11.3.2008, Absatz-Nr. (1 - 188

罪行為而利用預先存取資料規定之適用；其餘爭議條文，考量其涉及電信業者就通信資料之預先蒐集與相關儲存資料庫之建立，影響不可謂小，故於實體判決作成前定暫時處分停止適用。[210]事隔將近 2 年，德國聯邦憲法法院終於 2010 年 3 月 2 日作出實體判決，[211]宣告轉換歐盟 2006/24/EG 指令之電信法第 113 條 a 及第 113 條 b 以及刑事訴訟法第 100 條 g，與德國基本法第 10 條第 1 項所保障之秘密通訊自由相互牴觸而無效，先前於暫時處分期間依據電信法第 113 條 b 所蒐集與儲存之資料應即刻銷毀，判決中認定國家課與電信與網路業者進行預防性資料存取義務之規定，將對於基本法第 10 條第 1 項秘密通訊自由造成重大干預，[212]因這些被存取之資訊若透過全面性與自動化之處理，長時間分析與比對通訊之收、發話方、日期、時間與地點，個人圖像將躍然呈現，包括個人之社會或政治歸屬、個人嗜好、傾向與弱點等，將難保不會涉及個人私密領域。因此其立法必須基於正當之目的，而其據此採行之措施必須是適於達成該目的、必要且符合狹義比例性，並符合資訊安全性之要求、設定利用該等資料之限制、資訊利用之透明以及具有有效權利保護等配套機制，以取得法益間之均衡。德國聯邦憲法法院強調憲法上嚴格禁止國家基於不確定或尚未確定之目的而全面性地預先存取個人資料，此應為從嚴之例外情況，且必須有具體的事實足認資料之預先存取得保護重要法益免於受到損害；[213]而被課與保存義務之業者必須隨著技術進步與知識提升，提供相應之資訊安

---

http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html(最後瀏覽日期：2015 年 2 月 5 日)

[210]在德國聯邦憲法法院於 2009 年 3 月 11 日就歐盟 2006/24/EG 指令內國法化後之電信法條文宣告暫時停止適用，而引發歐盟 2006/24/EG 指令合憲之高度疑慮後，歐洲法院實有多次得審查其合憲性之機會，但皆僅輕描淡寫地將合憲性審查認為並非爭點，以致錯失釐清該指令究竟是否有違憲之機會，誠屬可惜。而歷經 5 年的時間，直至 2014 年 4 月 8 日，歐洲法院方「承襲」德國聯邦憲法法院之見解，作成指令無效之判決，亦招致對於基本權利保障漠然以待之批評。對相關判決之批評，Vgl. Rossi, Matthias,Anmerkung zu EuGH, Urteil vom 10. Februar 2009- C-301/06, Zeitschrift für das Juristische Studium 3(2009), S.299. Rößner, Sören, Vorratsdatenspeicherung in Deutschland- Ende des Umsetzungsdefizits in Sicht? Europäische Zeitschrift für Wirtschaftsrecht 4 (2014), S.135-136. Meyer, Jürgen(Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage, 2004, S.249.

[211]BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html（最後瀏覽日期：2015年2月5日），就此一決議另有 2 位聯邦憲法法院法官提出意見書。關於德國聯邦憲法法院判決之介紹與評析，請參考程明修，前揭註 172，頁 7。蔡宗珍，前揭註 167，頁 8-9。

[212]德國聯邦憲法法院於此並未就可能對資訊自決權造成之侵害進行審查，因其認為秘密通訊自由除了保障通訊的過程及內容外，同時也及於資訊或資料之處理程序，所以在通訊過程結束後，對於該過程中所產生的各式資料進行存取或利用等行為，皆構成對於秘密通訊自由之干預；且其相較於資訊自決權屬特別保障規定而應優先適用，惟此排除資訊自決權之判斷結果，是否與過去聯邦憲法法院對於資訊自決權保障內容之理解相合致，多有討論。Vgl. Roßnagel, Alexander/ Moser-Knierim, Antonie/ Schweda, Sebastiasn, a.a.O.Fn176, S.100-104.

[213]BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218,

全標準，並得供事後審查，且不得藉由與經濟上效益權衡後犧牲對於安全性之要求；[214]並應保持該預先存取資料利用過程的透明性，或至少應於事後通知當事人，以利其採行有效之權利救濟；[215]且考量基本權利受侵害之強度，對於預先存取資料之調取及傳遞均應引進法官保留（Richtervorbehalt），藉此強化對於基本權利之保障。[216]由上述判決之論述得知，德國聯邦憲法法院並未自始即認定系爭規定不符合比例原則，但考量其欲追求之目的過於抽象而不明確，加以存取資料與後續利用要件及程序之設計，亦未得通過比例原則及相關要求之檢驗，方為其受到無效宣告之關鍵理由。[217]

另外，針對歐盟 2004/24/EG 指令引發之高度爭議，歐盟法院亦於 2014 年 4 月 8 日就 C-293/12 與 C-594/12 兩案作成判決[218]，認定該指令對於分別明訂於歐盟基本權利憲章第 7 條之隱私權與第 8 條之個人資料保護將造成一不合比例之大範圍且極為嚴正的侵害，且其並非屬絕對必要，因而宣告歐盟 2004/24/EG 指令違反歐盟基本權利憲章之規定而屬無效[219]。

三、小結

（一）由憲法至法律之個人資料法制架構

---

http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html(最後瀏覽日期：2015 年 2 月 5 日)Roßnagel, Alexander/ Moser-Knierim, Antonie/ Schweda, Sebastiasn, a.a.O.Fn176, S.107-108.

[214] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 224, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html（最後瀏覽日期：2015 年 2 月 5 日）針對業者對於資料保護與資料安全之監督義務，目前依據德國聯邦個人資料保護法第 4 條 f 及第 4 條 g 之規定，要求企業內部應設置資料保護監察人專責監督，Vgl. Plath, Kai-Uwe(Hrsg.), a.a.O. Fn.181, S. 232ff.. Wolff, Heinrich Amadeus, Vorratsdatenspeicherung- Der Gesetzgeber gefangen zwischen Europarecht und Verfassubng? Neue Zeitschrift für Verwaltungsrecht 12 (2010), S.751.

[215]BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr.240, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (最後瀏覽日期：2015 年 2 月 5 日)

[216]BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 247ff., http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html（最後瀏覽日：2015 年 2 月 5 日）。關於法官保留之相關討論，Vgl.Wolff, Heinrich Amadeus, a.a.O. Fn.214, S.752.

[217]Wolff, Heinrich Amadeus,, a.a.O. Fn.214, S.751.

[218] ECJ Digital Rights Ireland Ltd v Minister for Communications, Joined Cases C-293/12 &C-594/12, (8 April 2014) online: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN(最後瀏覽日期：2015 年 2 月 5 日)

[219] Kühling, Jürgen, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 11/2014, S.681-682.

德國個人資料保護法制實以德國基本法所保障之秘密通訊自由與資訊自決權為中心開展：秘密通訊自由係保障通訊各方藉由通訊管道無形傳輸資訊之過程及其內容得免於公權力之干預，其保障範圍亦應及於資訊或資料之處理程序，而得拘束任何公權力對於因通訊而生資料或資訊之閱覽、紀錄與利用行為，其對於表意自由與人格發展具有重要的意涵。但秘密通訊自由之保障範圍並未及於所有與通訊行為相牽連之資料，因而需進一步討論 1983 年透過德國聯邦憲法法院於「人口普查判決（Volkszählungsurteil）」所確認之資訊自決權，其確保人民有權知悉關於國家如何以及蒐集了哪些個人資料與其利用的方式，其一方面乃作為國家蒐集與利用個人資料的權力的抗衡，更進一步要求國家應積極保護個人資料，防免其遭到他人不當利用，藉此維護個人人格得以自由型塑發展、意見得以充分表達發揮。但德國聯邦憲法法院在秘密通訊自由與資訊自決權之選擇上，秘密通訊自由因相較於資訊自決權屬特別保障規定而往往得出應優先適用之結果，惟兩種基本權保障範圍之區劃界限並非十分清楚明確，也因此往往招致標準不一之批評。

隨著科技的發展與進步，資料之蒐集與傳遞不再侷限於特定形式，在現代化資料處理模式下，個人資料被儲存及利用之型態更為多元，國家於此應加倍關注「人民有權決定其個人資料之公開與運用」此一受基本法所捍衛之核心價值，因此，當國家於法律位階尋求基本法中所揭示相關基本權保障之具體實踐時，若基於對其他法益的維護而需限制人民之基本權利，應具備重大公益之考量，並以法律明確規範其限制之要件、範圍與方式，使人民充分瞭解，更應注意謹守比例原則。

德國聯邦個人資料保護法作為個人資料保護之基準法，其立法目的即明文揭示「在於保護個人免於因個人資料之流通致其人格權遭受侵害」，就公務機單位及非公務單位就個人資料之蒐集、處理及利用設定以下基本原則：當事人同意原則、直接蒐集原則、資料節約原則、資料縮減原則、目的拘束原則、透明原則與必要性原則；並明訂當事人得主張之權利，包括查詢權、異議權、更正、刪除及封鎖之權利、申訴權及損害賠償請求權。進一步考量電信與網路事業經營者於提供相關服務時，亦多涉及個人資料之蒐集、處理及利用，另重新整合或修訂特別法以因應特定領域個人資料保護之需求，包括：面對網路世代來臨，於 2007 年整併昔日電子媒體法、電子服務個人資料保護法以及關於媒體服務國家契約之相關規範，

制定現行之電子媒體法；以及 2012 年就電信通訊法進行相關革新，規範個人資料之類型及其蒐集、處理及利用之要件。另外，德國屬歐盟之一員，自不能免於受到歐盟個人資料保護立法之影響與拘束，故其個人資料保護法制之發展，即與歐盟個人資料保護之政策與法規動態息息相關。

（二）個人資料之類型化及其蒐集、處理、利用要件

德國聯邦個人資料保護法作為德國個人資料法制之基準法，將個人資料區分為一般個人資料與特種個人資料，並分別定義其內含與蒐集、處理、利用之要件，惟上述資料均應得連結至特定人，方會被認定屬於個人資料，而適用聯邦個人資料保護法之相關規範。而就電信及網路事業之告人資料保護規範，則見於電信通訊法及電子媒體法中，兩者制定之體例均為先將涉及之個人資料予以類型化，再分別明訂其蒐集、處理及利用之要件。電信通訊法（TKG）在個人資料類型上區分為主資料、通信資料、帳單資料及位置資料四種；電子媒體法（TMG）則將個人資料之類型區分為主資料與使用資料（內含帳單資料），以下謹以表格方式呈現電信通訊法及電子媒體法中，針對不同之資料類型所定一般性之要件，其中電信通訊法及電子媒體法未為規定者，多得回歸聯邦個人資料保護法之規定予以適用。惟隨著智慧型手機逐漸普及，許多透過網路進行的活動，已難以清楚劃分，往往導致電信通信法與電子媒體法在適用範圍界分上的困境。

電信通訊法及電子媒體法均另有針對特定情況規範個資運用之特別要件，例如：為辨識、限定或排除通信設施干擾之目的，得蒐集與利用主資料與通信資料（電信通訊法第 100 條）；基於揭露威脅或騷擾電話，得應申請蒐集發話方之相關通信資料（電信通訊法第 101 條）；電信服務業者得提供來電號碼之顯示，但應給予收發話之雙方皆有以簡易之方式免費選擇持續性或個別性拒絕顯示號碼之機會（電信通訊法第 102 條）；針對垃圾電子郵件（Spam），要求信首及主旨不得掩飾或隱瞞寄件人及郵件訊息之商業本質（電子媒體法第 6 條第 2 項）；基於廣告、市場調查或是形成電子媒體所需之目的，得使用假名（Pseudonymen）製作使用履歷（Nutzungsprofil），但必須以使用者未表達異議者為限方得為之，且使用履歷不得與該假名所代表本人之個人資料進行整合（電子媒體法第 15 條）。

而電信服務業者所蒐集、處理之資料，往往有提供與第三人利用之情形。電

信通訊法就涉及公共安全之情況，規範包括電信服務業者蒐集、儲存電信基本資料之義務（電信通訊法第 111 條）；自動查詢程序之建置（電信通訊法第 112 條）；人工查詢程序之建置（電信通訊法第 113 條）；強制儲存通信資料之義務（電信通訊法第 113 條 a）及強制儲存通信資料之利用（電信通訊法第 113 條 b）等相關規範。然而，由於德國聯邦憲法法院曾宣告電信通訊法第 113 條 a 及第 113 條 b 與德國基本法第 10 條第 1 項所保障之秘密通訊自由相互牴觸而無效，在基於公共安全目的蒐集、處理及利用通信相關資料之目的、要件及程序上，均要求立法者應本於基本權利保障之觀點，為更完善周延之考量。

表 3-4 德國聯邦個人資料保護法

	定義	蒐集、處理及利用之要件	目的之告知與限制	保存期限	個資分享
一般個資	關於一特定或可得特定人（即所謂當事人）其個人或事物關係中的所有細節內容（第 3 條第 1 項）	以取得當事人事前出於自由決定之書面同意為原則（第 4 條 a 第 1 項）	必須基於特定目的為之，目的需於事前即已確定，並告知當事人	達成利用目的所需之必要期間	個資得委外處理，委託單位負監督之責
特種個資	指與種族及道德出身背景、政治見解、宗教或哲學信仰、所屬工會、健康或性生活有關之內容（第 3 條第 9 項）	同上，另應明確告知其所同意蒐集、處理或利用之特種個資種類（第 4 條 a 第 3 項），並需同時符合第 13 條第 2 項與第 14 條第 5 項之要件。 於自動化處理特種個資前應進行事前檢查（第 4 條 d 第 5 項）	同上	同上	同上

資料來源：本研究自行整理。

表 3-5 德國電信通訊法（TKG）

	主資料	通信資料	帳單資料	位置資料
要件	為達契約簽訂、變更或終止之目的而蒐集	限於電信法第 96 條第 1 項所定之 5 種類型	分別依主契約與通信資料之要件為之	需當事人同意，事後應得許其退出
利用目的限制	成立契約關係所必須	建立或維護通信	估算及結清費用所需	提供加值服務之必要範圍內

保存期限	契約結束後 1 年	原則上於通話連線結束後立即刪除	原則上保存至帳單寄送後 6 個月	--
分享與共同利用	--	--	得委託第三人為之（第 97 條第 1 項）	於必要範圍內，限於特定人
對第三人提供	需用戶同意或法律明訂，例如：公共安全之考量	需用戶同意或法律明訂，例如：公共安全之考量	需用戶同意或法律明訂	需用戶同意或法律明訂需

資料來源：本研究自行整理。

表 3-6 德國電子媒體法（TMG）

	主資料	**使用資料**	**帳單資料**
蒐集及當事人告知	本法或相關法令明訂，或是取得使用者同意方得蒐集或處理主資料及使用者資料（包括帳單資料）（電子媒體法第 12 條）		
利用目的限制	成立契約且為使用電子媒體所必要(電子媒體法第 14 條第 1 項）	使用或阻斷電子媒體所必要（電子媒體法第 15 條第 1 項）	劃歸為使用資料下之類型，基於收取費用之目的（電子媒體法第 15 條第 4 項）
保存期限	--	--	帳單寄送後 6 個月
分享與共同利用	--	--	達成收費目的之必要範圍內得傳遞與第三人(電子媒體法第 15 條第 4 項）
對第三人提供	得基於公益目的提供第三人查詢(電子媒體法第 14 條第 2 項）	--	基於市場調查目的提供其他業者，僅得以匿名方式為之（電子媒體法第 15 條第 4 項）

資料來源：本研究自行整理。

表 3-7 電信通訊法及電子媒體法之特別運用要件

	辨識、限定或排除通信設施之干擾	揭露威脅或騷擾電話	來電顯示與拒示	使用履歷	商業電子郵件
依據	電信通訊法第 100 條	電信通訊法第 101 條	電信通訊法第 102 條	電子媒體法第 15 條	電子媒體法第 6 條第 2 項

利用目的與要件	辨識、限定或排除通信設施之干擾，相關資訊由企業監察人保存 2 年	揭露威脅或騷擾電話，限於提供申請後（威脅或騷擾電話）發話方之主資料及相關通信資料	給予收發話之雙方皆有以簡易之方式免費選擇持續性或個別性拒絕顯示號碼之機會	基於廣告、市場調查等行銷目的，給予當事人異議權，使用假名製作	基於商業目的，要求信首及主旨不得掩飾或隱瞞寄件人及郵件訊息之商業本質

資料來源：本研究自行整理。

第三節 英國

一、英國法制之沿革及現況概述

在 1995 年歐盟通過個資保護指令 (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)[220]以前，英國關於個人資料保護係以 1984 年個資保護法 (Data Protection Act 1984) 與 1987 年個人檔案使用法 (Access to Personal Files Act 1987) 為主要規範依據。之後為落實 1995 年歐盟個資保護指令之立法要求，並整合個資保護法律規範，乃於 1998 年制定現行個資保護法 (Data Protection Act 1998; 以下稱 DPA 1998)[221]。DPA 1998 屬於一般性的個人資料保護規範，實體保障層面之主要內容，包括基本概念 (如個人資料) 之定義[222]；個資主體 (data subject) 的權利[223]；個資控制者 (data controller) 之義務[224]；個資保護的例外條款 (exemptions)[225]；並透過附表 1 (Schedule 1) 將個資保障八大原則納入作為個資控制者必須遵循之規範[226]。執行面之主要內容，包括獨立主管機關 Information Commissioner's Office (以下稱 ICO)之設置[227]與權限[228]；違反個資保護的民事救濟[229]，行政罰鍰[230]與刑事責任[231]等。

近年隨著網路與通訊科技之突飛猛進，個人利用電信裝置 (如智慧型手機或平

---

[220] See ERU-Lex, at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT (2014/03/03 瀏覽).

[221] Data Protection Act 1998, at: http://www.legislation.gov.uk/ukpga/1998/29/contents (2014/03/03 瀏覽).

[222] DPA 1998, s. 1(1).

[223] DPA 1998, s. 7 以下。如資料主體對於個資之瀏覽與取得之權利；要求停止蒐集、處理與利用個資之權利等。

[224] DPA 1998, s. 17 以下。

[225] DPA 1998, s. 28 以下。

[226] DPA 1998, s. 4。

[227] DPA 1998, s. 6。

[228] DPA 1998, s. 40 以下。

[229] DPA 1998, s. 13, 14。

[230] DPA 1998, s. 55A 以下。

[231] DPA 1998, s. 60。

板電腦) 透過電信事業者建構之數位通訊網路從事訊息傳輸日益頻繁，引發電信領域的個資保護疑慮。歐盟為了確保 1995 個資保護指令建構之個資保障體系在電信領域同樣獲得落實，復於 2002 年通過電信個資與隱私保護指令 (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)[232]，英國亦於 2003 年因應制定隱私與電子通訊規則 (The Privacy and Electronic Communications (EC Directive) Regulations 2003; 以下稱 2003 Regulations)[233]，明確將個人透過電信網路交換或傳輸之訊息納入保障，並要求業者應確保通訊網路之安全 (security) [234] 與通訊資訊之保密性 (confidentiality)[235]。

此規則相較於 DPA 1998，針對電信領域有以下特別規範：對利用傳真、電話或電子郵件從事直接行銷 (direct marketing) 活動作出限制[236]；規範所謂「流量資料」(traffic data)，如通訊日期、所經線路與通話持續時間之處理與利用[237]；規範所謂「位置資料」(location data)，如電信裝置上安裝之定位軟體所指出之個人所在地理位置、行進方向與定位時間等資訊之利用限制[238]；允許業者在符合特定條件下於個別使用者之終端設備儲存資訊或取得儲存於該等設備之資訊[239]。

最近修訂的 Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (以下稱 2011 Regulations)[240]，則進一步對利用電信網路或服務而

---

[232] See ERU-Lex, at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:NOT (2014/03/03 瀏覽).

[233] The Privacy and Electronic Communications (EC Directive) Regulations 2003, at: http://www.legislation.gov.uk/uksi/2003/2426/contents/made(2014/03/03 瀏覽).

[234] 2003 Regulations, Regulation 5(1).

[235] 2003 Regulations 2003, Regulation 6(1).

[236] Regulation 19(1), 21(1), (2) of the 2003 Regulations 對利用電話從事直接行銷作出原則禁止之規定；Regulation 20(1)禁止利用傳真從事直接行銷；Regulation 22(2), 23 則禁止利用電子郵件從事直接行銷。

[237] 2003 Regulations, Regulation 7(1), (2), (3), 8(1), (2).

[238] 2003 Regulations, Regulation 14(2), (3), (5).

[239] 2003 Regulations, Regulation 6(1), (2), (4). 於網路使用者電腦上儲存 cookie 檔案並讀取其瀏覽歷程即為一例。

[240] The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, at: http://www.legislation.gov.uk/uksi/2011/1208/made (2014/03/03 瀏覽).

造成個資侵犯 (personal data breach) 之行為態樣下定義[241]，並對電信服務業者課以「發現個資侵犯時」對主管機關 ICO 之通報義務[242]；另外明文承認個人得透過調整網路瀏覽器隱私設定或其他應用程式以表彰同意 (signify consent) 業者透過電信網路儲存或利用其個資[243]。

簡言之、英國關於電信事業涉及之個資保護議題，係以 DPA 1998 作為一般基礎規範，針對特殊議題，再佐以 2003Regulations 與 2011 Regulations 對電信通訊個資之特別規定。以下將針對英國法制下個資之蒐集、處理、利用要件，安全維護，監督機制等議題分別敘述，最後並就英國主要電信事業者為因應個資保護法律規範要求而制定實施之隱私權政策(privacy policy) 加以介紹。

二、英國法制下個人資料處理之共通原則

依據 DPA 1998 之定義，個資 (personal data) 係指「與現存之個人有關之資料」，而「個人可以由該等資料被辨識[244]」，或「個人可由該等資料與其他現於資料控制者持有或可能持有之資料被辨識[245]」，包括對於該個人之評價的表達[246]。而所謂資料 (data)係指「透過依指令自動運作之設備處理之資訊[247]」，或「意圖依自動運作設備處理而記錄之資訊[248]」，或「被記錄成為相關檔案系統之一部分或意圖作為相關檔案系統之一部分而紀錄之資訊[249]」。除此之外，「不符合上開定義，但構成第 68 條定義下可使用紀錄 (accessible record)之一部分之資訊[250]」，如醫療紀錄[251]，就

[241]依據 2011 Regulations 之定義，個資侵犯係指「違反保全措施導致透過公共電信網路傳輸，儲存或處理之個資，遭意外或不法摧毀，喪失、變更、未經授權揭露或利用」。"[P]ersonal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service;" Regulation 3(b) of the 2011 Regulations 增訂上開「個資侵犯」定義於 Regulation 2(1) of the 2003 Regulations.

[242] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5(A).

[243] 2011 Regulations, Regulation 6(4)增訂 2003 Regulations, Regulation 6(3A).

[244] DPA 1998, s. 1(1), definition of "personal data", (a).

[245] DPA 1998, s. 1(1), definition of "personal data", (b).

[246] DPA 1998, s. 1(1), definition of "personal data".

[247] DPA 1998, s. 1(1), definition of "data", (a).

[248] DPA 1998, s. 1(1), definition of "data", (b).

[249] DPA 1998, s. 1(1), definition of "data", (c).

[250] DPA 1998, s. 1(1), definition of "data", (d).

[251] DPA 1998, s. 68(1)(a), (2).

學紀錄[252]，公共可使用紀錄 (如地方政府公共租屋與社會救助紀錄)[253]等亦屬之。最後、「在上述類型之外，由政府機關所紀錄之資訊[254]」亦屬本法定義之「資料」。DAP 1998 將個資控制者定義為「決定個資 processing 目的與方法之人[255]」。而「processing」在 DPA 1998 定義下係廣義地泛指對個資之蒐集、處理與利用等行為[256]。

(一) 蒐集之限制

根據 DAP 1998 第 4 條相關規定[257]，個資控制者有義務遵守附表 1 第 1 部分所列之個資保護原則[258]：

原則一：個資之蒐集、處理與利用必須合理 (fairly)並且合法 (lawfully)；

原則二：個資的蒐集必須基於特定目的，且不得以牴觸該目的之方式為後續處理與利用；

原則三：被蒐集、處理與利用之個資，就其蒐集、處理與利用之目的而言，必須充足，有關聯性且未超出範圍；

原則四：被蒐集、處理與利用之個資必須精確，且必要時保持更新；

原則五：被蒐集、處理與利用之個資，不得保留超過其蒐集、處理與利用之目的所必要期間；

原則六：個資之蒐集、處理與利用必須依據本法下資料主體所有之相關權利為之；

原則七：應採取適當措施以防制未經授權或不法之個資蒐集、處理與利用，並預防個資之意外喪失、毀滅或損害；

原則八：個資不得傳輸至歐洲經濟區 (European Economic Area; 以下稱 EEA)以外

252 DPA 1998, s. 68(1)(b).

253 DPA 1998, s. 68(1)(c).

254 DPA 1998, s. 1(1), definition of "data", (e).

255 DPA 1998, s. 1(1), definition of "data controller".

256 DPA 1998, s. 1(1), definition of "processing". 依此定義，processing 之行為態樣包括對個資之取得，紀錄、持有、操作 (包括重組、改編、變更)、以及使用、透過傳輸或散佈而揭露，結合，消除、銷毀。

257 DPA 1998, s. 4.

258 DPA 1998, Schedule 1, Part I: The Principles.

之國家或地區，除非該國家或地區亦針對個資之蒐集、處理與利用對資料主體提供足夠等級之保護。

在原則一「合理性」與「合法性」的條件下，個資之蒐集、處理與利用必須再滿足附表 2(Schedule 2) 所列要件之一始得為之[259]，附表 2 列舉要件如下：

要件一：個資主體事前同意 (has given his consent) 個資之蒐集、處理與利用[260]；

要件二：個資之蒐集、處理與利用係為履行個資主體為當事人之契約義務所必要[261]；

要件三：個資之蒐集、處理與利用係應個資主體之要求，為締結契約所為前置作業所必要[262]；

要件四：個資之蒐集、處理與利用係資料控制者為遵守其契約義務以外之 法定義務所必要[263]；

要件五：個資之蒐集、處理與利用係為保護個資主體之重要利益 (vital interests) 所必要[264]；

要件六：個資之蒐集、處理與利用係為司法程序之行政管理 (administration of justice) 所必要[265]；

要件七：個資之蒐集、處理與利用係為國會行使職權所必要[266]；

要件八：個資之蒐集、處理與利用係為任何人依制定法行使職權所必要[267]；

要件九：個資之蒐集、處理與利用係為行政機關行使職權所必要[268]；

---

259 DPA 1998, Schedule 1, Part I, 1(a).
260 DPA 1998, Schedule 2, 1.
261 DPA 1998, Schedule 2, 2(a).
262 DPA 1998, Schedule 2, 2(b).
263 DPA 1998, Schedule 2, 3.
264 DPA 1998, Schedule 2, 4.
265 DPA 1998, Schedule 2, 5(a).
266 DPA 1998, Schedule 2, 5(aa).
267 DPA 1998, Schedule 2, 5(b).
268 DPA 1998, Schedule 2, 5(c).

要件十：個資之蒐集、處理與利用係為任何人基於公共利益行使與公眾有關之職權所必要[269]。

簡言之，除非符合要件二至要件九之例外情形，否則 DPA 1998 對於個資蒐集、處理、利用，原則上係採需事先徵得個資主體同意之「選擇加入」(opt-in)模式。

就敏感性個資 (sensitive personal data) 如種族、政治立場、宗教信仰、工會會籍、身心健康狀況、性生活、犯罪紀錄等[270]，則必須滿足附表 3 (Schedule 3) 所列要件之一始得蒐集、處理與利用[271]。附表 3 列舉要件如下：

要件一：個資主體事前明示同意 (has given his explicit consent) 敏感性個資之蒐集、處理與利用[272]；

要件二：敏感性個資之蒐集、處理與利用，係個資控制者針對就業事務 (employment) 行使其法定權利或履行法定義務所必要[273]。

DPA 1998 對敏感性個資亦採「選擇加入」(opt-in) 模式，且個資主體之同意提升至更嚴格之明示同意，而例外不須個資主體同意之情形，則大幅限縮至「個資控制者處理就業相關事務之必要」為限。

(二) 利用目的之特定

如上述 DAP 1998 第 4 條規定，個資控制者必須遵守附表 1 所列之個資保護原則，其中原則二即要求個資的蒐集必須基於特定目的，且不得以牴觸該目的之方式為後續處理與利用。

(三) 個資蒐集、處理、利用之告知

根據 DPA 1998 附表 1, 第 2 部分之相關規定，個資控制者在蒐集、處理、利用個資時，必須在初次蒐集或處理或對第三方揭露以前或隨後[274]，對個資主體告知包括「個資控制者之身分」與「個資利用之特定目的」等事項[275]；個資控制者

[269] DPA 1998, Schedule 2, 5(d).
[270] DPA 1998, s. 2.
[271] DPA 1998, Schedule 1, Part I, 1(b)
[272] DPA 1998, Schedule 3, 1.
[273] DPA 1998, Schedule 3, 2(1).
[274] DPA 1998, Schedule 1, Part II, 2(1), 2(2).
[275] DPA 1998, Schedule 1, Part II, 2(3).

若未盡到此告知義務，則不能認為其遵守附表 1 第 1 部分原則一關於合理利用個資之義務[276]。

(四) 目的外利用之限制

關於已經基於原特定目的而蒐集、處理、利用之個資，個資控制者能否為原特定目的外之利用？依 DAP 1998 第 4 條引用附表 1 之八大原則，並未明確規範目的外利用之情形，依 ICO 之解釋，須視此目的外利用是否符合原則一即個資利用「合理性」之要件，為滿足此要件，個資控制者至少應就目的外利用通知個資主體，並給予選擇退出 (opt-out) 之機會[277]。

(五) 個資保存期限

如上述 DAP 1998 第 4 條規定，個資控制者必須遵守附表 1 所列之個資保護原則，其中原則五即要求個資控制者對其所蒐集、處理與利用之個資，不得保留超過其蒐集、處理與利用之目的所必要期間。除此之外，DAP 1998 並無關於個資保存最高或最低期限之明確規範。

(六) 第三方分享個資 (data sharing)之限制

1、個資分享之類型

依據 ICO 之分類，個資分享包括「個資委外處理」、「不同個資控制者間常態性分享個資」以及「個資控制者臨時對第三方提供個資」。個資委外處理係指個資控制者將已蒐集之個資委由獨立第三人代為處理，此時該第三人稱為個資處理者 (data processor)；不同個資控制者間常態性分享個資係指不同個資控制者基於特定目的事先締結協議約定將其所持有之個資由一方分享於他方或將雙方持有之個資匯入共同資料庫個資控制者臨時對第三方提供個資則係指在無事先協議下個資控制者因應第三方要求對其提供個資通常是在緊急情況下如意外事故救援或偵查防制犯罪[278]。

---

[276] DPA 1998, Schedule 1, Part II, 2(1)(a).

[277] ICO, The Guide to Data Protection, pp.46-47, paras 18-19, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf (2014/10/20 瀏覽).

[278] ICO, Data sharing code of practice, pp.9-10, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx (2014/10/20 瀏覽).

2、個資委外處理

根據 DPA 1998 附表 1, 第 2 部分之相關規定[279]，個資控制者在蒐集、處理、利用個資時，必須在初次蒐集或處理或對第三方揭露以前或隨後，對個資主體告知包括「個資控制者之身分」與「個資利用之特定目的」等事項；而個資控制者將個資委由第三方代為處理，亦屬於對該第三方為個資揭露，故在個資委外處理之情形，委託方之個資控制者仍需再度告知個資主體，以符合附表 1 第 1 部分原則一關於合理與合法利用個資之條件 (包括依據附表 1 第 2 部分相關部分盡到告知義務，並依附表 2 或附表 3 取得個資主體同意或符合其他利用條件)。此外、個資控制者必須以書面契約約定，限制受委託處理個資之第三方個資處理者僅能依循其指示處理個資，且該第三方個資處理者必須採取等同於委託方個資控制者依 DPA 1998 附表 1 原則七下所採取之個資安全維護措施，否則委託方個資控制者將被認定違反附表 1 原則七[280]。

3、常態性個資分享

如以上第 2 點所述，個資控制者將其已經蒐集、處理、利用之個資，與第三方分享，構成對第三方之個資揭露，故應就此個資分享再次對個資主體盡到告知義務以符合附表 1 第 1 部分原則一關於合理與合法利用個資之條件 (包括依據附表 1 第 2 部分相關部分盡到告知義務，並依附表 2 或附表 3 取得個資主體同意或符合其他利用條件)。

4、臨時對第三方提供個資

臨時對第三方提供個資之情形，若符合 DPA 1998 第 27 至 38 條列舉之例外事由，例如涉及關於國家安全、醫療行為、偵查防制犯罪、學術研究活動等等，則無需依照第 4 條遵守附件 1 所列之個資保護原則 (如徵得個資主體之同意，告知特定利用目的等)[281]。

(七) 對 ICO 登錄公告事項

DPA 1998 第 17 條設有關於個資控制者蒐集、處理與利用個資時應盡到之公告

[279]前註 274-276.
[280] DPA 1998, Schedule 1, Part II, 12
[281] DPA 1998, s. 27.

義務。根據第 17 條第 1 項規定，資料控制者原則上必須先向 ICO 申請登錄於資料控制者名冊 (register)，經核准登錄完成，始得為個資之蒐集、處理與利用[282]。此名冊係 ICO 依第 19 條第 1 項所設置[283]，且對公眾開放免費檢索[284]。提出登錄申請之個資控制者必須提交相關資訊，包括個資控制者自身資訊與附表 1 之原則七所要求之個資防護保全措施之概述[285]。所謂個資控制者自身資訊包括：個資控制者與其代理人之名稱與地址；被蒐集、處理與利用之個資之描述以及個資主體之歸類；蒐集、處理與利用之個資之目的；個資控制者意圖或可能揭露個資之對象；個資控制者有意或可能將個資直接或間接傳輸所至之國家或地區等[286]。任何人違反第 17 條第 1 項，未經登錄於個資控制者名冊而為個資之蒐集、處理與利用，構成刑事犯罪行為[287]。

(八) 個資主體之相關權利

1、個資查閱權

依據 DPA 1998 第 7 條相關規定，個資主體有權以書面向個資控制者查詢個資主體之個資是否被個資控制者利用[288]；若是、則個資控制者應告知「利用之個資型態」、「利用之目的」與「個資可能揭露之對象」[289]；個資主體並有權要求個資控制者提供關於其被利用個資之相關資訊以及個資來源[290]。此屬於個資主體對其個資之查閱權。

2、個資利用制止權

根據第 10 條相關規定，若個資之利用有可能造成個資主體或他人之顯著損害，個資主體有權以書面通知個資控制者要求停止個資之利用[291]。

3、個資行銷制止權

---

[282] DPA 1998, s. 17(1). 在特例情形下，資料控制者得免於登錄，參見 s. 17(2), (3), (4).
[283] DPA 1998, s. 19(1).
[284] DPA 1998, s. 19(6).
[285] DPA 1998, s. 18(1), (2).
[286] DPA 1998, s. 16(1).
[287] DPA 1998, s. 21(1).
[288] DPA 1998, s. 7(1)(a).
[289] DPA 1998, s. 7(1)(b).
[290] DPA 1998, s. 7(1)(c).
[291] DPA 1998, s. 10(1).

個資主體有權於任何時間以書面通知個資控制者停止利用其個資從事直接行銷活動[292]。

4、個資更正與刪除權

若個資控制者所持有之個資不正確，個資主體有權請求法院作出裁決，命令個資控制者更正或刪除此錯誤個資[293]。

(九) 個資安全維護義務

依據 DAP 1998 第 4 條規定，個資控制者有義務遵守附表 1 列舉之個資保護原則。其中原則七要求資料控制者應採取適當措施以防制未經授權或不法之個資蒐集、處理與利用，並預防個資之意外喪失、毀滅或損害；換言之、個資控制者對於其所蒐集、處理與利用之個資有義務採取適當之安全防護措施。依據附表 1 第二部分對個資保護原則之解釋，就原則七「個資安全防護」部分，個資控制者之個資安全防護義務包括以下事項：

1、個資安全防護措施必須對應個資之性質與可能發生之個資事故，提供適當之保全等級[294]；

2、個資控制者必須採取必要措施以確保其有權接觸個資之員工之可靠性[295]；

3、在個資控制者授權個資處理者 (data processor) 實際經手個資之情形，個資控制者必須挑選對個資安全防護能足夠保證之個資處理者，並採取必要作為以確保其遵守個資安全防護措施[296]；

4、在個資控制者授權個資處理者實際經手個資之情形，除非個資蒐集、處理與利用之實施係基於雙方書面契約，且個資處理者僅依照個資控制者指示行事，且系爭契約賦予個資處理者等同於個資控制者在原則七下之個資安全防護義務，否則個資控制者不能視為已遵循原則七之個資安全防護義務[297]。

---

[292] DPA 1998, s. 11(1).
[293] DPA 1998, s. 14(1).
[294] DPA 1998, Schedule 1, Part II, 9(a), (b).
[295] DPA 1998, Schedule 1, Part II, 10.
[296] DPA 1998, Schedule 1, Part II, 11(a), (b).
[297] DPA 1998, Schedule 1, Part II, 12(a), (b).

特別注意的是，在 DPA 1998 架構下，個資控制者並無任何法定義務要通報個資侵害事件，惟 ICO 仍建議個資控制者在發生個資侵害事件時，考慮通知受到影響之個資主體，ICO、以及其他相關單位 (如警方)[298]。

三、英國法制下關於電信個資之特別規範

2003 Regulations 並未對電信個資之蒐集或處理另為定義，故在 2003 Regulations 條文中「processing」亦泛指對個資之蒐集、處理、利用等行為[299]。此外、針對使用電信通訊設備或裝置所產生之網路瀏覽歷程、流量資料與位置資料，2003 Regulations 設有特別規定，但此等規定不免除資料控制者依循 DPA 1998 蒐集、處理與利用個資應負之義務[300]。換言之、關於網路瀏覽歷程、流量資料與位置資料以及其他類型電信個資之蒐集、處理與利用，除須遵守 DPA 1998 之規定以外，亦須滿足 2003 Regulations 之額外要件始為合法。惟若係基於保障國家安全之目的而蒐集、處理、利用電信個資者，不在此限[301]。

(一) 電話行銷

1、預錄訊息式電話行銷

依據 2003 Regulations 之定義，預錄訊息式電話行銷是指利用自動化撥號系統，依預設指令對多數受話方自動依序撥號發話，且該發話內容屬預先錄製，非現場真人對話[302]。此種電話行銷方式，除非受話方事先同意，否則不得利用其電話號碼對其為之[303]。

2、真人對話式電話行銷

依據 2003 Regulations 第 21 條相關規定，關於現場真人對話式之電話行銷，若用戶已預先將其電話號碼登錄於電信事業主管機關 (Office of Communications;

---

298 ICO, Notification of Data Security Breaches to the ICO, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/breach_reporting.ashx (2014/10/20 瀏覽); 亦參見 ICO, The Guide to Data Protection, p.91, para 29.

299 2003 Regulations, Regulation 2(2).

300 "Nothing in these Regulations shall relieve a person of his obligations under the Data Protection Act 1998 in relation to the processing of personal data." 2003 Regulations, Regulation 4.

301 2003 Regulations, Regulation 25(1).

302 2003 Regulations, Regulation 19(1), (4).

303 2003 Regulations, Regulation 19(1), (2).

以下稱 OFCOM) 依第 26 建置之「請勿來電名冊」[304]，任何人即不得撥打該號碼對用戶從事電話行銷[305]；但經用戶事先同意者不在此限[306]。用戶事後亦得隨時撤回其同意[307]。但針對未將其電話號碼登錄於請勿來電名冊之用戶，若該用戶事先告知個資控制者不得來電，則不得對其從事電話行銷。反面言之，可以對未登錄於「請勿來電名冊」之電話用戶從事真人對話式電話行銷，但該用戶得以「事先告知不得來電」方式選擇退出 (opt-out)[308]。

(二) 來電顯示或拒示

依據 2003 Regulations 第 10、11 條相關規定，電信事業者應提供用戶相關機制，允許其於撥號發話時隱藏其發話號碼，不在受話方顯示[309]；在發話方號碼可顯示於受話方之情形，電信事業者亦應提供受話方相關機制，以隱藏發話方電話號碼，不在受話方顯示[310]；在發話方隱藏其發話號碼之情形，電信事業者應提供受話方拒絕接聽此種隱藏發話號碼之機制[311]；電信事業者亦應提供受話方相關機制，使其受話號碼不顯示於發話方[312]。惟上開關於「發話方有權隱藏其發話號碼不顯示於受話方」之規範，若涉及騷擾電話之追查，或緊急求救或報案電話者，不適用之[313]。原則上、關於電話號碼顯示採選擇退出(opt-out)。

(三) 傳真行銷

依據 2003 Regulations 第 20 條相關規定,任何人不得未經個資主體事先同意，對其從事傳真行銷 (即利用個資主體之傳真號碼將行銷資訊傳真至該個資主體)[314]；個資主體若將其傳真號碼登錄於 OFCOM 依第 25 建置之「請勿傳真名冊」[315]，任

304 2003 Regulations, Regulation 26(1).
305 2003 Regulations, Regulation 21(1)(b).
306 2003 Regulations, Regulation 21(4).
307 2003 Regulations, Regulation 21(5).
308 2003 Regulations, Regulation 21(1)(a).
309 2003 Regulations, Regulation 10(2), (3).
310 2003 Regulations, Regulation 11(2).
311 2003 Regulations, Regulation 11(3).
312 2003 Regulations, Regulation 11(3).
313 2003 Regulations, Regulation 10(1), 15, 16.
314 2003 Regulations, Regulation 20(1)(a), (2).
315 2003 Regulations, Regulation 25(1).

何人即不得對該個資主體為傳真行銷[316]，除非該個資主體事先同意[317]；且該個資主體事後仍得隨時撤回其對接收傳真行銷資訊之同意[318]。

(四) 電子郵件行銷

2003 Regulations 對利用電子郵件從事直接行銷 (direct marketing) 設有以下限制：首先、除非符合例外規定，若未經電子郵件收信方事先同意，任何人不得傳送或促使傳送以直接行銷為目的之電子郵件[319]，故原則上採「選擇加入」(opt-in) 模式；在例外情形，若電子郵件發信方在銷售過程或協商商品或服務之提供過程中已取得收信方聯絡資訊，且係關於發信方之類似商品或服務，且收信方取得拒絕接收行銷之機制，則得為直接行銷而傳送或促使傳送電子郵件[320]，換言之、此種情況下例外採「選擇退出」(opt-out) 模式。此外、若隱匿發信方身分，或未提供「請求停止寄送」之有效回復地址，則不得傳送或促使傳送直接行銷之電子郵件[321]。

(五) 瀏覽履歷 (cookie)

2003 Regulations 第 6 條第 1 項明定：任何人除非滿足同條第 2 項要件，否則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[322]，如利用 cookie 檔案紀錄網路使用者之網路瀏覽歷程相關資訊。第 2 項則規定上開行為之合法要件：包括對用戶或使用者提供「關於儲存或讀取終端設備上資訊之目的」之明確且完整訊息，且用戶或使用者已對終端設備上資訊之儲存或讀取予以同意[323]。2011 Regulations 對此「同意」之認定進一步增訂：用戶透過調整網路瀏覽器軟體之隱私設定，或透過其他應用程式，可表彰其同意[324]。2003 Regulations 第 6 條第 4 項則針對第 1 項訂出例外規範：包括單純基於電信網路傳輸之目的所為之技術性儲存或讀取資訊行為；或對用戶或使用者提供其要求之資訊社群服務 (information

316 2003 Regulations, Regulation 20(1)(c).
317 2003 Regulations, Regulation 20(5).
318 2003 Regulations, Regulation 20(6).
319 2003 Regulations, Regulation 22(2).
320 2003 Regulations, Regulation 22(3), (a), (b), (c).
321 2003 Regulations, Regulation 23.
322 2011 Regulations, Regulation 6(2)修訂 2003 Regulations, Regulation 6(1).
323 2011 Regulations, Regulation 6(3)修訂 2003 Regulations, Regulation 6(2).
324 2011 Regulations, Regulation 6(4)增訂 2003 Regulations, Regulation 6(3A).

society service) 所必要之技術性儲存或讀取資訊行為[325]。

(六) 流量資料 (traffic data)

根據 2003 Regulations，流量資料係指「基於透過電信網路傳遞特定通訊之目的而處理之資料」，或「關於該特定通訊之計費而處理之資料」，且包括「該通訊之傳遞線路，持續時間與日期[326]」。2003 Regulations 對流量資料訂有以下規範：依據第 7 條第 3 項，關於電信網路之用戶或使用者之流量資料，公共電信服務提供者 (provider of public electronic communications service) 得於符合以下要件時為蒐集、處理、利用與儲存[327]：

(a) 流量資料之蒐集、處理、利用與儲存係為對用戶或使用者行銷其電信網路服務或提供加值服務 (value added services)，且

(b) 用戶或使用者先前已通知服務提供者其對流量資料之蒐集、處理、利用與儲存之同意[328]，且

(c) 流量資料之蒐集、處理、利用與儲存僅存續於上開(a)要件下服務所必要期間。

用戶或使用者基於第 3 項所為之同意得隨時撤回 (withdraw) 之[329]。

依據第 7 條第 2 項，公共電信服務提供者基於計費之目的所持有之流量資料，得於同條第 5 項之特定期間內為蒐集、處理、利用與儲存[330]。此特定期間係指：用戶或使用者欠費之追討期間；若業者於該期間內提起訴訟，則至該訴訟終局確定為止[331]。在上開第 2、3 項之條件下，當流量資料之蒐集、處理、利用與儲存不再為通訊傳輸所必須時，該等資料應被消除 (erased) 或修改至不成個資 (cease to be data that would be person data)[332]。

---

325 2003 Regulations, Regulation 6(4).
326 2003 Regulations, Regulation 2(1), definition of “traffic data”.
327 2003 Regulations, Regulation 7(3).
328 2011 Regulations, Regulation 7 修訂 2003 Regulations, Regulation 7(3)(b).
329 2003 Regulations, Regulation 7(4).
330 2003 Regulations, Regulation 7(2).
331 2003 Regulations, Regulation 7(5).
332 2003 Regulations, Regulation 7(1).

2003 Regulations 第 8 條對於依照第 7 條第 2、3 項進行流量資料之蒐集、處理與利用設有進一步限制。依據第 8 條第 1 項，除非用戶或使用者接獲「關於被蒐集、處理與利用之流量資料之類型」與「蒐集、處理與利用持續期間」之訊息，特別是在第 7 條第 3 項「基於行銷或提供加值服務」而蒐集、處理與利用流量資料之情形，用戶或使用者在同意前即已得知上開蒐集、處理與利用「類型」與「期間」之訊息，否則業者不得為流量資料之蒐集、處理與利用。又依據第 8 條第 2 項，依第 7 條對流量資料所為之蒐集、處理與利用，僅能由業者本人或其授權之人基於特定目的為之[333]：

(a)帳務或流量管理；

(b) 顧客查詢；

(c) 詐欺之預防或偵測；

(d) 電信服務之行銷；

(e)加值服務之提供。

(七) 位置資料 (location data)

位置資料則係指「任何透過電信網路處理的資料，能指出公共電信網路特定使用者所使用之終端設備 (terminal equipment) 之地理位置所在[334]」，包括關於該終端設備所在之經度、緯度與海拔高度[335]；使用者之行進方向[336]；以及相關位置被紀錄之時間[337]。2003 Regulations 對於位置資料訂有下列規範：依據第 14 條第 2 項，公共電信網路或公共電信服務之用戶或使用者之位置資料僅能基於以下情形被蒐集、處理與利用[338]：

(a) 用戶或使用者無法經由該位置資料被辨識；或

(b)經用戶或使用者同意，為提供加值服務所必要。

---

333 2003 Regulations, Regulation 8(2), (3).
334 2003 Regulations, Regulation 2(1), definition of “location data”.
335 2003 Regulations, Regulation 2(1), definition of “location data”, (f).
336 2003 Regulations, Regulation 2(1), definition of “location data”, (g).
337 2003 Regulations, Regulation 2(1), definition of “location data”, (h).
338 2003 Regulations, Regulation 14(2).

在依第 14 條第 2 項第 b 款取得用戶或使用者同意之前，業者必須對用戶或使用者提供下列資訊[339]：

(a)將被蒐集、處理與利用之位置資料的類型；

(b) 該等資料被蒐集、處理與利用之目的與持續期間；以及

(c) 該等資料是否基於提供加值服務之目的而被傳輸至第三人。

基於第 14 條第 2 項第 b 款而同意業者蒐集、處理與利用其位置資料之用戶或使用者得隨時撤回其同意[340]，且針對各次公共電信網路之連線，或各次通訊傳輸，應被賦予撤回同意之機會，且得以簡捷且免費之方法為之[341]。位置資料之蒐集、處理與利用，僅能由公共通訊提供者，提供加值服務之第三人，或經此兩方授權之人為之[342]。基於提供加值服務之目的而蒐集、處理與利用位置資料時，僅限於達成該目的之必要範圍內為之[343]。

(八) 帳單資料 (itemized billing)

關於帳務資料之利用，根據 2003 Regulations 第 9 條第 1 項，公共電信服務業者因應用戶之要求，應提供未附明細 (not itemized)之通訊帳單[344]；換言之、關於帳務資料，如撥出號碼、通訊日期、持續期間等資料，用戶得以選擇退出(opt-out)之方式，不同意業者為處理或利用。

(九) 電信個資安全維護義務

2003 Regulations 針對公共電信服務提供者與公共電信網路提供者之個資安全防護義務作出相關規定。根據第 5 條第 1 項，公共電信服務提供者對於其提供之服務應採取「適當」安全防護措施[345]。業者採取之相關措施是否「適當」，應視該措施所能發揮之保障作用與所對抗之風險是否符合比例，並考量當代科技發展水

339 2003 Regulations, Regulation 14(3).
340 2003 Regulations, Regulation 14(4)(a).
341 2003 Regulations, Regulation 14(4)(b).
342 2003 Regulations, Regulation 14(5)(a).
343 2003 Regulations, Regulation 14(5)(b).
344 2003 Regulations, Regulation 9(1).
345 2003 Regulations, Regulation 5(1).

準與施行該措施之成本[346]。又依據 2011 Regulations 第 4 條對 2003 Regulations 第 5 條之增修，2003 Regulations 第 5 條第 1 項所指之「安全防護措施」至少應[347]：

(a) 確保個資僅能由被授權人員基於合法授權目的而取得；

(b) 保護儲存或傳輸之個資免於意外或非法摧毀，意外喪失或修改，未經授權或非法儲存，處理、取得或揭露；且

(c) 確保關於個資處理之安全防護政策之實施。

2003 Regulations 第 5 條第 2 項復規定，必要時、公共電信網路提供者應與公共電信服務提供者合作提供前項之防護措施[348]。

第 5 條第 3 項進一步規定，儘管業者已依同條第 1 項採取相關措施，若其所提供之公共電信服務仍有安全上的顯著風險(significant risk)，業者應告知用戶下列事項[349]：

(a)該風險之性質；

(b) 用戶得對抗該風險之任何適當措施；以及

(c) 用戶採取該等措施可能產生之費用。

業者對於此等事項之告知不得對用戶額外收費[350]。

(十) 電信個資侵害事件之處理

2011 Regulations 針對個資安全防護增訂處理「個資侵犯」事件之相關規範。首先、發生個資侵犯事件時，業者應通報 (notify) ICO，不得無故延遲[351]。通報應包含以下內容[352]：

(a) 個資侵犯事件之性質；

---

346 2003 Regulations, Regulation 5(4)(a), (b).
347 2011 Regulations, Regulation 4(1)增訂 2003 Regulations, Regulation 5(1A).
348 2003 Regulations, Regulation 5(2).
349 2003 Regulations, Regulation 5(3)(a), (b), (c).
350 2003 Regulations, Regulation 5(5).
351 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5A(2).
352 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5A(4).

(b) 個資侵犯事件之結果；以及

(c) 業者已採取或建議採取之應對措施。

若個資侵犯事件可能對用戶或使用者的個資或隱私造成不利影響，業者應通報用戶或使用者，不得無故延遲[353]。通報應包含以下內容[354]：

(a) 對個資侵犯事件性質之描述；

(b) 關於向業者取得更多相關訊息之聯繫資訊；以及

(c) 推薦用戶採取措施以減輕個資侵犯可能造成之不利影響。

若業者向 ICO 證明，其已採取適當保護措施，使任何未經授權取得個資之人無法判讀該個資侵犯事件所涉及個資內容，則業者無需踐行對用戶或使用者之通報程序[355]。若業者未遵照規定通報用戶或使用者，ICO 得考量個資侵犯事件之可能不利影響，要求業者通報用戶或使用者[356]。

四、英國主要電信事業者之隱私權政策

(一) 英國電信

關於英國電信事業者如何因應並落實上述個資保護相關法規，以主要業者英國電信 (British Telecom; 以下稱 BT)[357]網站所揭示之隱私權政策為例[358]，在 BT 官網之隱私權頁面，使用者可以依其有意取得之電信服務類型瀏覽之[359]。點選進入特定服務類型頁面後，BT 會進一步告知消費者個資保護之相關資訊。如點選進入寬頻網路 (Broadband) 服務頁面，BT 即告知使用者：若欲訂購服務，其姓名、地址、電話、電郵地址等個資將被 BT 取得；BT 使用此等個資之目的包括通知服務內容變動；在消費者同意之前提下作行銷之利用。此外 BT 亦明確告知消費者其使用網路之流量資料將被記錄與儲存，包括 IP address 與消費者造訪之網站，以便

[353] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5A(3).
[354] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5A(5).
[355] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5A(6).
[356] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5A(7).
[357] BT, About BT Group, at: http://www.btplc.com/Thegroup/ (2014/06/20 瀏覽).
[358]作者無法取得 BT 對客戶提供相關服務之合約紙本，現階段先以網站揭示之隱私權政策說明之。
[359] BT, Welcome to our Privacy Centre, at: http://home.bt.com/pages/navigation/privacypolicy.html (2014/06/20 瀏覽).

BT 了解消費者使用網路之情形並管理其網路系統。BT 並告知消費者 BT 依法負有對政府機關提供犯罪偵防相關資訊之義務[360]。

在 Cookies 頁面，BT 首先解釋 cookie 之概念：即伺服器儲存於用戶終端裝置(如電腦、智慧型手機、平板等) 上之文字檔，其功能包括記憶用戶瀏覽過之網站，或儲存用戶之瀏覽偏好，或便利用戶切換於同一網站之不同網頁間，或置入廣告等。BT 須徵得使用者同意始得使用 cookie[361]。BT 並描述所利用之 cookie 類型與目的[362]。事實上當用戶第一次連結到 BT 網站主頁，關於使用 cookie 之警示視窗即會彈出，使用者得選擇接受 cookie 與否。BT 並告知使用者得利用瀏覽器軟體功能選項設定接受或拒絕 cookie[363]。

在法律資訊 (Legal) 頁面，BT 進一步告知消費者其個資將在 BT 集團內各子企業間基於本隱私權網頁所提到之目的而分享；BT 可能會將個資傳輸至 EEA 以外地區，但將要求相對方採取與英國相同之個資安全防護標準；基於教育訓練與確保服務品質之目的，BT 可能會監控並記錄與客戶間之通訊內容；為確保 BT 持有之用戶個資精確無誤，用戶有權聯繫 BT 要求更正或清除個資，或查詢 BT 持有個資之類型，或索取個資複本 (需付費)；用戶得依網頁所附地址聯繫 BT[364]。

(二) 佛達風

佛達風 (Vodafone)為另一英國主要電信事業者。Vodafone 於其個人用戶官網公告其隱私權政策，包括用戶個資被蒐集之時機 (如購買產品或註冊登記以取得特定服務)，蒐集、處理與利用個資之類型 (如用戶個人資料，消費習慣與偏好，帳戶資料等)，另外也包括使用 cookie 以蒐集用戶之網路瀏覽歷程。Vodafone 亦會利用 web beacon (一種小型圖像檔案) 記錄用戶在 Vodafone 官網之活動歷程。Vodafone 有告知用戶如何拒絕 cookie 或調整瀏覽器軟體之隱私設定，並明列其所

[360] See generally, Broadband, at: http://home.bt.com/pages/navigation/privacypolicy.html?page=Broadband (2014/06/20 瀏覽).
[361] See generally, Cookies, at: http://home.bt.com/pages/navigation/privacypolicy.html?page=Cookies (2014/06/20 瀏覽).
[362] See generally, more about cookies, at: https://www.bt.com/static/includes/globalheader/cookies/more-about-cookies.html (2014/06/20 瀏覽).
[363]同前註。
[364] See generally, Legal, at: http://home.bt.com/pages/navigation/privacypolicy.html?page=Legals (2014/06/20 瀏覽).

使用之 cookie 類型[365]。

Vodafone 亦告知用戶其蒐集、處理與利用個資之目的，包括信用查核，通訊服務之提供，行銷、帳務處理、管理與保護電信通訊網路，研究與分析客戶之通訊利用習慣，以及在特定對象間分享用戶個資 (包括 Vodafone 集團內各子公司，提供服務之合夥商或代理商，信用查核機關，帳務催收機關，政府與執法機關，法院等)。Vodafone 亦告知用戶關於個資之安全維護措施，包括 Vodafone 委託第三方代為處理用戶個資之情形，Vodafone 將透過合約要求該第三方採取適當措施以保護個資安全；必要時 Vodafone 將派資安人員檢視該第三方之資安保護措施是否符合 Vodafone 之要求。

最後 Vodafone 告知用戶其個資相關權利，包括申請閱覽個資，更正個資，以及停止利用個資，並提供聯繫管道[366]。

五、小結

英國法制下，關於電信個資保護，係以 DPA 1998 作為一般法，其規範除適用於一般個資以外，亦適用於電信個資，但 2003 與 2011 Regulations 等特別法針對電信個資有特別規範者，則從其特別規定。其主要特色有以下三點

1. 強化個資主體自決權

英國法制下，無論一般個資或電信個資，其蒐集、處理、利用均係以事先取得個資主體同意 (opt-in) 為原則，opt-out 為例外，與前揭歐盟指令之立場一致。此種立法例固然符合個資保護之基本精神：即個人為自我資訊利用之決定權人，但此種高強度之立法例，在現代化資訊社會中，是否會造成業者大量利用個人資料之障礙或不便，最終形成整體社會交易成本之增加，是否有更妥適之個資利用與保障平衡點，有待後續案例與可能修法方向之持續觀察。

2. 電信個資類型化

因應電信通訊科技之進步，針對可能侵犯個資保障之電信個資利用態樣，盡

[365] Vodafone, Our cookie policy, at: http://www.vodafone.co.uk/about-this-site/our-privacy-policy/privacy-and-cookies/index.htm (2014/06/27 瀏覽).

[366] See generally, Vodafone, Understanding our privacy policy, at: http://www.vodafone.co.uk/about-this-site/our-privacy-policy/index.htm (2014/06/27 瀏覽).

量加以類型化，並加以明確之規範；如業者利用電子郵件行銷，電信用戶上網瀏覽網頁所形成之瀏覽歷程之記錄 (如 cookie)，以及流量資料與位置資料等，一方面強化現代生活中之個人通訊個資保障，同時減少法律適用之不確定性，使個資利用者 (如電信業者) 有遵循之依據。

3. 個資侵害事件處理流程明確

相較於我國個資法對於發生個資洩漏事件，僅於第 12 條簡略規定「發生個資侵害事件，應以適當方式通知當事人」，英國法明定個資利用者對主管機關與個資主體均有通報義務，並明確規範通報之時間點與具體通報內容，如事件性質，應對方案與後續處理程序等，值得我國效法。

綜上所述、茲就英國個資保護重點項目整理如下表所示：

表 3-8 DPA 1998 對個資之基本規範

	個資蒐集之條件	利用目的之告知	利用目的之限制	保存期限	個資分享
一般個資	事前同意(選擇加入)或另外九項條件得為利用；第 27 至 38 條例外	必須告知利用目的	必須基於特定目的	不得利用目的之必要期間	1. 個資委外處理，原則上應再履行告知義務 2.常態性個資分享，原則上應再履行告知義務 3. 臨時對第三方提供個資，符合第 27 至 38 條例外時得為之
敏感性個資	事前明示同意 (選擇加入)或另外一項條件得為利用；第 27 至 38 條例外	同上	同上	同上	同上

資料來源：本研究自行整理。

表 3-9 2003Regulations 與 2011 Regulations 對電信個資之特別規範

	電話行銷	電話號碼顯示	傳真行銷	電子郵件
利用要件	預錄式行銷；事先同意 (opt-in) 對話式行銷：有登錄於請勿來電名冊者，事先同意 (opt-in) 未登錄者，選擇退出 (opt-out)	選擇退出 (opt-out)；但為追查騷擾電話，或顯示報案或求救電話 (999) 不適用	事先同意 (opt-in)	事先同意，並不得隱瞞發信方身分，且須提供請求停止寄送之聯絡方式
利用目的	直接行銷	無特別規定	直接行銷	直接行銷
個資分享	無特別規定，依 DPA 1998 處理	無特別規定，依 DPA 1998 處理	無特別規定，依 DPA 1998 處理	無特別規定，依 DPA 1998 處理
	通訊履歷	流量資料	位置資料	帳務資料
利用要件	需告知利用目的並取得同意 (排除純粹傳輸技術行為)	須預先告知蒐集個資類型與利用期間否則不得蒐集 (2003 Regulation,7)	需取得同意並將個資主體去識別化，且須告知額外特定事項 (2003 Regulation, 14(3))	選擇退出 (opt-out)(2003 Regulation,9(1))
利用目的	無特別限制	限於下列目的：(a)帳務或流量管理；(b)顧客查詢；(c)詐欺之預防或偵測；(d)電信服務之行銷；(e)加值服務之提供。	無特別限制	無特別限制
個資分享	無特別規定，依 DPA 1998 處理	無特別規定，依 DPA 1998 處理	無特別規定，依 DPA 1998 處理	無特別規定，依 DPA 1998 處理

資料來源：本研究自行整理。

第四節 日本

一、日本法制之沿革及現況法制構造之鳥瞰

(一) 沿革

日本憲法第 21 條第 2 項明定「通信秘密」為基本人權而予以保障，其本旨乃藉由保障每個人經營社會生活上必要不可或缺之溝通交流手段「通信」，以更完整維護、內實「表現自由」，同時並兼含保障隱私權之作用。而所謂「通信」則指：特定之發出信息人與特定之收取信息人間，所進行之交流溝通行為，書寫信件固不在話下，包含電話、網路傳送電子郵件等所有型態之通信；基此概念下，如為對不特定多數人作開放性訊息之溝通者（又稱「具有公然性」之通信，則被認定為不屬於此處所稱之「通信」，而應歸屬「表現」自由之領域[367]）。

在此憲法保障人權之理念下，日本在 1953 年電信事業尚未民營化前，其公眾電氣通信法中即明定保障通信秘密，之後 1985 年電信事業民營後所訂定之「電氣通信事業法」，在其第 9 條亦設置保護「通信秘密」之規定:不同於其他民間部門，電氣通信領域，在早期即有保護「個人資料」之持續特有法制度存在，而當時對「通信秘密」所保護之範圍，「通信內容」固然被包含在內，而如通信之主體或通信本身是否存在之事實，是否在保護射程內，則係由法院判決累積予以界定[368]；自通信內容逐漸擴展至通信當事人之住所、姓名、電話號碼、發受信息場所、通信之日時、時間、次數等。

後至 1990 年後，因 OECD 公佈保護個人資料之八大原則[369]及 1995 年歐盟公布個人資料保護指令[370]，個資保護受到先進國家重視，而相繼全面性立法。當時

---

[367] 高橋和之，立憲主義と日本國憲法，第三版，頁 238，有斐閣，2013 年。

[368] 札幌地院昭和 59 年 3 月 27 日判決，判例時報(下稱判時)第 1116 條，頁 143。京都地院昭和 41 年 4 月 15 日判決，訟月 12 卷 6 號，頁 868。大阪高等法院昭和 42 年 12 月 25 日判決，判例タイムズ，218 号，頁 226。東京地院平成 14 年 4 月 30 日判決。

[369] 經濟合作及開發組織(Organization for Economic Co-operation and Development)OECD，宣示各加盟國處理個人資料時，最低限度應遵守之八大原則：Recommendation of Council Concernining Guideline to Protection of Privacy and Transborder Flous of Personal Data。

[370] Directive 95/46/EC of European Parliament and of the Council of 24 October 1995 on the individuals regard to the precessing of personal data and the free movement of such data, 395L,

日本則僅對「行政機關保有電子計算機處理個人資料保護法」立法予以規範[371]；故民間部門之電信事業則為依舊郵政省（現在之總務省）於 1991 年定立之「電氣通信事業有關個人資料保護之ガイドライン（Guide Line）[372]」（下稱電信 GL），以行政指導之方式規範電信事業者對個資之保護，但此僅為依 OECD 八大原則所作之一般性規定；至 1998 年郵政省再參酌 EU95 指令修正電信 GL，此時有關通信履歷（Itemised billing）、位置資料（Location data）、等資料已列入保護範圍[373]。之後因日本於 2004 年制定全面性規範公務部門及民間部門蒐集、處理或利用之個人資料保護法[374]，確立個人資料保護之總則性規範；總務省再於 2004 年 8 月修正電信 GL，後經數次修正，其最新修正版則為 2011 年總務省公告之第 465 號電信 GL，本研究主要即以此版電信 GL 為對象。

(二) 電氣通信業者保護個人資料法制之鳥瞰

綜上所述，日本為保護個資而對電氣通信業所建立之法制，為基於最上位憲法所保障之通信秘密及隱私權，而先依電氣通信事業法第 4 條第 1 項規定電氣通信業者不得侵害其所處理之通信秘密，及同法第 104 條對違反業者之處罰規定；而主管電氣通信事業之中央政府機關（先為郵政省，經政府組織精簡後歸併為現在之總務省），則訂立電信 GL 以行政指導方式規範者以保護利用電氣通信當事人之個資。又因個資法立法後，定位保護個資之總則性規範，故原為行政機關所頒定、位階為行政指導之電信 GL，亦須在此總則下，針對電信事業者所處理個資之特性及方式為更細緻之規範；且此時與通信本身無關，原不屬於通信秘密之電信契約當事人資料、電信費率支付方法、滯納電信費率金額等個資亦須全部納入保護對象。以下為日本規範電信事業者保護個資之法制構造

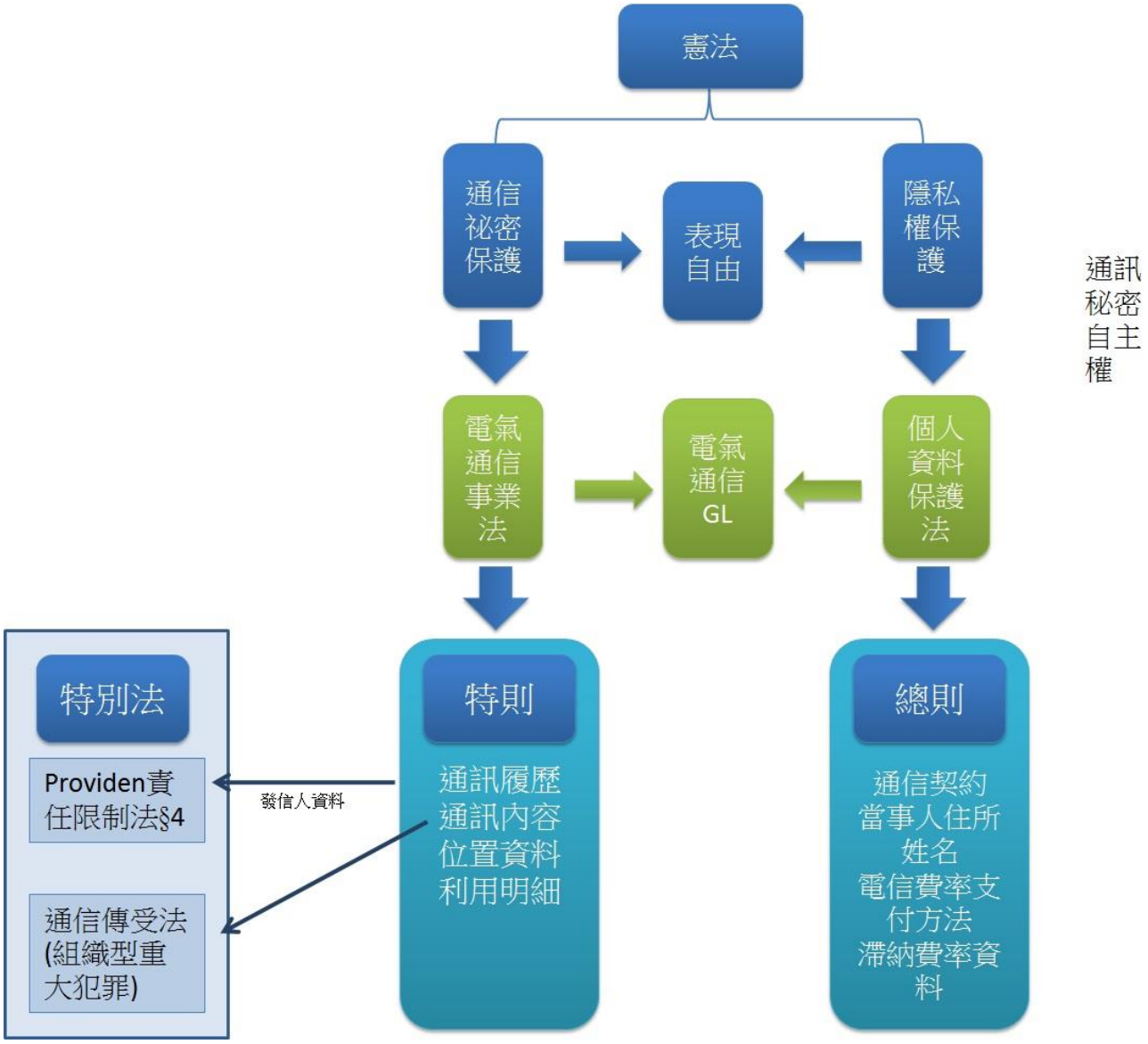
2246, official Journal L281.23/11/1995

371 昭和 63 年法律第 95 號：行政機關の保有する電子計算機處理に係る個人情の保護に關する法律。

372其詳細制定經過，請參閱，堀部政男，電気通信分野の個人情報保護に見る世界の潮流とわが国の取り組み，法律文化，2004 年 August，頁 13。

373 個人情報の保護に關する法律，平成 15 年法律第 57 號。

374 參閱岡村久道著，個人情報保護法(新訂版)，頁 167，商事法務，2009 年。


憲法
通信祕密保護
表現自由
隱私權保護
通訊秘密自主權
電氣通信事業法
電氣通信GL
個人資料保護法
特別法
Providen責任限制法§4
通信傳受法(組織型重大犯罪)
發信人資料
特則
通訊履歷
通訊內容
位置資料
利用明細
總則
通信契約
當事人住所
姓名
電信費率支付方法
滯納費率資料

二、電信 GL 之說明

如前述日本依循個資法所揭示之總則，再由總務省召集電信事業者，針對電氣通信業者所處理個資之特色，定出業者處理個資時應遵守之較高密度規範，故其電信 GL 共分為四大章共 30 條，第二章為總則性之個資處理共通原則，而第三章則為針對電信事業者所處理特別性質之個資所應遵守之有關蒐集、處理或利用要件。

(一) 個人資料處理之共通原則

此部分為電信 GL 第二章自第 4 條至第 22 條之規定，其重要內容說明如下：

1、 蒐集之限制

依電信 GL 第 4 條規定：電信事業者限於為提供電信通訊服務而有必要之場合，得為個資之蒐集。且對有關個人思想、信仰及宗教之資料，及有關人種、出身門戶、身體、精神障礙、犯罪前科、病歷及其他有造成社會差別待遇原因之虞之敏感性資料，原則上不得蒐集，僅在例外為保護本人或第三人之權利而有必要時，或其他社會上認為相當之場合，始得蒐集。

2、 利用目的之特定

依電信 GL 第 5 條規定：電氣通信業者，於處理個資時，應儘可能特定其利用目的。而上述特定目的不得超越為提供電氣通信服務所必要之範圍。且此特定目的應儘可能具體、明確，不得概括以「為提供服務」、或「為遂行業務」表明之；例如應表明為：「因確認立契約人本人」、「為通話費率之請求」、「費率、服務之變更及中止或廢止服務之通知」、而利用契約用戶人之姓名、住所、電話號碼[375]。

3、 利用目的之限制

依電信 GL 第 6 條：電信事業者於預先未得到本人之同意下，不得超越達成特定目的之必要範圍，為個資之處理。此為以特定利用目的，限制業者在一定範圍內為個資之蒐集、處理或利用。如電信事業者因合併或事業讓與等事由而自其他電信事業者繼受取得個資時，於預先未得到當事人之同意下，不得超越達成該當個資被繼受前之利用目的之必要範圍而為個資之處理或利用。

---

[375] 電気通信事業における個人情報保護に関するガイドラインの解説，頁 8。資料網址 http://www.soumu.go.jp/main_content/000254520.pdf

但例外於（1）法令有明文規定時，（2）為保護人之生命、身體或財產而有必要，且得到當事人同意有困難時，（3）為提升公眾衛生或推進兒童之建全育成而特別有必要，且得到當事人同意有困難時，（4）國家機關或地方自治團體或其他受其委託者，對法令所定事務之遂行有協助之必要時，因得到當事人同意，對該事務之遂行，有發生妨礙之虞時，則可不受原特定利用目的之限制而為該當個資之蒐集、處理或利用。與個資法基本原則不同而特別應注意的是，電信事業者所處理之個資如性質上屬於通信秘密者，如通信履歷等，除非有當事人同意者或有其他阻卻違法事由存在者，仍不得超越原特定利用目的而為該資料之蒐集、處理或利用，亦即此時並無上述 4 項例外事由之適用，係較個資法為更嚴之規範。

4、 利用目的之通知

電信事業者於取得個資時，除已預先公布其利用目的外，應儘速通知本人或公布其利用目的。電信事業者，如與本人間契約締結，而取得其於契約書面或其他書面（包含電子方式、磁器方式、其他藉由人知覺無法認識方式所做成之紀錄）上所記載個資、或其他取得自當事人記載於書面之個資者，應先對當事人明示其利用目的。但，為保護人之生命、身體或財產為緊急且有必要時，不在此限。又，上述通知義務於：①將利用目的通知本人或公布，有損害當事人或第三人生命、身體、財產、其他權利利益之虞者；②因通知本人或公布利用目的，而有致生損害於該當電氣通信事業之權利或正當利益之虞者，③對國家或地方自治團體遂行法定事務有協助必要者，因通知當事人或公布利用目的，將該當事務之遂行有產生障礙之虞者，④自其取得狀況觀之，得認為其利用目的為顯著者，則可例外免除。

5、 保存期限

依電信 GL 第 10 條規定：電信事業者原則上應於達成利用目的之必要範圍內定其個資之保存期限，於該當保存期限經過後，或該當利用目的達成後，應即刪除該當個資。而於有該當下列各款之事由者，得於保存期限經過後或利用目的達成後不予刪除：①基於法令規定必須保存者（例如稅法第 126 條），②得有本人同意者，③於電信事業者遂行自己業務之必要限度內，未刪除該當個資為有相當之理由者，例如：過去因滯納通信費率而停止利用者之資料，於解除契約後仍予以保存者。④除前 3 款事由外，未刪除該當個資為有特別之理由者，例如：因其為刑事事件之證據而有來自於搜查機關之保存請求時。

6、 隱私政策之定立

所謂隱私政策（privacy policy），係指該當電信事業者對推動個資保護上，所宣示之理念或方針。依電信 GL 第 16 條規定，電信事業者應公布其隱私政策，並予遵守。此乃為讓業者透明化其保護個資之義務，建立社會大眾對電信事業者保護個資之信賴，而上開隱私政策中應記載事項如下：①個人資料保護法及電氣通信事業法，其他關係法規之遵守；②電信 GL 之遵守；③電信 GL 第 16 條第 1 項各號所定應公布以下事項：甲、電信事業者之名稱；乙、個人資料之利用目的；丙、利用目的通知或公開、或因應來自本人要求訂正個資等之方法及程序；丁、當事人申訴之窗口；戊、認定個人資料保護團體之名稱及解決申訴之窗口；④電信 GL 第 11 條有關安全管理措施之方針；⑤有關保護利用者權利利益之事項：甲、對有本人之請求時，所因應之如指定電話行銷[376]傳送之停止等，當事人得自主請求停止利用之事項；乙、公告有無委託外部處理個資、明示所委託事務之內容及對象等，以透明化委託事務；丙、電信事業者考量其事業內容，應就個資利用類型，限定其利用目的並予以明示；或是電信事業者自主性建構讓本人得做選擇以限定利用目的之機制等，對當事人加強明示其利用目的。丁、個資之取得來源或取得方法（取得來源之種類等），儘可能具體載明。

7、 對第三人提供之限制

(1) 選擇加入制（opt-in）

依電信 GL 第 15 條第 1 項規定，電信事業者於事先未得到當事人之同意下，除有該當於以下所述各款之事由者，不得將個資提供給第三人。此處之同意不限為當事人之個別同意，如在雙方訂定之提供通信服務契約上，定有提供給第三人之約定條款時，亦得解釋為當事人同意：而其所列事由為①法令有明定者，如依法官發給令狀之強制處分而進行搜索、收押，或來自法律上有權限者之要求照會（如少年法第 6 號之 4，與律師法第 23 條之 2 等）。②為保護人之生命、身體或財產而有必要，且得到當事人同意為有困難時;惟有關通信秘密之個資，則必須有該當於緊急避難之要件等阻卻違法事由存在時，始得無須當事人同意。③為提昇公眾衛生或推進兒童之建全育成，而特別有必要，且得到當事人同意有困難時；④對國家機關或地方自治團體或受其委託遂行法令所定事務，有協助之必要者，因得到本人

[376] Direct mail：係指先鎖定特定對象以電話進行商品等之行銷。

同意有對該當事務之遂行產生障礙之虞時；故對第三人提供個資原則上採 opt-in 制；但應特別注意的是，如對第三人所提供之當事人個資為屬通信秘密保護之通訊履歷等資料時，則除有當事人同意，或法院核發之令狀，或有正當防衛、緊急避難等阻卻違法事由外，仍不得對外提供，是為更嚴格之規範。

(2) 選擇退出制（opt-out）

依本條 GL 第 2 項則另有選擇退出制度之設計；亦即，電信事業者一般而言，可依契約約定方式，於得到當事人同意而將其個資提供給第三人，如同意登載姓名於電話簿；然即使已得到當事人同意，仍應盡可能尊重當事人之意思，故當事人申請停止提供時，得利用本項規定選擇退場。據此，電信事業者依本條 GL 第 2 項規定，應將下列事項預先通知當事人，或置於當事人容易得知之狀態下；①對第三人提供為其利用目的，②提供第三人之個資項目；③對第三人提供之手段或方法，以方便當事人申請退出。

(3) 第三人範圍之界定(共有個資之容許)

因現今企業為節省成本方便自己為大量個資之蒐集或利用，而委託其它專業公司進行顧客資料之編輯、存檔、製成資料庫以方便檢索利用，已為非常普通之現象；如因此而提供個資給第三人，仍必須一一得到當事人同意，事實上耗時且增加成本;又因電信事業者如委託他人處理個資時，原依電信 GL 第 12 條即被課予有選定適當受託人之義務，且有對受託人進行監督之責任，如未善盡其責任時，委託之企業須與受託人負相同之法律責任；故電信事業者如為達成其遂行業務之必要範圍內，而委託他人處理個資者，應得視為電信事業者原本業務之施行，而該當受託人即不屬於本條之第三人。

再者，近年來企業競爭激烈，企業因經營策略、擴大市場之需要，常進行企業間之收購、合併等，而在企業間因營業之讓與、合併而繼受取得被讓與、合併業者之顧客資料時，如亦必須一一個別取得該當資料當事人同意時，勢必造成業者龐大負擔，形成企業合併之障礙；另一方面，依電信 GL 第 5 條第 2 項規定，伴隨事業移轉而取得轉讓企業之個資受讓者，仍應受轉讓個資之業者原所定利用目的之限制，而為該當個資之利用，故對個資本人而言，實質上僅為蒐集、處理個資之業者更換名稱而已，大體上不至於因而致其權利受損，故此時亦不宜將繼受

事業視為本條之第三人。[377]

此外，將特定集團之成員間，共同利用個資以進行事業之行銷或提供服務，降低營運成本，亦非常常見，例如金融控股集團各成員企業間，共同利用顧客資料、行銷金融產品，第一類電信事業者與同事業集團之第二類電信事業者，共同利用用戶個資推展業務；則此時集團間之其他成員，是否應認定為第三人，亦有爭議。

基於上述之考量，本條 GL 第 3 項規定，如有該當於下列之事由而取得個資者，不該當於本條所稱之第三人：①電信事業者為達成其利用目的之必要範圍內，將個資處理事務之一部或全部委託者；②因合併或其他事由而繼受事業者，因而伴隨取得之個資者；③與特定人間共同利用個資，而其宗旨及被共同利用個資之項目、共同利用者之範圍、利用者之利用目的、及對該當個資之管理責任人姓名或名稱，於事先已通知當事人，或置於容易得知之狀態下者。

據上，電信事業者如與自己集團間之關係企業共用客戶個資，並已於當事人契約上明定，或預先已公告於其隱私政策上時，即得彼此共用個資。

8、 應公告事項

為確保當事人行使公開等請求權之實效性，謀求保障電信事業者處理個資之公平性。故電信 GL 第 16 條規定，下列事項應置於當事人隨時得知之狀態（包含應當事人請求時，應即時回答。）：①該當電信事業者之名稱或姓名、②所有個資之利用目的、③當事人請求告知利用目的、閱覽、訂正個資等時之對應手續（如須負擔費用時，包括費用金額）、④該當電信事業者所設置個資處理申訴之窗口、⑤該當電信事業者如屬認定個資保護團體之對象事業者時，該當認定個資保護團體之名稱、及處理申訴之窗口。且本條 GL 第 2 項規定，如當事人要求通知具識別性個資之利用目的時，除有下列例外事由外，應即時通知之：①該當事人之具識別性個資之利用目的，已明確者；②有該當於前述電信 GL 第 8 條第 4 項 1 號至 3 號之事由者。亦即前所述，通知本人或公告利用目的，有害於本人或其他人之生命、身體財產或權利利益之虞者，或有害於電信事業者權利或正當利益之虞者，或對國家機關或地方自治團體遂行法定職務有協助之必要者，有產生妨礙之虞者。

[377] 園部逸夫編，個人情報保護法の解說，改訂版，頁 156，ぎょうせい，2005 年。

9、 個資之閱覽及訂正

依電信 GL 第 17 條規定，當事人請求公開其具有識別性之個資時（通知被請求個資不存在者亦同），電信事業者應即以書面方式（亦得依請求人所同意之方法）對當事人公開該當資料。但其公開有該當於下列事由之一者，得為全部或一部不公開：（1）有損害當事人或第三人之生命、身體、財產、其他權利利益之虞者；（2）對該當電信事業者適當業務之施行，有造成明顯障礙之虞者，例如在網頁伺服器（web-server）上暫時留存於 cookie 資料（上網履歷），電信事業者如要因應當事人請求公開，因請求人眾多，可能對其造成莫大負擔；（3）或違反其他法令者。

另外，如電信事業者受當事人請求訂正，補充或停止利用、提供個資給第三人之時，應即進行調查；如發現該當資料內容確非事實者，或已逾保存期限者，其他該當個資處理被認為有不適當者，應即進行訂正、補充或停止利用等。且電信 GL 第 19 條規定：電信事業者，應明定受理有關前述當事人請求閱覽、訂正、補充、停止利用等之應對程序、方法，以方便當事人行使其請求權；亦即受理請求之窗口、申請書之樣式、確認請求人為當事人、或其法定代理人代理之方法等均應訂明。應注意的是，本條第 3 項明定：雖該當代理人具有當事人具體委任而請求公開，如其係侵害本人通信秘密者，或有該當於前述第 17 條所定不得提供當事人閱覽之事由者，仍不得給予閱覽。

10、洩漏事故發生時之處理

電信 GL 第 22 條主要是電信事業者於所保有個資有洩漏等事故發生時，所被課予之通知及報告義務。電信事業者於上述事故發生時，應立即將洩漏等之相關事實通知當事人，並基於防止二次被害之發生、或為避免將來類似事件再發生之考量，應將事故發生之關係資料公開，此外尚須向主管機關總務省報告。特別者為其但書之規定，亦即如果該當個資之洩漏是因筆記型個人電腦等，手機末端、PDA 等通信端末機器、USB（隨身碟）等，外部紀錄媒體、被攜帶外出、利用之機器等遺失或被竊取而發生者，且其已先採取適當之保護技術措施，對當事人不會發生第二次被害時，即不在此限。例如紀錄媒體內之個資保存處，對所可能利用之全領域，已自動密碼化，或被密碼化之資料及其復原鍵已被分開做適當之保管或管理，除有權限掌管資料復原金鑰之人，其他人無法複製或再生者。

(二) 各種資料之蒐集、處理或利用之特別要件

在電信 GL 第三章係為各論，自第 23 條至 29 條為特別針對電信事業者提供服務時，所蒐集、處理或利用之個資區分為：通信履歷、利用明細、發信人資料、位置資料、滯納費率用戶等資料、發送垃圾郵件等契約用戶人之資料、電話號碼資料等七類型，再分別就其蒐集、處理或利用訂定特別之要件。

1、 通信履歷

此處所謂通信履歷，係指利用電信服務人其通信內容以外之通信日時、次數，該當通信之相對人、其他有關利用者之通信資料等。

(1)紀錄之蒐集

通信履歷通信之構成項目及內容，應屬電信事業法第 4 條第 1 項被保護之通信秘密；因此如電信事業者將之蒐集、儲存，為該當於侵害通信秘密，但為考量電信事業者必須保存通信履歷以計算通信費率，或製成明細表作為向用戶請求付款之根據，故不問契約用戶人是否同意，在必要範圍內對此資料之蒐集乃電氣通信業者之權利，亦為其義務。

(2)利用目的之限制

電信 GL 第 23 條規定：電信事業者限於為計算通信費率作成明細表以請求通信費用、處理申訴，防止不正當利用、其他遂行業務有必要之事由存在時，始得紀錄蒐集通信履歷。但如是為探知發信人為何人而進行解析通信履歷，則不僅為個資之目的外利用，亦構成通信秘密之侵害，故僅得在有阻卻違法事由存在時，始得為之。例如通信業者之伺服器或通信網路受到攻擊或有人大量散發垃圾信件傳染病毒時，為維護電信網路之安全、自由流通之環境及保護電信事業者正當利益，此時，蒐集探知發信人之位置及身分等個資，被認為屬於正當防衛之行為。[378]

(3)對第三人提供

因通信履歷係屬通信秘密，除為依從法院所發給之令狀等或有阻卻違法事由存在者外，亦不得提供給其它之人。故因應法律上有照會權限之人之查詢，參見前述電信 GL 第 6 條之解說，未必能阻卻違法，原則上被認為不適當之行為。此處最受爭議者，為以犯罪搜查為目的而提供監聽、監督通信內容之行為之合法性，

[378] 宍戸常寿，通信の秘密に関する覚書，高橋和之，古稀紀念論文集，「現在立憲主義の諸相」(下)，頁 151，有斐閣，2013 年 12 月

亦即日本之「通信傳受法」[379]之立法，是否侵害通信秘密而違憲則引發爭訟，直至最高法院平成 11 年判決後，始確認其合憲性。[380]

(4)保存期間

所蒐集紀錄之通信履歷，依前述電信 GL 第 10 條規定，原則上在紀錄目的必要範圍內設定保存期限，其期限經過後，利用目的已達成者，應儘速刪除。另外依刑事訴訟法第 197 條第 3 項，搜查機關於有扣押之必要時，得對電信事業者要求以 30 日以內為期限之保存。

2、 利用明細

所謂利用明細是指：記載電信契約利用電氣通信之日期，通信時間，各個通信之對方、依一定費率計算之通信費用、及其他記載有關通信契約用戶資料之書面。如此之利用明細，對通信業者而言為顯示其請求支付費率之根據，對契約用戶人而言亦得用以確認其費用，故為重要資料；但自其記載資料內容觀之，利用明細與前所述屬於通信秘密之通信履歷幾乎相同，故須考量與通信秘密為相同程度之保護。

依電信 GL 第 24 條規定：①記載資料之範圍：不得超越達成利用明細目的之必要範圍。利用明細記載事項為得確認、計算費率有關利用狀況之資料，故限定於通信開始日時，通信時間、對方電話號碼、各次通信之金額、如為國際通信時其通話對方地點等，較為適當。又如有侵害通信對方隱私之不必要資料亦不適合記載，例如對方為利用手機、PHS 者、而表示其收受訊號之地區。②資料之提供閱覽：得閱覽利用明細人，基本上應為契約用戶本人，但有契約用戶人通報之其他經常使用者存在時，上述使用者或其他關於閱覽有正當利益之費率支付人，亦包含在內。

3、 發信人資料

所謂發信者資料係指包含發信人電話號碼、姓名、住所、生年月日、其他記述、得識別個人之編號、記號或其他符號、影像或聲音或發信位置等得以識別該當特定發信人之資料，上開資料常藉由發信電話號碼通知服務而提供給收信人。

[379] 相當於我國之通訊保障及監察法。
[380] 最高法院平成 11 年 12 月 16 日判決，刑集 53 卷 9 號，頁 1327。

(1)opt-out 之制採用

因上開資料為該當於通信秘密，依電信 GL 第 25 條則委由發信人自己就每一個通信判斷是否通知對方。故其規定電信事業者應就每一次通信，設置讓發信人得阻止通知發信者資料之機能，此為採 opt-out 機制；換言之，發信人就其通信未阻止提供發信者資料通知服務時，即得解釋為發信人對其通信之對方並無隱匿以保護其資料之意思，故不構成侵害通信秘密。且電氣通信業者應將前開阻止通知機能、方法等讓發信人(利用者)充分理解，以保護發信人(利用者)之利益。

(2)對第三人提供之禁止

電信事業者除有提供通信者資料服務、其他服務之必要者外，不得將發信人資料提供給第三人；但如發信人、受信人雙方同意者，或依從法院發給之令狀者，或依從搜查機關及被害人之請求為追蹤現正利用電話進行恐嚇、脅迫、犯罪者之所在地者，或如有自殺預告等，在對人之生命、身體等有急迫危險之緊急通報，依該通報人之請求而進行搜索者，或其他有阻卻違法事由者，不在此限。應注意的是如其僅依通信當事人一方同意時，仍不符合本項要件。

4、 位置資料

(1)性質

所謂「位置資料」是指：表示移動通信體端末持有人所在場所之資料[381]。由電信事業者所保有之位置資料，係屬通信構成要素，故應依電氣通信事業法第 4 條第 1 項予以保護之；對此亦有認為在通話以外時移動體端末持有人，在每一個區域移動而被送傳到基地台之位置登錄資料，僅是以讓通信能接通為前提之機械式被傳送往電信事業者，而被積存於服務控制局之資料，應非屬通信秘密，應解為屬隱私保護之事項；但即使得如此解釋，因其仍為具有私密性、保護必要性高之資料，與通信間又有密接不可分之關係，故應視同通信秘密予以保護[382]。又 GPS 之位置資料是否為通信秘密，雖然其相較於基地台位置資料具有更高之精確度，然其並非以成立通信為前題而被傳送至電信事業者之資料，故不屬於通信秘密，

[381] 此處之位置資料應將第 25 條所規定之表示發信人位置之資料除外；其為此基地台區域或登錄區域為更狹小之範圍。

[382]宍戸常寿，前揭註 378，頁 509。

而應為隱私保護之問題。[383]

(2)對搜查機關之提供

依通信 GL 第 26 條，準用通信秘密之保護規定，除有當事人同意者、依從法院發給之令狀者、或有其他阻卻違法事由者外，不得提供給他人。又依本條第 3 項規定：電氣通信業者，於有來自搜查機關請求位置資料之提供時，不受通信 GL 第 4 條規定之限制，但應將該當位置資料被取得一事讓利用者得知，且須從法院所發給之令狀始得提供。

(3)對第三人之提供

電信事業者提供位置資料服務，或在與第三人合作下提供時，應考量其對社會之有用性與通信秘密或隱私保護間之衡平，故電信事業者提供位置資料給加入之用戶者或其所指示之人，依本條第 2 項規定，應採以下具體「必要措施」：①基於用戶或利用者之意思進行位置資料之提供，此同意之取得，除為各別每個位置資料之要求提供時外，亦可能在服務提供開始之事前，且事前同意原則上應得隨時撤回。②應確保電信服務利用者對位置資料之提供有認識、預見之可能性，例如藉畫面表示或或移動體端末之鳴動等方法，使其提供之事有被認識之可能。③應考慮採取無權限者不得監看移動體端末所顯示之位置資料、或設定密碼、限制近用等措施；此外應設計讓自己所管理之基地台資料，不被他人不當利用之管理規則。④與第三人合作而提供服務時，考量依記載於合作契約之保密條款等方式，以保護使用電信服務者之隱私。

5、 滯納支付費率者之資料

依電信 GL 第 27 條規定，電信事業者，為防止有關電氣通信服務費率不支付，或不正當的利用攜帶型音聲通訊服務，而有特別必要且被認為適當時，與其他電氣通信業者間，得交換滯納支付費率者等資料。所謂滯納支付費率者等資料，包含滯納者之姓名、住所、生年月日、未支付金額等資料。

本條定立之理由為：與其他業者間因未支付費率而被解除契約者，因再與其他業者締結契約，其結果同樣不支付費率之可能性極高；或與因未同意他電信事

[383] 同前揭註 375，總務省公告之，電気通信事業における個人情報保護に関するガイドラインの解説，頁 45。

業者進行契約當事人確認，而被停止利用者締結契約時，同樣可能會發生無法確認當事人之結果，不僅造成無法請求支付費率之事件，亦與利用匿名手機進行不正當利用之行為有連帶關係；為對應上述問題之發生，容許最小限度內之滯納費率者等資料在業者間進行交換，以阻止滯納費率者重新定立新契約，對於減輕業者經營風險有特別必要性時，滯納費率者等之資料交換被認定為合法而得以進行。

(1)資料交換之同意與告知

於業者間交換滯納費率者等資料時，應在契約條款上予以明記並得到契約當事人之同意；且依電信 GL 第 2 項規定，欲進行前項資料交換者，應在事前將下列事項通知當事人或置於其容易得知之狀態，①交換之意旨，②被交換之滯納費用者等資料項目，③交換資料之電信事業者範圍，④對被交換之資料負有管理責任者之姓名或名稱。

(2)目的外利用之禁止

進行交換滯納費率者資料之電信事業者，不得將該當資料，利用於審查加入契約以外之目的；因滯納費率者資料，性質上為個人信用資料之一種，故不得為目的外利用。

6、 寄送垃圾郵件之契約用戶資料

有關寄送垃圾郵件等[384]，除其行為構成違法[385]外，因送信量大，對電信事業者之服務系統造成負擔、引起其他利用電信服務者電子郵件收送信之遲延等障礙，可能對資訊通信網路造成極大損害。而寄送垃圾郵件之契約用戶，如於受一家電信事業者停止利用之處置後，又與其他電信事業者締結契約，而得再繼續寄送垃圾郵件等時，事實上未能有效防止其違法行為。又因發送垃圾郵件等契約當事人之資料，性質上無關郵件內容，送信對象、日時、收送場所、送信次數等事實，非屬個別郵件之送信資料，一般不認為其屬通信秘密資料。故電信 GL 第 28 條規定，電信事業者為防止因電子垃圾郵件濫發等造成電子通訊網路之障礙，於必要且被認為適當時，得與其他電氣通信業者，交換該當濫發郵件等契約當事人資料，

[384] 例如偽造送信者資料（發信之電子信箱號碼），以廣告、宣傳等目的大量寄送電子郵件，或為自己或他人營業而以屬電子信箱作發信網址而大量寄送電子郵件。

[385] 平成 14 年法律第二十六號。

如姓名、住所等。

而此個資之交換與前述 5 交換滯納費率者資料同，須預先通知或置於當事人可得而知之狀態，亦不得將該當交換所得契約當事人資料，用於締約時審查以外之目的上。

7、 電話號碼資料(提供查詢電話號碼之服務)

電氣通信業者常將用戶電話號碼印發電話簿,或提供電話查詢服務業務使用，電話號碼雖為個資，一般被認為公開為有利於人與人間之溝通交流，但仍考量因此而侵害契約當事人之隱私，故電信 GL 第 29 條為如下之規範：

(1)選擇機制之建立

亦即電信事業者須給契約用戶選擇是否加入之機會,如當事人選擇不加入時，應即時自電話簿或電話查詢服務對象中移除其資料。此處要注意者為電話服務以外之有關通信服務之 ID（電子郵件之信箱號碼）,因日本考量現今其並未如電話號碼之公開狀態，故為非為本條規範對象，其處理依前述電信 GL 第二章有關個資保護之共通原則。

(2)記載項目之最少化

記載於電話簿上之得以確認特定當事人之資料,應以最低限度為範圍,姓名、住所、電話號碼為必要登載事項，除此之外之資料即不適合登載；且住所是否全部登載亦非無檢討空間。

(3)對外提供

電話號碼之對外提供，依前述一般原則，例如照會特定通話之發信電話號碼所屬用戶為何人，因其為有關通信秘密之事項，則需要有法院發給之令狀等前所述祖卻違法事由存在時，始得為之；但若僅為一般查詢某電話號碼所屬之用戶人為何人，因未涉及通信秘密，則僅要屬法律上有照會權限人即可。

三、小結

(一) 行政指導方式之規範

綜觀日本對電信事業者蒐集、處理或利用通信服務者之個資，除以憲法為依據而在電信事業法第 4 條定有通信秘密保障規定，而另一方又依個人資料保護法

建構規範之最低框架，再由中央主管機關制定位階等同於行政指導之 GL，揭示電信事業者在個資法遵守上被課予之行為準則與義務。

(二) 特別規範之個人資料

在日本之 GL 中特別將電信事業者因提供電信服務時所蒐集、利用之個資中，有關通信履歷(不包括通信內容之通信時日、通信相對人、通信次數)、利用明細、發信人資料、位置資料、滯納費率用戶之資料、發送垃圾郵件等契約用戶資料、電話號碼提供服務資料等 7 種類型之通信個資，特別有別於個資法，另訂立其蒐集、利用、或提供給第三人之要件，為較嚴密之保護，此可謂是日本電信 GL 最大之特色。因日本自來民族性保守講究團體之一致性，因此即使定位僅為主管機關發布之「行政指導」GL，該當受監督領域之事業仍不輕言違反，以免自己被同業排擠。

(三) 一般性個資之要件

表 3-10 一般性個資之要件

要件 / 個資	利用目的告知	個資保存期限	利用目的限制	與第三人共有共同利用個資	對第三人提供之限制	事故發生之通知
除通信內容、通訊履歷等特別規範之 7 種個資外	除有預先公告外，應儘速通知當事人，但如以書面契約取得當事人資料者，則應明示	於達成利用目的之必要範圍保存	於事先未得本人同意下，不得為超越原公告或通知之特定目的外之利用	1.因達成利用目的，而委外處理時，與受委託人共有者 2.因事業繼承或合併而取得者	原則上採 opt-in 制，須事先得到當事人同意	應即通知當事人，公開事故之發生，並向主管機關報告
	有 4 個例外事由得不通知當事人	有 3 個例外事由得不採保存期限經過後刪除之	有 4 個例外事由時得為目的外利用	但共同利用個資之項目、共同利用者之範圍、利用目的等事項，應事先通知當事人	但有 4 項例外事由	但如有採保護技術措施之可攜式外接載體，當事人不會第二次被害時，不在此限

資料來源：本研究自行整理。

(四) 特別規定之要件

表 3-11 特別規定之要件

個資種類／特別要件	通信內容	通信履歷	利用明細	發信人資料	位置資料	滯納費率資料	垃圾郵件之契約用戶資料	提供查詢電話號碼之服務
蒐集及當事人之告知	原則上不得進行，除符合通信傳受法之要件者外	無須得到使用人之同意	無需契約當事人之同意	提供給通信之對方採 opt-out	在提供加入者服務時應 opt-out 制	必須得契約用戶之同意	預先告知當事人或置於其所得知之狀態	告知….採同意加入 opt-in 制
利用目的之限制	提供檢警偵查組織型重大犯罪	限於為計算通信費率、制成費率明細表、處理申訴、防止不正當利用等目的	不得超越達成利用明細利用目的範圍外	原則上只用在提供服務之用	以通信能接通為目的或提供加入者服務	不得用於審查加入契約外	防止垃圾郵件之濫發，不得用於審查加入契約外	提供電話查詢服務
對第三人之提供	只限於通信傳受法之規定	原則上禁止，除有法院發給令狀，或有阻卻違法事由外	例外得提供給契約用戶所指定之使用人或對閱覽明細有正當利益之人	則禁止，但如通信雙方當事人同意或法院發給令狀，或有阻卻違法事由時例外	原則上禁止，僅於當事人同意或法院發給之令狀，或有其他阻卻違法事由外得例外	得與其他電信業者交換	得與其他電信業者交換	

資料來源：本研究自行整理。

第五節 韓國

一、 法制現況

韓國於 2011 年 3 月 29 日公布施行個人資料保護法[386]，而在此之前有關個人資料保護之法律為公、私部門分治二元制，亦即公務機關係依公共機關個人資料保護法，非公務機關則區分不同領域定有資訊通信網利用及保護法、信用資料保護法、通信秘密保護法等[387]；因在高度資訊化社會之今日，法制上卻欠缺全面統一之規範，導致有缺漏未受法保護之領域，及各法規間要件寬嚴不一之不合理現象發生[388]；故而自 2004 年開始韓國花費七年時間立法，完成公、私統一，最基本總則性之個資保護法規範。

又韓國預定於 2014 年 6 月完成相關法律規範之整理，其檢視目前各法律有重複或不合時宜的部分、強化個人資料保護委員會之機能、提升個人資料保護之執行效率等。目前已擬定之新個人資料保護法制大致上將過去分別散落於教育、醫療、公共行政、金融/信用、資訊通信等五大領域的個人資料保護重新整理，以個資法規範個人資料保護基本原則並作為整套體制之基本框架，將各領域的個人資料保護納入此一框架，去除重複、多餘或缺漏的部分，以兼顧提升個人資料保護效率和產業發展的策略[389]。

---

386 法律第 10465 號

387 參看張睿英，韓國における個人情報保護法制の問題と改善案，The journal of Environmental and Information Studies, Tokyo City University (11), 39-46(2010)。

388 參看崔祐溶，韓國の個人情報保護法の内容と個人情報保護管理体系。
http://in-law.jp/archive/kenkyukai/2012-02-18/che.pdf

389 個人資料保護相關政策與機制

(1) 韓國個人資料保護法的制訂過程及其內容(韓國資料保護振興院)
(2) 2015~2017 年個人資料保護基本計畫(行政安全部)
(3) 個人資料保護法律手冊(行政安全部、放送通信委員會)
(4) 現行《資訊通信網利用促進與資料保護法》個人資料保護規定之適用範圍(放送通信委員會)
(5) 民間企業個人資料保護手冊(行政安全部)
(6) 通信業者關於利用者保護業務評價相關細部施行方案之研究(放送通信委員會)
(7) 通信業者關於利用者保護業務評價制度之研究(放送通信委員會)
(8) 個人資料保護委員會之職務與角色(個人資料保護委員會)
(9) 資料通信服務提供者之個人資料保護指南(放送通信委員會、韓國網路振興院)

二、個資法之重要內容

(一) 個資法之適用對象

個資法之適用對象包括：1、國會、法院等機構及國家人權委員會、 中央與地方行政機關、各種行政法人等約 28,000 個公共機關；2、72 個產業部門及其所屬人員；3、 產業公協會、校友會、職業團體等非營利組織。

個資法之個人資料處理者 的範圍：1、國會、法院等機構及國家人權委員會、中央與地方行政機關、各種行政法人等約 28,000 個公共機關；2、72 個產業部門及其所屬人員；3、產業公協會、校友會、職業團體等非營利組織。

(二) 個資法的基本原則

依其個資法第 3 條保護個資之基本原則有八項：1、必須根據目的在必要且最小的範圍內，合法並適當蒐集；2、必須在處理目的範圍內，保障其正確性、完整性與最新性；3、必須達到處理目的之明確化；4、必須在必要目的之範圍內合法處理，禁止在目的以外範圍之運用；5、必須考量資料主體的權利侵害性，確保其安全性；6、必須經常公開個人資料處理事項；7、必須保障閱覽請求權等資料主體的權利；8、必須竭力遵守及實踐個人資料處理者之責任，確保信賴性。

(三) 個人資料之蒐集與利用

依個資法第 15 條規定:

1、蒐集與利用之要件 個人資料處理者，得在符合下列要件下蒐集個人資料

①獲得資料主體之同意者

②法律有特別規定或為遵守法律義務而不可避免者

③為執行公共機關依法所訂之所屬業務而不可避免者

④為簽署及履行與資料主體之契約而不可避免者

⑤在資料主體及其法定代理人無法行意識表示或住所不明無法取得事前同意

---

(10) 個人資料保護法之主要議題及對應策略(韓國網路振興院)

(11) 新修正資料通信網法(資訊通信網利用促進與資料保護法)個人資料保護制度(韓國網路振興院)

(12) 移動通信服務提供者之個人資料保護方針(放送通信委員會)

之情形下，判定對資料主體及第三人具有急迫性之生命、身體、財產利益之必要者

⑥為達成個人資料處理者之正當利益,且明顯比資料主體的權利具有優先性，允許資料處理者在不超過其正當利益及具有相當關聯且合理之範圍內行之

資料處理者在執行上述各項時，必須事先告知資料主體以下各項，並且告知蒐集時應告知事項須遵守下述說明。

2、告知蒐集時應告知事項

蒐集者應告知資料主體下列事項，而各項有變更情形時亦須告知且獲得同意：

①個人資料之蒐集與利用目的

②欲蒐集之個人資料項目

③個人資料之保有與利用期間

④有拒絕同意權利之事實及拒絕同意而有不利益情形之不利益內容

3、資料蒐集之限制

依個資法第 16 條，個人資料處理者蒐集個人資料時，必須依其目的蒐集必要而最少的個人資料；個人資料處理者在獲得同意蒐集必要而最少資料以外之資料時，必須具體告知無法取得同意的事實後才得蒐集個人資料；個人資料處理者不得以資料主體不同意蒐集必要而最少資料以外之資料的理由，拒絕對資料主體提供財貨與服務。

4、對第三人之提供

依個資法第 17 條，個人資料處理者在獲得資料主體之同意及不超越蒐集目的之範圍時，得將個人資料提供給第三人；個人資料處理者必須在取得資料主體同意時，告知以下各項內容，並且在各項有變更情形時都必須告知且獲得同意：

①個人資料接受者

②個人資料接受者之利用目的

③所提供之個人資料項目

④個人資料接受者之資料保有與利用期間

⑤有拒絕同意權利之事實及拒絕同意而有不利益情形之不利益內容

個人資料處理者將個人資料提供給國外第三人時，亦必須告知資料主體上述各項內容並取得同意，如有違反本法之規定，不得簽訂個人資料移轉國外契約。

(四)蒐集利用與提供之限制

依個資法第 18 條:

1、蒐集之限制

個人資料處理者不得逾越蒐集、利用與提供目的之範圍，惟在該當下列各項事由下，除對資料主體及第三人有不利益疑慮之資料以外，可將個人資料目的以外的資料提供給第三人：①、獲得資料主體之特別同意；②、其他法律有特別規定；③、資料主體及其法定代理人無法行意識表示或住所不明無法取得事前同意之情形下，判定對資料主體及第三人具有急迫性之生命、身體、財產利益之必要者；④、為統計及學術研究等目的無須告知特定個人而提供個人資料。⑤、 依據其他法律規定不得不執行主管業務時，經由保護委員會之審議及決議者；⑥、為履行國際協定而必須提供他國政府與國際組織者；⑦、犯罪搜查及公訴之提起與維持等必要情況者；⑧、法院裁判業務所需要者；⑨、行刑、監護與保護處分所需要者。惟，第 5~9 項限定於公共機關。

2、處理之限制

個人資料處理者在獲得資料主體之同意及不違反蒐集目的之範圍時，得將個人資料提供給第三人；個人資料處理者必須在取得資料主體同意時，告知以下各項內容，並且在各項有變更情形時都必須告知且獲得同意：

①.個人資料接受者 ②.個人資料之利用目的(提供時敘明資料接受者之利用目的)③.利用與提供之個人資料項目④.個人資料之保有與利用期間(提供時敘明資料接受者之保有與利用期間)⑤.有拒絕同意權利之事實及拒絕同意而有不利益情形之不利益內容。

(五)資料來源之告知

依個資法第 20 條，個人資料處理者從資料主體以外之處蒐集並處理個人資料

時，如資料主體提出要求的話，必須告知下列事項：1、個人資料之蒐集出處；2、個人資料之處理目的；3、個人資料處理停止規定。惟，如依個資法第 32 條

為安全行政部行使業務所需而規定登錄事項，或因告知而對其他人之生命、身體有侵害疑慮，或是對他人的殘產及其他利益有損害疑慮者，則不在此限。

(六)取得資料主體同意之方法

依個資法第 22 條，個人資料處理者必須根據個別同意事項明確使資料主體(包含法定代理人)瞭解之後取得同意，取得資料主體同意之方法包括：1、個人資料處理者必須在取得資料處理同意時，在契約上載明「無須資料主體同意處理之個人資料」及「必須取得同意處理之個人資料」；其中，「無須同意處理之個人資料」的舉證責任由個人資料處理者負擔。 2、個人資料處理者為保護資料主體之財貨、服務或是勸誘買賣而取得處理個人資料之同意時，必須使資料主體明確瞭解後獲得同意。3、個人資料處理者處理未滿 14 歲兒童之個人資料時，必須取得其法定代理人之同意，為此得在無法定代理人同意之下，自該兒童處蒐集最少且必要之法定代理人個人資料。

(七)身分證號之處理限制

依個資法第 24 條，個人資料處理者除了以下各項情況以外，不得處理身分證號：1、法律具體要求或許可身分證號之處理；2、判定對資料主體及第三人有急迫性之生命、身體、財產利益之必要者；3、安全行政部認定不可避免必須處理身分證號之情況。惟，即使依據此三項規定得以使用利用者之身分證號，也必須提供不使用利用者身分證號確認本人的方法。

三、2013 年個資法新修正之重要內容

2013 年 9 月 30 日韓國政府新修正個資法(2014 年 8 月 7 日開始施行)，針對個人資料保護之技術性保護措施義務化之內容進行增修，要求企業必須建置顧客資料流通與遮斷措施方案。內容包括三項：1、身分證號之蒐集利用：原本在資料主體的同意並具體根據法令規範得蒐集利用；新修正為原則上禁止身分證號之處理，並且必須在本法施行 2 年內銷毀(2016 年 8 月 6 日)。2、罰款制度：原本無此規定；新修正為身分證號遺失、盜用、洩漏、變造及毀損時，得罰金 5 億韓元，惟安全性確保措施均已遵行者例外。3、CEO 懲戒勸告：原本規定在職務執行者違反個人

資料法規時，勸告其所屬機構之最高首長予以懲戒；新規定則明確將該當責任者之代表人及人員全都納入懲戒範圍。

四、資訊通信網利用促進與資料保護法之重要內容

(一) 個人資料之定義

依資訊通信網法第 22 條，其所定義之「個人資料」，包括得以明顯據以知悉特定個人的資料，如姓名、身分證號、生日、地址、生物性資料等，以及顯示特定個人之過去和現在的狀態，例如教育、財務、診療與健康情形等；同時，也包括即使根據該資料無法知悉但與其他資料連結可輕易辨識特定個人之資料，例如特定社團的平均年薪、特定大學某一年度畢業生的就業率等。換言之，只要是可以直接顯示或間接連結特定個人的資料均屬個人資料保護的對象，包括代號、文字、聲音及影像等資料。

(二) 2、個人資料蒐集與利用之同意

依資訊通信網法第 22 條，資訊通信服務提供者欲利用資訊通信利用者之個人資料而蒐集時，必須充分告知利用者下列各項並取得同意，並且在各項有變更情形時也必須告知且獲得同意：(1)個人資料之蒐集與利用目的；(2)欲蒐集之個人資料項目；(3)個人資料之保有與利用期間。惟，如有下列各項情形時，可未經利用者的同意而蒐集和利用其個人資料：(1)為履行資訊通信服務提供契約，因經濟、技術性因素而有取得同意之困難者；(2)根據資訊通信服務之提供進行資費計算；(3)其他法律有特殊規定者。

(三) 個人資料蒐集之限制

依資料通信網法第 23 條，資訊通信服務提供者不得蒐集思想、信念、過去的病歷等與個人權利和利益有關之具有侵害私生活疑慮的個人資料。惟，如取得利用者的同意或是根據其他法律許可之特別蒐集對象的個人資料，得蒐集其個人資料。

資訊通信服務者在蒐集利用者個人資料時，必須蒐集為提供資訊通信服務所需之必要而最少的個人資料；不得以利用者不提供必要而最少資料以外之資料的理由，拒絕提供服務。

(四) 身分證號之使用限制

依資料通信網法第 23-2 規定，資訊通信服務提供者除了以下各項情況以外，不得蒐集利用該利用者之身分證號：(1)獲得「本人確認機構」之指定；(2)法律許可蒐集、利用利用者之身分證號；(3)放送通信委員會公告之為營業目的不可避免蒐集、利用利用者之身分證號的資訊通信服務提供者。惟，即使依據此三項規定得以使用利用者之身分證號，也必須提供不使用利用者身分證號確認本人的方法(以下稱為「替代手段)」。

(五) 「本人確認機構」之指定

資料通信網法第 23-3 所謂之「本人確認機構」之指定，是一種替代身分證號的手段，由放送通信委員會指定。該機構必須具備確保本人確認業務安全性之技術、財務與管理能力，並具有一定規模之相關設備。

(六) 個人資料提供之同意

依資料通信網法第 24-2 規定，資訊通信服務提供者欲將利用者之個人資料提供給第三人時，除了根據資訊通信服務之提供進行資費計算(第 22 條第 2 項第 2 款)以及其他法律有特殊規定者(第 22 條第 2 項第 3 款)以外者，均必須將下列各項告知且獲得利用者之同意：(1) 接受者；(2)接受者之資料利用目的；(3)提供之個人資料項目；(4)接受者之資料保有與利用期間。接受者不得在未經利用者同意或其他法律有特殊規定之下，將所接受的利用者個人資料再轉手給第三人，或是使用於接受目的之外的用途。

表 3-12 韓國有關個資蒐集、處理及利用之要件

	利用目的之告知	利用目的之限制	與第三人共同利用或提供第三人	事故發生之通知	個資保存期限
一般個資(身分證字號除外)	須事先告知	不得逾越原蒐集之目的	需得到當事人同意。例外於法律有特別規定或履行法律義務，或公務機關執行法定職務者，得無須同意。	立即通知資料相關當事人及呈報安全行政部。	無
個資網蒐集之資訊通訊	須事先告知，且得到當事人同意始得蒐集	限於提供通訊服務之必要範圍	除為提供資費計算、或法律有特別規定外，必須事先得到當事人同意。		無

資料來源：本研究自行整理。

表 3-13 韓國個人資料保護相關法律

編號	所屬機關	法令名稱	主要內容
1	**行政安全部**	**個人資料保護法**	● **對象：公、私部門** ● **個人資料處理標準及保護措施**
		公共機關資料公開法(§9)	● 對象：公共機關 ● 個人資料之管理和技術性保護
		民怨事務處理法(§22)	● 對象：公共機關 ● 民怨當事人身分資料洩漏禁止
		身分登錄法(§30)	● 對象：行政機關及行政業務委託機關 ● 個人資料非公開
		電子政府法(§4)	● 對象：中央行政機關及地方政府 ● 個人身分登錄資料處理與保護
		電子署名法(§24)	● 對象：行政機關 ● 個人資料及隱私保護基本原則
		公職人員倫理法(§13)	● 對象：行政機關 ● 公職人員財產登記資料保護
2	**放送通信委員會**	**資訊通信網利用促進與資料保護法**	● **對象：通信業者** ● **個人資料管理和技術性保護**
		位置資料保護與利用法(§3)	● **對象：通信業者等位置資料業者** ● **個人位置資料秘密保護**
		網址資源法(§15)	● **對象：網址管理機關** ● **網址使用者資料保護**

3	金融委員會	信用資料利用與保護法(§16)	● 對象：金融機關、信用評比機關 ● 信用資料之提供、運用及保護措施
		保險業法(§177)	● 對象：保險業者 ● 個人資料洩漏/提供之禁止
		銀行法(§21 之 1)	● 對象：金融機構委員及職員 ● 資料洩漏、目的以外用途之禁止
		金融實名交易與秘密保障法(§4)	● 對象：金融機構 ● 交易資料之運用及保護
4	保健福祉部	醫療法(§21 之 1)	● 對象：醫療機構 ● 患者交易資料之運用及保護
		健康診察基本法(§18)	● 對象：中央機關、地方政府 ● 診察資料之運用及保護
		器官移植法(§27)	● 對象：器官移植管理機關 ● 器官移植者秘密保護
		生命倫理與安全法(§35)	● 對象：健康診察機關 ● 遺傳資料保護
		人體組織安全與管理法(§2)	● 對象：醫院 ● 組織捐贈者資料保護
5	教育部	教育基本法	● 對象：教育機構 ● 學生基本資料與生活紀錄資料保護
		初中等教育法	● 對象：初、中、高等學校 ● 學生相關資料提供之

			限制
6	**法務部**	**通信秘密保護法**	● **對象：通信業者及通信網管理者** ● **通信網資料傳輸之保護**
		出入境管理法	● 對象：出入境管理業務專責機構與人員 ● 出入境管理資料之保護
7	公交易委員會	消費者基本法	● 對象：中央機關、地方政府 ● 消費者個人資料之保護
		電子交易消費者保護法(§11)	● **對象：電子交易利用企業** ● **消費者資料利用之保護**
		訪問買賣法(§48)	● 對象：訪問買賣業者 ● 消費者資料誤用、濫用及盜用之防止
8	企劃財政部	關稅法(§116)	● 對象：海關人員 ● 關稅資料之保護及利用
		關稅師法(§14)	● 對象：關稅師、關稅師助理 ● 業務機密
9	產業通商資源部	電子交易基本法(§12)	● **對象：電子交易利用者** ● **利用者個人資料之保護**
10	外交部	護照法(§18)	● 對象：中央機關(外交部) ● 個人資料保護措施
11	國土交通部	仲介師業務與不動產交易	● 對象：仲介業者、仲

		申報法(§22)	介師 ● 業務機密
		汽車管理法(§69)	● 對象：中央機關(國土交通部) ● 汽車所有人之隱私保護
12	雇用勞動部	勞動委員會法(§28)	● 對象：勞動委員會委員、職員 ● 業務機密
13	國稅廳	國稅基本法(§81 之 13)	● 對象：國稅廳、稅務師 ● 企業及個人納稅人資料之保護
14	統計廳	統計法(§33)	● 對象：中央機關、地方政府 ● 統計用個人資料之保護
15	警察廳	警察職務執行法(§2)	● 對象：警察 ● 治安資料之蒐集、製作及散發
16	兵務廳	兵役法(§80)	● 對象：兵役負責機關及人員 ● 兵役資料之蒐集及利用
17	監察院	監察院法(§27)	● 對象：監察院 ● 監察目的以外之資料使用禁止

資料來源：本研究自行整理。

第六節 美國

由於個人資料屢遭濫用，危害隱私甚鉅，而在保護隱私的各種國內或國際層級的法律體制中，主要有兩種模式，代表著兩種不同控制個人資料流通的思維與方法[390]。主要代表之一的歐洲聯盟，乃「政府管制」模式的擁護者，採行「全方位式」(comprehensive)的立法（如「歐盟資料保護指令」，the EU Data Protection Directive），以防止個人資料遭到不當濫用，因此，大部分關於個人資料蒐集、使用、分享與儲存的活動皆受一定的拘束，而非放任資料蒐集者恣意為之。相反地，另一派主要代表的美國，乃「市場機制」模式的擁護者，將個人資料的蒐集、使用或分享問題委由當事人個人與資料蒐集者雙方自行透過自由市場的機制協商，政府不積極介入管制，必要時再輔以產業界自訂的自治、自律規範(self-regulation)。然而，在某些特定產業的領域，個人資料遭濫用問題嚴重，形成隱私保護的危機，美國政府乃特別訂立僅適用於該特定「部門」(sector)的法令，以謀有效解決市場失靈。

從歷史的角度而言，美國與歐洲對於隱私保護的方法與取向歷來即不同。歐洲人對於個人隱私的重視，部分起因於德國第三帝國以侵入式手法濫用個人資料來追蹤遭鎖定的目標團體之歷史教訓。所以，當前的歐洲國家傾向於使用全方位式的立法保護以處罰那些個人資料的濫用者，而美國則猶對市場機制充滿信心，僅於個人資料重大外洩或遭竊等危機發生時，才採「頭痛醫頭、腳痛醫腳」的因應之道，訂立僅適用於特定行業或領域的隱私法令。再者，就個人資料交易市場失靈的問題，美國當代辯論的核心，多數集中從產業界自律規範與科技層面尋求答案，少數從法律或規範層面尋求解決之道。進一步言，自律規範體系的設計乃用以鼓勵產業界與消費者合作，共同發展保護資訊隱私的機制。自律規範，乃不用政府高度介入、某種程度上授與產業自主的表現，實為美國市場經濟的重要基石[391]。按學者 Fred H. Cate 指出，比起一般保護隱私的法律，自律規範更具彈性與

[390] Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 Ind. L. Rev. 173, 179 (1999).

[391] David A. Castor, Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year, 12 Ind. Int'l & Comp. L. Rev. 265, 272-273 (2002).

敏感性，允許個人與資訊蒐集者之間就資訊的使用尋求利益平衡[392]。事實上，保護資訊隱私最有效的方法，乃委由消費者自行採取行動[393]。相對於美國所採用的自律規範，歐盟則傾向於嚴格的消費者個人資料保護法制（如歐盟資料保護指令），並產生跨越國界保護資訊隱私之效果[394]，在經濟全球化的浪潮裡，歐盟資料保護指令的域外影響力，提升了美國[395]與其他非歐盟國家的資訊隱私保護標準。其實，與歐洲人民的態度一樣，台灣人民也缺乏美國人民對於自由市場經濟體系的樂觀與信心。可以想見，對於規範個人資料蒐集、使用與分享的相關問題，台灣所信奉的哲學價值與解決之道無疑地更接近於歐盟，而非美國。因此，如同歐盟的取向，台灣所選擇保護個人資料的體制乃以「政府管制」為主、「市場機制」為輔的模式，有別於美國以「市場機制」為主、「政府管制」為輔模式的個人資料保護體制。

歷來，美國從未有過全方位式的聯邦立法[396]，以保護隱私權。美國聯邦貿易委員會在 1998 年提交國會的報告[397]提及：「對於美國隱私法制的最佳詮釋，即為「部門式」(sectoral)，即由一堆不同性質法典所組合而成的，用以規範從事個人資料蒐集的不同特定產業。」此「部門式」的解決之道，源自於美國較少依賴政府管制力量而較多依賴市場力量、自律規範或科技的方式，來保護隱私權[398]。

在所謂「部門式」的立法中，對於個人資料的蒐集、處理、利用及分享，美國政府部門因「1974 年隱私法」而受到面向較廣的拘束，但私人部門則欠缺如「歐盟資料保護指令」的全方位式保護個人資料的規範[399]。自 1970 年代起，美國國會陸續通過不少僅適用於特定產業部門的隱私法律，如公平信用報告法(Fair Credit Reporting Act)、家庭教育權利及隱私法(Family Educational Rights and Privacy Act)、

---

392 Fred H. Cate, Privacy in Perspective 10-12 (2001).

393 Daniel J. Solove, The Digital Person: Technology and Privacy in the information Age 80-81 (2004).

394 Steven R. Salbu, Corporate Governance, Stakeholder Accountability, and Sustainable Peace: The European Union Data Privacy Directive and International Relations, 35 Vand. J. Transnat'l L. 655, 666 (March, 2002).

395 Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1, 6 (Winter, 2000).

396 Henry H. Perritt, Jr. & Margaret G. Stewart, False Alarm?, 51 Fed. Comm. L.J. 811, 812 (May, 1999).

397 Federal Trade Commission, Privacy Online: A Report to Congress 62 (1998), at http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited January 15, 2015).

398 Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive 21 (1998).

399 Jody R. Westby, American Bar Association, International Guide to Privacy 11 (2004).

金融隱私權法(Right to Financial Privacy Act)、隱私保護法(Privacy Protection Act)、有線通信政策法(Cable Communications Policy Act)、影帶隱私保護法(Video Privacy Protection Act)、電話消費者保護法(Telephone Consumer Protection Act)、駕駛人隱私保護法(Driver's Privacy Protection Act)、健康保險可攜性與責任法(Health Insurance Portability and Accountability Act)、兒童線上隱私保護法(Children's Online Privacy Protection Act, COPPA)、金融服務現代化法案(Gramm-Leach-Bliley Act)、未經邀請而主動推介色情與市場銷售之侵犯管制法(Controlling the Assault of Non-Solicited Pornography and Marketing Act, Can-Spam Act)、銀行秘密法(Bank Secrecy Act)、美國愛國法(The USA-Patriot Act) [400]、電信法(Telecommunications Act[401])等，對於個人資料之蒐集、使用或分享加以規範，甚至要求應賦予當事人得「選擇加入」(opt-in)或「選擇退出」(opt-out)之同意權行使機會。

其中，直接涉及電信領域之個人資料保護之最主要法律規範，除 1996 年通過之「電信法」外，尚有其他諸多相關法律規範。以下乃從電信事業個人資料保護規範之流變、1996 年電信法及聯邦通訊委員會(Federal Communications Commission, FCC)所陸續頒布命令(order)、相關施行細則(regulation)之規範內容與相關訴訟案例、以及對於垃圾電話、傳真或電子郵件之管制，加以分析。

一、美國電信事業個人資料保護規範之流變

大部分的「電信」服務，就隱私的保護，均形成兩種不同類型的挑戰：涉及通訊內容(Communications Content)者，以及涉及通訊特徵、特性(Communication Attributes)者。本部分乃從「通訊內容」與「通訊特徵」二方面，探討美國電信事業關於個人資料保護規範之流變。

(一) 通訊內容

「內容」係一種易於理解的概念，其用以描述在使用電話、傳真或網際網路時，所傳遞的「實質資訊」(actual information)。自 1967 年 Katz v. United States[402]案，

---

[400] Daniel J. Solove and Marc Rotenberg, Information Privacy Law 23-24 (2003); and Jody R. Westby, American Bar Association, International Guide to Privacy 15-63 (2004).

[401] The Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.), available at http://www.gpo.gov/fdsys/pkg/PLAW-104publ104/pdf/PLAW-104publ104.pdf (last visited June 8, 2014).

[402] Katz v. United States, 389 U.S. 347 (1967).

美國聯邦最高法院承認，對於電話的通話內容，存在著憲法上受保護的隱私利益。本案涉及 Charles Katz 因被行政機關懷疑違反了賭博相關法律，而遭聯邦行政機關利用安裝在 Charles Katz 使用中的電話亭外面的電子竊聽器的合憲性問題。法院判定，這種蒐集證據的方法，雖然沒有侵犯 Katz 的財產權，但是侵害了其受憲法第四修正案保障的權利。法院認為，憲法所保護者，係每個人企圖保留為私密(private)之所有事項，縱使係處於公眾可接觸之領域。

Harlan 大法官在協同意見書中，提出後來成為法院用以界定憲法第四修正案[403]內涵之「私密」判斷標準。Harlan 大法官指出，憲法第四修正案所保護的隱私範圍，係藉由個人的「實際（主觀）隱私期待」而加以界定，且其所能期待的程度必須係「社會願意認定為合理者」。於 1968 年最高法院採用了此項標準，並持續適用至今日。因此，政府如未事先取得令狀(warrant) [404]，即不能合憲地監聽或截聽電話通話內容。

在 1934 年的「通訊法」(Communications Act of 1934)，國會立法規定電話監聽或截聽(interception)係違法行為，然而，此項禁令卻受限於寬泛的例外排除適用之情形。而在最高法院 Katz 案判決之後的六個月，國會於 1968 年通過了「全面犯罪管制及安全街道法」(Omnibus Crime Control and Safe Streets Act of 1968)，在第 3 章(title III)中，明確規定私人對於通訊所為的監聽或截聽乃違法行為，但允許行政機關於符合嚴格程序要件時，得為監聽或截聽。然而，只有司法部長或州的檢察總長能核准竊聽之申請，且只能用於調查某些嚴重的犯罪。再者，行政機關必須取得法院授權進行通訊監察的命令，而法院的授權同意，僅限於一些特定情形，以及只有在其他調查程序已不能達成、不大可能達成、或倘進行該調查程序將過於危險之情形。一旦調查已完成，受監察之對象應被告知有此監察之存在。倘該監察係屬違法，則藉由該監察所取得之所有證據應被捨棄。且該違法監察之負責人應負擔實際損害賠償、懲罰性賠償與訴訟費用，以及要面臨罰金與最高五年之

[403] According to the Fourth Amendment (Amendment IV) to the United States Constitution, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[404] Fred H. Cate, PRIVACY AND TELECOMMUNICATIONS, 33 Wake Forest L. Rev. 1, 37-38 (Spring 1998).

有期徒刑[405]。

1986 年通過的「電子通訊隱私法」(Electronic Communications Privacy Act of 1986)，禁止監聽、截聽或揭露任何電子通訊(如電話通話、電子郵件)的內容，或甚至包含任何「通話內容」—只要該「通話內容」係出於通話參與者展現「在有理由的情形下，通訊將不會被監聽、截聽」之期待而進行通話者。此項隱私權固然為防範受到他人的不當侵害，而擴大其適用範圍，然而，其也因存在諸多除外規定而造成適用上的隱諱不明，尤其，最重要的例外，乃該禁止規定不適用於通話任一方對於揭露通話加以同意之情形。再者，交換機經營者、電信服務業者員工、聯邦通訊委員會員工或任何協助持有令狀(warrant)之人，只要係屬於其職務範圍內所為之行為者，該禁止規定對之亦無適用餘地[406]。

對於電話通訊內容，某些州甚至要求更嚴格的保護。伊利諾州、加州、麻州與賓州要求，在電話被錄音或記錄前，應取得所有通話當事人的同意。然而，無論是聯邦或各州的法律[407]，均未對於經過合法錄音或記錄的電話通話之後續使用或保存情形加以進一步限制。

近來，於 2014 年 6 月 25 日，在 Riley v. California 及 United States v. Wurie [408] 兩案中，美國聯邦最高法院無異議地判決，執法機關要搜索被捕嫌犯的手機內容(如簡訊內容、位置資訊、聯絡名單、照片、錄影等資訊)，必須先取得搜索票。[409]在權衡執法人員查獲重要事證的利益以及憲法賦予的公民自由權利後，最高法院認定，手機應和住家等其他個人財產一樣受到美國憲法第四修正案保護，得免於「不合理的搜索和扣押」。[410]

(二) 通訊特徵

1996 年以前，關於電信交易的資訊(如電話號碼、通話時間、通話地點與通話

---

405 *Id*., at 38.

406 *Id*., at 39.

407 *Id*., at 38-39.

408 134 S. Ct. 2473 (2014) .

409 Ed Hightower, US Supreme Court rejects unlimited warrantless cell phone searches, World Socialist Web Site, available at http://www.wsws.org/en/articles/2014/06/26/cell-j26.html (last visited June 27, 2014).

410 俞智敏，「美最高法院：警查手機須持搜索票」，自由時報，2014 年 6 月 27 日。

長短)，係不受法律保障。在 1979 年的 Smith v. Maryland[411]案，聯邦最高法院明確地拒絕賦予憲法上的保障。法院判定，Michael Lee Smith 對於其所撥打的電話號碼沒有隱私合理期待(reasonable expectation of privacy)，而該號碼是警方在未先取得令狀下，從安裝在其電話線上的電話記錄器(pen register)而得來。法院質疑，一般人是否會對於他們所撥打的電話號碼有實質上的隱私期待；法院並指出，那些號碼係為了能完成通話而例行性被揭露予電信公司，且例行性被電信公司記錄下來，以利計算帳單與審計之用。再者，法院也認定，倘個人活動的紀錄為第三人所持有者[412]，該當事人對於其活動的紀錄並無憲法上的隱私權。

由於前揭的 1986 年的「電子通訊隱私法」不適用於電信「交易」相關資訊，因此，對於服務提供者關於蒐集、儲存或揭露該等資料之行為，並無法律加以限制。事實上，電子通訊隱私法明確允許得使用電話記錄器或追蹤電話設備，以記錄其他人的對話與傳輸之資訊。而在「數位電話法」(Digital Telephony Act)中，國會藉由立法要求執法人員在取得電信交易資訊前，應取得令狀或法院命令，因而擴張了對於電信事業所持有之交易紀錄的保護。然而，就關於用戶之姓名、住址、電話帳單紀錄、電話號碼、使用時間與所使用的服務類型之資訊，該法免除了上開「應取得令狀或法院命令」要求；就該等資訊，只需要行政、大陪審團或審判的傳喚調查即可。此外，數位電話法也容許，電話業者得向非政府組織自由地揭露所有包含於消費者交易紀錄之資訊。[413]

惟於 1996 年 2 月 8 日，國會通過了 1996 年「電信法」，制定了保護「用戶專屬線路資訊」隱私的條款。該法除對於「用戶專屬線路資訊」(Customer Proprietary Network Information, CPNI)加以定義外，且該資訊係用戶依業者與用戶(carrier-customer)間之關係而允許電信事業加以使用，因此，電信事業只有在提供該等資訊因而衍生之電信服務或或對於提供該等電信服務所必要之服務時[414]，電信事業才可使用、揭露或允許接觸可辨識個人之「用戶專屬線路資訊」。

二、1996 年電信法及聯邦通訊委員會所陸續頒布之命令、施行細則之規範內容及相關訴訟案件

411 Smith v. Maryland, 442 U.S. 735 (1979).
412 *Supra* note404, at 39.
413 *Id*., at 39-40.
414 *Id*., at 40.

(一) 電信法第 222 條關於電信事業個人資料保護之規範內容

如前揭，按 1996 年通過之電信法第 222 條規定，電信事業有義務保護用戶專屬資訊之秘密性。而為了保護消費者隱私，電信法第 222 條對於電信事業為提供電信服務予用戶而取得的「用戶專屬線路資訊」(customer proprietary network information)之用途加以限制。

電信事業使用「用戶專屬線路資訊」的理由，有很多種。最重要者，「用戶專屬線路資訊」係一種有價值的市場利器。「用戶專屬線路資訊」可以協助電信事業發現潛在用戶、設計更有效率的服務及更能滿足用戶需求。[415]簡言之，可利用「用戶專屬線路資訊」，以創造非常精準與詳細的直接行銷名單。然而，電信事業為提供電信服務而從其他業者接收或取得專屬資料(proprietary information)者，僅能為該服務而使用該資料，以及不能為本身行銷目的而使用該資料。[416]

1、 「用戶專屬線路資料」定義

按電信法第 222(f)(1)[417]條，「用戶專屬線路資料」為：「（A）涉及電信事業用戶使用電信服務之數量、技術規格、型態、目的地與總額之資訊，且該資訊係用戶單純依業者與用戶間之關係而允許業者使用者；以及（B）電信事業的用戶所收到涉及電話交換機服務或付費電話服務的帳單之資訊，除非用戶名單的資訊不包括在其中。」簡言之，所謂「用戶專屬線路資訊」，即業者於提供電信服務時從用戶取得的資訊。[418]

---

[415] Leah E. Capritta, COMMUNICATIONS LAW: U.S. WEST, INC. V. FCC INTERPRETS THE FIRST AMENDMENT RAMIFICATIONS OF "CUSTOMER PROPRIETARY NETWORK INFORMATION," 77 Denv. U. L. Rev. 441, 442-443 (2000).

[416]" A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts," 47 U.S. Code § 222(b), available at http://www.law.cornell.edu/uscode/text/47/222 (last visited October 8, 2014). .

[417] The term 'customer proprietary network information' means— (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information., 47 U.S.C. § 222(f)(1), available at http://www.gpo.gov/fdsys/pkg/PLAW-104publ104/pdf/PLAW-104publ104.pdf (last visited June 8, 2014).

[418] Antonia Runac, CONTROL OVER PERSONAL INFORMATION: WHO HAS IT, THE CONSUMER OR THE INDUSTRY?, 12 Loy. Consumer L. Rev. 68, 69 (1999).

2、 使用、揭露或取得「用戶專屬線路資料」的限制

對於「用戶專屬線路資訊」的使用、揭露或取得的限制，電信法第 222(c)(1) [419] 條規定如下：「電信事業因提供電信服務而收受或取得用戶專屬線路資訊者，除依法律規定或經用戶同意外，應僅能使用、揭露或允許接觸該可辨識個人(individually identifiable)的用戶專屬線路資訊，於提供（A）該等資訊因而衍生之電信服務，或（B）對於提供該等電信服務所必要或使用之服務，包含電話簿的出版。」換言之，除業者取得用戶同意或法律另有規定外，電信事業不得為了與衍生用戶專屬線路資訊之服務無關之目的而使用、揭露或允許接觸「用戶專屬線路資訊」。[420]

3、 使用、揭露或取得「用戶專屬線路資料」的限制之除外情形

就上開電信法第 222(c)(1)條所闡明的隱私要件，第 222(d) [421]條規定四種例外情形，電信事業得使用、揭露或允許接觸用戶專屬線路資訊：（1）為電信服務的開始、提供、帳單的開立和收費；（2）為保護電信事業的權利或財產；或為保護該等服務的用戶與其他業者免於遭受詐欺、濫用或非法的使用或訂購該等服務；（3）

---

419 "Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.," 47 U.S.C. § 222(c)(1), available at http://www.gpo.gov/fdsys/pkg/PLAW-104publ104/pdf/PLAW-104publ104.pdf (last visited June 8, 2014).

420 *Supra* note418, at 69-70.

421 "(d) EXCEPTIONS.—Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents— ''(1) to initiate, render, bill, and collect for telecommunications services; (2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or (3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332 (d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)— (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services; (B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or (C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.," 47 U.S.C. § 222(d), available at http://www.gpo.gov/fdsys/pkg/PLAW-104publ104/pdf/PLAW-104publ104.pdf (last visited June 8, 2014).

倘用戶主動打電話及用戶同意使用該等資訊以提供服務，而在該通電話通話時間內為提供做為內部(inbound)作業用途的電話行銷、轉接或行政服務予用戶者；或(4)倘為下列情形而將商業行動電話服務或 IP 驅動語音服務之用戶之打電話「位置資訊」(location information)加以提供：(A)為回應用戶打電話請求緊急服務之需求，而提供予公共安全回應據點(public safety answering point)、緊急醫療服務提供者或緊急派遣提供者、公共安全、火警服務、執法官員、醫院急診處或外傷照顧處所；(B)於涉及死亡或身體嚴重傷害之虞之急迫情況，而將用戶之位置加以通知予用戶之法定監護人或用戶之親近家人；或(C)為回應緊急服務之需求，而提供予資訊或資料庫管理服務之提供者，以供協助提供緊急服務之目的。

(二) 電信法「用戶專屬線路資訊」相關命令、施行細則及合憲性之挑戰

如前揭，除依法律規定或經用戶同意者外，電信事業禁止以電信法第 222 條所定以外方式而使用、揭露或允許接觸「用戶專屬線路資訊」。其中，惟關於「用戶專屬線路資訊」之使用、揭露或允許接觸，第 222(c)(1)條未明定，應以何種方式取得用戶同意。對此，聯邦通訊委員會曾數度在不同年度中，公布「用戶專屬線路資訊」相關命令(“CPNI Order”)[422]及因此修改施行細則，但卻曾被提起訴訟並被質疑其是否合憲。

1、 1998 年「用戶專屬線路資訊」相關命令、施行細則及合憲性之挑戰

由於就「用戶專屬線路資訊」之使用、揭露或允許接觸，第 222(c)(1)條未明定，應以何種方式取得用戶同意。對此，聯邦通訊委員會在 1998 年「用戶專屬線路資訊」相關命令[423]中，提及聯邦通訊委員會為實施電信法第 222 條而制定之「施行細則」，要求以「選擇加入」方式而取得用戶同意[424]。然而，針對上開「用戶專

[422] See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (1998 CPNI Order); Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002) (2002 CPNI Order); Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (2007 CPNI Order).

[423] In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Second Report and Order and Further Notice of Proposed Rulemaking (“CPNI Order”), February 19, 1998, available at http://transition.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt (last visited March 1, 2014).

[424] 47 C.F.R. §64.2007(b).

屬線路資訊」施行細則，在 U S WEST, Inc. v. FCC 案[425]，卻被質疑其是否合憲。

(1)1998 年「用戶專屬線路資訊」相關命令、施行細則之主要規範內容

綜合前述，除依法律規定或經用戶同意者外，電信事業禁止以電信法第 222 條所定以外方式而使用、揭露或允許接觸「用戶專屬線路資訊」。惟關於「用戶專屬線路資訊」之使用、揭露或允許接觸，第 222(c)(1)條未明定，應以何種方法取得用戶同意。

對此，美國聯邦通訊委員會在 1998 年「用戶專屬線路資訊」相關命令[426]中，提及聯邦通訊委員會為實施電信法第 222 條而制定之「施行細則」(regulations)，要求以「選擇加入」方式而取得用戶同意[427]。即要求電信事業以書面、口頭或電子方式，取得用戶之事前明示同意[428]。聯邦通訊委員會認為，明示同意的機制將是強化國會欲「保護隱私與市場競爭的利益，又同時保存了用戶能夠控制敏感資訊的散佈」之願望的最佳方法。

此外，1998 年「用戶專屬線路資訊」相關施行細則規定，如果業者就整個服務關係以外範圍而取得用戶之同意，則在用戶撤回或限制該同意之前，該同意仍有效。最後，為確保用戶賦予同意前已被告知其法律上權利，在業者向用戶請求同意之前[429]，就「用戶專屬線路資訊」之使用、揭露或允許接觸，業者應告知用戶得加以限制。

(2)1998 年「用戶專屬線路資訊」相關施行細則之合憲性挑戰

由於電信法並未明定電信事業取得用戶同意的方法為何，乃滋生爭議。因此，針對 1998 年聯邦通訊委員會為落實電信法第 222 條所制定之上開施行細則而要求以「選擇加入」方式而取得用戶同意，在 U S WEST, Inc. v. FCC 案[430]中，第十上訴巡迴法院認為其乃違反美國聯邦憲法第一修正案。關於「用戶專屬線路資訊」之使用、揭露或允許接觸應取得用戶「選擇加入」之同意方式，乃被該法院加以

425 U S WEST, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).
426 *Supra* note423.
427 47 C.F.R. §64.2007(b).
428 *Id*.
429 *Supra* note418, at 72 .
430 U S WEST, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

推翻。按該法院的決定，電信事業毋庸取得用戶的事前明示同意，即可以為行銷而利用「用戶專屬線路資訊」。據此，除非用戶「選擇退出」，否則，電信事業等同取得用戶的默示同意而得利用「用戶專屬線路資訊」。[431]

在 U S WEST, Inc. v. FCC 案，上訴人 U S WEST, Inc.質疑聯邦通訊委員會之 1998 年「用戶專屬線路資訊」相關施行細則要求電信事業利用「用戶專屬線路資訊」前應先取得用戶明示同意之規定，違反美國憲法第一及第五修正案。第十上訴巡迴法院認為，其乃違反美國聯邦憲法第一修正案。

第十上訴巡迴法院認為，(I)就第一修正案言論自由條款之宗旨，「用戶專屬線路資訊」係「商業言論」(commercial speech)；(II) 聯邦通訊委員會未能證明，該規定能夠直接及重要地增進聯邦通訊委員會所宣稱在隱私及促進競爭方面之利益；(III)對於為了增進所宣稱之利益，該規定未經「嚴密關聯的設計」或「嚴密剪裁」（narrowly tailored）。對於上開理由，進一步分析如下[432]：

① 「用戶專屬線路資訊」相關施行細則是否影響第一修正案言論自由?

聯邦通訊委員會雖主張，「用戶專屬線路資訊」施行細則並未違反或限制上訴人第一修正案權利，但為第十上訴巡迴法院所駁回。聯邦通訊委員會指稱，該施行細則僅防止上訴人利用「用戶專屬線路資訊」而針對或鎖定用戶，並未禁止或限制上訴人與用戶之間的聯繫溝通。法院表示，聯邦通訊委員會的主張根本係錯誤的，因為第一修正案係為保護表達言論者與作為對象的聽者(聽眾)，以及對於二者之一所加的限制即屬對於言論的限制。因此，法院用以駁回政府主張之基礎，乃係先從表達言論者與聽者之間關係可導出的針對性言論(targeted speech)之概念出發；再從限制第一修正案言論自由的角度觀之，針對特定聽者的言論與隨機針對不特定聽者的言論，應是等量齊觀的。

最後，法院總結，上訴人針對性言論之目的雖係為推銷之用；但相反地，針對性言論乃構成商業性言論。因此，「用戶專屬線路資訊」施行細則因對於受保護的商業言論加以限制，乃構成對於第一修正案言論自由的限制。又當事人雙方均主張，基於「用戶專屬線路資訊」所為的商業言論，均是真實且非誤導的。

---

431 *Supra* note418, at 79 .

432 *Id*., at 74-78.

② 政府對於利用「用戶專屬線路資訊」加以管制是否具有重要利益?

聯邦通訊委員會主張,「用戶專屬線路資訊」相關施行細則能夠增進「用戶隱私」及「促進競爭」之兩項國家重要利益。雖然法院承認,對於隱私的擔憂促使電信法第 222 條的制定,但除非政府能明確地指出隱私利益並加以正當化,否則,無法符合 Central Hudson Gas & Electric Corporation v. Public Service Commission of New York ("Central Hudson")[433]案所建立之第二重審查標準。

再者,法院表示,就言論自由限制的範疇而言,欲藉由維持某些資料的機密性以保護隱私,則政府必須證明:資料的流通將對於當事人造成特定及重要的損害。法院並由「用戶專屬線路資訊」相關施行細則推論,「用戶專屬線路資訊」的揭露將對某些當事人形成難堪之局面,因此,將構成對於當事人之損害。然而,隱私利益是否確實如此重要,乃深受質疑;且政府為了上訴之故,才主張對於保護消費者免於被揭露敏感、令人難堪的資料具有重要利益。

法院並駁回政府對於競爭具有利益之主張。法院認為,縱使電信法廣泛之宗旨在於促進競爭,然而,第 222 條乃用以增進顧客隱私。因為法院認為促進競爭與保護隱私二者乃互相衝突的;法院並認為,以第 222 條平衡競爭與隱私利益之嘗試,將會與電信法支持競爭之宗旨相互矛盾。再者,法院的見解乃基於下列三項結論而來:(I) 第 222 條的字面意義主要係處理隱私;(II)「用戶專屬線路資訊」相關施行細則之前的限制,乃用以增進競爭,第 222 條與之有所不同,第 222 條係適用於所有電信事業而非僅主要幾家業者而已,按法院見解,其乃造成競爭之限制;(III) 第 222 條容許,倘取得用戶同意,得完全進行「用戶專屬線路資訊」之利用。

基於上述考量及第 222 條立法宗旨,第十上訴巡迴法院認為,政府主張對於

[433] 447 U.S. at 557 (1980). In Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, the United States Supreme Court reversed the New York Court of Appeals' decision sustaining a regulation of the New York Public Service Commission which banned, in totality, promotional advertising by an electrical utility. The regulation was based on the Commission's finding that the interconnected utility system in the state of New York did not have a sufficient fuel supply to satisfy consumer demands for the 1973-74 winter. The Supreme Court held that the regulation violated the First and Fourteenth Amendments because the state's complete suppression of commercial speech was more extensive than necessary to further the state's asserted interest in energy conservation. The Supreme Court's four part analysis in Central Hudson can be summarized as follows: (1) Is the expression protected by the First Amendment; (2) Is the asserted governmental interest substantial; (3) Does the regulation directly advance the governmental interest; and (4) Is the regulation more extensive than necessary to serve that interest? Antonia Runac, s*upra* note 418, at 74.

競爭之利益本身並不足以正當化其對於「用戶專屬線路資訊」之利用所加諸的限制。同時，法院認定，競爭並非第 222 條制定的主要目的，但法院表示其將連同用戶隱私的保護而一併考量政府所主張在競爭方面的利益。

③「用戶專屬線路資訊」相關施行細則是否直接增進政府利益?

按 Central Hudson 案所建立之第三重審查標準，政府必須證明，所造成的損害是立即的，以及其所採取的限制措施確實能重大程度上減緩其損害。法院認定，政府未能證明，對於隱私或競爭確實造成立即的損害。法院表示，由於政府未能證明：「用戶專屬線路資訊」將可能如何被揭露及確實如何被揭露；因此，政府擔憂資料的流通可能造成令當事人難堪的局面，實係無事實基礎的抽象擔憂而已。類似地，法院亦認定，政府未能分析：電信事業利用「用戶專屬線路資訊」以行銷新服務所可能或確實地阻礙競爭。

④「用戶專屬線路資訊」相關施行細則之規範是否經過嚴密關聯的設計?

法院認為，即使政府主張對於隱私、競爭有重要利益及該施行細則能夠直接增進該等利益，聯邦通訊委員會所通過的施行細則對於目的的達成仍未經嚴密關聯的設計或嚴密剪裁。根據法院見解，一個施行細則欲符合 Central Hudson 案所建立之第四重審查標準，該施行細則立法所採之手段與所欲達成目的之間必須互相合適、合身(fit)，不必然完美、但應合理，即使不必係唯一最佳安排、但其手段之範疇與欲促成之利益應成比例原則。因此，政府所採之手段對於政府目的之達成，應係經嚴密關聯的設計或嚴密剪裁。

聯邦通訊委員會主張，所提供之檔案充分證明，該施行細則經嚴密關聯的設計或嚴密剪裁，因為 U.S. West 公司的一項研究顯示，當被要求對於「用戶專屬線路資訊」的被利用是否加以明確同意，多數消費者均拒絕同意。再者，該項研究顯示，接到電話的消費者有 33%拒絕授權使用其「用戶專屬線路資訊」、28%同意授權、39%掛斷電話或要求別再打電話來。

此外，雖然已將立法紀錄納入，政府仍主張，其乃根據經驗所為的「常識判斷」(common sense judgment)而制定施行細則，然而，法院拒絕擴張「常識判斷」之適用至本案，因為聯邦通訊委員會之「常識判斷」僅可證明其制定施行細則乃出於理性行事，但按 Central Hudson 案之標準，政府必須證明其施行細則乃經嚴密關聯的設計或嚴密剪裁。對此，法院駁斥 U.S. West 公司的研究足以做為消費者不

欲電信事業使用其「用戶專屬線路資訊」之充分證據，因此，亦駁斥政府認為其施行細則乃經嚴密關聯的設計或嚴密剪裁之信念。最終，法院認定，聯邦通訊委員會所制定之施行細則乃未經嚴密關聯的設計或嚴密剪裁；法院並認為，聯邦通訊委員會未能充分證明「選擇退出」方案(即推定消費者同意其「用戶專屬線路資訊」之利用，直到消費者選擇退出為止)未能充分保障消費者隱私。再者，法院表示，由於聯邦通訊委員會之檔案中欠缺關於「選擇退出」方案之討論，因此，其很難反應出已經過關於規範商業言論所要求之成本效益的詳細評估。

⑤小結: 第十上訴巡迴法院之判決

第十上訴巡迴法院判決主張，政府在依照電信法第 222 條頒布系爭「用戶專屬線路資訊」相關施行細則時，未能考慮其對於憲法第一修正案的影響。按法院見解，即使政府所宣稱利益是重要的，但聯邦通訊委員會未能對於其採用「選擇加入」之決策程序，加以正當化。法院認為，系爭施行細則未能滿足 Central Hudson 的四個審查標準，因此，系爭施行細則至少已引發合憲性爭議。由於聯邦通訊委員會引發合憲性的擔憂，因此，法院乃宣告聯邦通訊委員會「用戶專屬線路資訊」的命令及相關施行細則，應為無效。

2、 2002 年「用戶專屬線路資訊」相關命令、施行細則

① 採行「選擇退出」與「選擇加入」雙軌並行的「同意」行使模式

如前揭，在 U.S. West, Inc. v. FCC 案，上訴法院認定，就電信事業利用用戶個人資料而與用戶溝通之憲法第一修正案言論自由的權利，聯邦通訊委員會 1998 年的相關施行細則對之不當地加諸了違憲的限制，因為聯邦通訊委員會未能證明倘未採取「選擇加入」取向將不足以充分保護用戶隱私。

於是，於 2002 年 7 月，為回應第十巡迴法院之見解，聯邦通訊委員會發布新的命令[434]，並修改相關施行細則[435]。事實上，在發布新的命令前，聯邦通訊委員

[434] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, § 1 at para. 2 (FCC Third Report and Order and Third Further Notice of Proposed Rulemaking July 25, 2002), available at http://www.steptoe.com/assets/attachments/1655.pdf (last visited June 28, 2014).

[435] FEDERAL COMMUNICATIONS COMMISSION, 47 CFR Part 64, Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Connumications Act of 1934, as Amended, available at

會注意到「金融服務現代化法案」(Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999)加諸隱私保護義務於廣泛適用的金融機構之上，以及聯邦貿易委員會(Federal Trade Commission)因此制定的施行細則所引起的相關訴訟。因此，聯邦通訊委員會所發布的新命令，乃針對「用戶專屬線路資訊」接收者與電信事業關係之不同，而採行「選擇退出」與「選擇加入」雙軌並行的「同意」行使模式[436]。

具體言之，2002 年的命令與相關施行細則，對於電信事業與關係企業之間基於電信相關目的而分享「用戶專屬線路資訊」，僅明示要求「選擇退出」的同意模式即可，但電信事業亦得自行選擇採取較嚴格之「選擇加入」同意模式[437]。至於揭露用戶個人資料予無關的第三人或非提供電信相關服務的關係企業[438]，則要求「選擇加入」同意模式。

2002 年的命令與相關施行細則雖允許電信事業為電信相關服務行銷之目的，而得與關係企業(affiliate)、合資夥伴(joint venture partner)或獨立的契約締約相對人(independent contractor)分享用戶資訊。然而，聯邦通訊委員會認定，按 1996 年電信法，上開第三人並不符合「電信事業」資格，因此，不受第 222 條保密要求之拘束。據此，聯邦通訊委員會要求電信事業除提供「選擇退出」通知予用戶外，電信事業尚必須與合資夥伴或獨立的契約締約相對人簽屬「保密契約」，以保護用戶個人資料。[439]

② 通知之要求及內容

2002 年的命令再度確認聯邦通訊委員會先前所頒佈關於「通知」之施行細則[440]，

---

http://www.gpo.gov/fdsys/pkg/FR-2002-09-20/pdf/02-23199.pdf (last visited June 28, 2014).

[436] FCC Adopts Dual Opt-in and Opt-out Regimes for CPNI, Privacy In Focus, **Newsletters,** WILEY REIN LLP (August 2002), available at http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=4&id=3939 (last visited July 1, 2014).

[437] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, § 1 at para. 89 (FCC Third Report and Order and Third Further Notice of Proposed Rulemaking July 25, 2002), available at http://www.steptoe.com/assets/attachments/1655.pdf (last visited June 28, 2014).

[438] David J. Phillips, BEYOND PRIVACY: CONFRONTING LOCATIONAL SURVEILLANCE IN WIRELESS COMMUNICATION, 8 Comm. L. & Pol'y 1, 13-14 (Winter, 2003).

[439] MAJOR COURT DECISIONS, 2009, 17 CommLaw Conspectus 869, 871 (2009).

[440] 47 CFR § 64.2007.

要求電信事業的通知必須完整及不得有誤導情事，並要求書面通知必須清楚易讀、使用夠大的字體、及放置位置讓用戶能明顯易讀[441]。電信事業尋求取得用戶同意前，應先通知用戶有權得限制「用戶專屬線路資訊」之使用、揭露或接觸。[442]倘電信事業未遵守相關命令及施行細則時，聯邦通訊委員會將對之提起執行之訴訟。

而對於通知之方式，在「選擇加入」之通知，2002 年的命令賦予電信事業較大之彈性，以決定何種型態通知最適合用戶之需求；但在「選擇退出」之通知，2002 年的命令則採取較嚴格之通知要求，以確保就「用戶專屬線路資訊」之使用，用戶能夠理解其選擇及表達其喜好。[443]2002 年的命令要求，電信事業尋求取得用戶「選擇退出」同意前，應提供具體(書面或電子方式)的通知，但在電信事業尋求取得用戶「選擇加入」之通知，則可以使用書面、電子或口頭方式的通知[444]。

此外，電信事業提供用戶通知及「選擇退出」機會後，必須等待最短 30 天之期間，才可推定用戶同意對於其「用戶專屬線路資訊」得加以使用、揭露或允許接觸[445]。電信事業倘使用「選擇退出」機制以取得用戶同意者，應每二年提供通知予用戶[446]。

對於用戶之通知，應提供充分資訊，以促使關於是否允許電信事業使用、揭露或接觸「用戶專屬線路資訊」，用戶能為「告知後決定」(informed decision)。[447]因此，通知之內容，包括(I)依聯邦法得以保護「用戶專屬線路資訊」秘密性之用戶的權利或電信事業的義務；(II)應明確化「用戶專屬線路資訊」所涵蓋之個人資料類型及將接收「用戶專屬線路資訊」之特定主體、應敘述「用戶專屬線路資訊」

441 47 C.F.R. §§ 64.2008(c)(4)-(c)(5).

442 47 C.F.R. § 64.2008(a).

443 Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, § 1 at para. 89 (FCC Third Report and Order and Third Further Notice of Proposed Rulemaking July 25, 2002), available at http://www.steptoe.com/assets/attachments/1655.pdf (last visited June 28, 2014).

444 Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, § 1 at para. 90-94 (FCC Third Report and Order and Third Further Notice of Proposed Rulemaking July 25, 2002), available at http://www.steptoe.com/assets/attachments/1655.pdf (last visited June 28, 2014).

445 47 C.F.R. § 64.2008(d)(1).

446 47 C.F.R. § 64.2008(d)(2).

447 47 C.F.R. § 64.2008(c).

之利用目的、以及告知用戶其有權得不同意該使用與隨時拒絕或撤銷對於其「用戶專屬線路資訊」之接觸；(III)應建議用戶得賦予或拒絕其「用戶專屬線路資訊」被接觸之明確步驟、應清楚敘述接觸的拒絕將不會影響用戶所訂購服務之提供、以及得以清楚中性之用語簡述倘缺乏「用戶專屬線路資訊」直接導致之後果等。[448]

③ 使用與揭露「用戶專屬線路資訊」之安全維護措施

電信事業應實施一種系統，在使用「用戶專屬線路資訊」前，得用以確認已先取得用戶的同意[449]。電信事業應訓練其員工判斷是否取得使用「用戶專屬線路資訊」之授權，並建立明確的訓練流程[450]。電信事業應以電子或其他方式保存其本身與關係企業使用「用戶專屬線路資訊」之銷售與行銷活動之檔案。電信事業亦應保存將「用戶專屬線路資訊」揭露、提供予第三人或第三人被允許得接觸「用戶專屬線路資訊」之所有情形之檔案。該檔案應包括每次活動之敘述、被使用於活動中之特定「用戶專屬線路資訊」、活動中所銷售之產品與服務、以及該檔案應至少保存一年。[451]

關於電信事業為外部行銷而遵守本部分之安全維護措施之規範，電信事業應建立監督審查程序，電信事業也應保存其遵守規範情形之相關檔案至少一年。尤其，行銷員工欲進行外部行銷而請求用戶同意者[452]，應取得監督的同意(supervisory approval)。[453]

另外，電信事業應採取合理措施，以發見及防止未經授權而意圖接觸「用戶專屬線路資訊」之行為。電信事業基於用戶方面所主動開始之電話接觸、網路上帳戶接觸或造訪店內而揭露「用戶專屬線路資訊」之前，應適當地查核驗證用戶之身分。[454]

④ 此外，針對聯邦通訊委員會 2002 年的命令[455]，並無任何訴訟被提起而對其效

[448] 47 C.F.R. §§ 64.2008(c)(1)-(c)(3).
[449] 47 CFR § 64.2009(a).
[450] 47 CFR § 64.2009(b).
[451] 47 CFR § 64.2009(c).
[452] 47 CFR § 64.2009(d).
[453] Andrew B. Serwin, Peter F. McLaughlin & John P. Tomaszewski, Privacy, Security and Information Management, 196 (2011).
[454] 47 CFR § 64.2010(a).
[455] MAJOR COURT DECISIONS, 2009, 17 CommLaw Conspectus 869, 871 (2009).

力加以挑戰。

3、 2007 年「用戶專屬線路資訊」相關命令、施行細則及合憲性之挑戰

2005 年電子隱私資訊中心(Electronic Privacy Information Center)請願要求修改聯邦通訊委員會關於用戶個人資料分享的相關規範。其請願書提及，網路上從事個人資料買賣的資料仲介者數量日漸增多，其並表達憂心該等資料仲介者能極其容易地從電信事業及其他主體取得用戶個人資料。因此，聯邦通訊委員會展開法規制定的新程序、接受評論，以及發布了 2007 年命令[456]。事實上，在聯邦通訊委員會發布 2007 年命令之二個月前，美國國會通過「電話紀錄與隱私保護法」(Telephone Records and Privacy Protection Act of 2006) [457]，對於未經授權而接觸網路消費者帳號、販賣或移轉用戶資訊、明知係詐術取得的用戶資訊而仍加以購買或接收者，必須負擔刑事責任。

(1)2007 年「用戶專屬線路資訊」相關命令、施行細則之主要規範內容

①與合資夥伴或契約締約相對人分享「用戶專屬線路資訊」之規範內容

美國聯邦通訊委員會於 2007 年發布命令[458]並修改「用戶專屬線路資訊」相關施行細則[459]。

針對「用戶專屬線路資訊」，只要電信事業所分享的關係企業係通訊相關的業者，其同意模式乃採「選擇退出」方式，毋庸取得用戶的事前明示同意。針對與非關係企業之第三人分享「用戶專屬線路資訊」部分，倘電信事業欲將「用戶專屬線路資訊」揭露予合資夥伴或獨立自主的契約締約相對人或允許其得接觸使用「用戶專屬線路資訊」時，電信事業應取得用戶「選擇加入」同意(“opt-in” consent)。[460]因此，電信事業欲供行銷目的而揭露用戶個人資料予非關係企業之第三人或允許其得接觸使用該等個人資料前，電信事業必須事前先取得用戶同意，即使所行

456 MAJOR COURT DECISIONS, 17 CommLaw Conspectus 869, 871-872 (2009).

457 MAJOR COURT DECISIONS, 17 CommLaw Conspectus 869, 872 (2009).

458 In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Second Report and Order and Further Notice of Proposed Rulemaking (“CPNI Order”), March 13, 2007, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf (last visited March 1, 2014).

459 47 C.F.R. § 64.2007.

460 *Supra* note458, at 22-23.

銷者係電信相關服務，亦如此。

事實上，上開「選擇加入」同意的條款，未變更先前的相關規定，即就電信事業自行行銷電信相關服務予用戶，允許電信事業得選擇使用「選擇加入」或「選擇退出」機制，以取得用戶之同意。進一步言，電信事業得繼續使用「選擇加入」或「選擇退出」的用戶同意機制，以授權電信事業得接觸「用戶專屬線路資訊」或得揭露「用戶專屬線路資訊」予從事電信服務相關的關係企業或代理人，因此，該等主體得使用用戶的個人資料，而對於用戶進行電信服務的行銷活動。[461]換言之，就超出所有服務目的而在公司內部使用「用戶專屬線路資訊」或揭露「用戶專屬線路資訊」予從事電信服務相關的關係企業或代理人之情形，2007 年僅輕微修改的「用戶專屬線路資訊」相關施行細則[462]，未影響原本所採的「選擇退出」機制。

③ 「位置資訊」的相關規範內容

1999 年制定的「無線通訊公眾安全法」(Wireless Communications Public Safety Act of 1999[463])修正了 1996 年電信法的部分規定，而將「位置」(location)資訊納入「用戶專屬線路資訊」的定義中。因此，2007 年「用戶專屬線路資訊」相關命令乃修改相關施行細則[464]，用以包括「通話細節資訊」(call detail information)在內，而「通話細節資訊」包含傳遞特定電話通話所涉及的相關資訊與撥入、撥出電話的撥打所在「位置」。由於「通話細節資訊」係屬於「用戶專屬線路資訊」之一部分，對於行動電話用戶而言，位置資訊乃被視為「用戶專屬線路資訊」而受到保護[465]。

「無線通訊公眾安全法」並修正了電信法關於使用、揭露或允許接觸「位置資訊」的規定，而規定「未經用戶事前明示授權(express prior authorization)者，就商業行動服務用戶的通話位置資訊(call location information)的使用、揭露或允許接

---

461 2007 CPNI Order, at App. B, Subpart U, 4(b) (amending 47 C.F.R. § 64.2007).

462 Id; Nancy J. King, DIRECT MARKETING, MOBILE PHONES, AND CONSUMER PRIVACY: ENSURING ADEQUATE DISCLOSURE AND CONSENT MECHANISMS FOR EMERGING MOBILE ADVERTISING PRACTICES, 60 Fed. Comm. L.J. 229, 274-275, at note 180 (March, 2008).

463 Wireless Communications and Public Safety Act of 1999, 47 U.S.C. § 609 (1999).

464 Telecomm. Carriers' Use of Customer Proprietary Network Info. And Other Customer Info., Rpt. And Order and Further Notice of Proposed RM, 22 F.C.C.R. 6927, para. 4 (2007).

465 *Supra* note462, Nancy J. King, at 277 (March, 2008).

觸，用戶不應被視為已經加以同意[466]。」惟情況緊急者[467]，得例外地使用、揭露或允許接觸該「位置資訊」。

④ 網路電話(VoIP) 的相關規範內容

聯邦通訊委員會並於 2007 年「用戶專屬線路資訊」相關命令中釐清，網路電話(VoIP)及 IP 驅動的網路電話提供者亦應遵守「用戶專屬線路資訊」相關的規範。事實上，網路電話或其他網路電話是否如同「資訊服務」(information service)而應受到通訊委員會較寬鬆的管制，過去一直不甚明確。相對地，電信事業則受到聯邦通訊委員會較嚴格的管制。然而，2007 年「用戶專屬線路資訊」相關的命令既已生效，因此，就「用戶專屬線路資訊」，網路電話用戶應受到等同於傳統電信事業用戶一樣的保護[468]。

④違反「用戶專屬線路資訊」安全保護措施之通知

電信事業違反「用戶專屬線路資訊」之相關規範時，應通知執法機關。電信事業完成依法通知執法機關之程序前，不論係出於自願或依聯邦、地方法律規定，不應通知用戶或公開地揭露該等違反情事。在合理地判斷該等違反情事後之可行範圍或最遲七個工作日之內，電信事業應經由中央通報設施以電子方式通知美國特勤局(United States Secret Service)與聯邦調查局(FBI)。[469]電信事業應以電子或其他方式保有所發現之違反情事及曾通知美國特勤局與聯邦調查局情事之檔案，並應保持該檔案至少兩年。[470]所謂「違反」，係指某人未經授權或逾越授權而故意接

---

466 47 U.S.C. § 222(f).

467 According to 47 U.S.C. § 222(d)(4), " Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents— (4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)—to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services; (B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or (C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency."

468 Nancy J. King, *supra* note 462, at 275.

469 47 C.F.R. §64.2011(a) -(b).

470 47 C.F.R. §64.2011(d).

觸、使用或揭露「用戶專屬線路資訊」。[471]

(2)2007 年「用戶專屬線路資訊」相關施行細則之合憲性挑戰

針對美國聯邦通訊委員會乃於 2007 年關於與合資夥伴或契約締約相對人分享「用戶專屬線路資訊」的相關施行細則是否違反美國憲法關於言論自由的第一修正案或是否屬於恣意裁量而違反行政程序法(Administrative Procedure Act)，在 National Cable & Telecommunications Association v. Federal Communication Commission 案[472]中，進行審查。對於是否違反美國憲法關於言論自由的第一修正案乙事，首先，法院審查是否有「重要政府利益」的存在，如同 U.S. West 案中第十巡迴法院的見解，本案法院亦認定，保護用戶隱私的利益在於避免當事人的困窘。法院並解釋，隱私乃涉及當事人可以決定何時、如何及對誰揭露其個人資料予他人之權利。

其次，法院審查 2007 年「用戶專屬線路資訊」相關命令是否能「直接促進」(directly advance)可辨識的政府利益乙事，法院則認定，除非對於電信事業揭露用戶個人資料加以限制，否則，用戶隱私將無法獲得保障。法院認為，電信事業未經用戶同意，而與合資夥伴或獨立自主的契約締約相對人分享用戶個人資料，乃係對於用戶隱私的侵犯，其正是 2007 年「用戶專屬線路資訊」相關命令所欲針對而加以規範的侵害。因此，聯邦通訊委員會關於「選擇加入同意的要求乃能直接且實質地促進保護用戶隱私及確保用戶對於個人資料的控制」之認定，係合理的。

最後，法院所考量的最後要求，係對於商業言論的限制必須不得比促進該重要利益所必需者更為廣泛或更為擴張。因此，唯一必須論證者，係法律的管制與所欲促進的利益必須成比例，而法院認為聯邦通訊委員會 2007 年「用戶專屬線路資訊」相關命令符合上開要求。聯邦通訊委員會「選擇加入同意」的方案先假設，消費者不欲其個人資料被分享，除非其有明確的不同指示。相反地，上訴人則想要「選擇退出同意」的方案，因其有相反的假設。

在 Trans Union II[473]案中，法院認定「選擇退出同意」方案對於第一修正案的

---

471 47 C.F.R. §64.2011(e).

472 National Cable & Telecommunications Association v. Federal Communication Commission, 555 F.3d 996 (D.C. Cir. 2009)。

473 Trans Union Corp. v. FTC, 267 F.3d 1138, 1143 (2001).

目的而言，僅比「選擇加入同意」方案邊際上較不具侵犯性而已，因此，法院支持對於分享用戶信用資料必須經「選擇加入同意」之幾乎相同的法律體制。法院認為，聯邦通訊委員會比較過兩種取向的不同，而相關證據也支持聯邦通訊委員會為傾向「選擇加入同意」方案的決策。該證據顯示，相對於與關係企業而言，用戶較不願意讓其個人資料與第三人分享，據此，聯邦通訊委員會關於「用戶個人資料一旦離開電信事業而落入不受電信法第 222 條規範之主體(entities)之手，將處於揭露的極大風險」之認定，係合理的。

至於，針對聯邦通訊委員會 2007 年「用戶專屬線路資訊」相關命令是否屬於恣意裁量而違反行政程序法，法院則不認為其違反行政程序法，因為基於與上訴人關於違反美國憲法第一修正案主張被駁回之相同理由，有相當證據支持聯邦通訊委員會制定 2007 年「用戶專屬線路資訊」相關命令之正當性。[474]

由於聯邦通訊委員會 2007 年「用戶專屬線路資訊」相關命令要求部分領域應回歸經過「選擇加入」同意的做法，乃係因應資料被仲介使用日漸增多之現象而來，以及對於選擇電信事業與第三方行銷夥伴之關係之原因，聯邦通訊委員會已充分加以解釋，故法院乃駁回該上訴，因為聯邦通訊委員會已為決策所需的合理分析。事實上，在進行修改施行細則期間，聯邦通訊委員會發現，倘未事前取得消費者同意，消費者將因此不太支持電信事業與第三人分享其個人資料；因此，聯邦通訊委員會乃要求[475]，倘電信事業欲與合資夥伴或獨立自主的契約締約相對人分享「用戶專屬線路資訊」者，應經用戶明示同意。

(三) 行動設備所蒐集「用戶專屬線路資訊」亦應受電信法及相關施行細則之規範

近來，科技的快速發展，對於立法者、主管機關或市場運作，均形成新的挑戰。尤其，針對電信事業利用新發展的軟體(如 Carrier IQ)，將其安裝於終端用戶的行動設備(mobile devices)之上，而蒐集及儲存資訊(如來電的電話號碼、所撥打出去的電話號碼、撥打或接收電話的時間、通話的持續時間、通話的地點)。因此，聯邦通訊委員會乃於 2013 年 6 月 27 日發布的「確認決定」(Declaratory Ruling[476])

[474] MAJOR COURT DECISIONS, 2009, 17 CommLaw Conspectus 869, 872-874 (2009).

[475] MAJOR COURT DECISIONS, 2009, 17 CommLaw Conspectus 869, 872-874 (2009).

[476] In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, at 3, available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-89A1.pdf (last visited June 30, 2014).

中指出，由於電信事業利用軟體而控制用戶的行動設備，進而蒐集關於使用電信服務之數量、技術規格、型態、目的地與總額之資訊[477]，且該資訊係用戶單純依業者與用戶間之關係而允許業者使用[478]，因此，該等用戶的行動設備乃係「用戶專屬線路資訊」。

綜此，藉由對於用戶行動設備的控制而蒐集「用戶專屬線路資訊」之電信事業，應按電信法及相關施行細則規定而保護「用戶專屬線路資訊」。

然而，並非行動無線設備所蒐集之所有資訊均係「用戶專屬線路資訊」。某些軟體所記錄的資訊未涉及電信服務，亦未涉及「用戶專屬線路資訊」法定定義所要求之使用電信服務之數量、技術規格、型態、目的地與總額之資訊。再者，當前行動作業系統驅使用戶必須下載由第三人所開發而卻會進行個人資料蒐集之「應用程式」、「應用軟體」(applications)。雖該第三人所開發之「應用程式」、「應用軟體」勢將引發隱私議題的關注。

但是，一般而言，其卻超出電信法及相關施行細則之適用範圍。例如，第三人所開發之「應用程式」、「應用軟體」所蒐集之個人資料中，倘係受電信事業指示而蒐集者，則為「用戶專屬線路資訊」；倘非受電信事業或其代理人指示而蒐集者，則不會基於業者與用戶間之關係而提供予電信事業使用。再者，儲存於行動設備之資訊(如聯絡名單【contact list】、通話紀錄【call log】)，倘非受電信事業之控制、亦非用以傳遞予電信事業、或者電信事業亦無法接觸，則非屬「用戶專屬線路資訊」，因為其不會提供予電信事業使用。[479]

(四) 美國電信事業配合「用戶專屬線路資訊」相關電信法及施行細則之情形

---

[477] 47 U.S.C. § 222(h)(1) (defining "customer proprietary network information"); see also § 222(f)(1) (requiring express prior authorization of the customer for the use or disclosure of or access to location information). Subsequent to the adoption of section 222(c)(1), Congress added subsection (f). Section 222(f) provides that, for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. 47 U.S.C. § 222(f).

[478] 47 U.S.C. § 222(h)(1).

[479] In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, at 10-11, available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-89A1.pdf (last visited June 30, 2014).

美國電信事業(如 AT&T[480]及 Verizon[481])為配合上開「用戶專屬線路資訊」相關電信法及施行細則之規定，一般均在其「隱私權政策」(privacy policy)中明示，未經用戶同意者，將不會與非關係企業分享其「用戶專屬線路資訊」；但會與關係企業分享「用戶專屬線路資訊」，惟用戶得限制之。再者，該等「隱私權政策」常亦包括下列資訊之描述：所蒐集個人資料為何、如何蒐集個人資料、所蒐集個人資料用途為何、所蒐集個人資料是否與第三人分享、所蒐集個人資料之匿名化與其相關彙整(aggregate)、用途及分享為何、用戶對於被蒐集個人資料之用途或分享得行使之選擇與控制為何、保護所蒐集個人資料以避免被未經授權之接觸、利用或揭露之安全措施為何、用戶對於被蒐集個人資料之接觸或加以更正補充之管道為何、「隱私權政策」有重大變更時用戶所得行使之選擇為何(如「選擇退出」)、取得隱私標章為何(如 TRUSTe Privacy Program)。

三、垃圾電話、傳真或電子郵件之管制

1991 年通過的「電話消費者保護法」(Telephone Consumer Protection Act)，用以限制自動撥號系統、人工或預錄語音訊息、簡訊與傳真機器之使用。除取得接收者之事前明示同意外，否則，「電話消費者保護法」與聯邦通訊委員會(FCC)所制定之相關施行細則，要求行銷業者不得於早上 8 點前或晚上 9 點後打電話、應保有要求不要再接到電話之消費者之「不要打電話」(do-not-call)名單、以及禁止發送未經邀請之廣告傳真。但對於業者既有客戶之電子行銷電話，則不在此限[482]。

再者，「電話消費者保護法」關於未經邀請之廣告傳真之規範被 2005 年通過之「垃圾傳真防止法」(Junk Fax Prevention Act of 2005[483])所修正，而賦予垃圾傳真接收者得於州法院向發送者求償。2003 年通過的「未經邀請而主動推介色情與市場銷售之侵犯管制法」(Controlling the Assault of Non-Solicited Pornography and Marketing Act, Can-Spam Act)係確立美國關於商業電子郵件之國家標準，於 2004 年 1 月 1 日生效。「未經邀請而主動推介色情與市場銷售之侵犯管制法」未禁止所

480 AT&T Privacy Policy, available at http://www.att.com/Common/about_us/privacy_policy/print_policy.html (last visited July 1, 2014).

481 Verizon Privacy Policy, available at http://www.verizon.com/about/privacy/ (last visited November 15, 2014).

482 Jody R. Westby, *supra* note399, 70-71 (2004).

483 Junk Fax Prevention Act of 2005, https://www.asaecenter.org/files/FileDownloads/S714-HouseSenate2005.pdf (last visited November 15, 2014).

有形式之未經邀請而主動推介之商業電子郵件，但其要求應有一致性之通知與「選擇退出」之規範。

「選擇退出」之資訊應包括實體郵寄地址及應指出所寄送之電子郵件係一種主動推介(solicitation)。而垃圾郵件(spam)之某些欺罔手法乃被禁止的，例如：(a)使用不實或誤導之標題或信件資訊、(b)藉由取道其他電腦或重送之方式而偽裝垃圾郵件之來源、(c)藉由不實偽裝或陳述而取得網域名稱(domain name)、發信電子郵件地址或 IP 地址。「未經邀請而主動推介色情與市場銷售之侵犯管制法」並要求聯邦通訊委員會應制定規範，以保護消費者免於接收不需要之行動服務之商業信件。再者，倘違反「未經邀請而主動推介色情與市場銷售之侵犯管制法」者，將被視為不公平或欺罔(unfair or deceptive)之行為或慣例，而為聯邦貿易委員會加以執行管制之對象。[484]

四、結論

如前揭，多數的電信服務，就隱私的保護，均會對「通訊內容」與「通訊特徵」形成挑戰。其中，涉及通訊內容者，自 1967 年 Katz v. United States 案之後，最高法院即認定，政府如未事先取得令狀，即不能合憲地監聽或截聽電話通話內容；且 1986 年「電子通訊隱私法」亦禁止監聽、截聽或揭露任何電子通訊的內容。另外，涉及通訊特徵者，1996 年以前，關於電信交易的資訊(如電話號碼、通話時間、通話地點與通話長短)，係不受法律保障；然而，1996 年通過的電信法，則包含了保護「用戶專屬線路資訊」之隱私條款。

按 1996 年電信法，除依法律規定或經用戶同意者外，電信事業禁止以電信法第 222 條所定以外方式而使用、揭露或允許接觸「用戶專屬線路資訊」。惟關於「用戶專屬線路資訊」之使用、揭露或允許接觸，該條未明定，應以何種方式取得用戶同意。對此，美國聯邦通訊委員會曾數度公布「用戶專屬線路資訊」相關命令及施行細則，但卻曾被提起訴訟並被質疑其是否合憲，因此，聯邦通訊委員會乃適度修改施行細則，以兼顧電信事業運用「用戶專屬線路資訊」之行銷需求與用戶「用戶專屬線路資訊」之隱私保護。

整體而言，按聯邦通訊委員會所公布命令及施行細則，就應取得用戶同意之

[484] Jody R. Westby, *supra* note399, 62-63 (2004).

方式，現行有效之制度，乃針對「用戶專屬線路資訊」接收者與電信事業關係之不同，而採行「選擇退出」與「選擇加入」雙軌並行的「同意」行使模式。針對「用戶專屬線路資訊」，只要電信事業所分享的關係企業係通訊相關的業者，其同意模式乃採「選擇退出」方式，毋庸取得用戶的事前明示同意；針對與非關係企業之第三人分享「用戶專屬線路資訊」部分，倘電信事業欲將「用戶專屬線路資訊」揭露予合資夥伴或獨立自主的契約締約相對人或允許其得接觸使用「用戶專屬線路資訊」時，電信事業應取得用戶「選擇加入」同意。

另外，聯邦通訊委員會 2007 年修改「用戶專屬線路資訊」相關施行細則，用以包括「通話細節資訊」之撥入、撥出電話的「位置」資訊。聯邦通訊委員會並於 2007 年「用戶專屬線路資訊」相關命令中釐清，網路電話(VoIP)及 IP 驅動的網路電話提供者亦應遵守「用戶專屬線路資訊」相關的規範。再者，藉由對於用戶行動設備的控制而蒐集「用戶專屬線路資訊」之電信事業，亦應按電信法及相關施行細則規定，進行「用戶專屬線路資訊」之保護。

表 3-14 美國個資要件整理

個資 要件	用戶使用電信服務之數量、技術規格、型態、目的地與總額之資訊	備註
利用目的告知	電信事業通知內容應敘述「用戶專屬線路資訊」之利用目的。	
個資保存期限	一、電信事業應保存將「用戶專屬線路資訊」揭露、提供予第三人或第三人被允許得接觸「用戶專屬線路資訊」之所有情形之檔案至少一年。 二、電信事業應以電子或其他方式保有所發現之違反「用戶專屬線路資訊」情事及曾通知美國特勤局與聯邦調查局情事之檔案，並應保持該檔案至少兩年。	
利用目的限制	僅能使用、揭露或允許接觸該用戶專屬線路資訊，於提供（A）該等資訊因而衍生之電信服務，或（B）對於提供該等電信服務所必要或使用之服務，包含電話簿的出版。	四項例外事由
與第三人共同	針對「用戶專屬線路資訊」，只要電信事業所分享的關	

利用個資	係企業係通訊相關的業者，其同意模式乃採「選擇退出」方式，毋庸取得用戶的事前明示同意。	
對第三人提供之限制	針對與非關係企業之第三人分享「用戶專屬線路資訊」部分，倘電信事業欲將「用戶專屬線路資訊」揭露予合資夥伴或獨立自主的契約締約相對人或允許其得接觸使用「用戶專屬線路資訊」時，電信事業應取得用戶「選擇加入」同意。	
事故發生之通知	電信事業違反「用戶專屬線路資訊」之相關規範時，應通知執法機關。電信事業完成依法通知執法機關之程序前，不論係出於自願或依聯邦、地方法律規定，不應通知用戶或公開地揭露該等違反情事。	

資料來源：本研究自行整理。

第四章　電信事業監管機制之介紹

第一節 概述

一、背景

在全世界超過 22 億人利用網路之今日，網路已成為人們工作、學習、社交、交易等生活上不可或缺之工具。更因企業經營國際化，以及雲端科技產業興起，國內外間跨國傳遞已為跨域國界的問題個人(如顧客、員工)資料已為企業事業活動之一環，從而個資之保護須跨國合作執行始能落實，紛爭或違法事件之解決及救濟，更須國際間互相協助，始能發揮實際救濟效力。

長年來如何在各個國家間取得一定共識，建立相同水準及有實效性之國際性保護個資公約，以保障個資安全、自由於國際間傳送，為各個有關個資保護法之國際組織首要議題。從而個資法之執行已非僅為國內事務，乃須經常性與各國互動、協議之國際事務，政府實需設置有統一事權得代表國家參與國際會議，與各國進行國際協議、合作執法等之機關。

其次，尤其近年各國以防止恐怖組織活動、打擊犯罪維護治安為由，廣設監視攝影器或監視人民之電子通訊記錄等事件頻傳[485]，嚴重侵害人民之資訊自主權。因此對行政機關之蒐集處理或利用個資，必須設置獨立監督機制，以有效監督政府機關合法蒐集、處理或利用人民個資，防止弊端發生。非公務機關民間之蒐集、處理或利用個資，雖得由各目的事業主管機關或地方政府機關監督其遵守個資法，然因關於當事人請求閱覽刪除、訂正等糾紛之處理程序，常涉及法律之解釋與適用，為避免執法者各自為政，造成法律執行上寬嚴不一，及個資安全體制(security system)之建立時，規格、技術水準須求統一，實有必要設一獨立機關提供諮詢及予以輔導。

此外，當事人與個資之蒐集、處理或利用者發生紛爭時，常係以單一個人力

[485]2013 年 6 月 16 日曾任美國中央情報局之技術人員史諾登(Edword Snowden)於香港揭露美國國家安全局(NSA)用以監視網路平台之「稜鏡計畫(PRISM)」。

量對抗行政機關或企業、團體，有資力不對等，救濟程序費時，訟源增加之問題；如有一獨立機關得先介入當事人紛爭中調查、調解，對當事人之救濟較有利，亦可減少訴爭。故設一獨立機關，擔任各機關、團體或個人有關個資問題之諮詢，發現個資處理上有問題時，提供建議或調解糾紛，負責遵法之宣導、資訊安全、教育訓練等事宜，除監督個資法之施行外，更能主導個資法之落實與發展。

二、國際之現況

(一) 歐盟指令

查歐盟個人資料保護指令（Directive 95/46/EC）第 6 章第 28 條第 1 項[486]即規定各加盟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；此機關行使法定職務時，應完全獨立。前開歐盟指令不僅要求加盟國有義務賦予監督機關獨立性，關於其職權之行使，依同條 2、3 項更規定應有如下權限：①會員國於個資處理上，如對個人權利及自由保護，採取行政措施或制定規則時，應與其進行協議；②有調查權、處理對象資料之近接權、及遂行監督職務收集所有必要資料之權限；③干預權限：對資料當事人權利及自由帶來危險之虞的處理作業進行事前勸告，並有適當公開勸告、命令封鎖、刪除或毀棄個資檔案，或以暫時或確定命令禁止處理之權限，警告或懲戒管理者之權限，將法施行之問題點照會國會或其他政治機關之權限；④有違反依本指令制定之本國法令情事時，得提起訴訟或將其通知司法機關之權限。⑤接受個人或代表個人之團體有關個資處理之權利及自由之請求並通知關係個人其請求結果。接受有關個資處理合法性之請求，通知個人進行調查之事。⑥定期作成活動報告書並予以公開。

(二) 歐洲理事會（Council of Europe, CoE）[487]

---

[486] Article 28 (Supervisory authority)
1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them.

[487] 為 1964 年設置於人權，民主主義，法支配等領域主導國際社會基準認定之泛歐洲國際組織。至 2014 年 4 月已訂 216 項條約。「個人資料自動處理有關個人保護條約（Convention for the protection of Individuals with regard the Automatic Processing of Personal Data）」，為 1081 年 1 月 28 日訂立 1985 年 10 月 1 日生效之條約第 108 號，後於 2001 年在同條約追加監督機關及跨境資料流通之議定書。(CoE, Additional Protocol to the Convention, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data)

歐洲理事會第 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、訴訟程序之同時、應聽取所有人之觀其個人資料之權利及基本自由之申訴。

在歐洲議會各加盟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裝備[488]。

(三) 資料保護及隱私委員（International Conference of Data Protection and Privacy Commissioners：ICDPPC）[489]

各個資保護先進國間之資訊官為交換各國執行個資法之經驗及意見而召開之會，其限於設置有獨立、自主個資監督機關國家之資訊官，始得參加每年所舉辦之國際會議；在此會議上，各國討論並通過有關個資保護之國際基準、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。會議結果對各國具有重大影響力；該國際會議則對申請參加國家所設立個資保護機關定有審查基準（CRITERIA AND RULES FOR CREDENTIALS COMMITTEE AND THE ACCREDITATION PRINCIPLES），其 B 部分即揭示資料保護機關須具備以下兩要件：

1. 法之依據：須為依據適當法律所設置之公部門。

2. 自主性：應保證其行使權能有相當程度之自主性、獨立性[490]。

至 2013 年該會議約有 70 個國家、地區共 500 人參加。

上述國際發展之背景，亦是因應近年快速普及於無國界、無時間限制下，個

[488]參閱石井夏生利，個人情報保護法の理念と現代的活動，勁草書房，頁 349，2008 年。堀部政男，社会保障・税番号大綱と個人情報保護─行政との関連性の検討，季刊情報公開・個人情報保護，vol.42，2011 年 9 月，頁 11。

[489]為 1979 年召開第一次會議之國際會議，至 2013 年 9 月於波蘭華沙召開 35 次會議。當初召開目的是歐洲個人資料保護先進國家間之資訊官交換意見之平台。

[490]International Conference of Data Protection Commissioners Criteria and Rules for Credentials Committee and the Accreditation Principles，Adopted on 25September 2001 and Amended on 9 September 2002。http：//privacy conference 2007. Gc.ca/PRIVACY-190100-vl-Accreditation – principles-and- Committee-rules-ENG.pdf(最後瀏覽日：2014 年 6 月 25 日)。

資保護之貫徹與有效之法律執行，在國際間勢必須建立具相同水準保護及執法體制。加諸各國為推展電子商務或發展雲端運算中心提升國際競爭力，有關個資保護之法制必須與國際接軌，在各國間不受阻礙，安全傳送或接收個資為必要之前提要件。因此在個資保護法制中，建置符合國際規約要求之獨立監督機關，實為國家建構完整個資保護法制，進入全球數位市場不可或缺之配備。

基此背景，歐盟各國自不待言，除美國因其原即無全面適用之個資法，且重視資本主義市場自由，對資訊之自由流通政府不宜介入干涉，因此未設有個資法執行之監督機關；而世界其他區域或國家則為與世界接軌，減少電子商務之貿易障礙，其位階或職掌、組織方式或有不同，然多設有監督個資法施行之專責機關或部門；本章以下即就研究對象之國家介紹分析之。

第二節 德國

一、自律之機制

(一) 認證標章

根據聯邦個人資料保護法第 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）。」由於至今尚未針對聯邦個人資料保護法第 9a 條第 2 項所定事項進一步制頒相關規範，故現行對於個人資料保護之認證多為各企業自主採行，藉以贏取費者對於其維護個人資料能力之信賴。

除了一般國際通用之 ISO27001 外，德國本身亦有就個人資料保護之領域提供相關認證的機構，如：TÜ V 及 DEKRA，其屬較具規模且受國際所認可之獨立驗證機構，其認證後所提供之標章對消費者而言亦較具公信力。TÜ V 有提供例如 TÜ ViT 之認證，專就所有用戶透過室內電話每日所產生之所有資料的蒐集與處理程序進行檢驗：另外就電信事業資料庫之運作、所採行安全措施及使用情況亦提供相關認證。DEKRA 則對於通過「聯邦個人資料保護法所要求之資料保護及資料安全」認證後，授予 DEKRA-Siegel（標章），電信事業者多透過此一外部檢驗自主表彰其在遵法義務上之踐履。

認證標章要發揮其功能，必須確保程序透明、客觀且安全；認證機關獨立並專業，標章運用之期限及所及範圍皆應有明確規定，惟在目前缺乏對於認證標章與驗證管理一致性標準，且未強制公開檢驗結果之情況下，一般對於認證單位是否確實獨立客觀，或其檢驗結果是否值得信賴，往往仍有所質疑。[491]

(二) 資料保護監察人（Datenschutzbeauftragter）之設置

不論之公務單位或是非公務單位，只要是有自行或受託蒐集、處理或利用個

[491]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.364-366.

人資料者，均應依聯邦個人資料保護法第 9 條規定，採行適當之技術與組織上必要措施，確保符合該法對於個人資料保護水準之期待。[492]其中德國聯邦個人資料保護法第 4f 條及第 4g 條所規範之資料保護監察人，即為透過組織與人員之設置，以求達到此一法律要求之相應機制[493]。

德國聯邦個人資料保護法第 4f 條第 1 項規定，無論是公務單位或非公務單位，只要有以自動化方式蒐集、處理或利用個人資料之情形，即需以書面指定資料保護監察人，專責監督個人資料保護之相關事項，確保個人資料保護相關規範之遵行（第 1 句）。非公務單位至遲應於開始運作後 1 個月內任命資料保護監察人（第 2 句）。若是以其他方式蒐集、處理或利用個人資料，而有 20 位以上人員因此受僱時，亦同（第 3 句）。但至多雇用 9 位以下員工負責自動化處理個人資料之非公務機關，不適用上述第 1 句及第 2 句之規定（第 4 句）。而針對非公務單位執行自動化處理時應遵守事先管控，或於商業過程中，以傳遞、匿名化傳遞或市場或意見調查為目的，而自動處理個人資料者，不問其負責該自動化處理個人資料之員工人數，均應指定 1 名資料保護監察人（第 6 句）。而針對依法無須任命資料保護監察人之非公務機關，德國聯邦個人資料保護法第 4g 條第 2a 項將其個人資料保護之責任轉交由該非公務單位之負責人，要求其應另尋適當之方式落實本法交付與資料保護監察人之任務。

德國聯邦個人資料保護法第 4g 條第 1 項就資料保護監察人之任務加以規範：「資料保護監察人應負責本法及其他有關資料保護之規定被遵守。資料保護監察人基於此一目的，於有疑義時，得向負責單位中對資料保護控管之主管部門洽詢。他尤其應：1. 監督對協助處理個人資料之資料處理程序，使其運用符合規定；為此目的，他對於自動化處理個人資料之計畫應適時受到通知。2. 使辦理個人資料處理之人員，經適當之措施，使其熟悉本法及其他個人資料保護之規定，以及個案中資料保護之特別需求。」

---

[492]聯邦個人資料保護法第 9 條第 1 句之附件中，就公司運作程序及 IT 系統之個人資料保護領域應建置適當之技術性與組織性措施，包括：進入處理與利用個人資料機構之權限管制（Zutrittskontrolle）;資料處理系統使用管制(Zugangskontrolle);取得權限之管制(Zugriffskontrolle);傳遞之管制（Kontrolle der Weitergabe）; 輸入管制（Eingabekontrolle）; 被授權者之管制（Kontrolle des Auftragsnehmers）; 資料保存之控管（Verfügbarkeitskontrolle）與目的分離原則（Trennungsprinzip）。

[493]關於德國聯邦個人資料保護法設置資料保護監察人相關規範之說明與介紹， Vgl. Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.199ff.. Wohlgemuth, Hans H./ Gerloff, Jürgen, Datenschutz, 3. Aufl., 2005, S. 145-150.

在資料保護監察人之任用資格上，德國聯邦個人資料保護法第 4f 條第 2 項要求其應「具備符合其所任單位資料處理規模與個人資料保護需求之充分專業（Fachkunde），並且可靠(Zuverlässigkeit)」。但為維持執行職務之獨立性，其於組織架構上雖直接隸屬於所任單位之負責人，惟其於依專業執行個人資料保護業務之範圍內不受指揮（weisungsfrei），且不得因此受有不利待遇（德國聯邦個人資料保護法第 4f 條第 3 項）。就資料保護監察人履行職務所需，包括為維持專業而需之訓練及進修、行使職務必要之人員、場地與設備配置等，其所屬單位均應給予相應之協助。[494]

資料保護監察人對於執行職務之過程中所接觸之個人資料負有保密的義務，在德國聯邦個人資料保護法第 4f 條第 4 項規定，除經當事人免除上述義務之情況外，其對於彰顯當事人識別性，以及得尋繹出當事人情況之資料負有保密義務；或是因執行職務接觸到他人應拒絕提供作為證據之相關資料時，其亦同受拘束，不得對外提供（德國聯邦個人資料保護法第 4f 條第 4a 項）。

上述以法律要求各企業內設置資料保護監察人之規定，某種程度上融合了自律與他律之特質：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，並與監督機關保持密切的聯繫，提供一雙向溝通之管道；[495]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[496]；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，實具重要性。

二、他律機制：德國資料保護之監督機關

依據德國電信通訊法（TKG）之規定，除以聯邦民生網絡署（Bundesnetzagentur, BNetzA）作為主管機關，依據該法負責電信服務業者營運之監督與管理外；另就電信服務業者蒐集、處理、利用個人資料之行為，依據電信通訊法第 115 條第 4 項交由聯邦資料保護與資訊自由監察機構（Bundesbeauftragter für Datenschutz und

[494]德國聯邦個人資料保護法第 4f 條第 3 項第 7 句及同條第 5 項規定參照。

[495]聯邦個人資料保護法第 26 條第 4 項規定，聯邦個人資料保護與資訊自由監察官應與各邦主管監察資料保護之公務單位及第 38 條所稱之監督單位，於個人資料保護之任務範圍內共同合作。

[496]依據德國聯邦個人資料保護法第 4f 條第 5 項規定，當事人得隨時洽詢資料保護監察人。

Informationsfreiheit, BfDI）依據德國聯邦個人資料保護法之相關規定負責監管。關於聯邦民生網絡署之組織、權限、行使程序等，皆明文規定於德國電信通訊法第 8 部分，第 116-141 條中，但因其職權與個人資料保護之監管業務並無直接關連性，故於後將論述重心置於與本研究所關切之「個人資料監管機制」，就聯邦資料保護與資訊自由監察機構進行介紹與說明。

依據德國聯邦個人資料保護法之規定，就非公務機關之個人資料保護業務監管，一方面透過德國聯邦個人資料保護法第 4f 條及第 4g 條所要求企業依法指定之內部資料保護監察人，進行內部自律控管；另一方面，則是透過他律之機制，由主管監督機關進行外部監管，此部分又可再區分為客戶個人資料與非客戶個人資料保護之業務，前者劃歸由聯邦資料保護與資訊自由監察機構（BfDI）負責，後者則由各邦所設立之資料保護監察機構（Landesbeauftragter für Datenschutz, LfD）作為監督機關[497]。

資料保護監察機構的獨立性一直為其運作上備受重視的環節，歐洲法院與德國聯邦憲法法院多次於判決中指出，個人資料保護之監督（Datenschutzaufsicht）是確保資訊自決權所不可或缺之把關機制，對此基本權利之侵害僅有在一獨立個人資料保護監察機關存在之前提下方得被允許[498]。有鑑於各邦所設立之資料保護監察機構（LfD）多隸屬於各邦政府，其獨立性恐有欠缺，歐洲法院於 2010 年 3 月 9 日做成 C-158/07 判決，認德國違反歐盟 95/46/EG 指令第 28 條第 1 項之規定，未得讓非公務單位之監督機關以「全然獨立（in völlig Unabhängigkeit）」之型態履行其任務[499]。為達成此一高度獨立性之要求，現行德國聯邦個人資料保護法預計將修法刪除聯邦政府之法律監督及聯邦內政部之職務監督規定[500]，若得通過，則其未來將僅受國會及法院之監督，力求排除其設置於行政機關之下而無法「全然

[497]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.897, 900. Wohlgemuth, Hans H./ Gerloff, Jürgen, a.a.O. Fn.493,S. 143.

[498] Zöllner, Dieter, Der Datenschutzbeauftragte im Verfassungssystem, Duncker & Humblot, Berlin,1995, S.167-170.

[499] EuGH C-518/07, 09.03.2010, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5a7fbfe61f36641abb75ccfe06cd6bdab.e34KaxiLc3qMb40Rch0SaxuObN50?text=&docid=79752&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=126943(最後瀏覽日期：2015 年 2 月 5 日）

[500]聯邦個人資料保護與資訊自由監察機構就此所發布之新聞請參考：http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2014/18_Unabhaengigkeit.html?nn=5217154 (最後瀏覽日期：2015 年 2 月 5 日）

獨立」之疑慮。

(一) 德國聯邦資料保護與資訊自由監察機構

為確保個人資料保護監督機關之獨立性，於 1977 年依德國聯邦個人資料保護法於聯邦層級設置德國聯邦資料保護及資訊自由監察機構[501]，其首長為聯邦資料保護及資訊自由監察官，由聯邦議會（Bundestag）選任，獨立執行職務不受干涉。德國聯邦資料保護與資訊自由監察機構在組織上雖隸屬於行政機關，但其首長或重要成員之人事任命權皆由國會掌握，其組織設計與人士任命制度，介於我國監察院與行政院所屬獨立機關之間，有其特色，以下僅分就其選任、法律地位及職權進行說明。

1、 選任

依德國聯邦個人資料保護法第 22 條，聯邦資料保護及資訊自由監察機構設聯邦資料保護與資訊自由監察官 1 名，選舉時需年滿 35 歲，由聯邦政府提名，經聯邦議會表決同意後由聯邦總統任命，任期 5 年，得連任 1 次，[502]薪資由聯邦政府支付，比照法官與高級公務員，其與聯邦政府間屬公法上職務關係（öffentlich-rechtliches Amtsverhältnis），而非公務員關係(Beamten Verhältnis)，聯邦政府享有法律監督之權限（Rechtsaufsicht），其設立於聯邦內政部內，由其提供執行職務所需之人員及設備，並受其職務上之監督（Dienstaufsicht）。[503]

2、 法律地位

聯邦資料保護與資訊自由監察官之職務關係始於任命狀（Ernennungsurkunde）之交付，而因任期屆滿或被免職終止，其免職應具備與終身職法官免職相同之理由，由聯邦總統應其本人請求或聯邦政府之建議，免除其職務，惟若聯邦內政部

[501]德國聯邦資料保護及資訊自由監察機構，請參見：
http://www.bfdi.bund.de/DE/Home/home_node.html (最後瀏覽日：2015 年 2 月 5 日）

[502]請參見聯邦個人資料保護法第 22 條第 1 項:「聯邦資料保護與資訊自由監察官由聯邦政府提名，經聯邦眾議院議員超過法定人數半數以上同意選任之。其於選舉時需年滿 35 歲。當選人由聯邦總統任命之。」及同條第 3 項：「聯邦監察官之任期 5 年，連選得連任一次。」聯邦個人資料保護法中譯請參考法務部編，德國聯邦個人資料保護法，收錄於外國個人資料保護法規彙編，2002 年。

[503]請參見聯邦個人資料保護法第 22 條第 4 項：「聯邦資料保護與資訊自由監察官依本法與聯邦為公法上職務關係。其依據本法。獨立行使職權。其受聯邦政府法上之監督。」及同條第 5 項：「聯邦監察官設立於聯邦內政部中。其受到聯邦內政部職務上之監督。聯邦監察官應得運用完成職務所必要之人員及設施；其應於內政部所題計畫報表中以獨立一章記載。人員之進用應與聯邦監察官協議為之。進用人員如不遵行監察官所擬行之措施，經與其協議後，得將其調職、暫時移調或轉職。」Vgl. Kruse, Julia, Der ö ffentlich-rechtliche Beauftragte, Duncker & Humblot, Berlin,2007, S.218-221.

長提出請求時，聯邦資料保護與資訊自由監察官有義務繼續擔任此職務至下一任監察官繼任為止。（德國聯邦個人資料保護法第 23 條第 1 項）

依據德國聯邦個人資料保護法第 23 條第 2 項規定，聯邦資料保護與資訊自由監察官禁止兼職，其除本職外，不得擔任其他有給職、從事營業與職業，亦不得加入營利企業、政府或聯邦或邦之法人所屬董事會、監察會或行政管理部門。且不得收受報酬而為法院以外之鑑定書。

聯邦資料保護與資訊自由監察官負有保密義務，即便於職務關係結束後，仍有就其因職務知悉事項保密之義務，但職務上溝通之說明、顯而易見之事實或依其性質無保密必要者不在此限。未經聯邦內政部長之同意，即便已去職，於法庭內外皆不得陳述或說明上開應保密之事項。但法律明訂之告發犯罪及維護自由民主秩序免於受到危害之義務，不在此限。（德國聯邦個人資料保護法第 23 條第 5 項）

3、 職權

(1) 監察(Kontrolle)

聯邦個人資料保護法第 24 條賦予聯邦資料保護與資訊自由監察官監管公務單位是否有遵行德國個人資料保護法及其他有關資料保護規範之任務（第 1 項），其監督之範圍包括：聯邦公務單位所獲得關於書信、郵政之通信內容及細節情況之個人資料；屬於職業秘密或特殊公務機密之個人資料，尤其是依據租稅通則第 30 條屬租稅秘密者（第 2 項）。於此，德國基本法第 10 條所保障之書信、郵件及秘密通信將受到限制。

聯邦公務單位依據聯邦個人資料保護法第 24 條第 4 項負有協力義務，提供聯邦個人資料保護與資訊自由監察機構及受其委任之人履行任務所需之支援，特別是透過答覆其詢問及提供其所需所有資料之閱覽；另外，確保其隨時得進入所有的辦公處所，以助其遂行監督職權。[504]

(2) 糾正(Beanstandung)

聯邦資料保護與資訊自由監察官依據聯邦個人資料保護法第 25 條規定得享有

[504]但第 6 條第 2 項與第 19 條第 3 項中所列機關僅負有配合聯邦個人資料保護與資訊自由監察官本人或經其書面特別授權之人之義務。且若經聯邦最高行政機關於個案中認定，答覆或提供查詢之內容將有可能危及聯邦或邦之安全時，即不受此拘束。請參見聯邦個人資料保護法第 24 條第 4 項第 3 及 4 句。

糾正之權限：其於確認個人資料之處理或利用有違反聯邦個人資料保護法或其他資料保護規範或是有其他缺失者，得提出糾正並定期要求相關單位[505]表示意見（第 1 項），表示意見中應包括針對糾正內容所採取措施之說明（第 3 項）。然若情節輕微或缺失已排除，聯邦資料保護與資訊自由監察官得據聯邦個人資料保護法第 25 條第 2 項不為糾正或免除被糾正機關表示意見之義務。此一權限應屬得作為確實監督個人資料保護事項之強力後盾。[506]

(3) 提供改善建議與諮詢

聯邦資料保護與資訊自由監察官依據聯邦個人資料保護法第 24 條第 5 項之規定，應將其監督之結果通知公務單位，其中並得提出改善建議，內容應特別結合對於已確認之處理或利用個人資料缺失的排除。

聯邦資料保護與資訊自由監察官依據聯邦個人資料保護法第 26 條第 3 項之規定，得向聯邦政府與第 12 條第 1 項所列之相關聯邦單位提出資料保護之改善建議，並就其所面臨之問題提供諮詢。

(4) 公開業務報告

根據聯邦個人資料保護法第 26 條第 1 項規定，聯邦資料保護與資訊自由監察官每 2 年必須對國會及社會大眾提出有關資料保護重要發展的業務報告，並將該報告刊登在國會公報以及其網站上。[507]

(5) 提供鑑定意見

聯邦資料保護與資訊自由監察官應依聯邦眾議院或聯邦政府之請求，提出鑑定書與報告（聯邦個人資料保護法第 26 條第 2 項第 1 句）。德國法院於審理程序中，往往亦會借重個人資料保護監察機構之專業，請其本於客觀中立之立場，提

[505]聯邦個人資料保護法第 25 條第 1 項下有 4 款，就糾正對象分別定為：1.關於聯邦行政者，向聯邦最高主管機關；2. 關於聯邦鐵路財產者，向其董事會；3. 關於由聯邦郵政特殊財產捐資依法設立之企業，且當其依據郵政法享有排他權利者，向其董事會；4. 關於聯邦所轄之公法社團、營造物與財團，以及此種社團、營造物與財團之結合組織，向其董事會或其他有代表權之機關。針對第 4 款單位之糾正，應同時通知其主管監督機關。

[506]Wohlgemuth, Hans H./ Gerloff, Jürgen, a.a.O. Fn.493, S. 143-144.

[507]聯邦個人資料保護與資訊自由監察官所提報之最新一期業務報告乃第 24 期（2011-2012）業務報告，請參考：
http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/24TB_11_12.pdf?__blob=publicationFile&v=7 (最後瀏覽日期：2015 年 2 月 5 日)

供相關鑑定意見（Gutachten）作為判決之參考，[508]例如德國聯邦憲法法院於 2005 年 7 月 27 日作成之預防性電信監察判決中，即於審理程序中請求聯邦個人資料保護與資訊自由監察官及下薩克森邦個人資料保護監察官提供鑑定意見，並往往明列於判決書中一併對外公開。

(6) 調查

依聯邦議會（Bundestag）、請願委員會（Petitionausschuss）、內政委員會（Innenausschuss）或聯邦政府之請求，聯邦資料保護與資訊自由監察官應進一步調查聯邦公務單位就資料保護事務與流程所發布之指令（聯邦個人資料保護法第 26 條第 2 項第 2 句）。

(7) 接受申訴

德國聯邦個人資料保護法第 21 條規定，任何人如認為聯邦公務單位蒐集、處理或利用其個人資料致其權利受到損害者，得向德國聯邦資料保護與資訊自由監察官提出申訴。若其申訴之標的乃針對聯邦法院蒐集、處理或利用個人資料之行為，並僅以行政事項（Verwaltungsangelegenheiten）為限，方有其適用。[509]

(8) 共同合作

德國聯邦個人資料保護法第 26 條第 4 項要求聯邦資料保護與資訊自由監察官應與各邦內負責監管個人資料保護之公務單位共同合作，其中亦包括同法第 38 條所稱之監督機關。

聯邦資料保護與資訊自由監察機構行使上述職權，以確保電信服務業者善盡法定之個人資料保護義務，其除得就電信服務業者之違失行為，依據德國聯邦個人資料保護法予以裁罰外；亦可通報其主管機關，即聯邦民生網絡署（BNetzA），由其依據電信通訊法之規定，再行判斷應如何處罰。

(二) 各邦之資料保護監察機構

德國就個人資料保護之落實與監督，在非公務機關的部分授權各邦政府或其

[508]例如德國聯邦憲法法院於 2005 年 7 月 27 日作成之預防性電信監察判決中，即於審理程序中請求聯邦個人資料保護與資訊自由監察官及下薩克森邦個人資料保護監察官提供鑑定意見，該判決中譯請參考謝碩駿譯，前揭註 167。

[509]德國聯邦個人資料保護法第 24 條第 3 項針對德國聯邦資料保護與資訊自由監察官得就聯邦法院進行監督之範圍，亦有相同的限縮。

授權之單位指定組成監督資料保護執行之監督機關，實際負責執行各邦個人資料保護事項，因此監督機關之名稱及設立依據，將因各邦而異。[510]聯邦與各邦之資料保護機構之地位平等，目前維持一年召開 2 次會議，由聯邦及各邦等 17 個個人資料保護主管機關共同協調改進及須增加或解釋事項，以及中央、地方分治事項之劃分，充分展現個人資料保護之管理與監督，亟需各機關共同合作之特性。

電信事業之個人資料保護業務，若非涉及客戶資料，而屬其內部資料，如人事檔案管理，即以各邦之資料保護監察機構作為其監督機關。根據聯邦個人資料保護法第 38 條第 1 項規定，監督機關掌管本法及其他資料保護法規之執行。監督機關提供資料保護監察人及負責單位諮詢並支援其特殊需求。監督機關基於監管之目的可處理或利用其所儲存之資料，或將之傳遞與其他監督機關。監督機關若認定有違反聯邦個人資料保護法或其他資料保護法規時，有權通知相關人、向負責調查或懲處之機關舉發其違反之情況，甚至於嚴重的情況，通報工商業管理機關採行相關管理措施。監督機關應經常性地，至少每 2 年，公開其職務報告，確保其透明性。[511]

聯邦個人資料保護法第 38 條第 2 項要求監督機關應製作登記簿，針對同法第 4d 條規定有登記義務之自動化處理，記載第 4e 條第 1 句所規定之事項。登記簿得供任何人查閱，但不及於第 4e 條第 1 句第 9 款及有權接觸資料之人等事項。

應依監督機關之要求，受檢查之單位及其所委任之主管應儘速呈報監督機關於執行職務時所必要之資料（聯邦個人資料保護法第 38 條第 3 項）[512]。受監督機關委任之監督或檢查人員，於執行職務所必要之範圍內，得於營業與上班時間內，進入該受檢查單位之土地與辦公室進行檢查與巡視，受檢查單位於此負有容忍之義務。其檢閱之項目包括業務文件如依據第 4g 條第 2 項第 1 句所製作之一覽表及相應儲存之個人資料與資料處理程式（聯邦個人資料保護法第 38 條第 4 項）[513]。

[510]聯邦個人資料保護法第 38 條第 6 項規定參照。以巴伐利亞邦為例，其目前分設 2 個專責機關，分別負責公務機關與非公務機關之監管業務。德國目前各邦依據德國聯邦個人資料保護法授權，就非公務機關所設立之之監督機關，請參考：
http://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html (最後瀏覽日期：2015 年 2 月 5 日)

[511]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.899-907.

[512]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.909-910.

[513]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.910-915.

為確保本法與其他資料保護規定受到遵行，監督機關得就違反個資蒐集、處理、利用之情況或是技術上或組織上缺失，採行排除之相關措施。面對重大違反或缺失，尤其是會對於人格權帶來特別危害之情況，若無法透過第 38 條第 5 項第 1 句所採行之措施加以排除，且經科處怠金仍無法於相當期限內排除時，監督機關得禁止蒐集、處理、利用個資或個別程序之運作（聯邦個人資料保護法第 38 條第 5 項）[514]。

三、小結

就電信服務業者蒐集、處理、利用客戶個人資料之行為，依據電信通訊法第 115 條第 4 項規定，乃交由聯邦資料保護與資訊自由監察機構負責監管。而其分別在組織位階、型態與職權上具有以下特色：

（一）組織位階

聯邦資料保護與資訊自由監察機構設立於聯邦內政部內，由其提供執行職務所需之人員及設備，並受其職務上之監督；其與聯邦政府間屬公法上職務關係，而非公務員關係，聯邦政府享有法律監督之權限。

資料保護監察機構的獨立性一直為其運作上備受重視的環節，歐洲法院與德國聯邦憲法法院多次於判決中指出，個人資料保護之監督是確保資訊自決權所不可或缺之把關機制，對此基本權利之侵害僅有在一獨立個人資料保護監察機關存在之前提下方得被允許

現德國聯邦個人資料保護法刻正進行修法，預計將刪除聯邦政府之法律監督及聯邦內政部之職務監督規定，若得通過，則其未來將僅受國會及法院之監督，力求排除其設置於行政機關之下而無法「全然獨立」之疑慮。

（二）組織型態

依德國聯邦個人資料保護法於聯邦層級設置之德國聯邦資料保護及資訊自由監察機構，採首長制，設聯邦資料保護及資訊自由監察官 1 名，由聯邦政府提名，經聯邦議會表決同意後由聯邦總統任命，選舉時需年滿 35 歲，任期 5 年，得連任 1 次，薪資由聯邦政府支付，比照法官與高級公務員，德國聯邦資料保護與資訊自

[514]Plath, Kai-Uwe(Hrsg.),a.a.O.Fn181, S.915-916.

由監察機構在組織上雖隸屬於行政機關，但其首長或重要成員之人事任命權皆由國會掌握，獨立執行職務不受干涉。其任期僅得因任期屆滿或被免職終止，免職應具備與終身職法官免職相同之理由，由聯邦總統應其本人請求或聯邦政府之建議，免除其職務。

（三）職權

監督相關機關是否有確實遵循個人資料保護法之規範；確認個人資料之處理或利用有違反聯邦個人資料保護法或其他資料保護規範或是有其他缺失者，得提出糾正並定期要求相關單位表示意見糾正；提供相關單位關於個人資料保護之建議與諮詢；每 2 年須對國會及社會大眾提出有關資料保護重要發展的業務報告，並公開之；依聯邦眾議院、聯邦政府或是法院之請求，提出鑑定書與報告供其參考；聯邦資料保護與資訊自由監察官應依請求進行相關調查；而任何人如認其個人資料遭蒐集、處理或利用致權利受損時，則得向德國聯邦資料保護與資訊自由監察官提出申訴。

表 4-1 聯邦資料保護與資訊自由監察機構之組織與職權

個人資料保護監管機關	聯邦資料保護與資訊自由監察機構
組織位階	屬獨立行使職權不受干涉之機關，設立於聯邦內政部內，受其職務上之監督，而聯邦政府享有法律監督之權限
組織型態	首長制，由設聯邦資料保護及資訊自由監察官 1 名，由聯邦政府提名，經聯邦議會表決同意後由聯邦總統任命。受任期保障，免職應具備與終身職法官免職相同之理由，由聯邦總統應其本人請求或聯邦政府之建議，免除其職務，以確保其獨立性。
職權	監察、糾正、提供建議與諮詢、公開業務報告、提供鑑定意見、調查、接受申訴

資料來源：本研究自行整理。

第三節 英國

一、自律機制

1、 個資保護指導原則

關於英國電信事業者如何落實個資保護，在「自律監督」方面，產業界有相關之自律組織，如全國個資保護人員協會 (The National Association of Data Protection Officers; 以下稱 NADPO)，成立於 1993 年，定位為個資保護實務與創新構想之傳播交流平台，由全英國公私部門負責個資保護業務人員加入組成[515]。NADPO 除了報導各國關於個資保護最新發展動態，如政府政策、立法例、實際案例等[516]，亦定期舉辦關於個資保護理論與實務之研討會，座談會、工作坊等活動[517]，並發布產業個資保護自律規範與行為準則[518]。

除了產業界自律組織所制訂之自律規範以外，英國個資保護主管機關 Information Commissioner's Office (以下稱 ICO) 依據 DPA 1998 規範，得在諮詢產業同業公會與個資主體代表之意見後，依職權發布關於遵循個資保護之指導原則 (codes of practice for guidance)[519]，或鼓勵個資控制者自行研擬發布個資保護之相關自律規範[520]。較為特別的是，關於個資控制者之間個資分享 (data-sharing) 行為，ICO 必須 (must) 制定相關指導原則[521]，且在制定此等指導原則之前，必須先行諮詢產業同業公會與個資主體代表之意見[522]。ICO 依據不同產業與個資利用類型發布相關指導原則[523]，茲擇要簡述如下：

---

515 參見 NADPO, About us, at: http://nadpo.org.uk//about.php (2014/10/20 瀏覽).
516 NADPO, News, at: http://nadpo.org.uk//news.php (2014/10/20 瀏覽).
517 NADPO, Events, at: http://nadpo.org.uk//events.php (2014/10/20 瀏覽).
518 此部分須付費加入該組織成為會員始得登入特定網頁瀏覽。
519 DPA 1998, s. 51(3).
520 DPA 1998, s. 51(4).
521 DPA 1998, s. 52A(1).
522 DPA 1998, s. 52A(3).
523參見 ICO, Guidance index: data protection, privacy and electronic communications, at: http://ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications (2014/06/27 瀏覽).

以中小企業如何遵循個資保護之一般性指導原則為例，ICO 訂有‘AQuick “How to Comply”Checklist’，以淺顯易懂之查核表 (checklist)模式列出一系列問題，如業者是否知悉取得個資之目的為何；個資主體是否知悉其個資已被業者取得；業者取得之個資是否被安全保管；業者是否確信個資正確性；業者是否對員工實施個資保護之教育訓練；業者是否知悉在何種況下得將個資分享於第三人等，促使業者自我檢視是否有違反 DPA 1998 相關規範之風險[524]。

再以防治個資侵害 (data breach) 之員工教育訓練為例，針對資源有限之中小企業，ICO 訂有 ‘Training checklist for small and medium sized organisations’，分別就「保護個資安全」、「滿足客戶合理期待」、「透過電話揭露客戶個資」、「對 ICO 之通報義務」、「如何處理個資主體對其個資之請求」五個項目列出參考指標。以保護個資安全為例，ICO 列舉以下重點，例如：

- ˙員工是否知道應注意經常更換電腦密碼，且不對外洩露；
- ˙離開座位時鎖住或登出電腦；
- ˙將敏感文件以碎紙機銷毀；
- ˙防範電腦病毒攻擊，不開啟不明電子郵件與附件，不瀏覽可疑網站；
- ˙訪客進出辦公區域應登記並由員工陪同；
- ˙個資帶離辦公區域時應行加密；
- ˙將資料定期備份等。

以上為業者教育訓練員工如何防止個資外洩之重點參考項目[525]。

針對個資分享 (data sharing)，ICO 訂有詳盡之‘Data sharing code of practice’供個資控制者參考。此準則本身不具備法律效力，僅為 ICO 對於 DPA 1998 抽象法條規範之解釋與適用之指引，並作為個資控制者如何遵循關於個資分享規範之建議

[524] ICO, A Quick ‘How to Comply’ Checklist, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/getting_it_right_-_how_to_comply_checklist.ashx (2014/10/20 瀏覽).

[525] ICO, Training checklist for small and medium sized organisations, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/TRAININGCHECKLIST_V1_WEB_VERSION.ashx (2014/10/20 瀏覽).

[526]。此準則包含以下部分：

- ˙個資分享之定義與類型：如組織內分享與組織外對第三方分享；例行系統性分享 (systematic data sharing)；非常態性分享 (ad hoc or 'one-off' data sharing)[527]；
- ˙從事個資分享時應考慮之因素：如分享之目的，分享之個資類型，分享之對象，如何分享，個資分享之可能風險等[528]；
- ˙個資分享之合法要件：如針對一般個資之同意，與敏感性個資之明示同意；

● 或為履行個資主體為當事人之契約；或個資控制者為遵守法定義務；或為保障個資主體關於生命或健康之重要利益[529]；

- ˙個資分享的公正性與透明性 (fairness and transparency)：如關於個資分享的隱私權通告 (privacy notice)[530]；個資分享流程所涉及之個資安全 (security) 維護，包括實體安全 (physical security)措施之考量因素 (如門禁管制，資料銷毀)，與安全技術 (technical security) 措施 (如個資加密技術，個資存取等級限制)[531]；
- ˙個資分享協議重要內容與責任歸屬[532]；
- ˙締結個資分享協議前的隱私衝擊評估 (privacy impact assessment)：包括確認雙方處理個資之系統格式相容性，確認所分享個資之正確性，就分享個資之留存時間與刪除達成協議等[533]；
- ˙應避免之不當作為：如對個資主體隱匿個資分享之意圖，分享過量

[526] ICO, Data sharing code of practice, p.8, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx (2014/10/20 瀏覽).
[527] Ibid, p.9-10.
[528] Ibid, p.14-15.
[529] Ibid, p.15-16.
[530] Ibid, p.17-18.
[531] Ibid, p.23-25.
[532] Ibid, p.26.
[533] Ibid, p.27-29.

(excessive) 或不相關 (irrelevant)個資等[534]

此準則並分別對例行系統性個資分享與非常態性分享設計簡明之檢核表供個資分享雙方參考[535]。並於附件三列舉關於個資分享之各種假設案例與因應之道。如零售業者合作建立素行不良之離職員工資料庫，以便在未來聘僱過程中檢核求職者素行，此時業者應盡到告知義務，即告知員工其若因素行不良遭解聘，該等事由將記錄至此資料庫中；員工亦有權檢視該等紀錄之正確性，並要求更正或刪除，或要求註明其對於該等記錄內容之不同意[536]。

針對 2003 Regulations 架構下，關於利用電信網路從事個資之蒐集、處理與利用，ICO 亦制定有 'The Guide to Privacy and electronic communications'[537]，提供詳盡的遵循指引。此指導原則分為二大部份，第一部分以 Q&A 方式說明在 2003 Regulations 規範下，個資控制者利用不同型態之電信通訊模式，如電話、傳真、電子郵件從事行銷時，應注意之個資保護規範與義務。第二部分則就 2003 Regulations 之其餘規範加以釋疑，例如個資侵害事件之通報義務；cookie、流量資料、位置資料等之利用條件與例外情形；電信用戶要求帳單不附通話明細之權利；電信事業者提供用戶隱藏發話方或受話方電話號碼之機制；用戶要求追查騷擾電話之權利；用戶電話或傳真號碼，電子郵件地址收錄於電信事業者製作之目錄之條件等等。

2、 個資保護自律團體之設置

英國 DPA 1998、2003 Regulations 與 2011 Regulations 均未明文規範關於個資保護自律團體之設置事宜。惟民間仍自發性成立如上述 NADPO 之組織。

3、 個資保護標章制度

關於個人資料與隱私保護，英國標準協會 (The British Standards Institution; 以下稱 BSI) 於 2009 年制訂了 BS10012：2009 個人資訊管理系統 (personal infornation management system; PIMS; 以下稱 BS10012)，設定公私部門機構處理個人資料之

534 Ibid, p.35.
535 Ibid, p.46-47.
536 Ibid, p.52-58.
537 ICO, The Guide to Privacy and electronic communications, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Privacy_and_electronic/Practical_application/the-guide-to-privacy-and-electronic-communications.pdf (2014/10/20 瀏覽).

自律標準[538]。要達到 BS10012 之自律標準，不論是公務或非公務部門，均應滿足以下要求，例如設有管理個人資料保護之專責單位；對專責人員提供個資保護與風險評估之教育訓練；識別並記錄個人資料之處理利用；個資的蒐集、使用、傳遞、銷毀與保存；定義個資類別清單，清楚定義單位收集的個資範圍，釐清並界定何種資料須受保護，以及個人資料保護之層級；處理資料主體行使個資權益之請求；對第三方揭露與轉包處理個資之控管等等[539]。

二、他律監督管理機制

英國為符合 1995 年歐盟個資保護指令（Directive 95/46/EC）第 6 章第 28 條 1 項關於「各會員國應設置獨立行使職權之個資保護監督機關」之要求，依據相關規範，設立 ICO 作為個資保護之獨立主管監督機關。ICO 前身為 Data Protection Act 1984 下設置之 Data Protection Registrar，於 2000 年隨著 DPA 1998 生效，改稱為 Data Protection Commissioner, 2001 年因應 Freedom of Information Act 將政府資訊公開相關業務併入其職掌範圍，乃再度更名為現今名稱[540]。關於 ICO 機關首長、任期、人員組織、預算等規範於 DPA 1998 附表 5 (Schedule 5)。由於 DPA 1998 第 6 條直接明文創設 Information Commissioner 的職位[541]，復於附表 5 明訂 Information Commissioner 有權任命至多二位副手 (Deputy Commissioners) 以及其他官員與職員 (officers and staff)[542]，因此 ICO 應係採首長制而非委員會合議制。其組織架構可參見 ICO 官網[543] (二位 Deputy Commissioners 中，一位負責政府資訊公開相關業務 (Director, freedom of information)，另一位負責個資保護相關業務 (Director, data protection)，另外有一位副執行長 (Deputy Chief Executive Officer) 負責行政管理)。

關於 DPA 1998 之監督對象，依據 DPA 1998 之定義，個人資料之定義包括「公

538 參見鄭伊雯，植基於 ISO27001 建立符合 BS10012 之個人資訊自我評鑑模式，中原大學碩士論文，2012 年 7 月，頁 21。

539 參見 BSI, BS10012：2009 Essential, at: http://www.bsigroup.tw/upload/Training/2011_web_document/PIMS%20Ess.pdfhttp://www.bsigroup.tw/upload/Training/2011_web_document/PIMS%20Ess.pdf (2014/11/08 瀏覽).

540 ICO, History of the ICO, at: http://ico.org.uk/about_us/our_organisation/history (2014/06/15 瀏覽).

541 DPA 1998, s. 6(1), (2).

542 DPA 1998, Schedule 5, 4(1).

543 ICO, Organisational structure, at: http://ico.org.uk/about_us/our_organisation/~/media/documents/library/Corporate/Practical_application/icoorganisationalchartpdf.pdf(2014/11/03 瀏覽).

務機關」 (public authority) 持有之足以辨識個人之資料[544]，而作為本法規範對象之個資控制者，係指個別或與他人共同決定個資處理之目的與方式之人[545]，依據 ICO 發布之 The Guide to Data Protection 就此進一步解釋，個資控制者必須是依據英國法律所承認之「人」，包括自然人與法人，且包含政府機關在內[546]。故 DPA 1998 規範之對象包含公務機關與非公務機關。

關於 ICO 主要職權，茲分述如下：

1、 執行通知之作成

依 DPA 1998 相關規範，經 ICO 認定個資控制者有違反個資保護原則情事者[547]，ICO 得對其發出「執行通知」(enforcement notice)，要求其為下列行為以期遵守個資保護原則[548]：

(a) 於通知期限內採取通知所定特定行為，或於通知期限屆至後避免為通知所定特定行為；或

(b) 於通知期限屆至後，避免為個資之蒐集、處理與利用。

執行通知之記載事項應包括：指明當事人被 ICO 認定違反之特定個資保護原則，以及當事人依 DPA 1998 第 48 條向法院資訊專門法庭上訴之權利[549]。ICO 決定是否發出執行通知時，應考量違反個資保護原則之事例是否已造成或可能造成任何人之損害[550]。執行通知做出後，若 ICO 認定「對於個資保護原則之遵循」，當事人已無必要遵守該執行通知之一部或全部，ICO 得以書面通知當事人取消或變更該執行通知[551]；當事人亦得主張因情勢變更，「關於個資保護原則之遵循」，當事人已無必要遵守該執行通知之一部或全部，請求 ICO 取消或變更該執行通知

---

544 DPA 1998, s. 1(1), definition of "data" and "personal data".

545 DPA 1998, s. 1(1), definition of "data controller".

546 ICO, The Guide to Data Protection, p.26-27, at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf (2014/11/03 瀏覽).

547 依據 2003 Regulation, Schedule 1, 1(a)之修訂條文，個資控制者被改稱為個人 (person)，個資保護原則改稱為要件 (requirements)。為避免混淆並求用語之前後一致，本文仍沿用舊稱。

548 DPA 1998, s. 40(1)(a), (b).

549 DPA 1998, s. 40(6).

550 DPA 1998, s. 40(2).

551 DPA 1998, s. 41(1).

[552] 。

2、 資訊通知之作成

英國嗣後制定 The Privacy and Electronic Communications (EC Directive) Regulations 2003(以下稱 2003 Regulations) 修訂 DPA 1998 第 43 條相關規範，允許 ICO 基於「合理取得資訊以認定當事人是否遵守個資保護原則」之需要，得對於該當事人作出「資訊通知」(information notice)，要求當事人依通知時限將「遵循特定個資保護原則與否」之相關資訊提交 ICO[553]。此資訊通知應包含「特定資訊與當事人是否遵守特定個資保護原則之認定有關」之聲明與相關理由[554]。

依 DPA 1998, 不遵守上開執行通知或資訊通知，或在遵循上開執行通知或資訊通知時故意或因重大過失為不實聲明者，構成刑事犯罪行為[555]。

3、 第三人資訊通知之作成

英國晚近復制定 The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (以下稱 2011Regulations) 對 2003 Regulations 增訂相關規範，賦予 ICO 作出「第三人資訊通知」(third party information notice) 之權限[556]。透過第三人資訊通知，ICO 得要求業者提出「第三人使用電信網路或服務」之相關資訊，若該資訊係就調查任何人是否遵循 2003 Regulations 所必要[557]。第三人資訊通知應記載下列事項[558]：

(a) 被要求提供之資訊；

(b) 此資訊應以何種形式提供；

(c) 提供此資訊之期限；以及

(d) 對此通知依法得上訴之權利。

---

[552] DPA 1998, s. 41(2).
[553] 2003 Regulations, Schedule 1, 4.(a)修訂 DPA 1998, s. 43.(1).
[554] 2003 Regulations, Schedule 1, 4.(a)修訂 DPA 1998, s. 43.(2).
[555] DPA 1998, s. 47(1), (2).
[556] 2011 Regulations, Regulation 12 增訂 2003 Regulations, Regulation 31A(1).
[557] 2011 Regulations, Regulation 12 增訂 2003 Regulations, Regulation 31A(2), (3).
[558] 2011 Regulations, Regulation 12 增訂 2003 Regulations, Regulation 31A(4).

在緊急狀況下，ICO 得於第三人資訊通知加註「緊急個案」之聲明並載明理由；在緊急個案中，當事人應有至少 7 日之期間以提供被要求之資訊[559]。當事人對第三人資訊通知不服者有權提起上訴[560]；在上訴裁決作成或上訴撤回以前，當事人無須提交被要求提供之資訊[561]。

4、 場所進入與檢視權

依據 DPA 1998 附表 9 (Schedule 9)規定，為了調查個資控制者是否違反本法下的任何個資保護原則，或是否觸犯本法所訂之犯罪行為，ICO 得向地區法院法官聲請令狀 (warrant)[562]，以使 ICO 有權進入(enter)特定場所 (premises) 並搜索(search)之；並得檢視(inspect)、扣押(seize) 該場所內相關物品，並要求該場所內人員配合說明相關事項[563]。

5、 一般個資違反事件與個資侵犯事件之行政罰鍰

依據 DPA 1998 規範，若 ICO 認定個資控制者有嚴重違反本法所料個資保護原則之情事，且此等違反可能造成實質損害 (substantial damage)，而個資控制者故意違反或明知或可得而知 (knew or ought to have known) 有可能違反且此等違反可能造成實質損害，而未採取合理措施以預防此等違反者，ICO 得對個資控制者作出罰鍰通知 (monetary penalty notice)[564]。唯在發出罰鍰通知前，必須先對個資控制者作出關於可能之後續罰鍰之意向通知 (notice of intent)[565]。此意向通知必須載明當事人得於特定期限內針對可能之後續罰鍰提出書面陳述 (written representations)[566]。在當事人得為書面陳述期間屆滿之前，ICO 不得作出罰鍰通知[567]。當事人收到罰鍰通知後得向法院資訊專門法庭提起上訴[568]。

2011 Regulations 將公共電信服務提供者納入 ICO 之監督權限範圍，明文規定：

---

559 2011 Regulations, Regulation 12 增訂 2003 Regulations, Regulation 31A(6), (7).
560 2011 Regulations, Regulation 12 增訂 2003 Regulations, Regulation 31B(1).
561 2011 Regulations, Regulation 12 增訂 2003 Regulations, Regulation 31A(5).
562 DPA 1998, Schedule 9, 1(1).
563 DPA 1998, Schedule 9, 1(3).
564 DPA 1998, s. 55A(1), (2), (3).
565 DPA 1998, s. 55B(1), (2).
566 DPA 1998, s. 55B(3)(a).
567 DPA 1998, s. 55B(4).
568 DPA 1998, s. 55B(5).

ICO 為確保服務安全，得監督業者採取之相關措施[569]。此外 2011 Regulations 就 ICO 對於個資侵犯事件之監督權限[570]，增訂以下規定：為使 ICO 驗證業者是否確實遵守相關規範，業者應建置個資侵犯資料庫 (inventory) 並充分保存以下資料[571]：

(a) 個資侵犯事件之相關事證；

(b) 個資侵犯事件之影響；以及

(c) 採取之補救措施。

若業者未遵守個資侵犯事件通報義務之相關規範，ICO 有權對業者作出 1000 英鎊定額罰鍰通知 (penalty notice)[572]。唯 ICO 作出罰鍰通知以前，必須先對當事人發出意向通知[573]。此意向通知必須記載特定事項，包括：當事人名稱、地址；系爭個資侵犯事件之性質；載明後續罰鍰金額；告知當事人免於後續罰鍰之機會；載明 ICO 得作出後續罰鍰之日期；並載明自意向通知送達後 21 日內當事人得針對後續罰鍰提出書面陳述[574]。當事人得於收受意向通知後 21 日內向 ICO 繳付 800 英鎊以免除後續罰鍰之責任[575]。在上開意向通知所載書面陳述期間消滅以前，ICO 不得作出後續罰鍰通知[576]。當事人不服罰鍰者，得向法院資訊專門法庭提出上訴[577]。

[569] 2011 Regulations, Regulation 4(2)增訂 2003 Regulations, Regulation 5(6).
[570] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5B.
[571] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5A(8).
[572] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5C(1), (2).
[573] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5C(3).
[574] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5C(4)(a)~(f).
[575] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5C(5).
[576] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5C(6).
[577] 2011 Regulations, Regulation 5 增訂 2003 Regulations, Regulation 5C(8).

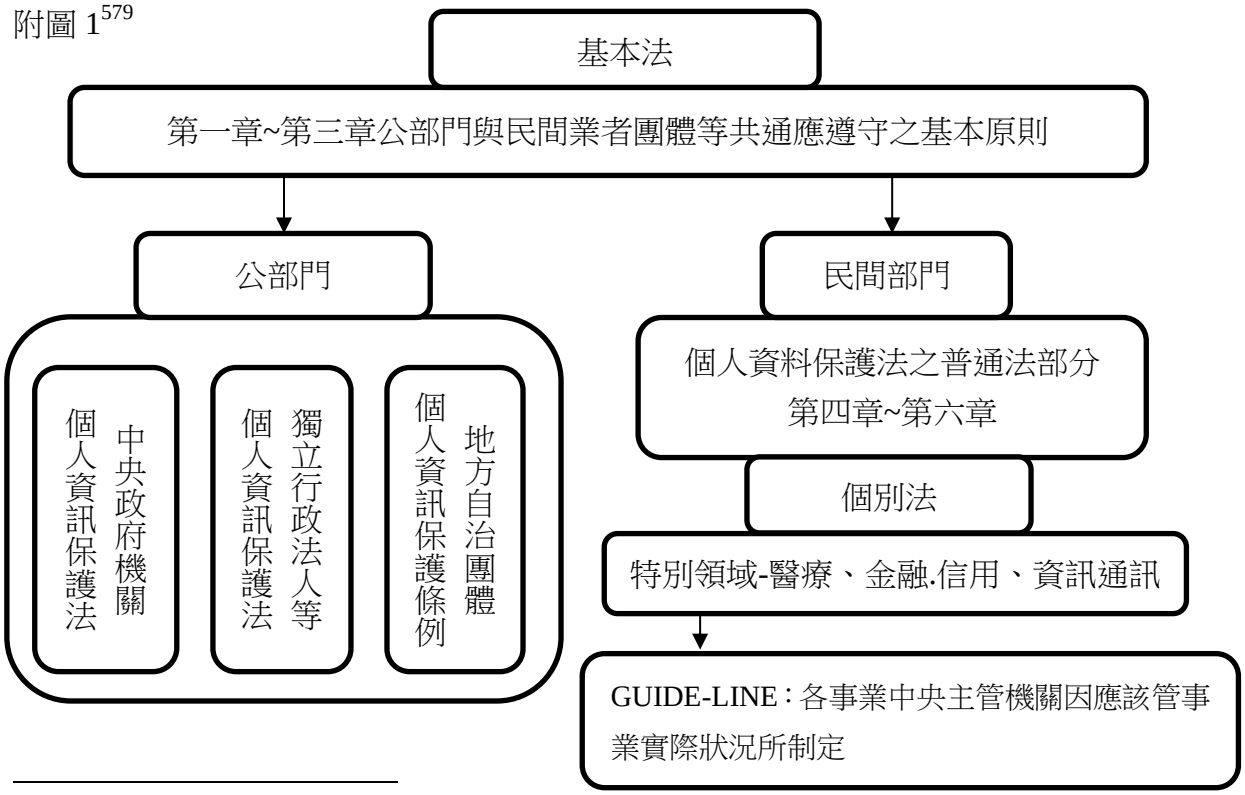
第四節 日本

一、自律之機制

(一) GL 之制定與定位

於 2005 年制定個資法時，因考量民間企業等多因經營事業之需，基於契約或準契約關係而蒐集、利用個資，原屬私法自治之領域，性質上甚至僅為組織內部處理個資，如行政機關過度干涉將涉及營業自由之問題，亦可能牴觸表現自由（例如傳播業、出版業等），故僅以基本法確立民間業者處理個資之總則性規定，在立此基礎上，分別由主管之行政機關與民間業者協議後，依各事業領域處理個資之性質訂出符合實際所需之指導規範[578]。

附圖 1[579]



[578]田島泰彦、三宅弘編，個人情報保護法，頁 4，明石書店，2003 年。宇賀克也，「個人情報保護法の逐条解説」（2 版），2005 年，頁 18。

[579]本圖改修自岡村久道，個人情報保護法，頁 129。

如上圖所示，日本對民間業者規範以尊重各業者之自律、自主為原則[580]。其個資法第四章以下對民間業者蒐集處理、利用個資，僅於必要最小限度內作總則性之共通最低標準規範[581]；於 2004 年 4 月公佈施行個資法後，其第八條規定各種事業主管機關針對其該管業者，依其事業領域實際所需，須制定或修正有關處理個資之指導原則－Guide Line(GL)，至 2014 年 6 月各省廳合計共有 27 個業種領域 40 個 GL[582]被制定公佈。而有關電信通訊業者之 GL，已於本計畫報告書第三章第四節說明。

(二) 認定個人資訊保護團體之設置

如前述日本個資法立法目的希望以行政指導輔導業者以自律方式，自發性合法、適當處理個資；為推動業者自律並落實本法立法宗旨，本法特別設計「認定個人資訊保護團體」之制度，由各業界、業者自主組織之民間公益法人團體，於經中央事業主管機關許可認定後，得依其所屬業界處理個資之種類、方式，以中央事業主管機關所頒佈之 GL 為藍本，訂立更具體、詳細之個資處理規則「個人資訊保護指針」供其團體成員共同遵守；此外於業者與本人間為個資處理發生爭執時得介入斡旋，擔任裁判外紛爭處理之任務；因此本法第四章第二節設置「以民間團體推進個人資訊保護」之規定，建構以團體力量確保其成員適當處理個資為業務目的之民間團體認定制度，期於建立社會對其信賴後，有助於民間團體之自律確實發揮作用。

1、 取得認定

申請認定個人資訊保護團體(下稱「個資保護團體」)依本節第 41 條第 1 項，可分為二種類型之團體，一類為以處理個資業者所屬業界為單位(例如銀行業界)所設立之業界團體、連合會等(例如全國銀行個人情報保護協議會[583])，通常由原已存立業界團體本身提出申請受許可認定後成為「認定個人資訊保護團體」，而其原

[580]藤原靜雄，「逐條個人情保護法」，頁 18，弘文堂，平成 15 年。見平成 16 年（2006 年）4 月 2 日內閣會議決議公佈之「個人情報の保護に関する基本方針」１、（２）②。

[581]田島泰彦編，「個人情報保護法と人権」，明石書店，2002 年，頁 136。藤原靜雄，個人情報保護法に関する制度の整備ーその成果と課題，ジュリスト No.1287，2005 年 1 月，頁 2。

[582]內閣府 HP：http://www.cao.go.jp/seikatsu/kojin/(最後瀏覽日：2014 年 6 月 25 日)。

[583] 為平成 17 年（2005 年）4 月 15 日，以銀行、長期信用銀行、銀行控股公司、全國各地銀行協會及全國銀行協會為會員，受主管機關認定所成立之個人資訊保護團體，至平成 18 年（2006 年）4 月 1 日，共有 247 個會員。

構成會員業者即為其業務對象。另一類為橫跨各業界訂立出個資保護共同規則，並對符合其標準之業者授與隱私保護認證標章之團體(例如財團法人日本情報處理開發協會，JIPDEC，下稱 JIPDEC)，其成員為同意成為其認定業務對象之個資處理業者。申請取得認定為個資保護團體，依本節第 37 條規定並不一定須具有法人資格，僅設有代表人或管理人之非法人團體亦得申請認定。

欲設立認定個資保護團體者，應依政令所定事項，向中央事業主管機關申請；該管機關則依本節第三九條所列基準進行審查申請者是否符合甲、訂有適當且確實進行其業務所必要之施行方法；乙、具有適當且確實進行其業務之足夠知識、能力與管理之基礎； 丙、於進行認定業務以外之其他業務時，不因此而造成認定業務有不公平之虞等三要件，如確認滿足上述三項要件時，即為許可之認定，並予以公告。

2、 業務

取得許可認定之個資保護團體，依本節第 37 條第 1 項規定得進行下列三項業務：甲、處理有關其會員或構成員業者在處理個資上發生之申訴事件；乙、提供有助於會員業者適當處理個資之相關資訊；丙、除前二項外，其他協助會員業者適當處理個資之必要業務(例如提供研習、收集資料、辦理宣導活動等)。

關於上開甲、之處理申訴處理業務之進行，同節第 42 條更具體規定，資訊本人對其會員業者處理個資有不滿而提出申訴時，該當個資保護團體須因應其訴求，為必要之建議；並於調查申訴事實之同時，將申訴內容通知該當會員業者，要求其迅速解決。又個資保護團體為解決前述申訴事件於必要時，得對該當會員業者要求提出文書或口頭說明或資料；而該當業者對上開要求，如無正當理由不得拒絕。依此規定個資保護團體有義務受理申訴並迅速處理。又為確保其有效處理申訴事件，本條規定再賦予其對會員業者有要求說明之權及資料提出請求權。

此外，為讓個資保護團體有效幫助其會員業者能確實遵守本法規範，適當處理利用個資，發揮其團體自律機能，本節第 43 條規定：個資保護團體應依本法規定意旨，努力作成並公表包含特定利用目的、安全管理措施、本人申訴處理程序等事項之「個人資訊保護指針」；並對團體會員業者進行遵守指針所必要之指導、勸告及其他輔助措施。此指針之性質相當於該業者團體處理個資之 GL，讓同屬相同業界之業者有一具有明確性、一致性適當處理個資之規範，徹底發揮團體自律

之力量。

3、 信賴度之提高

又為提高國民對個資保護團體之信賴，充分發揮其功能，本節第 44 條至第 48 條訂有主管機關監督等相關規定。屬消極面有第 44 條規定：個資保護團體於進行認定業務時所獲知之資訊，不得供認定業務以外之目的使用。如有違反者，事業主管機關得撤銷其許可認定。第 45 條規定：其他非個資保護團體，不得使用個資保護團體名稱或可能使人誤認之名稱，以保護資訊本人或消費者，並防止惡德業者冒用名義進行非公益活動。屬積極面有第 46 條規定：事業主管機關於必要時，得對個資保護團體要求提出有關認定業務之報告;又為擔保此報告徵收權之效力，本法於第 57 條規定，如該當個資保護團體不為提出，或為虛偽報告者，將被處以三十萬元以下之罰金。除此之外有必要時，得再依第 47 條命令個資保護團體，改善認定業務施行方法、變更個資保護指針及採取其他必要措施。且於該當個資保護團體不遵從上開命令時，事業主管機關得撤銷其認定，以確保本條命令之效力。

綜上可見，日本個資法希望以團體自律、自治方式確保各個業界業者適當合法處理個資；因業者為維護自己商譽，在其所屬業界保有生存空間，就必須遵守團體之規則，否則難以獲得同業間奧援，甚至受到排擠。以讓業界自律方式，彼此互相發揮監督力量，一方面可以讓各業界依其處理個資之性質及方式，自訂出符合實際需求之處理個資具體規範；一方面亦可避免公權力過度介入業者經營自由，主管機關退居於第二線進行監督即可。日本データ通信協会，在 2005 成立「電気通信個人情報推進センター」並受至總務大臣認定為電氣通信事業領域之認定個人情報保護團體。

4、 Privacy mark 制度(下稱 P-mark 制度)：

日本最初於 1988 年制定有關個資保護法，其規範對象僅限於行政機關，而民間則委由業者自訂自律規範。其後，1995 年歐盟議會及理事會之個人資料保護指令(通稱 EU 指令) ，第 32 條規定要求各加盟國於三年內將個人資料保護完成法制化，第 25 條規定加盟國對非加盟國移轉個資時，限於該非加盟國對個資之保護已具備十分水準者，始得為之。為世界貿易大國之日本為因應此一要求，當時之通商產業省(即現今經濟產業省)於 1997 年 3 月，依 OECD 八大原則及 EU 指令訂立

有關民間業者處理個資之 GL；更為促進業者導入遵守及擔保其實效性，當時所採政策之一即由前述財團法人日本資訊處理開發協會(JIPDEC)於 1998 年 4 月創設 P-mark 制度。

所謂 P-mark 制度係指處理個資業者對個資之處理方式及程序，經評價被認定符合日本工業規格 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(通稱個資保護 JIS)者，將由 JIPDEC 發給 P-mark 之認證標章供其使用於事業活動上[584]。一般社會大眾可依此認證標章判斷該當業者處理個資已符合 JIS 所定透明化、安全性、正確性之標準，消除其對業者之不信任感，亦可取得事業往來對象之信賴。又依此制度業者於取得認證標章後，關於個資處理有消費者諮詢或申訴時，JIPDEC 得聽取該當業者報告或調查其事實，再據其結果給予改善建議，如業者未遵從建議改善者，亦得撤銷其認證標章，係為具有繼續性監督效力之制度。

此一制度運作至今取得認證標章之業者有一萬三千九百四十五家[585]，其中運輸通信業者有六百三十五家，且在許多政府採購案或招標案之合約上載明投標廠商須取得 P-mark 之認證[586]；此政策讓業者更有意願及動力取得認證，間接促使業者積極遵守法律、建立合法安全管理、利用個資之體制，與行政機關之監督及業者團體之自律機制，共同建構完整保護個資之安全網。上所述「電気通信個人情報推進センター」於 2006 年 6 月亦開始進行 P-mark 認定業務。

如前述日本個資法考量業者之營業自由與為能符合各業界處理個資之多樣性，故以行政指導方式，輔助業者自主、自律合法處理個資為最終立法目的，自始即未授權行政主管機關以公權力作強力之行政監督。

二、他律之監督機制：主務大臣制

日本之中央事業主管機關為達成本法保護當事人權利、利益之目的，亦得對「個資處理業者」、「認定個資保護團體」，依本法規定行使一定監督權限，但為避

[584]関本貢、プライバシーマークー制の運用状況、法律のひろば、2003 年 9 月、42 頁以下。亦可參酌 http://privacymark jp/網站。另外，2008 年 3 月 10 日行政院科技顧問組舉辦「台日資安防護交流研討會」中之「日本の情報セキュリティ促進政策―プライバシーマークー制度の紹介」亦有詳細說明。プライバシーマーク付与事業者一覧，http://privacymark.jp/certification_info/list/clist.html

[585] プライバシーマーク付与事業者一覧，http://privacymark.jp/certification_info/list/clist.html，造訪日 2015 年 3 月 8 日。

[586]藤原静雄、個人情報保護に関する制度の整備、ジュリスト，N0.1287，2005 年 4 月，8 頁。

免主管行政機關以直接廣泛之監督權限，不當干涉業者之營業自由[587]，與本法期許業者自律之立法本意有所背離，故其監督權限行使方式，乃由緩而嚴之漸進式進行[588]，留給業者改善之機會與空間；並於相關條文中均設有於業者履行本法定義務之「必要範圍內」，或「為保護個人權利利益有必要時」，為權限行使之要件，藉以確保行政機關採謙抑、自制之立場進行監督。其監督權限行使方式如下：

(一) 報告之提出

中央事業主管機關於監督民間業者履行法定義務之必要限度內，依個資法第 22 條得要求該當業者提出有關個資處理之報告。此為主管機關對業者行使「行政調查權」之根據，但權限僅為要求提出報告而不及於現場之調查。因本條所定要件為法定義務「履行必要限度內」，並不以業者有違法行為為要件。雖本法第四章第一節所定業者應遵守之義務也包含有業者之努力義務(例如第 19 條應努力保持資料內容正確且最新性之義務)而非全強制性法定義務，然中央事業主管機關認為確保該等義務之履行而有必要時，仍得依本條要求該當業者提出報告。而此「提出報告之要求」性質上為行政處分，業者得對其聲明不服或提起行政訴訟請求救濟[589]。如業者怠於提出報告，或提出虛假之報告書，依同法第 57 條規定，得處以 30 萬元以下罰金。

(二) 建議

中央事業主管機關於監督民間業者履行法定義務之必要限度內，得對業者提出有關處理個資之建議。所謂「建議」性質上屬行政法上之行政指導，希望藉以幫助業者先行自主性改善個資處理上之缺失以防止問題擴大，而未具有法之強制拘束力。

(三) 勸告

中央事業主管機關對處理個資業者要求提出報告，並給予建議而仍無法解決或改善該當業者不當行為時，最終仍須具有強制力之行政命令，始足以有效監督業者遵守法定義務。

[587]岡村久道，前揭 579，頁 302。
[588]宇賀克也，個人情報保護法の逐条解説(第 3 版)，有斐閣，2009 年 4 月，頁 163。
[589]園部逸夫編，個人情報保護法の解說，ぎょうせい，2003 年，頁 38、187。

事業主管機關依本條對業者進行勸告之要件有二：一為業者有違反本法規範之行為者，主要有違反本法第 16 條為特定利用目的外之利用、第 17 條以不正當手段取得個資、第 18 條未預先公布或通知利用目的、第 20 條未對個資之安全管理為必要且適當之措施、第 21 條未對處理個資之從業人員為必要且適當之監督、第 22 條未對受託處理個資之受託人為個資安全管理上必要且適當之監督、第 23 條未得當事人同意將個資提供給第三人、第 24 條未依法公告保有個資之相關事項、第 25 條拒絕對當事人提供閱覽該當保有個資、第 26 條未依法為該當個資之停止利用等。而第 15 條利用目的之特定，因其性質屬於業者內部管理行為，尚不及於實際利用階段，故排除於本條適用範圍外[590]。第二要件為：認為有保護當事人權利利益必要時，相較於前條之建議，其要件更為嚴格；此乃因建議為單純之行政指導，而勸告雖同為行政指導，但卻為命令之前置程序，亦即對接受勸告而無當理由不遵從改善之業者，該管事業主管機關得進一步以行政命令要求業者改善，因此其要件須更為嚴謹。

(四) 下命處分

如前述業者於受到主管行政機關勸告後,無正當理由未進行任何改善措施者，依本法第 34 條 2 項，主管機關認為對個人權利利益有迫切侵害時，得命令該當業者依從勸告進行改善。因此命令為具有法律強制力之行政命令，事業主管機關應更謹慎為之，故本項中再增加「認為對個人權利利益有迫切之侵害」之要件；且此命令應不得逾越先行勸告之內容，即事業主管機關不得為更高強度之命令。如業者仍違反命令時，依本法第 56 條得處 6 個月以下拘役或 30 萬元以下罰金。

綜上所述，事業主管機關對業者之監督，通常係以要求提出報告→建議→勸告→命令之順序，循序漸進，先為柔性勸導，無效後再繼以具強制力之行政命令；並在實質及程序要件上配合作適度之調整，作用在節制行政機關過度介入干涉業者處理個資之事務[591]。

(五) 緊急措施

同前 34 條 3 項規定：個資處理業者違反本法第 16 條為特定目的外之利用、

[590]藤原靜雄，前揭 586，頁 115 。
[591]宇賀克也，前揭 588，頁 156。

違反第 17 條以不正當手段取得個資、違反第 20 條未對個資安全管理為必要且適當之措施、違反第 21 條未對處理個資之從業人員為必要且適當之監督、違反第 22 條未對受託處理個資之受託人為個資安全管理上必要且適當之監督、違反第 23 條 1 項未得本人同意將個人資料提供給第三人時，因有損害個人重大權利利益之事實，認為有採取緊急措施之必要者，事業主管機關得對該當業者，命令其中止違法行為或採取必要之改善措施。此項規定係前項勸告前置主義之例外，事業主管機關得直接對該當業者發佈緊急措施，故特別限定其適用對象；僅針對有違反重要法定義務之行為，並已造成個人重大權利利益損害之業者，為終止損害繼續發生而有立即採取必要措施時，始有本項之適用。如業者違反本項緊急措施時，依本法第 56 條得處 6 個月以下拘役或 30 萬元以下罰金。

綜上，日本採「主務大臣制」，對民間部門以行政指導乃至下命處分作彈性監督，非如歐盟等設置獨立機關以行使監督權限。

但應注意的是，獨立監督機關之設置一直為日本自個資法立法時，以及之後政府或學者專家所檢討之課題。故日本於 2013 年 5 月 26 日定位為個資法特別法之「行政程序中為識別特定個人之編號利用法」（行政手続における特定の個人を識別するための番号の利用等に関する法律，一般日本稱為「番號法」(マイナンバー法)，以下均稱以個人編號法） 完成立法，除少數條文公布後即施行外，大多數預定於一年半至三年內施行。而藉個人編號制度立法，先對社會保障、稅務及災難救助領域之蒐集利用個資事務，建立具獨立性「個資保護委員會」監督機關，對政府機關及施行關連業務之民間事業團體所為蒐集、處理或利用個資行為進行監督，以此為基礎，將來再依其施行狀況逐步擴展至其他領域之個資保護上。從而，日本亦已開始建置獨立監督機關，解決其長期以來被指摘之缺失。

三、個資保護委員會

以下就日本因應個人編號法施行所新設置之監督機關－特定個人情報保護委員會(下稱「保護委員會」)之定位、組織及權限等分別說明之。

(一)、定位－內閣府外局之委員會

因保護委員會為監督包含中央級行政機關有關特定個資之處理及利用，且必須具有獨立性，在參考如掌理警察行政之國家公安委員會及公正取引委員會(相當於我國公平交易委員會)等，同為須具有高度獨立性、位於各省(相當於我國二級機

關之部會)之上，屬內閣府設置法第 64 條 所定之內閣府委員會設置方式；個人編號法立法時，於第 36 條將保護委員會定位為依內閣府設置法第 49 條所設之內閣府外局機關，由內閣總理大臣(首相)管轄，以保障其不受其他行政機關之干涉及壓力下，得有獨立行使監督之權限。同時又因有關保護個資監督機關得對監督對象行使指導、建議、勸告、命令、檢查等強力權限，須作高度專業之法律及資安技術判斷，由委員會組織方式進行各方意見之交換及討論係較理想可達成任務之運作方式。

(二)、組織

1、保護委員會之組成

依個人編號法第 40 條規定，保護委員會由委員長及 6 名委員共 7 人組成；其中 3 人為兼任委員；委員及委員長須經參、眾議院同意，由總理大臣任命，以確保政治之中立性及受民主之統制。委員中須有資訊處理技術、社會保障制度或稅制之學識經驗者；此外，尚應包括對證券、保險等民間企業實務運作具有充分知識及經驗者，以及連合組織(為地方自治法第 263 條之三第 1 項所稱如律師公會、經濟連合會等)所推薦者。期能結合不同領域之學者或專家以進行會議，充分討論後依決議方式作出適當之決定。

2、任期與身分保障

委員及委員長任期，依個人編號法第 41 條規定為 5 年，且得連任。為確保保護委員會持中立立場、獨立行使職權，並於第 42 條規定在任期中，委員除有①受破產程序開始決定；②違反本法而被處以刑罰；③受有期徒刑宣告及④被委員會認定身心障礙無法執行職務，或有違反職務上義務及其他不適合為委員長或委員之行為者，不得違反本人意思予以免職。

(三)、業務及職權

1、業務

個人編號法第 38 條揭示委員會所掌業務為，①監督或監視有關特定個資之處理及對申訴之案件進行斡旋；②特定個資保護之評價：包括保護評價指針之作成、公表，及對評價書之審查、承認；③有關特定個資保護之宣導或研習活動；④為施行前揭事務所為必要之調查，如 EU 保護規則草案之動向、各國外有關個資保護

制度；⑤有關所掌事務之國際合作，如參加國際資訊官會議，以及與國外相關機構之聯繫等；⑥其他法令所定屬於保護委員會之事務。

2、職務之執行

為完成上述監督等業務，個人編號法規定保護委員會得為下列職務之執行：（1）指導及建議：保護委員會得對有關特定個資處理上必要之指導及建議。（2）勸告及命令：個人編號法第 51 條規定，保護委員會對違反特定個資處理法令之行為者，為確保正當處理特定個資而認為有必要時，得定期限勸告其採取改正或中止該當違法行為之必要措施。接受勸告者無正當理由而未採取勸告措施時，得定期限命令其採取有關勸告之措施。對違反本條命令之行為人，得依同法第 73 條處以 2 年以下有期徒刑，或 50 萬圓以下罰金；（3）報告及進入檢查：依同法第 52 條規定，保護委員會得對處理特定個資者、其他關係人，要求提出有關特定個資處理之必要報告或資料。其職員並得進入該當事務所或必要場所進行質問，或檢查帳冊書類等物件。此檢查權限性質上屬行政調查，無須事前得到法院之許可。(4)意見之提出：有關政府施行政策或法令制定改善等，依同法第 55 條規定，保護委員會得對內閣總理大臣陳述意見；(5)對國會之報告：同法第 56 條規定，保護委員會每年應經由內閣總理大臣對國會報告所掌事務之處理狀況，同時公布其概要；讓人民理解保護委員會之運作狀況，藉此透明化本法之施行狀況，達到全民監督之效果。

表 4-2 特定個人資料保護委員會

層級	內閣府之局外機關，直屬總理大臣所轄。(與公平交易委員會同級)
組織方式	委員會制，由委員長一人及委員六人所組成。經國會參、眾兩院同意後，由總理大臣任命，任期五年，得連任。
職權	法明訂各委員唯獨立行使以下職權: 1、監督或監視有關機關對特定個資之處理 2、對申訴案件之斡旋 3、對政府機關或處理個資之業者進行指導、建議、勸告及下命令中止行為 4、特定個資保護之評價 5、個資保護之宣導、研習活動之舉辦 6、調查各國有關個資保護法制之發展 7、進行個資保護執行之國際合作與聯繫，參加個資保護國際會議

資料來源：本研究自行整理。

第五節 韓國

一、政府監督機制

(一) 設立個人資料保護委員會

為了有效審議與監督個人資料保護之相關內容與運作機制，韓國政府於 2011 年 9 月依據〈個人資料保護法〉第 7 條及第 8 條，成立「個人資料保護委員會」，負責審議個人資料保護基本計畫、政策、制度與法令增修等事項。個人資料保護委員會共由 15 名委員組成，其組成方式由總統指定 5 名、大法院院長指定 5 名、其餘 5 名則由國會選出；委員任期為 3 年，可連任一次；委員長由委員中之非公務員出任。個人資料保護委員會中設有專業委員會，由包含委員長在內之 5 名委員組成；同時設有 1 個事務局下轄 3 個科室，實際執行相關業務。

個人資料保護委員會的業務主要有二：「審議議決事項」及「調查研究」；審議議決事項包括：（1）擬定政府整體個人資料保護基本計畫，以及各部門之施行計畫；（2）改善個人資料保護相關政策、制度及法令；（3）調停公共機關對於個人資料之處理；（4）個人資料保護法令之解說及運用；（5）針對公共機關對個人資料侵害施政措施之勸告；（6）撰寫個人資料保護年度報告書並至國會進行報告；（7）總統、委員長及 2 名以上委員提出事項之討論；（8）其他相關法令與機關委任事項之處理。調查研究則包括：（1）個人資料之蒐集與利用、個人資料保護法等實際施行情況之調查；（2）業務目的以外之個人資料利用、提供第三人等實際運作情況之調查與分析；（3）海外個人資料保護執行體系及個人資料保護主要動向之研究；（4）個人資料保護法令與制度強化方案之研究。

在實際運作上，關於擬定個人資料保護基本計畫方面，個人資料保護委員會於 2012 年 1 月通過了「2012~2014 年個人資料保護中長期計畫」，設定了政府未來在個人資料保護之願景、目標和推動方向；2012 年 4 月，個人資料保護委員會與 46 個中央行政機關通過「2012~2013 年個人資料保護施行計畫」。

關於提高個人資料保護意識與強化相關機構之交流與合作方面，2012 年 6 月，由個人資料保護委員會、國會立法調查處和個人資料保護法學會共同舉辦「個人資料保護法立法課題學術研討會」；同時也舉辦了「個人資料保護博覽會」，該會

議是由個人資料保護委員會和保安新聞社共同舉行，會中呈現了個人資料保護學術研究成果，以及介紹個人資料保護之最新技術，2012 年 11 月，個人資料保護委員會和個人資料保護法學會共同舉辦了「個人資料保護國際學術研討會」；2013 年 10 月，個人資料保護委員會和安全行政部共同舉辦了「個人資料保護施行 2 周年紀念學術研討會」。

關於個人資料保護相關實際施行情況調查方面，個人資料保護委員會於 2011 年 10~12 月期間，共針對公共機關和民間團體，進行 3 次的個人資料保護相關義務事項履行實態基礎調查；2012 年 2 月，個人資料保護委員會針對中央與地方及共 1,198 個公共機關及其所屬機關，其施行個人資料保護法的情況進行調查；2013 年 6 月，個人資料保護委員會再次進行個人資料保護實態調查，施行對象包括 2,000 名資料主體、2,500 個公共機關及 2,000 個業者。

關於個人資料保護政策改善勸告方面，2012 年 6 月，個人資料保護委員會針對 Google 個人資訊取得方針提出糾正勸告，主要因為 Google 個人資訊取得違反韓國國內法，因而對其提出了修正意見；2012 年 11 月，放送通信委員會和安全行政部共同針對未確實管制個人資料流出之業者，提出修正措施勸告，並且課以罰金；2013 年 7 月，個人資料保護委員會針對智慧型手機個人資料處理提出修正勸告，主要要求智慧型手機在產生與貯存資料的處理(傳送)過程中，必須更普及使用者確認和阻斷手段；2013 年 1 月，個人資料保護委員會針對首爾地鐵公司地鐵車廂內監控電視（Closed-Circuit Television, Closed-Circuit Television, CCTV）運作方式提出修正勸告，除了為預防緊急情況，或是為保護乘客生命、安全及財產等必要性正常監控以外，禁止其他攝錄運作。

(二) 設立個人資料糾紛調停委員會

為了在糾紛發生時能夠迅速獲得解決，韓國政府在設立個人資料保護委員會的同時，也依據〈個人資料保護法〉第 40 條，成立「個人資料糾紛調停委員會」，負責調解個人資料相關當事人之間的紛爭事項。個人資料糾紛調停委員會由安全行政部部長委任 20 名委員組成，委員成分包括副教授級以上之教授、法官、檢察官、律師、公民社會團體、消費者團體推薦者及產業工會代表等，領域相當多元且富有專業性，專門負責接受個人資料保護相關糾紛案件之申請與調停。

在申請人與相對方接受個人資料糾紛調停委員會所做的調停決定後，再依據

調停成立情形製作成調停書。調停書的內容則依據〈個人資料保護法〉第 47 條第 5 項之規定賦予「裁判和解」(民事訴訟法上確定判決與同一效力)。如果當事人在調停成立後發生不履行已決定內容之情事，得由法院發出執行令強制執行之。

二、最新進展

韓國放送通信委員會有鑑於邇來金融、通信等產業部門之個人資料保護流出情況日益嚴重,已成為社會性議題,因此於 2014 年 3 月針對網路的個人資料保護，進行了一系列的檢討，包括：個人資料有效期間縮短與加密對象擴大、因應 IT 環境變化檢討〈資訊通信網法〉之發展方向、建立巨型資料庫（big data）指南。其中，放送通信委員會特別關注網路之身分證號碼使用限制，基本上，自 2012 年修訂〈資訊通信網法〉以來所蒐集到的身分證號碼，其有效時間在 2014 年 8 月 17 日已到期必須完全刪除，8 月 18 日以後即禁止身分證號碼之蒐集，違反者必須課以 3,000 萬韓元以下之罰鍰。目前由放送通信委員會和韓國網路振興院（KISA）負責提供中小型、微型業者（中小型：年營業額 30 億韓元以下與編制內員工 50 人以下之業者；微型：年營業額 1 億韓元以下與編制內員工 5 人以下之業者）關於身分證號碼刪除及資料庫銷毀之技術協助。

其次，關於企業之個人資料收集最小化方面，新的政策方針要求企業為了提供服務而蒐集個人資料必須將數量降至最少，個人資料同意書必須更淺顯易懂使利用者可以一目瞭然做最正確的決定，不必要的個人資料必須刪除。

三、特色

韓國之個人資料保護委員會，為直屬於總統下而獨立於其他政府機關部會外所設置者，因此可避免其他政府機關之干涉或介入而能保持其獨立性，符合歐盟指令所要求監督機關應具獨立性之要件。另外其組成之委員包含有由民間個資保護團體所推薦人、個資處理業界團體所薦舉之人及具有個資保護專業知識之人員，亦應能代表社會多元之意見，不至偏頗。最特別的是委員會之職權並非如歐盟指令所訂，包含執行監督、調查、介入紛爭協調，及處罰違法；其有関個資安全保護部分係由安全行政部主管，紛爭之解決則由個資糾紛調解委員會負責，有關個資法施行之監督則由中央行政機關，就其所管轄之領域執行並得進行裁罰；故我國法務部稱此為「分散整合式」 之監管機制。

表 4-3 韓國個人資料保護委員會之層級、組織方式及職權

層級	設置於總統之下，並獨立於其他政府部會之外
組織方式	委員制。 由總統、國會、大法院院長，各指定五人，共十五人。 任期三年，得連任一次。
職權	一、 議決、審議事項 1、 中央行政機關之個資保護計畫、個資保護之改善政策、法制。 2、 個資法之解說與運用 二、 調查研究事項 1、 個資法實施狀況之調查。 2、 國外個資法制之動向研究。 三、 撰寫個資保護施行之年度報告，並向國會提出。

資料來源：本研究自行整理。

第六節 美國

關於美國電信事業個人資料蒐集、處理、利用或分享之監理機關，主要有兩個聯邦行政機關：聯邦通訊委員會(Federal Communications Commission, FCC)及聯邦貿易委員會(Federal Trade Commission, FTC)。茲分述如下：

一、聯邦通訊委員會

聯邦通訊委員會(FCC)主要係主管及執行電信事業個人資料蒐集、處理、利用或分享之相關隱私法律及行政命令。其中，美國聯邦通訊委員會曾數度公布「用戶專屬線路資訊」相關命令及施行細則。事實上，聯邦通訊委員會制定行政命令、法規命令(rulemaking)或行政立法之正式過程，由發布「提議制定行政命令之通知」(Notice of Propsed Rulemaking[592])或「諮詢之通知」(Notice of Inquiry[593])開始。「提議制定行政命令之通知」包括要觸及議題的討論、用以解決該議題而提議之行政命令草案，以及通常也包括做為該提議行政命令草案之基礎的說明。「提議制定行政命令之通知」尋求利害當事人對於提議作為之評論(comment)。當然，利害當事人常在「提議制定行政命令之通知」發布前，即與聯邦通訊委員會進行溝通，希望能影響提議之行政命令草案內容，但「提議制定行政命令之通知」發布後有法定的尋求評論期間，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。而「諮詢之通知」將會促使所欲觸及的議題及尋求評論的出現，但通常尚未提議制定任何特定的行政命令。

一般而言，「提議制定行政命令之通知」發布於「諮詢之通知」之後。在「提議制定行政命令之通知」或「諮詢之通知」發布之後，聯邦通訊委員會將接受及審慎審查評論後，發布通常被稱為「報告與命令(Report and Order[594])」之行政命令。

---

[592] See, e.g., THIRD REPORT AND ORDER AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING, available at http://www.steptoe.com/assets/attachments/1655.pdf (last visited October 15, 2014).

[593] See, e.g., In the Matter of Acceleration of Broadband Deployment: Expanding the Reach and Reducing the Cost of Broadband Deployment by Improving Policies Regarding Public Rights of Way and Wireless Facilities Siting, https://apps.fcc.gov/edocs_public/attachmatch/FCC-11-51A1.pdf (last visited October 15, 2014).

[594] See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Second Report and

而當某一「報告與命令」之行政命令發布後，相關程序尚非到此為止。利害當事人得陳情聯邦通訊委員會重新考慮(reconsideration)其決定，但聯邦通訊委員會罕有同意該陳情者。[595]其實，促使聯邦通訊委員會重新考慮其決定之較有效的管道，乃包括國會得藉由立法而推翻聯邦通訊委員會的決定，以及受損害當事人得以聯邦通訊委員會決定乃違反聯邦法律[596]而對於其提起訴訟。[597]

而關於電信事業個人資料保護之相關法律規定，如前揭，按 1996 年電信法，除依法律規定或經用戶同意者外，電信事業禁止以電信法第 222 條所定以外方式而使用、揭露或允許接觸「用戶專屬線路資訊」。惟關於「用戶專屬線路資訊」之使用、揭露或允許接觸，該條未明定，應以何種方式取得用戶同意。對此，美國聯邦通訊委員會曾數度公布「用戶專屬線路資訊」相關命令及施行細則，但卻曾被提起訴訟並被質疑其是否合憲，因此，聯邦通訊委員會乃適度修改施行細則，以兼顧電信事業運用「用戶專屬線路資訊」之行銷需求與用戶「用戶專屬線路資訊」之隱私保護。

整體而言，按聯邦通訊委員會所公布命令及施行細則，就應取得用戶同意之方式，現行有效之制度，乃針對「用戶專屬線路資訊」接收者與電信事業關係之不同，而採行「選擇退出」與「選擇加入」雙軌並行的「同意」行使模式。針對「用戶專屬線路資訊」，只要電信事業所分享的關係企業係通訊相關的業者，其同意模式乃採「選擇退出」方式，毋庸取得用戶的事前明示同意；倘電信事業欲將「用戶專屬線路資訊」揭露予合資夥伴或獨立自主的契約締約相對人，或者允許其得接觸使用「用戶專屬線路資訊」時，電信事業應取得用戶「選擇加入」同意。

另外，聯邦通訊委員會 2007 年修改「用戶專屬線路資訊」相關施行細則，用以包括「通話細節資訊」之撥入、撥出電話的「位置」資訊。聯邦通訊委員會並於 2007 年「用戶專屬線路資訊」相關命令中釐清，網路電話(VoIP)及 IP 驅動的網路電話提供者亦應遵守「用戶專屬線路資訊」相關的規範。再者，藉由對於用戶

Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (1998 CPNI Order); Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002) (2002 CPNI Order); Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (2007 CPNI Order).

595 Stuart Minor Benjamin, Douglas Gary Lichtman, Howard A. Shelanski & Philip J. Weiser, Telecommunications Law And Policy 60-61 (2006).

596 See, e.g., U S WEST, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

597 *Supra* note595, at 61 (2006).

行動設備的控制而蒐集「用戶專屬線路資訊」之電信事業，亦應按電信法及相關施行細則規定，進行「用戶專屬線路資訊」之保護。

二、聯邦貿易委員會

聯邦貿易委員會(FTC)於 1914 年成立，其原始宗旨係為確保商業活動的公平競爭。後來，聯邦貿易委員會的權限逐步擴張。其中，最重要的擴張，即國會於 1938 年通過「聯邦貿易委員會法」(Federal Trade Commission Act) 之 Wheeler-Lea 修正案，因此，聯邦貿易委員會擴張權限至除得禁止商業中或影響商業的不公平競爭方法之外，亦得禁止不公平或欺罔(unfair or deceptive)之行為。換言之，聯邦貿易委員會除得藉由反托斯(antitrust)方式外，亦得直接保護消費者。據此，「聯邦貿易委員會法」第五條(Section 5 of the FTC Act[598])的通過，促使聯邦貿易委員會得對於違背反托斯及消費者保護之法律者[599]，加以處罰。

1995 年在國會催促下，聯邦貿易委員會開始處理消費者隱私議題。聯邦貿易委員會最初鼓勵產業「自律」(self-regulation)，因為擔心「政府管制」(regulation)將與網際網路活動的發展有所扞格。由產業自訂自律規範，以免除由聯邦貿易委員會制定規範，但仍由聯邦貿易委員會執行該自律規範。因此，聯邦貿易委員會乃扮演「自律」機制之後援角色，賦予聯邦貿易委員會監督及執行的功能[600]。

聯邦貿易委員會處理消費者隱私議題之法源，主要係「聯邦貿易委員會法」第五條，用以禁止商業中或影響商業的不公平或欺罔行為及慣例。所謂「不公平或欺罔行為或慣例」，係指「可能誤導理性消費者並受損害之重要陳述、省略或慣例」(material "representation, omission or practice that is likely to mislead the

---

[598] Section 5 of the Federal Trade Commission Act (FTC Act), Ch. 311, §5, 38 Stat. 719, *codified at* 15 U.S.C. §45(a), prohibits entities from engaging in unfair or deceptive acts or practices in interstate commerce. It states, in pertinent part: **(1)** Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful. **(2)** The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a (f)(3) of this title, Federal credit unions described in section 57a (f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C. 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C. 227 (b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

[599] Daniel J. Solove & Woodrow Hartzog, THE FTC AND THE NEW COMMON LAW OF PRIVACY, 114 Colum. L. Rev. 583, 598(April, 2014).

[600] *Id*. at 598-599 (April, 2014).

consumer acting reasonably in the circumstances, to the consumer's detriment[601])或「導致或可能導致消費者未能合理避免之重大損害及該重大損害大於對於消費者或競爭所產生之利益」(causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"[602])的一種慣例。因此，聯邦貿易委員會按「聯邦貿易委員會法」第五條而處理消費者隱私議題時，得以「不公平」或「欺罔」二種交易慣例為基礎而認定違反隱私保護[603]。

聯邦貿易委員會主要係以構成「欺罔」交易慣例為由而對於「隱私權政策」加以監督，縱使聯邦貿易委員會漸以構成「不公平」交易慣例為由而對於產業加以起訴。由於聯邦貿易委員會僅能對於賦予其管轄權限之「聯邦貿易委員會法」或其他法律之違反事件加以執行，以及其欠缺自行制定隱私法令之權限，因此，不受上開賦予聯邦貿易委員會管轄權限之法律拘束之公司倘又欠缺「隱私權政策」時，則聯邦貿易委員會將無權對之加以執行。因此，聯邦貿易委員會僅能限於執行公司所保證或允諾之事項，但對於個人資料如何被蒐集、處理、利用或分享，大多數公司均無義務必須為保證或允諾(promise) [604]。

綜上，由於多數法律並未強制要公司應提供「隱私權政策」予消費者，但倘其提供後卻又違反該「隱私權政策」者，則聯邦貿易委員會可以違反「聯邦貿易委員會法」第五條所「禁止商業中或影響商業的不公平或欺罔(unfair or deceptive)行為及慣例」為由而加以執行之。

當前，聯邦貿易委員會雖被視為係實質上(de facto)之個人資料保護主管機關。在許多國家的個人資料保護法體制中，通常均設有個人資料保護的專責機關，即指定一個執行個人資料的特定機構。有些批評者認為，聯邦貿易委員會過於弱勢且無實效性，但許多法律專業人士及公司則均視聯邦貿易委員會是一個令人敬畏的執法機關，其並審慎審視聯邦貿易委員會的決定，以做為業者決策之指引。其

---

601 Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce 174-76 (Oct. 14, 1983).

602 15 U.S.C. § 45(n).

603 *Supra* note599, at 599 (April, 2014). 劉定基，欺罔與不公平資訊行為之規範--以美國聯邦交易委員會的管制案為中心，公平交易季刊，第 17 卷第 4 期，頁 77-83，2009 年 10 月。

604 *Id*. at 600 (April, 2014).

實，縱使聯邦貿易委員會執行消費者隱私保護的個案及人員不多[605]、且未被賦與執行民事私權之權利[606]，但聯邦貿易委員會仍成為個人資料保護之最具主宰性的主管機關，乃因聯邦貿易委員會管轄權相當的擴張，以及聯邦貿易委員會的執行架構與決策者所提倡的「自律」[607]規範取向比起聯邦通訊委員會[608]更具有獨特的相容性。[609]

聯邦貿易委員會成為實質上之個人資料保護主管機關，乃天時地利人和配合的結果。自 1970 年起，聯邦貿易委員會即有權執行公平信用報告法(Fair Credit Reporting Act)，以確保信用報告機構保護消費者隱私。1998 年兒童線上隱私保護法(Children's Online Privacy Protection Act)賦予聯邦貿易委員會制定法規命令及執行之權限。1998 年金融服務現代化法(Gramm-Leach-Bliley Act)賦予聯邦貿易委員會及其他機關權限，制定適當標準，以保護金融機構客戶個人資料。其實，賦予聯邦貿易委員會之相關隱私法律通常相當程度依賴「通知與選擇」(notice-and-choice[610])之機制。例如，兒童線上隱私保護法要求通知及父母同意，而通知即以「隱私權通知」方式進行之。金融服務現代化法亦創造「通知與選擇」機制，乃以「隱私權通知」及選擇退出(opt-out)方式進行之。此外，聯邦貿易委員會亦被賦予執行美國與歐盟之間的「安全港協議」(Safe Harbor Agreement)。此後，

---

605 *Id.* at 599-600 (April, 2014).

606 Joel R. Reidenberg, PRIVACY WRONGS IN SEARCH OF REMEDIES, 54 Hastings L.J. 877, 888 (April, 2003).

607 即當政府公權力無意介入隱私相關問題，則仍有其他選項—即民間部門得自行發展個人資料保護標準，而無庸政府部門的直接介入。在對於現行法規及市場運作干擾最小之情形下，得利用對於民間現有「信賴標誌」(trustmark)產業的自律規範方式，逐步建立具有執行效力的個人資料保護標準。類似於確認產品或服務符合特定品質或規格之「資格標誌」 (certification mark)，信賴標誌則用以確認某企業的個人資料蒐集、利用、傳遞及分享政策符合特定個人資料保護標準，落實「說他們所做的，做他們所說的」(say what they do and do what they say)，以建立消費者的信賴感。換言之，消費者藉由企業所張貼的信賴標誌，便可以肉眼簡單辨視交易相對人關於資訊隱私或個人資料保護之執行狀況（是否遵守核心隱私原則—通知、選擇、接近、安全），而企業亦得藉由取得信賴標誌之認證而建立關於資訊隱私保護之信用。再者，為確保取得信賴標誌（如「隱私標章」【privacy seal】）之企業能落實應有的資訊隱私保護措施，信賴標誌之產業授與者(如 BBBOnline 或 Truste)應負起協助企業建立內部措施及善盡監督之責。參閱翁清坤，論個人資料保護標準之全球化，頁 51-52，東吳法律學報，2010 年 7 月。

608 Philip J. Weise, THE FUTURE OF INTERNET REGULATION, 43 U.C. Davis L. Rev. 529, 557 (December, 2009).

609 *Supra* note599, at 599-600 (April, 2014).

610 *Federal Trade Commission*, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, 2, available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last visited August 29, 2014).

聯邦貿易委員會主要係以「通知與選擇」模式為基礎而執行聯邦貿易委員會法第五條之規範。[611]

雖然聯邦貿易委員會所處理案件的數量每年穩定的增加，但其數量不算特別多。自 1997 年起，聯邦貿易委員會所起訴案件超過 170 件，平均每年約 10 件。[612]進一步言，美國聯邦貿易委員會對於違反個人資料蒐集、利用或揭露之相關隱私權政策承諾或未經通知消費者即重大變更隱私權政策內容之公司，認為其隱私權政策係「錯誤且誤導的」(false and misleading)而有聯邦貿易委員會法第五條所定之不公平或欺罔之情事，乃要求改善。例如，2003 年聯邦貿易委員會認定，服飾製造商 Guess 未能落實個人資料加密(encryption)之安全措施而易遭駭客(hacker)攻擊，因此，其隱私權政策係錯誤且誤導的而有不公平或欺罔之情事。2004 年聯邦貿易委員會認定，Gateway Learning Corporation 違反其隱私權政策而蒐集個人資料，且未通知使用者當事人及未取得同意即變更其隱私權政策內容而向第三人分享該個人資料。[613]又 2009 年聯邦貿易委員會曾認定零售業者 Sears 追蹤下載研究軟體消費者的線上瀏覽紀錄，卻僅在消費者多重註冊層次的最後階段所提供的一份冗長授權契約(license agreement)中間處，才揭露該軟體所欲完全追蹤的個人資料範圍，係未能提供充分的通知(adequate notice)予消費者，乃構成欺罔行為，因此，要求 Sears 不得繼續蒐集個人資料及應刪除已蒐集的個人資料[614]。

2011 年針對被指控誤導消費者關於個人資料的使用，Facebook 與聯邦貿易委員會達成和解，因此，Facebook 於溯及既往的重大變更(material retroactive change)隱私權政策內容前，應經當事人同意。換言之，倘 Facebook 以有別於消費者原始同意的方式分享個人資料，應經當事人同意。[615]可知，為不同目的而利用或分享

611 *Supra* note599, at 602-604 (April, 2014).

612 *Id.*, at 600 (April, 2014).

613 Suzanna Shaub, USER PRIVACY AND INFORMATION DISCLOSURE: THE NEED FOR CLARITY IN "OPT-IN" QUESTIONS FOR CONSENT TO SHARE PERSONAL INFORMATION, 5 Shidler J. L. Com. & Tech. 18 (Spring, 2009).

614 FTC, Protecting Consumer Privacy in an Era of Rapid Change- A Proposed Framework for Businesses and Policymakers, 12-13, available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited October 15, 2014).

615 Julia Angwin, Shayndi Raice & Spencer E. Ante, Facebook Retreats on Privacy, The Wall Street Journal, November 11, 2011, available at http://online.wsj.com/article/SB10001424052970204224604577030383745515166.html?mod=WSJ_hp_us_mostpop_read (last visited August 30, 2014); FTC's settlement Agreement with Facebook, available at http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf (last visited August 30,

個人資料，應另外取得同意，否則，將被視為違法，例如，Google 告知 Gmail 用戶其個人資料僅供 email 目的使用，卻未事前取得當事人同意，即將其轉用於 Google Buzz 社群服務(social-networking service)之其他目的，而於 2011 年被美國聯邦貿易委員會認定為欺罔消費者[616]。

而關於「用戶專屬線路資訊」(CPNI)的保護，FTC v. Accusearch Inc.案[617]，聯邦貿易委員會主張，Accusearch Inc.未經用戶知悉及同意，即取得「用戶專屬線路資訊」並將其販售與第三人；具體言之，Accusearch Inc.使用不實的偽裝、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。因此，在該案中，第十巡迴法院認定，以欺罔方式蒐集個人資料乃構成「不公平」交易慣例，故其乃為一有利於聯邦貿易委員會之簡易判決[618]。

事實上，聯邦貿易委員會已對於業者提起超過 170 個隱私相關的訴訟，但幾乎每一個訴訟均被撤回或和解，僅有一個訴訟係經過法院裁判，即上開 FTC v. Accusearch Inc.一案。[619]而絕大多案件均未經法院裁判即結束，其原因，即訴訟成本之考量，尤其，因違反「聯邦貿易委員會法」第五條不會有罰鍰之風險，故業者欠缺花費大量金錢與時間以對抗聯邦貿易委員會之誘因；其次，法院在審理訴訟案件時，仍須尊重聯邦貿易委員會對於「聯邦貿易委員會法」第五條或其他相關聯邦法律之解釋，降低業者勝訴之機率，而聯邦貿易委員會考量節省金錢、時間與降低訴訟不確定性之公共利益而和解；最後，和解的協議並非即責任之承擔，業者毋庸承認做錯而再行推動業務。[620]然而，一旦業者與聯邦貿易委員會進行和

2014).

616 SHAYNDI RAICE & JULIA ANGWIN, Facebook 'Unfair' on Privacy, NOVEMBER 30, 2011, available at http://online.wsj.com/article/SB10001424052970203441704577068400622644374.html#ixzz1fAwiQlu7 (last visited August 30, 2014); FTC news, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network, available at http://www.ftc.gov/opa/2011/03/google.shtm (last visited August 30, 2014) . 參閱翁清坤，告知後同意與消費者個人資料之保護，頁 279-280, 289, 302-303，臺北大學法學論叢，2013 年 9 月。

617 Complaint for Injunctive and Other Equitable Relief at 5, FTC v. Accusearch Inc., No. 06-CV-0105 (D. Wyo. Sept. 28, 2007) [hereinafter Accusearch Complaint], available at http:// www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf (last visited August 30, 2014).

618 *Supra* note599, at 641 (April, 2014).

619 *Id.* at 610-611 (April, 2014).

620 *Id.* at 611-612 (April, 2014).

解或業者敗訴者，該業者即被禁止再行從事系爭被認為係不公平或欺罔之行為及慣例，或該業者必須遵守聯邦貿易委員會之要求而修改其「隱私權政策」。[621]

三、小結

聯邦通訊委員會(FCC)主要係主管及執行電信事業個人資料蒐集、處理、利用或分享之相關隱私法律及行政命令。其中，美國聯邦通訊委員會曾數度公布「用戶專屬線路資訊」相關命令及施行細則。事實上，聯邦通訊委員會制定行政命令、法規命令或行政立法之正式過程，由發布「提議制定行政命令之通知」或「諮詢之通知」開始。一般而言，「提議制定行政命令之通知」發布於「諮詢之通知」之後。在「提議制定行政命令之通知」或「諮詢之通知」發布之後，聯邦通訊委員會將接受及審慎審查評論後，發布通常被稱為「報告與命令」之行政命令。而當某一「報告與命令」之行政命令發布後，利害當事人得陳情聯邦通訊委員會重新考慮其決定，但聯邦通訊委員會罕有同意該陳情者。其實，促使聯邦通訊委員會重新考慮其決定之較有效的管道，乃包括國會得藉由立法而推翻聯邦通訊委員會的決定，以及受損害當事人得以聯邦通訊委員會決定乃違反聯邦法律而對於其提起訴訟。

另外，當前聯邦貿易委員會(FTC)雖被視為美國實質上之個人資料保護主管機關，但其權限在法令上仍受到不同產業部門主管機關監理權限範圍之限制，因此，對於電信事業個人資料保護之監理，聯邦貿易委員會應尊重聯邦通訊委員會之權限。但由於「用戶專屬線路資訊」之流通與利用通常受電信事業「隱私權政策」的拘束，因此，仍將受聯邦貿易委員會之規範。倘違反一家公司「隱私權政策」之行為係構成「不公平、欺罔行為或慣例」者[622]，則聯邦貿易委員會有權蒐集相關資料、展開調查並可按聯邦貿易委員會法第五條規定提起訴訟，以保護個人資料。

621 *Id.* at 614-615 (April, 2014).

622 Lynn Chuang Kramer, PRIVATE EYES ARE WATCHING YOU: CONSUMER ONLINE PRIVACY PROTECTION-- LESSONS FROM HOME AND ABROAD, 37 Tex. Int'l L.J. 387, 715-716 (Spring 2002).

第七節 我國現行制度

一、自律機制

電信事業多透過提供客戶電信相關服務，並換取等價利益為目的，以其角度而言，客戶所給予之個人資料，經其整理歸檔後，即成為了其營運上不可或缺之資產，因此，如何降低營運風險，確保營運的永續性，進而獲取豐厚的投資報酬率與商機，應是值得投入心血關注的問題；[623]反之，以交付個人資料換取服務之客戶角度而言，其是否有落實個資法第 27 條第 1 項「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」與同法施行細則第 12 條[624]之要求,自技術面與組織面加強個人資料安全維護措施,值得關切。

目前我國電信事業積極針對其組織管理及稽核層面取得 ISO/IEC27001、ISO/IEC27011 與 BS10012 等國際認證，我國經濟部商業司亦積極推動臺灣個人資料保護與管理制度規範（TPIPAS）之認證，期待建立一套符合國際標準之資訊安全管理系統(Information Security Management System，ISMS)，以下僅就上述認證進行簡要介紹。

(一) 國際認證標準

1、 ISO/IEC27001 與 ISO/IEC27011

國際標準組織(ISO)與國際電工技術委員會(IEC)屬互補之組織，ISO/IEC27001 此一資訊安全標準為目前國際認證的資訊安全管理系統標章，其前身係英國標準協會(BSI)提出之 BS7799-2 標準，以其為基礎延伸整合為現今的樣貌[625]。由該規範

---

[623] 徐弘昌，以 ISO27001 為基礎評估電信業資訊安全管理─以第一類電信業者為例，國立交通大學管理學院碩士在職專班管理科學組，碩士論文，2009 年 6 月，頁 8。

[624] 個人資料保護法施行細則第 12 條規定：「本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

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。」

[625]其大致上之發展過程依序如下：1995 年，BSI 公佈 BS7799 PartI；1998 年，BSI 公佈 BS7799 Part II；1999 年，BSI 公佈新版 BS7799 Part I、Part II；2000 年，ISO 通過成 ISO/IEC 17799PartI；2002 年，BS7799：2-2002，成為資訊安全管理系統驗證規範；2005 年，BS7799：2-2005，同年 10 月成

之目標及控制措施觀察，其安全政策目標設定為「依照營運要求和相關的法律法規，提供管理階層對於資訊安全的指導與支持」與資訊安全事件管理目標乃「確保和資訊系統有關的資安事件與弱點，都擁有相對應的處理程序，並且能夠正確及時地被傳達通報」，並搭配採行「計畫、執行、檢查、行動(Plan-Do-Check-Act)」之控制措施，期待能針對不同風險所產生之資安問題，達成持續改進模式運作之目的。

參照國際標準或國家標章 CNS27000 系列之對應標準，ISO/IEC27001 係指資訊安全管理系統要求事項；ISO/IEC27002 係指資訊安全管理作業規範；ISO/IEC27005 係指資訊安全管理風險管理；ISO/IEC27011 則為電信事業資訊安全管理實作指引。實際運作上，須將其整合，方得在個人資料之保護上做到完臻，而此亦為目前國家通訊傳播委員會於其電信事業資通安全管理手冊中，建議電信事業應追求並達成之標準。

目前 ISO27001 已成為眾多政府機關及民間企業推動資訊安全導入的標章，其優點在於可保全資安防護證據，作為法院訴訟時之佐證。惟其驗證範圍，似有侷限於實體機房或資訊部門之情形，考量個資並非僅於上述部門間流通，若欲單純以 ISO27001 資安管理架構進行防護，建議應擴及全組織各部門。

2、 BS10012：2009[626]

英國標準協會(BSI)於 2009 年，參考經濟開發合作組織(OECD)，對於個人隱私權保護的八大原則，針對個人資料保護擬定一標準，設定落實個人資料保護之要求，而英國 BS10012 國際個人資訊管理標準，普遍被認為是推動個人資料保護的最佳實務標準。

英國 BS10012 要求不論是國家或企業組織，都應有專責管理個資的單位，該單位應職掌個資的蒐集、使用、傳遞、銷毀與保存；應事先定義所謂的個資類別清單，清楚定義單位收集的個資範圍，釐清並界定何種資料須受保護，以及個人資料保護之層級，並須清楚地掌握個人資料之流通，架構一個具有設置各種管控機制來控管個人資料保護之框架。

為國際標準 ISO27001。

[626]鄭伊雯，植基於 ISO27001 建立符合 BS10012 之個人資訊自我評鑑模式，中原大學碩士論文，2012 年 7 月，頁 21。

另外，其所列出之個人資料保護之八大基本原則，亦具參考價值，臚列如下：

(1)受到公平合法的處理；

(2)僅具體指明的取得，且處理方式符合此等目的；

(3)適當、相關且不過度；

(4)正確且最新；

(5)保留時間不超過必要程度；

(6)處理方式符合法律賦予個人的權利，包括標的存取權；

(7)獲得安全保障；

(8)不在未受到適當保護的情況下被移轉到境外的國家。

(二) 臺灣個人資料保護與管理制度規範

隨著個人資料保護法之修正，為達成個人資料保護法之立法目的「避免人格權受侵害，並促進個人資料之合理利用」，於此，如何協助企業適應現行個人資料保護法，實屬值得關注的議題，於此，遂參考國外制度與標準之作法，由經濟部商業司推動我國隱私權管理保護認證制度：「臺灣個人資料保護與管理制度規範(Taiwan Personal Information Protection and Administration System，TPIPAS)」，並委由財團法資訊工業策進會執行,以提升事業對於個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境，而其運作方式與 ISO/IEC27001 同樣皆採「計畫、執行、檢查、行動」(Plan-Do-Check-Act)，並達成以下四種實益：

(1)協助企業遵循個人資料保護法並降低責任風險；

(2)有效減少個人資料外洩事件，提升民眾放心從事電子商務活動；

(3)隱私標章作為企業識別，提升業者信譽，增強自律效果；

(4)與國際規範相互配合，有助跨國電子商務等交益活動活絡。

其與 ISO/IEC27001 最大之不同，在於其非僅偏重在資安管理上建立制度及標準作業程序，亦重視輔導業者全面性遵守個資法。

二、他律之監管

(一) 現行個資法之規定

查我國個資法所設置對非公務機關之適法蒐集、處理或利用個資之監督機制為典型之「主管機關制」，其主要內容為；(1)、檢查等權限：依個資法第 22 條規定，中央目的事業主管機關或直轄市、縣(市)，為執行資料檔案安全、業務終止後資料處理方法、國際傳輸限制，或其他例行性業務檢查，認為有必要或有違法之虞時，得進入檢查，並命令為必要之說明、配合措施或提供資料；(2)、個資檔案安全維護計畫，或業務終止後個資處理標準之訂立與指定：依個資法第 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立個資檔案安全維護計畫等，並訂立其計畫等標準。而對違反本法規定者，中央目的事業主管機關或直轄市、縣(市)政府得依個資法第 47 條及第 48 條處以非公務機關罰鍰，並限期令其改善；另得依第 25 條為禁止個資蒐集、處理或利用之處分，命令刪除檔案、沒入或銷毀違法之個資、公佈其違法狀況及姓名或名稱與負責人。此係以行政檢查及行政罰方式監督非公務機關合法蒐集、處理、利用個資。惟我國受個資法適用之非公務機關依第 2 條第 8 款規定，為除公務機關外，包括所有自然人、法人或其他團體，不問規模大小、是否營利為目的，範圍非常廣泛；中央目的事業主管機關或直轄縣市政府有無具備專業知識之人力執行檢查，首先已成問題；再各政府機關間對個資法之運用與解釋，因缺乏橫向溝通及交換意見之平台，亦可能有見解不同而造成法律適用上不一致之疑慮。

(二) 國家通訊傳播委員會之監督　——主管機關監督制

1、 行政規則之發布

作為電信事業有關資通訊安全主管機關之國家通訊傳播委員會(下稱:通傳會)，依通傳會組織法第 3 條第 8 款規定，並參考國際標準畫組織(International Organization for Standardization，ISO)公布之指引-ISO/IEC27011，制訂有「電信事業資訊通訊安全管理作業要點」提供「電信事業資訊安全管理手冊」，供給業者做為其內部稽核資訊安全之用，以強化資通訊安全管理機制。

2、 行政調查

倘若通傳會認為有必要時，依前開安全作業要點第 4 條得對電信事業者進行

相關文件等之索取、通知陳述意見或現場勘驗現勘等行政調查。

3、 資訊之提供—認證合格業者名單之公告

通傳會應定期公告，取得經該會認可之資通安全管理機制驗證機構驗證合格之業者名單，以供大眾參考。

三、小結

任何法律制度之落實，除以外來法律規範強制要求受規範者履行法定義務以以外，如受規範者能健全自己內部控管機制，進行自我檢點，自發性遵從法律，自可減少違法之機會，亦可降低主管機關法執行之成本。因此法律制度建置時，除立法明定受規範者之義務、授權主管機關進行行政檢查、對違法者得科處以行政罰甚至刑罰等他律機制之外，亦多有輔導受規範者取得認證等，自自己內部建構完善制度，降低風險或違法事情發生之自律機制，如此自外而內完整落實法制之效力。

自前述我國對電信事業遵守個資法之監督機制觀之，大致上他律與自律之機制均已建立，惟，自律部分主管之通傳會所致力輔導業者取得之 ISO 認證，再詳看其取得認證審查之項目則多偏重資訊安全之部分；當然資安確為個保護資之重要事項，然如何讓業者理解個資法規，自蒐集、處理至利用個資均符合法律規定，應為保護個資之根本；因此如何輔導業者能正確解讀個資法，知悉個資法所規定之各項蒐集、處理至利用之要件，恐為一項重要、不能忽視之課題。

第五章 結論與建議

綜觀前第二章我國之法制面對電信事業蒐集處理個資之規範，及第四章有關他律與自律之監管機制，再與英、美、德、日、韓及歐盟等相關法規範比較後，得到如下結論，分為四方面說明。

第一節　法律規範面

一、釋憲實務

依司法院釋字第 631 號解釋，通訊秘密在確保人民就通信之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵害之權利。而於同號解釋理由書更敘明：秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人私生活領域之免於國家、他人侵擾，及維護個人資料之自主控制，所不可或缺之基本權利。基此，通訊秘密內涵：通訊之有無、對象、時間、方式及內容等事項，應得先確認，且此所稱亦為維護個人資料之自主控制，得解釋為通訊秘密之保護同為個人資料之保護。

二、通訊保障及監察法

通保法保護之客體分作以下三類，一為通訊內容；其二為同法第 3 條之 1 規定之「通信紀錄」即電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電話號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄；及另一則為通訊使用者資料。

蒐集、處理或利用之要件：關於通訊內容之監聽，其對象須為同法第 5 條第 1 項所訂各款犯罪之被告或嫌疑人，或同法第 7 條第 1 項之外國勢力、境外敵對勢力其工作人員之通訊。而對通信紀錄及通訊使用者資料之調取，則須為同法第 11 條第 1 項或第 2 項或第 3 項所訂之犯罪偵查。再得為蒐集或利用者限定為檢察官或司法警察，且須事前或事後依書面申請法院核發或補核發通訊監察書或調取票。而該當資訊之利用依同法第 2 條、第 10 條僅限於確保國家安全，維持社會秩序而

調查犯罪證據之用，或國家安全預警情報之用。

資料保存期限：依同法第 17 條，就通信監察之內容，除已供案件證據之用留存於該卷宗或為監察目的有必要長期留存外，由執行機關於監察通訊結束後，保存五年。

三、電信法

(一) 保護之個人資料

依電信法第 7 條規定：電信事業或其服務人員、退職人員，對於電信之有無及其內容，應嚴守秘密。並授權主管機關訂定行政規則或作業程序，以保障通信祕密及規範當事人查詢相關個人通訊資料之程序。此外通信紀錄依電信法第 2 條第 8 項規定係指: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(電話號碼或用戶識別碼)、通信日期、通信起訖時間等紀錄。

又，所謂「使用者資料」依電信事業處理有關機關(構)查詢電信使用者資料實施辦法第 4 條訂為:電信使用者姓名、名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信事業務所填列之資料為限。

(二) 利用之要件

對**「通信內容」**除通信雙方當事人同意外，電信事業者應不得蒐集、處理之。

而**「通信紀錄」**為通信時電信系統自動留存之資料，係將來用以計算電信費率之重要根據，為電信事業營運業務之目的而正當合法所蒐集、處理、利用之資料。應注意者為應第三人要求而提供之目的外利用，對此電信法本身並未為規定，而係依電信事業處理有關機關查詢電信通信紀錄實施辦法為規範。而依前開辦法第 3 條:得要求提供之第三人為「有關機關」，不問是否為公務機關或非公務機關；其要件為：符合法律程序，載明法定應記載事項，送該電話用戶所屬電信事業所指定之受理單位辦理。

「使用者資料」依電信事業處理有關機關(構)查詢電信使用者資料實施辦法第 3 條，得要求提供之第三人為：(1)司法機關、監察機關或治安機關，(2)其他政府機關，(3)與公眾生命安全有關之機關(構)。要件為：(1)因偵查犯罪或調查證據所需，(2)因執行公權力所需，(3)為緊急救助所需；如為前(2)及(3)之請求者須敘明法律依據外，並備妥正式公文或電信使用者資料查詢單，載明應記明資料事項，送

該電信使用者所屬電信事業指定之受理單位辦理。

(三) 資料之保存期限

通信紀錄依據行動通訊管理規則第 72 條之 1 的規定，相關通信紀錄應至少保存六個月以上。固定通信(俗稱之市內電話)紀錄之部分，依據固定通信業務管理規則第 49 條之 1 的規定，將其分為一般室內電話及長途電話等作不同規範；前者依法至少必須保存三個月，後者則必須至少保存六個月以上。

網路通信紀錄之部分，依據第二類電信事業管理規則第 27 條規定，將其分為語音單純轉售服務通信紀錄、網路電話服務通信紀錄、網際網路接取服務和虛擬行動網路服務通信紀錄等四大類型，各類型之保存期限皆有所不同，最長為六個月，最短則為一個月 。

使用者資料保存期限，電信法對此並無明確之規範，惟依據國家通訊傳播委員會頒布之行動通訊業務管理規則第 73 條及固定通信業務管理規則第 49 條之 2 規定，電信事業經營者應核對及登錄使用者資料，並至少保存至服務契約終止後一年。

四、檢討及問題之發現

綜合分析上述法律或釋憲實務有關電信事業提供電信服務，對個人資料之蒐集、處理或利用所揭示之規範後，得發現我國現在有以下情況：

(一) 法律之適用關係複雜

規範電信事業提供電信通訊服務時對個資蒐集、處理或利用之法規範如上所說明，包含有通保法、電信法、及個資法；而此三法之適用關係，個資法應為普通法，電信法則為個資法之特別法，通保法則又為電信法之特別法。亦即檢察官或司法警察如為前述法定犯罪事件之偵查而有必要時，應先依通保法於取得法院核發之通訊監察書或調取書，蒐集特定個人之通訊內容或通訊紀錄資料、使用者資料。非屬通保法所定特定犯罪偵查之需要，而有關機關查詢特定人通信紀錄時，則依電信法授權訂立之電信事業處理有關機關查詢電信通信紀錄實施辦法；有關機關(構)若為查詢使用者資料時，又係依電信法授權訂立之電信事業處理有關機關(構)查詢電信使用者資料實施辦法以為進行。如非為機關(構)之一般人向電信事業查詢他人之通信紀錄或使用者資料時，或機關(構)非為電信事業處理有關機關(構)

查詢電信使用者資料實施辦法第 3 條 1 項 3 款所定目的查詢電信使用者資料時，則應有特定目的後，依個人資料保護法第 19 條向電信事業查詢以為蒐集，同時電信事業應依同法第 20 條但書判斷是否得為目的外利用而提供之。形成因查詢人之不同、查詢資料之不同、查詢目的之不同，分散由個別之法規規範，而有下列之問題：

1、 保護客體之不一致

通保法所定之「通信紀錄」內涵項目，較之電信法所定者多且詳細，其中「位置」、「信箱」等資料未被電信法所明列，其原因可能是後者為較早期之立法，無線網路通信未普及故而未納入保護之範圍，當然現仍可依擴張解釋方式解決疏漏之問題。

然卻造成同樣之法律名詞在不同之法中卻有不同內涵之虞，再綜觀各外國相關法規多將位置資料納為電信事業所蒐集、處理或利用之個資予以保護，更彰顯規範法規不足之處。又所謂信箱應是電子郵件信箱網址，在現今幾乎與傳統語音通信匹敵而為大眾慣用之通信手段，亦為電信加值網路服務之項目，被遺漏在保護客體範圍外亦有未妥。

2、 規範位階之疑慮

有關通信紀錄及使用者資料之提供第三人查詢，其要件依電信法第 7 條第 2 項規定為依法律規定查詢者，而查詢作業程序則授權電信總局以「電信事業處理有關機關(構)查詢電信使用者資料實施辦法」及「電信事業處理有關機關查詢電信通信紀錄實施辦法」規定。故電信事業者對「依法律規定查詢者」，提供通信紀錄及使用者資料時，原即為有法律依據之合法行為，僅依法規命令再揭示其執行辦法，不生問題；然依辦法第 3 條第 3 款，與公眾生命安全有關之機關及機構，為緊急救助所需之查詢，電信事業對之提供使用者資料時，應得認定其為緊急避難而阻卻違法，但此內容涉及構成要件之規定，是否適合以法規命令規定，並非無疑慮。

3、 相關法令分散繁多

如前述對電信事業查詢通信紀錄及電信使用者資料須依不同之法令，且區分查詢者為機關(構)與一般人不同，又依不同之法律規範；更有甚者關於資料之保存

期限，依資料種類之不同及因傳訊方式為市話或行動電話、網路電話等之不同，分別在各個不同法規上為長短不一的期限規定，法律之適用事實上過於混亂與困難。

(二) 個人資料保護法之欠缺

1、資料共同利用之疑慮

依個人資料保護法第 2 條第 4 款稱「處理」為建立或利用個人資料檔案所為之資料…內部傳送。而總公司與子公司，或事業集團內之各公司間互相傳送彼此所蒐集之個資檔案，以利用為行銷、開發產品等，可減低經營成本，拓展市場，應係各大事業團體期盼之事；但如此共同利用個資檔案之行為，能否解為「內部傳送」之合法行為，對此亦多有疑慮。為此，金融監督管理委員會依金融控股公司法定訂立金融控股公司子公司間共同行銷管理辦法，以規範金融控股公司與旗下之子公司利用客戶基本資料、往來交易資料及其他相關資料行銷。電信事業所經營之事業項目隨加值網路服務之多樣發展，形成事業集團多角經營為必然、應然之趨勢，然因個資法在此部分規範不明確之狀況下，造成電信事業怕觸法而有所顧忌，對電信事業之多面向發展多角經營恐成阻礙。

2、關於個資之蒐集、處理或利用之委外〈outsourcing〉欠缺實效性規範

現在各事業為降低經營成本，常將客戶資料蒐集、處理或利用等事務委由其他業者進行，例如，資料庫之建立、帳單之列印、寄發，甚至欠收帳款之催收等，此作為將增加當事人所無法預見之風險，且應負個資保護之責任者將無法釐清，將損害當事人權益，故對此行為必須加以規範；依現行個資法第 4 條則規定為:受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。如受委託者為國內業者且資力亦相當者，一旦違法致使當事人受損時，自得依法追究其法律責任並要求賠償當事人，如為境外委託，或現在之雲端處理，該第 4 條之規定將無法發揮作用；且施行細則第 8 條已增加受規範者之義務，是否能在法規命令中作如此處理，大有疑慮。

3、目的外利用之寬泛

如本章前所述通保法及依電信法授權訂立之電信事業處理有關查詢通信紀錄實施辦法，均限定為檢察官等特定機關〈構〉為特定目的始得調取；其他人或機

關如定特定目的後，再依個資法第 19 條第 6 款「與公共利益有關」，向電信事業蒐集通信紀錄或使用人資料時，電信事業再依第 20 條但書第 2 款「為增進公共利益」之事由，甚或「為防止他人權益之重大危害」，認定依法得為目的外利用而提供給他人。以此不確定概念所定之法律要件，可能讓電信事業在無須調取票下，即將通信紀錄或使用人資料提供他人利用，相較於檢察官等特定機關之嚴格調取要件，其不合理處不言而喻。

4、不完備之事故通知規定

依個資法第 12 條規定: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。此立法理由乃為將資料洩漏等事故發生告知當事人，避免當事人因此被詐騙，並讓當事人得採適當措施防止損失擴大；但在「查明後」始通知當事人，則是否未查明時，即無須通知當事人?如查明竊取事故真相曠日費時者，當使本條立法目的喪失殆盡。又通知之人僅限當事人，無須向最有能力防止損害擴大之主管機關通報，亦屬立法之缺失。事實上，事故之發生亦應向社會大眾作適當之公開，讓其他業者警惕勿重蹈覆轍，更可防止善意第三人發生，故本條立法亦難謂完善。

(三) 空白之領域

電信事業者所經營之業務，自早期僅有線語音通訊服務，因資訊科技快速進步之故，發展至行動通訊，再因資訊數位化之原因，增加簡訊通訊方式及其他加值服務；近年行動通訊更結合有網路之功能，使電信事業已跨足網路服務；加之智慧型手機及行動裝置軟體(App)之普及化，傳統語音通訊服務逐漸被網路通訊取代。此一現狀自前第一章說明介紹之電信事業所經營之事業項目除語音通訊服務外，藉由加值網路擴展至電子郵件傳送，電子公告欄、網路電話、上網查詢資料等服務，可明確察知；但也因此使電信事業面臨新的挑戰，如惡意散播病毒郵件或垃圾郵件等，致使網路通信發生障礙甚至癱瘓，造成經營網路電信事業者損失，或濫發廣告簡訊導致電信用戶感到困擾等事件，電信事業者應如何防止這些事件，於前述電信法中並未有明文；而提供電信通信服務之業者依現行個資法似亦無任何條文得援用以檢閱電子郵件加以攔阻。立法院曾於 101 年 4 月審議通過二讀卻未完成立法之「濫發商業電子郵件管理條例草案」，試圖解決問題。亦足證我國有關法律對此部分之規範，顯有不足。

又，近年來裝置於智慧型手機上之軟體運用程式 Line，所提供之免費通信服務，已被普遍利用；因其提供服務之軟體程式公司，為外國法人，且在我國未設有任何分公司，致使我國無法可管。其通訊安全有諸多疑慮，亦在媒體上被多次報導有洩漏使用者個資之事件發生，且嚴重威脅我國合法電信事業通訊服務之市場，形成不公平之競爭；對此問題應如何在法治面、技術面解決，應是我國政府機關要積極面對之重要緊急課題。

第二節　監管機制面

一、自律之部分

所謂徒法不足以自行，單僅依賴主管機關之監督，因對象業者眾多，又涉及許多事業內部之管理作業，實有其界限，未能完全杜絕業者之違法行為。如能再建立其他機制，敦促業者自己做好內部控管，自發性遵守法律，事實上可補強監督機關執法未盡之處，個資保護認證標章制度即基此理念而產生者。

通傳會於「電信事業資通安全管理手冊」中，即建議電信事業應達成國際所要求有關資訊安全之認定標準；目前我國電信事業者已多取得如 ISO/IEC27001 等國際個資保護與管理制度安全認證標章。

除上述 ISO 之認證外，尚有經濟部商業司委託財團法人資訊策工業策進會(下稱資策會)，規劃及推動「台灣個人資料保護與管理制度(Taiwan Personal Information Proection and Administration System, TPIPAS)」，亦即公司或業者如通過 TPIPAS 管理系統之審查，即可取得經濟部商業司「資訊隱私保護標章(Data Privacy Proection Mark.DP. Mark)」。雖其適用對象初期示以經營電子商務之業者為對象，但將來隨業務之擴展與需要預計擴及至其他業界甚至公務機關。

業者在取得認證標章之過程中，必須依標章認證機構所設立之各項檢驗標準，包括保護個資安全之各種軟硬體設施之裝置完備、人員教育等，一一自我檢視，並評估風險，於接受檢測，被認定符合標準後，始能取得認證標章，且之後必須定期重新受檢。因此業者為取得或保有認證標章，必須在內部建立並維持一定水準之個資保護制度，致使業者自發性守法，發揮自律之作用；另一方面取得認證標章之業者亦得對外揭示其標章，提高社會之信任度與商譽。

二、他律之部分

如本報告書第四章第七節所述，對電信事業有關個資遵法之監管，依個資法之設計，係由目的事業主管機關負責。而現今通傳會亦依其組織法第 3 條第 8 款所明定之職掌而頒布「行動通訊管理規則」、「電信事業資訊通信安全管理作業要點」及「電信事業處理有關機關查詢電信通信紀錄實施辦法」等多項法規命令，對電信事業者進行監督管理。因通傳會握有電信事業經營之特許、許可權限，且有個資法規定之行政罰為後盾，如能確實執行監督職務，當能發揮相當之監督效力。但如前述監管法令分割零碎，缺乏統一規劃為其不足之處。

綜上，我國現今對電信事業之監管機制，確為主管機關制之他律為主，而輔以認證標章之自律為輔所構成，以期規範電信事業者合法、安全為個資之蒐集、處理或利用。但如前述有關認證標章之取得有太偏重資安部分之疑慮；再業者取得認證之花費，對營業規模小之第二類電信事業而言，為不輕之負擔；現實中有未取認證之業者仍照常營業者，如未有更大之獎勵措施或誘因，事實上將會影響業者取得認證標章之意願。

第三節 實務面

一、隱私政策之公告

為符合 OECD 及歐盟指令透明化原則，世界各國之企業均在其網站首頁公布其隱私政策「Privacy Policy」，對社會大眾揭示其蒐集、處理或利用客戶等個資之法依據、個資之種類、利用目的、告知當事人得行使之權利、資安策略、客訴處理機制等，讓處理個資之過程透明化，降低大眾之疑慮，亦是對社會保護個資之承諾。

我國之各大電信事業亦均在其網站首頁公布其隱私政策，本研究團隊上網查得中華電信等五大電信事業公告之隱私政策，經閱讀後，發現其內容差異不大；而對蒐集之個資類別，三大電信事業則多揭示以:「主管機關公告之個人資料類別」、「電信事業或加值網路業務執行所必要之個人資料」及「申請文件之客戶及其法代理人資料」，對「通訊紀錄」、「位置資料」隻字未提，亦即未針對電信事業者所得蒐集之與其他業者不同之個資，作特別揭示。再，在「利用範圍」之一項，原

應包含蒐集所得個資之利用目的、利用人、利用期間等項目；結果在「利用人」之範圍，三大電信事業均定為：供母公司及母公司關係企業及合作廠商或委外之廠商；至於母公司關係企業、合作廠商或委外之廠商為何，則未見作任何交代。對客戶或利用人而言實不易得知是何業者利用個資，造成當事人承擔不可預見之風險。且如前述我國個資法第 4 條係將受託人視同委託人予以規範，並未對委託人在締結委託時應盡之注意義務及對受託人應負擔之委託事務監督,作任何規定；若有個資被洩漏或竊取等侵害當事人事故發生時,不僅責任之歸屬容易發生爭議，因當事人可能連受託人為何人亦無從知悉，致使其求償無門。如此利用範圍之揭露，是先天立法缺失再加諸業者告知不足之後天失調，不符合個資保護之基本原則。

二、業務服務契約中個資蒐集告知條款

依本研究團隊所蒐集三大電信事業與客戶所訂立之第三代行動通信業務租用申請書，其上記載有關個資條款均僅有一條，且內容僅有「因業務上所掌握之相關資料負有保密義務，除當事人要求查閱本身資料，符合個人資料保護法及相關法令規定，不得對第三人揭露(含與本公司合作之內容服務提供者)」。未說明「取得如何之個資」、「特定利用目的為何」、「是否得用來行銷」，顯然對契約當事人用戶之說明及保護均有不足。

其中較理想者則為中華電信，其另訂有一紙「客戶個人資料蒐集告知條款」，就利用人範圍、利用目的，對客戶得行使之查詢等權利明確告知；而對行銷亦得由當事人勾選是否同意。

三、焦點座談及深度訪談之所見

(一) 法制面之見解及針對特別法規之制訂之必要性:

依學者專家之見解，對目前個資法之規定有認為過於嚴苛，未必完全符合電信事業者之實際運用上之需要;或與現時資訊科技(如 APP)發展與大量被使用脫節，造成無法可管之空白地帶；或同一業者因經營之業務項目不同，而有不同主管機關之問題。亦有認為關於個資法之解釋，各主管機關最後須依賴法務部，人民無申訴之管道。

又依外國之法制多對電信事業之蒐集、處理或利用個資，訂有特別之法或行

政法規，以為規範。為讓電信事業者有更明確之法規範可依循，減少違法之疑慮，事業主管機關得針對電信事業之現況與需要，在現行個資法之基礎上考慮制訂更詳細之法規命令。

(二) 關於事業集團或分公司共有資料

大部分業者未正面回答是否有集團間共用用戶資料之事實;依法務部之意見，認為電信事業主管機關可參考金管會依修正之金融公司控股法，制訂事業集團間共用用戶個資之規範。學者專家則認為電信事業應告知用戶共用個資之範圍、及利用目的。

關於委外問題，除中華電信外，多數電信事業關於帳單之列印、費率之催收等，確有委外處理之事實，雖有電信公司表明與受託人間訂有保密契約等，然對受託人之監督是否確實?本研究團隊難以查證。

至於電信黑名單，業者未承認有此事實之存在，但確曾與主管機關討論其必要性。

(三) 獨立監督機關之設置

大多數學者專家認為現行、由主管機關監督制雖可行，亦有其優點，但立於個資法常須跨國執行必須與世界接軌，我國有積極加入國際性個資保護組織之必要；再，對個資法之統一解釋、人民申訴窗口之明確化，建議有設置監督個資法施行之第三人監督機關之必要。其問題在於該獨立監督機關之層級及所屬，依目前之中央行政機關組織基準法，設有種種限制，要如何突破?

電信事業則認為,目前其目的事業主管機關通傳會已實行種種規範監督機制，無須再設獨立人監督機關使其遭受多重機關之管制。

(四) 認證標章之取得

多數學者專家認定確有助於業者自律性遵守個資法，各大電信事業亦積極取得認證在案；但取得認證所需費用，對小規模之第二類電信事業者，被認為是沉重的負擔，且主管機關似乎缺乏鼓勵業者取得認證之誘因。

第四節 外國法制之借鏡

一、個別法規之制訂

因電信事業締結契約之用戶或利用者數量龐大，且不同於其他業者，只要一提供通信服務，在通信系統上於當事人未查覺中即開始蒐集、儲存利用人個資，而所蒐集得之個資不僅有締結契約客戶之基本資料，尚包括為通訊秘密所保護之通訊履歷甚至通訊內容、位置資料、帳單資料等，性質不同、重要性〈要保護性〉各異之個資，並非僅為普通法之個資法即得以完全應對。尤以近年因電腦網路普及，及通訊科技日新月異，通訊方式已不拘於傳統固定線路之語音傳遞，電信事業藉由加值網路提供通信以外如電子郵件、上網、下載圖鈴等各種服務，然也因此得以蒐集、儲存用戶或利用人更多如閱覽履歷等新類型個資。為補足個資法不足之處，加強利用電信服務通信者之個資保護；為本計畫研究對象之各外國，多以個人資料保護之基本原則為基礎，再如第三章所介紹，針對電信通信業之蒐集、處理或利用個資，制定特別法或或頒布行政法規加以規範。

二、保護個資之類型化

依第三章所介紹歐盟及各國有關規範電信事業保護個資之法規時，可得知一共通處，亦即其保護之個資均予以類型化，然後再分別明定其蒐集、處理或利用之要件。

而在綜合比較各國之法規後，雖因各國用詞及翻譯有不同，但觀其定義乃相同之概念，故大至上可將被列舉特別保護之個資整理如下：

1、通信履歷-----歐盟稱「通訊資料〈Traffic Data〉2002/58/EG 定義於第 2 條第 b 項；詳細規定在第 6 條」、「涉及電信事業用戶使用電信服務之數量、技術規格、型態、目的地與總額之資訊」屬「用戶專屬線路資訊〈Customer Proprietary Network Information)」之一部分、德國稱「使用資料〈Nutzungsdaten〉」(電子媒體法第 15 條第 1 項）或「通信資料〈Verkehrsdaten 〉」(電信通訊法第 96 條第 1 項)、英國稱「瀏覽履歷〈如 cookie, 2003 Regulations, 第 6 條第(1),(2)款〉」及「流量資料〈traffic data, 2003 Regulations, 第 7 條〉」、日本稱「通信履歷」。

2、使用者資料----歐盟稱「發話與受話者之來電顯示及拒示(Presentation and

restriction of calling and connected line identification)」2002/58/EG 第 8 條、英國稱「來電顯示與拒示〈calling or connected line identification, 2003 Regulations, 第 10, 11 條〉」、德國稱「來電顯示與拒示〈 Rufnummeranzeige und-unterdrückung〉」(電信通訊法第 102 條)、日本稱「發信人資料」、美國稱「用戶專屬線路資訊〈Customer Proprietary Network Information)」。

3、位置資料-----歐盟稱「位置資料〈Location Data〉」、美國稱「 位置資訊〈location information〉」、德國稱「位置資料〈Standortsdaten〉」(電信通訊法第 98 條)、英國稱「位置資料〈Location Data, 2003 Regulations, 第 14 條〉」、日本稱「位置資料」。

4、帳單資料------歐盟稱「計費明細〈Itemised Billing〉 2002/58/EG 詳細規定在第 7 條中 」、英國稱「帳單資料〈itemized billing, 2003 Regulations, 第 9 條〉」、德國稱「通話明細〈Einzelverbindungsnachweis〉」(電子媒體法第 15 條；電信通訊法第 99 條)、日本稱「利用明細」、美國稱「帳單資訊」〈information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier〉。

對上開各類型個資，各國大多明定其蒐集要件須事前得到當事人同意，亦即採「opt-in」制；而對將其揭露或提供給第三人者，多限定在有特別要件，如為調查犯罪或緊急救助之需等事由下始得為之。

三、發展趨勢及特別之規範

一般而言，各國現行對電信事業之有關個資保護之規範，多仍限定在傳統一對一、具有非公然性之包括語音與文字通信領域，至於一對多之具有公然性之通信如 BBS 公告欄、部落格或臉書(Face Book)等，則未納入規範。但因智慧型手機之普及，人人宛如手持小型電腦之終端機，在手機上上網閱讀新聞、查詢資料或地圖、甚至購物或觀看電視；如電信事業者透過提供之入口網站，設置軟體程式蒐集使用人瀏覽履歷，再分析出使用人上網之習性，如上網時間帶、常造訪之網頁、購物習慣、消費金額等，再用於特定商品行銷或開發市場；然因此亦為對使用人個資之蒐集，有侵害特定人隱私之虞；此外利用自動化撥號系統之電話行銷，或以電子郵件大量寄送廣告，亦常造成用戶之困擾，因而有國家特別對其訂立以下之規範。

(一) 瀏覽履歷〈cookie〉蒐集之規範

例如本研究報告第三章第三節英國之 2003Regulations 第 6 條第 1 項即明訂須對用戶或使用者，提供將儲存或讀取資訊之目的之完整訊息，並經用戶或使用者同意。而同章第二節德國電子媒體法第 15 條第 3 項於使用者未提出異議之前提下，以匿名方式基於廣告、市場調查或是形成電子媒體所需之目的，在使用者未表明異議之前提下，使用假名製作使用履歷（Nutzungsprofil），並應明確告知其所享有之異議權。歐盟於歐盟電信通訊個資保護指令(2002/58/EG)第 5 條 3 項中規定使用者或用戶必須在被告知明確資料瞭解個資處理目的時，和資料控管者有給予該用戶拒絕的權利時方得使用。

(二) 電話行銷之特別規定

英國於 2003Regulations 第 19 條規定，以預錄訊息利用自動化撥號系統進行電話行銷者，必須事先得到受話方之同意。而於現場以真人對話方式進行電話行銷者，依 2003Regulations 第 21 條規定，如該用戶已預先將其電話號碼登錄於電信主管機關依第 26 條建置之「請勿來電名冊」，則任何人不得撥打該電話進行行銷。再者，美國「電話消費者保護法」亦規定，除取得接收者之事前明示同意外，行銷業者不得於早上 8 點前或晚上 9 點後打電話、應保有要求不要再接到電話之消費者之「勿來電」(do-not-call)名單、以及禁止發送未經邀請之廣告傳真。

(三) 垃圾郵件

而英國對利用電子郵件寄送行銷廣告信件，於 2003Regulations 第 22 條規定限制，除在例外情況下，須事先得到收信當事人同意。日本如本報告前所介紹，雖有另立法規範垃圾信件發送，但又另於電信 GL 第 28 條規定，電信事業者間得交換濫發垃圾郵件用戶之名單，以阻絕惡性濫發電子郵件之用戶。德國於電子媒體法第 6 條第 2 項針對垃圾電子郵件（Spam）規定，如透過電子郵件寄發商業通信，信首及主旨不得掩飾或隱瞞寄件人及郵件訊息之商業本質，並於同法第 16 條第 1 項明訂違反上述規定者，最高可處 5 萬歐元罰鍰。美國「未經邀請而主動推介色情與市場銷售之侵犯管制法」要求美國聯邦通訊委員會應制定規範，以保護消費者免於接收不需要之行動服務之商業信件。

四、獨立監督機關之設置

如本報告第四章所說明，因歐盟及國際個人資料保護組織之指令或協約均明訂，各加盟國或加入組織之國家或區域均須於國內設置保護個人資料之獨立監督機關，除美國外因自始未制訂全面適用於非公務機關領域之個資法，而由聯邦貿易委員會以事後處罰之方式管制個資之合法蒐集、處理或利用，其餘英、德、韓及日本式均設有組織上獨立之個人資料保護監督機關，且具有下列特色：

(一) 獨立行使職權之機關

如英國之 IOC 依 DataProtection Act，附表 5，Part I，第 1 點，為獨立法人，僅對國會負責。德國之聯邦個人資料保護及資訊自由監察機構，係為首長制，雖其組織上隸屬於聯邦政府，但其首長及重要人事任命均由國會掌握，亦為獨立行使職權不受干涉。而韓國之「個人資料保護委員會」，則為直屬於大總統下所設之獨立機關。而日本則是在 2013 年藉個人編號法之立法，特別設計獨立於各行政機關外之「特定個人情報保護委員會」以監督「個人編號法」之運用，此為設置個人資料保護獨立監督機關之第一步，並預定以此為基礎，將來將擴展至全體公務機關及民間業者。德國聯邦個人資料保護法就非公務機關個人資料保護之監管，主要由聯邦資料保護與資訊自由監察機構（BfDI）負責，其首長為聯邦資料保護及資訊自由監察官，係由聯邦議會選任，得獨立執行職務不受干涉。

(二) 職權

各國立法賦予獨立監督機關之權限，範圍並不一致；一般而言均具有監督、調查個資法施行狀況之權限，對認定有違反個資法之機關等要求提出報告，或為改善措施;並得對機關提出有關個資法施行上及制度上之建議或接受有關之諮詢。且每年應向國會提出個資保護業務報告，並將報告對社會公布。

而韓國則另設個人資料糾紛調停委員會，介入調停公共機關與人民因個資處理所發生之紛爭。而德國聯邦個人資料保護及資訊自由監察機構，得接受人民因聯邦機關處理或利用其個資致其權利受損之申訴。

第五節　建議

依上四節所探討之我國問題，及在對各國相關法制作綜合分析後，本研究團

隊試圖對我國有關電信事業對個人資料之保護及其監管機制，依其實現所需時間之長短，提出以下短期得施行、中期得施行及長期可實現之建議，供有識之士參考。

一、短期得實施之建議（主辦機關：通傳會）

(一) 統整相關法規命令與明確化秘密通訊範圍：電信事業主管機關應將查閱通信紀錄及通信使用人資料，及用戶本人之查閱資料等相關規範，統整成一法規；將得查閱人，查閱之目的及要件、程序訂明。另外有關紀錄保存期限，應由現在分散為固定線路、行動電話等時限長短不一、個別法規規定方式，統整由一法規規定。

(二) 通訊秘密範圍之重新訂明：建議電信事業主管機關依司法院釋字第 631 號解釋，將秘密通訊範圍以法規命令予以重新明定，加入位置資料，改善現今與電信法規定有出入之處。在通信履歷部分應加入網路瀏覽紀錄，以符合現在智慧型手機發展之趨勢。

(三) 檢視各大電信公司隱私政策：請電信事業主管機關檢視各大電信公司隱私政策，是否有依照個資法第 8 條之項目宣示，以及重新審視其業務服務契約書上有關個資保護條款，是否依個資法第 8 條充分盡告知之義務，其不足之處，應輔導業者改善。另外應加強業者對個資法規定內容之理解，至少應定期要求各電信事業之法務人員，參加個資法之教育訓練及並對個資案例之法院判決作介紹、分析。

(四) 業者委外處理個資之輔導：業者多有委外處理帳單、代理與用戶訂契約或收取費率者，主管機關應依個資法施行細則第 8 條，明定業者委外契約中應訂明之事項，如：對受委託人有監督其合法處理個資之權利，限制其不得為特定目的外處理或利用、並對其處理之個資應盡保密義務及採取適當之安全維護措施。

(五) 明訂獎勵措施：建議電信事業主管機關考量後明訂獎勵業者取得個資保護認證標章之措施。

二、中期得施行之建議（共同主辦機關：通傳會、法務部）

(一)法規命令之訂立：電信事業主管機關與法律主管機關會商，參酌外國有關規

範電信事業蒐集、處理或利用個資之法令，依法規命令(如:電信事業個人資料保護辦法)先將電信事業所蒐集、處理或利用之個資類型化為:（1）通信紀錄、（2）用戶或使用者資料、（3）位置資料、（4）帳單資料等，再依個資法第 8 條、第 19 條、第 20 條分別定明其告知、蒐集、利用之要件。對前開通信紀錄、用戶或使用者資料等之蒐集，依現行個資法第 19 之規定，應於法律有明文規定，或與當事人有契約關係或類似契約關係下，始得無需當事人同意而為之。換言之，應採事前同意之 Opt-in 制，不應採事後選擇退出之 Opt-out 制。

(二)電信法相關法律之修正:電信法第 7 條第一項所訂電信業及其服務人員應保密之「電信之有無」與「內容」之用詞，建議修正為「通信紀錄」與「通信內容」。如此亦與通訊保障暨監察法之用詞一致，亦較原「通訊之有無」之定義清楚。

目的外利用要件之明訂：提供第三人其通信服務時所取得之個資，係屬典型之目的外利用，因涉及權利、及義務規定，故建議修正電信法第 7 條，將電信事業處理其提供第三人調閱、查詢通信內容、通信紀錄及使用者資料之事，配合通保法相關規定，明訂要件。亦即:

1、通信內容:須為符合通訊保障暨監察法第 5 條相關規定之要件者，須為特定事件，並經法院核准始得提供，採嚴格之「令狀主義」。

2、通信紀錄:明訂除經本人書面同意，或本人為契約履行、費率計算外，僅限於公務機關執行法定職務之必要範圍內，始得查詢。且除有因人之生命身體或財產遭受急迫危難之情事者，可事後由法院追認外，原則上應事前取得法院許可。

3、使用者資料查詢:因其規定內容涉及得查詢者資格及得查詢之要件規定，不宜依現在之「電信事業處理有關機關(構)查詢使用者資料實施辦法」規範，應將其位階提升為法律規定於電信法。

現行之「電信事業處理有關機關查詢通信紀錄實施辦法」及「電信事業處理有關機關(構)查詢使用者資料實施辦法」，留存申請程序及費用徵收方法即可。

(三)共同利用個資之規定:建議電信事業主管機關參照金融控股公司法修正前第 43 條，訂立電信事業與其子公司或關係企業共用用戶或使用人個資行銷時，僅限於該當當事人之姓名、住址，其他之資料應依個人資料保護法相關規定則不得共同利用。

(四)名單查詢機制之建立:建議電信事業主管機關依個資法第 19 條第 2 款及第 20 條但書第 4 款規定,且明定限制使用於審查契約目的下,電信事業得對欠繳費率、濫發電子郵件客戶或使用人,建立名單查詢之機制。

三、長期得實施之建議(主辦機關:行政院人事總處;協辦機關:通傳會)

(一)因智慧型手機之普及,有關電信事業以網路提供服務之營業項目,大量增加,除傳統語音、文字之通訊服務外,提供購物、小額付款、電視播放等服務項目,已屬擴展至商業、服務業領域之業務,故不屬於通傳會主管,形成同一家業者因經營事業項目不同,卻由不同行政機關主管之現況;另外網路上通信或傳播訊息之方法越來越多且方便迅速,如此之通訊常非為傳統特定人對特定人之訊息傳達,更有為具有公然性之通信者;面臨如此之發展,電信通訊與網路通訊是否應依同一法規規範之問題,此為國家在思考 IT(InformationTechnology)產業發展策略時,必須全面考量之課題。但不問是否整合由同一法律規範,對利用者個資之保護則仍應依現行個資法採一致之標準。

(二)獨立監督機關設置之建議

有關電信事業之監督機關,依現行之「主管機關制」自係由通傳會擔任,在監管資安之執行上應無困難,惟於涉及個資法條文適用上之疑慮時,恐仍須由法務部提供意見,大抵上不致有大問題。然依本研究報告第四章之第一節所說明之國際現況,基於國家長遠發展之觀點,本研究報告最終之建議,則仍以設置個資保護之獨立監督機關為最佳之選擇方向。而有關獨立監督關之組織方式、職權及我國現行法下等可能面臨之困境等建議如下。

1、 設置專責監督機關之理由

綜觀本研究計畫所調查研究之德國、英國、日本、韓國等四國,雖可能個資執行監督機關設置層級或其組織方式及掌有職權容有不同,惟至少是設有一專責機關在負責;亦如本研究報告第四章之第一節所說明之國際現況,除美國之外,幾乎各國均為個資法之執行設有獨立機關以為監督。當然其原因之一係因歐盟指令之要求,及為符合參加重要之有關個資保護國際會議之條件。然事實上歐盟如此規 定是有其深層之理由,亦為其他國家所認同,始能成為世界之趨勢。

(1) 法律解釋與適用上統一之必要

個資法適用範圍廣泛，為橫跨各領域包括公務機關與非公務機關、個人均受其規範之法律，所定之條文難免有概括難以理解之處，易於在適用上造成爭議；另外個資保護尚涉及資訊安全維護之部分，資安維護制度之建立與風險評價，應不分領域公私要求具備一定水準，依同樣之標準進行，凡此即不宜由各領域或業界之主管機關各自為政，自行應對處理，而應統一由專責機關監督執行，才可避免法解釋與適用之混亂，及安全維護標準之不一致之問題，且執法成本亦較低。

(2) 公正、中立執法之必要

因個資之蒐集、處理及利用，為現今政府行政管理，大企業行銷所必須者，而資料之當事人則僅為一般個人；換言之，當事人間資力常明顯不對等，尤其政府機關常不問當事人是否願意，基於執行職務之必要即得蒐集或利用，因此為避免政府機關濫用公權力不當蒐集或利用人民個資，並於人民不知情下利用於其未預見之目的上；或大企業利用不對等契約關係，過度蒐集消費者個資，用於行銷，故而必須有一獨立於政府機關外之監督機關以中立立場，在不受政治等外力干涉下，得監督政府機關或大企業依法蒐集、處理或利用個資，讓個資法之規範落實，以保障人民權益，或得對政府保護個資之政策或相關法令之修正提出建議。

(3) 跨國合作窗口單一化之必要

在電子商務發展蓬勃發展，及網路普及化之今日，跨國傳送個資已為日常商務活動之一環，個資蒐集、處理或利用，非僅限於一國國內之事，受個資所傳送之對方國家是否能保護個資安全、合法利用，自然成為保護個資之一環；又若侵害個資行為如發生於外國時，亦必須透過國際合作始有救濟之可能，故而國際間為區域之經濟發展，保護個資安全自由之傳遞，長時以來即為各國重要之課題；如本研究報告第四章第一節之說明，EU 等國際組織即每年召開有關個資之會議，討論加盟國間有關個資跨國傳送之共同規則，合作方式等議題。而我國參加之最重要國組織「亞洲太平洋經濟合作會議 Asia-Pacific Economic Cooperation ，APEC 」於 2010 年 7 月 16 日開始生效之「跨境隱私權執行協定」[627] ，依其會議資料所公布之四項目的，其一即為:為促進 APEC 區域隱私權執行機關間資訊之共有、及在隱私權保護法之執行上，設立促進隱私權執行機關間有效之跨境合作之機制，包

[627] APEC DATA PRIVACY SUBGROUP. APEC Cooperation Arrangement for Cross-Border Privacy Enforcement,2010/SPMI/ECSG/DPS/013(Feb.28,2010),http://aimp.apec.org/Documents/2010/ECSG/DPSI/10_ecsg_dps1_013.pdf.

含相關事務之照會、並行或共同調查或執行個資案件。而所謂「隱私權執行機關」係指擔負隱私權法之執行責任，為擁有權限以施行調查或進行執行程序之所有公務機關。從而為會員之我國有必要設置一個監督個資法執行之專責機關，其除為APEC之事務外，更能代表國家參加其他國際重要之有關個資保護會議，與各國交換個資保護之最新資訊、執法經驗，並得為國家與外國進行侵害個資法事件之共同調查或司法合作執行之聯絡、談判窗口，此較之由各機關各自進行所轄事務之國際合作，將更能代表國家表達政策或意見且具有效率。

2、 組織方式

應以委員制較適合，蓋個資之蒐集、處理及利用，涉及政府機關行政管理、民間業者經營事業之利益、或傳播、出版之表現自由、甚至學術研究等公共利益，在與保護個人之資訊自主權間如有衝突時，如何衡量取捨則是需要多方意見反映各種不同之價值觀，並得到多數人之認同，故以委員制之方式，遴選能代表社會各領域專家(包括業界及消費者)及法律、資訊技術之學者組成委員會負責監督個資法之施行應較能作出公正、不偏頗之決定。

3、 獨立監督機關之職權

對監督對象機關等蒐集處理或利用個資之事務，參酌前述歐盟及日本之例，得對政府提出有關個資保護政策、修法建議，對監督對象進行檢查及聽取報告並給予建議、命令改善，得代表國家參加國際會議、與外國商談個資法執行之合作，應為基本之職權；是否得介入當事人間調解紛爭，甚至代表資料當事人進行訴訟？關於此問題，依現行個資法已有團體訴訟制度之設計，似無需後者之職權，然於訴訟前如得介入協調，在考量減少訟源下則有必要。

4、 設置獨立監督機關之缺點及在我國將面臨之困難與可能之選擇

(1) 難以了解各行業或領域個資利用之實際狀況

因幾乎所有公務機關或業界均涉及個資蒐集、處理或利用，且各有其不同之蒐集方法與利用目的，加諸所蒐集之個資上性質更大有差異，例如醫院、學校、銀行、旅遊業等，係自高敏感性之醫療資訊至一般連絡方式，當然是其目的事業主管機關最熟知其蒐集與利用個資之方法，而能針對存在之問題進行有效監管。而獨立之監督機關則未必能完全掌握業界全部之狀況，能否切中問題進行調查或

輔導業者解決，作確實、有效之監督，並非無疑慮。

(2) 中央政府組織基準法之限制

依本研究報告第四章第一節所介紹之歐盟指令或歐洲理事會追加議定書之規定，及日本、韓國、英國等所設之個資監督機關，不問組織方式為何，不受任何其他政府機關指揮、監督，依法獨立行使職權之專責機關， 性質上與我國中央政府組織基準法第 3 條第 2 款所規定之獨立機關相符；而依同法第 32 條第 2 項之規定，得設立之總數限定為三個，查我國現今設立之二級獨立機關則已有中央選舉委員會、公平交易委員會、國家通訊傳播委員會，換言之，在法律上已無再新設二級獨立機關之空間，勢必須要修改中央政府組織基準法始有可能性，而修法即可能引起各機關間權力之分配及政治上之角力，確有相當之難度。

(3) 現行可能之選擇

行政院為積極推動國家資訊通信安全政策,加速建構國家資訊通訊安全環境，提升國家競爭力，特設「國家資通安全會報」[628]。係由行政院副院長擔任召集人，委員為十八人至三十五人，除召集人、由行政院長指派之副召集人及國家安全會議諮詢委員兼任之協同副召集人為當然委員外，其餘委員由院長就推動資通安全之有關機關、直轄市政府副首長及學者、專家派(聘)兼之。其下設網際防護及網際犯罪偵防二體系;前者由行政院資通安全辦公室主辦,負責整合資安防護資源、推動資安政策等事務，而後者則由法務部主辦，負責防範網路犯罪、維護民眾隱私等事務，其下並設有個資保護及法制推動組。該會報已為資通訊安全相關技術及法律及執行面，建立一跨部會、產官交流平台，其實質任務偏重在資訊安全，及網路安全及犯罪之防範，對監督各機關或民間遵循個資法蒐集、處理或利用個資，未多作著墨，依其設置要點第 7 點原則上每半年召開一次會議，其能處理之事務或發揮之功能必有限；且依其組成方式各委員能否獨立行使職權，不受任何外力介入，尚非無疑慮。

但行政院下既有此專責單位之存在，在設置獨立監督機關有困難之情形下，退而求其次，可以其為基礎，先建構公務機關個資保護施行之監督機制。

亦即，增設體系，將原網際犯罪偵防體系下之個資保護及法制推動組，改為

[628] 請參閱行政院國家資通安全會報設置要點，及行政院國家資通安全會報組織架構。

監督個資保護施行體系，由法務部主辦。

其任務為：

- 檢討個人資料保護基本計畫、政策、制度與法令增修等事項。
- 調查各機關個人資料之蒐集與利用、個人資料保護法等實際施行情況、業務目的以外之個人資料利用、提供第三人等實際運作情況。
- 研究國外個人資料保護執行體系及個人資料保護法制主要動向。

然此僅為個資保護施行監督機制之起步，其組織方式及獨立性與歐盟等之要求，當然不符；依國際發展之現況，及考量個資法立法目的之實現，加入國際重要會議之必要性及迫切性下，仍建請行政院提議修法，再新設有關監督個資施行之獨立機關，實乃國家應認真思考之方向。

參考文獻

中文部分

專書

李惠宗，《憲法要義》，元照出版，2009 年版，台北。
李震山，〈論資訊自決權〉，收錄於《人性尊嚴與人權保障》，元照出版，2011 年 10 月，台北。
法務部編，〈德國聯邦個人資料保護法〉，收錄於《外國個人資料保護法規彙編》，法務部出版，2002 年，台北。
謝碩駿譯，〈「預防性電信監察」判決〉，《德國聯邦憲法法院裁判選輯（十四）》，司法院，2013 年 4 月，頁 1-30，台北。
陳新民，《憲法學釋論》，6 版，三民出版，2008 年 9 月，台北。
陳麗娟，《里斯本條約後歐洲聯盟新面貌》，2 版，五南，2013 年 3 月，台北。
黃昭元，〈無指紋則無身份證？換發國民身份證與強制全民捺指紋的憲法爭議分析〉，收錄於《民主、人權、正義：蘇俊雄教授七秩華誕祝壽論文集》，國際刑法學會台灣分會編，2005 年 9 月，頁 461-508，台北。
詹鎮榮譯，〈「電信通信記錄」判決〉，《德國聯邦憲法法院裁判選輯（十一）》，司法院，2004 年 10 月，頁 247-271，台北。
蕭文生譯，〈關於「1983 年人口普查法判決」〉，《西德聯邦憲法法院裁判選輯（一）》，司法週刊雜誌社印，1990 年，台北。

期刊

王廷俊，〈國內第二類電信事業經營現況與問題探討〉，《通訊雜誌》，第 59 期，1998 年 12 月，頁 76-77。
王服清，〈里斯本條約對歐盟組織與法律架構之影響與調整〉，《憲政時代》，第 38 卷 2 期，2012 年 10 月，頁 173-214。
王勁力，〈新版個資法的衝擊與影響：論我國公務機關對特種個資的管控與監督〉，

《科技法律評析》，第 4 期，2011 年 12 月，頁 63-110。
王郁琦、林雅惠，〈我國電信事業分類規範之探討─以網路電話為例〉，《月旦法學雜誌》，第 102 期，2003 年 11 月，頁 128-146。
王郁綺、張家慧，〈網路語音服務在現代電信管制架構下的政策與法律爭議〉，《萬國法律》，第 114 期，2001 年 12 月，頁 25-37。
田炎欣，〈個人資料保護法「目的拘束原則」對新聞報導的限制〉，《中央警察大學犯罪防治學報》，第 18 期，2013 年 12 月，頁 77-96。
田炎欣，〈警察偵查犯罪侵害個人資料保護法「目的拘束原則」之探討(上) 〉，《台灣法學雜誌》，第 256 期，2014 年 9 月，頁 85-94。
田炎欣，〈警察偵查犯罪侵害個人資料保護法「目的拘束原則」之探討(下) 〉，《台灣法學雜誌》，第 257 期，2014 年 10 月，頁 85-95。
石世豪，〈電信自由化下通訊安全規範的轉型趨勢─通信秘密、個人資料保護與電信事業的管制變革〉，《全國律師》，第 9 卷第 5 期，2005 年 5 月，頁 32-51。
江耀國，〈無限寬頻接取應用服務之電信監理分析〉，《科技法律透析》，第 24 卷第 1 期，2012 年 1 月，頁 28-45。
吳兆琰，〈網路環境下的監察法制〉，《科技法律透析》，第 17 卷第 2 期，2005 年 2 月，頁 36-62。
李婉萍，〈個人資料保護脈絡下的「綑綁式同意」〉，《科技法律透析》，第 24 卷第 1 期，2012 年 1 月，頁 18-41。
李婉萍，〈歐盟個資小組對「目的拘束原則」之詮釋及該詮釋對界定個資法上「特定目的」之啟發〉，《科技法律透析》，第 25 卷第 9 期，2013 年 5 月，頁 18-24。
李惠宗，〈個人資料保護法上的帝王條款—目的拘束原則〉，《法令月刊》，第 64 卷 1 期，2013 年 1 月，頁 37-61。
李惠宗，〈裁判書上網公開與個人資訊自決權的衝突〉，《月旦法學雜誌》，第 154 期，2008 年 3 月，頁 21-34。
李榮耕，〈現行通訊保障監察法制的困境及去路〉，《司法改革雜誌》，第 99 期，2013 年 12 月，頁 22-25。
李榮耕，〈論偵察機關對通信紀錄的調取〉，《政大法學評論》，第 115 期，2009 年 10 月，頁 115-147。
周慧蓮，〈論行動化生活之資訊隱私侵害─以定位服務為例〉，《月旦法學雜誌》，

第 99 期，2003 年 8 月，頁 152-165。
周慧蓮，〈電信法中關於網際網路服務提供者權義規範簡析〉，《科技法律透析》，第 16 卷第 8 期，2004 年 8 月，頁 10-14。
林三欽，〈通訊監察與秘密通訊自由〉，《憲政時代》，第 23 卷第 2 期，1997 年 3 月，頁 4-50。
林達峰，〈行動生活之隱私爭議─現行法制能否妥善處理位置資訊衍生問題〉，《科技法律透析》，第 18 卷第 6 期，2006 年 6 月，頁 44-61
邱文聰，〈從資訊自決與資訊隱私的概念區分─評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，第 168 期，2009 年 5 月，頁 172-189。
邱伊翎，〈OECD 關於個人資料保護的八大原則〉，《TAHRPAS 報 7 月號》，2008 年 7 月，頁 6。
洪聖濠，〈行動定位服務中的位置資料隱私保護〉，《科技法律透析》，第 17 卷第 1 期，2005 年 1 月，頁 8-13。
張乃文，〈解析個人資料國際傳輸之法規範趨勢〉，《萬國法律》，第 181 期，2012 年 2 月，頁 33-41。
郭戎晉，〈論數位環境下個人資料保護法制之發展與難題─以「數位足跡」之評價為核心〉，《科技法律透析》，第 24 卷第 4 期，2012 年 4 月，頁 18-39。
陳秭璇，〈我國個資法對於國際傳輸之限制〉，《科技法律透析》，第 25 卷 12 期，2013 年 12 月，頁 20-25。
陳銘祥，〈電信規範體制之探討〉，《經社法制論叢》，第 23 期，1999 年 1 月，頁 61-81。
陳銘祥，〈衛星通信法律規範之研究〉，《經社法制論叢》，第 26 期，2000 年 7 月，頁 31-61。
廖淑君，〈智慧聯網之發展與個人資訊隱私保護課題：以歐盟之因應為例〉，《科技法律透析》，第 23 卷 11 期，2011 年 11 月，頁 18-42。
廖緯民，〈資安政策與法律課責─兼論我國 2010 年個人資料保護法中的資安政策管理體制〉，《前瞻科技與管理》，第 2 卷第 2 期，2012 年 11 月，頁 37-51。
劉孔中，〈關於電信管制政策與法規的一些檢討意見〉，《萬國法律》，第 114 期，2000 年 12 月，頁 12-24。
劉孔中、趙晞華，〈通訊保障及監察法修正意旨之辯證與再修正方向之檢視〉，

《軍法專刊》，第 60 卷第 3 期，2014 年 6 月，頁 37-48。
劉定基，〈欺罔與不公平資訊行為之規範--以美國聯邦交易委員會的管制案為中心〉，《公平交易季刊》，第 17 卷第 4 期，2009 年 10 月，頁 57-91。
劉定基，〈個人資料的定義、保護原則與個人資料保護法適用的例外─以監視錄影為例(上) 〉，《月旦法學教室》，第 115 期，2012 年 5 月，頁 42-54。
劉定基，〈個人資料的定義、保護原則與個人資料保護法適用的例外─以監視錄影為例(下) 〉，《月旦法學教室》，第 119 期，2012 年 9 月，頁 39-53。
劉靜怡，〈不算進步的立法：「個人資料保護法」初步評析〉，《月旦法學雜誌》，第 183 期，2010 年 8 月，頁 147-164。
劉靜怡，〈通保法究竟保障了誰？〉，《司法改革雜誌》，第 99 期，2013 年 12 月，頁 30-33。
蔡美智，〈「通訊保障及監察法」關於網路監聽的相關爭議〉，《資訊法務透析》，第 11 卷第 12 期，1999 年 12 月，頁 32-45。
蕭奕弘，〈論個人資料保護法的法制性問題〉，《成大法學》，第 23 期，2012 年 6 月，頁 141-191。
顏婉旬，〈防災應變之挑戰─談關鍵基礎設施保護〉，《科技法律透析》，第 23 卷第 8 期，2011 年 8 月，頁 13-18。
顏婉旬，〈資訊安全與電子商務─談資訊安全通報機制〉，《科技法律透析》，第 23 卷第 11 期，2011 年 11 月，頁 43-63。
蘇文萱、李科逸，〈產業研發投入智慧能源於隱私保護與資安因應建議-以歐盟動法制政策為研析〉，《科技法律透析》，第 24 卷 12 期，2012 年 12 月，頁 48-62。

學位論文

徐弘昌，《以 ISO27001 為基礎評估電信業資訊安全管理─以第一類電信業者為例》，國立交通大學管理學院碩士在職專班管理科學組，碩士論文，2009 年 6 月。
鄭伊雯，《植基於 ISO27001 建立符合 BS10012 之個人資訊自我評鑑模式》，中原大學碩士論文，2012 年 7 月。
蘇三榮，《網路時代通訊監察與個人資料保護之法制研究》，國立交通大學科技法律研究所碩士論文，2009 年 6 月。

研討會論文

程明修，〈政府資訊蒐集與隱私權-以德國聯邦憲法法院「儲備性資料存取案」判決之發展為中心〉，司法院大法官一百年度學術研討會，主題「憲法解釋與隱私權之保障」，司法院主辦， 2011 年 12 月 3 日，頁 1-30。

黃舒芃，〈歐盟基本權利憲章對各會員國之拘束：由新近實務發展與理論爭議反思基本權利保障在歐盟的實踐途徑〉，歐洲聯盟法律專書研討會，臺灣歐洲聯盟中心主辦，臺灣大學社會科學院第一會議室，2014 年 5 月 17 日，頁 26-53。

蔡宗珍，〈通信記錄強制提供義務之基本權關聯性：BVerfGE 125, 260 與 BVerfGE 130, 151 判決評析〉，第二屆翁岳生教授公法研討會：德國聯邦憲法法院 2010-2013 年重要判決之研究，臺灣大學法律學院公法研究中心主辦，2014 年 6 月 14 日，頁 1-25

蔡宗珍，〈憲法人格權之保障及其界限-兼論網路人格權保護之憲法挑戰〉，第 9 屆憲法解釋之理論與實務學術研討會，中央研究院法律學研究所，2013 年 6 月 21、22 日，頁 1-23。

研究報告

財團法人資訊工業策進會，《公務機關個人資料保護方案計畫研究成果報告》，法務部委託研究，2012 年 5 月。

章毓群，《服務業科技應用之個人隱私權保護相關法制之研究》，行政院經濟建設委員會委託研究，2004 年 12 月。

潘維大、余啟民、黃心怡、張錕盛，《資訊服務業者配合政府公權力提供客戶資料之法制研究》，行政院經濟建設委員會委託研究，2006 年 12 月。

日文部分

專書

田島泰彦、三宅弘編，個人情報保護法，明石書店，2003 年。

田島泰彦編，「個人情報保護法と人権」，明石書店，2002 年。

石井夏生利，個人情報保護法の理念と現代的活動，勁草書房，2008 年。

宇賀克也,「個人情報保護法の逐条解説」(2 版),2005 年。
宇賀克也,個人情報保護法の逐条解説(第 3 版),有斐閣,2009 年 4 月。
宍戸常寿,通信の秘密に関する覚書,高橋和之古稀紀念論文集「現在立憲主義の諸相」(下),有斐閣,2013 年 12 月。
岡村久道,個人情報保護法,新訂版,商事法務,2009 年。
高橋和之,立憲主義と日本國憲法,第 3 版,有斐閣,2013 年。
園部逸夫 編,個人情報保護法の解說,改訂版,ぎょうせい,2005 年。
藤原静雄,「逐條個人情保護法」,弘文堂,2003 年。

期刊與其他資料

関本貢,プライバシーマークー制の運用状況,法律のひろば,2003 年。
張睿英,韓國における個人情報保護法制の問題と改善案,The journal of Environmental and Information Studies, Tokyo City University (11), 39-46(2010).
藤原静雄、個人情報保護に関する制度の整備、ジュリスト,N0.1287,2005 年。
藤原静雄,個人情報保護法に関する制度の整備ーその成果と課題,ジュリスト No.1287,2005 年。
堀部政男,社会保障・税番号大綱と個人情報保護―行政との関連性の検討,季刊情報公開・個人情報保護,2011 年 9 月。
堀部政男,電気通信分野の個人情報保護に見る世界の潮流とわが国の取り組み,法律文化,2004 年。
崔祐溶,韓國の個人情報保護法の内容と個人情報保護管理体系。http://in-law.jp/archive/kenkyukai/2012-02-18/che.pdf
電気通信事業における個人情報保護に関するガイドラインの解説,資料網址 http://www.soumu.go.jp/main_content/000254520.pdf

英文部分

英文書籍

Stuart Minor Benjamin, Douglas Gary Lichtman, Howard A. Shelanski & Philip J.

Weiser, Telecommunications Law And Policy (2006).
Fred H. Cate, Privacy in Perspective (2001).
Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change-Recommendations for Businesses and Policymakers (March 2012).
Daniel J. Solove and Marc Rotenberg, Information Privacy Law (2003).
Daniel J. Solove, The Digital Person: Technology and Privacy in the information Age (2004).
Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (1998).
Jody R. Westby, American Bar Association, International Guide to Privacy (2004).

英文期刊

Fred H. Cate, Privacy and Telecommunications, 33 Wake Forest L. Rev. 1(Spring 1998).
Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 Ind. L. Rev. 173 (1999).
David A. Castor, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 Ind. Int'l & Comp. L. Rev. 265 (2002).
Leah E. Capritta, COMMUNICATIONS LAW: U.S. WEST, INC. V. FCC INTERPRETS THE FIRST AMENDMENT RAMIFICATIONS OF "CUSTOMER PROPRIETARY NETWORK INFORMATION," 77 Denv. U. L. Rev. 441 (2000).
Nancy J. King, DIRECT MARKETING, MOBILE PHONES, AND CONSUMER PRIVACY: ENSURING ADEQUATE DISCLOSURE AND CONSENT MECHANISMS FOR EMERGING MOBILE ADVERTISING PRACTICES, 60 Fed. Comm. L.J. 229 (March, 2008).
Lynn Chuang Kramer, *PRIVATE EYES ARE WATCHING YOU: CONSUMER ONLINE PRIVACY PROTECTION-- LESSONS FROM HOME AND ABROAD*, 37 Tex. Int'l L.J. 387 (Spring 2002).
David J. Phillips, BEYOND PRIVACY: CONFRONTING LOCATIONAL SURVEILLANCE IN WIRELESS COMMUNICATION, 8 Comm. L. & Pol'y 1(Winter, 2003).

Henry H. Perritt, Jr. & Margaret G. Stewart, *False Alarm?*, 51 Fed. Comm. L.J. 811(May, 1999).

Antonia Runac, CONTROL OVER PERSONAL INFORMATION: WHO HAS IT, THE CONSUMER OR THE INDUSTRY?, 12 Loy. Consumer L. Rev. 68(1999).

Joel R. Reidenberg, *PRIVACY WRONGS IN SEARCH OF REMEDIES*, 54 Hastings L.J. 877 (April, 2003).

Simon Stokes, "A decision to quickly forget; Google Spain and Google on the right to be forgotten" , 25(7) Ent LR (2014).

Steven R. Salbu, *Corporate Governance, Stakeholder Accountability, and Sustainable Peace: The European Union Data Privacy Directive and International Relations*, 35 Vand. J. Transnat'l L. 655 (March, 2002).

Suzanna Shaub, *USER PRIVACY AND INFORMATION DISCLOSURE: THE NEED FOR CLARITY IN "OPT-IN" QUESTIONS FOR CONSENT TO SHARE PERSONAL INFORMATION*, 5 Shidler J. L. Com. & Tech. 18 (Spring, 2009).

Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 Yale J. Int'l L. 1(Winter, 2000).

Daniel J. Solove & Woodrow Hartzog, *THE FTC AND THE NEW COMMON LAW OF PRIVACY*, 114 Colum. L. Rev. 583 (April, 2014).

Brown, Ian and Korff, Douwe, Foreign Surveillance: Law and Practice in a Global Digital Environment (April 30, 2014). European Human Rights Law Review 3: 243-251. Available at SSRN: http://ssrn.com/abstract=2521433

European Union Agency for Fundamental Rights, *Handbook on European data protection law,* 61-101 (Jan. 2014).

Kourtrakos, Panos, To strive, to seek, to Google, to forget, 3 E.L. Rev. 293(2014).

Ausloos, Jef, *The 'Right to be Forgotten' e Worth remembering?*, 28 Computer Law & Security Review 143 (2012).

Available at:

http://ac.els-cdn.com/S0267364912000246/1-s2.0-S0267364912000246-main.pdf?_tid=f6c43e6c-635f-11e4-97bb-00000aacb35d&acdnat=1415022636_861e31ad49273ad17f8

e7d4e274b1e12
Cheung, Anne S.Y., *Location privacy: The challenges of mobile service devices*, 30 Computer Law & Security Review 41 (2014).
Available at:
http://ac.els-cdn.com/S026736491300201X/1-s2.0-S026736491300201X-main.pdf?_tid=2727ac60-6360-11e4-9833-00000aacb361&acdnat=1415022715_3fd722847fd921b0e23b554f406be0fe
King, Nancy J. &Pernille Wegener Jessen, *Profiling the mobile customer e Privacy concerns when behavioural advertisers target mobile phones e Part I*, 26 Computer Law & Security Review 455 (2010).
Available at:
http://ac.els-cdn.com/S0267364910001044/1-s2.0-S0267364910001044-main.pdf?_tid=e0757a10-635d-11e4-9ce4-00000aab0f27&acdnat=1415021737_c4e551fcf9b821cbe9fa67b9d25c04cf
Jones, Richard &DalalTahri, *An overview of EU data protection rules on use of data collected online*, 27 Computer Law & Security Review 630(2011).
Available at:
http://ac.els-cdn.com/S0267364911001488/1-s2.0-S0267364911001488-main.pdf?_tid=5760a6ca-6356-11e4-9337-00000aacb35f&acdnat=1415018501_a2526288692b4593166b3136bd95a175
Vagelis Papakonstantinou & Paul de Hert, *The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implentation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights*, 29 J. Marshall J. Computer & Info. L. 29 (2011).
Available at: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1698&context=jitpl
Rebecca Wong, *Data protection: The future of privacy*, 27 Computer Law & Security Review 53, 56 (2011).
Available at:
http://ac.els-cdn.com/S0267364910001718/1-s2.0-S0267364910001718-main.pdf?_tid=639d78dc-6356-11e4-b82f-00000aab0f02&acdnat=1415018521_bdd95424794e5baf446

c9508d6d1e205
Papakonstantinou, Vagelis& Paul De Hert, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, 28 Computer Law & Security Review 130 (2012).
Aavailable at:
http://ac.els-cdn.com/S0267364912000295/1-s2.0-S0267364912000295-main.pdf?_tid=9ff91b70-6355-11e4-9ce4-00000aab0f27&acdnat=1415018193_f63edad57f238d77af4e84aadc6edd02
Paul M. Schwartz and Danie J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877 (2014).
Available at: http://scholarship.law.berkeley.edu/californialawreview/vol102/iss4/7
Raffaele Zallone, *Here, There and Everywhere: Mobility Data in the EU (Help Needed: Where is Privacy?)*, 30 Santa Clara High Tech. L.J. 57 (2014).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol30/iss1/3

其他英文文獻

Julia Angwin, Shayndi Raice & Spencer E. Ante, Facebook Retreats on Privacy, The Wall Street Journal, November 11, 2011.
Available at
http://online.wsj.com/article/SB10001424052970204224604577030383745515166.html?mod=WSJ_hp_us_mostpop_read
Federal Trade Commission, Privacy Online: A Report to Congress 62 (1998).
Available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf
FTC, Protecting Consumer Privacy in an Era of Rapid Change- A Proposed Framework for Businesses and Policymakers.
Available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
The Telecommunications Act of 1996, Pub. L. No. 104-104.
Available at
http://www.gpo.gov/fdsys/pkg/PLAW-104publ104/pdf/PLAW-104publ104.pdf

Ed Hightower, US Supreme Court rejects unlimited warrantless cell phone searches, World Socialist Web Site.
Available at http://www.wsws.org/en/articles/2014/06/26/cell-j26.html
In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Second Report and Order and Further Notice of Proposed Rulemaking ("CPNI Order"), February 19, 1998.
Available at
http://transition.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt
Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,(FCC Third Report and Order and Third Further Notice of Proposed Rulemaking July 25, 2002)
Available at http://www.steptoe.com/assets/attachments/1655.pdf
Article 29 Data Protection Working Party, *Working Party 29 Opinion on the Use of Location Data with a View to Providing Value-Added Services*, 2005 2130/05 (WP 115) (EN).
Available at
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf
Brown, Ian, *The challenges to European data protection laws and principles, Working Paper No.1 for a "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, European Commission, 2010.
Available at:
http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_1_en.pdf
Directive 1995/46/EC of 24 October 1995 on protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23/11/1995, 31-50).
Directive 1997/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the

telecommunications sector (OJ L 24, 30/01/1998, 1-8).
Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector (OJ L 201, 31/07/2002, 37-47).
Emily Steel, *WPP's digital ad arm pushes into China*, Financial Times (last visited; Nov. 15, 2014).
ECJ Digital Rights Ireland Ltd v Minister for Communications, Joined Cases C-293/12 &C-594/12, (8 April 2014).
Available at
http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=192360
ECJGoogle Spain SL, Google Inc.vAgencia Española de Protección de Datos (AEPD), C-131/12, (13 May 2014).
Available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN (last visited: Nov. 15, 2014).
C-486/12, Judgment of the Court Eighth Chamber (12 December 2012).
Available at:
http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0486&lang1=en&type=TXT&ancre=
Deutsche Telekom AG v Bundesrepublik Deutschland, Case C-543/09, Judgment of the Court Third Chamber (5 May 2011).
Available at:
http://curia.europa.eu/juris/celex.jsf?celex=62009CJ0543&lang1=en&type=TXT&ancre=
Google Spain and Google v AEPD (C-131/12) [2014] E.C.D.R. 16.at [80].
Institutprofessionnel des agentsimmobiliers (IPI) v Geoffrey Englebert, Case C‑473/12, Judgment of the Court Third Chamber (7 November 2013).
Available at:
http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0473&lang1=en&type=TXT&ancre

=
International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy-The Madrid Solution* (Nov. 5, 2009).
Available at:
http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf
Josef Probst v mr.nexnet GmbH, Case C 119/12, Judgment of the Court Third Chamber (22 November 2012).
Available at:
http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0119&lang1=en&type=TXT&ancre=
New EU data protection laws: European Parliament proposes restrictive data protection laws in Europe C.T.L.R. 2014, 20(2), 64.
Search removal request under data protection law in Europe, Google, available at:
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en
Sullivan, Danny, How Google's New "Right To Be Forgotten" Form Works: An Explainer, Search Engine Land (May 30, 2014).
Available at: http://searchengineland.com/google-right-to-be-forgotten-form-192837 .
The right to privacy catches up with search engines: the unforgettable decision in Google Spain v AEPD C.T.L.R. 2014, 20(5), 131.
Vincent, James, Google begins implementation of 'right to be forgotten' ruling with online takedown form, The Independent (May 30, 2014).
Available at:
http://www.independent.co.uk/life-style/gadgets-and-tech/google-begins-implementation-of-right-to-be-forgotten-ruling-with-online-takedown-form-9459209.html
ICO, The Guide to Data Protection, available at:
http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf
ICO, Data sharing code of practice, available at:

http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx
ICO, Notification of Data Security Breaches to the ICO, available at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/breach_reporting.ashx

德文部分

Bull, Hans-Peter, Informationelle Selbstbestimmung- Version oder Illusion, 2. Auflage, 2011
Bumke, Christian/Voßkuhle, Andreas, Casebook Verfassungsrecht, 5.Auflage, 2008
Durner, Wolfgang, Anmerkung zu EuGH, Urteil vom 08. 04. 2014- C-293/12 und C-594/12, Deutsches Verwaltungsblatt 11 (2014), S.712-715
Jotzo,Florian, Der Schutz personenbezogener Daten in der Cloud, 2013
Kruse, Julia, Der Ö ffentlich-rechtliche Beauftragte,2007
Manssen, Gerrit, Staatsrecht II Grundrechte, 5.Auflage, 2007
Meyer, Jürgen(Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage, 2004
Pieroth, Bodo/ Schlink, Bernhard, Grundrechte, Staatsrecht II, 24. Auflage, 2008
Plath, Kai-Uwe(Hrsg.), BDSG, Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, 2013
Rossi, Matthias, AnmerkungzuEuGH, Urteilvom 10. Februar 2009- C-301/06, Zeitschriftfür das JuristischeStudium 3 (2009), S.298-299
Roßnagel, Alexander/ Moser-Knierim, Antonie/ Schweda, Sebastiasn,
InteressenausgleichimRahmen der Vorratsdatenspeicherung, 2013
Rößner, Sören, Vorratsdatenspeicherung in Deutschland- Ende des Umsetzungsdefizits in Sicht? EuropäischeZeitschriftfürWirtschaftsrecht 4 (2014), S.134-138
Simits, Spiros(Hrsg.), Bundesdatenschutzgesetz, 6. Auflage, 2006
Stein, Torsten/ von Buttlar, Christian, Völkerrecht, 12. Auflage, 2009
Tinnenfeld, Marie-Theres/ Buchner, Benedikt/ Petri, Thomas, Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 5.

Auflage,2012
Westphal, Dietrich, Kommentar zu EuGH,Vorratsdatenspeicherung,
Kommunikation&Recht 6（2014）, S.410-413
Wohlgemuth, Hans H./ Gerloff, Jürgen, Datenschutz, 3. Aufl., 2005
Wolff, Heinrich Amadeus, Vorratsdatenspeicherung- Der
GesetzgebergefangenzwischenEuroparecht und Verfassubng?
NeueZeitschriftfürVerwaltungsrecht 12 (2010), S.751-753
Wolff, Heinrich Amadeus/ Brink, Stefan, Datenschutzrecht in Bund und die Ländern, 2013
Zöllner, Dieter, Der DatenschutzbeauftragteimVerfassungssystem, ,1995

附錄一 第一類電信事業經營者名單暨其業務項目

製表日:103/11/05

序號	經營者名單	業務項目									
		固定通信網路業務				行動通信網路業務					衛星固定通信業務
		綜合網路業務	國際海纜電路出租業務	市內、國內長途陸纜電路出租業務	市內網路業務	行動寬頻業務	無線寬頻接取業務	第三代行動通信業務	行動電話業務	數位式低功率無線電話業務（一九〇〇兆赫）	
1	三大有線電視			V							
2	三冠王有線電視			V							
3	大屯有線電視			V	V						
4	大台北區瓦斯			V							
5	大安文山有線電視			V							
6	大眾電信						V			V	
7	大揚有線電視			V							
8	大新店民主有線電視			V							
9	大豐有線電視			V							
10	大同電信						V				
11	中投有線電視			V	V						
12	中華電信股份有限公司	V				V		V	V※		V

13	天外天有線電視			V							
14	世新有線電視			V							
15	北亞環球光纖通訊網絡		V								
16	北桃園有線電視			V							
17	北健有線電視			V							
18	北港有線電視			V							
19	北視有線電視			V							
20	台亞衛星通訊										V
21	台灣大哥大			V		V		V	V ※		
22	台灣中油			V							
23	台灣固網	V									
24	台灣國際纜網通信		V								
25	台灣數位寬頻有線電視			V							
26	台灣基礎開發科技				V						
27	永佳樂有線電視			V							
28	全球光網電訊		V								
29	全聯有線電視			V							
30	全球一動						V				
31	吉元有線電視			V							
32	吉隆有線電視			V							
33	台灣佳光電訊			V	V						
34	亞太電信	V						V			
35	佳聯有線電視			V	V						
36	侑瑋衛星通訊										V
37	東台有線電視事業			V							
38	東亞有線電視			V							

39	欣中天然氣			V							
40	金頻道有線電視			V							
41	長德有線電視			V							
42	信和有線電視			V							
43	南天有線電視			V							
44	南桃園有線電視			V							
45	南國有線電視			V							
46	威寶電信							V			
47	屏南有線電視			V							
48	紅樹林有線電視			V							
49	洄瀾有線電視			V							
50	家和有線電視			V							
51	國際環球通訊網絡		V								
52	國聲有線電視			V							
53	港都有線電視			V							
54	華人衛星網路										V
55	陽明山有線電視			V							
56	新世紀資通	V									
57	新台北有線電視			V							
58	新永安有線電視			V							
59	新竹振道有線電視			V							
60	新唐城有線電視事業			V							
61	新海瓦斯			V							
62	新視波有線電視			V							
63	新頻道有線電視			V							
64	萬象有線電視			V							

65	群健有線電視			V							
66	遠傳電信			V※		V	V	V	V ※		
67	鳳信有線電視			V							
68	慶聯有線電視			V							
69	聯禾有線電視			V							
70	聯維有線電視			V							
71	豐盟有線電視			V							
72	雙子星有線電視			V							
73	麗冠有線電視			V							
74	寶福有線電視			V							
75	觀天下有線電視事業			V							
76	觀昇有線電視			V							
77	威達雲端電訊			V	V ※		V				
78	威邁思電信						V				
79	台灣智慧光網				V						
80	台灣之星電信					V					
共計 80 家（107 張執照)		4	4	61	10	4	6	5	8	1	4

※	中華電信 2G 行動電話業務有 GSM900、DCS1800 各 1 張，共計 2 張執照
※	台灣大哥大 2G 行動電話業務有 2 張 GSM900、1 張 DCS1800，共計 3 張執照
※	遠傳電信 2G 行動電話業務有 1 張 GSM900、2 張 DCS1800，共計 3 張執照。陸纜電路出租業務(併和信電訊)有 2 張執照。
※	威達雲端電訊市內網路業務臺中市、彰化縣、雲林縣、南投縣共 4 張執照

附錄二 第二類電信業者名單及其營業項目

(103 年 12 月)

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
寶碩財務科技								V	V	V					
奇唯科技										V					
時報資訊									V	V					
凱衛資訊										V					
全球商業網								V		V					
關貿網路										V					
瑪凱電信	V	V		V	V			V	V	V	V	V	V		
先啟資訊系統								V	V	V					
宏碁				V	V			V	V	V	V				
倚天資訊								V		V					
天河電訊									V	V					
博訊科技					V			V	V	V		V			
英商路透台灣分公司				V				V	V	V					
比利時商訊達國際電訊網路台灣分公司					V			V	V	V		V			
台灣國際商業機器					V			V	V	V					
太聯科技					V			V	V	V					
偉盟系統									V	V					

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
優網通國際資訊										V					
香港商香港電訊台灣分公司					V	V		V	V	V		V			
香港商易廣國際電信台灣分公司	V				V	V		V	V	V		V			
台灣恩益禧								V	V	V					
家福								V	V	V					
協志聯合科技	V	V						V	V	V		V			
南頻電信	V	V					V	V	V	V	V		V		V
宏遠電訊	V	V			V		V	V	V				V		V
英商英國電信台灣分公司	V				V		V					V			
北台數網電訊	V	V		V	V			V	V	V					
台灣恩悌					V	V		V				V			
歐宜耳科技事業				V									V		
神乎科技										V					
萬宙商信	V				V	V	V	V			V	V			
慧訊國際									V	V					
財金資訊										V					
微傳電訊科技	V	V						V	V	V					
精誠資訊				V				V	V	V	V	V			
旭眾科技													V		

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
是方電訊	V	V	V	V	V	V		V	V		V	V			
台灣美訊國際通訊網路服務					V	V	V	V	V	V	V	V			
遠傳電信	V	V		V	V			V		V					
領航電信	V	V			V			V							
風騰國際事業													V		
神坊資訊	V	V			V			V		V	V				
祥碩興業													V		
和宇寬頻網路	V	V		V				V		V					
台灣世紀聯合通訊網絡					V			V	V	V					
統一資訊					V			V		V	V	V			
鼎基資訊電腦	V	V													
嘉實資訊										V					
大眾電信								V							
今網資訊科技								V							
香港商第一線台灣分公司					V	V	V	V			V	V			
仟晉資訊	V			V									V		
互聯通					V	V	V	V							
萬寶網路科技													V		
數位通國際網路								V							
敦緯數位服務								V		V					
達網國際	V	V						V	V						

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
三通網資訊	V	V													
台灣寬頻通訊顧問								V							
遊戲橘子數位科技								V							
易達通網路系統					V			V	V			V			
台灣大哥大	V	V			V			V	V	V					
美商易利康電信台灣分公司	V	V						V		V					
長進資訊	V	V													
全球光網電訊		V			V	V		V				V			
安碁資訊										V					
中嘉和網股份有限公司				V				V							
台灣碩網網路娛樂								V					V		
聯華電信	V														
聯維有線電視								V							
寶福有線電視								V							
世新有線電視								V							
中華國際通訊網路	V	V	V							V			V		V
優墾整合行銷		V		V									V		
天昱通													V		
康特國際	V	V													

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
統振				V											
環世通科技				V											
美商彭博新聞台北分公司									V	V					
台灣基礎開發科技		V	V					V							
遠達全球通訊	V														
大台北寬頻網路		V		V				V							
台灣亞太環通海纜						V									
英屬維京群島商新基電訊台灣分公司	V	V			V	V		V							
寰訊國際				V											
天外天有線電視								V							
上銀全通電訊	V	V												V	
康特國際	V	V													
統億電信				V											
松崗科技				V											
甲虫科技				V											
捷通電訊	V														
新通環宇	V					V		V				V			
中華聯合電信				V											
光寶匯才資訊								V							

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
服務															
嘉聯資通				V											
國際都會光網通信					V			V							
創意聯合				V											
鈞通國際				V											
偉傳電訊	V	V											V		V
神通電信科技				V											
通航國際電信				V											
大台南科技	V	V						V		V					
薛丁格				V											
大新店民主有線電視								V							
豐譽電信事業								V		V					
都訊聯合電訊	V	V		V											
便利達康				V											
台灣信通網絡	V	V				V				V					V
和記環球電訊						V		V							
三和電訊				V											
台灣斯普林特電信					V	V		V				V			
新加坡商都科摩英達特網絡台灣分公司								V							
真茂科技								V							

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
華勉科技				V				V							
艾德網科技				V									V		
三愛科技	V	V													
大大寬頻								V							
艾奇網路科技	V	V													
艾克斯電訊	V	V													
聯保科技								V							
廣聚科技	V	V		V											
呼風喚雨電訊				V											
華群科技							V			V	V		V		
京威電信				V											
互動在													V		
安源資訊								V	V	V			V		
雙盈通訊整合				V											
東豐科技						V		V		V	V				
泰富國際網絡					V	V		V							
寶潤資訊科技	V	V		V											
富爾特科技				V											
泛亞通通訊科技				V											
正源科技								V							
臺灣集中保管結算所									V	V					
台灣國際纜網	V				V			V							

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
通信															
達錡網訊科技				V											
全景電訊		V													
北亞環球光纖通訊網絡	V	V			V	V		V							
華通聯網	V														
僑興資訊		V								V					
偉僑	V	V													
聲采科技				V											
全網通科技	V		V	V											
精網資訊	V	V													
冠揚科技	V	V													
超時代電訊	V	V		V											
宅急網								V							
大師管理顧問				V											
芯盛資訊													V		
米瑟奇媒體				V											
亞述電信				V											
明欣科技網路								V							
士鑫國際寬頻				V											
先博通訊	V	V													
倚碩科技		V						V							
方陣策略													V		
東鑫電信				V											

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
有限公司															
優軟科技				V											
煌碁資訊				V											
中嘉寬頻								V							
標準網絡	V			V		V									
毅通網絡	V	V													
聯信華達網路服務		V													
亞洲標準電訊				V											
尖端電腦				V											
冠北電信網路科技				V											
創勝電訊網絡				V											
芊豐科技				V											
富績科技		V		V											
昱源科技				V											
聯訊數位資訊								V							
赤玉科技有限公司				V											
滿利科技				V											
新世紀資通										V					V
網鈦科技有限公司				V											
超宇網際網路國際股份有限公司								V							
序宸科技有限公司				V											

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
台灣固網										V					V
晨富股份有限公司				V											
全球有聲網				V											
上晉電信				V											
永佰科技有限公司								V							
東亞有線電視								V							
泓笙數位				V											
神奇科技								V							
合益電信				V											
銘儒電腦資訊								V							
凱擘股份						V		V							
併力科技								V							
普羅通信				V											
佳佑科技										V			V		
冠宏科技								V							
殷富資訊														V	
好消息資訊				V											
九亨國際				V											
合昱科技	V	V		V			V			V	V		V		
華偉科技								V							
願景國際電信						V		V							
上禹企業				V											
科奇資訊網路								V							
統一超商								V		V					V

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
弘富網通								V							
全虹企業														V	
亞東電信	V														
生活網科技服務								V							
仲聯國際				V		V									
藍洋電訊				V											
台灣信京電訊	V	V		V											
元豐昌電信				V											
弘富寬頻科技								V							
遠東寬頻科技								V							
攸風國際				V											
印堤科技國際				V											
尚沛資訊				V											
威揚映像科技								V							
安源通訊								V							
環球電通				V											
昕癸科技				V											
荃城								V							
匯智資訊								V							
力網								V							
柏客司資訊事業													V		
冶達科技				V											
侑瑋衛星通訊						V									

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
乒乓話網				V											
洄瀾有線電視								V							
馬紹爾群島商浩揚網通台灣分公司				V											
臨謙科技								V							
駛達						V		V							
聯鑫網科技								V							
智信資訊				V											
家樂福電信										V					V
資傳電訊				V											
第一線電訊					V	V	V	V			V	V			
利合博電訊				V											
群晟數位								V							
廣龍實業										V					
安石國際商務顧問									V	V					
環球互動網路													V		
海豐工程								V							
光鍵	V	V		V											
保誠科技						V		V		V					
汎宇電商										V					
東穎數位科技								V							
宏科聯網								V							
賀威科技				V											
春秋資訊				V											

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
台灣凱訊電信					V										
御品寬頻科技								V							
陽立科技													V		
連科通訊		V													
杰網電訊科技				V											
台灣新電信					V	V	V	V				V			
歐邁電訊				V											
捕夢網數位科技								V							
迅聯網國際				V											
遠見網絡								V							
興發資訊								V							
台灣塔塔通訊					V	V									
希德國際									V						
欣聖股份								V							
旭威資訊								V							
泰通科技				V											
天外天網路科技								V							
佳音網電科技				V											
台亞衛星通訊					V	V		V							
創意人資訊								V							
鉅鏵科技								V							
承豪資訊								V							
奕信網思								V							

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
廣聚綠能科技				V											
澧豪科技				V											
臺灣網路認證									V	V					
康盛機電								V							
享銘科技								V							
冠陽光電科技				V											
宏達網通科技								V							
聯恆數位資訊								V							
翰樺電信				V											
立鏵企業				V											
二三五網路								V							
安立資訊				V											
菲特科技	V	V													
第一網通科技								V							
亞洲第一電訊				V											
利穎科技								V							
亞立碼通訊科技				V											
鴻網								V							
佳得				V											
凱勝電訊				V											
宏享資訊				V											
台傳科技				V											
威寶電信								V							
健元電子				V											

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
台灣海盟數位								V							
神通資訊科技								V							
新北市寬頻科技								V							
原神鳥網路科技								V							
優像數位科技								V							
鈊象科技								V							
訊偉電信科技				V											
立喬數位國際								V							
易聯數位科技								V							
群揚資通								V							
永達網								V							
興邦資訊				V											
聯閤科技				V				V							
銓鍇國際								V							
台灣迅通網路服務				V								V			
澳大利亞商澳電電信國際台灣分公司					V	V		V							
禦騰科技								V							
遠振資訊								V							
雲達科技								V							
崇遠股份				V											
和信超媒體雲端服務				V											
光璟資通								V							

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
網美科技								V							
家州資訊								V							
拓雲國際網路								V							
和穗實業								V							
全球數位通				V											
鋐捷科技								V							
齊宏企業社								V							
祥網實業				V											
銓貿資訊科技								V							
亞訊								V							
台灣智慧光網								V							
弘通國際寬頻電信				V											
全球視訊系統								V							
全騏資訊								V							
中神通科技				V											
奇優數位科技								V							
傳景科技				V											
盼達資訊								V							
元訊寬頻網路								V							
果核數位								V							
永瀚行銷顧問						V		V		V					
富鴻網								V							
三大有線電視								V							
中華聯網寬頻	V			V				V						V	

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
合威語音科技企業													V		
協辰電信				V											
兆達電訊科技				V											
倍穎資訊	V	V													
威達雲端電訊								V	V	V					
好站網控電子商務								V							
新世技國際				V											
歐鵬寬頻科技						V									
大東海速頻科技						V									
泰通電信通訊行	V	V					V			V	V		V		
暉捷科技				V		V		V							
速達通				V				V							
亨通語音科技				V									V		
天翔通信				V											
米卡資訊								V							
金大業國際企業				V											
居安科技國際有				V											
豐穗國際				V											
立誠電腦資訊								V							
洋基電信								V							
磐石寬頻系統整合								V							
定位傳媒				V											

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
樂網企業社								V							
優懋網電科技				V											
世界通國際整合行銷								V							
愛卡國際				V											
嘉荷路司								V							
捷威興業													V		
數位極光科技								V							
華鈺光纖科技								V							
捷一資訊服務								V							
和勝網路科技								V							
緯益資訊								V							
傑勝網路資訊								V							
訊南科技								V							
新永安有線電視								V							
聖祥電信				V											
華聯電信	V	V			V		V	V	V						
全盛國際科技				V											
大揚有線電視								V							
台固媒體								V							
大嘉義行銷管理								V							
快易通網路科技								V							
藍網電訊				V											
靖騰電訊	V	V		V											V

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
南國有線電視								V							
華網資訊社				V						V	V				
金福樂 國際寬頻電信				V											
眾意傳播								V							
聯答科技								V		V					
發現資訊				V											
全科資訊								V							
五洋科技				V											
天承行													V		
宅頻道 光電科技								V							
聯網寬頻電訊								V							
瑋勝電訊科技				V											
中華金廈聯網				V				V							
網際科技								V							
鈺峰弘科技								V							
山鋙科技資訊				V						V					
鴻翔國際雲端				V									V		
第三波科技								V							
利洋資訊								V							
全家電訊				V											
中華聯興科技													V		
三冠王 有線電視						V		V							

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
雙子星有線電視						V		V							
您的生活網行銷顧問								V							
奇星數位科技								V							
萬通國際人力開發				V										V	
益慶科技								V							
碼鈦科技								V							
全球通資訊				V											
同學系統科技								V							
台灣鼎鑫電通								V							
智冠科技						V		V							
振台電腦科技								V							
雲高科技								V							
博程資訊								V							
佳明電信科技				V											
統悅寬頻網路								V							
創煜網路科技								V							
亞太新科技								V							
美智達興業				V											
通寶移動通信														V	
永訊資訊								V							
東台有線電視事業								V							
迅聯科技								V							
晶品數位科技								V							

經營者名單	語音單純轉售服務	非E.164網路電話服務	E.164網路電話服務	批發轉售服務	公司內部網路通信服務	頻寬轉售服務	語音會議服務	網際網路接取服務	存轉網路服務	存取網路服務	視訊會議服務	數據交換通信服務	付費語音資訊服務	行動轉售服務	行動轉售及加值服務
衛鴻														V	
加陽資訊								V							
合計：433	61	56	4	149	38	37	13	221	38	68	16	21	32	7	10

附錄三 第一場焦點座談紀錄

「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫焦點座談會紀錄

時間：103 年 06 月 24 日（週二）下午 2 時 0 分

地點：文化大學大新館(台北市延平南路 127 號)403 號教室

出（列）席單位及人員：中華電信公司代表、亞太電信公司代表、威寶電信公司代表、遠傳電信公司代表，以及本研究團隊全體成員

*原威寶電信(股)及台灣之星移動電信(股)兩家公司已於 2014/10/31 合併為台灣之星電信(股)。

一、座談問題提綱

主題一：遵法義務之實踐

1、 如何擬訂和告知特定目的？

2、 蒐集之電信利用人/契約用戶之資料種類？資訊分享第三人(關係企業或非關係企業)？如何遵守他國或我國個資法規定？分享個資範圍僅為基本資料(如姓名、地址、電話號碼) ？或包括電信往來資料(即含電話通聯記錄) ？

3、 有無依個資法第 4 條委外處理個資？如何監督受委託者？

4、 有無特定目的外利用？自行使用或提供資訊給第三人(檢警單位、救難單位等第三人)。

5、 電信利用人/契約用戶主張資訊自主權之處理流程。

主題二：安全維護機制

1、隱私影響之評估。

2、事故通報之流程。

3、個資資料庫之管理規範、流程。

主題三：監督機制之設立

1、目前監督機制為何？自律或他律？

2、目前落實自律之方式？

3、對於設置第三人獨立監督機構(他律)之意見。

二、訪談紀錄

主席：十分感謝各位業者在百忙之中抽出時間來參加座談會。簡略介紹本研究團隊成員(略)。首先說明本次座談會召開背景，本團隊接受國發會委託執行我國電信事業個資保護和監管機制研究，舉辦本次座談會主要目的，是為了瞭解我國電信事業對於現行個資法之遵法狀態以及有無任何在執行上感到困擾之處。以下就請各位業者代表進行說明。

威寶：在新法施行前，就依據個資法規定修改隱私條款(政策)以求符合法律規定，無論是契約書、網頁說明等部分，並且進行教育訓練。在整個申請流程上依法進行修改，變更對用戶作個資蒐集、處理和利用的告知說明之方法。

中華：誠如威寶代表所說，其所碰到和所作的修改事項，也是我們進行的事務。我們公司在新法施行前，就以極嚴謹的標準和態度，投入極大的人力及耗費重資，依據個資法規定修改隱私條款(政策)以求符合法律規定，無論是契約書、網頁說明等部分，並且修改系統和進行員工教育訓練，包含客服和門市櫃台人員；在監控方面，也對預警標準進行修改。尤其行銷方面，早期如同其他業者，會配合行銷需求提供必須資訊給受託第三方，現在則是全面禁止，不准委託並且載明於隱私政策。對於門市的電腦會進行管控，門市無法以任何方式(比如 USB)存取。

在此提出一個問題，相信也是其他業者有面臨到的問題，欠缺個資外洩定義，到底洩漏幾筆資料才算是個資外洩，就我所知日本在這方面有所規定，這點希望研究團隊能對此進行研究。

亞太：本公司於新法施行前已訂定個人資料檔案安全維護管理之作業規範，於新法施行後本公司將原負責資通安全的常設性編制「資通安全組」擴編為「資通安全暨個資保護組」主導資通安全與個資保護之推動，且由各單位委派人員成立跨部門的安全維護網「個資專案小組」，並聘請顧問進行輔導，同時我們也和法務就法律條文密切的討論，共同依新法訂定個人資料保護作業準則及流程。於新法公告實施之初，本公司首要推動的作業為個資盤點，

並依資料敏感與重要性程度進行分級；個資盤點的過程中，也重新確認每項個資資產的生命週期，包含蒐集、處理、利用、傳輸以及銷毀等流程，它們是環環相扣的。我們也建立個資事件分級制度及通報流程。另外亦修改網站公告資訊以符合個資法規定。本公司資通安全暨個資保護組經常對全體同仁及委外廠商進行教育訓練，個資法實施之初我們更是積極對客服、直營店及加盟店辦理多場次[個人資料保護法之認識與調適]實體教育訓練，並對蒐集個人資料時之告知事項、客戶個人資料之合法運用、客訴的處理等加強宣導，以避免觸法。委外的部分在締約時即明訂權利義務及責任歸屬，並依個資法及細則規範監督廠商，且每半年對委外廠商進行定期查核。本公司個資資料的留存是依據個資法和其他相關法令法規之規定留存，並據以訂立本公司個資儲存保存期限暨銷毀管理表，以作為本公司申請銷毀文件之依據。

遠傳：本公司除了由第三方認證，取得國際認證，比如 ISO27001、BS10012 在內部則組成跨部門安全維護組織，訂定作業準則、流程，確認網頁公告資訊是否符合個資法規定，定期進行稽核盤點，相較於新法施行前是以更謹慎、更嚴格處理公司各部門接觸到的個資。不提供個資給不相關第三方。

本公司與加盟店會透過經銷契約和法律規定進行控管，依權限進行控管與限制並會定期進行稽核。相關紙本，最終還是回送公司，不留存門市。

用戶可依照通傳會訂定之辦法調閱個人的通話明細，公司依照一定的標準流程處理，包含核對身分。

有關當事人主張刪除時，本公司會依法規規定處理。

綜答：對於提供資訊給第三人(檢警單位、救難單位等第三人)是依據通傳會訂定的「電信事業處理有關機關查詢電信通信紀錄實施辦法」和通訊保障監察法進行配合檢、警、調、法等有關機關(構)、稅務機關執行法定職務，提供其查詢之客戶資料。原則上，通聯紀錄是由檢警單位符合相關規範，發公文致業者，業者被動配合。

中華：生命線、張老師、119、110、112 等特定單位個資需求，因隸屬特碼服務，自動顯示來話單位，本公司依相關法規配合辦理急難救助與人道救援作業。倘若未行文，以電話連繫要求提供資訊進行救助，會依照規定流程處理，

比如回撥確認等，不會輕率提供。

主席：請問各位業者對於新法之施行有無任何在執行上感到困擾之處？

綜答：對於目前執行個資法最大的困擾是「法解釋一致性問題」，尤其是間接識別性問題，到底在何種情況下達到間接識別性標準。

威寶：對於此類「法解釋一致性問題」，個人認為如果政府或相關單位能訂出施行細則、管理辦法，讓事業在執行時作為依據，是樂觀其成。

中華：針對間接識別性問題，本公司在系統建置去識別化功能。法規規定模糊，各自解讀，評估風險，調查系統受影響度並進行修正。事實上，本公司對於這些問題已投入極大心力和時間處理執行面細節問題。

亞太：「法解釋一致性問題」，若政府或相關單位能對易於混淆的「定義」的問題釋疑，讓企業在執行時有具體的依據可遵循，我們樂觀其成。

綜答：從新法施行到現在，各家業者早已投入心力以高標準規格力求符合個資法規範，對於新法之施行已有所調適，擔心的是現在才擬定指導準則會不符現況，額外造成更多不必要的負擔。

主席：請問各位業者是否進行個資風險評估？有無個資事故通報流程？

綜答：對於任何一項政策之實施，必定會進行個資風險評估，並就評估結果進行相對應的修正，包含系統設定、影響等級。

由於自律遵循 BS10012 的認證要求，所以已制訂與遵循個資事故通報流程。

主席：請問業者間有無研擬自律認證機制？有無必要成立專責機關？

綜答：外部遵循通傳會的要求取得 ISO27001 認證，以及自律規範方面是內部稽核和遵循 BS10012 的認證要求。

法管理層次與標準以明確、清楚最佳，切勿多頭馬車讓業者無所適從。

威寶：回歸基本面，主要是「法解釋一致性問題」。建議應先了解民間業者執行個資法之實況與需求，在進一步研議有無成立必要。

附錄四 第二場焦點座談紀錄

「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫焦點座談會紀錄

時間：103 年 06 月 25 日（週二）下午 2 時 0 分

地點：文化大學大新館(台北市延平南路 127 號)403 號教室

出（列）席單位及人員：請參見簽到表。

一、座談問題提綱

主題一：現行法規之檢討

1、 憲法第 12 條秘密通訊自由及電信法第 6、7 條第所保護範圍能否含括所有電信通訊利用人之個資？

2、 現行個資法之規範對電信事業者而言是否已臻健全能完全應對？

3、 在電信服務日新月異之今日，對電信事業者之蒐集處理或利用個資，有無個別立法之必要?

主題二：監督機制之設立

4、對電信事業者之有關個資法遵法義務之履行，應如何監督?自律或他律？

5、有無另設獨立監督機關之必要?若無則在現制下應由何機關負責?

6、若有設置獨立監督機關之必要，應如何建置？有何權責?

二、座談紀錄

(一) 法務部代表：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

(二) 台灣隱私權顧問協會 劉佐國秘書長

研究計畫標的應限縮在電信業裡面這些個人資料保護的相關問題。電信事業涉及之個人資料，大致上可分為：用戶基本資料、通訊內容資料、通聯紀錄以及

其他資料，在其他資料中最重要的即是位址資料。

針對以上四種分類所產生的問題， 提出些建議研究問題： 1.經過特定地區收到附近業者之行銷簡訊，是業者與電信公司合作之結果，即未經當事人同意，利用民眾位址資料提供行銷簡訊是否有違反個資法？ 2.電視購物台因皆須客戶加入會員，故其為合法蒐集個人資料，惟，其會定期寄推銷資料、發行銷簡訊，通常是與電信公司合作的方式辦理。依照個人資料保護法第 4 條規定，電信業者接受委託會視同為委託機關，所以在為電視購物台提供行銷簡訊服務時，也須注意是否有違反個資法的問題？3.當民眾利用攜碼轉換電信業者服務時，在最初一個月撥打該電話者，其會聽到 NCC 要求電信業者以答鈴聲提供所撥打門號已經轉換電信業者的訊息，惟當事人不一定願意給其所有朋友知悉其已轉換電信公司，但電信公司卻在未告知當事人的情形下，提供答鈴告知來電者轉換電信業者之資訊，而 NCC 針對此回應表示，該答鈴轉換電信業者的訊息提示，僅是行政指導行為，並無相關法律依據，此部分是否有違反個人資料保護法問題？有無逾越必要範圍的問題(個資法第 5 條)?似應研究。

關於現行法制部分，應聚焦於三點：其一，是否應成立獨立專責的個人資料保護主管機關，其因在於，此乃現今國際上潮流，我國應可嘗試成立，獨立專責機關之權責範圍可對全國個人資料保護業務做完整之的統合，更能使我國有更多機會參與國際個資保護相關會議，互相交換意見，使個資保護業務與國際接軌，立法技術亦可更臻完善；其二，是否應定義加值服務所處理的個資種類與內容，並告知電信公司應遵循的基本規範，並針對所蒐集的個資種類及利用目的加以規範；其三，主管機關若能特別訂定相關之綱領或指令，如 APP Guideline 等，更可使業者在蒐集、利用個人資料的過程中，有所依循而避免違法。

(三) 中興大學法律系 林昱梅副教授

研究計畫標的雖聚焦於傳統電信加值部分，但並不代表研究範圍無法拓展，以來電答鈴為例，即便不具個人資料，卻會涉及隱私，表現出個人興趣與嗜好。再者，以自身經驗為例，申辦某電信公司時是讓客戶選擇勾取是否接收行銷類的廣告，而非勾取需要哪些，可觀察出高度外洩風險。

現行法規檢討，在憲法基本權部分須加補充的有兩點，其一，資訊隱私權與秘密通訊自由間的差異，相較而言，秘密通訊自由僅限於通訊時期，而其通訊結

束後便僅適用資訊隱私權或資訊自決權；其二，當面對其他機關時，通信履歷歷史是否可加以利用？以德國聯邦憲法法院為例，財稅機關或偵查機關欲保留個人資料，被宣告違憲，另外，近期對業者提供安全防護與浮動 IP 亦有些見解。

法規範部分，可分為二點，其一，個人資料保護法之規定，其保留通訊紀錄，究竟係因有提供的義務，抑或針對其他特定機關有需要才保留？是否又有額外訂定法律規範關於儲存通信紀錄，此乃須額外探討問題；其二，關於電信法第 7 條第 2 項之規定，法規範過於抽象，可能導致中央目的事業主管機關不敢使用。

是否個別針對個人蒐集與利用個別立法，可換角度思考：電信事業有其目的事業主管機關，應可建立雙重管制(又稱雙門管制)，使保有資訊與申請資訊的雙方皆有法源依據，若訂立專法，似有過於抽象，無法針對各業務特別性個別利用。

自律團體等問題，可借鏡食品安全法規採行認證標章，或可參考著作權法提供 safe harbor 提高業者嚴格自律動機；至於訂定類似 guideline 方式，可回頭搭配認證標章再結合技術層面完成。專責機關這部分的探討問題應回歸到事業目的主管機關，以我國現況較為妥適，等其內控上軌道後，再探討外部管制。

(四) 中原大學法律系 江耀國教授

研究計畫標的界定， 可先從釐清電信法上之概念開始，首先，以使用者角度而言，較在意的是詐騙集團的詐騙行為，然而這是否與這邊所須研究的標的，可再思考；再者，電信事業在我國是法律概念，電信加值網路業並不是，因此，可歸納出幾點：其一，電信事業本身即有電信網路，從電信網路可連接到網際網路，而這兩者是不同的，因此，如果從電信網路連到網際網路，並非電信網路的問題，而是網路法的問題。

附帶一提，近幾年來，電信事業者推行之雲端服務，可探討是否有違反個人資料保護法第 4 條。

關於個人資料保護法在遵行上，有關於自律部分，牽扯到的問題可從傳統與組織思考之，國外之所以可自律之原因，在於其具有幾百年的傳統，然而，這並不代表我國無法建立自律機制，此時，須靠強而有力的組織，用公權力委託的概念，先使所有業者加入該民間組織，使其能影響所有業者。

再者，是否應成立獨立機關，可先從我國個人資料保護法探討，首先，法務

部是解釋法規的機關，然而，目的事業主管機關卻仍是按照業別去尋找，然而，卻可能造成民眾申訴無法處理，因此，要將事實與問題結合在一起，再去想現行制度是否已足夠。

另外，從英國資訊委員辦公室(ICO)資料，可發現其在個人資料保護法上面是採行 Guideline 方式再搭配自律模式。值得探討的是，Code Of Practice 並非法規命令，是由主管機關所頒布的，所以法律效力可視為行政指導，會產生信賴保護的問題，再者，違反此規範究竟有無違法問題，更是可探討的。

(五) 政治大學法律系 劉定基助理教授

關於主題一的第一個問題，通訊保障及監察法第 3 條之 1 其實較電信法第 6 條、第 7 條更有關聯性，且通訊保障及監察法第 3 條之 1 所稱「通信紀錄」的範圍較廣。然而在適用上，通訊保障及監察法的適用對象有所限制（檢察官、司法警察官、情報工作機關），在此範圍內，通訊保障及監察法應優先於個人資料保護法適用；至於對電信業者或其他公務機關或非公務機關而言，仍應適用個人資料保護法。

關於主題一的第二及第三個問題，現行個人資料保護法規範內容應算完整，因為抽象來講有關電信資料的蒐集、處理或利用都可以在該法找到應對規定，暫無個別立法之必要；然而，若部分規定（如：行銷部分）有特殊考量，或許可以考慮放寬而有比較不同的規定。個人認為如果有所謂的 Guideline 或 Code Of Practice 是較妥適，可以讓業者容易遵循。

關於監督機制的設立，自律部分當然可以與他律並行，且可藉此鼓勵同業競爭；然而推動自律的同時也要注意監督，如何設置監督機制，目前仍缺少法源依據。個人認為獨立監督機關有成立的必要，但必須是全面性而非僅針對特定產業。

(六) 資策會 科技法律研究所 新業務暨策略規劃中心 吳兆琰主任

研究範圍議題可分兩個層次，分為探討通訊監察或網路犯罪偵查或電信事業的管制？總結而言，可從事件資料分類來看，首先即是資料直接的內容與非內容以及即時取得與非即時取得。而所有資料都不脫此四種特性，MSN 交談與通訊當下被攔截出去，皆屬於內容的即時通訊內容，法規範適用通訊監察法，其餘回歸刑事訴訟法扣押之規定；若是被儲存下來的，應屬非即時取得，而這部分欠缺法

規範，而此部分則回到資訊自決權之議題，此處之例子即可以帳單資料為例，基本上仍可用刑事訴訟法有關搜索扣押之規定。

若再從監督機制是該採取集中式管理抑或分散式，應採後者較妥適，如此才能個別瞭解，個別了解後再從業務主管機關角度採取集中式管理。然而，個人認為電信事業應採分散式管理，其因在於該業別已成熟發展多年；然而，電信加值網路業就目前而言，應先採集中式管理，等其業務類別步上軌道後，再採取分散式管理。

再者，個資法之規範似乎有點過嚴，導致業者戒慎恐懼，無形中可能造成其在產業發展過程中，誤觸法網，依此較期許能以中央目的事業主管機關，頒布特定命令，而這正呼應到前面之觀點─各業別較能理解其內部之規範與技術層面可達程度。個人認為即便成立獨立監督機關，必須是全面性而非僅針對特定產業。

(七) 双榜法律事務所 周逸濱律師

首先，秘密通訊與資訊自決權之差異在於秘密通訊僅能於通訊過程中提供權利保護依據。另外，個人資料保護法立法誠意屬高，然而是否可以仿效日本，每年大幅度地普查民眾想法，徹底了解未來修法方向，更能知道 guideline 或相關法規該如何制定，而以日本法作為參考，其在特別行業皆有制定 guideline 予以輔助，如：金融領域、醫療領域或電信領域。

現行個人資料保護法，仍有些許瑕疵。舉例企業併購問題，先不論企業併購法之規範限制，若今天兩家公司合併時，其中一間公司握有龐大的個人資料，在其傳遞過程中，個人資料保護法於此介入時，應扮演何種角色，然而這當中資料傳遞的過程並不再是目的外利用。

又，究竟應採取自律抑或他律，國外作法或許能提供參考：將第三方公正單位納入公會，抑或透過公權力委託亦可。若有監督機關，其性質是否獨立，應可再探究屬業務上獨立，又或是組織上的獨立，再者，現今較令人模糊的是，法務部為統一解釋單位，然而其卻缺少技術層面，導致申訴管道上有漏洞，因此，成立跨部會平台，應更有實益。附帶一提，基於技術科技中立發展，日本將電信與通信概念視為一體，因此電信法與網際網路一同規範，或許這未來是我國可朝向的目標。

附錄五 第二場焦點座談會 法務部書面意見

針對「我國電信事業及電信加值網路業者個人資料保護與監管機制之研究」委託研究計畫焦點座談會之討論題綱，本部意見如下：

一、議題一：現行法規之檢討

（一）憲法第 12 條規定：「人民有秘密通訊之自由。」其旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利(司法院釋字第 631 號參照)。又電信法第 6 條規定：「電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。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。」及第 7 條規定：「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。(第 1 項)前項依法律規定查詢者不適用之；電信事業處理有關機關（構）查詢通信紀錄及使用者資料之作業程序，由電信總局訂定之。(第 2 項)電信事業用戶查詢本人之通信紀錄，於電信事業之電信設備系統技術可行，並支付必要費用後，電信事業應提供之，不受第一項規定之限制；電信事業用戶查詢通信紀錄作業辦法，由電信總局訂定之。(第 3 項)」上開規定之保護範圍可否兼及所有電信通訊利用人之個人資料，宜須先行界定「電信通訊利用人個人資料」之範圍，並進一步探求上開規定之立法原意與規範目的為何，予以判斷。

（二）按個人資料保護法（下稱個資法）係針對所有公務機關與非公務機關蒐集、處理及利用個人資料之一般性規範，尚難就各種特殊情形為詳盡規定，故其他法律如就個人資料之蒐集、處理及利用有為特別規定者，依特別法優先於普通法之法理，自應優先適用該其他法律(個資法

第 2 條修正理由參照)。至現行個資法規定，是否足以因應電信事業者蒐集、處理及利用個人資料之特殊性？乃至於應否為特別規範或個別立法？仍應由電信事業之目的事業主管機關本於權責審度之。例如德國聯邦個人資料保護法第 4a 條第 1 項就當事人同意之方式設有原則性規定，然為因應電信及電子媒體之特殊性，另於電信法第 94 條及電子媒體法第 13 條第 2 項中為特別規定。

二、議題二：監督機制之設立

（一）由於各個行業均有其目的事業主管機關，有屬中央者，有屬地方者，而個人資料之蒐集、處理或利用，與該事業之經營關係密切，應屬該事業之附屬業務，自宜由原各該主管機關，一併監督管理與其業務相關之個人資料保護事項。因此，個資法乃規定各該目的事業主管機關具有監督與管理權限，諸如第 21 條發布或作成限制國際傳輸之命令或行政處分、第 22 條行政監督權之行使以及第 48 條至第 50 條裁處罰緩之權限等。此外，依個資法第 27 條第 2 項及第 3 項之規定，目的事業主管機關得考量個別行業之特殊性，訂定安全維護計畫及處理方法之標準等相關事項之辦法，並指定個別行業訂定個人資料檔案安全維護計畫或業務終止處理方法。是以，個資法對於非公務機關個人資料保護事項之監督與管理，係以他律為原則，並兼含有自律之色彩。

（二）至未來有無設置個人資料保護獨立監督機關(構)之必要，因涉及法律制度之重大變革，宜由研究團隊蒐集相關國家之立法例，並進而研究、利弊分析，以及比較國內外法律體制之異同，以為我國未來法制修正之參考。

附錄六 第三場焦點座談紀錄

「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫焦點座談會紀錄

時　　間：103 年 10 月 24 日（五）下午 14：00

地　　點：文化大學大新館（台北市延平南路 127 號）401 教室

出（列）席單位及人員：法務部法律事務司代表、通傳會代表、林昱梅老師、黃銘輝老師、劉定基老師，以及本研究團隊成員。

議題一：傳統電信通訊與網路通信之分與合

1、通訊秘密的討論：

（1）位置資料：

位置資料從 3G 到 4G 後會越來越普及。擬訂標準時，有商請業者提供對於位置資訊部份的意見。目前的了解，業者對於位置服務推動並不是很積極。因為現在在手機上已提供很多類似位置的服務。業者對於這部分還要提供並不容易。

位置資訊是根據行動基地台(Cell ID)涵蓋範圍去找到用戶概略位置。目前我們針對 110、119，例如登山失蹤救難通報屬於緊急危難時，特定目的外的要求業者提供，基於公眾利益是沒有問題的。其他情形，業者利用這樣的資訊，於其他商家像是餐廳結合，已經有一些資料庫結合手機內建的 GPS，事實上也不用業者提供，業者提供的是在手機終端無法提供的，才要去開發。事實上，業者曾數次提出利用位置資訊進行商業利用之需求申請，如廣告行銷，但本會考慮到用戶隱私都保護，所以不予開放。

（2）通訊秘密的範圍：

范姜：電話號碼的顯示日本採 opt-in，一開始打電話就讓用戶選擇，我國是 opt-out，

原則上都會顯示。請問各位電話號碼顯示與否是否要規範？

通傳會：這應該屬於隱私保護問題，會涉及公共利益與隱私。

翁清坤:除了電信事業者會蒐集 location data 之外,手機製造商例如蘋果也會蒐集。通傳會如何處理？

通傳會：電信法是管電信事業。目前以型式認證方式處理，手機內建軟體採自願性型式認證，本會會進行手機資訊揭露，但目前尚在研議進行中；如果使用者購買手機後自灌的其他應用程式則適用工業局的管理機制。由於禁止需要法律授權，初步內部討論是先資訊公開，讓業者為了商機利益重視資訊安全而自願性申請接受認證。

黃銘輝：現在企業集團化多角經營，不知集團確切營業範圍如何。我們在法制的設計上除了單純前端給與同意與否的選擇以外，應該包括課予資訊轉授者更大責任,其他集團使用不是從當事人本身提供個資時,在利用個資時要課予告知義務，民眾才有辦法追本溯源。對於業者並不是太大的負擔，又尊重個人自主決定權。

高啟中：就是個資流向的控管

劉定基:其實由電話號碼間接識別個人的可能性很高。我覺得位置資料也是個資，只是位置資料加上電話號碼才有意義。回到電話號碼，現行通保法還有大法官解釋 631 也特別強調，這是目前間接識別資料比較重大的問題，在現行法上沒有機制或單位能夠確保這些資料能合理區隔。特別是網路上可能還有很多資訊是可以連結組合的。

林昱梅：就我而言電話號碼已經是可供識別的個資，像是商店會員，只要電話號碼不需要姓名就可以知道相關資訊。其實可以很直接地就把它認定為個資，認定之後要如何管制或是如何利用是兩回事。

2、通訊軟體：

范姜：在日本發生 Line 的問題，一般電信事業者跟 Line 提供一樣的服務，結果一般電信事業者必須要受到國內法規個資法限制，但 Line 不用（申請執照），在競爭上造成不公平的現象。

通傳會：現在的網路電話，透過 app 運作，兩端都是手持裝置或電腦，這部份是

資訊服務目前不屬本會管轄。但是倘若其中一端需要利用電信中心網路通訊則要申請電信執照。

3、電信事業與自己事業集團中之其他事業，有無共用客戶個資之需要? 如有需求，應在何等範圍內，制定那些要件?

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

黃銘輝：單純的電話號碼是不是個人資料因科技而變複雜。例如 who's call 這個 app 利用網路資料可以抓到來電者的個人資訊，甚至細到身分證號碼都會有。

林昱梅：申請電信事業務時沒有勾選就不能辦理，拒絕人民使用電信的權利，產生電信的近用權問題。電信事業不能因人民的不同意就拒絕。另外，提供自己事業群內部使用個資的同意部份，也可以納為客戶同意選項，企業要主動說明個資給哪些特定事業使用，並於提供時立即通知，且應提供使用者事後變更選擇的聯繫窗口。

范姜：韓國，如果要求客戶提供資料跟提供的服務沒有直接關連性，客戶拒絕提供時，不可以拒絕締結通信契約。我們個資法中也有講到只能蒐集跟利用目的有關連的資料，但實務上業者仍將同意選項作為拒絕服務與否的前提。

黃銘輝：我跟劉老師想到營業自由的問題。如果簽了這些服務，我給你一些優惠，這樣可不可以？這不是是市場經濟、營業自由的範圍？公權利要干涉的程度可以到哪？

4、電信事業者間，有無共用客戶個資之需要?如有需求，應在何等範圍內，制定那些要件?

主席：此問題是要探討電信事業者間黑名單的互相交換，在日本用 guide line 限定特定目的電信事業者在審查契約時可以共用名單。

高啟中：英國也有類似概念，兩家公司建立不良員工紀錄，但也是要取得當事人同意。

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

通傳會：通傳會：之前 165 資料庫，可以查詢電話是否為詐騙電話，僅可以看到電話號碼，無法看到更細資訊，是具有比較強的公益性。至於行動電話欠費等黑

名單的部分，99 年時立法院有要提案修法，當時本會報告幾個重點。第一，電信服務相較屬於一般商品，跟金融個人信用相比只是小額交易，違約損害比較小；第二、通訊自由是憲法保障的基本權利，若成立電信中心，主要目的還是給各電信業者間去排除使用者的欠費。省思以上兩點以及通訊自由比例原則的裁量，建議立法院要審慎立法，目前尚無進一步進展。

黃銘輝：因為立法目的正當性不夠，以現在個資法來看，欠費怎麼看都不算重大，所以不認同仿效日本之作法。

5、對大量之垃圾信件或傳送有害訊息之信件(E-mail、BBS)之遏止，日本、韓國均有專法或特別規定予以規範，我國現行個資法有無增修以因應業者實際作業需求之必要?

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

黃銘輝：事實上，很多關於 spam 造成的問題已透過科技解決，再加上電信技術的進步，spam 也不會占用太多頻寬（浪費太多資源），所以由此看來難謂有立法的急迫需求且如何執法會是問題所在。

劉定基：由於政府已將草案送至立法院，所以從研究計劃實用的角度來看，現在不是那麼迫切。

通傳會：通傳會：阻攔 spam 應該算是業者附帶的資訊服務。阻攔 spam 的主要理由是要維護電子商務的暢通、網路安全的維護；以及對於消費者的便利。目前持續推動立法但一直沒有過，這部份其實有很強的自律方式，用定型化契約方式，業者有權利過濾垃圾郵件。但是還是需要通過立法取得授權才有法源依據，畢竟合約存在模糊地帶。

議題二：監管機制建立模式與方法之探討

1、現經濟部推動隱私保護管理認證制度 TPIPAS，以及通傳會設定驗證標準，如 ISO27001 等，並定期進行稽核。後者主要在通信安全管理部分建立標準程序及制度。在無獎勵機制或誘因下，業者取得認證之意願為何？

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

2、承上題又我國已推動之食品安全認證標章最近受到嚴重之質疑，相同之問題有

無可能發生在資安認證標章上，應如何因應？

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

通傳會：本會推動 ISO27001 及 ISO27011，因為資安有個很重要的部份是在 IT 心臟部份會儲存大量個資，此部分的落實跟資安認證有關係，所以 ISO 認證包括網管系統資訊安全採取實體隔離、維護人員遠端遙控作業標準、用戶資料機密分級管理辦法，比如說透過雙碼安全認證、呈現加密傳輸等，都是保護用戶個資資料，包括通訊安全，新設備安裝要有掃毒、偵測等確保系統安全；另一個是在設備監控方面，也會偵測流量有無異常及受到攻擊。另外還有門禁管制進出等。目前第一、二類有約 570 家左右做過這樣的宣導、辦過教育訓練，約有 50 家已經通過認證。雖然是個自律機制，但現在赴陸投資或陸資來台者，我們已經在研擬相關配套規範須要取得 ISO 認證。

3、電信事業者依個資法第 4 條委外處理個資的情形，如何監督委託者(電信事業者)及受委託者？

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

4、電信事業跨國傳送個資時，個資法第 21 條賦予目的事業主管機關針對特定事項的監督權限。試問實際上通傳會如何監督管制各該業者？

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

5、對個資法之施行，設置第三人監督機關已為國際之趨勢，且為參加國際有關個資保護會議或組織必備之要件，而我國在現行中央政府組織基準法之限制下，應如何踏出第一步？

法務部：(由於法務部已提供書面意見，本紀錄不予贅述請參閱附錄。)

林昱梅：應該是用三級獨立機關處理，重點在於具有獨立的地位但不見得要有個獨立機關設計。

劉定基：我認為有必要設置獨立機關。至於可能遇到的幾項問題(例如獨立機關對於個別行業沒有目的事業主管機關熟悉)，可以透過制度或機關間的合作解決。比如，由獨立機關發布一些行業指導原則時，可以會同目的事業主管機關擬定，獨立機關的作用在於統合與維持基本標準；雖然論及非正式的影響力，當然還是目

的事業主管機關比較強，但透過行政機關之間的合作，仍可以對受管制的行業施加一定的壓力。
倘若仍維持目前由各個目的事業主管機關監督的模式，行政層面要設置好管考制度，以督促各目的事業主管機關確實執行個資法所賦予的任務。

通傳會：設獨立機關有其優點，該機關熟知整體個資法制，輔以各個目的事業主管機關提供產業面之建議，由兩者研議訂定辦法，考量涵蓋層面廣及源頭至終端管理，是較具效能之作法，會比較容易解決問題，也利於個資法制執行。

黃銘輝：個資法第 21 條已經把監督非公務機關的權限交給各目的事業主管機關，各行各業形態不一樣，由一個單一機關來統合，是否功能最適？如果有第三人監督機關，第一個受監督對象就是公務機關自己；第二，要監督目的事業主管機關有無善盡監督之責，類似管考，首先是思考有無必要性，再者，可以考慮監察院是否適合？就監督行政的角度、獨立性、機關位階等等思考，似是合適的選擇。

林昱梅：國際合作很重要，像是核能監管也有技術面，而技術面的提升一定需要國際合作，所以個資保護也必須有一個窗口負責國際合作等。

附錄七 第四場焦點座談會紀錄

「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫焦點座談會紀錄

時間：103年10月28日（週二）下午2時30分

地點：文化大學大新館(台北市延平南路 127 號)403 號教室

出（列）席單位及人員：中華電信公司代表、亞太電信公司代表、威寶電信公司代表、遠傳電信公司代表、瑪凱電信公司代表，以及本研究團隊全體成員

Δ 由於與會業者代表們對於議題之發言大抵立場一致，所以原則上本紀錄未標示發言者，僅於有表述不同意見或情況時寫明業者。

*原威寶電信(股)及台灣之星移動電信(股)兩家公司已於 2014/10/31 合併為台灣之星電信(股)，

議題一：傳統電信通訊與網路通信之分與合

1、 電信事業與自己事業集團中之其他事業，有無共用客戶個資之需要？如有需求，應在何等範圍內，制定哪些要件？

一般而言，與自己事業集團之其他事業，共用客戶個資之情形，多為委外帳單印製、加盟店等情況。倘若委外處理，在實務運作上會與受託者簽訂契約，並於契約內附加維護客戶個人資料條款,並向其告知說明個人資料保護法相關規定，並簽訂保密協議書，以此作為課予其維護電信用戶之個人資料義務之基準。契約進行時，依相關程序規定，每半年定期檢查一次；契約終止後，依照各公司擬定之銷毀流程和契約條款監督受託者銷毀在受委託期間內之內基於業務需求取得的個人資料。值得注意的是，中華電信公司僅有內部資料傳送，並無資訊分享之情形；遠傳電信表示並無與自己事業集團之其他事業共同客戶個資。

2、 電信事業間，有無共用客戶個資之需要？如有需求，應在何等範圍內，制定

哪些要件？

基本上，依照目前實務之狀況，原則上，我國電信事業無共用客戶個資之行為，特殊情況為號碼可攜服務，依照「號碼可攜服務管理辦法」由財團法人電信技術中心協助提供電信號碼可攜服務。目前仍無法律授權共用之例外規定，若電信事業間擅自分享，恐有違法疑慮。惟本研究團隊參酌日本立法例，基於社會公益目的，立法允許電信事業針對不當使用電信服務之用戶建立共享名單，或業者上傳資料至第三方平台進行註記，並提供業者查詢。因此於會中提出此項建議與各個業者代表討論有無仿效引進之需求。簡言之，建議立法者可考慮「惡意積欠高額電信費用或濫用電信服務發送惡意郵件、廣告信件」等諸如此類有害公共利益之情形，是否可作為電信事業間共用客戶個資之例外事由。經討論後，業者們大抵認同此一基於公益目的而制定共享例外事由的作法，樂見其成；但討論中慮及此項作法涉及用戶們受到憲法保障的通訊自由，所以研擬如何施作之細部規範時必須注意此項問題。

3、 對大量之垃圾信件或傳送有害訊息之信件(E-mail、BBS)之遏止，日本、韓國均有專法或特別規定予以規範，我國現行個資法有無增修以因應業者實際作業須求之必要？

(一)E-mail

目前，通傳會仍持續推動「濫發商業電子郵件管理條例草案」，但是尚未完成立法，仍值於尚無法可管時期。電信事業大抵是透過契約方式，明定於契約條款終止服務事由，比如「未經對方同意，擅自寄發電子訊息至對方信箱造成對方困擾之情事者」、「於論壇區張貼與主題無關之訊息之情事者」、「濫發電子郵件、蓄意破壞他人信箱或其通信設備之情事者」，作為對應處理方式。此外，業者們透過電子技術（反垃圾郵件軟體），以及投入人力於攔截電子郵件，自 1997 年至今已逐年改善，但仍希望有法規可供遵循，除了健全廣告市場機制和保障用戶權益，同時減輕業者負擔以利於將資源投入於改進技術與提升服務品質。

(二)BBS

由於電信事業僅提供網路服務，原則上無法匿名使用者身分，因其屬於站台管理者之責任，電信事業之角色僅是在法律明文規定下，被動地配合檢警單位查

詢，並無主動查禁之權力。

議題二：監管機制建立模式與方法之探討

4、 現經濟部推動隱私保護管理認證制度 TPIPAS，以及通傳會設定檢驗標準，如 ISO27001 等，並定期進行稽核。後者主要在通信安全管理部分建立標準程序及制度。在無獎勵機制或誘因下，各該業者取得此類隱私保護認證之意願為何？由此致生之成本負擔對各該業者之影響程度為何？

目前，第一類電信事業皆以據國家通訊傳播委員會(NCC)所頒布之行政規則，通過 ISO/IEC27001 之認證，且其亦會定期檢查，因此，欲推行國內電信事業之認證標章，應考量到第二類電信事業之資本與實際運行狀況，以及是否會有疊床架屋之可能性，故就目前現況而言，推行認證應無實益。再者，縱使政府未針對電信事業推廣此一制度，業者本身亦會循國際標準之認證，使用戶對其更具信心。易言之，相較於第一類電信事業，事實上，第二類電信事業規模多半比較小，取得此類認證，相較其所帶來的不確定經濟效益，營運成本考量會是第二類電信事業較為掛慮的問題。

5、 電信事業依個資法第 4 條委外處理個資的情形，如何監督受委託者？

實務上，電信事業會與其簽訂契約，並於契約內附加維護客戶個人資料條款，並向其告知說明個人資料保護法相關規定，並簽訂保密協議書，以此作為課予其維護電信用戶之個人資料義務之基準。簡言之，受託者必須簽訂保密協定(包含合約書中之個資保護條款、委外廠商簽具保密同意書、委外處理人員簽具保密切結書)。契約進行時，依相關程序規定定期檢查；契約終止後，督促銷毀其在受委託期間內所取得之相關個人資料文件。

6、 電信事業跨國傳送個資時，個資法第 21 條賦予目的事業主管機關針對特定事項的監督權限。試問實際上各該業者如何遵行通傳會之監督管制？

按國家通訊傳播委員會於民國 101 年 9 月 25 日發布通傳通訊字第 10141050780 號：「衡酌大陸地區之個人資料保護法令尚未完備，通訊傳播事業於國際傳遞及利用個人資料時，應考量接受國家或地區對個人資料有完善之保護法令，爰依，『電腦處理個人資料保護法』第 24 條第 3 款規定，限制通訊傳播事業經營者將所

屬用戶之個人資料傳遞至大陸地區。」可知目前僅發布該令針對國際傳輸做禁止，業者將恪遵國家通訊傳播委員會法規命令辦理。

附錄八 第三場焦點座談會 法務部書面意見

本部針對「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫第 3 場焦點座談會討論題綱問題之回應意見

議題一：傳統電信通訊與網路通信之分與合

1. 電信事業與自己事業集團中之其他事業，有無共用客戶個資之需要?如有需求，應在何等範圍內，制定那些要件?

本部回應意見：

一、 按電信事業與自己事業集團中之其他事業體係屬不同之法人(例如：母公司與子公司或子公司間)，為不同之個人資料蒐集主體，且蒐集之特定目的及相關業務內容均有不同，故若須共同使用客戶之個人資料(按：即母公司提供個人資料予子公司或子公司間交換使用個人資料)，因屬特定目的外之利用，故須符合個人資料保護法(下稱個資法)第 20 條第 1 項但書規定情形之一(例如：法律明文規定、經當事人書面同意等)，始得為之。

二、 又電信事業與自己事業集團中之其他事業體間，若有共同利用客戶個人資料之需要，可參考金融控股公司法第 43 條有關金融控股公司之子公司間進行共同行銷之規定，及依該條第 3 項規定就金融控股公司事先應向主管機關申請核准共同行銷應具備之條件、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等，授權訂定之「金融控股公司子公司間共同行銷管理辦法」，於相關電信法規中訂定有關電信相關事業體間共同蒐集或利用客戶個人資料之特別規定。

2. 電信事業者間，有無共用客戶個資之需要? 如有需求，應在何等範圍內，制定那些要件?

本部回應意見：

電信事業者間(例如：中華電信股份有限公司與遠傳電信股份有限公司間)係屬不同之法人，為不同之個人資料蒐集主體，故有關共同利用客戶個人資料部分，同前一題之回應意見。

3. 對大量之垃圾信件或傳送有害訊息之信件(E-mail、BBS)之遏止，日本、韓國均有專法或特別規定予以規範，我國現行個資法之規範有無增修之必要?

本部回應意見：

一、 針對「大量之垃圾信件或傳送有害訊息之信件」，國家通訊傳播委員會持續推動商業電子郵件管理立法， 101 年 4 月「濫發商業電子郵件管理條例草案」已進入立法院二讀審議程序，且該會亦辦理相關防制「垃圾郵件」之業務(防制濫發電郵宣導網，http://antispam.ncc.gov.tw/Spam_zone.html)。未來上開草案若立法通過，即屬個資法之特別規範，合先敘明。

二、 按現行個資法規定，「電子郵遞地址」(代號 C001 識別個人者)雖屬個資法第 2 條規定之聯絡方式，然僅有「電子郵遞地址」不一定即屬得以直接或間接方式識別特定個人之資料，故倘業者依電腦程式隨機製作組合之「電子郵遞地址」傳送電子郵件以行銷，此部分可能無個資法之適用。又倘業者已依個資法第 19 條規定蒐集消費者之個人資料(符合「與當事人有契約或類似契約之關係」、「經當事人書面同意」等情形)，進而利用消費者之個人資料為行銷(特定目的內或特定目的外之利用)，個資法第 20 條第 2 項及第 3 項規定雖被動賦予當事人拒絕行銷之權利，惟尚無法針對「主動傳輸之商業訊息」積極採取相關行政管制措施，故若欲對「主動傳輸之商業訊息」積極採取相關行政管制措施或規範，因屬國家通訊傳播委員會之業管範圍，須由該會依其權責採取相關行政措施並積極研議推動「濫發商業電子郵件管理條例草案」，而非於屬於普通法性質之個資法中增修相關規定。

議題二：監管機制建立模式與方法之探討

1. 現經濟部推動隱私保護管理認證制度 TPIPAS，以及通傳會設定驗證標準，如 ISO27001 等，並定期進行稽核。後者主要在通信安全管理部分建立標準程序及制度。在無獎勵機制或誘因下，業者取得認證之意願為何？

本部回應意見：

業者取得相關認證，可藉此對其所保有之個人資料檔案建立相關管理流程及風險評估機制，以確保對個人資料檔案適當安全維護措施之採取，防止個人資料被竊取、竄改、毀損、滅失或洩漏等，可降低個資法相關行政、民事及刑事責任之風險。相關「TPIPAS」及「ISO27001」之誘因或獎勵機制，宜由主政機關經濟部及通傳會說明之。

2. 承上題又我國已推動之食品安全認證標章最近受到嚴重之質疑，相同之問題有無可能發生在資安認證標章上，應如何因應？

本部回應意見：

「食品安全認證標章」係針對食品製造之成品與「資安認證標章」係針對個人資料管理制度，二者性質不同，故似非可並同比較。

3. 電信事業者依個資法第 4 條委外處理個資的情形，如何監督委託者(電信事業者)及受委託者？

本部回應意見：

按電信事業者依個資法第 4 條規定委外處理個資之實際情形，應由主管機關國家通訊傳播委員會說明。至於如何監督委託者(電信事業者)及受託者乙節，個資法規定各目的事業主管機關具有監督與管理權限，例如「發布或作成限制國際傳輸之命令或行政處分」、「行政監督權之行使」、「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處理方法」、「訂定安全維護計畫及處理方法之標準等相關事項之辦法」、「對於非公務機關違反本法相關規定時，裁處罰鍰之權限」等(按：個資法第 21 條至第 22 條、第 24 條至第 27 條、第 41 條、第 47 條至第 49 條、第 52 條至第 53 條及第 56 條規定參照)；另按個資法施行細則第 8 條規定，委託者(電信事業者)應對受託者為相關事項之監督，且受託者應於受委託之範圍內，蒐集、處理或利用個人資料。

4. 電信事業跨國傳送個資時，個資法第 21 條賦予目的事業主管機關針對特定事項的監督權限。試問實際上通傳會如何監督管制各該業者？

本部回應意見：

本問題應由國家通訊傳播委員會回應。

(按：因大陸地區現行並未訂有個人資料保護之相關法規，經電信事業之中央目的事業主管機關國家通訊傳播委員會以101年9月25日以通傳通訊字第10141050780號令「限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區」，個資法第21條第3款規定(舊電腦處理個人資料保護法第24條第3款規定)參照)

5. 對個資法之施行，設置第三人監督機關已為國際之趨勢，且為參加國際有關個資保護會議或組織必備之要件，而我國在現行中央政府組織基準法之限制下，應如何踏出第一步？

本部回應意見：

一、 依歐盟指令或其他有關個資之國際協約等，個人資料保護專責(監督)機關(構)應具有獨立行使職權之法定地位，亦即具備相當之獨立性，惟囿於現行中央行政機關組織基準法第32條第2項規定，相當二級機關之獨立機關總數以 3 個為限，而現已有中央選舉委員會、公平交易委會及國家通訊傳播委員會等 3 個機關，事實上已無法再增設二級之獨立機關；另依同法第33條第1項、第3項規定，二級機關及相當二級機關之獨立機關為處理技術性、專門性業務需要得設附屬之機關，同條第4項規定，第1項及第3項署、局之總數除地方分支機關外，以70個為限，而目前設立之三級機關總數已達70個上限，故若欲設置屬於上開三級機關性質之機關亦有困難。惟依中央行政機關組織基準法第32條第3項規定，第1項以外之獨立機關(即非相當二級機關之獨立機關)，其內部單位之設立，依機關掌理事務之繁簡定之，又同法第33條第4項所定署、局之70個總數限制，似未包含相當三級機關之獨立機關(按：獨立機關為合議制機關，應稱委員會，同法第6條參照；目前相當中央三級獨立機關有飛航安全調查委員會)，故依上開中央行政機關組織基準法規定，倘於行政院下設「相當中央三級獨立機關」之個人資料保護專責機關，亦無牴觸現行法制。惟是否設置個人資料保護專責或獨立監督機關，涉及行政院之政府組織改造決策權，本部對此不表示意見，並尊重行政院之決策權。

二、 目前在現有資源與條件未變更，而無法設置專責或獨立監督機關之情

況下，本部仍將基於個人資料保護法之法律解釋主管機關之立場，以有限的人力、預算致力於個人資料保護法相關之研擬、解釋及推動工作；各中央目的事業主管機關或直轄市、縣（市）政府則就所管事業（團體、個人）就關於個人資料之蒐集、處理、利用及安全維護等事項加以監督管理；至於中央目的事業主管機關與直轄市政府、縣（市）政府間之權責劃分，則依各該主管機關原對該事業監管權責之業務分工為之。又為解決各機關執行非公務機關個人資料保護事項所生爭議，行政院於 101 年 10 月 22 日以院臺法揆字第 1010061195 號函同意本部函頒之「個人資料保護法非公務機關之中央目的事業主管機關」，故各機關按其原對該事業監管權責之業務分工，受理有關個資法之申訴案件，與單一窗口功能相同。另關於各機關因權責劃分所產生之管轄權爭議，除依行政程序法第 13 條、第 14 條規定處理外，並由本部視爭議情形主動邀集相關機關共同商議，以期建立聯繫協調機制，解決個資法申訴案件之管轄爭議，加快案件之妥適處理。

附錄九 隱私權協會深度訪談紀錄

「我電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫
深度訪談：台灣隱私權顧問協會

訪談日期：2014 年 9 月 24 日

受訪者：劉佐國秘書長

問題 1：對現在 dp.mark 制度，有多少理解？在台灣這類自律能有多少功效？能否有其他自律機制可以建議？

答：據本人所知，此機制當初是由相關政府機關與部分學者建議仿效日本 P-mark 制度，建立一套適合我國國情和產業現況的個人資料保護制度認證標章。目前主管機關為經濟部商業司，並委由資策會進行研究和執行，初始設定的適用對象為電子商務業者。

此標章屬於民間自律機制，參見最近的 GMP 標章事件（食用油問題）可以想見此類自律機制的功效不彰，本人認為主因在於個資保護意識不彰，民眾和企業對於個資保護概念仍懵懂且易於錯誤解讀法規，以及民間監督力量有限，再加上日本與我國之國情與民族性存在差異，所以目前仍難以想見將來能達到日本 P-mark 制度在日本所發揮的個資保護功效。

目前個資保護的世界潮流趨勢是建立專責機關全權處理個資保護事務和事件，本人認為我國應加速腳步朝此方向努力。

問題 2：現在對電信事業之監督：在資安上由通傳會主管，通傳會亦制定有一些法規命令進行監督，且因其對電信事業有執照准許之生殺大權或有發揮監督之功效，但如跨國傳送之認定上，如何處理？

答：由於通傳會乃是我國電信事業的目的事業主管機關，與業者之間往來密切，且為顧及產業發展和對我國經濟發展之影響，以及政治角力等問題交疊，若由通傳會監督我國電信事業的個資保護，民眾多所認為通傳會行事易受掣肘，質疑專業度，觀感必然不佳。再者，通傳會本身非個資法主管機關，難以期待其對於個資法之法源有充分正確認知，亦即恐錯誤解讀法規，所以一如前述，本人認為我國應建構主掌個資保護的專責機關，全責監督公私機構(單位)的個資保護作業。

問題 3：法務部有能力監督？

答：雖然法務部是個資法的主管機關，但是其對於我國電信事業之熟悉度、專業度是否足夠，令人存疑。換言之，由任一部會單獨監督個資事務皆會存在專業度是否足夠之疑義。

事實上，由目的事業主管機關監督個資保護，調查該事業的個資事件，著實令民眾對該機關之立場、人力(能力)難以信任。

問題 4：依現今世界潮流都採對個資法之施行設立機關進行監管，我國有無設立單一監督機關之必要？

答：此乃國際趨勢且也是對於我國之經濟發展和國際地位必要之務。參與國際個資保護會議的前提必須是個資保護的專責機關，參與這些國際會議可以得知國際個資保趨勢且產生影響力，對於我國經濟政策之擬定與發展至關重要。事實上，早些年個資保護發展未及於我國進展的新加坡也已設立個資保護專責機關，作為該國參加這些重要國際個資保護會議之代表，本人認為我國政府應儘速研擬建置計畫，以避免將來被國際(各國)排除於外之困境發生。

問題 5：如設置獨立監督機關應為如何層級（行政機關之一級、二級、三級機關）？其職權、組織方式有何建議？

答：建議修改中央行政機關組織基準法，在行政院底下設置如同消費者保會委員會的個資保護專責委員會，專責處理公私立機關的個資保護作業，偕同各個目的事業主管機關進行個資外洩事件調查與究責，以及專責職司個資法之解釋適用，召開解釋協商會議偕同各個目的事業主管機關進行討論作出統一定見，以改進現行多頭馬車，各機關適用標準不一之嚴重問題。

附錄十 瑪凱電信公司深度訪談紀錄

「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫深度訪談
深度訪談：瑪凱電信

訪談日期：2014 年 9 月 29 日
受訪者：瑪凱電信公司代表

主題一：監督機制

在德國聯邦個人資料保護法之框架下，德國各電信公司所發布之隱私權聲明中，皆有自律監督機制之設計，透過於企業內部任命獨立之資料保護監察員，一方面監督其內部個人資料保護業務，同時作為一溝通橋樑，釐清並答覆用戶對其個資運用上之疑慮；另一方面，與國家個資保護專責機關密切合作，共同促進個人資料保護。因而，想進一步瞭解我國電信事業就個資保護業務如何配置相關人員或組織以及與監督機關之協調與合作模式。

日本「電氣通信事業有關個人資料保護之指導綱要（下簡稱「電信 GL」)」規定電信通信業者於事故發生時，應立即將洩漏之相關事實通知當事人，並基於防止二次被害之發生、或將來類似事務再發生之避免之考量，應將有用之事故發生關係資料公開，此外尚須向主管機關總務省報告。

英國法發生個資侵犯事件時，業者應通報獨立主管機關，不得無故延遲。通報內容包含個資侵犯事件之性質、個資侵犯事件之結果；以及業者已採取或建議採取之應對措施。若個資侵犯事件可能對用戶或使用者的個資或隱私造成不利影響，業者應通報用戶或使用者。通報用戶之內容包括對個資侵犯事件性質之描述、關於向業者取得更多相關訊息之聯繫資訊；以及推薦用戶採取措施以減輕個資侵

犯可能造成之不利影響。

所以本研究團隊欲進一步瞭解上述規定與我國電信事業者現行做法是否相同？若是不同，倘若將來採行相類似規範，對於我國電信事業者可能產生之影響？

答：基本上，本公司是將個資洩漏當作資安洩漏層級來處理，依照「國家資通安全通報應變作業綱要」定義事件等級以區分通報等級；當然，本公司也有制定通報流程作業規則，除此之外，本公司也有訂定個資資料庫之管理規範和流程以管理人員，以及維護電子資料庫與紙本檔案之安全。比如，因工作或業務而有接觸用戶個資需求的話，必須填寫申請單，取得主管同意。

然而疑問為何謂個資洩漏，個資外洩之定義並不明確。如果採納英國法之相關規範，要求業者評估該起個資外洩事件對用戶或使用者之不利影響，此點對於業者是相當有難度的，因為難以預料竊取者會如何使用遭竊個資；倘若明定通報內容以供業者遵循，會是相較可行的方式。

另外，關於本公司對於設置第三人獨立監督機構(他律)之意見，本公司認為雖然設置監管個資保護事務專責機關有其優點，但是業者的顧慮為該機構是否足夠了解各產業之實況而能夠兼顧各產業不同之特性與需求；目前依法通傳會是第二類電信事業的目的事業主管機關，通傳會十分了解產業之需求，就目前來說由各個目的事業主管機關各自監督該事業的個資保護事務是相較妥適的方式。

至於，dp.mark 個資保護標章的認證問題，參見最近的 GMP 標章事件（食用油問題），本公司對於此類認證機制的效用是有所質疑的。事實上，第二類電信事業者規模多半比較小，取得諸如 ISO、dp.mark 等此類認證，相較其所帶來的不確定經濟效益，營運成本考量會是第二類電信事業者較為掛慮的問題。

主題二：資訊分享

按照美國聯邦通訊委員會所公布命令及施行細則，針對「用戶專屬線路資訊」，即業者於提供電信服務時從用戶取得的資訊，只要電信事業者所分享的關係企業係通訊相關的業者，其同意模式乃採「選擇退出」方式，毋庸取得用戶的事前明示同意；倘電信事業者欲將「用戶專屬線路資訊」揭露予合資夥伴或獨立自主的契約締約相對人，或者允許其得接觸使用「用戶專屬線路資訊」時，電信事業者應取得用戶「選擇加入」同意。

日本「電氣通信事業有關個人資料保護之指導綱要（下簡稱「電信 GL」)」對於電信事業者提供資訊給第三人設有限制規定,原則上不得將個資提供給第三人，除非符合例外是由，例如法令有明定者、為保護人之生命、身體或財產而有必要，且得到當事人同意為有困難時之事由者。一般而言電信事業者可能多依契約約定方式，得到當事人同意而將其個資提供給第三人；然即使已得到當事人同意。

因而，本研究團隊想進一步瞭解我國電信事業對於上述之資訊分享限制規定之看法？以及現行處理方式是否有類似之處？

答：基本上，本公司對於提供個資給第三人之處理方式較為謹慎，皆以取得當事人書面同意為原則，比如發生盜刷信用卡事件，銀行請求提供資料時，本公司於實務上請當事人填寫同意書。

主題三：委託第三方

德國聯邦個人資料保護法對於將個人資料傳遞予第三人之情況，要求德國各電信公司需有法律依據或基於對當事人履行契約義務或是其授權而交付。若交付之第三人非公務機關時，該個人資料之原始蒐集公司，應確保該個人資料乃被合法地處理或利用。

日本「電信 GL」規定以下非屬「第三人」；1、電信事業者為達成利用目的之必要範圍內，將個資之處理之全部或一部委託時；2、因合併或其他事由而繼承事業所伴隨之受提供個資者；3、與特定人間共有個資而利用者，應預先將下列事項通知本人，或置本人容易得知之狀態，其要旨、被共同利用之資料項目、共同利用者之範圍，其利用目的及對該當個資有管理責任之人之姓名或名稱。但另一方面，電氣通信業者於委託處理個資時，依電信 GL 負有責任選定適當之受託人，並對其進行適當且必要之監督；如有未盡上述之責任，而產生問題時，身為委託人之電信事業者也應負責。

英國電信事業者 Vodafone 為遵守英國個資保護相關法規，透過合約要求該第三方採取適當措施以保護個資安全；必要時 Vodafone 將派資安人員檢視該第三方之資安保護措施是否符合 Vodafone 之要求。

因而，本研究團隊想進一步瞭解我國電信事業對於此類規定之看法？以及我國電信事業者是否亦採行上述類似方式以監督受託執行事務之第三方？又或是有

何不同之處？亦即我國電信事業者依個資法第 4 條委託第三方處理之樣態或業務有哪些類型? 如何防止其濫用客戶個人資料?

答：基本上，本公司認為英國法的規定是較為合理的。原則上，對於第二類電信事業者而言，公司規模大都無法比擬第一類電信事業者，由於成本考量問題，如能自己處理就自行完成，因為即便可透過合約規範第三方，但是在監督方面是相當大的負擔，很難確保第三方到底會不會發生問題。即便派人定期檢查，實際成效仍多得仰賴合作的公司自律約束。

主題四：隱私權政策

日本「電信 GL」規定電氣通信業者應公布其隱私政策，並予遵守。該隱私權政策內容包含個人資料之利用目的；利用目的通知或公開，或因應來自本人要求訂正等之程序；申訴之窗口；有無委託、明示所委託事務之內容等。舉例而言，日本最大二家電信事業者 NTT ドコモ（NTT docomo）股份有限公司及ソフトバンク（soft bank）股份有限公司所揭載之「隱私政策」，內容大致上包含七大項：I 個資之利用目的、II 個資之對第三人提供、III 個資之提供閱覽、IV 依 direct mail 等服務介紹之停止、V 有關個資處理之商談窗口、VI 認定個資保護事業團體、VII 安全管理措施。

英國電信事業者為因應並落實英國個資保護相關法規，以佛德風 (Vodafone) 所揭示之隱私權政策為例告知用戶其蒐集、處理與利用個資之目的，包括信用查核，通信服務之提供，行銷、帳務處理、管理與保護電信通訊網路，研究與分析客戶之通訊利用習慣,以及在特定對象間分享用戶個資 (包括該集團內各子公司，提供服務之合夥商或代理商，信用查核機關，帳務催收機關，政府與執法機關，法院等)。其亦告知用戶關於個資之安全維護措施，包括其委託第三方代為處理用戶個資之情形。同時，Vodafone 告知用戶其個資相關權利，包括申請閱覽個資，更正個資， 以及停止利用個資，並提供聯繫管道。

美國電信公司 Verizon 在其隱私權政策揭示之內容，除了說明該公司針對關係企業與非關係企業進行資訊分享之內容，並進一步提及日後若公司合併時對於用戶個資之處理方式。

上述隱私權政策揭示之內容，均對電信用戶的個資保護有其重要性，惟對照我國電信者公示於眾的隱私權政策，發現內容詳細程度存在差異，因此本研究團

隊欲瞭解我國電信事業者對於此番差異之看法，以及是否會考慮仿效之。

答：本公司未在網站上公開隱私政策，但是本公司仍是有依照個資法、資安相關規範訂定隱私政策，目前已在研議將相關規定寫入隱私政策並公開放置於本公司官網，提供消費者閱覽。另外，以電話卡為例，除了透過網路銷售，亦有經由實體賣場販售，所以本公司最近也在研議是否將同意書置放於包裝內，但又有使用者是否回擲之問題。換言之，因為電話卡的開通使用方式問題，所以尚在討論應以何種方式處理較為妥適。

附錄十一　通傳會深度訪談紀錄

「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫
深度訪談─國家通訊傳播委員會

訪談日期：2014 年 9 月 30 日

受訪者：法律事務處、資源技術處以及通訊營管處

一、本團隊在進行各國法制研究時發現，至少日本或是韓國等對電信事業所處理之較一般不同之個資例如:位置資料、帳單資料、通信履歷等，有特別之法規命令或行政指導要綱(GL)對其蒐集，處理，利用要件對電信事業另作規範，(通常是設立更各嚴格之要件)。依本團隊查得貴會對電信事業者目前所定之行政命令，似乎較偏重在資安及客服部分,可否請問貴會對有如外國特別對電信事業另者有蒐集、處理或利用用戶個資之特別規範有何看法或意見 ?而貴會在執行個資法之監督業務上，有無窒礙難行之處?

答：總括來說，這些資料可分為使用者資料以及通信紀錄[629]，前者是所謂的靜態資料[630]，後者即是使用實體網路(集中式電信網路)所產生的資料，包含發話地點、通話分鐘數等，主要用於計帳目的，屬於動態資料，依照電信法之規定必須是技術上可行。由於目前通信網路正朝向全 IP 網路（Network Convergence－All-IP Network）發展，所以越來越難以區分資訊服務和通訊服務。例如定址服務，現在智慧型手機本身及內建 GPS 定位系統，此外亦可透過網際網路，完全毋須透過電

[629] 電信法第 2 條第 1 項第 8 款 通信紀錄：指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。

[630] 電信事業處理有關機關(構)查詢電信使用者資料實施辦法第 4 條：本辦法所稱使用者資料，指電信使用者姓名或名稱、身分證統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限。前項所稱電信號碼，係指電話號碼或用戶識別碼。

信事業者。

至於個資法就國內電信事業實務之執行有無窒礙難行？是否足夠處理，有無另立專法之必要，目前尚無定論，依現行數位匯流之情形，重點應在於監督範圍之劃分，承前所述，電信網路已逐步架構於網際網路之上，語音訊號數位化，如何區分資訊服務和通訊服務是必須先處理的問題，接而才能進一步討論如何執行監督問題。

二、在目前個資法之現制下，有關個資法之施行之監督事務，依其第 19 條國際傳輸、第 22 條資料檔案安全維護與警察搜查事項，第 17 條二項指定非公務機關訂定個資指導安全維護計畫，均為由中央目的事業主管機關主管執行。如此中央各目的事業主關機關，針對所管事業各自能依其事業特性進行監管之方式，其優點當然是因熟悉其主管事業經營方式為最能解決問題之所在，精確有效率解決問題；但其缺點可能是，各自為政，各自解讀法律，有造成執法寬嚴不一之可能。請問：貴會對此有何看法？

答：根據個人資料保護法第 27 條授權，本會得訂定電信事業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之標準等相關事項之辦法，本會已擬定草案並召開多次研議會議與業者進行討論。各個目的事業主關機關係依據各產業之實況和需求，擬定符合個資法且不阻礙產業發展之辦法，以本會為例，本會管轄之事業不僅止於電信事業，還有廣播電視事業等，各有其細部複雜之處，如何統合，顯為難事。

三、尤其在跨境傳遞個資之事務上，自歐盟 EU 指令開始，許多國際有關個資保護之協定或公約，均要求傳遞個資之相對國須有獨立監督機關始符合安全保護水準。我國個資法第 19 亦有規定，請問:貴會對此部分，目前之作法為何?如何認定？

答：跨國傳遞個資問題，最為顯著即是 Google 公司之類的跨國公司跨國傳遞個資行為，這也是世界各國皆面臨的問題，非屬任何國家可以單獨處理之問題。基本上，只要該公司在我國申請營業，即依據營業範圍所適用之法規予以規範。美商 Google 公司之個資中央目的事業主管機關係由經濟部擔任 。以提供 skype 通訊軟體 3 服務的連科通訊股份有限公司為例，該公司經營第二類電信事業服務(非 E.164 用戶號碼網路電話服務）目前仍未鋪設管線基礎設施，依電信法之規定屬於第二類電信事業，所以適用第二類電信事業管理規則。

四、當然目前之法制度下，有關電信事業者之個資法遵守，由貴會主管監督，如自個資法長期發展之觀點，及個資因網路之發達下有跨國執行問題之考量，我國似應設有個資法施行之獨立監督機關。請問：貴會之意見。

答：設置獨立監督機關乃是國際個資保護趨勢且為參加國際會議之資格要件，加上我國一向順應世界潮流，努力在各方面與世界接軌，所以誠屬必然之事。再者，此為建構健全法制的必經之途，各個目的事業主關機關雖熟知其主管事業並具有專業度，但對於個資法之解讀非屬其職責所在；此外，就效能面而言，該機關熟知整體個資法制，輔加各個目的事業主關機關提供產業面之建議，由兩者研議訂定辦法，考量涵蓋層面廣及源頭至終端，是謂較具效能之作法。

五、如有必要設置個資法施行之獨立監督機關，在現行中央行政機關組織基準法對二級及獨立機關均有設置總數之現制下，應如何突破？

答：中央行政機關組織基準法是採納總量管制的概念，以落實「政府再造」。設置之前提是必須確認有無必要性，倘若有其必要性，相對應之作法應該是修法，無論是修改基準法或個資法，抑或是整併機關，而非侷限於現行規定。

六、如無法突破中央行政機關組織基準法之限制，而要在現行二級機關中有何機關是貴會認為在人力、物力上是適合擔當此監督之大任者。

答：依據法務部組織法第 2 條之規定，法務部職責之一是行政院及其所屬機關法規研議、法規適用之諮商，誠如計畫主持人所說，由於法務部接受各部會機關諮商如何適用法規（具有專業能力），所以往往最先被認為是適合擔當此監督之大任者，接之而來即是人力能否負擔之考量。然，一如前述，設置監督機關之前提是有無必要性，倘若經評估所得結論是必須且必要，或可透過擴編人力解決此一問題。

七、目前貴會在監督電信事業者有關個資法之遵守上，最常遇見之問題為何?業者最常被用戶或利用人投訴之問題為何?

答：何謂個資之認定是最常遇見的問題，並且也是最容易發生混淆之問題。此外，法務部即便答覆諮詢問題，往往也建議目的事業主管機關視個案具體情況自行判斷。目前僅能期待法院作成判決而能有司法判例可供依循。未來就個資法的修正，宜增加個資的保護與利用之間應取得平衡意旨，以促進電子商務之發展，諸如增

加去別識別化機制、第三方認證機制，及跨國合作等。目前消費者通常最先向消保會投訴，再經由消保官轉介給本會負責處理的單位，由於經過消保官先行過濾，所以歉難表示意見。

附錄十二 台灣大哥大電信公司深度訪談紀錄

「我電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫
深度訪談：台灣大哥大

訪談日期：2014 年 10 月 1 日

受訪單位：稽核室資訊安全組、法務室

主題一：遵法義務之實踐

1、個人資料運用特定目的之擬訂與告知

台灣大哥大公司(以下簡稱本公司)對於個人資料運用特定目的之擬訂與告知，係以遵守個人資料保護法(以下簡稱個資法)為出發點，發展出「在各門市放置立牌」、「隱私權聲明」與「建立電話語音系統」三種方式，達成告知之義務，此三種方式之特色，茲分述如下：

(一) 在各門市放置立牌

使欲申辦電信服務之客戶，得以清楚明瞭業者之個人資料保護政策，不僅使客戶使用上得安心使用，業者亦可落實個人資料保護法中之誠實信用原則。

(二) 隱私權聲明

本公司之隱私權聲明可透過本公司官網得知。

(三) 電話語音系統

使客戶在簽約後，若對於個人資料之運用有疑慮時，可撥打客服專線，透過語音系統選擇聽取本公司個人資料告知事項，獲得相關諮詢與協助。

2、 蒐集之電信使用人/契約用戶之資料種類；資訊分享第三人(關係企業或非關係企業)之情況及分享的個資類型與範圍

就本公司分享個資之關係企業與非關係企業，就其情況及分享個資類型與範圍，茲分述如下：

(一) 關係企業

本公司委託子公司─台灣大數位公司經營直營門市業務，故於前述範圍內委託其處理個資。然而，其在執行業務過程中，仍須受個資保護最高指導原則─Need-to-know 原則之約束，以策客戶個人資料之安全。

(二) 非關係企業

此部分可約略分為：帳單列印、帳單外催與物流公司，本公司均與負責上述業務之非關係企業簽訂附具保密條款之契約，並依其所接觸個資之類型與情況評估個資外露之風險高低，據以要求其採行不同層級的個資保護措施，而其中最須受到管控之部分，即為物流公司，因在運送過程中，客戶個人資料保護之風險相對較高，故本公司擬定相關之配套措施，確保並監督委外之個資安全性與本公司內部所採標準屬同一層級。

3、 跨國傳遞個資的實務運作

行政院國家通訊傳播委員會(NCC)曾頒布命令[631]，明確禁止傳遞用戶個人資料至中國，此乃為本公司所遵行。本公司目前並無進行國際傳輸，若未來有此需求，在進行跨國傳遞個人資料前，會諮詢相關法規單位，以維護客戶之個人資料安全。

4、依個資法第 4 條委外處理個資的情況，如何監督受委託者

業者在監督受委託者方面，大致上分為「一般同仁」、「門市人員」與「委託廠商管理單位」，而有關其運作情形茲分述如下：

(一) 一般同仁

此類人員，本公司在實務運作上採行機敏性資料保護原則，透過 e-learning 方式指導一般同仁熟悉個資保護的秘訣：「授權（僅有被授權者方有權限取得該筆資料）」、「降等（依據資料類型設定密等，若有降低密等的需要，則應先將密等較高的內容刪除，不予提供）」、「限收（避免轉寄、設定副本等情況）」、「加密（每份檔案資料皆須加密，僅有特定設備配合密碼方得觀看）」、「銷毀（要求於一定時限

[631]國家通訊傳播委員會令 通傳訊字第 10141050780 號。

內將資料銷毀，並定時稽查）」避免客戶之個人資料受到不當處置。

(二) 門市人員

門市人員於交付文件予物流人員時，就該文件皆設定文件回送條碼，以確切掌握客戶之個人資料流向，避免個資外流。若有逾時卻仍未到件的情形，立刻追查，掌握追回個資的黃金時間，將損害降至最低。

(三) 委外廠商管理單位

依據「委外廠商作業檢查表」，分就人員管理、風險管理、業務管理、資料管理、系統管理、通報應變等項目進行稽核，約每季或每半年進行一次，並進而取得資安證書，完善風險事故處理流程。

5、 特定目的外利用個資的情況有哪些？多為自行使用或提供資訊給第三人(檢警單位、救難單位等第三人)？

於特定目的外之利用，係依法提供予檢警或其他有權調閱單位。於執行上，本公司法務室下設有一專責小組負責，本公司若難以界定來函者之定位，仍會要求其提出說明及法源依據，否則即予以婉拒。若確屬司法或檢察或其他有權調閱機關時，則會依 NCC 法令及本公司內部所定「司法監察機關警政查詢作業」配合提供相關資料。

6、 電信利用人/契約用戶主張資訊自主權之處理流程

此類情形通常出現在客戶不希望收到有關折扣優惠等促銷之簡訊，故現今採用之方法，便是在雙方訂立契約時，詢問客戶之意願，若其不希望收到，將會透過內部之技術，替客戶攔截該類型簡訊，若仍收到，亦可透過「電話語音系統」向本公司表達，若日後客戶表示仍繼續收到此類簡訊，則會將其轉為客訴案件處理。惟，若是攸關客戶權益之通知，仍會依本公司之「權益簡訊辦理原則」，以發送簡訊方式通知，避免客戶權益受到影響。

客戶提出其相關資料之查詢，必須填寫申請表，檢附雙證件；若是代為查詢，則需另外再檢附委託者之雙證件。相關資料將另外郵寄予該客戶（而非委託者）。

主題二：安全維護機制

1、 隱私影響之評估

本公司定期進行風險評鑑，並以「計畫、執行、檢查、行動(Plan-Do-Check-Act)」為中心，擬訂相關流程，交由本公司資訊安全維運小組負責，該小組由本公司各單位各派一人共同組成，屬本公司個資保護業務之最高決策單位。

2、 事故通報之流程

關於事故通報流程係以「資訊安全事故管理作業規範與程序」處理之，該處理程序符合 ISO 認證所要求之水準。

3、 個資資料庫之管理規範、流程

關於此規範與流程，分別針對檔案、人員、營運場所、檔案存取授權與空管、檔案之正確及維安操作等，並以「通訊與作業管理作業流程及程序、存取控制管理作業流程及程序、資訊系統獲取、開發及維護管理作業流程及程序、資訊安全事故管理作業流程及程序、業務持續管理作業流程及程序與遵循性管理作業流程及程序」等為據，去管理並制定相關流程，以維護客戶之權益。

主題三：監督機制之設立

7、 個人資料保護監督機制之建置情況，包括自律以及他律之面向

(一) 自律方面

本公司自 2005 年至今持續接受 ISO 驗證[632](每三年換證時擴大審查範圍)，業已取得 ISO27001，並新發展出 133 項控制原則擴張其保護密度，亦在近期由委託外部稽核公司：SGS 檢驗公司進行審查，期許能在第三方公正單位檢驗下，在個人資料維護上更加完臻。

本公司設有資訊安全委員會並定期開會，討論與擬定公司資安維護方針與策略，並由資訊安全維運小組成員與稽核室之資安管理部門共同推動，並由稽核室

[632]台灣大哥大新聞中心 2014 年 9 月 25 日報導：為了充分落實資訊安全管理，提升用戶服務品質，自 2005 年，台灣大哥大領先全球取得第一張 ISO 27001 資訊安全管理系統驗證，並於今年同時通過 ECSA 驗證及新版 ISO 27001：2013 三年全面重審驗證，不僅資安防護再升級，也將旗下運算雲服務提升至國際級水準。台灣大順利取得 ECSA 驗證也成功引起了國際注意，包含飛雅特（FIAT）汽車集團等業者紛紛表示願意來向台灣大取經。歐盟雲端聯盟(ECE)副主席 Dr. Tobias 亦表示，未來將在歐美等地行銷台灣大之經驗，以台灣大作為推廣個案，向世界展示國際級雲端服務四顆星的最高榮譽。http://corp.taiwanmobile.com/press-release/news/press_20140925_629870.html
(最後瀏覽日期：2014 年 10 月 3 日)

監督全公司之實踐情況。

(二) 他律方面

行政院國家通訊傳播委員會(NCC)要求每年均需回覆個人資料保護之自評報告，同時會不定期會同相關技術專員，進行稽核檢查，瞭解個人資料之維護方針及其實踐情形。

8、 對於設置第三人獨立監督機構(他律)之意見

承上所述，就目前自律與他律併行運作實況上，對於個資保護誠屬足夠，應無再設置第三人監督機關之必要。

附錄十三 資策會深度訪談紀錄

「我電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫
深度訪談：財團法人資訊工業策進會 科技法律研究所
科技應用法制中心

訪談日期：2014 年 10 月 7 日

受訪者：邱映曦主任

主題一：臺灣個人資料保護與管理制度規範之執行現況

1、 業者對於 TPIPAS 之接受度？反應如何？

答：99 年至 101 年為基礎建立階段，包含建立輔導機制與運作、企業試辦導入等等；101 年至 103 年深耕擴大階段，完備制度正式運行，強化推廣企業導入；104 年開始進入全面擴散階段，推動國際互相認證，持續因應法制與實務調整，強化國際參與連結。以推廣說明會參與對象分析(台北場與高雄場合計)，公務機關約占二成、非公務機關約估八成。目前已取得標章之事業有 13 家，尚有多家業者仍在輔導導入階段。

2、 TPIPAS 之執行成效？對於個人資料保護之強化有無實際效果?

答:TPIPAS 之主旨是協助國內事業建立管理制度落實個資保護,分作四階段循環，依序是推動與規劃個資保護與管理制度計畫、依據計畫內容加以運作制度、監督與審查個資保護與管理制度運作、改善個資保護與管理制度。核發通過驗證之事業 dp.mark，有效期限以兩年為期，本標章與日本 P-mark 標章於建置過程即有相互交流，未來有機會相互認證。TPIPAS 協助個資管理，包括安全維護措施、安全維護事項以及適當之安全措施[633]，透過個人資料盤點與法規盤點檢視公司內部從

[633] 個人資料保護法施行細則第 12 條第 2 項：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、

執行面、人力管理和文件管理流程，要求事業為建置個人資料管理制度，應製作個人資料保護管理手冊，訂定具體規則，並提出有效方式維持機制運作，供事業依循使用[634]。

3、 dp.mark 與既有之 ISO 和 BS 區別

答：ISO 為資訊安全管理系統標準之認證，針對組織資訊資產為驗證範圍，事業可以指定特定範圍進行稽核。BS10012 由英國標準協會基於 OECD、APEC 籍資料保護法對於個人資訊管理制定而來，事業可以指定特定範圍進行驗證，證書之發放無區別全事業或特定範圍通過，消費者難以區別證書效力。TPIPAS 係以我國個人資料保護法與其施行細則作為基礎所建立之標準，內容涵括法遵與資訊安全面，事業須以全事業、全流程申請驗證，於通過書面審查與實地審查後方可取得 dp.mark 標章之使用資格（隔年會進行期中查核，確保事業個資保護工作之落實度），事業建置過程中若有需要先就完成之流程進行評估，可申請特定範圍檢視，惟檢視完成並不會獲得標章授證，而係針對檢視流程範圍之評估報告。事業仍需完成全部制度建置通過驗證方能取得標章。

主題二：輔導電信事業取得資料隱私保護標章

1、 輔導電信事業導入 TPIPAS 之規劃？

答：早期僅限電子商務業，但是自 102 年起，導入產業已無行業別限制，所有產業皆可申請導入。制度建置步驟分作人才培育[635]、建置準備[636]和導入工作[637]。推廣時期，多家電信事業亦有派員參加推廣說明會，以及目前也有派送人員參加 TPIPAS 專業人員資格課程[638]接受 TPIPAS 專業人員訓練[639]。dp.mark 標章之核發是

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。

[634]具體規則內容至少包括：(1) 識別法令與其他相關規範。(2) 識別事業所保有之個人資料。(3) 事業蒐集、處理或利用個人資料之事宜。(4) 個人資料相關之風險分析及管控措施。(5) 事故緊急應變。(6) 事業各部門以及層級所擁有個人資料管理權限與責任。(7) 當事人權利之行使。(8) 維持個人資料正確性。(9) 安全管理措施。(10) 事業人員之監督與獎懲。(11) 委託蒐集、處理或利用個人資料之監督。(12) 教育訓練。(13) 個人資料管理制度之文件與紀錄管理。(14) 當事人申訴及諮詢。(15) 內部評量。(16) 矯正及預防措施。(17) 最高管理階層定期檢視。

[635] 培育 TPIPAS 管理師、TPIPAS 內評師和 TPIPAS 驗證師，但驗證師非必要培育人員。

[636] 建置個人資料保護與管理制度推動小組、各功能小組分工以及各程序與管理文件建立準備。

[637] 確定導入作業流程或部門，全事業或分階段導入；導入範圍分工；規劃各工作完成時間。

[638] TPIPAS 專業人員資格課程：指制度維運機構所開設之個人資料管理師、個人資料內評師及個人資料驗證師課程。

以法人格為單位，所以事業體較為龐大、繁雜者，因此曾有電信事業者詢問是否得以分公司名義取得標章,但依照規定標準仍是建議該事業採行分階段導入方式，終至全事業導入完成並驗證通過後才能依規定核發標章。

2、 已核發 dp.mark 之數量？目前已取得 dp.mark 之事業類別？

答：目前已取得標章之事業有 13 家，分別為臺灣集中保管結算所股份有限公司、統一資訊股份有限公司、日翊文化行銷股份有限公司、統一超商股份有限公司、全家便利商店股份有限公司、康迅數位整合股份有限公司、欣亞數位股份有限公司、博客來數位科技股份有限公司、台灣樂天市場股份有限公司、亞東電子商務股份有限公司、特力屋股份有限公司、特力屋室內裝修設計股份有限公司、香港商雅虎資訊股份有限公司臺灣分公司，包含電子商務業(75%)、金融業(8.3%)、資訊業(8.3%)和物流業(8.3%)。

3、 承上題，前述業者從導入 TPIPAS 到取得 dp.mark 所需時間、成本？

答：目前採行輔導與驗證分流方式，驗證規費具有統一標準，但是輔導單位的輔導方式依受輔導事業體之需求而有數種方案，當然所需費用亦因方案不同而有所差異。綜言之，業者從導入 TPIPAS 到取得 dp.mark 所需時間、成本依事業體規模大小而有所差異，耗費時間預估半年到三年不等，成本從數十萬至上百萬不等。

[639] TPIPAS 專業人員：指個人資料管理師、個人資料內評師及個人資料驗證師。

附錄十四 法務部法律事務司深度訪談紀錄

法務部針對國家發展委員會「我國電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫之研究團隊訪談問題之回應意見

一、 在現行個資法之規定下，有關民間部門遵守個資法之監督事務，依其第 19 條之國際傳輸、第 22 條之資料檔案安全維護等檢查、第 27 條第 2 項指所主管業者訂立安全維護計畫等，均為由中央目的事業主管機關擔任。則:

(一) 面對眾多之所管事業，中央目的事業主管機關有無執行上之困難?

(二) 有無在中央目的事業主管機關各自為政下，發生法律解釋互相矛盾，執法寬嚴不一問題之虞?

(三) 個資法涉及許多資訊科技之問題，如雲端等，中央目的事業主管機關在資訊專業人力上，能否應付?

本部回應意見：

(一) 上開問題所述有關「國際傳輸」部分，應係規定於個資法第 21 條，而非第 19 條；另就個資法第 22 條有關「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」等檢查業務之執行，係由中央目的事業主管機關或直轄市、縣（市）政府執行之，而非均由中央目的事業主管機關為之,又中央目的事業主管機關與直轄市、縣(市)政府間之權責劃分，應依各該主管機關原對該事業監管權責之業務分工決定之，合先敘明。

(二) 問題 1 及 2 部分，鑒於非公務機關蒐集、處理及利用個人資料乃附隨於其所經營之事業，而各個行業均有其目的事業主管機關，自宜由各該目的事業主管機關針對各行業屬性及特殊性，一併監督管理附隨於該業務之個人資料保護事宜，故個資法規定各目的事業主管機關具有監督與管理權限，

而本部則為個資法之法律解釋主管機關。是以，有關中央目的事業主管機關對於其所管轄非公務機關之監督及管理有無執行上之困難，尚非本部所能回應。至於目前中央及地方各機關如有個資法解釋適用之疑義或解釋不一致之情形，本部基於法律主管機關之立場，均會提供釋示或法規諮商意見。

(三) 問題 3 部分，中央目的事業主管機關在資訊專業人力上能否應付乙節，應視各機關之業務需求及所配置之資訊人員專業能力而定。

二、 跨國傳遞個資已為大企業事業營運之所需，依歐盟指令或其他有關個資之國際協約等，為保護個資之安全，大多要求相對國須有完整之個資保護法制，其中獨立監督機關之設置為必要之條件，而我國目前為止並未設置相當之機關，請問貴部對此問題有何建議或想法?

本部回應意見：

(一) 參諸我國以外國家或地區之個人資料保護機關(構)(例如：英國、法國、加拿大、香港、澳門等)，所謂「個人資料保護專責機關」，除負責個人資料保護之政策法規制定外，尚包含監督管考事項（督導、調查、處罰、協調、建議、統計、訂頒指南、評鑑考核、施行報告、人員培訓、法規宣導等），再依歐盟指令或其他有關個資之國際協約等，更應具有獨立行使職權之法定地位，亦即具備相當之獨立性，惟囿於現行中央行政機關組織基準法第 32 條第 2 項規定，相當二級機關之獨立機關總數以 3 個為限，而現已有中央選舉委員會、公平交易委會及國家通訊傳播委員會等 3 個機關，事實上已無法再增設二級之獨立機關；另依同法第 33 條第 1 項、第 3 項規定，二級機關及相當二級機關之獨立機關為處理技術性、專門性業務需要得設附屬之機關，同條第 4 項規定，第 1 項及第 3 項署、局之總數除地方分支機關外，以 70 個為限，而目前設立之三級機關總數已達 70 個上限，故若欲設置屬於上開三級機關性質之機關亦有困難。惟依中央行政機關組織基準法第 32 條第 3 項規定,第 1 項以外之獨立機關(即非相當二級機關之獨立機關)，其內部單位之設立，依機關掌理事務之繁簡定之，又同法第 33 條第 4 項所定署、局之 70 個總數限制，似未包含相當三級機關之獨立機關(按：獨立機關為合議制機關，應稱委員會，同法第 6 條參照；目前相當中央三級

獨立機關有飛航安全調查委員會)，故依上開中央行政機關組織基準法規定，倘於行政院下設「相當中央三級獨立機關」之個人資料保護專責機關，亦無牴觸現行法制。惟是否設置個人資料保護專責或獨立監督機關，涉及行政院之政府組織改造決策權，本部對此不表示意見，並尊重行政院之決策權。

(二) 目前在現有資源與條件未變更，而無法設置專責或獨立監督機關之情況下，本部仍將基於個人資料保護法之法律解釋主管機關之立場，以有限的人力、預算致力於個人資料保護法相關之研擬、解釋及推動工作；各中央目的事業主管機關或直轄市、縣（市）政府則就所管事業（團體、個人）就關於個人資料之蒐集、處理、利用及安全維護等事項加以監督管理；至於中央目的事業主管機關與直轄市政府、縣（市）政府間之權責劃分，則依各該主管機關原對該事業監管權責之業務分工為之。又為解決各機關執行非公務機關個人資料保護事項所生爭議，行政院於 101 年 10 月 22 日以院臺法揆字第 1010061195 號函同意本部函頒之「個人資料保護法非公務機關之中央目的事業主管機關」，故各機關按其原對該事業監管權責之業務分工，受理有關個資法之申訴案件，與單一窗口功能相同。另關於各機關因權責劃分所產生之管轄權爭議，除依行政程序法第 13 條、第 14 條規定處理外，並由本部視爭議情形主動邀集相關機關共同商議，以期建立聯繫協調機制，解決個資法申訴案件之管轄爭議，加快案件之妥適處理。

三、 如有獨立監督機關設置之必要，在現行中央行政機關組織基準法對二級、三級機關均設有總數之限制下，如不進行修法應如何突破此一限制?

同前一題回應意見。

四、 在不修正中央行政機關組織基準法下，改以在現有二級機關中，有無可能設置位階如局、署等機關(當然須為委員組成之合議制)，擔任監督之職權?如有可能，則在何二級較為合適?

本部回應意見：

鑒於歐盟指令或其他有關個資之國際協約等對於個人資料保護獨立專責機關之認定標準，現行相當於二級獨立機關之國家通訊傳播委員會，正符合獨立於行政機關外、獨立行使職權之委員制機關，且依國家通訊傳播委員會組織法第 4 條

第 3 項規定，該會委員應具電信、資訊、傳播、法律或財經等專業學識或實務經驗；同法第 3 條第 8 款規定，該會之職掌包括「資通安全之技術規範及管制」，而個資法規範事務中包括個資之國際傳輸及安全管理措施，應得由該會統一管理。是以，考量現今網際網路之普及，及相關科技產業之蓬勃發展，個人資料之國際傳輸頻繁，不論係公務或非公務機關基於商業、科技或國家安全等動機所為，其所衍生相關個人資料保護措施、安全管理之建置等問題，均有賴於相關專業知識、技術始能為監督及管理，故似可考量於國家通訊傳播委員會下設一局或署，專責監督各機關有關個資法之施行，惟同前所述，目前設立之三級機關總數亦已達 70 個上限，故於未修法前，於現有二級機關中設置位階如局、署等機關，似尚無可能。

附錄十五 中華電信公司深度訪談紀錄

「我電信事業及電信加值網路業個人資料保護與監管機制之研究」委託研究計畫
深度訪談：中華電信

訪談日期：2014 年 10 月 15 日

受訪者：資訊處、法務處、客服處、行銷處

主題一：遵法義務之實踐

1、個人資料運用特定目的之擬訂與告知。是否就個資蒐集、利用或分享，事先取得客戶之同意(同意方式為何)? 並告知客戶將進行其個資蒐集、利用或分享(告知方式為何)? 客戶反應為何?

答：1.門市人員引導客戶閱讀本公司「客戶個人資料蒐集告知條款 」，依法執行告知義務，並 請客戶簽名，取得書面同意。在新法施行前(舊法時期的客戶)依當時法律規定以公告方式為之。2.客戶接受度高，並無特別反應。

2、蒐集之電信使用人/契約用戶之資料種類；資訊分享第三人(關係企業或非關係企業)之情況及分享的個資類型與範圍。

答：1.本公司蒐集客戶個資係屬一般個資，且本公司並無資訊分享之情形。2.各門市電腦均連結至資訊系統，門市人員以專屬帳密登入，方能作業，且每次作業系統皆留下紀錄。3. 客戶申請業務之紙本文件係依據本公司訂定的文件處理流程進行保護，門市不能以任何方式留存數位形式之客戶個資。4.本公司管控各門市電腦硬體、軟體，電腦螢幕僅顯現必要之資訊，客戶個資欄位以部分隱碼方式呈現。

3、跨國(與國外或中國大陸業者之間)傳遞個資的實務運作。

答：本公司無跨國傳遞個資業務或相關作業，倘遇特殊狀況是提供設備號碼進行

查詢。

4、依個資法第 4 條委外處理個資的情況，如何監督受委託者？

答：委外處理個資依本公司個資管理規範執行，並定期執行監督作業：1.受託者必須簽訂保密協定(包含合約書中之個資保護條款、委外廠商簽具保密同意書、委外處理人員簽具保密切結書)。2.本公司委託單位負責查核受託廠商，每年指派專人定期到各門市、營運處實地查核個資保護情形。3.銷毀個資文件時，指派專人全程監督銷毀過程，並拍照或錄音錄影。

5、特定目的外利用個資的情況有哪些？多為自行使用或提供資訊給第三人(國安單位、檢警單位、救難單位等第三人)？

答：依據通訊傳播委員會訂定之「電信事業處理有關機關查詢電信通信紀錄實施辦法」1.配合檢、警、調、法等有關機關(構)、稅務機關執行法定職務，提供其查詢之客戶資料 2.至於生命線、張老師、119、110、112 等特定單位個資需求，因隸屬特碼服務，自動顯示來話單位，本公司依相關法規配合辦理急難救助與人道救援作業。

6、電信利用人/契約用戶主張資訊自主權(如個資法第 3、10 條)之處理流程。

答：1.本公司已建立客戶主張法定個資權利處理機制與流程：客戶可至本公司各門市或透過客服專線主張個資權利(如申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用個人資料等)，比如客戶拒絕接收廣告行銷資訊，一經提出要求，門市或客服人員受理後，均登錄系統並予註記，往後本公司不再傳送此類資訊給此客戶。2.依「固定/行動通信業務管理規則」，攜碼轉入他家電信公司及結束契約關係之客戶紙本資料留存期限，至少須保存 1 年，期滿後依客戶要求予以銷毀。

主題二：安全維護機制

1、隱私影響之評估。

答：1.本公司個資風險評估準則分作普中高三級，類型分為公務個資、一般個資與特種個資。2. 在風險評估過程中，對所有包含個資之作業系統、業務流程皆會進行盤點，針對資料保密層級擬定系統安全措施進行資訊管理與存取限制。3. 每年會重新檢視風險評估之正確性，並進行制度規範修訂作業。各機構有設置個資管

理師與個資內評師 ，可提供個資問題之諮詢。

2、事故通報之流程。實際客訴之樣態有哪些?

答：1.承前所述，本公司已訂立事故通報作業流程，依據資料層級和嚴重性區分通報等級進行分級處理，如發生重大個資事故將通報至總公司或通傳會。2.客訴最常詢問的問題是收到廣告簡訊或不明簡訊，一旦收到此類反應會進行內部查核，確認是否發生內部外洩情況，並將處理情況回覆客戶。

3、個資資料庫之管理規範、流程。關於個資安全維護(程序上及組織上)之具體作法為何，以符合個資法施行細則第 12 條規定?

答：本公司有訂定個資保護政策與規範，總公司至分公司皆設立個資保護小組，以各單位副首長(含)以上作為核心人員，進行整體串連管理；個資管理分作九大體系，各體系依業務內容訂立作業準則。

主題三：監督機制之設立

1、個人資料保護監督機制之建置情況，包括自律以及他律之面向。

答：1.在自律部分，本公司對於個資之處理、利用和蒐集，以個資法為基準訂定作業流程與作業準則，並對本公司員工和協力廠商之員工進行教育訓練（e-learning 系統）和定期檢測。2. 基本上，無論本公司員工或協力廠商之員工皆須簽訂保密協定。個資外洩罰則，一筆資料外洩處罰三萬元，累計處罰。3. 本公司使用資訊系統進行作業處理，每個同仁皆有專屬帳號與密碼作為識別（依照公司規定禁止共用帳密，違者依罰則處分），當使用帳密登入資訊系統後，每次個資作業皆會留下紀錄，各個單位主管每日會收到紀錄報表(註記使用目的)，並立即針對特異使用行為進行處理。4. 客服專線部分現正全面導入 BS10012 認證，預計明年全部完成。公司每年會定期進行個資查核，並針對發現之問題進行處理與修改作業規範。綜言之，以遵循國際標準、個資法及通傳會公布之規定，用最嚴謹的標準進行個資保護作業。

2、對於設置第三人獨立監督機構(他律)之意見。

答：對於設置監管個資保護事務專責機關的第一個顧慮為該機構是否能夠兼顧各產業不同之特性與需求；再者，該機構是否熟悉(了解)各產業之實務狀況。第三，目前的監督機關在中央有通傳會，在地方則有各地方縣市政府監督，所以已是層

層交疊；法規解釋部分則有法務部，目前作業程序運作順暢、意見溝通交流無阻，所以就現況而言，似乎未有此需求。若是在現行體制外又增加新機構，會使業者無所適從。

附錄十六 期中審查意見回應表

103 年度「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」委託研究計畫案期中報告審查意見回應表

審查意見	回應說明
一、研究方法	
(一)本研究計畫擬從法規面、實務面與比較法等三面向進行闡述分析，惟前兩部分內容偏向於條文及章則的說明，比較法部分則未回饋至研究本身，建議後續應針對現行法令爭點、缺失與未來改善的方向加以分析，並於各章後增加小結說明，以強化各章節的連結性。	因研究計畫之初期重在各對象國法規及其現況之調查與資料蒐集，故各國負責之老師僅先就蒐集所得資料整理分析，尚未進行綜合之比較，及與我國法規之檢討部分；關於我國現行法令與外國立法例之比較，以及對我國法之檢討與未來修法建議，請參閱第五章。 感謝審查委員之建議，本研究團隊會於撰寫期末報告時，在各章結尾增加小結說明。
(二) 有關國外比較法制部分尚稱完整，惟仍屬偏向各國法制內容的介紹，建議針對未來應如何引進國內作為政策參考，進一步分析整理，並與我國相關規定列表比較。另文獻分析除美國部分引用專業論文資料外，其他各國法制仍為條文介紹或透過網路檢索的相關資料，建議加強學術及實務上的參考資料，並適度引用各國相關司法案例與行政法令，以提高參考價值。	關於國外立法例如何引進並與國內立法例比較或作為修法參考，為屬於本研究計畫後半段之重心。請參閱第三章。
二、研究內容	
(一) 第二章章名為「自憲法、個資法和通保法檢視個人資料保護之『重要	將遵循審查意見自憲法保障通訊秘密之基本人權，其重要性及內容作補

審查意見	回應說明
性』」，惟多數內容僅係就相關法條內容進行說明，未論及其重要性。另因各章節尚未就現行法令爭點與缺失進行整理分析，故中文文獻部分偏重憲法及科技法部分，建議後續強化政府管制行為的行政法學理說明，並適時納入行政案例的相關見解。	充說明。又政府管制行為的行政法理學部分，因其屬於原計畫中監督管制專章部分之內容，為本計畫期中報告後行之重點，期末報告已在第二章和第五章加以處理；實務案例部分請參見第三章。
(二) 有關我國個人資料保護之法規與實務問題，應分就「政府管制」與「市場機制」面向，探討兩者如何配套實施，以進一步探求制度的全貌。	個人資料之保護與市場機制之同樣為涉及政府對業者(不限電信業者)之監管深度與強度之問題，亦即業者之自律與他律之政策選擇，此部分同樣在第四章監督管制專章中朝貫徹自律與他律兩個面向之研究角度作討論。舉例而言，業者自律部分，比如隱私權政策 (privacy policy)或是輔導與取得個資保護認證標章，例如：臺灣個人資料保護與管理制度規範（TPIPAS）和 DP Mark，請參閱附錄和第四章監管機制專章。
(三) 依據第三章章名主要係對我國電信業個資保護進行介紹，惟章節中亦有國際認證標準的相關內容，建議研究團隊對相關章節編排內容予以調整。	國際認證標準乃係業者為符合個資法對資安維護之要求，以廣義定義而言，此亦為我國電信業者為遵循個資保護所採取之實際自律措施，因此於期中報告時暫定於第三章呈現；然，期末報告已將國際認證如 ISO、英國之 BS、日本之 P-MARK 制或我國的 DP Mark 等性質上屬業者自律機制，改為在監督管制專章中作討論。
(四) 本計畫研究對象為「電信業及電信加值網路業」，惟現行期中報告內容僅聚焦於第一類電信業者部分，後續宜就第二類電信業者及電信加值網路業部分內容進行補充。	有關類電信業者與電信網路加值業部分，將於本計畫報告第二章說明其沿革，及其營業內容，在就其提供服務部分與電信有關之部分討論所涉及個資之蒐集、處理及利用之問題。

審查意見	回應說明
(五) 有關研究資料部分，建議可再參考法務部之公務機關「個人資料保護執行程序暨考核作業手冊」與 Protecting Consumer Privacy in an Era of Rapid Change：Recommendations For Businesses and Policymakers(FTC.2012)等資料。	感謝審查委員的建議，本研究計畫將納入建議參酌資料，並已在期末報告中(歐盟、美國)妥適之章節加以討論。
三、研究初步發現與建議	
(一) 有關建議訂定「指導綱要」的意義，應再進一步說明，因行政指導並非行政處分，不得據以要求業者為強制措施，其並不符合「政府管制」的公權力要求，爰是否仍應強化業者的法定義務，建議研究團隊予以說明。另可再參酌法務部「個人資料保護執行程序暨考核作業手冊」及國外相關機制，探究電信業個資保護機制之指導綱要的必要性與主要內涵。	「指導要綱」確為行政指導，故對業者無強制拘束力，如對電信業者要強化其法定責任，進行強制性管制必須立法或修改，此亦為政策考量之選項之一，此部分亦為中間報告尚未處理之部分，已在期末報告第四章監督管機制和第五章問題發現與建議專章中作討論。
(二) 研究發現欠缺對我國現行法制缺失的檢視，且內容說明多數電信業者期望主管機關通傳會訂定「指導綱要」，與建議事項中要求法務部主政部分，兩者似有矛盾。爰未來應如何協調配合，建議研究團隊予以說明，並提供下列建議：	此部分亦將在參考各國制度後，並比較我國之現行法制後，建議電信業者蒐集、處理及利用個資之主管機關(監管機關)如何決定較適當、其組織、職權等均會在結論中交代，法務部所疑慮之事會納入考量，以提出可行之建議。請參閱第五章問題發現與建議專章。
(三) 初步研究發現歐盟會員國的英國與德國，除了修正該國主要個資法規範以符合歐盟指令要求外，並同步修訂該國電信法相關規範以期符合標準，惟期中報告似尚未針對我國電信業及電信加值網路業之行業特殊性，提出專門性之個人資料保護與監管機	誠如審查意見所述藉由參考外國立法例，研擬適用我國之法制與監管機制之期待，亦為本研究計畫之重要目的，如前述回應意見，，已在期末報告第四章監督管機制和第五章問題發現與建議專章中作討論。

審查意見	回應說明
制具體政策建議，建議研究團隊持續蒐集資料及外國立法例，進行相關分析及研究，並於期末報告提出適用我國的法制策略及監督管理機制。	
(四) 建議研究團隊後續可參酌現行電信產業的個資保護現況議題，加以深入分析探討。如個人資料之國際傳輸課題，通傳會已於 101 年 9 月 25 日公告明訂限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至中國大陸地區。其次有關小米手機因將用戶個人資料回傳至位於北京的伺服器，所引發的相關爭議。此外，歐盟法院在 google 案中，判決民眾可向網路搜尋引擎業者主張「被遺忘權」，所可能產生的衝擊影響等議題。	個人資料之國際傳輸(跨國傳輸)確實在歐盟指令及 OECD 之指導原則有特別規定，是可探討之議題;另外如個資委外處理之規範、蒐集告知之方式、資訊隱私政策(privacy policy)之公告內容等，均會在後續之研究中加以探討。 關於小米機之問題，事實上市手機製造時藏置於硬體中類似於 cookie 之軟體，用以蒐集使用者之資料，基本上非為電信通訊者之所為。另外歐盟法院所承認之「被遺忘之權利」，實質上為當事人請求刪除權之加強或延長，且為針對如 GOOGLE 之蒐尋網站，在公開領域蒐集個資之行為，賦與當事人之權利，似乎與本研究計畫針對電信業者蒐集、處理個資之研究方向有所差異。 歐洲法院在 Google 一案中所指明之「被遺忘權」，主要乃確證人民有權向網路搜尋引擎業者請求封鎖載於其資料庫特定個人資料與記錄之權利，該判決適切地展現歐盟新近個人資料保護的走向，確有其重要性。惟該權利是否得擴張拘束本研究計畫之主要對象：電信業及電信加值網路業之業者，仍有疑問，故擬將其列為介紹歐盟個人資料保護趨勢之司法案例之一，持續充實。

審查意見	回應說明
(五) 因應科技之進步與產業擁有大量客戶個人資料之特性，各國就個人隱私保護法制之設計，除一般立法外，更有專精化立法或制訂特別法之趨勢，未來我國的立法策略為何？此外，通訊傳播產業正朝向整合的方向前進，包括電信、傳播與網際網路在內，電信業者的個人資料管理，是否需要有類似金融控股公司之子公司間進行共同行銷的相關規範，均值得研究團隊加以思考探究。	感謝審查委員的建議。關於是否針對電信產業特立專法處理類似金融控股公司之子公司間，利用個資進行共同行銷之規範問題。本研究團隊會參酌外國立法例並考量我國電信業共享實況後，在期末報告相關章節中分析並提出建議。金融控股公司之子公司間，利用個資進行共同行銷，則為個資共同利用之問題，本研究案將在個資利用之部分討論。
四、文字格式與其他	
(一) 研究報告各章應由單數起頁，相關版面配置(頁眉)宜符合本會委託研究作業要點規範，另附錄文字字型大小均請與本文格式一致。 (二) 附錄中有關德文「行為準則」條文應譯為中文，以提供閱讀上的參考價值。 (三) 報告第 4 頁倒數第 5 行提及「依我國個資法第 27 條之規定，無論公務機關或非公務機關皆應採行適當之安全措施，…」惟個資法第 27 條僅有規範非公務機關個人資料檔案之安全維護事宜，公務機關個人資料檔案之安全維護事項係規範於個資法第 18 條，相關文字應予修正。 (四) 報告第 13 頁有關個人資料之定義部分，似有所缺漏，建請修正。 (五) 報告第 48 頁提及歐盟個人資料保護指令要求加盟國有義務賦予個資保護監督機關獨立性，權限第 3 點提及「關與權限」語意不明，建請一併	感謝指正，關於文字格式與字義增補、個別統計數據等問題，本研究團隊皆會在期末報告中一併加以改正。 德國電信（Deutsche Telekom）企業內部所適用之行為準則，由於在期中報告中已就與本研究相關部分進行譯介（頁 69-74），故附錄中並未再附上中譯。團隊討論後未於期末報告佐附作為附錄。

審查意見	回應說明
援引原文，以資明確。 (六) 第 170 頁第二類電信業者名單資料，建議比照第 150 頁於表末增列各業務項目之個別統計數據。 (七) 報告中交錯使用「民國年」與「西元年」，宜將相關格式一致化處理。	

附錄十七 期末審查意見回應表

103 年度「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」委託研究計畫案期末報告審查意見回應表

審查意見	回應說明
一、劉教授宗德（政治大學法律學系）	
(一) 第二章我國法制現況部分稍顯簡略，尤其第五節小結(頁 38)可再強化補充。第三章各國法制部分，各國撰寫體例不一，部分僅止於法條或規章的翻譯，且未針對司法爭訟進行完整分析，建請補正。另各國法制後小結內容過於單薄，建議強化說明各國現況困窘之處，以利我國借鑒參考。此外，比較法制中日文期刊論文較為簡略或陳舊，建請進一步補充。	已於第二章加強說明。第三章撰寫體例不一之問題，因研究對象國家有屬大陸體系之德、日等國，有屬英、美體系之國家，各自有法制展之背景，實難以同一體例撰寫，本研究團隊已盡力就各國現況分析其有關個資保護法制及電信事業蒐集、處理或利用個資之要件以供我國參考，並已加強個小結之內容，對各國特色作說明。閞於司法爭訟之分析，除美國外其他國家有關個資法之案例雖多，然針對電信事業蒐集、處理或利用個資之案例不多見，日本有離職員工洩漏用戶資料之事件。中、日文期刊之缺失已補正。 第五章第一節將與第二章第五節小結進行整併與強化，惟就我國目前所面臨之問題與困境之提出，擬仍維持統一於第五章第一節中說明，以求與緊接其後所提建議緊密結合。第三章第一節歐盟與第二節德國部分，將於既有之司法判決論述上再予強化，增加

審查意見	回應說明
	新的裁判分析。並分別就小結部分進行補強。
(二) 有關各國法制面向資料，說明如下： (1)宜強化我國現行所電信業個人資料保護現況所面臨困境的相關分析(頁 38)。 (2)歐盟資料宜依據前述內容予以擴充小結內容(頁 63)。另於德國內容部分，則建議釐清基本法的規範、法律與法規命令的層次，並強化補充小結的內容(頁 84)。此外，針對歐盟與德國具代表性的訴訟案件，亦可依照英美分析體例予以補充。 (3)建議針對英國小結部分，可再整理出英國的特色(頁 106)。而美國資料部分，則可參考劉靜怡教授與劉定基教授相關文章(頁 158)，強化參考資料的豐富性。 (4)日本資料部分所提及 guideline 係屬行政規則(頁 108)，惟其是否尚有其他法律或法規命令的規範，建議再進一步的確認，或補充說明日本國民與業者遵法的意識與法文化。另小結部分則可再以文字敘述補充強化相關內容(頁 122)。 (5)建議針對韓國資料部分，增列小結之內容，以符各國撰寫體例(頁 131)。	就我國現況與困境的分析，將統一置於第五章第一節中說明，以求與緊接其後所提建議緊密結合。 針對第三章第一節歐盟與第二節德國部分之小結均予以補充強化，德國法制位階的層次，已於第二節一、首段說明釐清。而關於訴訟案件之補充，由於德國屬歐陸法系國家，司法裁判乃作為輔助性法源，其效力及影響力皆不如屬英美法系之英國與美國，故於研究報告之論述安排上仍以成文法規為主，但仍欣納審查委員之建議，適時補充司法實務見解作為輔助。 針對美國資料部分，國內幾無直接涉及美國電信業個人資料保護之中文文獻，但劉定基教授大作「欺罔與不公平資訊行為之規範--以美國聯邦交易委員會的管制案為中心」則與本研究案「聯邦貿易委員會」之功能介紹有關，故予以補充。頁 228。 日本之 Guide-line 為行政指導，日本有個資之保護法制度，係以個人資料保護法為基本法，各領域之個資保護依其為基礎，中央主管機關與業者商議後訂出 Guide-line 作為各該領域之業者應遵守之規範。關於日本此部分之文化與法意識，已於該節小結中說

審查意見	回應說明
	明。已在該節小結中說明，並增列表格顯示。頁 220。 已針對韓國資料部分，增列小結之內容。頁 224
(三) 有關各國與我國監管機制部分，章節編排上應先探討他律或自律機制，建議研究團隊宜有整體性的結構安排與說明，並統一各國體例格式(包含第五章檢討部分)。另第 204 頁有關我國他律部分的監管內容應予補充強化。	章節編排已作調整統一，另 204 頁已補充說明，頁 236-237。
(四)有關報告中所提及法律相關問題，說明如下： (1)第 20 頁註 36 所提通傳會令的法律性質，係法規命令或一般處分的公告，應說明清楚。 (2)第 188 頁第(四)項「命令」應修正為「下命處分」、第(五)項「緊急命令」應為「緊急措施」；又第 189 頁第二段所提「行政命令」應為「下命處分」或「緊急措施」，請研究團隊修正。 (3)第 204 頁第(二)大項第 1 項所提「行政命令」應為「行政規則」，且不需經過發布程序；第 2 項文件索取、通知陳述意見或現場勘驗之措施，則應給予行政程序法上的定位；第 3 項公告認證合格業者名單的法律定位，涉及主管機關係運用何種法規範進行管制，研究團隊宜進行完整的說明。	(1)和(2)之回應 已遵指示修正。國家通訊傳播委員會(NCC)於 2012 年依當時電腦處理個人資料保護法第 24 條第 3 款（現行個人資料保護法第 21 條第 3 款）規定，發布通傳通訊字第 10141050780 號令，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。此一由通傳會依據法律授權所發布之命令，性質上應為行政程序法第 150 條第 1 項所稱：「…行政機關基於法律授權，對多數不特定人民就一般事項所作抽象之對外發生法律效果之規定」，而屬法規命令，爰依審查意見新增說明於第二章第二節三、（三）3、中，頁 22。 (3) 已於標題上給予法律定位，頁 236-237。

審查意見	回應說明
(4)第 209 頁提及「是否適合以行政命令規定」，宜請先確認係指法規命令或行政規則(一般性規定、裁量基準或解釋性規定)，並請以行政程序法上用語說明，以資明確。 (5)第 215 頁第 6 行所提制訂更詳細的法規命令，其法規範的層次為何，宜有更清楚的說明。	(4) 已訂正為法規命令，頁 242。 (5)已作修正，頁 253-254。
(五)短中期建議尚屬具體可行，惟長期建議部分： (1)針對電信通訊與網路通訊兩者，適用統一法規予以規範之建議過於籠統，應提出具體明確之制法或修法的建議。 (2)獨立監管機關之設置，建議於通傳會下設一局或署之三級機關，似不可行。建議可研議將「行政院國家資通安全會報」升格為委員會(任務編組)，並令其兼管個資保護，較為可行。	(1)關於電信通信與網路通信是否統合由同一法律規範?因網路通信有具公然性與非公然性之通信，前者固可與傳統電信通信統合由同一法律規範，而後者涉及表現自由之問題，實不宜與傳統電信通信統合由同一法規範，此為立法或修法時須慎重考量之事，故目前本研究計畫僅建議將非公然性之通信如 E-mail 等納入電信法中保護。頁 254-259。(2)謝謝指教，此部分已於第五章全面改寫。頁 255-259。
(六)報告內容與文字疏漏部分： (1)第 1 頁提及民國 100 年部分請修正為西元年、另報告中所提「大法官會議」宜統一修正為「司法院解釋」(頁 11)。 (2)第 2 頁倒數第 3 行提及第一類電信業者，以及第 32 頁至 40 頁將第一類電信事業個人資料保護政策進行比較，建議予以平衡報導處理，以避免誤解。	將統一使用西元年，並將用語修正為司法院釋字第 000 號解釋。審查意見所提出本報告就第一類電信個人資料保護政策進行比較之部分，採樣多家第一類電信事業之隱私權政策或聲明進行相互對照，包括中華電信、台灣大哥大、遠傳電信、威寶電信及亞太電信，避免偏重任何一家電信事業，力求謹慎維持研究之中立與衡平此部分已全部修正，格式問題已依照建議

審查意見	回應說明
(3)第 6 頁圖表第一欄位第二透過網路論壇，應予調整。第 9 頁預期目標一併修正。 (4)第 18 頁註 29 所提前揭註應為註 24、第 22 頁註 42 所提前揭註應為註 40，相關註釋均請一併檢視與修正調整。 (5)註 352(頁 117)所提高橋和之論文全稱、出版年月。註 361 及 362(頁 125)等相關書目宜補充資料出處。註 545(頁 183)所提藤原靜雄同註 15，應屬誤植，請修正補充。 (6)第 161 頁提及歐盟指令「③『關與』權限」應修正為「干預」、第 162 頁第(3)項應修正為「資料保護及隱私委員」、第 213 頁第 3 行「法遵」宜修正為遵法的義務。 (7)第 186 頁第三段所提 13,753 家業者取得認證標章資料應予更新、另第 187 頁第二行提及日本監督權限行使方式是由緩而嚴之漸進式，應補充「附圖二」之資料。 (8)第 189 頁末段說明「個人編號法」預定三年內施行，惟該法有些內容應係自公布日開始實施，請研究團隊重新對照加以修正。	修改。如頁 189，修正為「資料保護及隱私委員」；頁 215，更正最新業者樹和資料網址。
二、劉秘書長佐國（臺灣隱私權顧問協會）	
(一) 建議強化研究建議相關具體作法的說明，俾提高政策建議的可行性。	已於第五章建議中加強說明，頁 252-259。

審查意見	回應說明
(二) 第 209 頁第 2 項所提「規範位階之疑慮」內容，行政規定與行政命令的概念似有混淆，建請釐清後加以修正。	已修改為法規命令，頁 242。
(三) 第 221 頁第(二)項提及「金融控股公司法」第 43 條已修正，建議確認相關修法情形。另第(三)項建議主管機關依個資法第 19、20 條規定建立名單查詢機制，相關條文引用似有疑義，建議強化辦理方式之可行性。	已作確認依修正後之第 43 條說明。關於名單查詢機制，因屬訂約時查詢是否為積欠費率用戶或濫行發送垃圾郵件之用戶，故應可依個資法第 19 條第 1 項第 2 款與當事人有類似契約關係之規定合法蒐集。而提供者得依第 20 條 1 項第 4 款為防止他人權益之重大危害之規定提供；如有違比例原則之虞慮，則建議在與客戶訂立服務時，在蒐集利用個資條款中加入得蒐集並利用此項資料之同意條款，避免爭端。頁 254-255。
(四) 個資法施行細則第 8 條規定委託事項監督之事宜，建議研究團隊適時納入研究報告中探討分析。	已加入於第二章將個人資料保護法施行細則第 8 條委託機關監督受託機關之事項，由原先註腳提升至本文中加以說明。頁 20。
(五) 第 220 頁有關蒐集個人資料之告知義務的相關建議，可補充建議業者向當事人蒐集個人資料時，應多採取讓當事人選擇加入(opt-in)的方式，而非選擇退出(opt-out)的方式，且告知不應為形式上的告知，俾真正落實保護個人資料的立法精神。	已如建議作補充。頁 253-254。
三、戴資訊長豪君（財團法人資訊工業策進會）	
(一) 本研究於實務面向觀察隱私政策	已建議通傳會全面審視各電信事業之

審查意見	回應說明
之公告，與電信業者在服務契約中個資蒐集告知條款，結論具有一定貢獻，建議可進一步請通傳會進行相關定型化契約範本或隱私政策指引的研擬作業。	服務契約。頁 253。
(二) 因電信產業擁有大量客戶個人資料之特性與科技快速發展的趨勢，各國就個人隱私保護法制之設計，除一般立法外，更有專精化立法或制訂特別法之趨勢。本計畫結論認為各國多以個人資料保護之基本原則為基礎，針對電信通信業個人資料之蒐集、處理或利用，制定特別法或、頒布行政法規加以規範，或可作為我國立法策略之參考。	謝謝指教
(三) 本研究所提短期實施建議尚屬可行，惟應建議通傳會自行檢視是否已依個資法要求建立各項相關規範，包括訂定個人資料檔案安全維護計畫、業務終止後個人資料處理方法、行使行政檢查權之規定，以及訂定各種個人資料特定目的等，及其執行成效與優缺點。	已作建議，頁 253。
(四) 在中期得實施建議部分，考量通訊傳播產業正朝向整合的方向發展，包括電信、傳播與網際網路在內，有關電信業者之個人資料管理，建議訂立電信事業與其子公司或關係企業共用用戶或使用人個資行銷之範圍及要	如二之 3 之回應

審查意見	回應說明
件，應予以肯定。其次，就電信事業得對欠繳費率、濫發電子郵件客戶或使用人，建立名單查詢之機制，應是在現行徵信機制與「濫發電子郵件管理條例(草案)」仍無法有效落實的前提下方可進行。	
(五) 在長期得實施建議部分，研究團隊所提出於通傳會下設三級個資保護獨立監督機關，應同時考量其若面對所有行業的主管機關，有無足夠的人力與量能，以同樣的標準處理各產業個人資料管理工作。此外，宜將目前組織改造相關法令規範納入考量，爰建議或可朝向各部會內部設專責單位方向思考，不再侷限於設置局或署的概念。	此部分已作全面之改寫，頁 255-259。
(六) 第二章討論我國個資保護法制與業者因應機制，建議適度納入相關司法案例、行政法令或相關函釋，俾報告內容更為周全。	就期末報告初稿中既有之相關司法案例與函釋再行深入討論外，另補充與本研究計畫相關之司法實務案例：補充之 M+Messenger（台北地院 103 年度北小字第 1360 號判決、台北地院 103 年度小上字第 155 號判決）、補充之全民健保資料庫（北高行 102 年度訴字第 36 號判決，最高行 103 年度判字第 600 號判決）、補充之 B&Q 特力屋（士林地院 103 年度湖小字第 537 號判決）以及行使被遺忘權請求移除網路搜尋結果(台北地法院 103 年訴字 2976 號判決)等司法判決。

審查意見	回應說明
(七) 有關第四章電信事業監管機制之介紹，其中提及歐盟之指令，部分使用名詞與描述方式與其他章節有所差異，建議予以調整。另第二節德國部分，係討論一般個人資料之監管機制，建議應針對電信事業主管機關如何進行個人資料管理進行補充。	第四章歐盟部分之用語予以修正調整（第四章第一節頁 188-189）。 依據審查意見於第四章第二節中新增德國電信事業主管機關之說明。依據德國電信通訊法規定，其主管機關除聯邦民生網絡署（BNetzA），依據該法負責電信服務業者營運之監督與管理外；另就電信服務業者蒐集、處理、利用個人資料之行為，依據電信通訊法第 115 條第 4 項交由聯邦資料保護與資訊自由監察機構（BfDI），依據德國聯邦個人資料保護法之相關規定負責監管。頁 193-201。
四、廖副教授緯民（中興大學法律學系，提供書面意見）	
1、本研究就比較法上處理對象廣泛而具有代表性，就本土實證查訪上尚稱妥適，惟就法條體系化、法文具體化、法制史的查考、法政策應有的分析工具則較未著力。 2、在法制面分析上穩重合宜，而對未來主管機關開展監理業務具有要點式提示作用。建議就更高階的「規制模式」，進一步提出具體論證。 3、本研究就電信網路相關法規之整理已得出個資法之定位與定性問題意識，惟建議可再加強探究近三年本土化法理與國際潮流已呈現的「資安化」走向，此議題在部會規制上具有重要意義。	1、已於各章節小結及修正第五章作補正及說明。 2、請參酌修改後第五章之說明 3、資安部分已於第二章我國自律部分說明通傳會目前之作法，資安固為重要之議題，然其前提恐尚須先有建全法制規範業者對個資之蒐集、處理或利用，故本研究計畫先將重點置於業者對各類型個資之蒐集、處理或利用時應遵循之各種法定要件作出報告。

審查意見	回應說明
4、就短期而言，將隱私權政策與認證標章列入探討恐需再查考論證。究其實，法務部所訂定注意參考事項與施行細則第 12 條皆提示「整體性」思考方向，亦即各受規範機關宜有政策或手冊，而後對其進行 PDCA 的持續改善。 5、從我國近年個人資料保護機制的發展情形顯示，如能找出一套小而美的規制模式，則不僅受規範機關可接受，未來的主管機關也可較能掌握重點且省力。本研究已整理出許多堪為指引或方針之資料，甚至及於法制面，如能強化掌握資安面向，就國際上行之有年之代表性規制模式予以探究，則可使本研究議題更為精進。	
五、李科長明忠（通傳會平臺事業管理處）	
(一) 有關國外法制資料部分論述完整，惟建議加以彙總比較分析，並探究是否有適合我國採行之處。	因我國個資法立法係參考歐盟之條文，許多個資之蒐集、處理或利用時應遵循之各種法定要件，多與歐盟個資保護指令相同，故美國、甚至日本之相關法令規定，與我國有所不同，除非修改個資法否則難採為我國所用。本研究報告亦以我國個資法為基礎指出個資法不足處，再研究電信法有關通訊秘密部分之個資保護之規定，分析其不足及可以修法之具體方向，請參看第五章第五節，頁 252 以下。

審查意見	回應說明
(二) 有關研究建議部分，建請研究團隊再深入探討，尤其所提現行電信法規保護個資不足或應調整之處，請評估更進一步具體敘明相關修正內容或修正條文對照表。	已在第五章建議說明，頁 255-266。
(三) 為因應數位匯流，通傳會正積極通盤檢討電信法與廣電三法的修正內容，惟如何更周延保護使用者個資，請研究團隊評估在本研究主軸上，提出短期修正電信法與中長期配合匯流法的修正建議方向。	數位匯流部分因牽涉部分太過廣範，本研究團隊因時間關係無法提出建議。
(四) 研究團隊建議明定限制於審查契約目的下，電信事業得對欠繳費率、濫發電子郵件客戶或使用人，建立名單查詢機制部分，因已超脫原服務提供者蒐集處理使用者資料的限制，恐涉及牴觸個資法與妨礙使用者之通信權益，且以欠費作為拒絕申辦服務之理由，似不符比例原則，爰請研究團隊再酌。	請參看劉秘書部分第 3
(五) 有關研究建議所列主協辦機關宜請通盤考量進行調整，如所提歐盟於 2002 年制頒「歐盟電子通傳中關於個人資料處理與隱私保護指令」之立法政策中，係就網際網路之新興科技服務，如社群網站、雲端計算等，納入電子通傳個人資料保護之體系中。我國有關資訊隱私保護標章之核發係屬經濟部權責，行政院資通安全辦公室	有關監督機制部分已於第五章全面改寫。頁 252-259。

審查意見	回應說明
則已配合行政院組織改造成為常設任務編組，主要任務為國家資通安全政策與措施之研擬及推動、國家資通安全事件之通報、應變及管考、國家資通安全重大計畫之推動與管考、國家資通安全相關法制及規範之協調、聯繫及推動，爰建構優質資安環境為行政院權責。而通傳會組織法第 3 條第 8 款規定掌理「資通安全之技術規範及管制」，所制訂「電信事業資訊通訊安全管理作業要點」，僅係供給電信業者做為其內部稽核資訊安全之用，對於電信事業以外之其他非電信事業資通訊安全管理機制，則宜回歸由各部會依其職掌負責所主管行業之個資監理事宜。此外，通傳會雖為獨立機關，但仍隸屬行政院，有關跨部會協調事宜，宜由上級機關處理。	
(六) 依據憲法第 12 條及釋字第 631 號、第 603 號解釋，秘密通訊自由與隱私權為憲法所保障的基本權，人民有不受國家及他人任意侵擾之權利，國家若需加以限制須有法律依據。有關機關查詢通信紀錄與使用者資料，係由其援引各自主管之法律規定向電信業者提出申請，並依電信法第 7 條第 2 項及其授權辦法(如「電信事業處理有關機關查詢電信通信紀錄實施辦法」、「電信事業處理有關機關(構)	有通保法與電信法有規範主體與保護客體之不同，本研究報告已於第二章第三節說明其間適用關係。頁 33-35。

審查意見	回應說明
查詢電信使用者資料實施辦理」)所訂查詢程序辦理，此規範於「通訊保障及監察法」修正前後均相一致。因此，有關機關依其業務職掌目的須向電信業者調取通信紀錄及使用者資料時，即應由各該機關援引其主管法律規定要求電信業者配合，通保法與電信法對此並無特別與普通法之關係。	
(七) 依電信法第 12 條第 6 項規定，第一類電信事業開放之業務項目、範圍、時程及家數，係由行政院公告。目前已開放經營的第一類電信事業業務項目，包括固定通信業務、行動電話業務、第三代行動電話業務、無線寬頻接取業務、行動寬頻業務及衛星通信業務等，並已有相對應的法規管理。研究報告僅將固定通信業務管理規則、行動通信業務管理規則，以及衛星通信業務管理規則中的第一類電信事業管理規範加以分析，建議研究團隊補充增列或以表格比較其差異。	關於此點已作補充，請參閱第二章第三節(頁 24-31)。第二章第三節中論及通訊保障及監察法屬特別法而應優先適用，乃相對於個人資料保護法而言，而主管機關經電信法授權所制定之各個法規命令，例如：電信事業處理有關機關查詢電信通信紀錄實施辦法、電信事業處理有關機關(構)查詢電信使用者資料實施辦理等，即誠如審查意見所論，乃各機關（構）向電信事業提出查詢申請時之依據，其間並未有特別與普通法之關係。於該段落相應處強化說明，並將引註之法務部函釋要旨之內容於註腳中完整呈現，以為釐清。於第二章第三節第一類電信事業之討論中，新增第三代行動電話業務、無線寬頻接取業務及行動寬頻業務之說明
(八) 我國現行第二類電信事業並無資本額限制，第二頁所提資本額 100 萬元的限制，宜請釐清；另第三頁提及	已作修正，頁 2、11。

審查意見	回應說明
skype，宜修正為 SkypeOut 較為妥適。	
(九) 附錄十五臚列第二類電信事業者名單，宜請更新至最近資料，並請增加各營業項目之家數統計數據。	已作修正，參閱附錄二，頁 300。
(十) Electronic communication 建請翻譯為「電子通傳」、telecommunication 則建議翻譯為「電信」。	已作通篇修正，在此不再臚列頁次。
六、法務部法律事務司（提供書面意見）	
(一)有關第 209 頁所提「規範位階之疑慮」部分，由於電信法第 7 條第 2 項規定授權訂定之「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」 及「電信事業處理有關機關查詢電信通信紀錄實施辦法」，係屬行政程序法第 150 條規定所稱之法規命令，故本報告第 209 頁倒數第 9 行所述「僅依行政規則再揭示其執行辦法…」乙段，應修正為「僅依法規命令…」。	已作修正(同劉教授部分)
(二)有關第 210 頁所提「(二)個人資料保護法之欠缺」之問題： (1)第 1 項「資料共同利用之疑慮」部分，依個人資料保護法(簡稱個資法)第 2 條第 4 款所稱內部傳送，指公務機關或非公務機關本身內部之資料傳送，例如公務機關內部各單位間之資料傳送（不包括上級機關傳送個人資料予下級機關），或法人、團體、自然人之內部資料傳送(個資法施行細則	(1)因條文規定「內部傳送」語意不清，適用上確有疑問，故而有貴部意見之說明，為讓電信事業團體更清楚法律規範，並參考國外之立法，故而有此意見。按法務部之意見，總公司與子公司、事業集團內各公司之間彼此提供個人資料檔案，應屬個人資料之「利用」而適用個資法第 16 條但書規定，然法務部所提第 16 條係規範公務機關，顯然不適用於一般民間業者，故

審查意見	回應說明
第 6 條第 2 項規定及修法理由)。有關總公司與子公司、事業集團內各公司之間共同利用個資檔案行為，係不同蒐集主體，非屬「內部傳送」，除有特別規定，否則總公司與子公司、事業集團內各公司之間彼此提供個人資料檔案，應屬個人資料之「利用」而適用個資法第 16 條但書規定。 (2)第 2 項「關於個資之蒐集、處理或利用之委外欠缺實效性規範」部分，依個資法第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」並未區分受託者須限於本國法人、團體或自然人，亦可委託境外廠商代為蒐集、處理及利用客戶個人資料。惟委託機關應對受託者為適當之監督，包含明確約定委託契約內容，以確保委託處理個人資料之安全管理（本法施行細則第 8 條及立法理由、本部 103 年 6 月 25 日法律決字第 10300570190 號函參照），受託者違反委託契約，委託者仍得主張民事損害賠償，故並無漏洞。 (3)第 3 項「目的外利用之寬泛」部分，依個資法屬普通法性質，個別法律（例如：電信法及其具體明確授權訂定之法規命令、103 年 1 月 29 日修正公布之通訊保障及監察法等）如對個人資	本研究不予採納。 (2)如為境外委託，或現在之雲端處理，該第 4 條之規定將無法發揮作用；且施行細則第 8 條已增加受規範者之義務，是否能在法規命令中作如此處理，大有疑慮。頁 243。 (3)此部分已於第五章第一節中說明 (4)此為參考外國法規之規定，如未查明則將可不通知當事人，顯不合理，亦無法防止損害之擴大，此非資安之問題。

審查意見	回應說明
料之蒐集、處理或利用另有特別規定，該特別規定應優先適用（法務部103年5月22日法律字第10303506200號函參照）。準此，他人或機構向電信事業調取個人資料當事人通訊紀錄之行為規範，已在通訊保障及監察法、電信法第7條第2項規定授權訂定之「電信事業處理有關機關（構）查詢電信使用者資料實施辦法」及「電信事業處理有關機關查詢電信通信紀錄實施辦法」規定，優先個資法第16條規定適用，應無目的外利用之寬泛問題。 (4)第4項「不完備之事故通知規定」部分，依個資法第12條規定所稱「應查明後以適當方式通知當事人」，何時查明，係屬事實認定，應個案判斷，並非法律缺漏，故公務機關違反本條規定而隱匿不為通知者，其上級機關應查明後令其改正，如有失職人員，得依法懲處；非公務機關違反本條規定而隱匿不為通知者，其主管機關得依第47條第2款規定限期改正，屆期仍不改正者，得按次處以行政罰鍰(個資法第12條修法理由參照)。至於是否須通報主管機關，本非個資法第12條規範功能，尚非立法缺失，如中央目的事業主管機關認有需要，可於依個資法第27條第3項規定，訂定「指定	

審查意見	回應說明
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」之辦法時，另行規定(例如: 金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第 6 條第 2 項規定，非公務機關遇有重大個人資料安全事故者，應即通報金融監督管理委員會)。	
七、委託研究機關	
(一)第一章第三節研究方法與步驟之報告內容，請依期末報告完成之情形進行撰寫說明。	已依照建議修改，頁 6。
(二) 第二章內容多就法制層面進行分析說明，建議可先就實務上電信業者所提供服務涉及個資的種類進行介紹，接續再就我國現行個人資料保護相關法規與實務作法上的不足或缺失進行分析。	考量我國個人資料法制所規範之體例並未如歐盟、德國、英國與日本之模式，先就個人資料之種類加以類型化，為凸顯此一差異，以作為後述第五章提出建議之基礎，故於第二章第二、三節仍維持以法規為分類基準之架構進行介紹說明，並於第五節小結中以表格方式呈現個人資料類型之區分，以為補強。
(三) 有關外國法制資料部分，宜補充說明選擇個案國家之理由，並就各國立法模式進行探究，再就不同模式優劣利弊進行分析，以瞭解適合我國的立法模式，俾進而研提後續研究建議。	已補充說明，頁 4-5。
(四) 有關第三章各國個人資料保護法制部分，建議將各國個人資料保護機制的一般性與特別性規定要件，以一	已盡力作出一致表格，頁 77-79、106-107、129-130、146-147、154 和 184，因各國立法方式不同，尤其美國

審查意見	回應說明
致化的表格進行整理說明，俾比較瞭解。	原無個資法總則性之規定，故無法作出表格。其他國家已作各國表格，並於各節明其特色，第五章第四節亦有分析。頁 249-252。
(五) 第四章第七節就我國個人資料保護監管機制進行介紹，惟報告內容多為現行法令規範的說明，建議研究團隊再就通傳會現行組織職掌進行分析，並就制度不足之處予以探究。	已在小結補充說明，頁 237。第五章第五節建議亦有分析。
(六) 第四章就相關國家個人資料保護監管機制進行探討，建議於該章末針對各國的監管機制、特色與優缺點進行簡要比較，並以表格加以統整呈現。	已盡力作出一致表格，請參考頁 201、220、224。
(七) 第五章第一節前半段內容仍著重於現行法令實務規範上的說明與分析，是否移至第二章第四節後通更為妥適，提供研究團隊參考。	為與該章後接續說明之建議能有連結，故仍保留原編寫法。 原第五章第一節前半段內容將移至第二章第五節。 因第四章為對電信事業之監督機制，而第五章建議部分。不單僅對電信事業之監督而是對個資法施行之監督，故本研究團隊仍認為不宜將所指部分內容移往他章，請諒察。
(八) 第五章第二節提及我國電信事業已多取得如 ISO /IEC27001 等國際個資保護與管理制度安全認證標章，惟其後亦提及經濟部商業司委託資策會所推動的「台灣個人資料保護與管理制度(簡稱 TPIPAS)」較為周全，爰未來如 TPIPAS 制度運用於我國電信業	已補充說明，頁 253。

審查意見	回應說明
及電信加值網路業，是否可行或有其不足之處，建議研究團隊加以評估說明。	
(九) 建議研究團隊可於報告中適時補充實務所發生之案例，如近日電信公司提供客戶識別網內外電話之判決內容，俾瞭解實務運作上的問題與爭議。	依據審查意見於本文中新增討論M+Messenger（台北地院 103 年度北小字第 1360 號判決、台北地院 103 年度小上字第 155 號判決）、B&Q 特力屋（士林地院 103 年度湖小字第 537 號判決）、全民健保資料庫（北高行 102 年度訴字第 36 號判決，最高行 103 年度判字第 600 號判決）以及行使被遺忘權請求移除網路搜尋結果(台北地法院 103 年訴字 2976 號判決)等司法判決。
(十) 研究團隊考量新設獨立機關之不易，建議於通傳會下設一局或署之三級機關，監督與聯繫協調各機關有關個資法之施行與安全保護事宜。惟新設三級機關(構)除應參照中央行政機關組織基準法之相關規定外，有關個資法之適用範圍包括各公務與非公務機關，爰此建議是否具論述基礎或可行性，建議研究團隊再予探究。	已於第五章之部分作全面改寫。
(十一)報告格式部分： (1)研究報告各表格請依序「表 1-1、表 1-2…」進行編號，各表格下方並請註明資料來源。 (2)報告中部分文字錯漏，如第 27 頁「行政院研究考核『協會』(現為國家	格式問題已依照建議修改，請參見目次與封面等處。表格為研究團隊自行整理，已註明資料來源。另已將「行政院研究考核協會(現為國家發展協會」更正為「行政院研究考核委員會（現為國家發展委員會）」。

審查意見	回應說明
發展『協會』」、第 206 頁第 3 及 4 段「通訊使者資料」、第 221 頁倒數第 11 行「手機關監管」、倒數第 10 行「獨立監督關」，宜請通篇檢視修正之。 (3)報告封面與內頁編號請修正為「NDC-DSD-103-014」，另表目次請由單數起頁。 (4) 研究報告請將摘要納入目次前，另期中報告審查與期末審查意見回應對照表亦請納為附錄。 (5)第四及五章請由單數頁起頁，第四章第二節則不另起頁；另參考文獻請移至附錄之前。	