研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制
期末報告

財 團 法 人 資 訊 工 業 策 進 會

日期：2019年2月

目錄

壹、 研析數位匯流法規及隱私保護法規之規範 1
一、 前言 1
二、 美國 4
(一) 概述 4
(二) 通訊傳播事業取得各種資料類別之行為規範 6
1. 1934 年有線電視隱私法（Cable TV Privacy Act, CTVPA） ... 6
2. 1986 年電子通訊隱私法（ Electronic Communications Privacy Act, ECPA） 6
3. 1996 年電信法（Telecommunication Act） 8
4. 1998 年兒童線上隱私保護法（Children's Online Privacy Act, COPPA） 9
(三) 通訊傳播事業個人資料保存機制 10
1. 適當安全維護措施 10
2. 保存期限之規定 12
3. 紀錄及證據保存之規定 12
(四) 通訊傳播事業資料釋出之授權規範 13
1. 釋出予第三人 13
2. 揭露（disclosure）個資之規定 14
3. 去識別化規定 15
(五) 隱私蒐集評估機制 16
(六) 小結 17
三、 日本 18
(一) 概述 18
(二) 通訊傳播事業取得各種資料類別之行為規範 19
1. 電信事業者對個人資料保護指引（下稱電信 GL） 21
2. 廣播領域對個人資料保護指引（下稱廣播 GL） 28
(三) 通訊傳播事業個人資料保存機制 29
1. 適當安全管理措施 29
2. 保存期間之規定 30

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(四) 通訊傳播事業資料釋出之授權規範 32
1. 提供個資予第三人 32
2. 提供給外國之第三人 35
3. 去識別化規定 36
(五) 隱私蒐集評估機制 38
(六) 小結 38
四、 英國 39
(一) 概述 39
(二) 通訊傳播事業取得各種資料類別之行為規範 42
1. 一般資料 42
2. 特種個資 44
3. 兒童資料之蒐集 46
(三) 通訊傳播事業個人資料保存機制 46
(四) 通訊傳播事業資料釋出之授權規範 50
1. 目的外利用規定 50
2. 授權他人代為處理個資之規定 51
3. 共同決定資料處理之規定 51
4. 去識別化規定 53
5. 通知規定 55
6. 資料可攜權 55
(五) 隱私蒐集評估機制 56
(六) 小結 57
五、 結論 58
(一) 法制背景綜合比較 59
(二) 取得各種資料類別之行為規範 61
1. 一般個人資料 61
2. 特種個資 67
3. 針對兒少之個資保護規範比較 71
(三) 個人資料保存機制 73
1. 適當安全維護措施 73
2. 保存期限之規定 76

本報告之智慧財產權歸屬於財團法人資訊工業策進會

3. 紀錄及證據保存之規定 78
(四) 資料釋出之授權規範 79
1. 釋出予第三人 79
2. 去識別化（匿名化）規定比較 81
3. 資料可攜權 83
(五) 隱私蒐集評估機制 87
(六) 資料側寫議題 88
(七) 資料加值應用與隱私保護之調和 90
1. 國際間資料保護標準並未因技術進步而退讓 90
2. 去識別化標準難定義 90
3. 利用技術協助賦權消費者，建立資料加值之信任基礎 91
貳、 舉辦業界訪談及研討會 94
一、 進行訪談 94
(一) 訪談情形 94
(二) 訪談內容歸納 95
1. 現有規範調整建議 95
2. 個資保護專責機關設置議題 97
二、 舉辦研討會 98
(一) 議程 99
(二) 與會人數 101
(三) 活動摘要 101
參、 研析及規劃參與國外通傳事業資料利用機制 133
一、 觀測與實地考察他國資料加值創新應用相關法制規範資訊 133
(一) 參與英國 IAPP 2018 歐洲資料保護密集研討會 133
1. 簡述 133
2. 重要內容 134
(二) 參與美國隱私與安全論壇 138
1. 簡述 138
2. 重要內容 139
(三) 參與日本 Gartner 研討會與 IT 應用展示 141

本報告之智慧財產權歸屬於財團法人資訊工業策進會

1. 簡述 141
2. 重要內容 141
二、 研析歐盟隱私及電子通訊規則（ePrivacy Regulation）草案 150
(一) 草案之背景 150
(二) 草案之最新發展情形 152
1. 歐盟議會審理情形 152
2. 歐盟理事會審理情形 155
3. 草案後續發展 158
(三) ePrivacy Regulation 草案的主要內容及重要爭點 159
(四) ePrivacy Regulation 與 GDPR 之競合 172
(五) ePrivacy Regulation 與 GDPR 規範差異之重點比較 173
1. 處理要件的限縮 174
2. 儲存時間的限制 176
3. 對隱私設定方式的明文化 176
肆、 成立通訊傳播產業資料創新運用法制諮詢服務小組 178
伍、 研析成立個資保護專責機構之必要 181
一、 國際間個資主管機構之趨勢觀測 181
(一) 分散主管機關模式：美國 181
1. 美國的分散主管機關模式 181
2. 通訊傳播領域主管機關 181
(二) 專責主管機關模式：以英國為例 182
1. 另一種選擇：專責主管機關模式 182
2. 專責主管機關模式概說：以英國資訊長辦公室為例 183
(三) 從分散到整合：以日本為例 185
1. 日本經驗：從分散到整合 186
2. 日本個人情報保護委員會簡介 187
二、 淺析我國之個資主管機關制度安排 188
(一) 當前我國個資主管機關設計 188
(二) 我國適足性談判對象：歐盟 GDPR 之規範 191
(三) 我國對獨立機關的規範建置 193
三、 代結論：我國個資主管機關可能之模式 197

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(一) 各國個資主管機關設置模式比較 197
(二) 我國個資主管機關可能之模式 199
1. 現有個人資料保護法主政機關轉型為獨立機關 199
2. 另立獨立機關 200
3. 其他可行方法 204
4. 小結 207
陸、 結論與建議 208
一、 數位匯流法規及隱私保護法規之規範 208
(一) 取得各種資料類別之行為規範 208
(二) 個人資料保存機制 209
(三) 資料釋出之授權規範 210
(四) 隱私蒐集評估機制 211
(五) 資料側寫議題 211
(六) 資料加值應用與隱私保護之調和 213
二、 歐盟隱私及電子通訊規則（ePrivacy Regulation）草案之發展 214
三、 研析成立個資保護專責機構之必要 216
附件一 訪談紀錄 217
附件二 英國出國報告 238
附件三 美國出國報告 268
附件四 日本出國報告 303
附件五 歐盟執委會版 ePrivacy Regulation 草案中譯版 322
附件六 歐盟執委會版 ePrivacy Regulation 草案英文原文 349
附件七 有線電視業者蒐集用戶收視紀錄及行為等之商務模式及服務樣態隱私議題分析 375
附件八 臉部辨識法制議題簡析 378

本報告之智慧財產權歸屬於財團法人資訊工業策進會

表目錄

表 1 各國一般個資規範比較表 63
表 2 各國特種個資規範比較表 69
表 3 資料可攜權與號碼可攜服務比較表 84
表 4 訪談時間與對象 95
表 5 研討會議程 99
表 6 ePrivacy Regulation 版本比較 160
表 7 諮詢服務紀錄 178
表 8 各國個資主管機關及法律主政機關比較 198

本報告之智慧財產權歸屬於財團法人資訊工業策進會

壹、研析數位匯流法規及隱私保護法規之規範

一、前言

近年來，提倡「開放資料」之風氣在國際上日益蓬勃，已成為許多國家發展之重點戰略，希望透過巨量資料等新興之技術，將資料附加之價值最大化，造就以資料為基礎之資料經濟。根據全球知名的管理諮詢公司——艾森哲（Accenture）估計，預計全球的資料經濟產值將在 2020 年時成長至 24.6 兆美元，約占全球 GDP 的 25%，並且持續看漲[1]。而我國也自 2012 年開始推動資料開放，並在 2015 年起，連續兩年在世界開放資料指標單位「開放知識基金會」（Open Knowledge Foundation）所編纂的「開放資料指標」（Open Data Index）中，資料開放程度排名世界第一，政府開放資料已有一定程度之成果。此一開放資料之風潮，不僅只於政府之資料，「科技、媒體及通訊」（Technology, Media, Telecom，簡稱 TMT）產業作為數位經濟發展的基礎，其資料之開放，也在數位經濟發展中扮演重要之角色。通訊傳播產業一般來說保有大量資料，若能妥善加值，其蘊藏之價值將會對相關科技之發展、商業模式之突破有相當大的助益。然而，由於前述通訊傳播產業中所保有的資料，有許多因為能直接或間接識別個人，而屬於「個人資料」的範疇。在這個範圍內，若要進一步加值利用通訊傳播產業所保有之個人資料，勢必面臨個人資料隱私保護與資料運用之衝突。

而我國業者對此也有類似的看法。在本研究所舉辦的研討會中，電信產業業者就提到「電信產業擁有大量的數據，尤其三大電信產業都各

[1] Accenture strategy, DIGITAL DISRUPTION: THE GROWTH MULTIPLIER, https://www.accenture.com/us-en/insight-digital-disruption-growth-multiplier (last visited Feb. 13, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

擁有 700 萬用戶的資料，大家其實都很清楚這個資料是有價的，可是不把它活化，就像土地一樣，它就沒有價值，一旦活化它才有價值的存在。」該業者表示：在萬物聯網的時代，「人們對物跟物、人跟物、人對人的相連，需要一個很強的信賴感」，因此對於電信業而言，資料加值最大的挑戰在於建構消費者對整個體系的信賴感。尤其是：「如何取得繁榮跟隱私（個資）之間的平衡點，因為產業在發展的過程中間，以後在 5G 的時代談到無人車、無人載具、遠距醫療，信賴就變成非常重要的一個狀況，在這個狀況中間，如何確保科技發展所帶來的繁榮跟個人資料的保護中間作一個平衡點，也就是我們所有業者發展的過程中間所看到的困境，也可以說是如何取捨的問題。」

而實際從事資料交易市集業務企業也強調：資料自主控制是發展資料經濟的關鍵。他認為應該「先讓使用者能夠回歸自主」，資料經濟才能妥善的發展。

另一家電信企業則認為，只要涉及到個人服務的資料加值應用，就很難繞開個資的爭議。當前對業者來說最需要得到的幫助是「怎麼在關鍵的方面設定好商業活動範圍，讓業者有遵循的方向、有一個指引，不會意外踩到紅線？」

而在本研究所執行的訪談中，臺灣本土 OTT 平台業者數據專案經理也表達了類似的意見。對於本土的 OTT 平台業者而言，目前對於資料加值應用最迫切的需要來自資料的交換；而希望能有方法「確認這樣的資料交換是合理、合規的」，因此，她認為當前最主要的問題是：「也就是資料交換到什麼程度才符合法律規定，能同時保護使用者也保護我們業者。」

本報告之智慧財產權歸屬於財團法人資訊工業策進會

由上述的法理整理以及針對業者的意見整理可以發現：當前業者思考資料加值應用的可能性時，最主要的顧慮仍然是圍繞在以個資法為首的法律爭議問題。具體來說，主要是如何確保其資料應用的方式符合個資法的相關規範，以及資料之管理是否能贏取消費者之信任、取得資料價值與個資保護間的平衡點。因此，我們可以簡單的歸納認為，在當前臺灣資料加值的發展階段，如何促進資料加值及如何確保資料之隱私保護，實為一體兩面的問題。若能有效釐清資料保護的爭議，並探求合理運用的空間，則亦將有助於資料加值之發展。

基於這樣的理解，本研究依據補助計畫徵求文件的指導，將從前端的個人資料蒐集、取得之規定，到中間階段的保存、利用，乃至後端的釋出、風險管理等議題，進行廣泛之資料蒐集與分析。

本研究採取比較分析法，分析美國、日本及英國等國對於通訊傳播資料之管理，在蒐集、保存、授權以及隱私蒐集評估機制之管理規範。在比較方法上，本研究採取行政法學研究上的「三層次分析方法」（將行政法學問題分析分為權利與救濟、制度與程序、政策與策略三個層次進行分析）[2]加以分析，其中，將聚焦在制度與程序、政策與策略兩個層次，主要觀察指標為：

(1) 在制度與程序上，各國對於通訊傳播資料是否有與其他個資有不同之規範？或者是否針對特定類型的通訊傳播資料有不同強度之規範？

(2) 在政策與策略上，觀察各國對於通訊傳播資料之管理，係以何種

[2] 葉俊榮，《行政法案例分析與研究方法》，頁 41-56（1999）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

形式加以規範？是採取具有法律拘束力的法律(或其授權之法規命令)；或是採取不具法律拘束力的其他形式規範（姑且借用國際法學的說法——「柔性規範」(soft law)）？

最後，本研究將針對前述議題之重要法律爭點，從隱私保護的角度嘗試酌擬議題之建議，並從資料加值之角度嘗試回應業界對於資料保護與資料加值權衡的需要。

二、美國

(一)概述

美國就個人資料保護方面，未有正式的單一特定主管機關，其通訊傳播事業的個資、處理、利用或傳輸之監管，主要涉及下述兩個聯邦行政機關——聯邦通訊傳播委員會、聯邦貿易委員會。通訊傳播事業主管機關為聯邦通訊傳播委員會（Federal Communication Commission, FCC[3]），負責管理及執行電信事業之個資蒐集、處理、利用之相關法律及行政命令。另，聯邦貿易委員會（Federal Trade Commission, FTC）則監督消費者隱私議題，法源係聯邦貿易委員會法（Federal Trade Commission Act）第 5 條（Section 5）之規定，據以禁止商業中或影響商業的不公平競爭或欺罔行為，而對業者違反隱私保護的行為進行管制。但在電信事業個資保護的監理，其權限上聯邦貿易委員會仍應尊重聯邦通訊傳播委員會之決定。

美國的個人資料保護目前並無統一適用的專法，而是採取個別立法的方式，因應時代變化和不同領域去制定相關個資保護規則。換言之，

[3] 47 US Code § 151- Federal Communications Commission created.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

美國在個資保護的特色，屬於特定部門（sector-based）的保護模式，除聯邦法外，尚有各州的州法規範個人資料保護。諸如，美國於 1973 年開始確立行動電話和電子郵件的技術、1890 年網際網路商用化開始，出現針對這些新技術的個人資料保護政策。在網際網路開始普及的 1990 年代導入關於處理電子資料的法律。而在恐怖活動開始頻繁出現的 2000 年後，為維護國家安全的個人識別資訊、以及有識別個人可能性資訊保護之法律也陸續被制定。然而，近期美國在聯邦法層級，有針對個人資料保護設立專法之草案討論，但因美國立法模式係採屆期不連續，草案未能在此屆議員任期內通過，後續仍待觀察。而州法規範的部份，美國加州在 2018 年 6 月通過了嚴格的個人資料隱私法規--加州消費者隱私保護法（The California Consumer Privacy Act[4]），將於 2020 年 1 月 1 日施行，主要著重於對網路消費者更完整的保護，該法案旨在讓消費者可以控制其個人資料並有權選擇企業如何蒐集和使用他們的個人資料。

美國針對通訊傳播事業領域之個人資料保護的相關法律規範有：隱私保護法(Privacy Protection Act)、有線通信政策法(Cable Communications Policy Act)、通訊傳播法（Communications Act of 1934）、視訊隱私保護法(Video Privacy Protection Act)、電話消費者保護法（Telephone Consumer Protection Act）、電信法(Telecommunications Act)、電子通訊隱私法（ Electronic Communications Privacy Act）等。

以下將以有線電視隱私法（Cable TV Privacy Act）、1986 年電子通訊隱私法（ Electronic Communications Privacy Act）、1996 年通過之電信法（Telecommunication Act）以及 1998 年兒童線上隱私保護法

[4] California Consumer Privacy Act, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375（last visited Dec. 25, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

（Children's Online Privacy Act）等，對於個人資料之蒐集、使用或分享之規範，做進一步說明。

(二)通訊傳播事業取得各種資料類別之行為規範

美國通訊傳播隱私之資料蒐集相關規範，整理如下：

1. 1934 年有線電視隱私法（Cable TV Privacy Act, CTVPA）

美國於 1984 年修訂了此通訊傳播法（Communications Act of 1934），增訂「有線通訊傳播（Cable Communications）專章；其中參考 1980 年的 OECD 的隱私準則，制定了「有線電視隱私法」（Cable TV Privacy Act，CTVPA），以保障有線電視訂閱戶的隱私權利。其取得個資的規範內容為，有線電視營運商在訂立提供服務相關協議時，須以書面聲明的形式向訂閱戶發出通知，並明顯告知訂戶蒐集的個人資料的性質、此類個資將被使用的用途、可能被揭露的性質和頻率及目的，而通知頻率至少每年一次[5]。

又，未經用戶當事人的事先書面同意或電子許可下，禁止系統業者利用有線電視系統「蒐集」，或向第三人「揭露」有關客戶的「可識別個人資料」（personally identifiable information）[6]。其中，法條中特別闡明，「可識別個人資料」一詞，不包含任何無法識別特定個人的匯總數據的紀錄（aggregate data）[7]。

2. 1986 年電子通訊隱私法（ Electronic Communications Privacy Act,

[5] 47 U.S. Code § 551 (a),(1),(B), https://www.law.cornell.edu/uscode/text/47/551（last visited Aug. 5, 2018).
[6] 47 U.S. Code § 551 (b),(c).
[7] 47 U.S. Code § 551 (a),(2),(A),

本報告之智慧財產權歸屬於財團法人資訊工業策進會

ECPA）

「電子通訊」（Electronic communications）係指透過州際或國外商業的電線、無線電、電磁、光電或光電系統傳輸全部或部分的任何性質之標誌、信號、圖像、聲音、數據資料或情報；但不包含以下方式傳輸或記錄之資訊：有線或口頭交流、透過呼叫設備進行通訊、來自追蹤設備的通訊、將金融機構儲存的訊息傳送到其電子儲存和資金轉移的通訊系統中[8]。

本法旨在保護儲存和傳輸中的通訊資料，禁止第三方未經授權監聽、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[9]。

惟，在下列兩種情形，得例外被允許：（1）通話任一方已對揭露其通話內容加以同意的情形；（2）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，屬於其職務範圍內所為的行為者[10]。

須特別說明的是，本法僅針對「儲存和傳輸中的通訊資料」，並不適用於電信「交易」相關資訊，因而電信服務提供者在限制蒐集、儲存或揭露該等電子通訊資料之行為，目前未有法律明文[11]。

[8] 18 U.S. Code § 2510 (12), https://www.law.cornell.edu/uscode/text/18/2510（last visited Aug. 6, 2018).
[9] 內政部警政署刑事警察局委託研究報告，網路平台業者紀錄保存規範之研究，101 年 11 月，頁 37-39，https://www.npa.gov.tw/NPAGip/wSite/ct?xItem=65364&ctNode=12581&mp=1（最後瀏覽日：2018/08/06）。
[10]國家發展委員會委託研究報告，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，104 年 04 月，頁 163，https://www.ndc.gov.tw/News_Content.aspx?n=E4F9C91CF6EA4EC4&sms=4506D295372B40FB&s=E78AD37054E8DB3E（最後瀏覽日：2018/08/05）。
[11] 同前註，頁 164。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

3. 1996 年電信法（Telecommunication Act）

主要規範了保護「用戶專屬資訊」（Customer Proprietary Network Information，CPNI）隱私的條款，條文內容定義了何謂「用戶專屬資訊[12]」，以及原則禁止電信事業以電信法第 222 條之外的方式，使用、揭露或允許取得「用戶專屬資訊」；除非例外依法律規定或取得用戶同意，始可為之。詳分述如下：

電信業者對於「用戶專屬資訊」的使用、揭露或取得的限制，規定於電信法第 222(c)(1)條：「電信事業因提供電信服務而收受或取得用戶專屬資訊者，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[13]。」換言之，該類資訊僅在電信事業為提供因而衍生之電信服務或所必要之服務的範圍內，電信事業才可使用、揭露或允許接觸可辨識個人之「用戶專屬資訊，業者不可基於本身行銷等目的使用該類資料。惟，關於「用戶專屬資訊」之使用、揭露或允許接觸，第 222(c)(1)條中未明定，應以何種方式取得用戶同意。

然而，電信事業對於「用戶專屬資訊」仍有下列 4 種得例外使用、揭露或取得情形，規範於電信法第 222(d)條：「（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閱

[12] 參見美國電信法第 222(h)(1)條：「用戶專屬資訊」係指，「（A）涉及電信事業用戶使用電信服務之數量、技術規格、型態、目的地與使用量總額之相關資料，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；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。」

[13] 47 U.S Code § 222, https://www.law.cornell.edu/uscode/text/47/222（last visited Aug. 5, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

該等服務;(3)若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）若係為下述情形而將商業行動電話服務或 IP 驅動語音服務之用戶之電話位置資訊（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，以供協助提供緊急服務之目的，而提供予資訊或資料庫管理服務之提供者。」

4. 1998 年兒童線上隱私保護法（Children's Online Privacy Act, COPPA）

主要係針對透過網路線上蒐集未滿 13 歲兒童個人資料的行為有特殊之保護規定，網站營運商須遵循的隱私政策[14]，包含：個人資料蒐集的通知、何時及如何向家長直接告知或取得父母或監護人可資驗證的同意（verifiable consent），以及明確向家長提供所蒐集之資料、將如何使用該資料等應盡之相關責任，並要求網站營運者須保護兒童的隱私安全，包含限制向 13 歲以下兒童銷售。同時，若外國網站直接或試圖向美國兒童蒐集其個資，本法亦適用於該外國營運的網站[15]。

其中，兒童線上隱私保護法亦有明確闡明該法中其「個人資料」之

[14] 15 U.S Code § 6502 (1998)
[15] FTC, Implementing the Children's Online Privacy Protection Act: A Federal Trade Commission Report to Congress, https://www.ftc.gov/reports/implementing-childrens-online-privacy-protection-act-federal-trade-commission-report （last visited Aug. 4, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

定義[16]，係指線上蒐集的個人可識別資訊，包含姓名和姓氏、住所或其他實際地址（包含街道、城市或城鎮的名稱）、電子郵件地址、電話號碼、社會安全號碼（ Social Security number）、受聯邦貿易委員會所允許以其他識別碼對特定個人進行物理或線上的聯繫、該網站自線上向兒童蒐集，並與定義中所描述的識別碼相結合的兒童或其父母的相關資訊等資料。又，聯邦貿易委員會尚針對本法制定了兒童線上隱私保護規則（COPPA Rule）[17]。

(三)通訊傳播事業個人資料保存機制

1. 適當安全維護措施

(1) 前述曾提及之「有線電視隱私法（Cable TV Privacy Act，CTVPA）」，同時規範系統業者必須向用戶提供必要措施的保護可識別個人資料免於他人的非法存取、並且給予訂戶合理機會以更正相關資料，且當原蒐集目的消失後銷毀相關資料[18]。

(2) 前述 1996 年電信法的部分，在聯邦通訊委員會所發布之「用戶專屬資訊」規則（47 CFR § 64）當中，提及：

A. 電信事業應實施一系統，在使用「用戶專屬資訊」前，透過該系統用以確認已先取得用戶的同意[19]。

[16] 15 U.S Code § 6501 (1998)
[17] FTC, Children's Online Privacy Protection Rule ("COPPA"), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule（last visited Aug. 4, 2018).
[18] 47 U.S Code §551(d),(e).
[19] 47 CFR §64.2009(a), https://www.ecfr.gov/cgi-bin/text-idx?SID=b85fc7ff03031ee50f5a4a7e657eff9f&pitd=20180719&node=se

本報告之智慧財產權歸屬於財團法人資訊工業策進會

B. 電信事業應培訓其員工判斷是否取得使用「用戶專屬資訊」之授權，並建立明確的訓練處分流程[20]。

C. 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「用戶專屬資訊」用於銷售與行銷活動之檔案紀錄。同時，電信事業亦須保存將「用戶專屬資訊」揭露、提供予第三人或第三人被允許得接觸「用戶專屬資訊」之所有情形的相關紀錄。且該紀錄應包括每次活動的敘述、被使用於活動中之特定「用戶專屬資訊」、活動中所銷售之產品與服務；該紀錄應至少保存一年[21]。

D. 電信事業須建立監督審查程序，以確保行銷員工對其用戶從事外部行銷時，合乎相關安全維護規範，並保留合規紀錄至少一年[22]。

E. 電信事業須採取合理措施，以發現和防止未經授權而意圖取得「用戶專屬資訊」之行為。當用戶方主動向電信營運商之電話聯繫、網路帳戶接觸或造訪店內，而在揭露「用戶專屬資訊」之前，電信事業應適當地查核、驗證用戶的身分[23]。

(3) 1998 年兒童線上隱私保護法在其規定中，要求網站或線上服務的營運商須建立合理的維護措施，以保護所蒐集兒童個人資料之

47.3.64_12009&rgn=div8（last visited Aug. 4, 2018).

[20] 47 CFR § 64.2009(b).

[21] 47 CFR § 64.2009(c).

[22] 47 CFR § 64.2009(d).

[23] 47 CFR § 64.2010(a), https://www.ecfr.gov/cgi-bin/text-idx?SID=b85fc7ff03031ee50f5a4a7e657eff9f&pitd=20180719&node=se47.3.64_12010&rgn=div8（last visited Aug. 4, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

機密性、完整性及可用性[24]。

2. 保存期限之規定

前述 1996 年電信法的部分，按聯邦通訊委員會所發布之「用戶專屬資訊規則」（47 CFR § 64），電信事業應保存將「用戶專屬資訊」揭露、提供予第三人或第三人被允許得接觸用戶專屬資訊之所有情形之檔案至少一年[25]。

3. 紀錄及證據保存之規定

前述 1996 年電信法的部分，按聯邦通訊委員會所發布之「用戶專屬資訊規則」（47 CFR § 64），電信事業應以電子或其他方式保存其發現任何違反「用戶專屬資訊」之情事，及曾向美國特勤局（USSS）與聯邦調查局（FBI）、用戶發出通知之相關檔案紀錄，且紀錄中須包含發現和通知的日期等，並保存該檔案至少兩年[26]。

而在 FTC 所發布之兒童線上隱私保護規則（COPPA Rule）中提及，網站或線上服務的營運商，在合理必要的時間內，可保留線上所蒐集的個人資料。但後續營運商須採取適當合理的措施刪除此類資料，以防止未經授權近用或使用與刪除相關的資料[27]。

---

[24] 15 U.S Code § 6502 (1998), https://www.law.cornell.edu/uscode/text/15/6502（last visited Aug. 4, 2018).
[25] 47 CFR § 64.2009(c).
[26] 47 CFR § 64.2011(d), https://www.ecfr.gov/cgi-bin/text-idx?SID=b85fc7ff03031ee50f5a4a7e657eff9f&pitd=20180719&node=se47.3.64_12011&rgn=div8, （last visited Aug. 5, 2018)
[27] 16 CFR §312 (2013) —CHILDREN'S ONLINE PRIVACY PROTECTION RULE, Data retention and deletion requirements, https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_11（last visited Aug. 4, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(四)通訊傳播事業資料釋出之授權規範

1. 釋出予第三人

1996 年電信法的部分，提供個資給第三人之限制而言，按聯邦通訊委員會 2007 年所發布之「用戶專屬資訊命令」（CPNI Order[28]），並修改了「用戶專屬資訊規則」（47 CFR § 64），針對與非關係企業之第三人分享「用戶專屬資訊」部分，若電信事業欲將「用戶專屬資訊」揭露給合資企業 (Joint Venture[29]) 或獨立的契約締約相對人 (independent contractor)，或允許其得接觸使用「用戶專屬資訊」時，電信事業必須事先取得用戶「選擇加入」（opt-in）的同意[30]；即便所行銷者為電信相關服務，亦同。目的在限制未經授權就揭露用戶專屬資訊的數量，並保護用戶對其隱私資訊的控制權[31]。

另，有特別針對與第三人共同利用「用戶專屬資訊」之規範[32]，當

[28] Federal Communications Commission(FCC),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, , at 22-24. available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf（last visited Aug. 5, 2018).

[29] 「合資企業(Joint Venture)」係指由不同投資者為謀共同利益，從而分擔共同風險所共同建立之企業。

[30]個資的保護方式，實務上有選擇加入（opt-in）與選擇退出（opt-out）兩種方式。選擇加入，也就是預設退出的模式，在個資保護上較嚴密，一開始即假設當事人原則上不同意提供個資，須有積極選擇加入的意思表示（如勾選同意），他人才可對其進行個資的蒐集、處理及利用。反之，選擇退出，也就是預設加入的模式，對個資保護較為寬鬆，因其預設當事人最初即同意提供個資，後續需其有積極選擇退出的意思表示（如勾選不同意），才排除他人對其個資的蒐集、處理及利用。

[31] 47 C.F.R. § 64.2007,
https://www.ecfr.gov/cgi-bin/text-idx?SID=b85fc7ff03031ee50f5a4a7e657eff9f&pitd=20180719&node=se47.3.64_12007&rgn=div8（last visited Aug. 5, 2018). 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,, at 24. available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf（last visited.Nov. 5, 2018).

[32] 47 C.F.R. § 64.2007

本報告之智慧財產權歸屬於財團法人資訊工業策進會

該電信事業所分享的代理商或關係企業[33]係通訊相關業者(carrier's agents or affiliates)，其同意模式係採「選擇退出」（opt-out）之方式，意即不須事前取得用戶的明示同意[34]。

此外，在 1998 年兒童線上隱私保護法（COPPA）規定中，要求該網站營運商或線上服務在進一步之資料蒐集、使用或傳遞（dissemination）時，需經過授權始可進行[35]。

2. 揭露（disclosure）個資之規定

參見 1988 年視訊隱私保護法（Video Privacy Protection Act，VPPA），主要適用於預先錄製的錄影帶、收視紀錄或類似視訊資料的租借、買賣或傳遞上之隱私[36]。旨在防止視訊內容服務提供者（例如錄影帶出租店）任意向他人揭露（disclosure）消費者的個人資料，只有於告知後取得消費者的書面同意（包括透過網路電子的方式）後，才可以揭露個人資料[37]。

又，本法規定視訊內容服務提供者對消費者租賃錄影帶及銷售的紀

[33] 關係企業(affiliates)之定義係指被直接或間接持有或控制者；或與另一公司共同或控制其所有權者。又，「持有」(own)一詞，指擁有超過 10%的股權(或其等價物)。詳細規範可參見 47 C.F.R. § 64.2003 規定提及：「關係企業一詞，與 1934 年通訊傳播法(Communications Act)第 3(1)條定義相同，其法條經修正後為 47 USC. 153（2）。」 https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=8a4d5de42f2afafd21bb9fbb6f6b289b&pitd=20180719&n=sp47.3.64.u&r=SUBPART&ty=HTML#se47.3.64_12003 。而 47 USC. 153（2）原文：The term "affiliate" means a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. For purposes of this paragraph, the term "own" means to own an equity interest (or the equivalent thereof) of more than 10 percent., https://www.law.cornell.edu/uscode/text/47/153（最後瀏覽日：2018/11/13）。

[34]前揭註 10，頁 183-185。Federal Communications Commission(FCC). 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,, at 22-24. available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf（last visited.Nov. 5, 2018).

[35] 15 U.S Code § 6502 (1998)

[36] 18 U.S Code§2710, https://www.law.cornell.edu/uscode/text/18/2710（last visited Aug. 5, 2018).

[37] 18 U.S Code §2710 (b)(2)(B).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

錄等資料之利用，若要向他人揭露消費者的姓名和地址之前提在於：視訊內容服務提供者應曾經以清楚、明瞭的方式給予消費者拒絕的機會，以及在不會被識別任何錄影帶或視訊資料的名稱、描述或主題（subject matter）的狀況下，才可對他人揭露消費者姓名及地址。但若該等資料僅是單純用於直接對消費者進行行銷商品或服務的目的，則揭露視訊資料的主題（subject matter）就例外不受限制[38]。

此外，1988 年所立的視訊隱私保護法，於 2012 年提出部分修正，2013 年 1 月由歐巴馬總統簽署通過此法律修正案（HR 6671[39]），修訂的內容包含：(1) 視訊內容服務提供者在消費者書面同意後，可向他人揭露消費者的個人識別資料(personally identifiable information)，而此類「同意」，允許透過電子的方式提供；亦允許透過消費者預先同意的方式為之，但時間不得超過兩年或直至消費者撤回同意，以較早者為準。(2) 要求視訊內容服務提供者為消費者提供個案可請求撤回此類同意，或有權選擇停止被繼續揭露的機會[40]。

3. 去識別化規定

美國對於去識別化資料，在法律中尚未有明確的標準，但參見 FTC 於 2012 年 3 月 26 日所公布的保護消費者隱私報告（Protecting Consumer Privacy in an Era of Rapid Change）[41]中，提及個人資料去識別化(de-identify)可資遵循的規定，係以「有無可合理連結(reasonable linkable)」

[38] 18 U.S Code §2710 (b)(2)(D).
[39] H.R.6671 - Video Privacy Protection Act Amendments Act of 2012112th Congress (2011-2012), https://www.congress.gov/bill/112th-congress/house-bill/6671（last visited Aug. 5, 2018).
[40] 18 U.S Code §2710 (b)(2)(B).
[41] FTC, Protecting Consumer Privacy in an Era of Rapid Change, P.20, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf（last visited Oct. 26, 2017).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

做為判斷標準。又，FTC 亦闡釋了以下三個要件，依此判斷經去識別化之個人資料無法合理連結到該個人：

(1) 採取合理的去識別化措施：並沒有既定的判斷標準，大致上透過資料的使用目的、現時技術所可能使用的方式進行個案判斷。

(2) 須公開承諾其維護和使用資料的方式，不會對去識別化資料進行重新還原（re-identify）：若企業對資料嘗試進行重行識別，FTC 可依據聯邦交易委員會法（Federal Trade Commission Act）第 5 條之規定，認定其行為涉及不公平（unfair）或欺罔（deceptive）[42]而違反隱私保護，對之採取行政或司法的強制措施。

(3) 當提供去識別化資料予第三人時，需訂立契約禁止接收者還原該資料：適當合理監督第三人是否遵循合約中禁止重行識別資料之約定，同時對違反者也須採取適切管理措施。

此外，FTC 亦在該報告書中揭示，當同時保有去識別資料與未經去識別化資料時，須對之分開保存與管理。

(五)隱私蒐集評估機制

美國目前在法規或政府之相關指引，就本研究蒐集範圍尚未有針對隱私蒐集評估機制之特殊規範。美國與歐盟所簽訂之「歐美隱私盾協議」（EU-U.S. Privacy Shield Supplemental Principles）中，亦未含有要求美

[42] 「不公平」係指一行為導致或可能導致消費者受損害，並且符合以下 3 個要件：(1)損害需顯著(substantial)；(2)該損害大於其他消費者所得享受或競爭上的利益；(3)該損害並非消費者可以合理避免者。而「欺罔」須為業者曾就其資訊行為或隱私權保護政策，作出不實或引人錯誤的說明。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

國企業進行隱私蒐集評估的規定[43]。不過，歐洲亦會在今年 7 月曾做出一個不具拘束力的決議，建議歐盟暫停隱私盾協議，此一決議被認為可能含有想要在歐美隱私盾協議下加入隱私衝擊影響評估等歐盟一般資料保護規則所新增規範的意圖[44]。

(六)小結

在法制方面，由於美國的個人資料保護並無統一適用的專法，而是依照各領域制定相關個資保護規範，因而研究中選擇下列和通訊傳播產業密切相關的法律做為討論基礎，有線電視隱私法（Cable TV Privacy Act）、1986 年電子通訊隱私法（ Electronic Communications Privacy Act）、1996 年通過之電信法（Telecommunication Act）以及美國更有特別專以兒童隱私保護對象制定了 1998 年兒童線上隱私保護法(Children's Online Privacy Act)。

針對通訊傳播事業取得資料之行為規範而言，電信法、有線電視隱私法、兒童線上隱私保護法，皆規範到在蒐集客戶資料前，須踐行通知程序或取得事前、事後同意。而電子通訊隱私法的部分，對於儲存和傳輸中的通訊資料之蒐集、儲存或揭露行為，目前對此尚未有法律明文。

個人資料保存機制方面，電信法、有線電視隱私法、兒童線上隱私保護法規範業者須對用戶資料的保存採取適當安全維護措施。

通訊傳播事業資料若要將個資提供予第三人方面，若電信事業欲將「用戶專屬資訊」揭露給第三人或用做行銷相關電信服務之用，需取得

[43] Privacy Shield Framework, U.S. Department of Commerce, https://www.privacyshield.gov/EU-US-Framework (last visited Nov. 15, 2018).
[44] Jennifer Baker, European Parliament: Suspend Privacy Shield unless US fully complies, IAPP, Jul. 5, 2018, https://iapp.org/news/a/parliament-suspend-privacy-shield-until-u-s-fully-complies/ (last visited Nov. 15, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

用戶事先同意，始得為之；但若是和第三人共同利用個資（如關係企業也是通訊相關業者），則事前無須取得用戶同意，而是採取事後當事人自行表示停止提供的「選擇退出」（opt-out）模式。兒童線上隱私保護法則被要求需經過授權，才可為之。

三、日本

(一)概述

日本政府於 2012 年 7 月公布「電子行政開放資料戰略」（電子行政オープンデータ戦略），開始重視資料加值與創新應用相關發展政策。

日本的資料開放係以地方自治團體和民間企業合作型態為主，藉由開放自治團體的資料來舉辦各式各樣的競賽以實現資料加值與創新應用，目前共有 23 個道府縣，157 個市區村提供資料加值與創新應用，而中央政府的資料加值與創新應用推動則以總務省(總務大臣)為核心的方式持續進行。

總務省為日本的通訊傳播事業之主管機關，但目前所有的民間機構，只要涉及利用個人資料者，皆受 2015 年修正的個人資料保護法（個人情報保護法）所規範，原則上以個人情報保護委員會作為獨立機關，負責監理、確保其遵守法令、訂立適當之自律規範等，以及統一法之解釋與適用。然而，針對特殊事業領域（例如：電信業），因考量其特殊專業技術背景、須監督確保其適當處理個人資料時，個人情報保護委員會可基於個人資料保護法第 44 條第 1 項[45]規定，得將相關權限委任特定範

[45] 個人情報の保護に関する法律,第四十四条第１項,「個人情報保護委員会は、緊急かつ重点的に個人情報等の適正な取扱いの確保を図る必要があることその他の政令で定める事情があるため、

本報告之智慧財產權歸屬於財團法人資訊工業策進會

圍及事項給目的事業主管機關(事業所管大臣)來監督管理。意即，個人情報保護委員會可將其對於通訊傳播事業之個資法監管權限，委任予總務省負責行使；但總務省需要依據個人資料保護法第 44 條第 2 項[46]，向個人情報保護委員會報告執行結果。另，目的事業主管機關(事業所管大臣)，又可按同法第 44 條第 3 項規定，將個人情報保護委員會所授予之全部或一部權限，委任下放給內閣府設立法（1999 年第 89 號）第 43 條所定的地方政府或機關首長執行[47]。

(二)通訊傳播事業取得各種資料類別之行為規範

法制方面，日本現行個資法第一章至第三章規範個資保護中，民間業者必須遵守之基本原則；第四章至第六章規範對象為民間業者，蒐集、處理及利用個資之總則性規定，確立共同最低標準，特別是對使用電腦或資料庫等儲存利用個人資料之相關單位（個人資料利用事業者），設定「個人資料利用事業者之義務」（個人情報取扱事業者の義務）。

通訊傳播事業對於個人資料之取得，係依循個人資料保護法之規定，該法在 2015 年修法時，區分為一般及特種個人資料，即修正條文第 2 條第 1 項第 2 款係規定「個人識別符號」；修正條文第 2 條第 3 項新增「敏感性特種資料」的規定。

個人情報取扱事業者等に対し、第四十二条の規定による勧告又は命令を効果的に行う上で必要があると認めるときは、政令で定めるところにより、第四十条第一項の規定による権限を事業所管大臣に委任することができる。」

[46] 個人情報の保護に関する法律,第四十四条第 2 項,「事業所管大臣は、前項の規定により委任された権限を行使したときは、政令で定めるところにより、その結果について個人情報保護委員会に報告するものとする。」

[47] 總務省，個人情報委員會授權委任予總務省之授權範圍，可參見：http://www.soumu.go.jp/menu_sinsei/kojin_jyouhou/index.html。法務部出國考察報告，考察日本因應大數據（Big Data）時代之個人資料保護法制及實務運作情形，106 年 10 月，頁 65-67，https://www.moj.gov.tw/dl-28588-5007e4fb32b94f0f84c7ab1d5da8a88b.html。日本個人情報委員會，權限委任可參見：https://www.ppc.go.jp/personal/legal/kengenInin/（最後瀏覽日：2018/11/12）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

「個人識別符號[48]」，係指將個人身體特徵所轉換成得以識別該特定個人的資訊，包含指紋資料、臉部辨識資料、護照號碼、證書執照號碼、電話號碼以及個人編號都被明確納入規範對象中。而「敏感性特種資料[49]」係指包括避免因本人之人種、信仰、社會身分、病歷、犯罪經歷以及因犯罪受有損害之事實以及其他會對本人造成不當差別、偏見以及其他不利益而必須特別就該資料之處理加以考量、且經政令規定之描述等之個人資料。此類敏感性特種資料，除法律規定、保護他人生命財產而難以取得同意、維護兒童健全身心發展、或公務機關依法遂行職務而難以取得同意等例外情形之外，原則上應經本人同意（參見第 17 條第 2 項[50]）。

又，個資法第 17 條規範了「適當取得之義務」，蒐集個人資料的業

[48]個人情報の保護に関する法律改正法，第二条第２項，この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。
一 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの。
二 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの。

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

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

一 法令に基づく場合。
二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
五 当該要配慮個人情報が、本人、国の機関、地方公共団体、第 76 条第１項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

者不得以欺騙或其他不正當手段取得個人資料。

此外，按前述個資法所揭示之原則，為推動個人資料保護政策的總合性具體推行，個資法第 7 條提及，政府應制定個人資料保護基本方針[51]，細節部分再行由總務省針對民間部門之電信、廣播事業業者所處理個資之個別特性，訂立「電信事業者對個人資料保護指引」(「電気通信事業における個人情報に関するガイドライン（Guide Line）」，下稱電信 GL）、「廣播領域對個人資料保護指引」（放送受信者等の個人情報保護に関するガイドライ ン，下稱廣播 GL）。以行政指導之方式，規範電信、廣播事業者對當事人之個資保護[52]。以下針對日本之通訊傳播事業，就電信和廣播領域如何取得個資之相關規定，分別進行說明。

1. 電信事業者對個人資料保護指引（下稱電信 GL）

電信 GL 共分為四大章共 39 條，第二章為總則性之個資處理共通原則(第 4 條至第 31 條)，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(第 32 條至第 38 條)。

從而，針對電信事業者蒐集個資之限制，規定於電信 GL 第 6 條：「電信事業者限於為提供電信通訊服務而有必要時，得為個資之蒐集。」同時，第 7 條第 1 項第 1 款規定，電信營運商不得以欺騙或其他不正當手段取得個人資料。

[51]個人情報の保護に関する法律改正法，第七条第 1 項，政府は、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、個人情報の保護に関する基本方針（以下「基本方針」という。）を定めなければならない。

[52]其法源依據為日本個資法第 8 條第 1 項：「国は、地方公共団体が策定し、又は実施する個人情報の保護に関する施策及び国民又は事業者等が個人情報の適正な取扱いの確保に関して行う活動を支援するため、情報の提供、事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その他の必要な措置を講ずるものとする。」

本報告之智慧財產權歸屬於財團法人資訊工業策進會

又，對於敏感性特種資料的蒐集，規定於電信 GL 第 7 條第 2 項，原則上需經該當事人同意；僅在下列例外情形，得蒐集：(1)依法令、(2)為保護本人生命、身體或財產的情形，取得本人同意有所困難時、(3)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時、(4) 協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，基於取得本人同意有可能對執行該事務造成阻礙的之虞時、(5)經由本人、國家機關、地方公共團體、個資法第 76 條第 1 項各款所揭示者、外國政府、外國的政府機關、外國的地方公共團體、國際機構、或在國外相當於個資法第 76 條第 1 項各款所揭示者公開該敏感之個資的情形時、(6)透過目視或拍攝到本人，取得其本人外形上明顯敏感之個人資料 (7)於第 15 條第 10 項各款所揭示之情形，接收敏感性之個人資料的提供等。

另，電信 GL 中亦就各種資料之蒐集、處理、利用訂立特別要件，以資料類型區分為七種，分別是：通聯紀錄、使用明細、發話人資料、位置資料、滯納費用之用戶資料、發送垃圾郵件芝契約用戶資料、電話號碼資料等（參見電信 GL 第三章第 32 條至第 38 條）[53]，茲分述如下。

(1) 通聯紀錄

> 按電信 GL 第 32 條第 1 項，通聯紀錄之定義，係指電信服務用戶使用該服務的日期、時間，與該通訊方除了其通訊內容以外之通訊相關資料。

[53]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本文，http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html（最後瀏覽日：2018/07/31）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

通聯紀錄為構成通訊的要素，受通訊秘密的保護，電信業者得蒐集通聯紀錄之範圍，僅限於為計算資費、請求繳費通知、客訴處理、防止不當利用及其他執行業務上之必要情形者。記錄最小必要限度內的通聯紀錄之行為，才可被視為正當業務行為以阻卻違法。

(2) 使用明細

按電信 GL 第 33 條第 1 項，使用明細，係指記載電信契約用戶通訊之日期、通訊時間、各通訊之對應方，並依一定費率計算通訊費用及其他記載有關通訊契約用戶資料之書面。意即，電信業者利用該明細作為請求、計算客戶所應支付費率的憑據；對用戶而言可據以作為確認其費用的清單。

自使用明細的記載事項觀之，內容包含了顯示開始通訊日期、時間、通話時間、對方電話號碼、每次通訊的金額、國際通話時的目的地等，幾乎等同於屬於秘密通訊的通聯紀錄，因此有必要考慮通訊秘密及個人隱私。因此，電信業者蒐集客戶使用明細之資料的範圍，不得超過達成使用明細之目的必要範圍。

此外，應避免記載不必要、可能侵害通訊對方之隱私資料，例如：在使用手機、PHS 的情形，根據對方的所在位置及與對方的距離設定資費系統時，由於對方收受訊號之地區的相關資料屬於繳費通知憑據的必要資料之一，但若記載對方所在位置過於詳細，可

本報告之智慧財產權歸屬於財團法人資訊工業策進會

能有不當侵害通訊對方之隱私權的疑慮，並不適當[54]。

另，針對使用明細資料之提供閱覽，按電信 GL 第 33 條第 2 項，得閱覽使用明細者，基本上為締約用戶本人，但也包含其他經用戶本人同意之經常使用者，及締約用戶以外關於閱覽具有正當利益的費率支付者[55]。

(3) 發話人資料

按電信 GL 第 34 條第 1 項，「發話人資料」，係有關發話人的電話號碼、姓名、住址、出生年月日及其他的敘述、得識別個人之編號、記號及其他符號、影像或語音等，得以辨識該特定發話人的資料，向受話人顯示的電話服務。「電話服務」則指固網電話、ISDN、行動電話、PHS、IP 電話等。

按電信 GL 第 34 條第 2 項，由於發話人資料通常屬通訊秘密，因此電信業者提供顯示發話人資料服務的情形時，為了確保使用者的權利應採取必要的措施。從委由發話人自行判斷是否向對方顯示發話人資料的觀點，電信業者應設置讓發話人每次通訊都可選擇不顯示發話人資料的功能。當發話人選擇向對方顯示發話人資料時，即被視為發話人對於受話人，並沒有欲將發話人自身資料隱匿的意思，因此並未構成通訊秘密之侵害[56]。

[54]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 109，http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html （最後瀏覽日：2018/11/20）。
[55]同前註，頁 110。
[56]同前註，頁 110、111。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(4) 位置資料

按電信 GL 第 35 條第 1 項，位置資料係指顯示持有行動設備終端機器者的位置資料，而非發話人資料的內容。本條中所提到的「行動設備終端機器」，係指除了行動電話終端機器（終端設備等規則（1985 年郵政省令第 31 號，第 2 條第 2 項第 5 款）及無線呼叫終端機器（同規則第 2 條第 2 項第 11 款）之外，泛指使用電波等進行通訊，所使用的終端機器。而所謂「位置資料」，係指顯示標記行動設備終端機器的持有人所在位置的資料，意即顯示基地台網域或概略位置登錄區域，或範圍更狹小的資料；但不包含使用明細中所記載的收訊地域（單位費用區域等）之類的內容。另，所謂「正當業務行為」係指從提供電信服務的觀點，具有正當業務目的，為了達成該目的之必要性及被認可之手段的相應行為。例如：為了使用行動電話進行通訊，在基地台等取得位置登錄資料的行為。

當電信業者事先得用戶同意時，僅以提供電信服務之相關正當業務行為及其他阻卻違法事由的情形為限，始可取得位置資料。理由係因，電信業者所持有之位置資料，亦被視為受通訊秘密保護[57]。

(5) 滯納費用之用戶資料

按電信 GL 第 36 條第 1 項，滯納費用之用戶資料，係指超過付

[57]同前註，頁 112、113 。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

款日期仍然拒繳電信服務相關費用者，包含行動語音通訊服務等相關契約之名義所有人的姓名、住址、滯納金額、電話號碼及其他該人或該名義所有人等，足以辨識個人之資料。

當電信業者為防止拒繳電信服務費用或不正當使用行動語音通訊服務，於有必要且被認為適當時，與其他電信業者之間，得交換滯納費用者之資料。但若交換該滯納費用者等資料，被認為可能有不當侵害本人權益的疑慮時，則不得為之[58]。

本條立法理由係：用戶因未支付電信費用而被解除契約，再和其他業者締結契約，其用戶同樣不支付費用之可能性極高；或與因未同意他電信業者確認雙方契約，而被停止用戶契約時，可能發生難以確認當事人的結果，造成無法向當事人請求電信費用之事件。為避免上述問題發生，容許最小限度內的滯納費用之用戶資料在業者間進行交換，防止該滯納費用之當事人一再重新向其他電信業者訂立新契約，減輕電信同業經營風險具必要性時，交換該類資料可被認為屬合法範圍[59]。

又，電信 GL 第 36 條尚規範了電信業者之間交換滯納費用者之資料的情形以及要求。詳細要件於後述章節「(四) 通訊傳播事業資料釋出之授權規範--提供個資予第三人」中論述之。

(6) 發送垃圾郵件之契約用戶資料

[58]同前註，頁 116、117 。
[59]前揭註 10，頁 143-144。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

按電信 GL 第 37 條第 1 項，當電信業者為防止因濫發電子垃圾郵件所造成電子通訊網路之障礙，於有必要且被認為適當時，與其他電信業者之間，得交換該濫發郵件之契約用戶資料，例如姓名、住所等。但若交換該資料，被認為可能有不當侵害本人權益的疑慮時，則不得為之。

本條規範目的係為了防止濫發垃圾郵件用戶以虛構電子郵件位址同時大量寄送電子郵件，而被電信業者解除契約後，該濫發垃圾郵件用戶又和其他電信業者締約，繼續大量寄送垃圾郵件，使電信業者伺服器的系統負擔加重的情事重複發生[60]。

又，此類資料提供予第三人之前提和要求與前揭交換滯納費用之用戶資料的方式類似。詳細要件亦於後述章節「(四)通訊傳播事業資料釋出之授權規範--提供個資予第三人」中一併論述之。

(7) 電話號碼資料

電信業者將電話號碼資料印製發行電話簿或提供電話號碼查詢之服務時，按電信 GL 第 38 條第 1 項規定，應給予締約用戶有所選擇的機會，若締約用戶選擇拒絕提供時，必須立即將該用戶的資料排除於刊載在電話簿或電話號碼查詢業務的對象之外。

又，電信業者刊載或提供電話號碼查詢業務時的限制，規定於電信 GL 第 38 條第 2 項，與達成其業務目的間，不得超過最低必要限度，其範圍應以刊載姓名、住所、電話號碼或刪除部分住址

[60]前揭註 54，頁 118-120。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

為限[61]。但經用戶同意時，則不在此限。同時，電信 GL 第 38 條第 3 項尚規定，電信業者發行電話簿或提供電話號碼查詢服務的形態，不得不當侵害本人之權益。

2. 廣播領域對個人資料保護指引（下稱廣播 GL）

本指引係對廣播相關資料、視聽紀錄之蒐集、處理及利用，包括匿名加工化，進行規範。

針對廣播業者蒐集個資之限制，規定於廣播 GL 第 6 條：「受信者資訊處理業者在取得放送受信者等的個資時，需僅限於必要時。」其中，「必要時」，不單指現在事業直接需要時，包含和其有關連性之情形（例如：新開發事業的問卷調查等）[62]。同時，第 7 條第 1 項第 1 款規定，廣播資訊處理業者不得以欺騙或其他不正當手段取得個人資料。

另，對於敏感性特種資料的蒐集，規定於廣播 GL 第 7 條第 4 項，原則上需經當事人同意；例外僅在依法令、為保護本人生命、身體或財產、公共利益或維護兒童身心健全發展而取得當事人同意有困難等情形，始得蒐集。

又，廣播 GL 第 34 條規定了廣播資料處理業者對「視聽紀錄的存取」，需注意無法從而推論出、或使第三人推知閱聽者本人的敏感性特種個資。例如，廣播資料處理業者依據特定健康資訊為主題的節目之視聽紀錄，推薦其他時間所播送的類似節目、以相似健康資訊為主題的節目之行為，不會有立即性問題發生。但，倘若係依據該用戶視聽紀錄的分

[61]前揭註 54，頁 121、122。
[62]放送受信者等の個人情報保護に関するガイドラインの解説，頁 110，http://www.soumu.go.jp/main_sosiki/joho_tsusin/040831_1.html（最後瀏覽日：2018/07/30）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

析結果，推論判讀出閱聽者或其家族成員的病歷或身體殘障等之行為，是不被允許的[63]。

同時，廣播 GL 第 35 條第 1 項規範了蒐集視聽紀錄之限制，當廣播資料處理業者，不得逾越視聽紀錄存取的範圍（即透過電磁方式計算相關費用，或向用戶要求支付費用為其目的時；或以做成統計數據為其目的；抑或以做成匿名化資訊為其目的），否則需事先得到當事人的同意為其要件。

此外，即便廣播資料處理業者先前已按前述第 35 條第 1 項取得當事人同意存取相關收視紀錄，當事人仍可依據廣播 GL 第 35 條第 3 項，後續有權向業者要求停止蒐集該視聽紀錄，此時，業者需將下列事項通知當事人，或使當事人處於知悉的狀態：（1）能回應當事人的要求，停止取得該當事人的視聽紀錄；（2）受理當事人請求的方法。

(三)通訊傳播事業個人資料保存機制

1. 適當安全管理措施

保存機制而言，依個資法第 20 條、電信 GL 第 11 條、廣播 GL 第 11 條，分別皆要求電信營運商、廣播資訊處理業者需建構必要且適當的個資安全管理措施，以防止其所蒐集到的個資外洩、丟失或毀損之情事發生。尤其在關於施行安全管理措施的具體方法，須考慮到個人資訊外洩時，當事人所受到權利利益侵害程度，以及事業的規模及性質、個人資料的處理狀況（包含存取個人資料的性質與量）等因素，進而評估

[63]同前註，頁 41。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

所會造成之風險，再做出必要且適切的處理[64]。

而廣播 GL 第 14 條亦要求廣播業主在播送節目用來存放個資的記憶裝置機器，與之連接通信網路設備時，需建置下列措施：（1）使用暗號方法等必要措施，確保所使用的機器和通信網路設備具個資傳輸的安全性，防止他人以任何方式復原密碼等不正當存取當事人個資的行為；（2）當節目放送時，發送認證資訊，需以不違反當事人意願方式為之。

再者，電信 GL 第 13 條、廣播 GL 第 13 條，要求業者需設置「個資保護管理者」（負責該業者的個資存取相關責任者），遵循本指引制定內部規程、監察機制以及監督業者的個資存取等事宜。意在為了防止資訊處理業者內部或外部的不正當行為，導致個資外洩等，使責任區分明確化[65]。

2. 保存期間之規定

在電信業者個人資訊保存期間方面，依據電信 GL 第 10 條第 1 項前段規定，電信業者處理個人資訊時，應以達成利用目的之必要範圍內訂定保存期間為原則。該保存期間屆滿後或該使用目的已達成後，應立即刪除該個人資訊。

但仍有資訊保存期間之例外情形，參見電信 GL 第 10 條第 1 項後段規定，包含：（1）基於法令規定應予保存者；（2）經本人同意者；（3）電信事業者為遂行業務之必要限度內，認為有保存個人資訊之需要，有相當理由不予刪除者；（4）有特別理由不予刪除者。換言之，電信事業者若認為有符合上述四種情形之一，即可於保存期間經過後或使用目的

[64]同前註，頁 53、117。
[65]前揭註 54，頁 57。前揭註 62，頁 57。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

達成後，仍保存該個人資料不予刪除。

且按電信 GL 第 10 條第 2 項規定，除非經用戶同意或有其他阻卻違法事由，否則電信業者不得儲存與通信秘密有關之個人資料，但即使被允許保存，也必須在達到使用目的後立即刪除該個人資料。

尤其，針對「通聯紀錄」的保存期間，雖然得根據電信商所提供之服務的種類、資費等、每個電信業者、通聯紀錄種類的差異，但也得考量執行業務上的必要性及進行保存時的影響等，應設定、限定保存期間。例如：在通聯紀錄中，關於網路連線服務之連線驗證紀錄（驗證使用者、網路連線必要的 IP 位址分配紀錄）、用戶契約、使用狀況等回應及安全使用對策等，在業務上可能具有高度的保存必要性。另一方面，用戶的表現行為及隱私權的關連可能較小的緣故，因此電信業者有必要執行這些業務時，一般允許保存 6 個月左右；而從確保正確地經營網路的觀點來說，有必要掌握年度狀況的情形時，在業務上有必要保存更長的情形時，則被允許保存 1 年左右[66]。

另，在廣播業者個人資訊保存期間方面，按廣播 GL 第 10 條第 1 項：「廣播資訊處理業者在存取閱聽者等之個人資訊時，應訂立使用目的範圍及保存期間，該保存時間屆滿後、或為達成使用目的而合理保留該個資的理由已不復存在時、或使用目的未達成，而事業中止等情況發生時，須盡速將該個人資料刪除。」以及同條第 2 項規定，廣播資訊處理業者在取得閱聽者等的個資時，除事先公告其保存期間外，須盡速通知當事人或公告其保存期間。

[66]前揭註 54，頁 108，。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(四)通訊傳播事業資料釋出之授權規範

1. 提供個資予第三人

「提供個資予第三人」的範疇包含：關係企業[67]、集團公司、加盟組織的總部與加盟店間的個人資料交換；電信事業業者間進行特定的個人資料交換[68]；及廣播資料處理業者間進行特定的個人資料交換[69]。

提供個資予第三人之限制而言,除日本個資法第 23 條第 1 項有所規範之外，亦分別訂於電信 GL 第 15 條第 1 項、廣播 GL 第 16 條第 1 項當中，皆有明確規範，即電信事業者/廣播資料處理業者，若要將個人資料提供予第三人時，原則上需事先取得本人同意，也就是採取選擇加入（opt-in）的個資保護模式；但下列四種情形除外：（1）基於法令者；（2）為保護個人生命、身體或財產之必要，且取得本人同意有困難者；（3）為提升公共衛生或促進兒童健全發展，有特殊必要，且取得本人同意有困難者；（4）國家機關、地方公共團體或受其委託者，對於遂行法令所規定之事務有協助必要時，且取得本人同意具有妨礙該事務遂行之虞者。而取得同意時，根據事業的規模及性質、個人資料處理狀況（包含所處理個人資料等之性質及數量）等，為期本人做出同意之相關判斷，必須在合理且適當的範圍內，以及事先可預知向第三方提供個人資料的

[67]日本「關係企業」（親子兄弟会社），意指母子公司和姊妹公司包含在內。針對母、子公司之定義可參見日本公司法第２條第３項及第４項、公司法施行細則第３條第２項，「子公司」係指依據法務省命令規定的公司，由母公司管理、控制，包括但不限於股份公司，其中大部分投票權歸母公司所有。而母公司係指控制、管理主導地位者，包含但不限於以股份公司作為其附屬公司。意即，實質上控制財務和業務政策決策的情形下，股權超過 50%，控股公司為母公司，被控制的是子公司。
[68]前揭註 54，頁 61。
[69]前揭註 62，頁 61。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

情形時，必須特定其使用目的[70]。

但仍應留意的是，電信 GL 第 15 條第 8 項對於涉及秘密通訊有特別例外規定，當提供第三人之個資為秘密通訊之資料(如：通聯紀錄[71]等)時，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，否則不得提供[72]。例如，公司遭大量且隨機發送之廣告郵件攻擊、癱瘓電腦系統，使自家網路和服務受到威脅，基於保護自己或他人權利之必要且不得已的情形，可允許將相關通聯歷程（發信者的 IP 位址及時間戳記等），提供予發信來源的所屬電信業者，例外不受提供通聯紀錄規定的限制[73]。

又，針對「發話人資料」對第三人提供之限制，亦有類似規定，按電信 GL 第 34 條第 3 項，電信業者除有提供顯示發話人資料服務及其他服務的必要情形之外，原則上不得向第三人提供發話人資料；但倘若（1）經發信人和受信人雙方同意；或（2）依法院核發之令狀；或（3）根據被害人及搜查機關的要求，進行反向追蹤現正利用電話進行恐嚇、脅迫的犯罪者之所在地者；或（4）人的生命、身體等有急迫危險之緊急通報的情形，依該通報人之請求而須進行反向追蹤時；或（5）有其他阻卻違法事由者，不在此限[74]。

而關於「位置資料」亦有對第三人提供之條件限制，按電信 GL 第 35 條第 2 項，電信業者僅限於事先取得用戶同意、依法院所核發之令狀及其他阻卻違法事由的情形時，才可將位置資料提供予第三人及做為其

[70]前揭註 54，頁 60、61。前揭註 62，頁 61、62。
[71]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，第 32 条第 2 項。
[72]前揭註 54，頁 69、107。
[73]前揭註 54，頁 108、109。
[74]前揭註 54，頁 111。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

他用途。再者，電信業者提供通知用戶或其所指示之人位置資料的服務，或向第三方提供的情形時，必須考慮其對社會上的實用性與秘密通訊或隱私權保護之間的衡平，按電信 GL 第 35 條第 3 項規定，為了防止不當侵害用戶權利的行為，須採取「必要措施」。就「必要措施」的具體內容而言，包括：（1）務必根據用戶的意願進行位置資料的提供；（2）關於位置資料的提供，務必確保用戶有認識、預見的可能性；（3）務必針對位置資料進行適當的處理，如：無權限者不得監看移動端所顯示之位置資料、或設定密碼、限制近用、訂立相關管理規則，以避免業者所管理的基地台資料被他人不當利用等方式；（4）在與第三方合作而提供服務的情形，涉及合作契約相關保密條款等記載，務必考量保護用戶之隱私。

電信 GL 第 36 條、第 37 條尚分別規範了電信業者之間交換「滯納費用者之用戶資料」、「發送垃圾郵件之契約用戶資料」的情形，應在契約條款中載明，事先通知當事人或使其可得而知較為適當，包含其（1）交換要旨、（2）被交換之用戶資料的項目、（3）交換之電信業者範圍、（4）負責管理該交換資料者的姓名或名稱。同時，因滯納費用之用戶資料屬於一種個人信用資料，電信業者不得將該類資料，使用於締約時審查目的以外之用途[75]。另，針對「發送垃圾郵件之契約用戶資料」，就使用目的之限制而言，也不可將該交換所得到的資料，使用於締約審查以外之目的[76]。

電信業者將「電話號碼資料」對外提供亦有所限制，依據電信 GL 第 38 條第 4 項規定，原則上，電信業者除為印製發行電話簿或提供電話

[75]前揭註 54，頁 117、118 。
[76]前揭註 54，頁 118-120。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

號碼查詢之服務以外，不得對外提供電話號碼之資料。但在下列所揭示的例外情形時，始可為之：(1)委外發行電話簿或從事電話號碼查詢業務時；(2)向發行電話簿或將其提供給從事電話號碼查詢引導業務者時；(3)其他適用第 5 條第 3 項各款的情形(即依法令；或保護他人生命財產而難以取得同意；維護兒童健全身心發展；或公務機關依法遂行職務而難以取得同意)。

此外，對於電信業者/廣播資料處理業者，另有選擇退出模式（opt-out）的設計，參見日本個資法第 23 條第 2 項、電信 GL 第 15 條第 2 項、廣播 GL 第 16 條第 2 項，基於尊重當事人的意思，即便已得到當事人的同意，若該當事人申請停止提供個資時，可依據此規定退出之，並應將下列事項預先通知當事人，或使當事人處於容易得知之狀態下：（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；（4）回應當事人請求，停止提供給第三人，能識別該當事人個人資訊；（5）接收當事人請求的方法[77]。

2. 提供給外國之第三人

提供給外國之第三人的限制而言，除日本個資法第 24 條有所規範之外，亦可參見電信 GL 第 16 條、廣播 GL 第 17 條。又，對提供予外國第三人之資料限制，可參考個人情報保護委員會所規定之「有關保護個人資料之相關法律的指引（向位於外國之第三方提供篇）[78]」（2016 年個人情報保護委員會公告第 7 號）為準則。原則上需先取得當事人同意才

[77]前揭註 10，頁 136-137。

[78]個人情報の保護に関する法律についての
ガイドライン（外国にある第三者への提供編）（平成 28 年個人情報保護委員会告示第７号）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

可提供，但下列四種情形除外：（1）基於法令者；（2）為保護個人生命、身體或財產之必要，且取得本人同意有困難者；（3）為提升公共衛生或促進兒童健全發展，有特殊必要，且取得本人同意有困難者；（4）國家機關、地方公共團體或受其委託者，對於遂行法令所規定之事務有協助必要時，且取得本人同意具有妨礙該事務遂行之虞者。並且，電信業者與個資接收者之間，該個資接收業者所建構之資料處理措施必須為持續性的，其判斷基準需符合下列任何一項：（1）須確保以適切且合理的方法，依照個資法第 4 章第 1 節規定為之；（2）其個資的存取需依據國際相關基準的認定[79]。

另，附帶一提，為推動日本及歐盟間，雙方得以順利互相傳輸個人資料，確保能保護接受歐盟境內安全適足性認定轉移的個人資料，個人情報保護委員會希望基於法律第 24 條規定，認定歐盟在保護個人權益上，已建立和日本同等水準之個人資料保護制度；同時，歐洲委員會亦基於 GDPR 第 45 條規定，判定日本足以充分保護個人資料。進而監督使用個人資料之業者，須適當且有效率履行義務，並以適度接受歐盟境內安全適足性認定轉移的個人資料此一觀點出發，制定了個人資料保護法關於歐盟安全適足性認定傳輸個資之補充規則[80]。

3. 去識別化規定

此外，資料匿名化及重新識別之規範方面，日本原先的舊個人資料保護法（個人情報保護法）未有明文規定，但為因應大數據加值與創新

[79]前揭註 54，頁 74。前揭註 62，頁 74。
[80]個人情報の保護に関する法律に係るＥＵ域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール ，2018 年 09 月，http://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf（最後瀏覽日：2018/11/15）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

應用等技術科技對個資使用的需求，2015 年展開修法工作，同年 9 月 3 日經眾議院修正通過，並於 2017 年 9 月施行。

此次個資法增修條文第 2 條第 9 項，新增「匿名處理資料」的概念，其係指「對個人資料採取一定的匿名化措施處理，使其無法識別特定個人所得之關於個人的資料，且該個人資料無法復原[81]。」。而所謂「匿名化措施具體內容」，是指將包含該個人資料等資訊的一部消除（但若該資訊包含得以識別個人符號時則必須全部消除），或是以不帶有可能復原個人資料規則性的方法替換成其他的記述。從而，經過「匿名處理資料」非屬於「個人資料」之範疇，因此一旦被視為屬「匿名處理資料」，可不受目的外使用或是向第三人提供規定的限制。惟，需特別注意的是，迄經匿名處理的資料並非完全不受任何限制，個資法對於作成「匿名處理資料」的「個人資料處理業者」以及「匿名處理資料處理業者」等，仍對之課以相當的義務（參見修正條文第 36 條、37 條、39 條）。

同時，修正條文第 36 條第 5 項以及第 38 條亦明文規定當處理「匿名處理資料」時，禁止重新識別。

又，針對去識別化的標準，日本個人情報保護委員會係以「去識別化指導方針」（個人情報の保護に関する法律についてのガイドライン

[81]個人情報の保護に関する法律改正法，第二条第９項，この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
一 第１項第１号に該当する個人情報 当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
二 第１項第２号に該当する個人情報 当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

本報告之智慧財產權歸屬於財團法人資訊工業策進會

（匿名加工情報編））[82]， 闡明去識別化的範例（包括移動資料等）、列舉識別因子、提出關於個人識別與再識別的風險、提示去識別化的方法（如：特異值消除、匿名化）等。

(五)隱私蒐集評估機制

日本目前無論法規或政府之相關指引，就本研究蒐集範圍尚未有針對隱私蒐集評估機制之規定。

(六)小結

在日本通訊傳播事業的個人資料保護法制方面，除了現行的個人資料保護法和其指引確立了共同最低總則性標準之外，考量電信、廣播事業業者其所涉個資的特殊性，特別對該領域訂有相關的保護指引與其相關解說文件（即電信事業者對個人資料保護指引、廣播領域對個人資料保護指引）。惟，不同於美國、英國，目前尚未有針對兒童隱私保護之特別規範。

針對通訊傳播事業取得資料之行為規範而言，電信、廣播事業業者蒐集個資之限制，區分為一般及敏感性特種資料。尤其在敏感性特種資料的蒐集，原則上需經該當事人同意；例外基於法令或公共利益、維護兒童身心發展等特殊情形下才毋須經同意。此外，尚有特別規範廣播事業業者對於「視聽紀錄」之蒐集限制，原則上亦以事先取得當事人的同意為其要件，但後續當事人仍有權向業者要求停止蒐集該視聽紀錄。

個人資料保存機制方面，皆要求電信營運商、廣播資訊處理業者需建構必要且適當的個資安全管理措施，並需設置「個資保護管理者」負

[82]個人情報保護委員会，個人情報の保護に関する法律についてのガイドライン（匿名加工情報編），https://www.ppc.go.jp/files/pdf/guidelines04.pdf（最後瀏覽日：2018/07/29）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

責監督業者之存取機制。

通訊傳播事業在對第三人提供個資方面，原則上採取得當事人事前同意之選擇加入的模式（opt-in)；但後續當事人仍有申請停止對第三人提供個資之權利。此外，日本在提供個資給「外國之第三人」的部分尚有特別規範，亦採取原則上事前須經當事人同意的模式；例外在基於法令或公共利益、維護兒童身心發展等特殊情形下才毋須經同意，並同時要求業者需建構持續性的管理措施。

四、英國

(一)概述

英國之個人資料保護有一專門法令——資料保護法規定，英國為因應歐盟一般資料保護規則（以下簡稱 GDPR）之施行，於今（2018）年 5 月通過「2018 年資料保護法」(Data Protection Act 2018)，除了透過內國法律程序完成 GDPR 的施行外，針對 GDPR 授權各國自行調整的部份亦有規定，也針對 GDPR 未規定之部份（包含「執法相關之個資處理」（Law Enforcement Processing）[83]、「情報相關之個資處理」(Intelligence Services Processing）[84]）以及資訊長[85]、資訊長辦公室之職權、組織還有執法等[86]事項。

其中，執法相關之個資處理，規定在 2018 年資料保護法的「第 3 編」(part 3)。規範執法相關之個資處理，包含預防、「調查」

[83] 參照 Data Protection Act 2018 (UK), part 3.
[84] 參照 Data Protection Act 2018 (UK), part 4.
[85] Information Commissioner，一般國內常見翻譯為「資訊專員」，惟因在我國語境中「專員」似乎較不能突顯其首長之性質，爰將其翻譯為資訊長。
[86] 參照 Data Protection Act 2018 (UK), part 5-6.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

（investigation）、「偵查」（detection）、「起訴」（prosecution）刑事犯罪或是執行刑罰（包含對公共安全的預防及保護等）[87]。該部份是為了將歐盟「執法指令」（Law Enforcement Directive EU 2016/680）的內容轉化為內國法所特別擬定[88]。至於情報相關之個資處理則是規定在第 4 編之中，規範英國「安全局」（Security Service，俗稱軍情五處）、「祕密情報局」（Secret Intelligence Service，俗稱軍情六處）以及「政府通訊總部」（Government Communications Headquarters，為情報部門非通訊傳播主管機關）等情報部門個人資料保護的相關事宜[89]。此二編所規範的皆是特定政府部門所為個人資料的保護，雖因其各自工作之性質，在某些規範尚有所調整，但基本的個人資料保護原則仍然適用[90]。不過，無論是通訊傳播事業或通訊傳播主管機關，皆未適用上開規範，而是依據 2018 年資料保護法規定適用 GDPR。

其中，執法相關之個資處理係將歐盟執法指令之內容轉化為內國法律規定。根據 2018 年資料保護法之規定，為預防、調查、偵查、起訴刑事犯罪或執行刑罰等目的而處理個人資料，須取得當事人之同意，或在其對於主管機關執行目的有必要時才可以進行[91]。而針對處理特種資料的要件則要求須取得當事人之同意並制定適當的政策守則，或是在有嚴格需要的情形下，限於特定目的並制定適當政策守則時才可進行處理[92]。2018 年資料保護法亦規定，因執法目的而蒐集之資料，不可將其保存超過原蒐集十隻特定目的所需之時間，並應建立適當的時間限制，定

[87] Data Protection Act 2018 (UK), art. 31.
[88] INFORMATION COMMISSIONER'S OFFICE, *An Introduction to the Data Protection Bill* 42 (2018).
[89] Data Protection Act 2018 (UK), art. 82.
[90] Data Protection Act 2018 (UK), art. 35-40 & 84-91.
[91] Data Protection Act 2018 (UK), art. 35(2).
[92] Data Protection Act 2018 (UK), art. 35(4)(5).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

期審查為何須因執法目的繼續儲存個人資料[93]。而在蒐集後，資料控制者無論如何必須將資料控制者之身份、聯絡方式、蒐集之目的、當事人可享有之權利以及若有資料保護專員時該專員的聯絡方式等使當事人得以知悉（無論是使這類資料可為大眾得知或直接通知當人皆可）[94]。此外，資料控制者亦須將處理之法律基礎、資料儲存期間、資料接收者類型、任何其他進一步之資訊（尤其是該蒐集是在當事人不知情的情形下進行的時候）告知當事人，但若是為了避免依法之調查、避免妨礙犯罪偵防或保護公共安全、國家安全、他人之權利等目的，資料控制者得在比例原則的考量下，限制提供上述資料的全部或一部給當事人[95]。也就是說，2018 年資料保護法要求依據執法目的蒐集資料之機關，原則上必須提供上述資料給當事人，僅在特定情形下得限制提供部份資料。最後，2018 年資料保護法亦要求，基於執法目的所為蒐集之資料控制者，如果考慮到期性質、範圍、脈絡以及處理之目的，認為其處理的型態可能將造成當事人權利與自由高度風險，則應在處理前進行資料保護衝擊影響評估；該評估應包含對於處理措施的一般性描述、對風險的評估、解決風險的措施及其他確保符合法率規範的安全維護措施，並考慮當事人的權利及合法利益[96]。

由於 2018 年資料保護法對於一般個人資料之保護（包含對通訊傳播事業之相關規範）皆依照 GDPR 之規定辦理；而英國資訊長亦表明，即便英國退出歐盟後，英國仍會繼續適用 GDPR 的相關規範[97]，因此本研究接下來將以 GDPR 相關規定為核心。

[93] Data Protection Act 2018 (UK), art. 36.
[94] Data Protection Act 2018 (UK), art. 44(1)
[95] Data Protection Act 2018 (UK), art. 44(2)(4)
[96] Data Protection Act 2018 (UK), art. 65
[97] Elizabeth Denham, Information Commissioner (UK), Remarks at IAPP Europe Data Protection Intensive 2018 (Apr. 18, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

同時，GDPR 規定，在歐盟下設立「歐洲資料保護委員會」（European Data Protection Board）[98]，該委員會可以為確保 GDPR 一致適用的目的，針對 GDPR 發布「準則」（Guideline）、「建議」（recommendation）以及「最佳實務」（best practice）[99]。這些文件，由於並非「歐洲聯盟運作條約」（Treaty on the Functioning of the European Union）第 228 條所規定具有法律拘束力之文件，因此並不具有形式的拘束效果（但由於可能實質尚有拘束的功能，因此也被認為具有「柔性規範」（soft law）的性質）[100]。另外，英國 2018 年資料保護法賦予英國資訊長針對法條內容發布相關指引之權利，該法亦未明言此指引有法律拘束力。上述指引雖未具有法律拘束力，但仍會有實質上給予業者指引之功能，故仍將這些指引納入討論。

(二)通訊傳播事業取得各種資料類別之行為規範

根據 GDPR 之規定，通訊傳播事業在取得個人資料時，針對一般資料與特種資料分別訂有不同之合法權源之規定，並對兒童之資料有特殊之規定，茲分述如下：

1. 一般資料

根據 GDPR 第 6 條的規定，對於一般資料，合法之處理[101]應符合下列六個條件之一：

[98] Regulation (EU) 2016/79, art. 68, 2016 (L119), 1, 76.
[99] Regulation (EU) 2016/79, art. 70, 2016 (L119), 1, 76-78.
[100] Soft law, EUROFOUND, https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/soft-law (last visited Aug. 2, 2018).
[101] 依照歐盟 GDPR 及英國個資法之定義，「處理」（process）包含我國個資法中所說蒐集、處理及利用等行為。本研究於討論英國相關法令規章時，所稱之處理，皆包含我國個資法所稱之蒐集、處理及利用，合先敘明。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(1) 當事人同意；

(2) 履行契約關係所必須（包含契約締結前，因當事人要求所採取之步驟）；

(3) 為遵守法定義務所必須：

(4) 為保護當事人或其他人的「重大利益」（vital interest）所必須；

(5) 為符合公共利益執行職務或受委託行使公權力所必須；

(6) 資料控制者為追求自己或第三人之「合法利益」（legitimate interests）所必須，且資料當事人之利益、基本權與自由並未優先於該合法利益（但公務機關執行職務時，不得以此主張）[102]。

其中，GDPR 對於「同意」的條件有特別詳細與嚴格的規定。GDPR 規定，同意須與其他一併提出之文件清楚明白的區分，若是未妥善區分（例如將非提供服務、履行契約所必須的同意事項與必須的同意事項掛勾），則該同意無效；同意的內容應以易懂、方便取得的格式，以及清楚、簡易的語言提供；同時，當事人有權隨時、容易的撤回同意[103]。依據歐盟個資指令所成立的第 29 條工作小組在 2017 年 11 月 28 日針對 GDPR 的同意規定曾經發布指引，而該指引又於 2018 年 4 月 10 日有過修正[104]。第 29 條工作小組雖已隨著個資保護指令失效而停止運作，但依據 GDPR

[102] Regulation (EU) 2016/79, art. 6, 2016 (L119), 1, 36-37.
[103] Regulation (EU) 2016/79, art. 7, 2016 (L119), 1, 37.
[104] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Article 29 Working Party Guidelines on consent under Regulation 2016/679* 1 (2018), *available* at. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (last visited Aug. 2, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

所設立的歐洲資料保護委員會在成立後已經宣佈將繼續適用此一指引[105]。

英國資訊長辦公室針對「同意」有更詳細的說明，在其為企業（組織）所發布的 GDPR 指引中特別說明，同意應該是積極的選擇，不可以是預先勾選或是默認的格式，並說明同意的要求應該要是「精細化的」，應該要避免將同意事項混合在一起取得同意；同時不要過度依賴同意，如果同意困難，「請尋找不同的合法依據」[106]。英國資訊長辦公室對於「同意」另外出具更為詳細的指引，於該指引中，特別例示何種實踐的方法符合 GDPR 之規範[107]。此外，資訊長辦公室也對其他合法權源有提供指引做更清楚之解釋[108]。

2. 特種個資

(1) 特種個人資料之類別

歐盟 GDPR 將種族、人種、政治意見、宗教或哲學信仰、工會會員身份、基因、用於識別個人之生物識別資料、健康、性生活或性傾向之個人資料列為特種個人資料[109]，同時歐盟對於前科資

[105] Endorsement of GDPR WP29 guidelines by the EDPB, European Data Protection Board, https://edpb.europa.eu/node/89 (last visited Aug. 2, 2018).
[106] Consent, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (last visited Aug. 2, 2018).
[107] Consent | what is valid consent?, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ (last visited Aug. 2, 2018).
[108] Lawful basis for processing, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited Aug. 2, 2018).
[109] Regulation (EU) 2016/79, art. 9, 2016 (L119), 1, 38-39.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

料亦有更為嚴格之規定[110]。

(2) 特種個人資料蒐集之合法權源

根據 GDPR 之規定，原則上特種個資是禁止處理的，只有在下列情況得以處理：

A. 得當事人「明確」（explicit）同意；

B. 履行契約；

C. 未保護資料當事人或他重大利益所必須，且當事人在物理上或法律上無法給予同意；

D. 當事人已經明確自行公開；

E. 建構、行使、防禦法律上之請求或法院執行司法權所必要；

F. 基於歐盟法或會員國法所規定、合比例性之重大公益所必要；

G. 公共衛生、醫學、非營利組織基於特定目的所必要；

H. 基於歐盟法或會員國法，為公共利益「建檔」（archive）、為科學或歷史研究、統計等目的且提供適當保護措施並經比例性檢驗[111]。

對於前科資料，則僅於公務機關控制下或由歐盟法或會員國法在

[110] Regulation (EU) 2016/79, art. 10, 2016 (L119), 1, 39.
[111] Regulation (EU) 2016/79, art. 9, 2016 (L119), 1, 38-39.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

採行適當保護措施下授權才可處理[112]。

英國 2018 年資料保護法則對上述的具體狀況有更為細節的規定，例如對於前述研究目的、健康目的等之內涵有更為清楚之規定[113]。同時，資訊長辦公室也針對此條文有初步之解釋，並表示將準備對此做出更詳細之指導[114]。

3. 兒童資料之蒐集

GDPR 要求，在對低於 16 歲的兒童提供資訊社會服務時，需要其法定代理人同意或授權，處理才合法，此一年齡授權會員國可調降[115]。英國 2018 年資料保護法將其降為 13 歲。也就是說，在英國對兒童提供資訊社會服務時，僅有 13 歲以下兒童才須由法定代理人同意或授權[116]。此外，英國資訊長辦公室亦針對此部份提供指引，包含提供檢核表等方法，協助業者符合 GDPR 之規定[117]。

(三)通訊傳播事業個人資料保存機制

(1) 適當安全維護措施

GDPR 針對個人資料之保存，在組織面上以及程序面上，都有不同的規定，以下將分別從組織面以及程序面上，分別加以介紹。

---

[112] Regulation (EU) 2016/79, art. 10, 2016 (L119), 1, 39.
[113] Data Protection Act 2018 (UK), sec.10,11,schedule 1..
[114] Special category data, Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last visited Aug. 2, 2018).
[115] Regulation (EU) 2016/79, art. 8, 2016 (L119), 1, 37-38.
[116] Children, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/ (last visited Aug. 2, 2018).
[117] *Id.*

本報告之智慧財產權歸屬於財團法人資訊工業策進會

A. 組織面

GDPR 要求，若資料的控制者或處理者的核心活動涉及系統性的大規模監控資料當事人，或涉及大規模處理特種個資的話，該控制者應指定「資料保護員」(Data Protection Officer)[118]。此一資料保護員應負責監督 GDPR 及相關個資保護政策之執行（包含責任分配、認知喚醒、教育訓練以及監督實行），並在資料保護影響評估等程序中提供建議，並與主管機關聯繫，此一資料保護員應確保其獨立性，並能直接向組織的最高管理階層報告[119]。第 29 條工作小組針對資料保護員之職責、須設立資料保護員之具體情況等曾於 2017 年 4 月發布指引[120]，歐洲資料保護委員會並繼續承認該指引[121]。英國資訊長辦公室的指引則進一步提供了檢核表、問卷以及示例，以協助組織確認是否須指定資料保護員，以及該如何設計資料保護員之職位與權限[122]。

B. 程序面

在程序上 GDPR 要求一個「全資料生命週期」的隱私保護，其規定要求控制者應採用科技化、有組織的措施保障資料安全，並定期審視與更新相關的適當資料保護措施[123]。並要求於處理時應確保系統與服務的機密性、完整性、可用性以及

[118] Regulation (EU) 2016/79, art. 37, 2016 (L119), 1, 55.
[119] Regulation (EU) 2016/79, art. 38-39, 2016 (L119), 1, 55-58.
[120] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers ('DPOs') WP 243 rev.01 (2017).
[121] *Supra* note105.
[122] Data protection officers, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/ (last visited Aug. 7, 2018).
[123] Regulation (EU) 2016/79, art. 24, 2016 (L119), 1, 47.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

彈性，並盡可能實施假名化或加密等措施，應視現有技術、執行成本以及處理的脈絡、範圍、本質、目的以及可能的風險等，採取各項適當之安全保護措施[124]。具體來說，GDPR 要求「從流程設計階段就包含隱私考慮」（privacy by design），並將隱私作為「預設」（by default）[125]。

然而，此一「從設計包含隱私，並將隱私作為預設」的概念仍然不夠清晰。對此，歐洲資料保護委員會亦尚未發布相關指引。英國資訊長辦公室所發布的 GDPR 指引中，雖然針對此一概念做出解釋，但也承認其無法提供一個顧及所有面向之全面性的指引；該指引提出幾個需要考慮的主要因子，並提出相關可能的示例，提供簡單的檢核表；不過此指引最後仍提醒控制者或處理者仍視情況可能需要另外諮詢專家，並提供加拿大安大略省資訊和資料保護長所提出的相關指引提供控制者及處理者參考[126]。以上都可看出，「從設計包含隱私」的概念仍然需要透過更多的指引及實務操作逐漸填充與發展，才能使具體內涵更加清晰。

(2) 保存期限之規定

GDPR 要求，個人資料之保存應「不長於處理目的所需之必要期間」[127]；並要求於直接蒐集時，將預計保存之時間（或決定保存

[124] Regulation (EU) 2016/79, art. 32, 2016 (L119), 1, 51-52.
[125] Regulation (EU) 2016/79, art. 25, 2016 (L119), 1, 48.
[126] Data protection by design and default, Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (last visited Aug. 7, 2018).
[127] Regulation (EU) 2016/79, art. 5, 2016 (L119), 1, 35-36.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

時間之方式）告知當事人；於間接蒐集時，則應於最晚一個月內或第一次利用（包含提供給其他人）或第一次與當事人聯絡時，通知當事人[128]。

同時，若資料對於其蒐集（或處理）之目的而言，已無保留之需要的話，當事人可以對控制者行使刪除權（被遺忘權），要求其刪除該個人資料[129]。

(3) 紀錄及證據保存之規定

根據 GDPR 的規定，資料之控制者與處理者應將處理活動進行記錄。

其中，控制者應保留下列資料：

A. 控制者（及其代表）、共同控制者（如有）、資料保護員（如有）之名稱、聯絡方式；

B. 處理目的；

C. 資料當事人類型之描述及個人資料類別之描述；

D. 資料揭露之對象類型；

E. 資料進行國際傳輸之對象，及國際傳輸之基礎（若採取適當保護措施時，其書面文件）；

F. 預設各類別個資之刪除期限（如可能）；

[128] Regulation (EU) 2016/79, art. 13-14, 2016 (L119), 1, 40-42.
[129] Regulation (EU) 2016/79, art. 17, 2016 (L119), 1, 43-44.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

G. 處理時所採取之安全措施概述[130]。

至於處理者。則須保留下列資料：

A. 處理者（及其代表）、資料保護員（如有）名稱、聯絡方式；

B. 所代表之控制者（及其代表）、其資料保護員（如有）之名稱、聯絡方式

C. 資料進行國際傳輸之對象，及國際傳輸之基礎（若採取適當保護措施時，其書面文件）；

D. 處理時所採取之安全措施概述[131]。

不過，若是控制者或處理者之員工人數不足 250 人，則僅須針對非偶然性的處理、可能對個人權利或自由造成風險的處理、對特種個資之處理等情形進行記錄[132]。

英國資訊長辦公室提供的指引中，例示了何種紀錄方式是符合 GDPR 的規定，哪些則是不符合規定的紀錄模式，並提供紀錄格式的模板，供控制者及處理者使用[133]。

(四)通訊傳播事業資料釋出之授權規範

1. 目的外利用規定

GDPR 原則上禁止與原始蒐集目的不同之處理，除非是：第一，基

[130] Regulation (EU) 2016/79, art. 30 2016 (L119), 1, 50-51.
[131] Regulation (EU) 2016/79, art. 30 2016 (L119), 1, 50-51.
[132] Regulation (EU) 2016/79, art. 30 2016 (L119), 1, 50-51.
[133] How do we document our processing activities?, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/ (last visited Aug. 2, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

於公共利益所為之建檔、為科學或歷史研究、或為統計目的而做之處理[134]；第二，經當事人同意；第三，基於歐盟法或會員國法規定，才可以做原始目的外之處理，否則就須經過此一新目的與原始目的的「相容性」（compatible），相容性應考量：第一，新目的與原先目的之「連結性」（link）；第二，蒐集個資之「脈絡」（context），尤其是資料主體與控制者之間之關係；第三，個資本身之「性質」（nature），尤其是是否屬於特種個資；第四，新目的處理之可能「後果」（consequences）；第五是否採取「適當安全保護措施」（appropriate safeguards）[135]。對此，英國資訊長辦公室提供之指引，特別以舉例的方式說明判斷之方法[136]。

2. 授權他人代為處理個資之規定

GDPR 要求，於授權他人代為處理個資的情形，控制者應確保其所委託的處理者能提供充足保證，其必定會採取適當、有組織的方法，以使處理行為符合 GDPR 規定，以保障當事人的權利[137]。

3. 共同決定資料處理[138]之規定

GDPR 規定，若兩個（或以上）控制者可以共同決定資料之處理的目的或方法時， 即為「共同控制者」（joint controllers）[139]。共同控制者應以透明方式安排彼此在 GDPR 下的義務，包含各自對資料主體的任務

[134] Regulation (EU) 2016/79, art.5 , 2016 (L119), 1, 35-36.
[135] Regulation (EU) 2016/79, art.6 , 2016 (L119), 1, 36-37.
[136] Principle (b): Purpose limitation, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (last visited Aug. 2, 2018).
[137] Regulation (EU) 2016/79, art. 28, 2016 (L119), 1, 49-50.
[138] 這種情形與「釋出」類似，是控制者間可以互相共享資料的一種形式。
[139] Regulation (EU) 2016/79, art. 26 2016 (L119), 1, 48.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

及關係，並應該將這些資訊的重點提供給資料主體[140]。

其中，所謂「共同決定資料之處理目的或方法」的解釋涵蓋範圍其實相當廣。以「歐盟法院」(Court of Justice of the European Union)在 2018 年 6 月的一個「先訴裁定」(preliminary ruling)為例，該院應德國聯邦行政法院之請求，針對 Facebook 粉絲專頁的管理員，是與 Facebook 構成共同控制者，從而須一起保護用戶個資等議題，做出裁定，認定 Facebook 粉絲專頁的管理員符合 1995 年個資保護指令「資料控制者」的定義，應被視為與 Facebook 公司負「共同責任」(jointly responsible)的資料控制者[141]。由於 1995 年個資保護指令並無「共同控制者」一詞，而 GDPR 對於資料控制者的定義，與 1995 年個資保護指令完全相同，因此論者認為：依照法院論理，在 GDPR 規範下，Facebook 粉絲專頁管理員與 Facebook 屬於共同控制者，應無疑問[142]。法院主要是認為：由於 Facebook 粉絲專頁管理者得以透過 Facebook 設定的定義參數，影響或促成 Facebook 處理使用者之個資的目的和方式；因此縱使其無法直接近用使用者的個人資料，仍會因為其可以決定個資處理的目的與方式，而該當「控制者」的定義[143]。此一案件起因是 2011 年時德國個資監管機構以其未通知 Facebook 粉絲專頁上互動的使用者個資之蒐集處理行為為

---

[140] *Id.*

[141] Court of Justice of the European Union, The administrator of a fan page on Facebook is jointly responsible with Facebook for the processing of data of visitors to the page, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081en.pdf (last visited Jan. 17, 2019).

[142] *E.g.*, Joe Jay de Haas, *ECJ: Facebook fan page administrator is a joint data controller*, Stibbe (Aug. 23, 2018), https://www.stibbe.com/en/news/2018/august/ecj-facebook-fan-page-administrator-is-a-joint-data-controller (last visited Jan. 19, 2019); Facebook fan page administrators are joint controller together with Facebook, Cranium, https://www.cranium.eu/facebook-fan-page-joint-controller/ (last visited Jan. 17, 2019); *and* Robin Hopkins, *The 'Facebook Fan Page' judgment: joint data controllers, cookies and targeted advertising*, Panopticon (Jun. 5, 2018), https://panopticonblog.com/2018/06/05/the-facebook-fan-page-judgment-joint-data-controllers-cookies-and-targeted-advertising/ (last visited Jan. 17, 2019).

[143] *supra* note 141.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

由，要求德國一家從事教育的公司「Wirtschaftsakademie Schleswig-Holstein」停用其 Facebook 粉絲專頁，該公司不服該處分而向德國行政法院起訴，行政法院聲請歐盟法院針對 1995 年個資保護指令內容進行解釋所致，歐盟法院做出先訴裁判後，將交由德國行政法院繼續審理[144]。

此一判決出來後，論者認為這個裁定雖然將會廣泛影響數位雲端運算、金融科技等各種網路生態的法律架構，但其實對於 Facebook 粉絲專頁使用者來說，也是一種機會，因為「共同控制者」並不是要求兩個或多個控制者間負擔「相同」的責任，而是依據其利用資料的模式，決定負責的程度[145]。對此，論者建議 Facebook 粉絲專頁管理員應盡可能告知使用者自己會基於什麼樣的目的調整 Facebook 提供的設定選項，並進行充分的告知；而 Facebook 則應該調整其管理界面，通知粉絲專頁管理員相關操作選項，協助管理員完善資料保護措施[146]。

4. 去識別化規定

GDPR 前言第 26 點規定，去識別指的是考慮到合理使用之方法以及所有客觀因素（包含識別所需之成本、時間及技術等），包含控管者自己在內，已經無法識別特定個人的資料；若為去識別化資料，則就不屬於個人資料，而無須特別為授權規定[147]。

針對如何認定去識別，英國資訊長辦公室特別發布「去識別化：資

[144] *id.*
[145] Romain Perray and Guillaume Béal, *Joint Controllers: Constraint or Opportunity?*, Lexology (Dec. 26, 2018), https://www.lexology.com/library/detail.aspx?g=33988f50-e506-4216-ae48-2765bb621ff4 (last visited Jan. 17, 2019).
[146] Cranium, *supra* note 142.
[147] Regulation (EU) 2016/79, rec. 26, 2016 (L119), 1, 5.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

料保護風險管理應用準則」（Anonymisation: Managing Data Protection Risk Code of Practice[148]，以下簡稱「去識別化應用準則」）說明去識別化之標準。須特別值得注意的是，去識別化應用準則中特別說明，此一準則之目的在於「促進良好實踐」（promote good practice），其內容可能較法令之規定更為嚴格，因此此一準則並非強制性規定，亦沒有法律效力[149]。

根據去識別化應用準則的規定，「去識別化資料」係指資料本身無法識別任何個人，同時即便透過與其他資料的組合（combination），亦無可能識別任何個人[150]。英國資訊長認為，此種資料不再被認為是英國資料保護法中的個人資料[151]。但所謂「無可能識別任何個人」，並不是指完全的「沒有風險」（risk free），而是將資料識別之風險「減低」（mitigate）至其風險變得「極其微小」（remote）即可。

對於去識別化資料，英國資訊長認為，此類資料之釋出原則上便不需要取得當事人之同意；同時其也建議，即便是在取得當事人同意的情形下，若能提供去識別化資料，也是較佳的實踐作法[152]。

值得特別注意的是，前述的準則係依據英國 1998 年之個資法規定所提出，該版個資法已被 2018 年所通過之新版個資法所取代。然而，由於英國個資法之變動主要是因為歐盟個資法令變動而來，而無論是歐盟原

[148] Information Commissioner's Office, Anonymisation: Managing Data Protection Risk Code of Practice (2012), https://ico.org.uk/media/1061/anonymisation-code.pdf（last visited Oct. 26, 2018).
[149] *Id.*, at 10.
[150] Id. at 6.
[151] Information Commissioner's Office, Big Data and Data Protection (2014), at 5, https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf (last visited Jul. 30, 2018).
[152] *Supra* note 148, at 28-29.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

先的個資保護指令[153]，或是現在的 GDPR，對於去識別之規定其實並沒有改變，因此此一準則雖尚未於英國個資法修法後修正，但應該仍具有參考價值。

5. 通知規定

除了於釋出時有授權之相關規定外，GDPR 進一步將釋出者之責任延伸到當事人權利行使的時候。根據 GDPR 的規定，如果當事人行使資料更正權、刪除權（被遺忘權）以及限制處理權時，釋出者除非可以證明無法進行通知或通知所需耗費過鉅外，應將當事人之要求通知接收者[154]。而若是將資料「公開」（made the personal data public），則當當事人行使刪除權（含被遺忘權）時，控制者應考量現有科技及執行成本，採取合理步驟，通知正在處理該資料者當事人已經行使刪除權，進一步將通知義務擴大[155]。

6. 資料可攜權

比較特別的是 GDPR 課予資料控管者一個「釋出的義務」。資料當事人有權請求控管者以結構化、通常使用且機器可讀的格式，將其基於同意或契約關係所提供之資料，以及依據自動化方式處理之資料提供給資料當事人或其指定之其他資料控制者[156]。這個規定課予業者將其所掌有的特定資料提供給其他控制者的義務。

英國資料長辦公室針對資料可攜權所提供的指引包含了檢核表，並提供案例協助釐清可攜權的內涵爭議，並參考開放資料手冊以及歐盟公

[153] Directive 95/46/EC, rec. 26, 1995 O.J. (L 281) 31,33.
[154] Regulation (EU) 2016/79, art. 19, 2016 (L119), 1, 45.
[155] Regulation (EU) 2016/79, art. 17, 2016 (L119), 1, 43-44.
[156] Regulation (EU) 2016/79, art. 20, 2016 (L119), 1, 45.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

部門資料在利用指令等資料，定義「結構化」以及「機器可讀」的內涵，並表示可以使用 csv、sml 和 json 等開放格式來提供個人資料[157]。

(五)隱私蒐集評估機制

針對使用新科技處理個人資料，該處理之本質、範圍、使用情形及目的可能會導致當事人權利、自由高度風險的情形；特別是對自然人系統性、大規模的以自動處理技術（包含側寫）進行個人特質評估，並將基於該評估作成對當事人有法律效果或其他重大影響之決定；或是大規模處理特種個人資料；或是大規模系統性監控公共區域等情形，GDPR 要求應於處理前進行「資料保護影響評估」（Data Protection Impact Assessment），並授權各國主管機關可以另外規定哪些情形須進行資料保護影響評估，並明定哪些情形得不進行該評估[158]。根據 GDPR 規定，此一評估須包含：第一，處理之目的；第二，處理之必要性及比例性；第三，對資料當事人權利及自由之評估；第四，應對風險之方法（包含保護措施等）；同時，並要求於事發當時應徵詢當事人或其代表人之意見，並在風險發生變化時，應重新進行資料保護影響評估[159]。而若評估發現在未採取降低風險措施前，該處理將有高度風險時，控管者應於處理前徵詢主管機關[160]。

第 29 條工作小組有針對資料保護影響評估發布指引[161]，歐洲資料保

[157] Right to data portability, Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (last visited Aug. 2, 2018).
[158] Regulation (EU) 2016/79, art.35 , 2016 (L119), 1, 53-54.
[159] Regulation (EU) 2016/79, art.35 , 2016 (L119), 1, 53-54.
[160] Regulation (EU) 2016/79, art.36 , 2016 (L119), 1, 54-55.
[161] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

護委員會亦繼續承認該指引[162]。英國資訊長辦公室提供的指引則進一步將資料保護影響評估機制分為九個步驟，包含：第一，確認是否需要實施資料保護影響評估；第二，描述所涉及的處理行為；第三，考慮進行諮詢；第四，評估處理之必要性與比例性；第五，辨別其中之風險並加以評估；第六，確認應採取的減輕風險措施；第七，簽核評估結果並存檔；第八，將評估結果落實進處理計畫；第九，持續複查隱私衝擊影響評估；英國資訊長辦公室並針對各個步驟操作時應注意之事項做更細部的規定，同時亦提供評估的模板供業者使用[163]。

(六)小結

英國對於通訊傳播事業個人資料之管理，並未將其與其他產業之個人資料做不同程度之管理，而是依據英國個資法及 GDPR 所建構的同一套規定加以管理。不過在資料類別上，除了與我國相同有「特種資料」之類別外，也對兒童資料之取得有特別之規定。

在政策與策略上，英國在歐盟之架構下，主要是依據歐盟之 GDPR 以及其個資法為主要之管理依據。此外，英國個資主管機關——英國資訊長辦公室則針對個資管理的細節規範上，發布不具法律拘束力的指引，以檢核表、例示說明等方式，協助業者了解法律之規範。

在個別類別之管理上，英國依循 GDPR 之規定，對於當事人之「同意」設有嚴格之規定；同時要求業者在保存時應考慮風險，採取降低風險之措施，並有組織面上的要求；在授權規範上，對於授權等位於原先

[162] *Supra* note 105.
[163] How do we carry out a DPIA? , Information Commissioner's Office (UK), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/ （last visited Aug. 2, 2018）.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

目的外之處理行為，要求其除非取得當事人之同意，或基於契約之關係，否則應與原先之特定目的具備相容性；在隱私蒐集評估機制上，則是比較國家中唯一有強制要求業者在符合特定要件時，應於處理前進行隱私衝擊影響評估的國家。

此外，特別值得一提的是，英國在 GDPR 規範架構下對於自動處理技術（包含側寫）採取了相對更為嚴格之規範。除了要求處理前進行資料保護影響評估以外，其更規定除非是基於契約所必須、法律規定或當事人的明確同意，否則當事人上有權拒絕單純採用自動處理技術處理，對其造成法律效果或其他類似重大影響之個人資料處理的結果；而包含上述的例外在內，資料之控制者仍應對當事人提供部份參與、意見表達及挑戰該技術產生之決策等權利[164]。即便 GDPR 授權各會員國可因為國家安全、國防、公共安全等理由[165]或是基於公共利益所為之「建檔」（archiving）、科學或歷史研究目的、統計目的等原因[166]，放寬 GDPR 中特定條款之規定，英國在 2018 年資料保護法亦未放寬前述當事人之拒絕權及資料保護影響評估之義務規定[167]，可謂相當嚴格。

五、結論

本研究以下將首先就日、美、英三國法制背景進行綜合比較。接續將就我國個資法與日、英、歐盟及美國法規間相同和相異之處以本研究架構中個資之蒐集、保存、釋出、隱私衝擊影響評估等四個面向分別進行，並嘗試提出法制政策之建議。期中，因美國之個資相關規定分散於各不同領域之法律，並無統一之聯邦法，因此美國法比較部份，將僅摘

[164] Regulation (EU) 2016/79, art. 22 , 2016 (L119), 1, 46.
[165] Regulation (EU) 2016/79, art. 23 , 2016 (L119), 1, 46-47.
[166] Regulation (EU) 2016/79, art. 89 , 2016 (L119), 1, 84-85.
[167] *Supra* note 88 at 27-35.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

述有類似規定之處。

(一)法制背景綜合比較

綜合上述觀察結果發現：在制度與程序上，美國與日本都將通訊傳播業者持有之個人資料設有與一般個人資料有異之管理規範；而英國則一視同仁的對待。在政策與策略上，除了具法律拘束力的規範外，日本跟英國都以不具形式上法律拘束力的「指引」的模式，協助業者釐清法律的規範，並提供法律遵循方式的建議。其中，英國尤其在指引中，廣泛利用檢核表、例示說明等方式，協助業者更「情境化」的了解架構的內容，值得加以學習。綜上，觀察日、美、英三國規範，除美國無統一之個人資料保護法外，日本及英國皆以該國之個人資料保護法為主要之規範，僅在法律授權的規範內，才可能有對細節規範有不同之調整。我國之法律規範架構與日本及英國相似，應可參酌其規範之模式。主管機關可在現行個人資料保護法之授權範圍內，以法規命令或行政指導之模式，提供業者更詳細之說明即可。在實質內容上，我們也可以觀察到，上述三國並未因為新興技術的發展，而在通訊傳播領域放寬當事人同意之規範要求，甚至英國在 GDPR 的規範下，對於自動處理技術（包含側寫）等新興科技給予了更多的規範要求。資料當事人對其個人資料之同意及控制之權限，就本研究觀察所及，並無在通訊傳播領域中有放寬之跡象。

若從立法脈絡進行觀察，我們則可以看到各國在受到科技進步的影響，而有修正其個人資料保護規範的趨勢。我們可以明顯從日本及英國看到這樣的影響。英國對於個人資料保護立法背景受 1995 年 10 月所通過的歐盟「資料保護指令」影響，身為歐盟會員國之一的英國，其國內

本報告之智慧財產權歸屬於財團法人資訊工業策進會

的個人資料保護規定必須落實並符合歐盟對於個人資料保護所訂的相關規定，因而，英國當時為因應歐盟資料保護指令的施行，於 1998 年通過英國「1998 年資料保護法」，取代原先所制定的「1984 年資料保護法」。而後歐盟因為數位時代科技的進步，個人資料蒐集的質與量、處理的程度都數倍於制定資料保護指令的時代背景，而因此在 2016 年時圍成 GDPR 的制定工作。英國乃配合 GDPR 的施行，透過制定 2018 年資料保護法的方式，使其在英國國內發生效力。根據該法的規範架構，以及英國個資主管機關的說法，這樣的架構即使英國未來退出歐盟亦不會改變。

而日本的制度背景與個資監理機關的發展與我國較為類似，在過去日本與我國一樣，並未設有個資保護之專責機關。在其 2015 年個資法修法，設立單一個資主管機關後，仍特別以授權給總務省制定通訊傳播領域指引的方式，給予通傳領域個資不同之管理指導。而是次修法，日本特別針對巨量時代的來臨，為了因應資料加值與創新應用等技術科技對個資使用的需求，而在未放寬其他個人資料保護條件的狀況下，於日本個資法中新增了「匿名處理資料」等的相關規定。

美國本來就沒有統一的個人資料保護法，不同部門間有不同之管理密度。現行美國在通訊傳播領域相關部份所為之立法，最早可追溯至 1934 年，最晚則也是上個世紀的 1988 年完成制定，而且此一法律係回應網路發展對於兒童所帶來之影響，並未對因網路時代來臨所產生的各種個資議題做全面性的回應。我們可以這樣推論，當前美國在通訊傳播領域的法律架構，並未全面、直接的因應網路及巨量資料等技術帶來的影響，最多就是在法律架構的範圍內，在行政機關可行的範圍內，以相

本報告之智慧財產權歸屬於財團法人資訊工業策進會

當於我國行政規則或法規命令層級的方法加以因應。不過值得注意的是，近年來美國似乎有受到科技進步的壓力，而有進一步在法制上回應科技發展的趨勢。舉例而言，美國加州近來通過加州消費者隱私保護法，號稱是美國史上最嚴格的州層級隱私規範，其內容已有向歐盟 GDPR 靠攏的趨勢[168]。而與此同時，在聯邦法層級，也可以觀察到有國會議員試圖提出全面性個人資料保護設專法的嘗試。凡此種種似可理解為，美國亦已因為科技進步帶來對個人個資保護及隱私保障之衝擊，而有從法制上進一步完善相關規範的趨勢。

由上述的整理可以發現，日本與英國皆在科技進步的脈絡下，修正其個資保護規範。其中英國在 GDPR 的規範中，增加了不少保護數位時代個資的規範；日本也在未放鬆主要個資保護架構的情況下，透過匿名處理資料制度等的引入，來回應技術的需求。即便如採取分散式管理架構的美國，在州層級及聯邦層級，也都出現了因應科技發展而出現的個資保護立法或立法草案。依照本研究所得之觀察，至少可以認為個人資料法制確實可能存在因技術發展而調整之需求。

(二)取得各種資料類別之行為規範

1. 一般個人資料

歐盟 GDPR 之一般個人資料，包含姓名、識別號碼、位置資料、線上識別碼或經由其他一項或多項經濟、文化或社會身分特徵等，直接或間接識別的自然人。根據 GDPR 第 6 條的規定，對於一般個人資料，合法之處理應符合下列六個條件之一：(1)當事人同意；(2)履行契約關係所

[168] 蕭永蔚，〈美國加州於 6 月 28 日通過新版個資隱私法規〉，資策會科際法律研究所，2018/09，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=156&d=8106 （最後瀏覽日：2019/01/10）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

必須（包含契約締結前，因當事人要求所採取之步驟）；(3)為遵守法定義務所必須：(4)為保護當事人或其他人的「重大利益」（vital interest）所必須；(5)為符合公共利益執行職務或受委託行使公權力所必須；(6)資料控制者為追求自己或第三人之「合法利益」（legitimate interests）所必須，且資料當事人之利益、基本權與自由並未優先於該合法利益（但公務機關執行職務時，不得以此主張）。

日本個資法將一般個人資料之定義為「個人識別符號」，規定於第 2 條第 1 項第 2 款，即是將由個人身體特徵所轉換成得以識別個人的資訊，明確定義為受個資法保障的個人資料。包含指紋資料、臉部辨識資料、護照號碼、證書執照號碼、電話號碼以及個人編號都被明確納入規範。而該法第 3 條規定，處理個人資料時，須謹慎使用在尊重個人之人格原則下慎重處理，且按照正確方法處理。

我國個資法將一般個人資料規定於第 2 條，包含自然人之姓名、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、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。

而我國個資法規定對於一般個人資料之蒐集、處理、利用應有特定目的，並區分為公務機關與非公務機關，符合特定情形之一者。意即對於公務機關之蒐集或處理要求，規定於第 15 條：(1)執行法定職務必要範圍內。(2)經當事人同意。(3)對當事人權益無侵害。對於非公務機關之蒐集或處理要求，則參見第 19 條：(1)法律明文規定。(2)與當事人有契約或類似契約之關係，且已採取適當之安全措施。(3)當事人自行公開或其他已合法公開之個人資料。(4) 學術研究機構基於公共利益為統計或

本報告之智慧財產權歸屬於財團法人資訊工業策進會

學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。(5)經當事人同意。(6)為增進公共利益所必要。(7)個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。(8)對當事人權益無侵害。

又，公務機關及非公務機關對於個資之利用，分別規定於第 16 條、20 條，應於必要範圍內為之，並與蒐集之特定目的相符；但有例外 7 款情形之一者，得為特定目的外之利用：(1)法律明文規定。(2)為增進公共利益所必要。(3)為免除當事人之生命、身體、自由或財產上之危險。(4)為防止他人權益之重大危害。(5) 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經蒐集者依其揭露方式無從識別特定之當事人。(6)經當事人同意。(7)有利於當事人權益。

從而，觀察 GDPR、英國、日本以及我國個資法規定，對於一般個人資料之蒐集、處理、利用之相同處在於，提及需經當事人同意、尊重該個人或有利於當事人，對其權益無侵害等。茲綜合比較如下表所示。

表 1 各國一般個資規範比較表

	一般個資範圍	一般個資之蒐集、處理或利用
歐盟	姓名、識別號碼、位置資料、線上識別碼或經由其他一項或多項經濟、文化或社會身分特	合法之處理應符合下列六個條件之一：(1)當事人同意；(2)履行契約關係所必須（包

本報告之智慧財產權歸屬於財團法人資訊工業策進會

	徵等，直接或間接識別的自然人。	含契約締結前，因當事人要求所採取之步驟)；(3)為遵守法定義務所必須：(4)為保護當事人或其他人的「重大利益」（vital interest）所必須；(5)為符合公共利益執行職務或受委託行使公權力所必須；(6)資料控制者為追求自己或第三人之「合法利益」（legitimate interests）所必須，且資料當事人之利益、基本權與自由並未優先於該合法利益（但公務機關執行職務時，不得以此主張)。
日本	指紋資料、臉部辨識資料、護照號碼、證書執照號碼、電話號碼以及個人編號等，由個人身體特徵所轉換成得以識別個人的資訊。	處理個人資料時，須謹慎使用在尊重個人之人格原則下慎重處理，且按照正確方法處理。
我國	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、	● 公務機關之蒐集、處理應有特定目的，並符合特定情形之一者：(1)執行法

本報告之智慧財產權歸屬於財團法人資訊工業策進會

	教育、職業、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。	定職務必要範圍內。(2)經當事人同意。(3)對當事人權益無侵害。 ● 非公務機關之蒐集、處理應有特定目的，並符合特定情形之一者：(1)法律明文規定。(2)與當事人有契約或類似契約之關係，且已採取適當之安全措施。(3)當事人自行公開或其他已合法公開之個人資料。(4) 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經蒐集者依其揭露方式無從識別特定之當事人。(5)經當事人同意。(6)為增進公共利益所必要。(7)個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得

本報告之智慧財產權歸屬於財團法人資訊工業策進會

		保護之重大利益者，不在此限。(8)對當事人權益無侵害。 ● 公務機關及非公務機關對於個資之利用，應於必要範圍內為之，並與蒐集之特定目的相符；但有例外 7 款情形之一者，得為特定目的外之利用：(1)法律明文規定。(2)為增進公共利益所必要。(3)為免除當事人之生命、身體、自由或財產上之危險。(4)為防止他人權益之重大危害。(5) 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經蒐集者依其揭露方式無從識別特定之當事人。(6)經當事人同意。(7)有利於當事人權益。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

資料來源：本研究自行整理

2. 特種個資

歐盟 GDPR 第 9 條將種族、人種、政治意見、宗教或哲學信仰、工會會員身份、基因、用於識別個人之生物識別資料、健康、性生活或性傾向之個人資料列為特種個人資料，同時歐盟對於前科資料亦有更為嚴格之規定。原則上禁止處理特種個資；但有特定例外情形，得以處理。

日本個資法將特種個資定義為「敏感性個人資料」，規定於第 2 條第 3 項，對於那些會造成本人受到歧視待遇的人種、信仰、社會身分、病歷、犯罪經歷或是因犯罪而受有損害的事實、及其他對當事人造成不當的差別、偏見或其他不利益而必須特別就該資料之處理加以考量、且經政令規定之描述等個人資料，除法律規定、保護他人生命財產而難以取得同意、維護兒童健全身心發展、或公務機關依法遂行職務而難以取得同意等情況外，應取得本人同意（第 17 條第 2 項）[169]，且禁止以事後退出的模式取代事前同意，而向第三人提供資料（第 23 條第 2 項）[170]。又，

[169] 個人情報の保護に関する法律改正法，第十七条第２項， 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。
一 法令に基づく場合。
二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
五 当該要配慮個人情報が、本人、国の機関、地方公共団体、第 76 条第１項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合。

[170] 個人情報の保護に関する法律改正法，第二十三条第二項 ， 個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじ

本報告之智慧財產權歸屬於財團法人資訊工業策進會

個資法第 17 條規範了「適當取得之義務」，蒐集特種個資的業者不得以欺騙或其他不正當手段取得該類個人資料。

此外，日本尚有特別就通訊傳播事業，電信和廣播領域如何取得個資訂有相關規定，以行政指導之方式，規範電信、廣播事業者對當事人之個資保護。其電信事業對敏感性特種資料的蒐集，規定於電信 GL 第 7 條第 2 項，原則上需經該當事人同意；僅在下列例外情形，得蒐集：(1)依法令、(2)為保護本人生命、身體或財產的情形，取得本人同意有所困難時、(3)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時、(4) 協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，基於取得本人同意有可能對執行該事務造成阻礙的之虞時、(5)經由本人、國家機關、地方公共團體、個資法第 76 條第 1 項各款所揭示者、外國政府、外國的政府機關、外國的地方公共團體、國際機構、或在國外相當於個資法第 76 條第 1 項各款所揭示者公開該敏感之個資的情形時、(6)透過目視或拍攝到本人，取得其本人外形上明顯敏感之個人資料(7)於第 15 條第 10 項各款所揭示之情形，接收敏感性之個人資料的提供等。另，廣播事業則規定於廣播 GL 第 7 條第 4 項，原則上需經當事人同意；例外僅在依法令、為保護本人生命、身體或財產、公共利益或維護兒童身心健全發展而取得當事人同意有困難等情形，始得蒐集。

從而，比較日本及我國個資法(規定於第 6 條)位階，對於特種個資

め、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一 第三者への提供を利用目的とすること。

二 第三者に提供される個人データの項目

三 第三者への提供の方法

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

五 本人の求めを受け付ける方法

本報告之智慧財產權歸屬於財團法人資訊工業策進會

之蒐集、處理前提，相同處在於嚴格規定原則上皆需經當事人事前同意，始可為之。而按 GDPR 規定，原則上禁止處理特種個資。但有特定例外情形，則不在此限，而例外情形略有不同，茲整理如下表。

表 2 各國特種個資規範比較表

	特種個資範圍	特種個資之蒐集或處理
歐盟	種族、人種、政治意見、宗教或哲學信仰、工會會員身份、基因、用於識別個人之生物識別資料、健康、性生活或性傾向之個人資料。前科資料亦有更為嚴格之規定。	● 原則：禁止處理。 ● 例外：(1)得當事人「明確」（explicit）同意。(2)履行契約。(3)未保護資料當事人或他重大利益所必須，且當事人在物理上或法律上無法給予同意。(4)當事人已經明確自行公開。(5)建構、行使、防禦法律上之請求或法院執行司法權所必要。(6)基於歐盟法或會員國法所規定、合比例性之重大公益所必要。(7)公共衛生、醫學、非營利組織基於特定目的所必要。(8)基於歐盟法或會

本報告之智慧財產權歸屬於財團法人資訊工業策進會

		員國法，為公共利益「建檔」（archive）、為科學或歷史研究、統計等目的且提供適當保護措施並經比例性檢驗。
日本	人種、信仰、社會身分、病歷、犯罪經歷或是因犯罪而受有損害的事實、及其他對當事人造成不當的差別、偏見或其他不利益而必須特別就該資料之處理加以考量、且經政令規定之描述等個人資料。	● 原則：需經當事人事前同意。 ● 例外：(1)法律規定。(2)保護他人生命財產而難以取得同意。(3)維護兒童健全身心發展。(4)或公務機關依法遂行職務而難以取得同意。
我國	病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。	● 原則：需經當事人事前同意。 ● 例外：(1)法律明文規定。(2)公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。(3)當事人自行公開或其他已合

本報告之智慧財產權歸屬於財團法人資訊工業策進會

		法公開之個人資料。(4)公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。(5)為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。(6)經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

資料來源：本研究自行整理

3. 針對兒少之個資保護規範比較

本報告之智慧財產權歸屬於財團法人資訊工業策進會

以下針對兒少個資的蒐集、保存、釋出予第三人之規範，進行綜合論述。就兒少之個資保護而言，美國跟英國皆對此有特殊規定，日本則與我國較為近似，以個人資料保護法為規範基礎，並未針對兒少另立專法。年齡部份，美國係規定透過網路線上蒐集未滿 13 歲兒童個資的行為，網站營運商須踐行通知程序或取得父母或監護人事前、事後同意。GDPR 第 8 條規定則要求，在對低於 16 歲的兒童提供資訊社會服務時，需其法定代理人同意或授權，處理才合法，此一年齡授權會員國可調降。從而，英國 2018 年資料保護法將其年齡規定降為 13 歲，意即 13 歲以下兒童須經法定代理人同意或授權。惟，直接向兒童提供預防性（preventive）或諮詢性（counselling）之服務時，例外無須得其父母或監護人之同意。

又，美國之兒童線上隱私保護法尚規範業者須對用戶資料的保存採取適當安全維護措施。就資料蒐集、記錄保存的部份，網站或線上服務的營運商，在合理必要的時間內，可保留線上所蒐集的個人資料，但後續營運商須採取適當合理的措施刪除此類資料，以防止未經授權近用或使用與刪除相關的資料。

另，若欲將兒少之個資釋出予第三人，美國之兒童線上隱私保護法要求該網站營運商或線上服務在進一步之資料蒐集、使用或傳遞（dissemination）時，需經過授權，才可為之。

反觀我國，對於兒少個資的蒐集、保存、釋出予第三人係以個人資料保護法統一規範，並未加以細分，建議未來若欲規範業者透過網路蒐集兒童相關個資或向兒童提供資訊社會服務時，除踐行通知程序或取得父母或監護人事前抑或事後同意外，並訂定適當年齡之界線，或許可參

本報告之智慧財產權歸屬於財團法人資訊工業策進會

考民法之行為能力相關規定訂之。在推動個資相關法令之修改之前，短期內或許可以依據《兒童及少年福利與權益保障法》第 46 條第 1 項的規定，召集各目的事業主管機關、委託民間團體成立內容防護機構，推動網際網路平臺提供者就兒童、少年個資之蒐集年齡、取得父母或監護人同意之標準等，先行建立自律機制。透過由業者自律、民間團體及相關政府機關參與的多元協作模式，探索出實際符合我國國情之年齡規範及技術方法。以符合具有我國內國法效力之《聯合國兒童權利公約》第 16 條對於兒童隱私權保障之意旨。

(三)個人資料保存機制

1. 適當安全維護措施

美國之「有線電視隱私法」，規範系統業者必須向用戶提供必要措施的保護免於他人非法存取、並且給予訂戶合理機會以更正相關資料，且當原蒐集目的消失後銷毀相關資料。

而美國 1996 年電信法的部分，聯邦通訊委員會所發布之「用戶專屬資訊」規則（47 CFR § 64）當中，要求(1)電信事業應實施一系統，透過該系統用以確認已取得用戶同意。(2)以及電信事業應培訓其員工判斷是否取得相關授權，並建立明確的訓練處分流程。(3)又，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於銷售與行銷活動之檔案紀錄。亦須保存揭露、提供予第三人或第三人被允許得接觸之所有情形的相關紀錄。(4)同時，電信事業須建立監督審查程序，以確保行銷員工對其用戶從事外部行銷時，合乎相關安全維護規範。(5)電信事業須採取合理措施，以發現和防止未經授權而意圖取得資料之行為。當用戶方主動

本報告之智慧財產權歸屬於財團法人資訊工業策進會

向電信營運商之電話聯繫、網路帳戶接觸或造訪店內，而在揭露該資料之前，電信事業應適當地查核、驗證用戶的身分。

GDPR 針對個人資料之保存，在組織面以及程序面，有不同的規定。組織面而言，要求若資料的控制者或處理者涉及系統性的大規模監控資料當事人，或涉及大規模處理特種個資的話，該控制者應指定「資料保護員」。英國資訊長辦公室的指引則進一步提供了檢核表、問卷以及示例，協助組織確認是否須指定資料保護員，以及該如何設計資料保護員之職位與權限。程序面而言，GDPR 要求一個「全資料生命週期」的隱私保護，規定控制者應採用科技化、有組織的措施保障資料安全，及定期審視與更新相關的適當資料保護措施。並要求於處理時應確保系統與服務的機密性、完整性、可用性以及彈性，盡可能實施假名化或加密等措施，應視現有技術、執行成本以及處理的脈絡、範圍、本質、目的以及可能的風險等，採取各項適當之安全保護措施。

日本保存機制而言，依日本個資法第 20 條、電信 GL 第 11 條、廣播 GL 第 11 條，分別皆要求電信營運商、廣播資訊處理業者需建構必要且適當的個資安全管理措施，以防止其所蒐集到的個資外洩、丟失或毀損之情事發生。尤其在關於施行安全管理措施的具體方法，須考慮到個人資訊外洩時，當事人所受到權利利益侵害程度，以及事業的規模及性質、個人資料的處理狀況（包含存取個人資料的性質與量）等因素，進而評估所會造成之風險，再做出必要且適切的處理。而廣播 GL 第 14 條亦要求廣播業主在播送節目用來存放個資的記憶裝置機器，與之連接通信網路設備時，需建置必要措施。再者，電信 GL 第 13 條、廣播 GL 第 13 條，要求業者需設置「個資保護管理者」（負責該業者的個資存取相

本報告之智慧財產權歸屬於財團法人資訊工業策進會

關責任者)，遵循本指引制定內部規程、監察機制以及監督業者的個資存取等事宜。

我國個資法將安全維護措施，按公務機關與非公務機關分別規定於第 18 條、27 條。意即，公務機關/非公務機關保有個人資料檔案者，應指定專人辦理安全維護事項/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。又，針對非公務機關，中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。該計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。而個資法施行細則第 12 條第 2 項，尚提及適當之安全維護措施，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：(1)配置管理之人員及相當資源。(2)界定個人資料之範圍。(3)個人資料之風險評估及管理機制。(4)事故之預防、通報及應變機制。(5)個人資料蒐集、處理及利用之內部管理程序。(6)資料安全管理及人員管理。(7)認知宣導及教育訓練。(8)設備安全管理。(9)資料安全稽核機制。(10)使用紀錄、軌跡資料及證據保存。(11)個人資料安全維護之整體持續改善。再者，國家通訊傳播委員會尚有依據個資法第 27 條第 3 項，訂定「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法[171]」，使通訊傳播事業安全維護的管理更為具體。本辦法之適用範圍，包括依電信法、廣播電視法、有線廣播電視法或衛星廣播電視法取得許可或執照之非公務機關。其中，第 3 條特別規定，非公務機關蒐集、處理及利用達 5000 名用戶之個人資料者，其訂定之計畫及處理方法內容應包含國內(如：TPIPAS)或國際(如：P-Mark、

[171] 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法，https://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=502&law_sn=2575&sn_f=2575&is_history=0。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

ePrivacy-Mark、BS 等)個人資料安全稽核機制之規劃及執行計畫。此外，尚要求非公務機關應具體訂定應變、通報及改善機制，以及個資管理程序之事項和內容等。

從而，觀察上開各國對於安全維護措施之規定，歐盟、英國及日本，有要求控制者應指定「資料保護員」或業者需設置「個資保護管理者」，此類相關角色，其用意應在於為了防止資訊處理業者內部或外部的不正當行為，導致個資外洩等，使監督責任區分更加明確化。反觀我國目前之安全維護規範，並未強制要求設置此類似之保護監督管理者角色，與美國之規範較為類似，係要求業者向用戶提供必要措施的保護，例如資訊安全系統的維護、存取修改之相關歷程記錄、監督管理和驗證身分等方式。就組織上，我國僅要求應設置適當人員管理，對該人員之職權、應負責事項等，缺乏較明確之規定。然而，考量到通訊傳播事業掌管資料量相當龐大，建議可以參考日本及英國的規定，在國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法中，要求相關業者配置之管理人員人員應具有一定程度之獨立監督之職權，並應賦予其確保組織內部個資管理順暢之功能。

2. 保存期限之規定

美國 1996 年電信法的部分，按聯邦通訊委員會所發布之「用戶專屬資訊規則」(47 CFR § 64)，電信事業應保存將「用戶專屬資訊」揭露、提供予第三人或第三人被允許得接觸用戶專屬資訊之所有情形之檔案至少一年。

日本在電信業者個人資訊保存期間方面，依據電信 GL 規定，電信

本報告之智慧財產權歸屬於財團法人資訊工業策進會

業者處理個人資訊時，應以達成利用目的之必要範圍內訂定保存期間為原則。該保存期間屆滿後或該使用目的已達成後，應立即刪除該個人資訊。但仍有資訊保存期間之例外情形，包含：(1) 基於法令規定應予保存者；(2) 經本人同意者；(3) 電信事業者為遂行業務之必要限度內，認為有保存個人資訊之需要，有相當理由不予刪除者；(4) 有特別理由不予刪除者。換言之，電信事業者若認為有符合上述四種情形之一，即可於保存期間經過後或使用目的達成後，仍保存該個人資料不予刪除。同時，尚特別規定，除非經用戶同意或有其他阻卻違法事由，否則電信業者不得儲存與通信秘密有關之個人資料，但即使被允許保存，也必須在達到使用目的後立即刪除該個人資料。

另，日本在廣播業者個人資訊保存期間方面，按廣播 GL 第 10 條第 1 項：「廣播資訊處理業者在存取閱聽者等之個人資訊時，應訂立使用目的範圍及保存期間，該保存時間屆滿後、或為達成使用目的而合理保留該個資的理由已不復存在時、或使用目的未達成，而事業中止等情況發生時，須盡速將該個人資料刪除。」以及同條第 2 項規定，廣播資訊處理業者在取得閱聽者等的個資時，除事先公告其保存期間外，須盡速通知當事人或公告其保存期間。

GDPR 要求，個人資料之保存應「不長於處理目的所需之必要期間」；並要求於直接蒐集時，將預計保存之時間（或決定保存時間之方式）告知當事人；於間接蒐集時，則應於最晚一個月內或第一次利用（包含提供給其他人）或第一次與當事人聯絡時，通知當事人。同時，若資料對於其蒐集（或處理）之目的而言，已無保留之需要的話，當事人可以對控制者行使刪除權（被遺忘權），要求其刪除該個人資料。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

我國個資法對於保存期限規範可參見第 11 條，當個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。此外，國家通訊傳播委員會針對電信事業，定有《電信事業處理有關機關查詢電信通信紀錄實施辦法》及《第二類電信事業管理規則》，對相關資料之保存期限，有明確之規定。

綜合上述規範，日本及我國之個資規範原則上當保存期間屆滿後或該使用目的達成後，應刪除該個人資訊；除有例外情形，如基於法令、執行職務或業務之必要或經當事人同意等。歐盟則是要求在處理目的所需之必要期間內，且不論在直接或間接蒐集的情況下，皆需通知當事人，使其知悉。就此部份之規範而言，我國與上述國家並無明顯差異。此外，歐盟與我國個資規範皆賦予當事人可請求行使刪除該個人資料之權利。而美國及日本尚有特別針對電信業者或廣播業者在個人資訊保存期間方面，進行細部要求。我國目前在電信產業部份，對此亦有相關之規定。總體而言，我國與其他國家相較尚無明顯之差異。

3. 紀錄及證據保存之規定

美國 1996 年電信法的部分，按聯邦通訊委員會所發布之「用戶專屬資訊規則」（47 CFR § 64），電信事業應以電子或其他方式保存其發現任何違反「用戶專屬資訊」之情事，及曾向美國特勤局（USSS）與聯邦調查局（FBI）、用戶發出通知之相關檔案紀錄，且紀錄中須包含發現和通知的日期等，並保存該檔案至少兩年。根據 GDPR 的規定，資料之控制者與處理者應將處理活動進行記錄，例如控制者、共同控制者或處理者、資料保護員之名稱、聯絡方式；資料進行國際傳輸之對象，及國際

本報告之智慧財產權歸屬於財團法人資訊工業策進會

傳輸之基礎（若採取適當保護措施時，其書面文件）；處理時所採取之安全措施概述等。但，若是控制者或處理者之員工人數不足 250 人，則僅須針對非偶然性的處理、可能對個人權利或自由造成風險的處理、對特種個資之處理等情形進行記錄。

整體而言，我國個資法當中對於紀錄及證據保存，並非強制規定；依據個資法施行細則第 12 條第 2 項之規定，適當之安全維護措施，得包括使用紀錄、軌跡資料及證據保存，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。不過，國家通訊傳播委員會針對第一類電信事業、第二類電信事業、有線廣播電視系統經營者及有線電視節目播送系統、電視事業、訂戶數達三千戶以上之直播衛星廣播電視服務事業以及經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業訂有「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」，該辦法第 6 條對於個資紀錄及證據保存之內容，已有強制之規範。就此而論，我國通傳資料在紀錄及證據保存上，已有明確之規範，與其他國家並無明顯之差異。

(四)資料釋出之授權規範

1. 釋出予第三人

美國之通訊傳播事業資料若要將個資提供予第三人方面，若電信事業欲將「用戶專屬資訊」揭露給第三人或用做行銷相關電信服務之用，需取得用戶事先同意，始得為之；但若是和第三人共同利用個資（如關係企業也是通訊相關業者），則事前無須取得用戶同意，而是採取事後當事人自行表示停止提供的「選擇退出」（opt-out）模式。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

日本之通訊傳播事業在對第三人提供個資方面，原則上採取得當事人事前同意之選擇加入的模式（opt-in)；但後續當事人仍有申請停止對第三人提供個資之權利。

歐盟 GDPR 要求，於授權他人代為處理個資的情形，控制者應確保其所委託的處理者能提供充足保證，其必定會採取適當、有組織的方法，以使處理行為符合 GDPR 規定，以保障當事人的權利。此外，GDPR 規定，若兩個（或以上）控制者可以共同決定資料之處理的目的或方法時，即為「共同控制者」。共同控制者應以透明方式安排彼此在 GDPR 下的義務，包含各自對資料主體的任務及關係，並應將這些資訊的重點提供給資料主體。

我國個資法對於將個資「提供予第三人」雖無直接明文提及，但可參見法務部法律字第 10603509640 號函釋[172]所述，「涉及將客戶個資提供予當事人以外第三人為特定目的外之利用，應符合個資法第 20 條但書規定情形之一，始得為之。」因而，我國公務機關、非公務機關將個資提供予第三人，應可認為屬於「利用」，而分別適用個資法第 16 條、20 條之利用規定，意即原則上，利用應於必要範圍內為之，並與蒐集之特定目的相符；但有例外 7 款情形之一者，得為特定目的外之利用：(1)法律明文規定。(2)為增進公共利益所必要。(3)為免除當事人之生命、身體、自由或財產上之危險。(4)為防止他人權益之重大危害。(5)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經蒐集者依其揭露方式無從識別特定之當事人。(6)經當事人同意。(7)有利於當事人權益。

[172] 法務部法律字第 10603509640 號函釋，https://mojlaw.moj.gov.tw/LawContentExShow.aspx?id=I00100%2c%E6%B3%95%E5%BE%8B%2c10603509640%2c20171011&type=E&kw=&etype=etype5。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

綜觀上述美、日與我國對於將個資提供予第三人之規定相同處在於，原則上皆要求取得當事人事前同意，事後當事人尚有表示停止提供之權利；例外情形下，才毋須取得事前同意。我國與其他國家，在共通原則上尚無明顯之差異。

2. 去識別化（匿名化）規定比較

美國對於去識別化資料，在法律中尚未有明確的標準，但參見 FTC 公布的保護消費者隱私報告中，提及個人資料去識別化可資遵循的規定，係以「有無可合理連結到該個人」做為判斷標準。判斷要件有以下三個，即 1.採取合理的去識別化措施、2.以公開承諾其維護和使用資料的方式，不會對去識別化資料進行重新還原、3.當提供去識別化資料予第三人時，需訂立契約禁止接收者還原該資料，採取適切的管理措施。

日本 2015 年為因應大數據加值與創新應用等技術科技對個資使用的需求，對資料匿名化及重新識別新增相關規範於個資法之層次，如日本個資法對於「匿名處理資料」的概念，係指「對個人資料採取一定的匿名化措施處理，使其無法識別特定個人所得之關於個人的資料，且該個人資料無法復原 」。所謂「匿名化措施具體內容」，是指將包含該個人資料等資訊的一部消除（但若該資訊包含得以識別個人符號時則必須全部消除），或是以不帶有可能復原個人資料規則性的方法替換成其他的記述。亦明文規定當處理「匿名處理資料」時，禁止重新識別。

GDPR 前言第 26 點規定，提及去識別資料之概念；又，英國資料保護法對於去識別化之規定，只要資料經去識別化而無法直接或間接識別個人後，即非屬個人資料，而無英國資料保護法之適用餘地。另，針對

本報告之智慧財產權歸屬於財團法人資訊工業策進會

英國認定去識別化資料之標準，參見英國資訊長辦公室特別發布「去識別化：資料保護風險管理應用準則」，指已經無法識別特定個人的資料，即便透過與其他資料的組合，亦無可能識別任何個人。但此一準則並非強制性規定，亦沒有法律效力。

總結來說，美、日、英三國對於去識別化（匿名化）資料之規定，雖標準不盡然相同，日本個資法及歐盟 GDPR 係以法律位階對去識別化（匿名化）之相關定義加以明文；但英國認定去識別化資料之標準並非強制性規定、不具法律效力；反之，美國則非以聯邦法律位階進行規範。但大致上皆要求採取適當、合理的去識別化處理措施，無法使去識別化資料重新被還原或被識別。

反觀我國個資法對於去識別化並無具體規定，參見法務部 103 年 11 月 17 日法律字第 10303513040 號函之解釋[173]，目前僅說明去識別化應達到無法直接及間接識別特定當事人之程度，但做到什麼程度才符合法律規範，則並無明確說明，尚待進一步的參考依據。然而，根據本研究之訪談及研討會之討論，現行技術上似乎無法確切得出清晰、明確的去識別化（匿名化）操作步驟與方法。因此，觀諸我國未來此部分之修法方向，建議可針對去識別化（匿名化）資料之定義或概念加以明文化，以法律或規則等方式明確說明相關名詞概念，並禁止將此類資料重行識別。又，其去識別化（匿名化）資料之詳細判斷、建議標準，因其無法具備足夠清晰、明確之操作方法，可另以不具形式上法律拘束力的「指引」模式敘明之，協助業者釐清法律規範，並提供法律遵循方式的建議。

[173] 法務部 103 年 11 月 17 日法律字第 10303513040 號函，https://mojlaw.moj.gov.tw/LawContentExShow.aspx?type=e&id=I00100%2C%E6%B3%95%E5%BE%8B%2C10303513040%2C20141117。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

此外，考慮到其難以明確實施，必將存在風險等特性，除推動去識別化（匿名化）之定義外，參考本研究訪談中業者之建議，建議亦可輔導業者以資料自主為基礎，利用技術方法，推動以資料當事人能參與決策為前提的資料釋出機制（例如以技術方式協助資料當事人同意將其資料交換給其他資料當事人）。

3. 資料可攜權

英國與其他國家相較，在釋出規範上有一個特殊的「釋出義務」。也就是「資料可攜權」——資料當事人有權請求控管者以結構化、通常使用且機器可讀的格式，將其基於同意或契約關係所提供之資料，以及依據自動化方式處理之資料提供給資料當事人或其指定之其他資料控制者。這個權利是歐盟在 GDPR 中所新增的權利，其目的於回應科技的發展、促進當事人對資料的掌握。

此一權利雖未見於其他國家之規範，但仍相當值得我們注意。在網路世代，社群網路等各種網路上的服務興起，當事人有越來越多的行為是轉由通訊傳播之服務來行使，其於通訊傳播服務上所儲存的資料也越來越多。當當事人意圖轉換或新增服務提供者的時候，往往會因為資料量的龐大，而產生移轉上的困難，間接限制了當事人自由選擇與掌控的能力。歐盟乃是以創設權利的方法，希望能解決此一問題。同時，亦進一步促進業者之間彼此的合作。因而，歐盟在 GDPR 的立法理由第 68 點特別提到，希望能鼓勵資料控制者發展使資料具有可攜性的共同操作模式，就是希望透過合作，來降低資料當事人移轉資料的成本。

在我國，過去即發生過因為部落格服務中止，而使大量使用者搬移

本報告之智慧財產權歸屬於財團法人資訊工業策進會

資料至其他使用者的情形；行動電話通訊服務中，亦在討論後，決定開放「號碼可攜」服務；這些都是與「資料可攜」有關之議題。以我國狀況而言，目前個人資料保護法架構下，並未賦予當事人請求資料可攜權之權利。但這並不妨礙業者提供類似的權利給消費者，或主管機關依據其他法律規定，要求業者提供類似服務。但我國目前似乎並沒有類似的案例，以前述「號碼可攜服務」為例，雖然概念上有所相似，但兩者在資料傳送之要件、內容都有所不同，並非一樣的案例。(請參考下表)

表 3 資料可攜權與號碼可攜服務比較表

	GDPR 資料可攜權	我國號碼可攜服務
傳輸要件	當事人請求（不限理由、原資料控制者所有之資料不須刪除）	限於當事人申請號碼可攜服務
傳輸內容	基於當事人同意蒐集之個人資料、基於締結或旅行契約所需而蒐集之個人資料、以自動化方式處理之個人資料	號碼可攜服務必要資料[174]
傳輸對象	當事人或另一資料控制者（技術可行範圍）	其他經營者、集中式資料庫管理者

資料來源：本研究自行製作

[174] 號碼可攜服務管理辦法第 22 條

本報告之智慧財產權歸屬於財團法人資訊工業策進會

然而可以預見的，在未來隨著數位匯流的狀況逐漸發展，當消費者面對越來越豐富與多樣的數位通訊服務時，消費者可能想要同時尋求不同數位通訊傳播服務提供者之服務，或是希望能在不同數位通訊傳播服務提供者間轉移自己的資料，當事人在不同數位通訊傳播服務提供者間移轉其留存資料的需求，只會越來越高。這種對於個人資料掌握程度期待提高背景，也正是歐盟 GDPR 將資料可攜權納入規範的主要原因。

就資料可攜權這一議題而言，當前的時代面臨兩方面的問題：一者是隨著數位匯流的發展，消費者在不同的數位通訊服務提供者間選擇、交換的需求與期待提高。不過由於此一概念新穎，此一權利尚未在國際間獲得廣泛承認。一者則是對於資料傳輸的格式、形式等或因為不同業者的需求而有所不同、難以統一。

以歐盟資料可攜權的規範為例，其仍然係將實際資料之規格、互通之方法交由資料控管者彼此討論形成，英國個資主管機關也並未訂定明確內涵，僅是透過指引提供資料控管者建議，說明其可採取的自動化處理方法等。如此也反映出了不同領域資料控管者所需要的資料格式、標準可能不盡相同，難以在不同領域與產業間制定出統一圭臬的現實。

而在我國，即便是所需資料內容彼此較為類似的電子病歷，也是花了多年時間才逐漸制定出統一的規格。本次研究訪談專門從事資料處理的業者也提到，目前國際間大部份的領域缺乏資料的統一標準，僅有少數的如交通領域等才有發展出這類比較共通的內涵；他也認為這樣標準的訂定很難是由政府單方面完成；不過他也建議，政府如果有意發展類似標準，可以協助不同廠商彼此討論、對接，會比較有效率。因此，資料自動化處理技術和標準規格在服務型態各異的數位通訊傳播服務業者

本報告之智慧財產權歸屬於財團法人資訊工業策進會

間，將會是複雜的問題。面對這樣的困境，即便連歐盟也僅要求在「技術可行」的情況下，才須提供資料可攜的服務，亦可窺見此一難處。

換言之，資料可攜權雖為新時代下可能新興的權利種類，但其詳細的運作模式仍有待後續實務運作進行補充，並非完全成熟；現階段直接以強制性規範創設資料可攜權，要求通訊傳播業者提供相關服務，有事實上的難度。因此，建議我國短期內先不以法律形式承認資料可攜權。但考量到未來消費者確實可能出現類似需求，仍有持續探索此一權利發展的需要。

考慮到我國通訊傳播產業內的不同產業別業者組成相當不同，有因行業為特許性質，僅有少數業者參與的（如電信事業），參與業者數量較多，大小不一的行業類別。考慮到實行的可能性，建議可於通訊傳播領域中，業者組成相對單一、掌握消費者資料量較大，且其意願上及技術上皆可行的產業別，以自願型式進行試驗。透過主管機關與業者共同討論個人資料格式、欄位標準等議題，凝聚共識，並以不具拘束力型式的指引逐步釐清可攜權的技術內容。

一方面，業者組成較少可以降低資料格式整合之困難；一方面透過自願性的方式，其意願較高，較容易形成確實可行的規範。而先以此一較小規模的試驗建立典範後，因為其不具法律拘束的特質，較有規範變動的彈性，可以逐步觀察與修正資料格式、可攜之流程等具體議題。

待此一典範逐漸成熟後，再觀察國際間資料可攜權規範發展情形，以及國內民眾對於資料可攜權的需求程度，當可進一步擴大資料可攜的適用範圍，甚至是討論是否需要於法律層面承認此一權利。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(五)隱私蒐集評估機制

觀察目前我國、美國、日本對於隱私蒐集評估機制並無相關細部規範，僅有 GDPR 對於處理前進行「資料保護影響評估」有詳細要求規定，並授權各國主管機關可以另外規定哪些情形，須進行評估抑或得不進行該評估 。

此一評估須包含：第一，處理之目的；第二，處理之必要性及比例性；第三，對資料當事人權利及自由之評估；第四，應對風險之方法（包含保護措施等）；同時，並要求於事發當時應徵詢當事人或其代表人之意見，並在風險發生變化時，應重新進行資料保護影響評估 。而若評估發現在未採取降低風險措施前，該處理將有高度風險時，控管者應於處理前徵詢主管機關 。

英國資訊長辦公室提供的指引則進一步將資料保護影響評估機制分為九個步驟，包含：第一，確認是否需要實施資料保護影響評估；第二，描述所涉及的處理行為；第三，考慮進行諮詢；第四，評估處理之必要性與比例性；第五，辨別其中之風險並加以評估；第六，確認應採取的減輕風險措施；第七，簽核評估結果並存檔；第八，將評估結果落實進處理計畫；第九，持續複查隱私衝擊影響評估。

綜觀本研究所觀察之各國，隱私蒐集評估機制雖並非各國常見之制度。但其設計之本意，在於協助業者在採取新技術之前，透過影響評估識別出風險，並評估可採行之減輕措施。對於業者完善資料治理，建立民眾對資料使用之信任有所助益。此外，對於採用自動化決策處理技術進行資料處理前，應採取隱私影響評估機制的見解，目前雖僅有歐盟有

本報告之智慧財產權歸屬於財團法人資訊工業策進會

相關規定，但觀察國際發展，似乎已經逐漸形成共識的趨勢（詳下述）。建議我國可以以「鼓勵」與建議的方式，引導業者在採取應用新的技術之前，得以先採取類似之步驟，以降低技術可能帶來的風險。

(六)資料側寫議題

就本次觀測的國家而言，僅英國在 GDPR 架構下對於資料側寫技術有明確的規範。在這個架構下，英國規定使用資料側寫技術處理個人資料前應進行資料保護影響評估；同時，除非是基於契約所必須、法律規定或當事人的明確同意，否則應給予當事人拒絕單純採用側寫等自動化處理技術處理而對其造成法律效果或其他類似重大影響之個人資料處理的結果的權利。此外，無論如何資料之控制者仍應對當事人提供部份參與、意見表達及挑戰該技術產生之決策等權利。

這樣的規範建立在兩個假設之上：第一是採用側寫等自動化處理技術將對當事人造成特別之風險；第二則是決策仍應以人為中心，應確保側寫等自動化處理技術產生之結果是透明、可以解釋的（如此當事人才能對其決策進行挑戰）。

雖然目前僅有歐盟將這樣的規範直接規定入法律之內，但類似的倡議在國際間也已經不斷出現。舉例而言，由全世界 122 個中央或地方個資或隱私保護專責機關所組成的個人資料保護專責機關國際會議，在 2018 年 10 月第 40 次年會中就通過了「人工智慧道德與資料保護宣言」，認為應確保包含側寫在內的相關演算法技術是具有透明度、可解釋並具有可及性的；同時，亦主張對於這類技術的使用建立風險評估機制[175]。

[175] International Conference of Data Protection and Privacy Commissioners, DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE, 40th International Conference of

本報告之智慧財產權歸屬於財團法人資訊工業策進會

類似的討論與見解也可以在聯合國脈動計畫與國際隱私專業人員協會在2018年10月共同推出的「將倫理納入巨量資料和AI的隱私框架」報告中看到[176]。但同時，上述兩份報告也承認，對於可解釋演算法的研究，仍須持續投入。

也就是說，國際間對於採取資料側寫技術進行個資處理前應進行隱私風險評估以及對於相關技術應該具有可解釋性、透明性等，似乎已經逐漸形成共識。若以「議題規範化」的法制觀察觀點觀察，資料側寫技術的規範已經經過技術出現、議題形成的過程，逐漸過度到國際共識形成的階段，之後就將會是共識逐漸落實為規範的過程，相關共識將近一步的「實效化」[177]。換言之，我們似乎可以預期，針對資料側寫技術的風險評估及對其解釋性的要求，將會在近年內逐漸加強。

而回到臺灣本身通傳資料的脈絡，經過訪談及研討會的討論發現，業者亦有逐漸引入這類自動決策技術的傾向。這類技術的引入一方面將會降低資料控制者處理資料的成本，相對的也就可能可以使使用者能以更便宜的代價來換取服務。在國際間一方面對此一議題逐漸形成共識、漸有將其轉化為規範的趨勢；一方面對於技術的發展仍待投入的背景下；我國若能在此時，與資料當事人、業者就如何使側寫等自動決策技術具備解釋性、如何評估相關技術可能之風險等議題進行廣泛討論，逐漸形成我國之共識，並適當投入技術的研發。搭配我國相對成熟的技術

Data Protection and Privacy Commissioners, Oct. 23, 2018, https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf (last visited Jan. 10, 2019).

[176] UN Global Paulse and IAPP, BUILDING ETHICS INTO PRIVACY FRAMEWORKS FOR BIG DATA AND AI, https://iapp.org/media/pdf/resource_center/BUILDING-ETHICS-INTO-PRIVACY-FRAMEWORKS-FOR-BIG-DATA-AND-AI-UN-Global-Pulse-IAPP.pdf (last visited Jan. 10, 2019).

[177] 葉俊榮，《全球環境議題：臺灣觀點》，巨流，頁44-57（1999）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

環境，相信可以在國際逐漸形成規範的過程中，同步、甚至領導相關規範的形成。對於我國相關產業的發展，具有重要的意義。

(七)資料加值應用與隱私保護之調和

1. 國際間資料保護標準並未因技術進步而退讓

在技術進步的背景下，資料加值應用的可能性大幅增加。因此有人主張或許有因此降低資料保護規範的可能。然而，就本次研究所觀察的各國規範而言，目前尚未看到各國有因此降低資料保護的規範密度。與之相較，各國目前對於新興技術反而採取比較保守與謹慎的立場。以歐盟 GDPR 為例，針對資料側寫等自動化處理技術，GDPR 不只未放寬管制規範，甚至在自動化處理技術產生資料的目的外利用方面，有制定更為嚴格規定的傾向。同時，GDPR 亦增加對於個資可解釋性、透明性的要求，這些要求也逐漸成為國際間的共識。而近期美國在新技術發展的背景下，無論在在聯邦法層級或州法層級，都有更多資料保護規範的討論，美國加州 2018 年 6 月通過的加州消費者隱私保護法，更被視為有史以來最嚴格的美國隱私保護規範。由此可見，希望因技術發展而放寬管制密度，實非當前國際的發展趨勢。

2. 去識別化標準難定義

此前，我國討論資料加值應用時，往往希望透過政府清楚定義與規範去識別化之標準與實行步驟的方式，協助業者透過去識別化手段進行資料加值應用。然而，此一作法之可行性目前越來越受到質疑。

本研究所舉辦的研討會中，從事資料處理的業者就認為：從技術角

本報告之智慧財產權歸屬於財團法人資訊工業策進會

度來說,「個資的去識別化的確在技術上是不可行,沒有辦法完全去識別化」,因此建議不應該繼續強調去識別化的重要性。來自資料科學界的學者也認為從技術的角度來看,「今天要100%保護隱私的話,表示洩漏的資料量為0」;為與其追求這樣的隱私保護,不如將重點放在如何用技術的方法來建立系統的信任。

對於去識別化標準與實施步驟難以清楚規範的情況,在本研究所整理的各國資料中也可以見到類似的情形。美、日、英三國對於去識別化(匿名化)資料之規定,標準不盡然相同,但大致上皆僅能以規範要求業者要採取適當、合理的去識別化處理措施,並且使無法使去識別化資料重新被還原或被識別。但對於具體的去識別化規定要求,就相對起來難以清楚的描述(這樣的現象有意歐盟最為明顯)。

因此,至少短期內,要以去識別化方法最為資料加值應用的解決方案,是難度較高的。

3. 利用技術協助賦權消費者,建立資料加值之信任基礎

透過個資去識別化以促進資料加值應用雖有技術可行性上的難度,本研究建議可以透過其他技術協助消費者之賦權、建立消費者對資料加值應用之信任,以使資料經濟能妥善發展。

具體來說,資料處理業者認為資料加值應用真正的解決方法應該回到「資料當事人對於資料的自主決定」之上,只要確實賦予當事人自主決定權利,後面的商業規則很容易就可以發展出來。業者建議可以透過中介者協助資料當事人決策其資料應該如何使用以及被誰使用,「用代理人第三方的角度再下去做加值應用,這個可以達到業者損失的減少、消

本報告之智慧財產權歸屬於財團法人資訊工業策進會

費者利益的增加」。

在國際趨勢的發展上，本次研討會中，研究單位的代表也提到外國也有類似的服務模式。在單一企業上面，西班牙最大、世界前五大的的電信公司 Telefonica 開發了一個名為「Aura」的手機應用程式。透過該程式，Telefonica 一方面提供消費者語音助理的功能，包含行程、繳款等的提醒等；一方面，該公司也利用此一應用程式使消費者可以清晰的看到自己的個資是在何時產生，並基於何種目的、以什麼方式使用。因此，消費者可以透過此一程式了解自己個人資料的利用情形，並決定是否同意自己的個資流向哪一個第三方服務，以換取特定的服務。這種即時性的授權與檢核，已經相當的成熟。

除了個別企業外，研究單位代表進一步以歐洲廣電聯盟的例子說明，跨組織間也可以透過賦予當事人自主權的方式，促成資料的加值利用。歐洲廣電聯盟是由 30 幾個國家、50 幾個大型廣電相關的組織。該聯盟成立了一個跨平台資料交易的機制，提供使用者個人化月租的服務。透過串連多加業者，讓使用者得以在此一平台中，在「彼此在合規的情況下去交易彼此的資料」。他認為，這樣的平台有三方面的功能，在個資權利保障上，可以使消費者掌握自己個資流向；在商業上，可以促成跨平台的交易機制；在技術上，可以提供資料科學家進行科學研究。

本研究進一步發現，近年來國際間已經出現更多這類的平台。舉例而言，歐盟「展望 2020」（Horizon 2020）計畫所支持的「我的健康我的資料」（My Health My Data）計畫，就是希望能以技術方法賦權當事人，改善醫療資料等敏感性個資的加值利用情形。此一計畫是透過區塊鏈技術進行身份認證，使當事人可以自由決定資料授權之方式、條件，並借

本報告之智慧財產權歸屬於財團法人資訊工業策進會

由此一平台與資料利用者（包含企業、研究單位等）提供之條件進行配對，再輔以平台提供的多者加密技術手段，促成資料的流通與加值。而日本政府也於 2018 年時公佈「第一版資料信託功能認定指引」(情報信託機能の認定に係る指針 ver1.0)，希望透過設立具有仲介性質的「資料銀行」來促進資料的加值利用。日本計畫讓資料當事人委託資料銀行處理其個人資料，當事人預先指定其個資利用條件，由資料銀行與第三方進行配對，進一步促進資料的利用。

本研究認為，過去認為資料加值最大的難題在於難以取得當事人對資料利用條件的同意，但這樣的困境在近年來已經有逐漸改善的跡象。除了前述的各項外國案例外，我國衛福部的「雲端藥歷」其實也是類似的概念。本研究建議，我國可輔導業者透過技術的方法，使資料當事人更容易行使其權利。透過這樣的方法，使其信賴資料加值應用的體系，進而可以在使當事人個資受到保障的情況下，促進資料加值應用的發展。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

貳、舉辦業界訪談及研討會

一、進行訪談

(一)訪談情形

本計畫依進度完成訪談八場次，針對之重點主題包含以下三項：第一，對於現階段政府對於取得、保存、釋出個人資料的相關規定，是否有過嚴或不足，亦或是規定不清楚，而需要調整之處？第二，若有須調整之處，建議採取何種方式調整？是具有法律拘束效果的法規命令，或是以不具法律拘束力的行政指導提供？第三，我國是否應設立個資保護專責機關？是否曾因個資有多主管機關造成法律遵循上的困難？如須設立個資專責機關，建議採取何種形式、位階的方式設立？

本計畫將訪談對象分為法律學者、大型電信業者以及其他產生或利用通傳資料業者三類，分別就學術以及兩種不同類型業者蒐集當前通傳產業個人資料之管理架構以及我國整體個資管理架構的看法。詳細之訪談時間、對象請參考下表，部份受訪者資料依其意願模糊化處理。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

表 4 訪談時間與對象

時間	性質	對象
7 月 16 日	大型電信業者	中華電信法律事務處鍾國強協理
7 月 18 日	法律學者	中原大學財經法律系江耀國教授
7 月 19 日	大型電信業者	中華電信數位匯流事業處王莉貞總監
7 月 20 日	其他產生或利用通傳資料業者	景翊科技陳毅廷總經理
7 月 20 日	法律學者	國立交通大學科技法律研究所陳錡雄教授
7 月 25 日	大型電信業者	遠傳電信李和音資深副總經理
7 月 27 日	其他產生或利用通傳資料業者	麟數據佘志龍共同創辦人暨技術長、鄭名傑共同創辦人
8 月 2 日	其他產生或利用通傳資料業者	臺灣本土 OTT 平台業者數據專案經理

資料來源：本研究自製

(二)訪談內容歸納

1. 現有規範調整建議

就現有規範而言，訪談的大多數業者並不覺得現行個資保護規範「過於嚴苛」，認為現行的規範並不至於難以釐清。無論事業者或法律學者，對於我國現行規範最主要之建議，還是在於「去識別化標準」的釐清上。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

對此，訪談對象認為，政府可以考慮以建立「去識別化指引」的方式，協助業者執行去識別化的工作。而考慮到現實上去識別化「是否有效」往往難以清楚確認，許多業者及法律學者皆建議可以考慮引入第三方認驗證機制。透過第三方提供客觀的去識別化程度驗證，協助業者及民眾釐清資料之風險。以便在兼顧個人資料保護的前提下，釋放資料之價值。

另外，有部份業者建議，除了「去識別化」外，政府可以協助建立資料交換的平台或是機制，透過平台讓資料當事人也可以參與資料交換的過程。將權利交給個人，反而可以促進資料的流動。而對於較小型的業者而言，則期待能更清楚釐清在與第三方合作的時候，到底有哪些東西需要去確認？比如彼此應該符合什麼樣的規範或是資料應該如何儲存或是檢核？這部份的具體執行方法及注意事項如能釐清，可以讓業者更勇於與其他業者交換資料，發揮資料的價值。大型業者也表示，因為這類規範不夠熟悉的緣故，可能會降低其進一步與第三方活化資料使用的意願。此外，亦有部份業者建議，政府可以考慮放「同一集團間」(個人)資料交換的條件。目前個人資歷在同集團間傳遞的規範相對較少，希望能透過集團內部傳遞規範的釐清，來活化資料的價值。

至於實際執行的方式，業者建議的內容都相當類似。由於我國個資法修正未久，無論從企業遵循成本、熟悉規範成本上討論，都認為暫時無須、也不宜再次修正法律規範。因此，建議政府可以在現行的法律架構下，依據其本身的職權，以行政程序法中「行政指引」的定位，提供業者「不具拘束力」之指引，協助業者釐清個資法中的不確定法律概念。並可以針對特定之議題，例如資料之「識別性」、資料交換或傳遞時應注意之事項等，做較為詳細的說明，以促進資料之應用發展。而這樣的執

本報告之智慧財產權歸屬於財團法人資訊工業策進會

行方式，也為學者所認同。

2. 個資保護專責機關設置議題

在主管機關上，受訪業者普遍認為若能有單一之個資主管機關，對於遵循上，可以減少跨機關間執法標準不一的情形，對於法律遵循有所助益。尤其是部份業者經營領域橫跨不同產業，會依業務內容分屬不同目的事業主管機關管理個資規範，對於業務推展的時程等都有所影響，難以事實跟上該領域發展的情形。而有些業者其經營的型態可能橫跨不同目的事業主管機關，其認為現在個資的蒐集處理已經成為專門的領域，如果以統一的專責機關，有助於業者與主管機關互相溝通、協助，落實個資之治理。對此，學者亦採取相同的見解，認為單一主管機關不僅是國際常見的管制模式，亦有助於個資規範之落實。

至於單一主管機關之設置方式，業者普遍沒有特別意見。學者則認為應採取獨立機關的型式，但究竟採取何種模式，則有不同看法。有學者認為，考慮到目前相當中央二級機關之獨立機關已經建制已經達到上限，可以考慮以「相當中央三級機關之獨立機關」來管理個資的議題，並建議考慮到政府機關對於個資解釋、適用的熟稔程度，可以考慮將此一機關設立於法務部之下。另外有學者則建議，可以參考美國由聯邦貿易委員會以競爭法角度管理個資議題的模式，將我國的個資專責機關郊遊「由公平會管理」。同時，學者也建議，在中央組織尚未能調整之前，各機關內部可以先進行內部的組織調整，先行在機關內設立相對具有獨立性的會議、邀請外部專家協助對個資管理提出意見，以完善當前個人資料管理的治理。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

二、舉辦研討會

在後數位匯流時代與網路社會中，資訊快速散布的特性，更突顯出建構資料保護的重要性與迫切性，我們需綜觀對各界的影響，釐清處於模糊界線的法制環境和政策，才可進一步與國際法制接軌及正確認知個資制度規範對國家、產業、利害關係人及個人的影響，進而在發展創新經濟下，使個人資料能獲得充分保障，相關產業能更有效的遵法，為現今不容忽視之課題。

科技進步及技術演化為傳統通信傳播業帶來創新機會，在數位經濟時代下，手中握有大量客戶資料的台灣電信及通訊傳播業者，期待在龐大資料基礎下，透過跨產業、領域的合作，運用人工智慧等數位工具，推出消費者所需的應用服務。面對這些新經濟發展的期待，如何在滿足個人資料保護需求前提下，適當地讓這些以資料為基礎的經濟模式穩健發展，成為亟待解決之議題。

因而，於 9 月 20 日(週四)舉辦「資料經濟新紀元——通傳資料加值應用之法制展望」研討會，地點於通訊傳播大樓集思會議中心，會中邀請多位專家、學者到場就「資料經濟時代下之通訊傳播資料加值應用之需求與困境」、「通訊傳播資料經濟發展之法制發展與因應之道—以 GDPR 與 ePrivacy Regulation 草案發展為核心」以及「他山之石---國際應用案例之介紹與我國之借鏡」三個子題進行深入討論，透過匯集產、官、學、研各界人士交流對話，期盼作為主管機關未來擬訂整體法制政策發展或相關因應措施之參考，並協助產業界消弭於再利用開放資料時所遭遇之法制疑問，引領台灣走向資料經濟新紀元。當日議程、與會人數及研討會摘要，依序詳列如下。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(一)議程

表 5 研討會議程

時間	活動	活動內容
09:00-09:40	報到	來賓簽到
09:40-10:00	開幕致詞	資策會科技法律研究所　張瑞星所長 國家通訊傳播委員會　詹婷怡主委
【主題一】資料經濟時代下之通訊傳播資料加值應用之需求與困境		
10:00-12:00	主持人	張瑞星／資策會科技法律研究所所長
	主講人	宋佩珊／資策會科技法律研究所組長
	與談人	李和音／遠傳電信資深副總經理
		林雅惠／凱擘股份有限公司法務法規室副處長
		張維志／Open Data Tw 計畫負責人
		楊立偉／意藍資訊董事總經理
		楊秀一／中華電信大數據處技術總監
12:00-13:20	午休時間	
【主題二】通訊傳播資料經濟發展之法制發展與因應之道—以 GDPR 與 ePrivacy Regulation 草案發展為核心		

本報告之智慧財產權歸屬於財團法人資訊工業策進會

時間	活動	活動內容
13:20-15:00	主持人	顧振豪／資策會科技法律研究所副所長
	主講人	王德瀛／資策會科技法律研究所法律研究員
	與談人	江耀國／中原大學財經法律系教授
		陳銘雄／國立交通大學科技法研究所副教授
		翁清坤／輔仁大學財經法律系助理教授
		洪志勳／萬國律師事務所合夥律師
15:00-15:20	休息	
【主題三】他山之石---國際應用案例之介紹與我國之借鏡		
15:20-17:00	主持人	李 淳／中華經濟研究院 WTO 及 RTA 中心副執行長
	主講人	陳奕廷／景翊科技股份有限公司總經理
	與談人	曾更瑩／理律法律事務所合夥律師
		歐雨瑞／資策會數位服務創新研究所專案經理
		佘志龍／麟數據科技股份有限公司技術長暨共同創辦人
		李思壯／中研院資訊科技創新研究中心研

本報告之智慧財產權歸屬於財團法人資訊工業策進會

時間	活動	活動內容
		究員
17:00~	賦歸	

資料來源：本研究自製

(二)與會人數

主持人、主講人、與談人及貴賓共 22 人，與會來賓 149 人，媒體 1 人，總計 172 人。

(三)活動摘要

(1) 開幕致詞

A. 資策會科技法律研究所　張瑞星所長

在數位經濟時代下，消費者上網使用手機過程中，產生許多資訊與資料，且都集中在各家傳播媒體上，若能進一步的運用與加值，提供個人、市場上相關的服務，進而創造出更驚人的經濟價值。但資料在收集過程中，勢必會衍生出隱私權、個資法的問題，因而需要產、官、學等三方齊聚一堂，透過共同討論的方式，作為政府機關制定相關法規時的依循。

B. 國家通訊傳播委員會　詹婷怡主委

隨著新的商業服務與營運模式擴展，通訊傳播在行動化、數

本報告之智慧財產權歸屬於財團法人資訊工業策進會

位化、互動化及寬頻化的匯流趨勢下，過去垂直產業生態及營運模式已然大幅翻轉，不但消費者使用行為改變，產業型態及結構也必需面對改變。5G、IOT、AI、AR 等創新應用順利與否的核心，不僅僅是網路頻寬，也因產生大量數據，進而透過分析推出消費市場所需的服務。所以政府在推動寬頻環境時，必須要建立被信任的環境，否則最終將會延遲創新應用發展。當我們享受到科技發展的好處時，亦須了解到科技背後帶來的疑慮等。要如何建構隱私權架構，政府機關可以參考國際標準，例如：要關注提升資料運用透明度、企業要建立完善的個資保護制度、資安保護的重要性、資訊產品的資安問題等。

(2) 場次一：資料經濟時代下之通訊傳播資料加值應用之需求與困境

A. 主講人資策會科技法律研究所組長宋佩珊發言重點

數位資料經濟關鍵的核心在於「數據」(data)，利用創新科技技術而取得大量使用者的使用紀錄，並將之加以重組分析、加值應用，透過巨量分析(analytics)與資料探勘(data mining)方式，萃取出有用或可供預測的資訊，幫助業者瞭解使用者行為，所再產生的經濟、服務或者一些商品，推展新服務，促使數位經濟時代於焉形成。例如像人工智慧，抑或是無人載具，也需要大量的資料作相關的堆疊，作為運作的基礎；諸如像智慧製造、金融科技等科技，也是在資料的基礎上進行應用發展。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

以下從供給與需求、公平競爭、資料有價、風險控管四個面向，討論數位經濟市場機制的圖像。

第一個，供給與需求，係數位經濟市場必要的條件，須具有供給和需求去展開相關的資料圖像，資料本身供需必須建立，才能促進資料經濟的發展，並且透過跨境國界進行資料的輸入與輸出，擴大市場。先天上，我國為較小的國家，人民的數量比不上歐盟、美國、日本這樣大的市場，因而會有人才培育跟技術創新的問題，我們要提供夠好的產品，才有辦法輸出使用或是吸引人才建立。在人才培育的部分，目前產業本身累計非常多的資料，但是大家大多不知道這個資料是有價值性的，係因沒有足夠的人才去將資料變成有價化。有關技術創新的部分，我國產業必須有足夠創新或是獨特的技術，才能將技術輸出，進行國際化的合作，包括像資料API、資料平台、資料經濟應用技術的方面，也都將是未來必須進行的相關努力。

第二個，必須建構一個公平競爭的資料經濟市場，要完善市場的機制，增加國際的競爭力與自由流動的面向。在資料累計方面，業界或許覺得大部分掌握在外商的手上，所以國內廠商應該如何因應？我國必須規劃相關的公平市場競爭機制。公部門的部分，可以促進政府資料開放，畢竟在台灣來說，最大資料擁有者是政府，政府如何將資料合理的開放，去促進一個公平的競爭環境，係非常重要的點。私部門的部分，須建立合理的交易機制，免除不必要的法規障礙，或者

本報告之智慧財產權歸屬於財團法人資訊工業策進會

透過沙盒進行等方式。再者，更應積極強化國際競爭力，可以從國際合作計畫著手，或是資料品質認證的機制，進行資料交流的介接，都是可供我國參考的部分。

第三個，經濟規模的建立必須在資料上賦予它價值，所以建議需有鑑價制度跟公共資料開放，並且增加私部門資料流通的誘因。倘若資料都累計在自己公司內部，但未為一些創新的規劃，或者創新的誘因，業者們較不願意把資料釋出。又，促進公共資料開放，建立友善使用的接口而言，形成一個有效的社會地位措施的狀況，資料可以在各機構當中作有效的流通，當流通性越高，它的價值鑑定就會越高或是越具誘因，所以此一部分也是資料經濟中很重要的一環。

第四個，有關風險控管的部分，如果資料經濟的市場不是讓人信賴的環境，風險控管不足的話，將造成市場失序，大家較不願意把資料提出來，因而個資保護及資安管理就成為非常重要的項目，倘若大眾都不知道個資怎麼被利用的話，或不具透明化的過程、有機制的處理、一個受信賴的環境，民眾即不願意把自己的資料拿出來，業者也不知道該如何應用這些資料。因此，如何架構這樣一個信賴的市場環境，將市場的風險控制在可行的範圍內，變成非常重要的關鍵。此時，即需要相關的法律、政策作為管理、控制風險的要素。

是故，資料種類繁多，如何運用受到信任的資料，才能做進一步的資料分析與加值，否則將會因為不受消費者信賴，而讓在推動資料加值應用過程中受到限制。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

B. 與談人凱擘股份有限公司法務法規室副處長林雅惠發言重點

目前，隨著不同的產業的發展、轉型，尤其在現在視聽媒體環境情況下，有一些 OTT 的加入，有線電視的部分開始作一些轉型，至少在媒體產業的部分，因為數位化的演進，帶來蠻多媒體板塊的移動，以及在數位轉型上我們面臨的陣痛期。不管是在有線電視或者是傳統的頻道上，數位化之後，透過雙向的機上盒可以去了解用戶的收視行為分析，但是因為廣告或是收視時間的改變，更多的視聽的行為是在網路上，透過社群媒體、視聽影音網站或是 OTT，其實更多的網路服務上在蒐集民眾的收視行為表現。這樣的發展也讓我們發現，這一些收視行為的分析上，因為有不同的載具、不同的平台，其實整個產業的面向會變得更多元、更複雜。從內容來講，除了以往的頻道以外，現在有更多的影音視聽媒體，平台的部分也從有線電視、頻道來到像 OTT 或其他的影音市場；在載具的部分同樣也非常多元，從傳統的電視、手機，現在個人一般的發展。所以整個產業的上下游，就是因為數位匯流發展，有非常大面向的改變。

我們認為現在台灣的企業比較難預測用戶在收視行為的分析表現上，有幾個蠻重要的原因：首先，業者或者產業不願意投資在做這些數據的分析上。根據資策會在去年的調查報告，大概有 48%的比例，產業不太願意投入那麼多人力、資源去做這些，因為他們看不出來投入這麼多人力、投資設

本報告之智慧財產權歸屬於財團法人資訊工業策進會

備，到底後面會產生的效益在哪裡？這是第一個在實施上有一些困難的部分。第二個部分，在資料欄位的共同規範上，我們認為不同的產業所蒐集的資料，如果在資料欄位上沒有辦法作溝通跟討論，其實在資料的分析上也比較難做一個統一的處理。第三個部分，法令的部分，我們了解在資料取得上最重要是得到用戶的同意，得到用戶東西之後，要再做去識別化等程序。但是整個認證程序或是去識別化的程序，希望能有一個第三方的公正機構進來，協助作一些輔導跟討論。第四個部分，資料計價標準的部分，這個部分在台灣也是比較少被討論到的。

這幾個面向，歐盟認為要開放公部門、私部門跨產業的交流。如果公私部門可以作一些結合，就可以得到更多的發展。整個效益評估上跟資料共同規範的部分，這個部分涉及系統、平台或內容的部分，除了導入第三方加入，作資料共同欄位的開發、運算跟資料整合，政府在這個面向上是否可以給與一些協助？在私部門的資料整合上，其實跟公部門有非常多資料可以串接、比對，作一些服務的創新，這個部分是很重要的。在跨領域人才培育上，是台灣現在的當務之急，讓整個上下游產業的環境可以更健康、健全的被創造出來。

C. 與談人 Open Data Tw 計畫負責人張維志發言重點

首先，資料平台格式如果有政策性的規劃，其實不是格式的問題，是叫做資料的標準，從各個領域其實都有標準，但是

本報告之智慧財產權歸屬於財團法人資訊工業策進會

有標準有沒有人要遵守？是另外一回事。另外，台灣完全不缺人才，台灣在這方面的人才都非常優秀，寫程式的人非常多、很強的人非常多、可以參考國際計畫的也非常多，但是創新、創意、找出資料的價值，那是要跨領域、要知道到底想解決什麼問題，我們的教育沒有在教問問題，是在教回答問題。我們需要找出更多問題，才能知道我們今天講的所有東西的目的是什麼，才會有意義。所有事情都需要成本，今天講資料經濟的時候，我們遇到最大的問題是，面對這麼多需要成本投入的地方時，到底誰願意投入？當我不知道、我沒有能夠創造新價值的時候，我為什麼要投入？我有這些新的資料之後，該問什麼新的問題？這才是今天資料經過最大的問題。

接下來，我把基礎的架構定義出來。首先，資料要作分類，第一個叫做政府的資料政府，其中政府的公共資料，他的法制基礎從來都不是為了開放料所設計的，保障知的權利在今天，我們開始需要有完全不一樣的做法，我們需要更好的做法透過科技、技術的力量，來達成政府資訊公開。第二個，企業蒐集到的資料，企業願意把它的資訊、資料放出來，只有一個目標，就是促進讓自己的價值可以更大化；如果自己價值無法更大化，講再多要企業把資料丟出來，絕對不會有人理你。第三個，個人資料。個人資料不等於隱私，隱私是一個很抽象的概念，每個民族對隱私的想像都不太一樣，但是很難用法作規範，個資法只是把一些基本東西定義下來，所它不是模糊，但是接下來要落實、執行的時候，有很大的

本報告之智慧財產權歸屬於財團法人資訊工業策進會

討論空間的確沒錯，但不是它沒有把基礎想清楚（而是性質使然）。

在資料經濟中，有三個行為者：第一個是資料產出者，第二個是資料的擁有者（蒐集資料的人），第三個是資料的使用者，這三個人不是三個不一樣的人，這三個可以是同一個人，也可以同一個人扮演兩個不一樣的角色，重點在於資料有不同的使用方向和情境。有資料、有不同情境，就可以用法、執行程序以及科技的力量這三個面向來談議題。

第一個是「法」，法就是基礎的遊戲規則，政府的資訊是政府資訊公開法；個資是個資保護法；企業蒐集的資料有各自的法規範他的遊戲規則。法上新的需求，需要完全不一樣的玩法、不一樣的做法，讓它原本的目的可以做得更好、可以達到。第二個，我們有法之後有沒有「執行程序」？我們需要落實很多的執行程序，程序是需要經過設計過，現在政府的運作程序，很多都是照傳統的做法，10、20 年來不會改變。這些都需要借助科技的力量來加以改變。因此，第三個是「科技的力量」，我們有法、有程序，我們需要透過科技的力量讓前面這兩個真正達到它的目標。

回到通傳資料上，不管是私人企業也好、公部門也好，都會蒐集到非常多大量的資料，這些資料依照資料的屬性，該有完全不一樣的遊戲規則。這個遊戲規則必須要定義很清楚，這個遊戲規則就是法。有法之後，要想辦法讓它落實，落實和目標、目的有很大的關係，我們一直以來都是傳統的目的

本報告之智慧財產權歸屬於財團法人資訊工業策進會

沒有改變，會不會有更多的資料進來之後，我們有新的可能性出現？若有新的可能性，我們可能就需要進一步資料分級、分類，和使用權限的分級、分類，和裡面的授權模式。

資料是跨很多不同的領域，很多的不同專門的學術，很多不同專門的學術、不同的技術，它跟技術真的有很密切的關係，但千萬不要忘記它有一個核心的價值，就是 GDPR 在講的「資料自主權」。每個人資料是你們自己的，企業產生的資料是他自己的，要把中間的遊戲規則定義非常清楚。目前並不是法不清楚，而是中間遊戲規則不清楚。

另外，在信任的問題上，如何建立一個信任關係？政府需要把業界找過來，業者也需要傾聽使用者的聲音，需要協力的夥伴關係。而有些東西有些真的不是信任問題，但是我們可以有很多新的解決方法，這也是可以透過協力來釐清的。

D. 與談人遠傳電信資深副總經理李和音發言重點

從電信產業來看，電信產業的收入來源主要是語言跟 SMS 的收入，目前都呈現大幅下降的趨勢，現在產業的界限也越來越不清楚，大家也跨足其他不同的領域。其實業者都很清楚所掌握的資料是有價的，可是不把它活化，就像土地一樣，它就沒有價值，一旦活化它才有價值的存在。然而，在整個發展的過程當中，如何取得繁榮跟隱私（個資）之間的平衡點？產業在發展的過程中，5G 的時代會談到無人車、無人載具、遠距醫療，「信賴」就變成非常重要的要素。要如何確保科技發展所帶來的繁榮跟個人資料的保護中間作

本報告之智慧財產權歸屬於財團法人資訊工業策進會

一個平衡點，也是所有業者發展的過程中間所看到的困境，也可以說是如何取捨的問題。

而信賴，是隨著每個國家的發展，甚至每個經濟的體系會有不同的狀況發生，是取決於政府機關還有整個社會團體對信賴的機制是否存在。我們要怎麼在臺灣建構這樣一個信賴的機制會是最大的問題。

個資法從企業的角度來看，這其實是一個風險控管的問題。因為一旦造成不確定性的時候，其實代表的是那個信賴機制也隨時可能會破壞。所謂的明確或不明確完全是隨著時代演變，我們會希望政府能夠比較明確的，甚至可以跟業者共同探討，用一些創新的模式，探討以後應該要怎麼樣發展的趨勢。目前看到國發會有成立個人資料保護辦公室，我覺得是一個非常好往前邁進的一大步，未來我們也希望在個人資料保護辦公室上，能夠扮演更積極主動的角色，甚至能夠變成一個獨立機關解決有關個資上的疑慮，這樣對業者來說，會給業者比較大的發展空間。

E. 與談人意藍資訊董事總經理楊立偉發言重點

以下以一個資料業者的角度作發言。國外整個資料運用的趨勢，一般的公司轉行為資料公司，在這樣的領域當中，已經是不可逆的現象。我們公司在資料商業允許的範圍之內，也開始在允許法規的情況之下，不斷去尋找很多加值運用跟突破，這就是資料經濟本來的樣子。之前講大數據，是擁有大數據的人自己內部作使用，這沒有問題；現在看到更多的是

本報告之智慧財產權歸屬於財團法人資訊工業策進會

資料交換，而這才是整個資料經濟極大規模的特性。現在資料經濟進入到跨界、多種類的使用，這個最佳化沒有辦法由各公司自動產生，需要有一些力量去協助。有時候是因為資料接近壟斷的情況，彼此之間不流通、拒絕連結，以市場地位干擾，造成大家都沒有獲利，這是我覺得必須要突破的事情。

這部份可以分成兩個層次：首先，如果是通傳資料之利用能夠協助這個社會更好的發展，有一些比較基本的資料應該放出來變成比較開放的資料。這裡說的跟政府的資料無關，是講通傳相關業者的資料。比如說各家 ISP，或各家電信業者，在網路上流量不牽涉到個資的統計資料等。這種流量統計資料本身商機就很大，它會減少很多流量資料投資的浪費，對公眾利益有幫助。若能配合第三方單位、法人單位協助作一些發布跟統計，就會有增進公眾利益之效果。

第二個，針對哪些資料可以進一步作加值利用。在這裡要說明，個資的去識別化的確在技術上是不可行，沒有辦法完全去識別化。我們的個資法跟歐盟最重要一個概念叫做「自主」，通傳資料在使用者同意的情況下，就可以跨業者，甚至到第三方業者去做使用，可以達到利益的共享。以計費資料為例，如果透過資料共享，可以讓業者損失的減少，讓用戶拿到更加資費的優惠，有些用戶就有誘因願意交資料授權出來，願意的用戶資料就可以拿去使用。

因此，主要的建議有兩個：第一個，有哪些是能夠公開出來。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

如同剛剛所講的，以我們所在的業界，人才也不是問題、技術也不是問題、資料標準這都是小問題，最前面的問題反而是整體最佳化。在某些情況下，無法直接拿到最佳化，需要有一些力量的協助。某些資料大家不可以以市場地位反對、阻止，整個公眾利益顯相關、而且有幫助的資料應該開放出來給大家使用。第二個，原來在私領域的資料，先讓使用者能夠回歸自主。一旦回到自主的時候，其他後面的商業規則很容易就可以出來，我們用代理人第三方的角度再下去做加值應用，這個可以達到業者損失的減少、消費者利益的增加，貢獻的增加，這個才是我們今天談資料經濟以未來在看，為什麼規模性會這樣大、為什麼國外會這樣做，最大潛在的商機在這個地方。

F. 與談人中華電信大數據處技術總監楊秀一發言重點

我們可以換另外一個角度來看這件事情，實很多商業的活動假設分成幾個階段：市場調查、生產製作以及賣給對的人。今天很多消費行為、商業活動這麼精采，就是因為找到對的人，能夠精準對到那個人，這個時候就涉及到對個人資料或隱私的理解，這三個階段是有關係的，當你不希望你的個人資料被人家留下來使用的時候，你就不被列為對的人。

資料經濟可以從幾個角度來看：第一個角色，我是資料的擁有者，我們是要付成本去把資料留下來紀錄，直到最後資料變成價值之後才能把錢收回來；第二個角色，提供設備、工具讓大家處理這個資料的人，通常這個市場經濟很大一個部

本報告之智慧財產權歸屬於財團法人資訊工業策進會

分是這些人先得到，以後你要留下紀錄、產生紀錄，就要買設備。資料的供給現在應該不是太大的問題，因為只要準備好足夠的偵測設備，不管是實體或虛擬，都可以把資料存下來，任何一個公司都可以存各式各樣的資料，但是問題資料留下來做什麼？給誰使用？所以資料是誰來轉換？就是資料的科學家能夠把資料轉換它相關性的價值，資料的科學家在哪裡、他的技術怎麼培養？

還有一個問題衍生出來，資料的多樣性在哪裡？你自己企業的資料只能顧自己的方式，能不能給別人產生獲利？大型業者因為他有足夠大量的客戶、足夠大量的多樣性資料放在裡頭，所以對這個資料的主張權就有很大的話語權。其他人希望做到什麼？是不是可以做到資料的交換？因為資料的產生價值就是資料能夠交換，互補有餘，我缺的加上你的，我們兩個加起來就能產生新的應用。

資料交換怎麼辦？交換資料要能夠合併、要能夠識別，就需要把它連結，這個資料是人的連結還是設備的連結？如果是設備的連結，這個設備是不是有持有的人、那個人是誰？種種關係的連結，最後回到一個關鍵點，個人資料在這上面保護的關係是什麼？怎麼處理？些東西都限制住我們跨業資料交換跟連結。以個人資料來說，如果同意以後才開始作資料的交換跟合併，那數量是很少的，商業模式不太容易創新發展出來；可是如果不同意的話，就開始作資料的合併、交換，就會踩到法律的紅線。到底資料的交換可以朝怎麼樣的

本報告之智慧財產權歸屬於財團法人資訊工業策進會

方式可以做好？這個其實有很大的應用空間。某種程度還是回到一些關鍵的問題——個人資料的認定是什麼？現在此刻的工具就是去識別化，但會有再識別化的問題。目前實務上的作法是，如果資料綜合在一起的時候，他的個數少於一定的數量時，就不會把這個資料放出來，以避免相關風險。

另一個問題是，資料會產生價值，資料的價值應該歸誰？以前都不覺得消費的紀錄產生分析的利用價值要回饋給個人，現在為什麼會覺得所有活動紀錄被留下來要回饋給別人呢？如果這些回饋的資料是沒有辦法被利用，他會不會因此提高它的定價？你的活動留下來的資料被人家拿去產生價值，你也有得到你的價值，你得到資訊的價值、得到社交活動各方面的價值，但是你留來下的紀錄變成別人的金錢價值，所以整個生態鏈是這樣的關係，也許不容易從單一的面向談這個問題。

今日最關鍵的問題是，怎麼在關鍵的方面設定好商業活動範圍，讓業者有遵循的方向、有一個指引，不會意外踩到紅線？這或許沒有標準的答案，要嘗試著逐步釐清。

(3) 場次二：通訊傳播資料經濟發展之法制發展與因應之道—以 GDPR 與 ePrivacy Regulation 草案發展為核心

A. 主講人資策會科際法律研究所王德瀛法律研究員發言重點

介紹聚焦於歐盟之 GDPR、ePrivacy Regulation 草案兩項重要規範。可以從歐盟規範當中，觀察出其對資料保護展現了對

本報告之智慧財產權歸屬於財團法人資訊工業策進會

個人資料自主決定之尊重，以及對新科技的謹慎態度。

GDPR 是高標準的法規且納入新資料經濟發展的考量，台灣是否要遵循有待考量，台灣若未來與歐盟簽署適法性相關文件，很多部分都可能要做調整，但仍應注意法律遵循成本及文化差異，對個資法規定的要求細節不一定須全盤照搬。又，人工智慧（演算法）與區塊鏈等，新興技術對資料保護形成新的挑戰，亦需要更加地關注與重視。

因此，科技法律的發展需不斷在「權利保護」與「技術創新」間求取平衡點，因應科技匯流，促進數位時代的健全發展，維護國民權利，保障消費者利益，提升多元文化。

B. 與談人中原大學財經法律系教授江耀國發言重點

GDPR 在過去這一年變成顯學，因為它深刻影響美國主要網路上的大廠商，譬如像 Google 或者是 Facebook，事實上它也幾乎影響所有要跟歐盟作貿易的國家，包括我國。但我開始有一些想法，覺得是不是全世界的個資法都要修改的像 GDPR 這樣子？也就是說 GDPR 作為現在個資保護，是不是一個完全沒有懷疑餘地的標準版？對此我產生深刻的懷疑，想要藉由今天的場次作一些反思意見的提供。

第一個，離開個別的規範條文，GDPR 到底起源是怎麼來的？它不是無中生有的，是 1995 年指令的升級版。為什麼會在 2016 年的時候通過？看一些資料，表面上歐盟的資料說，因為大數據的關係、因為物聯網的關係，我們需要有更高的標

本報告之智慧財產權歸屬於財團法人資訊工業策進會

準來保護我們的個資。然而，實際上啟動 GDPR 的關鍵是美國。上個月參加了資策會科法所邀請一個奧地利顧問公司的管理師，他說 GDPR 在第一個版本出來的時候，在歐盟內部並沒有引起廣泛、高度的興趣。直到史諾登事件，讓歐盟覺得，原來美國的情治單位有可能透過網路在各個地方蒐集個人資料，因此而積極在 2013 年歐盟執委會有一個討論的版本，2016 年就通過，因為 2 年緩衝時間，所以在今年 8 月才實施。GDPR 的誕生，相當程度是因為歐洲作為一個強權要來對抗美國這樣另一個強權而產生的。第二個，很少看到一個法律的域外適用效力會像 GDPR 這麼強的，也就是全世界所有的廠商，不管是哪一個國家的廠商，只要你服務提供給歐盟裡面的一個人就適用了。背後的意義是什麼？它其實還是在對抗美國強權，這邊的強權指的是有重要影響力的網路廠商，像 Google、Facebook、Amazon 這樣的大廠商。這樣一個高規格的 GDPR 是世界兩強之間的爭奪，我們作為不是在這兩大陣營的國家，但是我們跟這兩大陣營都有一定的貿易關係，我們其實要思考的是自我的定位。如果只是因為 GDPR 的關係，所以國內就開始要照著改，我會覺得是一個沒有經過反省的論述。

我一直在思考個資法在過去 20 年間的發展。個資法整個模型的基礎就是在歐盟，但是如果去看歐盟比較早期的文獻，會發現歐盟個資保護指令也說，因為保護人民權利的需求，這邊的權利指的是隱私權，所以我們要保護個人資料。但是這 20 年來的發展已經逐漸跟隱私權脫離了，無論那個資料

本報告之智慧財產權歸屬於財團法人資訊工業策進會

有沒有隱私意涵，任何跟自然人有關的資料，只要這個自然人是已識別或可識別的話，那個資料就是個人資料。，2016年一個 Breyer v. Deutschland 的案子，這個案子爭點是：浮動 IP 是不是個人資料。歐盟法院的判決到最後說，有可能是個人資料，如果這個時候會有網路攻擊的話，檢調單位就有可能去查這個活動 IP 跟他連結使用的自然人是誰，他就是跟自然人有關的資料，這個就可以是個人資料。個人資料的範圍在歐盟的解釋之下，已經廣到難以想像的程度，所以我們的個資法是不是一定要往這個方向發展呢？

第三個，GDPR 讓我看到的東西是當事人權利不斷的擴大。當權利不斷的擴大，背後意謂著管理者的成本不斷的增加。管理者的成本不斷的增加跟權利擴大帶來的利益，兩者之間應該要有比例關係。比例原則不是只有作為法律執行的原則，應該是一個在立法政策上就應該考量進去的原則。如果權利擴大所帶來的利益顯然跟造成成本或者成本或損害之間有不相當的情況，我們確實需要思考非常高標準規格的 GDPR 是不是我們國家所要邁向的方向？舉例來說，GDPR 第 19 條規定，當事人主張更正或刪除的話，控制者就應該要把這樣的更正或刪除通知每一位接收者，而且如果當事人請求的話，控制者應該告知當事人每一位接收者的身分。意思是我的資料放在你那邊，除了你要幫我刪除或更正之外，我還要知道你在過去的 5 年、10 年曾經看過這個資料的所有人都幫我通知到了，如果你不通知的話，我要知道他們是誰，我自己行使更正權、刪除權、限制處理權。這樣的權利

本報告之智慧財產權歸屬於財團法人資訊工業策進會

擴大，已經擴大到覺得很難實施的程度。

立法制定要有合理性，我們要立法一個法追求的目標必須是合理重要的立法目標，對我們社會是適當而且公平的，在立法的過程當中，也要考慮到執法的成本跟企業遵法的成本，一昧說什麼是最好的個資法，把那個作為圭臬，說這個東西全世界都在往那個方向走，所以台灣也應該跟著走，這樣的說法是沒有經過反思的說法。

C. 與談人國立交通大學科技法研究所副教授陳銘雄發言重點

GDPR 有一個很大的特性，也就是對於新經濟的模式有作出新的規定？而這個東西是過去的個資法裡面所沒有包括，像是大數據裡面所涉到一些特殊的問題。比方大數據研究的目的，往往不容易在蒐集的時候就能夠確定，是先蒐集之後，後來才引發研究的目的，像這種特性，基本上在過去的個資法當中是難以去討論的。所以我們可以預期到，即使不需要達到像歐盟那樣高的標準，但是考慮到新興的科技形態，包括人工智慧、大數據、區塊鏈等等，或許還是必須要對我國的個資法作升級，而我們在升級的時候，勢必還是會參考歐盟的思維方式，這是一個很大的趨勢。

對台灣一個更實際的影響是我們跟歐盟之間的貿易關係，它的域外效應還有一個點是關於跨境傳輸的問題，跟我國個資法最大的差異，我國基本上是原則上允許跨境傳輸，例外才加以限制；但是歐盟的邏輯，這是從過去的保護指令就已經採取的立場，資料原則上是禁止作跨域傳輸，除非那個接收

本報告之智慧財產權歸屬於財團法人資訊工業策進會

國個資的保護程度能夠跟歐盟水準相當。資料到了台灣之後，又跑到第三國去，因為我國採取原則允許的態度，這也是我國為什麼在這一波裡面必須要作很大的調整的關係，因為這樣的規定就很難通過歐盟的適足性認定，我們跟歐盟作資料傳輸的來往就非常的困難。

在這裡我們看到幾個重要的趨勢：第一個，我國最近把個資的解釋機關從本來的法務部移轉到國發會，這表示有意識到需要有個資專責機構的存在。但是從研究個資法的人來看，這還是一個很大的疑問：因為歐盟對於個資專責機構的定義，他必須是一個獨立的機構，而且對於獨立機構有一些清楚的定義，包括人事上的獨立、功能上的獨立、財務上的獨立。國發會最主要的問題是它背負著經濟發展的任務，經濟發展的任務跟個資保護的宗旨有時候會產生利益衝突，另外他必須呼應行政院的政策。這些特性使得他能不能符合歐盟的標準，事實上是有懷疑的。

第二個，歐盟在這邊的思維其實包含一種國家之間競爭的考量，因為在資料經濟這個領域裡面，Amazon、Google、Facebook、Apple 這 4 個企業有點像資料的黑洞，資料進去就跑不出來了。每天不斷從全世界的人民當中吸收各種資料的資料，在未來的世界，例如人工智慧的發展必須要仰賴資料的分析、仰賴資料去訓練機器，這些資料的持有本身會對於國家產業發展的競爭優勢有很大的關聯性。我們要如何去跟這樣的企業對抗？我們自己國家如果想要發展人工智

本報告之智慧財產權歸屬於財團法人資訊工業策進會

慧、想要發展這些資料經濟的時候，我們有沒有什麼樣自我保護的機制？從歐盟的思考來看，是另外一種程度的保護主義，值得需要我們注意。

最後我想要提到兩個相較於新經濟裡面會涉及的議題：第一個，有關於拒絕權的問題，在學理上叫做解釋權。因為在人工智慧或者是電子化自動決策的系統裡面，往往會對人產生一定法律信用影響。人工智慧的發展有很大的議題是有關於演算法，往往是以營業秘密的方式存在。如果這個演算法的結果產生了歧視，很難從外部加以解釋，在美國這樣的事情已經不勝枚舉。歧視可能是程式設計師本身有歧視，或者在無意之間所產生的，另外訓練這個 AI 所用的資料來源也可能會影響到偏見的產生。這就是為什麼要有拒絕權（解釋權），要求當法律的某一個決策對人有影響，而這個決策是透過自動化決策進行的時候，資料的主體有權利要求申訴，有權利要求解釋這個決策是怎麼樣作成的。這對技術的研發會非常重要，表示當你在研發這一類自動化決策系統的時候，必須要保留一定的可能性，要讓機器的決策是可以被解釋的，而這個部分是我國法律的缺口。這個問題隨著 AI 人工智慧在社會上的普及，是我們必須要加以重視的。

另外一個議題是關於被遺忘權的問題，被遺忘權跟我國最大的差異是：我國被遺忘權的例外條款，如果在業務上有必要的時候，就可以不接受當事的請求而不刪除；但是在歐盟的做法，則要求進行某種程度的利益衡量，簡單來說如果當初

本報告之智慧財產權歸屬於財團法人資訊工業策進會

有一個正當的目的，可是後來那個目的不存在，這個時候可能會需要因應當事人的請求而加以消除；但是如果這個目的也不算完全消失，而對方有一個正當的請求時，要去做利益的衡量。

最後提到一個問題，它可能跟區塊鏈會產生一些衝突，因為區塊鏈的概念是去中心化，第一個，它有沒有控管者的概念？區塊鏈每一個節點上，其實每個人的資料都是平等，所以並沒有一個人有比較大的控制權，這個跟歐盟的概念就不太一樣；另外一個解釋方式則是每一節點都是故同控制者，大家都是共同控制這個資料，這也是可能的一種解釋方式。另外一個問題是區塊鏈讓成資料散布各處，要行使被遺忘權以及告知當事人的時候，會比較不一樣，可能是沒有辦法告知當事人，也沒有辦法刪除。在有些方式在討論區塊鏈要如何結合 GDPR，一個解決方式是，個人資料盡可能不要放在區塊鏈上面，變成使用代碼去表示，但這會讓區塊鏈的一些優點喪失掉。

D. 與談人輔仁大學財經法律系助理教授發言重點

在 GDPR 這種架構下，個資變成洪水猛獸，現在全世界運用個資比較多的行業，就是網路服務業、社群媒體，全部都是美國的公司，幾乎沒有歐洲的公司，為什麼會變成這樣子？有美國的學者認為，因為歐盟全方位適用個人資料保護，導致於企業沒有辦法從事這種資料經濟。我們可以看得出來，對個資態度的不同，影響到資訊經濟在全球市佔率的發展。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

如果從產業的角度來看，像美國的資訊服務產業為什麼在全世界所向披靡？因為他們可以儘量開發資訊背後的價值。在法律制度來講，使用者的資料是屬於業者的營業秘密，就是他們的財產權，可以處分。所以要討論一個概念，個人資料是不是財產？是什麼財產權？如果我們把它當作一般的財產權，但他不一定表示可以自由轉讓給第三人。這裡會有商業言論自由跟隱私之間衝突的問題。我們都知道保護隱私是憲法上的權利，那業者權利是什麼？就是有商業言論自由，承認這是他們營業秘密，就是一種財產權，這些其實都是受到憲法的保障。這兩個衝突的時候要怎麼解決？美國討論到很多，包括我們熟知的比例原則、侵害最小原則，他們就去判斷要求明示同意還是默示同意它的合憲性。

GDPR5 月生效，我們政府目標之一就是要申請 GDPR 適足性，現在少部分國家被歐盟認可，可是我們要付出的代價是什麼？保護隱私很棒，因為每個人是消費者，資料也都會被蒐集；可是如果站在國家的整體利益、產業的利益，產業興盛了，民眾生活水準提高、就業率提升，另外一種福祉也會提升。如果要追求適足性，可能就要修改現在個資法到更嚴格，適不適合台灣？這個我們可以來思考。

世界上 200 個國家，可以用個資保護程度分為三群，第一群就是最嚴格，像歐盟，或者是環太平洋的先進國家，像日本、韓國、台灣、香港、澳門、澳洲；第二群就是美國模式，有少部分產業被要求規範；第三群是幾乎沒有，這些國家集中

本報告之智慧財產權歸屬於財團法人資訊工業策進會

在比較貧窮、落伍的國家，或者是宗教國家，像中東。台灣現在已經到達一定的水準，如果 GDPR 所有的東西照抄，對於個人資料的保護、隱私保護是很棒，可是對於產業是不是再繼續扼殺他們的生命？這是一個我們要去思考，因為國家的目的有很多種，滿足個人的需要、產業、政府，整個社會各種利益，要怎麼折衝處理？這是一個蠻大的挑戰。這是我們這個世代大家所面對共同的難題，也要大家傷腦筋。

E. 與談人萬國法律事務所合夥律師洪志勳發言重點

我把我要討論的內容集中在自動演算的領域裡面。在未來整個生活中，資訊系統越來越發達，AI 計算的技術越來越多的時候，人類對於個人隱私權的期待，這種期待可能性我覺得是越來越低，未來整個人的生活裡頭還有身為人的自主性嗎？這大概就是這幾年，無論是整個資訊法制上的設計，甚至在整個個人資料保護法上面的管控，都是一個非常明顯的議題。

根據目前的統計，臉書現在線上的使用者已經達到 20 億人口，大概是全球的 1/4 人口比例，如果把臉書想像是一個虛擬的國家，大概已經控制全球 1/4 的人口。如果這 1/4 人口的思想跟未來生活的需求，都可以透過後端平台的演算法加以控制的時候，從中可以衍生出來的商機，是難以想像的，但相對就必須犧牲這 20 億人口的隱私權的期待可能。日後對於他人格發展方面，可能已經沒有辦法像過往有那麼充分自主性時，這時候是各個政府或許應該適當的反思，無論在

本報告之智慧財產權歸屬於財團法人資訊工業策進會

AI 的管控，甚至在資訊平台技術方面的發展，是不是要稍微適當的控制一下這些業者在背後透過 AI 的演算法，在不知不覺的過程當中，已經從他的使用者截取他所不應該取得的隱私權。

當個資法或者是 GDPR 管的越多的時候，真正有困難的是一般以個人資料為業的服務業者，如何在這樣的科技創新還有個人隱私權保護兩個議題上去取得一個平衡點，這應該是未來整個國家需要著重的地方。

(4) 場次三：他山之石---國際應用案例之介紹與我國之借鏡

A. 主講人景翊科技股份有限公司總經理陳奕廷發言重點

台灣推動開放資料多年，但並非所有資料都有價值，因此企業、政府應該思考如何讓資料真正具備價值。講者首先分享歐盟、日本、美國、新加坡等各地資料應用案例，接著提及資料交換、分享等平台，是我國目前發展所需，意即，資料交換、加值等階段，維護個人對資料之控制、退出為重要的發展方向。

另，觀察日本政府為了發展 AI，AI 需要經資料學習，而資料多來自於政府部門或是民間公司，但民間公司大多不願意把資料釋出，因而開始訂定資料契約的觀念，使得民間公司願意在契約規範之下，將資料交易出來，給予法人、研究單位作相關研究。而研究產出的結果，一種係公司可拿來用，一種是這樣的結果也可以拿來作什麼樣的販售，中間會有相

本報告之智慧財產權歸屬於財團法人資訊工業策進會

關聯的契約部分。因此，透過此種資料契約的模式，可協助運用資料後續，釐清相關當事人彼此權利義務關係。

如果從個人資料資料，再向下發展運用而言，目前看起來，大部分法規係以嚴格的限制保護隱私權、將決定權交給當事人，但並未因此將發展空間都限縮住，事實上仍存在許多空間和可以努力改善的方向。而在現行法規的框架下，應協助企業找到實際具體執行方面的做法，並讓國家對於資料流通的規範，提高監理的機動性跟有效的控管能力。

B. 與談人麟數據科技股份有限公司技術長暨共同創辦人佘志龍發言重點

我們公司業務是數位廣告監測，監測瀏覽資料。我很贊成資料交換的概念，因為在台灣作行銷廣告的部分都在交換，而且也是非常成熟的市場，不需要 IoT，它只需要滑鼠的點一點就可以。在台灣最大收資料的試用者是 Google，各位可以看到我們政府的網站，包括我們的主辦單位跟國家的網站.gov，或是一些民間法人的網站上都有埋一個叫做 Google and laTeX 的 code。但是美國的每一個政府的網站都沒有埋這個 code，因為他認為這個資料是有價值，可以被轉換的、可以被交換的；但是台灣沒有這樣的意識，更不用說我們所在的地方是一個開放的地方，更沒有對岸的資源跟權力。這是需要改變的。

我們公司在做一件事，在把這個知識放在數據搜尋之外，把資料存在自己的家，就是台灣，不會存在只有 Google 的中

本報告之智慧財產權歸屬於財團法人資訊工業策進會

心。我有一個想法是這些資料的交換價值與否、價值與否應該回到大家身上。但是在法規上，我們所蒐集到的資料能用嗎？不能用，台灣有很多像 KTV 的網站、售票的網站，都不敢直接拿資料出來賣，更不要說留下個人資料的這些網站，那更不可能。我覺得有一個問題大家回去思考看看：資料交換有沒有可能應用在行銷的領土？尤其在 Google 這個很成熟的市場，他每天都在用你的使用者、使用行為轉化成他的錢，我們可不可以轉化我們的資料，用國家的角度或是產業的角度，去看待這些資料可以在台灣交換？這是我們要一起想想的。

C. 與談人中研院資訊科技創新研究中心研究員李思壯發言重點

今天代表中央院資創中心的黃彥男主任在這邊討論資料經濟的問題，我們單位名稱是中央院資訊創新研究中心，實驗室名稱是資訊安全實驗室。大概在 3 年前開始，我們除了一般的入侵偵測也慢慢開始涉入隱私的議題？因為資料隱私跟資料保護，看起來也是安全中相當重要的一塊。我們有一個工作團隊，包括技術人員、法律研究所的老師、歐美研究所的老師，他們有一些是公民意識很強的，對於資訊隱私的執著是基本教義派的，跟我們這種比較應用派做技術的人一起交流。以我們中心的立場來看，資料隱私的保護比較不同於基本人權的角度，是從另外一個角度：如果現在越來越多法規在限制個人資料的交換時，有沒有一種技術機制，可以

本報告之智慧財產權歸屬於財團法人資訊工業策進會

讓個人資料的交換，在可以產生價值的同時，又不至於曝露個人的資料？

說明一下我們過去的心得。我們發現在學術的研究上，不管是法律或者是資訊科學的領域，學者們比較追求的是探討什麼是最極端的隱私保護。法律的學者會一直想辦法挑戰我們在做的去識別化或是合成資料的努力，都是不安全的，有一群人很努力做這個事情；資訊科學也有很多老師很吹毛求疵的聚焦在如何從理論上去證明，我有一個機制是 100%安全，而且在任何機率下都不會洩漏。

其實在學術端，資訊科學有很多演算法，法律學門有很多理論，但是一般民眾其實聽不太懂。另一方面，在很多應用端的部分觀察，在跟一般民眾對話的過程中也有發現，有的時候民眾對於隱私洩漏似乎是很在意的。但是，大家可以回想一下，在過去 1 個月裡面，是不是有在任何網站上登錄過我們的真實資料？如果有的話，我們真的有那麼重視隱私嗎？這個東西看起來是一個可以討論的話題。

人是不是可以用一些個人資料去交換一些好處？這件事情，看起來不是那麼牢不可破。以我們這邊的研究來講，我們就是希望透過去識別化、合成資料或者是對資料提供可否認性這些途徑，做一些有限度、可控、可調的保護，讓使用者可以自由去選擇要不要把這個資料放到市場上。甚至是無償、基於一個善心要把這個東西分享出去，都是可以的？但是一定程度上就讓他有一些控制權，這個是我們目前希望透

本報告之智慧財產權歸屬於財團法人資訊工業策進會

過隱私研究能夠達到的目的。

我們作資料隱私的研究比較不是想要達到 100%的保護，因為經過過去 3、4 年來的研究，看起來各個跨領域的學者在研究這個問題的時候，都很同意今天要 100%保護隱私的話，表示洩漏的資料量為 0，只要我講一點點，恐怕就已經有危害隱私的問題。所以我們還是希望應用性比較高的隱私研究是可以促進資料的交換。

D. 與談人理律法律事務所合夥律師曾更瑩發言重點

剛才在報告人的報告中可以看到很多自駕車的案例，我稍微查了自駕車其他國家的法規，本來以為可以查到，可以在不用在個資框架下去做自駕車的實驗？結果世界各國對自駕車都有某種程度的規範，不管是自駕車的實驗或者是責任，裡面提到個人資料或者是隱私權的時候，會重複一遍個資法標準的原則，包括：要透明化、要把自主權交給當事人、在自駕的測試之中要尊重隱私權等。不管是各國的 guideline 或是規定，不管是自律規範或者是汽車聯盟作出來一些業者這些規範裡面，都還是會把個資法傳統整個思考和基本的概念都帶進他們的概念裡面。

如果要從個人資料產生資料，再往下運用的話，目前看起來，全世界的法規至少明文白紙黑字說出來的都一樣：都要嚴格的限制、要保護隱私權、要把決定權交給當事人。這個框架，似乎是沒有任何的突破，雖然大家都覺得數據資料在經濟上會產生很大的效益，不過法規還是很嚴格，還是要從

本報告之智慧財產權歸屬於財團法人資訊工業策進會

一樣的邏輯去走。

再談歐盟，歐盟 GDPR 在個資法的國際傳輸上，法條上也沒有「國際傳輸」這個字，限制的是個人資料傳到第三國或國際組織。第三國就是歐盟以外的地方，所以 GDPR 限制的是個人資料流到歐盟以外的國家，而不是限制「國際傳輸」，這個是第一個觀念。第二個，歐盟從去年開始就有一個草案，非個人資料在歐盟境內的自由流通，在這個草案的規範過程中，歐盟自己有作很多的研究：如果能夠在資料數據上、經濟上的運用，更開放、促進它的流通的話，歐盟的 GDP 可以增加多少。歐盟一直在根據這些研究，寫出一個草案。也就是說，在歐盟境內非個資希望能夠自由的流通，打破資料在地化的概念。不希望歐盟的成員國有電信業者的資料只能放在本國這類的規定，讓非個人資料至少在歐盟境內像這樣資料可以自由流通。大家可以從這兩面可以看得得到歐盟在做什麼，就是希望把資料留在歐盟裡面作應用，去繁榮歐盟的經濟。我覺得大家都有看到資料的經濟，只是大家有各自的做法，台灣要遵守哪一邊？如果我們跟著歐盟這一條路，其實我們就是在他的遊戲規則裡面跑，因為他就是希望所有的東西留在歐盟，當然這個是大家以後要再思考比較大的議題。

E. 與談人資策會數位服務創新研究所專案經理歐雨瑞發言重點

我們是資策會數位服務研究所，我們主要的研究的興趣和領

本報告之智慧財產權歸屬於財團法人資訊工業策進會

域，是在 ICT 裡面的技術，怎麼樣去改造原來的服務樣貌進入我們的生活？進入生活以後這樣服務的體驗要怎麼樣被設計或者是被評估，才是對民眾的生活福祉帶來最高的好處。我們會提出關於影視音、廣告產業的數據應用我們分析的案例的小小心得。

到此為止，以歐盟 GDPR 的推行，假設我們把影視音產業資料轉換成價值這件事拆解來看，再回頭檢視國家層次、企業層次怎麼對應？可以先從目的性來講，影視音產業轉換成價值上，最重要兩件事可能是來自於兩個目的：第一個，影視音的內容怎麼樣更個人化？讓它可以產生更貼近個人、更能夠觸及人力的效果，從而提升影視音產製後續帶來的經濟效應。第二個，透過影視音瀏覽的行為、數據的分析，這種收視通常最大的收益是來自於是廣告，在廣告的面向上，怎麼樣透過影視音的數據去形成一個更有利的指標？去說服廣告主，或者取信於大眾？在這些面向上，又可以從國家層次乃至於到企業實際運用的層次，去看到很多不同的案例，針對這些目的作一些研究跟設計。

以歐盟來講，雖然推行 GDPR 是對於個人隱私權大幅的擴張，可能會帶來更多的限制；另一方面，歐盟也成立一個科研的基金，每年投入相當龐大的經費，在資助各種產學研究。除了影視音以外，也包括醫療、金融，或是一些其他國家監管方向的應用。透過科研基金來補助，是歐洲的業界、學界，共同組織一個題目，再對外徵求其他的法人或者學

本報告之智慧財產權歸屬於財團法人資訊工業策進會

校，去加入這個研究專案。這樣的科研基金在目的性上，一方面著手進行規範，一方面也在探索可能的樣態：有什麼樣新的資料加值應用陽台，是在法規限制之外，或者我有可能要進行調整的？這些可能也會回頭過來影響未來的政策走向。

在個別國家的部份，陸陸續續因為資料流通的本質，開始作一些監理上的機構整併，譬如像英國，現在已經把資料交易的安全跟規範事務，全部整併到文化、媒體、體育的事務部（簡稱 CDMS）。透過這樣的整併，讓國家對於資料流通的規範提高監理的機動性跟有效的管控能力。回到亞洲來看，我們可以看到走得最積極的國家莫過於新加坡，新加坡成立 AI 跟數據的倫理使用的諮詢委員會。因為他們明白：在相關的資料的規範上跟立法，過程必然是漫長，而且落後於企業實際上創新的需求。所以他們先成立這樣的跨產業、跨私人企業、跨政府部會跟研究機構的倫理委員會，研究各種資料加值應用的樣態，是否會有一些倫理上的議題？或者他們會提供一些建議，應該用怎麼樣的模式進行？透過這樣的方式，讓企業也許可以接受他們諮詢先去做事，另外一方面，他們也會回過頭過來建議國家的立法單位該如何修改，所以算是在法規穩定之前，協助企業找到一個實際執行方面的做法。

如果到企業的層次裡面，其實在歐洲也是跑得蠻快的，雖然他們面臨 GDPR 的限制，但他們現在有的企業嘗試用追溯的

本報告之智慧財產權歸屬於財團法人資訊工業策進會

技術和 AI 的方法，協助使用者更有效的追蹤他們的資料怎麼被使用。或是像，歐洲有一個歐洲廣電聯盟，是由 30 幾個國家、50 幾個大型廣電相關的組織形成的。他們是在建立一個跨平台資料交易的機制，要為每個人創造個人化月租的體驗。這樣一個平台目的是為了要從 Google 這樣的國際平台去槍回資料的自主權，留在自家的平台當中。所以串聯這麼多的業者，讓大家在這個平台上，可以彼此在合規的情況下去交易彼此的資料。平台就可以分成三個方向：一個是跨頻道之間交易的機制怎麼樣去進行？一個是資料科學家的運用平台，透過取用平台資料進行各種科學或研究性的目的去研究。第三個，可以透過這樣的一個平台形式一個無縫串聯，不同內容、供應者的機制，每個人進入這些聯盟裡面的內容平台上的時候，可以看到都是符合我個人興趣內容的組織。在歐盟看到，都已經有各種不同的公立或私立組織嘗試在合規的框架下去做資料的交換跟加值應用。我們研究進行到現在來看，倒也不覺得大家會因為這樣子空間都被壓縮了，事實上還看到相當多空間跟可以努力的方向。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

參、研析及規劃參與國外通傳事業資料利用機制

一、觀測與實地考察他國資料加值創新應用相關法制規範資訊

(一)參與英國 IAPP 2018 歐洲資料保護密集研討會

1. 簡述

本計畫參與今年 4 月於英國倫敦舉行之「IAPP 2018 歐洲資料保護密集研討會」（IAPP Europe Data Protection Intensive 2018），該研討會係由全球最大的資訊隱私專業社群「國際隱私專業人員協會」（International Association of Privacy Professionals，以下簡稱 IAPP）所舉辦，是 GDPR 施行前夕歐洲最重要的隱私相關座談會。本計畫藉由參與 IAPP 2018 歐洲資料保護密集研討會及倫敦當地兩場針對當地企業之說明會、工作坊，希望能了解歐盟會員國個資主管機關因應 GDPR 施行所作之準備及其對 GDPR 之預期、了解歐洲實務界及學界對於 GDPR 發展之看法，同時透過觀察英國倫敦在地企業因應 GDPR 施行之態度，折射出 GDPR 施行後可能之狀態。

此次赴英國參訪，主要針對下列議題進行觀測：歐洲各個資主管機關應對 GDPR 之作法、ePrivacy Regulation 之動態、拒絕權、被遺忘權與資料可攜權等新興權利之發展、個人資料處理合法權源之轉向（同意及「合法利益」（legitimacy interest）之爭）、APEC 地區個人資料保護之發展、GDPR 未竟之處、當地企業準備狀況與新創因應之道。最後則建議：針對 GDPR 施行，國內企業應調整作法，但不須太過慌張。同時，針對正在發展中的規範內容臺灣企業或可積極參與其內涵形成（如資料

本報告之智慧財產權歸屬於財團法人資訊工業策進會

可攜權等)。最後則是認為，ePrivacy Regulation 及 GDPR 都有須持續觀察之處。詳細之英國出國報告請參考附件二。

2. 重要內容

(1) 歐洲各個資主管機關應對 GDPR 之作法

從歐洲各主管機關在本次會議中的發表可以發現，各國主管機關面對 GDPR 的施行，在組織與員額上都有所擴充，並投入相當資源擬定適用的指引供大眾遵循。同時，從英國資訊長以及愛爾蘭個資主管機關代表的發言可以發現，資料外洩通報的運作或許是其中一個特別受到重視的要素。在未來，歐洲許多主管機關計畫持續進行教育與輔導各個企業符合 GDPR 的規範。在管理方式上，與臺灣輿論上普遍強調 GDPR 的高額罰鍰不同，各國主管機關其實並不特別強調高額罰鍰，而是更實際的強調 GDPR 中其他的管制措施或許會更常被主管機關使用。換言之，各國主管機關可能會透過 GDPR 賦予的權利，透過各種管制手段直接介入資料控管者或處理者處理資料的內容，而非消極的僅以處罰的方式來處理。

(2) ePrivacy Regulation 之動態

ePrivacy Regulation 的發展仍為會場許多參與的人士所關心，不過從英國政府及歐盟執委會代表的發言來看，歐盟理事會內部對於 ePrivacy Regulation 的內涵尚有許多需要討論，可能不會迅速的通過。而 ePrivacy Regulation 在歐盟理事會通過後，仍需要經過歐盟理事會、歐盟議會與歐盟執委會三方協商，才能正式通

本報告之智慧財產權歸屬於財團法人資訊工業策進會

過。因此，我們可以很篤定的認為 ePrivacy Regulation 勢必不可能在 GDPR 前正式實施。

從另外一個角度來說，ePrivacy Regulation 此前所通過的歐盟執委會及歐盟議會兩個版本已經有所歧異，在歐盟理事會討論後，勢必會有另一版本的出現，未來三個版本的差異，如何調整值得繼續觀察。而如同前述，在本次會議討論的過程中，已經可以發現 ePrivacy Regulation 草案中擴張適用範圍後，仍有一定程度的模糊地帶，對於這些範圍定義的釐清，以及各種 cookie 如何管制，或許將是未來討論的重點。

(3) 拒絕權、被遺忘權與資料可攜權等新興權利之發展

在 GDPR 加強、成文化或新增的各種資料當事人權利中，拒絕權與被遺忘權雖然在落實上尚有許多挑戰需要克服。但與會的專業人士與講者普遍認為實行上可能面對的最大困難應該是資料可攜權的內涵。包含應該如何統一資料格式、資料欄目如何對應等問題，在 GDPR 即將施行的現在，其實還沒有清楚的答案。而主管機關似乎無法，也不可能直接擬定相關的細節。因此，對於資料可攜權的實質內涵以及實務做如何進行，仍有待持續相關行業類別內部，持續討論與合作，才能逐步形成實質的內涵，也更值得我們繼續加以觀察。

(4) 個人資料處理合法權源之轉向：同意及「合法利益」（legitimacy interest）之爭

本報告之智慧財產權歸屬於財團法人資訊工業策進會

隨著「同意」的要件在 GDPR 內變得更加的嚴格，在本次會議的多場討論中，與會者紛紛討論到未來資料控管者與處理者可能將更重視「以合法利益為由處理個人資料」的途徑。部份學者與隱私相關的業者認為，若搭配假名化技術降低對當事人可能的隱私衝擊，以合法利益作為合法處理個人資料的權源可能作為許多企業在為來處理個人資料的方法。然而，也有部份講者認為，由於合法利益須與資料當事人的隱私權利加以權衡，這種權衡的損益過程存在一定程度的不確定性，因此在實務上考慮可能面臨的訴訟或爭議，這種處理方式仍然存在一定的風險，值得業者加以注意。

(5) APEC 地區個人資料保護之發展

亞洲地區或許因為文化背景的關係，或是發展程度的差異，個人資料保護制度存在高度的歧異性。這種的差異將使在亞洲地區展開跨國營運的業者增加實務工作的困難性。

目前 APEC 雖然有 CBPR 的制度，但此一制度發展已久東南亞許多國家仍未能加入，能發揮的功能或許仍然有限。我國目前正積極想要加入 CBPR 體系，新加坡做為最近一個加入 CBPR 的國家，其處理方法值得我們注意。未來，新加坡將要決定要以哪個單位申請成為 CBPR 的 AA。與此前傳出的消息不同，新加坡可能不會以個資主管機關申請，而會以非政府組織加入。新加坡的相關動態，可能在六月時會有更多資訊出現，值得留意與重視。

(6) GDPR 未竟之處：資料由控管者轉移至控管者

本報告之智慧財產權歸屬於財團法人資訊工業策進會

如同前面的討論，GDPR 對於資料控管者間資料的轉移並未有所規範。然而，當前討論的沸沸揚揚的 Facebook 與劍橋分析公司間的爭議，就是資料控管者間的轉移。透明性與資料傳遞者對於傳遞對象的監管這兩個項目，是目前討論中認為在這種資料移轉關係中最需要的條件。未來歐盟各主管機關會如何填補 GDPR 在這裡的規範空白，是否會參考 HIPAA 資料分享協議的相關規定，值得我們繼續加以觀察。

(7) 當地企業準備狀況與新創因應之道

本次報告人特別參與兩個當地針對小型企業所作的 GDPR 說明會或工作坊。從會議中與會者的討論來看，許多小型業者對於 GDPR 的施行仍然感到焦慮，甚至尚未因應 GDPR 的施行進行工作流程的改變。因此，即便許多歐洲的個資主管機關認為已經做了許多的宣導與指引，應該可以順利的過渡到 GDPR，但短時間內許多業者應該尚無法完全符合 GDPR 的要求，一定程度的混亂與銜接應該是可以預期的。

此外，從這類小型座談會中，我們也可以發現歐盟內部對於 GDPR 的了解還存在差異。例如其中一場的主講人在說明 GDPR 的適用範圍時，就認為 GDPR 的判斷標準應該是資料當事人的「國籍」(nationality)；然而 GDPR 強調的其實是針對「在歐盟境內的資料主體」，國籍應該不是重點。從這種小地方的差異可以佐證上判斷，在 GDPR 正式施行後，這些誤解或認知上的差距才會逐漸突顯，因此短期間內歐盟境內應該還是會有一段逐漸

本報告之智慧財產權歸屬於財團法人資訊工業策進會

適應的過程。

最後，這類小型最談會也提供了小型業者實際的因應手段。大英圖書館的講者特別建議小型或新創業者可以利用大型雲端企業提供之服務，如 Google 或 Dropbox 等服務來管理自己所保有的個人資料，因為這類大型企業提供的服務已經符合 GDPR 的規範要求。這種處理的方法對於歐盟個資數量不多的一些臺灣企業而言，也具有一定的參考價值。

(二)參與美國隱私與安全論壇

1. 簡述

本計畫參與於 10 月赴美國參與「隱私與安全論壇」（Privacy + Security Forum），論壇之內容包含隱私保護之法律政策與實務作法、目前國際所關注之隱私議題與發展趨勢，以及目前新興科技應用下所衍生之隱私保護等相關議題，並透過參與論壇第一日舉辦的座談會（Workshop），瞭解美國聯邦貿易委員會（Federal Trade Commission, FTC）對於隱私保護所採取之相關政策與措施，作為我國相關政策之參考。本次考察之效益，即為瞭解目前國際上 GDPR 相關遵法之經驗，並藉此瞭解目前美國、歐盟及其他國家相關隱私或資安法規領域最新之發展動態。本次考察亦可瞭解目前各國產業界因應 GDPR 以及準備相應遵法措施之經驗，並瞭解目前國際上對於隱私保護及資安之趨勢以及所面臨之困境。另於新興科技之發展上，人工智慧的應用日趨普遍，本次考察亦可瞭解其所衍生新的隱私或資安風險，以及可能面臨的相關法制問題，藉此汲取各界隱私與資安專家之經驗，作為未來我國政策規劃之借

本報告之智慧財產權歸屬於財團法人資訊工業策進會

鏡。

綜整此次參與論壇之經驗，目前國際上關於隱私保護之議題，主要仍聚焦在 GDPR 相關制度或措施之接軌或因應，而對於隱私保護之新興議題，則圍繞在 AI 人工智慧的應用上。詳細之美國出國報告請參考附件三。

2. 重要內容

(1) 隱私法制部份

歐盟 GDPR 雖於已於今年 5 月實施，然各國仍然處於調適之階段，企業部分亦嘗試不同之新興作法（如資料大使館），以達到 GDPR 之相關要求，故在此趨勢下，隱私相關之顧問諮詢企業（如 DataGuidance、OneTrust、 NYMITY、radar 等），亦依據法規之規範發展出不同之法遵流程措施提供參考，而相關隱私法規資料庫的建立及法遵系統，亦相當詳盡豐富，可見目前國際上對於個人資料隱私保護之趨勢，已朝向建立系統流程化之法遵管理方式。

在法規面上，各國之隱私法制有漸進調整之趨勢，GDPR 之部分內容逐漸為國際間所採納，故本屆論壇部分內容即針對目前各國之隱私法制為討論主題，如美國加州於今年 6 月所通過之加州消費者隱私法（California Consumer Privacy Act, CCPA）、韓國、加拿大之隱私法規等。整體而言，國際上對於隱私保護之法制架構，因 GDPR 之影響，產生了漣漪之效應，各國企業雖不見得

本報告之智慧財產權歸屬於財團法人資訊工業策進會

適用 GDPR 之規範，然卻逐漸提升了其隱私保護之水平。

此外，論壇之另一討論重點在於各國隱私法制間之調和，目前國際上部分國家係參考 GDPR 之相關規定而調整國內之隱私法規（如日本、韓國），並希望藉由取得歐盟之適足性認定，使其得以自由地與歐盟進行個人資料之跨境傳輸，部分國家則以協議之方式為之（如美國隱私盾協議）。而企業因應國際間不同之隱私監管法制，多以尋求隱私顧問諮詢企業或專業協助之方式為之，透過隱私專業人員之協助，以遵循當地之隱私保護法制措施。故可以想像，將來對於隱私保護之專業人才之需求將大幅提高，而我國則可考慮對於隱私專業人員進行有計畫之培訓，以因應將來隱私保護之趨勢。

(2) 隱私新興議題

在新興科技的隱私議題上，人工智慧為目前較為熱門之討論。特別是人工智慧應用之部分，如自動駕駛、健康資料等所衍生之隱私保護問題。

目前雖已開始討論人工智慧相關之法制建置、隱私保護及風險預防等面向，但就法制而言仍未能有一全面之架構，相關之法律框架及責任規範仍於討論中，本次論壇雖有多場議題與人工智慧有關，但多為提出可能之思考方向或可採行之建議或作法，具體架構及內容則尚未成形。然於人工智慧的深度學習過程中，涉及與隱私保護之衝突與挑戰，相關之思考方向及討論，仍可作為我國人工智慧發展之參考。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(三)參與日本 Gartner 研討會與 IT 應用展示

1. 簡述

本計畫於 107 年 11 月 11 日起赴日本東京，進行為期 5 天之考察。本次考察行程安排參加 Gartner 於東京舉辦的研討會與 IT 應用展示（SYMPOSIUM/ITXPO），該研討會之內容包含未來的關鍵科技趨勢與糙略，可作為我國相關政策之參考。本次赴日參加 Gartner 所舉辦的研討會，不只可了解以資料經濟為基礎之科技趨勢，同時也能就重點科技進行深入的探討，對於我國未來通傳產業資料加值應用的實務運作，能有更清楚的架構跟研析方向。

綜整此次參與研討會之心得，人工智慧是目前國際上最關心的議題，其也牽涉相當多的法律爭議。專家認為，我們目前並非在人工智慧的時代，而是處在學習的時代，一個新興數位的社會。相較於設定許多的原則，訂定自我的人工智慧倫理較為實際，尤其是將數位倫理運作立於設計的基礎。在風險管理方面，專家將其視為支持人工智慧創新的關鍵要求。允許接受風險是一個合法的商業決策，但是只有在做出理性決定時才能接受風險。另外，利用相對成本和風險緩解的可預測性來平衡風險，同時也要在評估中考慮風險規模。詳細之日本出國報告請參考附件四。

2. 重要內容

(1) 2019 年的 10 項科技趨勢

本報告之智慧財產權歸屬於財團法人資訊工業策進會

此次研討會特別針對 2019 年的 10 項科技趨勢進行介紹，簡略概述如下：

A. 自動化物品（Autonomous Things）

自動化物品從形式上可區分為機器人、車輛、無人機、家電與媒介平台，這些自動化物品將涵蓋路、海、空與數位領域，但是依據其技術的核心內容又可區分為三個不同的層次，包括性能、協作與智慧。

其中性能的強度由弱到強，分為人類協助者、部份自動化、有條件的自動化、高度自動化與全自動化。而協作的部份，由弱至強則分為隔離性質、具有獨立性、可連線的與共同運作。最後在智慧化的部份，由弱至強分為靜態的、半智慧化與動態的、獨立智慧化與動態的以及透過多工智慧化模式的動態蜂巢式互動。

B. 人工智慧（Artificial Intelligence, AI）導向的發展

依據 Gartner 的專家報告，預估到了 2022 年，至少有 40%的新應用發展計畫會納入人工智慧，來進行合作開發的任務。目前人工智慧分為四種型態，分別是人工智慧服務、人工智慧平台、人工智慧架構、人工智慧基礎建設。人工智慧服務包含了影像處理、語言處理、對話、知識服務、顧客型態等；人工智慧平台則主要為機器學習，諸如 Amazon、Microsoft、Google 與 IBM 都有進行研發；人工智慧架構則是以協助開發程式為主，諸如 Google 的 TensorFlow、Facebook 的 Torch

本報告之智慧財產權歸屬於財團法人資訊工業策進會

等，都屬於此種類型；而人工智慧基礎則重點在於去伺服器化的開發，例如 AWS Lambda、IBM 的雲端功能、Google 的雲端平台以及 Microsoft 的 Azure AI。

C. 數位雙胞胎（Digital Twin）

數位雙胞胎意指物件或系統的多元軟體模型，借助感測器來理解標的物件或系統的真實處境，讓使用者能精準快速地反應各種變動情況，從而改善物件或系統的的操作，或增添其附加價值[178]。數位雙胞胎的核心功能在於模式建立、資料蒐集、監控、分析與模擬，這些功能建立在資產資料、運作資料、控制的基礎上，尤其對於製造業的影響甚大。

D. 加強的邊際運算（Empowered Edge）

儲存、運算及進階的人工智慧與分析能力，將會在 2028 以前增進邊際運算設備的能力。另外，Gartner 的專家也指出，當邊際運算設備與 5G 這樣的基礎網路設施結合後，未來 5-6 年之間將創造出更快的速度、更少的遲延與更大的密集度，有利於邊際運算設備的發展。

E. 實境體驗（Immersive Experience）

實境體驗將會促進互動模式的改變，並且加強系統對人類，人類對系統的學習與適應能力。尤其可用在訓練與模擬、行銷、零售、虛擬設計、工作場合等，目前的智慧音箱也是實

[178] 「妙用 Digital Twin 加速驅動智慧轉型」，DigiTimes，2017.09.06. available at https://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&cat2=10&id=0000510929_m19llbtk1778a9lkqa178 (last visited Nov. 17, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

境體驗的一種模式。未來虛擬體驗的開發將不限於視覺，甚至包含聽覺、味覺、觸覺與冷熱感等。

F. 區塊鏈（Blockchain）

專家預估到了 2030 年，區塊鏈技術可創造 3.1 兆的商業利益。區塊練主要有兩個主要能力，一是區塊鏈帳本，另一則是選擇性的特色。

區塊鏈帳本的功能在於分享數位資產、加密化與分散式、不可改變及可追溯的紀錄以及去中心化的運作機制。而選擇性的特色在於智能合約、中央式管理、控管存取與更新、替代的共識機制。目前區塊鏈技術主要應用在貨物運送、電子健康紀錄、數位貨幣與不受限制的交易市場等。

G. 智慧空間（Smart Spaces）

智慧空間可以是實體或數位的環境，主要在於促進人機在互動、智能、自動化的科技上的結合。智慧空間的模式主要有四個階段，第一階段為獨立的無互聯的系統，侷限於團隊的共用；第二階段則是連結的系統，適合部門內部使用；第三階段則為共同運作的系統，具有半人工智慧的特點，適合組織內部使用；第四階段為人工智慧環境，是一個開放、互聯、共同合作、人工智慧的環境，適合生態系統模式。智慧空間未來對於連結工廠與數位供應鏈有很大的幫助，甚至可擴大為智慧城市模式。

H. 數位倫理與隱私（Digital Ethics and Privacy）

本報告之智慧財產權歸屬於財團法人資訊工業策進會

有鑑於未來將有上億的端點在蒐集資料，包括識別個人（臉部辨識、語音辨識、DNA、虹膜、指紋）、個人位置（GPS、行動電話追蹤、授權的多功能盤測儀、IP 位置、建築物保全）、個人行為（活動、心律、睡眠、血壓、血糖、行車偏好）及個人想法（搜尋引擎、社群網站、超級 cookies、智慧麥克風、電子郵件）。

與會專家認為，在數位倫理的議題下，應該從法遵導向轉為倫理導向，並據此做出對的決定並且創造價值。這樣的轉變分為內部導向與外部導向。內部導向包含了追求你的價值與創造特殊性，其中價值包含了自我詢問這是否是對的事情？如果這樣的事情可行與被允許，但是是否是我們所想要的？另外在特殊性的部份則是數位倫理是否為價值主張的一部分？這是否可使自身有特殊性？外部導向的部份，則在於減輕風險與法遵的部份。風險的部份在於是否有聲譽上的風險？或是所創造的產品或服務會傷害其他人？而法遵的部份則在於自身是否違反了相關法規？

I. 量子運算（Quantum Computing）

量子運算是一種非典型的運算型態，能夠大量增加運算能力，主要目前運用的案例在於優化問題、材料科學、化學、個人化醫療以及生技。

J. 秒速間找到同時發生之資料的不知名連結（Finding Unknown Correlations for Crop Yield-In Seconds）

本報告之智慧財產權歸屬於財團法人資訊工業策進會

透過人工智慧、資料聚集與操作，從大量資料中擷取到所需要的資料來進行分析，以色列的 SparkBeyond 公司即以此技術為主要產品與服務。

(2) 2019 年十大基礎架構與營運（I&O）趨勢與技術衝擊

2019 年與基礎架構與營運相關的趨勢與技術衝擊，包含無伺服器的運算、人工智慧衝擊、資料中心的終結、網絡的敏捷度、邊際運算、數位多元化的管理、基礎架構與營運的新角色、SaaS 技術的抵制、人才管理成為核心任務與全球化基礎建設之可行性。

其中在人工智慧的部分，根據每日新聞調查，121 個接受調查的日本公司中，有一半已經推出或計劃進行將人工智會導入他們的一些操作中。

三菱電機集團和麒麟控股將開始使用人工智慧進行研究，計畫將經驗豐富的員工的商業知識作為學習對象，未來人工智慧可能會負責複製精密光學零件的技能和任務，或是用於掌握啤酒釀造工藝。另外，人工智慧最主要的影響在於工作機會的減少，以日本為例，主要保險提供商表示，人工智慧可以取代數十名員工的工作，日本三井物產（Mitsui＆Co。）表示，人工智慧有削減少數人的工作的效果。許多接受調查的公司沒有表是人工智慧的引入是否會導致員工人數減少。但是有兩家公司透過人工智慧的導入，提出了減少人工負荷的具體數據。大日本印刷公司導入人工智慧後，相關用來檢查打印缺陷和其他任務得以移轉到人工智慧

本報告之智慧財產權歸屬於財團法人資訊工業策進會

系統上，相關的員工人力大約減少 20 名員工，因此讓公司人力資源盈餘。日本保險公司 Fukoku Mutual Life Insurance 導入 IBM 的 Watson Explorer AI，因而多出 34 名員工的員額，員工勞力被機器取代即將成為未來趨勢。

(3) 管理人工智慧的風險

依據 Gartner 的調查，人工智慧未來會成為重要核心技術的原因在於促進能力、顧客體驗、因自動化所省下的成本等。然而，針對人工智慧的挑戰調查，其中占最高比例的疑慮在於資安與個資保護的議題上。

從資訊技術組織的層面切入，人工智慧可能會透過以下方式損害企業系統：

- 缺乏可稽核性：黑盒算法使企業無法追踪或解釋為什麼人工智慧應用的結果。
- 管理不善：人為疏忽導致對客戶或其他人的傷害。
- 不可預測性：人工智慧應用程序被編程或進行學習和適應環境後，在開始後以不可預見的方式發生變化，產生有害影響。
- 互動：不同的人工智慧應用程式進行互動並改變彼此的編程，而帶來有害後果。

從企業的觀點來看，人工智慧可能會透過以下方式損害企業品牌或其他資產：

本報告之智慧財產權歸屬於財團法人資訊工業策進會

- 不倫理的活動：人工智慧應用程序的編程沒有符合人類的目標和社會規範。
- 技術依賴：人工智慧應用程序的故障影響商業營運。
- 從環境的觀點來看，可能從外部的因素造成損害：
- 經濟影響：由於自動化取代高科技人力，因此將造成大規模失業。
- 監控：可以不斷調整對策的人工智慧應用程序，可收集有關個人和公司的資訊。
- 惡意人工智慧：可以對應用程序進行編程以執行破壞性操作，例如，發動永久性網絡攻擊的程式。
- 超級智慧：人工智慧應用程序達到人類智慧和自治水平，此將使人工智慧無法受到控制。

基本上 Gartner 提供的人工智慧風險對策包括投資控制措施以管控風險、進行保險以轉移風險與選擇接受風險。專家特別將風險管理視為支持人工智慧創新的關鍵要求。允許接受風險是一個合法的商業決策，但是只有在做出理性決定時才能接受風險。另外，利用相對成本和風險緩解的可預測性來平衡風險，同時也要在評估中考慮風險規模。

(4) 人工智慧與倫理議題

人工智慧出現後，相關的倫理議題陸續出現，包括失業、不平等、

本報告之智慧財產權歸屬於財團法人資訊工業策進會

人性、人工智慧故障、偏見、安全、不可預測的結果以及控制等問題。與會專家提出了人工智慧應該被思考的治理原則，分述如後。

A. 機器學習悖論

人工智慧學習的最佳狀態，是使用現實世界的資料去創造有彈性的模式，但是這個前提是建立在這個彈性是在現實世界中所需要的功能。

B. 準確性困境

先進的學習科技應該會產生更準確的結果，但是如果過程不透明，所產生的結果也會難以解釋。

C. 接受的難題

人工智慧只有在了解或運算出人類想法時才會被接受，但是這樣的結果可能是充滿與吊詭的。

Gartner 專家建議，可以在資訊治理、分析治理與人工智慧治理帶入不同的要素。在資訊治理的層次，建立信認識最重要的，而在分析治理的層次，則是信賴加上透明度，至於在人工智慧的層次，則是信賴、透明度加上多樣性。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

二、研析歐盟隱私及電子通訊規則（ePrivacy Regulation）草案

(一)草案之背景

歐盟執委會在「數位單一市場戰略」（The Digital Single Market Strategy）的引領下，近年來展開對歐盟境內法令的翻修工作，今（2018）年 5 月剛剛正式實施的 GDPR 及為歐盟執委會在此一戰略下之修法行為。除了 GDPR 外，歐盟執委會亦在此一戰略下針對現行的電子通信隱私指令（Directive 2002/58/EC on Privacy and Electronic Communications, ePrivacy Directive）展開修法作業，其於 2017 年 10 月時提出正式的修法草案，計畫將原先須由各會員國自行立法轉化之 ePrivacy Directive 提昇為歐盟隱私及電子通訊規則（Regulation on Privacy and Electronic Communications，以下簡稱 ePrivacy Regulation），以確保其保護之標準與 GDPR 一致[179]。

在完成草案前，歐盟執委會先針對 ePrivacy Directive 展開「規範適合性與表現計畫」（Regulatory Fitness and Performance Programme）審查，結果認為指令的建構的框架之目標、原則仍屬合理[180]。然而，歐盟執委會也發現，自 ePrivacy Directive 於 2009 年修至以來，「OTT」（over-the-top）的通訊服務大量興起，消費者與企業越來越依賴以網路為基礎的新服務，例如即時訊息、網路通訊、電子郵件等；這些服務通常不受 ePrivacy Directive 的規範；因此有必要修改相關規定，將這些新服務的通訊納入

[179] Commission Proposal for a Regulation of The European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), at 1, COM (2017) 10 final (Jan. 10, 2017).
[180] *Id.*

本報告之智慧財產權歸屬於財團法人資訊工業策進會

保障的範圍之內[181]。

ePrivacy Regulation 草案與 ePrivacy Directive 的差異大致上可以分為下列幾個重點：

首先，將原先的指定改變為規則，可以齊一歐盟境內各國個人與法人電子通訊隱私所受到保護的水準，同時企業也有更統一的規範可以遵循[182]。

而在組織上，ePrivacy Regulation 草案將其落實的情形委由各國的「個資保護機關」（Data Protection Authorities）負責執行，預期將可以使執法更加有效[183]。

至於在實質規範面上，ePrivacy Regulation 草案為了保障歐盟人民的電子郵件及線上消息的隱私，將這些新的電子通訊服務提供商，例如 Gmail、WhatsApp、Facebook Messenger 等納入規範範圍[184]。

此外，對於通訊的內容及「詮釋資料」（metadata），ePrivacy Regulation 草案規定若未經過用戶之同意，此類資料僅能在計費目的下使用，否則就應將資料刪除或「去識別化」（anonymised）[185]。

而在垃圾郵件或訊息的防止上，ePrivacy Regulation 草案禁止任何未

[181] *Id.* 請參考原文：Consumers and businesses increasingly rely on new internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and web-based e-mail services, instead of traditional communications services. These Over-the-Top communications services ("OTTs") are in general not subject to the current Union electronic communications framework, including the ePrivacy Directive.

[182] Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions, European Commission, http://europa.eu/rapid/press-release_IP-17-16_en.htm (last visited Aug. 1, 2018).

[183] *Id.*

[184] *Id.*

[185] *Id.*

本報告之智慧財產權歸屬於財團法人資訊工業策進會

經請求的電子通訊，包含電子郵件、簡訊等內容[186]。

最後，ePrivacy Regulation 草案則針對 cookie 的規範有所簡化；其要求服務提供者提供簡便方法方便使用者接受或拒絕被 cookie 或其他類似技術追蹤；但若是不涉及隱私侵犯的 cookie（例如記錄購物網站購物車內容的 cookie、計算網頁訪問數量的 cookie）則不需要使用者同意，以改善網路服務體驗[187]。

(二)草案之最新發展情形

2017 年 1 月 10 日，送交歐盟議會及歐盟理事會依照一般立法程序進行審理，目前草案政由歐盟議會及歐盟理事會分別審理中[188]。

1. 歐盟議會審理情形

歐洲議會將草案交由「公民自由、司法暨內政委員會」(Committee on Civil Liberties, Justice and Home Affairs）審理，同時「環境、公共衛生暨食品安全委員會（Committee on Environment, Public Health and Food Safety)、「產業、研究暨能源委員會」(Committee on Industry, Research and Energy)、「內部市場消費者保護委員會」(Committee on Internal Market and Consumer Protection）以及「法規委員會」(Committee on Legal Affairs）亦將提供意見，嗣後環境、公共衛生暨食品安全委員會決定不提出意見，其餘三個委員會於 2017 年 10 月 4 至 6 日間陸續提供其意見，公民自由、司法暨內政委員會於 2017 年 10 月 23 日提交審

[186] *Id.*
[187] *Id.*
[188] Procedure 2017/0003/COD, EUR-LEX, https://eur-lex.europa.eu/legal-content/en/HIS/?uri=CELEX:52017PC0010 (last visited Aug. 1, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

理報告，送交大會等候「一讀」（first reading）程序[189]。

公民自由、司法暨內政委員由社會主義者和民主人士進步聯盟黨團議員 Sippel Birgit 擔任報告員，負責報告草案的起草，委員會內其餘黨團（包含歐洲人民黨黨團、歐洲保守派和改革主義者黨團、歐洲自由民主聯盟黨團、歐洲聯合左翼及北歐綠色左翼黨團、綠黨及歐洲自由聯盟黨團、民族和自由歐洲黨團）也都指派影子報告員表達意見[190]。

公民自由、司法暨內政委員提交給大會的報告對於 ePrivacy Regulation 草案修正的意見主要可分為以下 7 個面向：

(1) 範圍：委員會認為草案的範圍應包含：處理與終端使用者的終端設備有關或由該終端設備處理的信息、允許電子通訊的軟體；提供公開的電子通訊用戶目錄之服務；向終端使用者發送直接行銷之電子通訊的情形[191]。

(2) 通訊保密性：委員會建議草案應將與終端設備有關或由終端設備處理之資料納入電子通訊保密性的要求中，意即電子通訊網路和服務提供者僅在完成訊息傳輸有技術上必要的情況下，在維持該目的所需的時間內才可以處理電子通訊資料[192]。

(3) 保護儲存於使用者終端設備中或與其終端設備相關的訊息：為確保保護程度與 GDPR 相仿，委員會認為：應確保使用者同意的

[189] Procedure File: 2017/0003(COD), European Parliament, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en#tab-0 (last visited Aug. 1, 2018).
[190] *Id.*
[191] 2017/0003(COD) - 23/10/2017 Committee report tabled for plenary, 1st reading/single reading, European Parliament, http://www.europarl.europa.eu/oeil/popups/summary.do?id=1508613&t=d&l=en (last visited Aut. 1, 2018).
[192] *Id.*

本報告之智慧財產權歸屬於財團法人資訊工業策進會

條件與 GDPR 相同；不論是否收費，都不得在終端使用者拒絕提供非嚴格必要的資料的狀況下，拒絕其使用「資訊社會服務」（information society service）：在僱用關係下，雇主只有在執行員工任務有技術必要的狀況下才可以近用使用者之終端設備，並不得進一步用於監控員工[193]。

(4) 隱私設定選項：委員會認為草案應避免設立所謂的「cookie 牆」或「cookie banner」等無助於用戶保持對其個資及隱私控制及告知其權利的機制[194]。

(5) 電子通訊軟體義務：委員會認為此類軟體（包含瀏覽器、操作系統和應用程式）應該設置隱私保護的機制，並預設禁止第三方在終端設備上追蹤和儲存訊息，其應提供詳細選項，允許使用者針對不同類別給予不同的設定，並使其可以選擇在安裝後隨時更改或確認其隱私設定；同時，委員會認為這類軟體應設計一種訊號用以通知第三方用戶的隱私設定[195]。

(6) 用於直接行銷的未經請求之通訊：對於此類的通訊，應僅限於對事先同意的用戶使用，並應禁止發送這類通訊時隱蔽身份或使用虛假身份[196]。

(7) 對通訊秘密的保護：委員會對通訊秘密之保護應限於民主社會中必要且符合比例性的措施，包含國家安全、國防及公共安全等之

[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] *Id.*

本報告之智慧財產權歸屬於財團法人資訊工業策進會

維護[197]。

歐洲議會尚未完成草案的一讀程序，而是在 2017 年 10 月 26 日時決議將進入跨機關協商的階段[198]。

2. 歐盟理事會審理情形

歐盟理事會已經針對此一草案展開至少 30 餘次的討論[199]，並兩度舉行辯論[200]，但迄今尚未完成一讀程序。歐盟理事會輪值主席曾於今（2018）年 5 月時針對討論情形出具進度報告[201]。根據該報告，理事會目前主要聚焦討論以下內容：

(1) ePrivacy Regulation 之範圍及與 GDPR 之關係

主要爭論之焦點在電子通訊內容之保護上，尤其是 ePrivacy Regulation 保護與 GDPR 如何銜接；對此主要的討論是如何一方面清晰的規範，一方面同時可以遵守技術中立的要求[202]。

(2) 電子通訊資料（內容及詮釋資料）之處理

管制範圍擴大至包含處理有關安全性風險的行為；就此部份目前

197 *Id.*
198 *Supra* note 189.
199 *Supra* note 188.
200 *Supra* note 191.
201 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Council of the European Union, http://data.consilium.europa.eu/doc/document/ST-9079-2018-INIT/en/pdf (last visited Aug. 1, 2018).
202 *Id.*, at 3-4.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

已經取得共識，但仍有文字細節須處理[203]。

(3) 電子通訊詮釋資料之處理

對於如何平衡詮釋資料之資料安全保護與創新需求，各國仍未完全取得共識；目前有可能新增數項電子通訊詮釋資料處理之合法依據[204]。

(4) 終端設備資料之保護

各國對於隱私保護與合法商業模式間之平衡仍有爭論；目前各國討論的結果是其大致的架構仍會維持，但可能對例外許可蒐集資料的情形做出新的規定[205]。

(5) 隱私設定

目前最新的修正是僅要求軟體提供者須於安裝、第一次使用或更新隱私設定時，告知使用者相關內容及使用之方式[206]。

(6) 資料保存相關之規範

排除國安及國防相關之活動，並新增公共利益相關之規定[207]。

(7) 通話之限制與說明、連線識別以及近用緊急服務之例外

[203] *Id.*, at 4.
[204] *Id.*, at 4-5.
[205] *Id.*, at 5.
[206] *Id.*, at 6.
[207] *Id.*, at 6-7.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

增加在緊急情形下，終端的用戶不得拒絕隱藏識別資訊的連線，以及允許在緊急通訊的情況下近用用戶之終端設備以取得位置訊息[208]。

(8) 公眾可近用之目錄

對於以號碼為基礎的人際傳播服務（number-based interpersonal communications services），原先規定要取得用戶同意後才可將個資編入目錄。但可能修改為允許會員國在當事人可以事後退出的條件下，排除事前同意的適用；並增加了過度條款，在 ePrivacy Regulation 實施前的目錄，可以繼續存在；此外，對於誰有責任確保目錄的內容正確，會員國仍有不同之意見[209]。

(9) 不請自來的直接行銷通訊

將草案「直接通訊」定義中的「呈現」要件刪除；並在立法理由中表明，本法不包含網站上之公開廣告，同時針對相關規範進一步精簡。會員國目前意見漸趨一致，但仍須後續討論[210]。

(10)主管機關

許多會員國希望 ePrivacy Regulation 對於主管機關的權限與義務等能有更廣泛的彈性[211]。

目前，歐盟理事會仍持續就草案內容進行協商，截至本研究結束為

[208] *Id.*, at 7.
[209] *Id.*, at 7-8.
[210] *Id.*, at 8-9.
[211] *Id.*, at 10.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

止，歐盟理事會仍持續進行草案內容的協商與意見交流，尚未完成審議[212]。除了上述內容的變化外，歐盟理事會目前亦建議將 ePrivacy Regulation「開始適用」（entry in to applicication）的時間定為規則通過後的 24 個月[213]。

3. 草案後續發展

由上述的討論可以看見，目前歐洲議會的委員會已經完成初步審議，並決定進入「機關間協商」（institutional negotiations）的階段，但歐盟理事會尚未完成相關審理。未來，歐洲議會、歐盟理事會及歐盟執委會將進行機關間協商，解決其中歧異，再由歐洲議會、歐盟理事會分別圍成內部的審查程序，若雙方未對協商結果進行修改，草案及能生效，否則便須再次進行機關間協商、再進行雙方內部審理程序，待達成相同決定後，草案方能生效[214]。

目前，雙方對於草案的修改內容雖有相同看法，不過也存在歧異，可以預見未來此一草案並不會很快通過。類似的見解在本研究赴英國及美國參加重要國際隱私保護研討會時，也得到相似的印證；其中，在 IAPP 2018 歐洲資料保護密集研討會會議中，無論是在歐盟執委會中負責 ePrivacy Regulation 草案立法推動的執委會英國數位、文化、傳媒暨體育

[212] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Council of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14491_2018_COR_1&from=EN (last visited Dec. 7,2018).

[213] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Council of the European Union, 3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT&from=EN (last visited Dec. 7,2018).

[214] *See gerenally* EUROPEAN PARLIAMENT, HANDBOOK OF THE ORDINARY LEGISLATIVE PROCEDURE: A GUIDDE TO HOW THE EUROPEAN PARLIAMENT CO-LEGISLATES 11-26 (2017).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

部歐盟資料流動及歐盟與國際資料保護部門主管，或是負責英國於歐盟理事會討論 ePrivacy Regulation 草案的英國數位、文化、傳媒暨體育部歐盟資料流動及歐盟與國際資料保護部門主管都認為，目前尚無法清楚的預期草案真正通過的時程。然而，值得注意的是，雖然目前上無法得知草案的通過時程，但上述兩位實際負責 ePrivacy Regulation 立法的官員在研討會上表示，由於 ePrivacy Directive 立法後，已經有太多新的電子通訊型式出現，規範急需更新，而 GDPR 亦已經通過，有必要將電子通訊領域對隱私保護的水準與 GDPR 進一步拉齊，因此歐盟仍會持續積極的完成 ePrivacy Regualtion 的立法工作。與此同時，由於此次修法將大幅擴張 ePrivacy Regulation 的適用範圍，對於電子通訊領域隱私保護標準將帶來重要影響，未來仍應持續觀測其後續發展為宜。

(三)ePrivacy Regulation 草案的主要內容及重要爭點

ePrivacy Regulation 草案目前仍在歐盟立法程序中，本研究就目前可得之最新資料，將歐盟執委會提出的 ePrivacy Regulation 草案主要內容及歐盟議會及歐洲理事會目前對於草案的主要修正項目進行簡要比較。所比較之版本為歐洲議會公民自由、司法暨內政委員會的審查報告[215]以及歐盟理事會最新一份公開的討論版本（最新版本為 2018 年 10 月所公佈）[216]。從目前討論的版本看起來，ePrivacy Regulationa 草案對於通訊傳播資料（包含通訊傳播內容及其詮釋資料在內），會在不改變「以禁止為原則，以許可利用為例外」的情況下，進行部份的調整，其中對於雇

[215] *Supra* note 191.
[216] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, Council of the European Union, https://iapp.org/media/pdf/resource_center/ePR_10-19-18_draft.pdf (last visited Dec. 31, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

主利用電子通訊資料監控員工等部份規定的更為清楚與嚴格，但針對緊急服務放寬規定，並在不影響當事人權利的情況下，對於軟體業者等有適度的放寬規定。最後，則是因應會員國需要，可能不強制要求各國將個資及電子資訊相關業務交由同一主管機關執行，並調整施行日期等規劃內容。

表 6 ePrivacy Regulation 版本比較

執委會版本	**歐洲議會與歐盟理事會之修正**
第一章 一般規定	
不適用範圍： 歐盟法範圍外之活動、預防、調查、偵查及追溯犯罪或執行刑罰、歐盟共同外交及安全政策、非公開之電子通訊服務。	**歐盟理事會：** 新增下列三項不適用之範圍： 1 國家安全及國防有關活動。 2 終端使用者在接收後處理之電子通訊內容，或終端使用者委託第三方紀錄、儲存或以其他方式處理之電子通訊內容。 3 由終端使用者處理之電子通訊詮釋資料，或其委託第三紀錄、儲存或以其他方式處理之電子通訊詮釋資料。
適用範圍：	**歐洲議會：**

本報告之智慧財產權歸屬於財團法人資訊工業策進會

提供歐盟終端使用者電子通訊服務(無論是否付費)、使用該服務、保護位於歐盟之終端使用者的終端設備有關之資訊。	適用範圍應包含：處理與終端使用者的終端設備有關或由該終端設備處理的信息、允許電子通訊的軟體；提供公開的電子通訊用戶目錄之服務；向終端使用者發送直接行銷之電子通訊的情形。 **歐盟理事會：** 1 刪除「無論是否付費」之規定。 2 刪除「使用該服務」之規定。 3 新增「處理歐盟境內終端使用者電子通訊內容及電子通訊詮釋資料」之規定。 4 新增「在歐盟市場內允許電子通訊之軟體(包含於網路上搜索及提供資訊)」。 5 新增「提供位於歐盟境內電子通訊服務終端使用者公開目錄之服務」。 6 新增「向歐盟境內的終端使用者發送直接行銷之電子通訊之行為」。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

歐盟境內代表： 非設立於歐盟的電子通訊服務提供者，應以書面形式於歐盟境內指定代表。	**歐盟理事會：** 1 除電子服務提供者外，公共目錄提供者、電子通訊軟體提供者、使用電子通訊服務發送直接行銷之電子通訊者、使用終端用戶終端設備之除存貨處理能力且未設立於歐盟者，皆應指定歐盟境內代表。 2 若其活動僅為偶然性質，且其性質、脈絡、範圍和目的不太可能對終端使用者之基本權利造成風險，則可不用指定歐盟境內代表。
定義： 大部分定義參照 GDPR、歐盟電子通訊規範（Electronic Communications Code）指令（於 12/12 完成立法）、電信終端設備市場競爭指令（Directive 2008/63/EC）等規定。其中，電子通訊資料一詞指包含「電子通訊內容」及「電子通訊詮釋資料」（提供電子通訊服	**歐盟理事會：** 新增資訊社會服務之定義（參照資訊社會服務指令（Directive 2015/1535））。同時，將原先「電子郵件」修改為「電子訊息」，擴大名詞範圍，將簡訊（SMS）、多媒體簡訊（MMS）或其他類似服務納入。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

務下所產生的位置資訊以及日期、時間、持續時間和通訊類型等用於追蹤和識別通訊來源與木祕密之資料）兩者在內的資料。	
第二章 保護自然人及法人電子通訊及儲存於其終端設備之資訊	**歐盟理事會：** 修改章名為「保護終端使用者電子通訊及其終端設備之完整性」
電子通訊資料應保密	
允許電子通訊網路及服務提供者處理電子通訊資料的情形： 1 為實現通訊傳輸所需，於其所需時間內之處理 2 維持、恢復電子通訊網路和服務之安全性或檢測故障、錯誤等目的，於所需時間內之處理	**歐盟理事會：** 新增「有必要檢測或防止終端使用者之中端設備的安全風險或攻擊」作為允許處理電子通訊資料的情形。
允許電子通訊網路及服務提供者處理電子通訊詮釋資料的情形： 1 為符合歐盟法法強制性服務品質規範，於其所需時間內之處理。	**歐盟理事會：** 將「強制性服務規範」改為「技術性品質服務規範」，並新增下列處理之規範： 1 「網路」（network）管理或最佳

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2 計費、計算互聯費用、防治詐欺與濫用等目的 3 最終使用者同意且該目的無法透過匿名資訊處理者	化所需，於且去識別化處理資訊不足以執行，於所需時間內所為之處理」為允許處理電子通訊詮釋資料之要件。 2 在緊急情形下，為保護自然人重要利益，依據主管機關之要求或依據會員國或歐盟法律規定所為之處理。 此外，若進行與原蒐集目的不同之處理，應考量蒐集之特定目的與處理之特定目的之關聯、脈絡、性質、以及處理的可能結果與適當安全促等，以確定此一新目的是否與原目的相容。且僅能在無法以去識別化方式處理時以假名化方法處理，並不得用以決定最終使用者知本或未其建檔。
允許電子通訊網路及服務提供者處理電子通訊內容的情形： 1 為提供特定服務且最終使用者同意且該目的無法透過去識別資訊處理者。	**歐盟理事會：** 將第一項情形修改為：因最終使用者明確要求特定之服務，在僅限於此目的的範圍內經過最終使用者同意，且不對第三者的基本權利、

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2 最終使用者同意、該目的無法透過去識別資訊處理且經監督機關諮詢者。	利益造成不利影響，於所需時間內處理電子通訊內容。 於第二項情形，新增要求其須對處理造成的影響進行衝擊影響評估。
電子通訊資料的儲存與刪除： **電子通訊內容：**當預期的接收者收到後，電子通訊服務提供者應立即刪除內容或將其去識別處理。 **電子通訊詮釋資料：**當其不再需使用於傳輸通訊目的時，電子通訊服務提供者應刪除詮釋資料或將其去識別處理。但若基於計費目的，可保留相關詮釋資料至可爭執的期限結束。	
保護最終使用者終端設備中儲存之訊息及與終端設備有關之訊息： 原則上禁止使用終端設備的處理和儲存能力或蒐集該設備資訊，除非： 1 僅為透過電子通訊網路進行電子通訊。	**歐洲議會：** 1 應確保使用者同意的條件與 GDPR 相同； 2 不論是否收費，都不得在終端使用者拒絕提供非嚴格必要的資料的狀況下，拒絕其使用資訊社會服。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2 最終使用者同意(可以網路上之軟體程式進行)。 3 對最終使用者所要求之資訊社會服務有必要。 4 最終使用者所要求之資訊社會服務之提供者所進行之必要網路受眾測量。 原則上禁止蒐集使終端設備能連接到其他設備或網路之資訊，除非： 1 僅為了建立聯繫而於所需時間內進行 2 顯示清晰、明顯的通知，告知蒐集之方式、目的、負責人，以及 GDPR13 條之相關訊息。蒐集此類資訊須採取適當安全維護措施。並以標準化圖片說明。(執委會得訂定標準化圖片內容及提供程序)	3 在僱用關係下，雇主只有在執行員工任務有技術必要的狀況下才可以近用使用者之終端設備，並不得進一步用於監控員工。 **歐洲理事會：** 在第四項許可要件中，放寬允許資訊社會服務提供者，在符合 GDPR 第 28 條規定情況下，可以依其需求進行網路受眾測量。此外，新增下列允許條件：第一，軟體基於安全理由、未變更使用者隱私設定、且於每次更新時通知使用者並給予其暫停或關閉自動更新選項的機會下，更新軟體。第二，當最終使用者與歐洲緊急號碼（112）進行緊急通訊，而須定位終端設備時。 而對於連接到其他網路設備之資訊蒐集，新增當事人同意及「服務提供者因統計而有必要，且在達成目的後即去識別化或刪除的狀況

本報告之智慧財產權歸屬於財團法人資訊工業策進會

	下蒐集相關資訊」兩項條件。
同意： 適用 GDPR 同意規範。 電子通訊服務提供者應每 6 個月提醒使用者得撤回同意。	**歐盟理事會：** 將其移動至第一章。
提供隱私設定的資訊與選項： 提供電子通訊的軟體（包含在網路上搜索和提供訊息者）應提供「防止第三方在最終使用者終端設備上儲存或處理已存在資訊」之選項。 安裝時，軟體應通知最終使用者隱私設定選項；並應於安裝過程中取得最終使用者同意。 已於生效日前安裝之軟體，應於第一次更新時進行上述程序，並不得晚於生效後 3 個月。	**歐洲議會：** 1 應避免設立所謂的「cookie 牆」或「cookie banner」等無助於用戶保持對其個資及隱私控制及告知其權利的機制。 2 軟體（包含瀏覽器、操作系統和應用程式）應該設置隱私保護的機制，並預設禁止第三方在終端設備上追蹤和儲存訊息。 3 軟體應提供詳細選項，允許使用者針對不同類別給予不同的設定，並使其可以選擇在安裝後隨時更改或確認其隱私設定。 4 軟體應設計一種訊號用以通知第三方用戶的隱私設定。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

	歐洲理事會： 刪除相關規定。
限制： EU 或會員國可以立法限制前述之權利、義務範圍，但此一限制應基於保障 GDPR 第 23 條所稱之公共利益，並經過比例原則衡量 電子通訊服務提供者應依前述法令制定內部程序	**歐洲議會：** 公共利益應包含包含國家安全、國防及公共安全等之維護 **歐盟理事會：** 要求應符合 GDPR 對會員國限制權利時之要求。
第三章 自然人和法人控制電子通訊的權利	**歐盟理事會：** 修改章名為「終端使用者控制電子通訊的權利」
呼叫和連接線路識別 公共可用之以號碼為基礎的人際傳播服務提供者應以簡單、免費的方式提供下列可能性： 1 撥號者：可防止於每次通話、連接或永久性的出現線路識別資訊。 2 收話者：可防止出現撥號者	**歐盟理事會：** 無論是否為公共可用之號碼，皆適用本條規定。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

線路識別資訊。 3 收話者：可在撥號者遮蔽線路識別時拒絕來電。 4 收話者：可防止向撥號者提供線路識別資訊。 在第一種情形中包含發往第三國之呼叫；在其他三種情形中包含來自第三國之呼叫。 在與緊急服務通話的情況下，服務提供者不應遮蔽識別資訊。	
來電攔截 公共可用之以號碼為基礎的人際傳播服務提供者應以當前最佳科技、免費提供最終使用者： 1 阻止特定號碼或來自匿名來源的呼叫。 2 停止第三方自動將呼叫轉接到最終使用者的終端設備上。	**歐盟理事會：** 刪除公共可用之規定。 若撥號者為處理緊急通訊的組織，即便收話者服務提供者應在技術可行範圍內無視撥號者拒絕收訊的請求，而提供其連接。並應無視最終用戶的設定，對提供緊急服務的組織提供最終使用者的位置訊息。
公眾可近用之目錄	**歐盟理事會：**

本報告之智慧財產權歸屬於財團法人資訊工業策進會

目錄提供者於將資料納入目錄前應： 1 得到自然人最終使用者之同意;予法人最終使用者反對機會； 2 應給予其確認、更正與刪除的方法。 對自然人最終使用者，目錄提供者應在啟用搜尋功能前得到其同意。 上述服務應免費提供。	1 可能修改為允許會員國在當事人可以事後退出的條件下，排除事前同意的適用； 2 增加過度條款，在 ePrivacy Regulation 實施前的目錄，可以繼續存在。
未經請求之通訊 自然人及法人 皆可利用電子通訊服務，向已經同意之自然人最終使用者發送直接銷售通訊（若依據 GDPR 規定獲得電子郵件資訊，應於蒐集及每次發送時，給予反對權）（會員國可立法將語音對語音之呼叫限於未反對之自然最終用戶）。 進行直接銷售通訊者應：提供可聯繫之資訊或提供特定代碼以用於	**歐洲議會委員會：** 應僅限於對事先同意的用戶使用，並應禁止發送這類通訊時隱蔽身份或使用虛假身份。 **歐盟理事會：** 將草案「直接通訊」定義中的「呈現」要件刪除；並在立法理由中表明，本法不包含網站上之公開廣告。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

識別通訊性質；並應提供身份訊息以及使接收者可以簡單方式撤銷同意。	
檢測到之安全風險訊息 電子通訊服務提供者應向最終使用者通知檢測到之安全風險。若該風險並非服務提供者可採行措施所能解決，應告知其可能的補救措施。	**歐盟理事會：** 刪除本條規定。
第四章 獨立監督機關與執法	
會員國及 EU 原則皆由 GDPR 之監督機關負責	**歐盟理事會：** 刪除要求各會員國由 GDPR 監督機關擔任本法監督機關之規定。但在歐盟層級，維持由 GDPR 設立之「歐洲資料保護委員會」（European Data Protection Board）負責之規定，並將其職權進一步明確化。
第五章 補救措施與罰則	
與 GDPR 相同，分為兩階，罰則上限相同	
第六章 授權規定	

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第七章 最終條款	
原指令廢除。自 2018 年 5 月 25 日起適用。	**歐洲理事會：** 修改為通過後 24 個月開始適用。

資料來源：本研究整理自歐盟執委會、歐盟理事會及歐洲議會文件

(四)ePrivacy Regulation 與 GDPR 之競合

從規範的內容來看，相較於 GDPR 是廣泛針對個人資料不同面向的保護與管理議題進行規範，而 ePrivacy Regulation 則是特別針對電子通訊（electronic communications）領域的隱私進行規範；此外，不像 GDPR 僅規範「個人資料」之相關規範，ePrivacy Regulation 亦針對電子通訊領域中「非」個人資料進行管制，這包含了法人的資料等內容[217]。

根據 GDPR 第 95 條之規定，對於已經受到 ePrivacy Directive 管轄的與公共電子通訊服務有關之個人資料處理行為，GDPR 不對自然人或法人增加新的義務[218]。也就是說，對於網路活服務提供者而言，關於「安全和安全漏洞」（security and security breaches）、「流量資料」（traffic data）、「（網路）位置資料」（location data）、「逐項帳單」（itemised billing）以及「線路識別服務」（line identification services）等事項，只須符合 ePrivacy Directive 的規定即可[219]。

類似的規定也可以在 ePrivacy Regulation 草案中看到。根據歐盟執

[217] Conner Forrest, GDPR vs. ePrivacy: The 3 differences you need to know, tech republic, May 29, 2018, https://www.techrepublic.com/article/gdpr-vs-eprivacy-the-3-differences-you-need-to-know/ (last visited Jul. 30, 2018).
[218] Regulation (EU) 2016/79,art. 95, 2016 (L119), 1, 86-87.
[219] What are PECR?, Information Commissioner's Office UK, https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/ (last visited Jul. 31, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

委會提出的 ePrivacy Regulation 草案說明表示，就屬於個人資料的電子通訊資料而言，ePrivacy Regulation 可以視為 GDPR 的「特別法」（*lex specialis*），其對於這部份的規定有所補充，也更加具體；相對的，只要草案並未特別明定的個人資料處理行為，則受 GDPR 之管理；為了調和兩者之間的規範，在草擬 ePrivacy Regulation 的過程中，刪除了部份原先在指令有規定的事項，例如原指令第 4 條規定的安全義務等[220]。

簡單來說，在現有的 ePrivacy Directive 所規範之範圍內（以及未來 ePrivacy Regulation 所規定之對象）而言，僅須適用該指令（或規則）之規定即可，無庸再適用 GDPR 之規定。不過由於 ePrivacy Regualation 制定的其中一個重點就是要確保其保護程度與 GDPR 一致，因此應不至於有過多的適用上困擾。

(五)ePrivacy Regulation 與 GDPR 規範差異之重點比較

承上所述，ePrivacy Regulation 草案與 GDPR 間規範最主要的差異有二：第一，ePrivacy Regulation 草案中部份之規範範圍，並非 GDPR 所涵蓋的個人資料保護，這包含了草案中對於法人資料的保護，以及對於法人與自然人控制電子通訊的權利（包含號碼的呈現、來電阻隔、不請自來之通訊等）。第二，則是對於個人資料保護密度上的差異，大體而言，ePrivacy Regulation 草案普遍較 GDPR 更為嚴格。若依據歐盟執委會版的 ePrivacy Regulation 草案與 GDPR 進行比較，其主要之差異可以從下面幾部份進行觀察：

[220] *Supra* note 179, at 1.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

1. 處理[221]要件的限縮

GDPR 對於個人資料之處理，定有下列合法要件，包含：當事人同意、為履行契約或為訂定契約而有必要、法律規定、為保護當事人或他人重大必要而有必須、執行公務或受委託執行公權力以及為自己或第三人之合法利益所必須等六項[222]。而與此相較，ePrivacy Regulaion 草案則對於要件有更為嚴格之規定。該草案依據資料的類型，而有不同的規範。

針對電子通訊資料而言，僅限於「為完成通訊之傳送所必要，於達成目的期間進行處理」以及「為維護與恢復電子通訊網路與服務的安全、偵測技術缺失或錯誤有必要時，於達成目的期間內進行處理」兩項事由才可進行資料之處理。

除了上述的要件外，對於電子通訊詮釋資料及電子通訊內容，ePrivacy Regulation 草案另外開放了一些要件。在電子通訊詮釋資料方面，若符合以下要件，亦可以進行詮釋資料之處理：「為達成強制性服務品質要求而有必要時，於達成該目的期間內進行處理」、「為記帳、計算互連款項、偵測或停止詐欺、濫用或購買電子通訊服務而有必要時」以及「最終使用者已經同意為一或多個特定目的而處理其詮釋資料（包含提供給其特定服務），且不可以去識別化方式處理資料者」。至於在電子通訊內容方面，若符合以下要件，也可以進行處理：「最終使用者同意且若未處理該內容無法提供服務，則可在僅為此目的情況下處理」或是「若所有有關的最終使用者同意，且無法以去識別方式處理並向監管機關諮詢」。

[221] GDPR 與 ePrirvacy Regulation 所指之處理，包含蒐集、處理與利用。
[222] Regulation (EU) 2016/79,art. 6, 2016 (L119), 1, 36-37.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

總結來看，ePrivacy Regulation 草案在電子通訊資料（包含詮釋資料與內容）的處理要件上，較 GDPR 明顯限縮，除並無執行職務或受委託執行公權力、保護當事人或他人重大利益、為服務提供者自己或他人合法利益等要見外，在同意及執行契約兩項要件上，也都更加緊縮。草案往往要求僅能在無法以去識別方法使用資料，或若不處理變無法提供服務的情況下，才允許使用資料，甚至可能要求服務提供者要項監管機關諮詢才可進行。而在契約執行上，草案也對契約執行可以主張的種類（如維護服務安全檢測風險、計算款項等非常特定的情形下，才可處理資料。

而針對最終使用者終端設備的資訊蒐集（以及對其終端設備處理及儲存功能的使用）上，ePrivacy Regulation 則限於：「僅透過電子通訊網路進行電子通訊傳送有必要時」、「最終用戶同意」、「應請求提供資訊社會服務有必要時」以及「因最終使用者請求之資訊社會服務提供者進行網路受眾測量」等四項目的才可使用。與 GDPR 的規定相較，除當事人同意外，其餘的要件皆是將處理這類型資料的情形限縮於提供特定服務的範圍，與 GDPR 可以因執行契約而處理資料相比，更加限縮。且一無其他 GDPR 許可之項目。

在蒐集使終端設備能連接到其他設備或網路之資訊上，ePrivacy Regulation 草案更將其限縮在「未建立連接目的於特定時間內」以及「在當事人受到清楚與明顯通知」兩類情形下，對比 GDPR 規定，更顯收縮。

最後，在公眾可近用之目錄的製作上，ePrivacy Regulation 草案要求必須以自然人同意為蒐集資料的要件，並在開啟搜尋功能前須取得自然人之同意。在這類型的處理上來說，相較 GDPR 有六大類要件，草案僅給予「同意」這項要件，相當限縮。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2. 儲存時間的限制

GDPR 對於儲存時間，僅要求其「不長於處理目的所需之時間」，且可因基於公共利益之「建檔」（archive）目的、科學或歷史研究目的及統計目的，而保存超過處理目的所需的時間[223]。

相比之下 ePrivacy Regulation 草案對於儲存時間的規定顯的更為具體與嚴格。在電子通訊內容的部份，ePrivacy Regulation 草案規定，只要預期的接收者收到該內容，服務提供者就應該立即刪除或將其去識別處理。在電子通訊詮釋資料的部份，當該資料不再需要用於傳輸通訊的目的時，服務提供者就應該刪除該資料或進行去識別處理；但如果是為了計費所需，可以將資料保存至法定爭執期限結束為止。

總體而言，ePrivacy Regulation 草案規定，服務提供者在完成服務後，就應該立刻將資料刪除或去識別處理，若為了計費所需的詮釋資料，也只能保留到爭執期限結束後就必須刪除。服務提供者不能以其他目的、公共利益等原因，將資料再行留存。

3. 對隱私設定方式的明文化

GDPR 對於系統的隱私設定，由於其適用的個人資料控管者相當多樣，僅要求應提供當事人透明的資訊以及溝通管道[224]、適當採取科技化、組織化措施以符合 GDPR 規定[225]以及要求於從設計包含隱私、把個資保護設為預設等規定[226]。

[223] Regulation (EU) 2016/79,art. 5, 2016 (L119), 1, 35-36.
[224] Regulation (EU) 2016/79,art.12, 2016 (L119), 1, 39-40.
[225] Regulation (EU) 2016/79,art. 24, 2016 (L119), 1, 47.
[226] Regulation (EU) 2016/79,art. 25, 2016 (L119), 1, 48.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

相比之下 ePrivacy Regulation 草案對於隱私設定的方式，有相對比較清楚的規定。其要求提供電子通訊的軟體（包含在網路上搜索和提供訊息者）應提供「防止第三方在最終使用者終端設備上儲存或處理已存在資訊」之選項；並在安裝軟體時，通知隱私設定選項；在安裝過程中取得使用者的同意。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

肆、成立通訊傳播產業資料創新運用法制諮詢服務小組

本研究已於研究案開始起即時成立「通訊傳播產業資料創新運用法制」諮詢服務小組，提供業者及國家通訊傳播委員會有關 GDPR 及個人資料保護相關議題之諮詢服務，服務期間自計畫開始日起至計畫結束。於服務期間內，周一至周五上午 9 時至下午 4 時提供服務，可以透過電話、電子郵件或面訪等方式進行諮詢。國家通訊傳播委員會亦於 5 月 24 日，以通傳平臺決字第 10741020390 號函將聯絡資訊提供給第一、二類電信事業、有線廣播電視系統經營者、無線電視業者、新聞頻道業者、購物頻道業者、直播衛星業者、財團法人電信技術中心及其他檢測、認驗證服務機構。

本年度共累積諮詢 9 案，其中 2 案為國家通訊傳播委員會諮詢，其餘為相關業者之資訊。業者之諮詢中，主要以該公司是否適用 GDPR 為大宗，估計對大多數通訊傳播相關企業而言，辨認是否受 GDPR 管轄仍為當前最主要之困擾，僅有少部份企業因為明確確認須適用 GDPR，已經開始檢視公司相關規範。

諮詢服務之紀錄，請參考下表。

表 7 諮詢服務紀錄

時間	單位	人員	詢問方式	問題內容	回覆方式	回覆內容
107/5/28	國家通訊傳播委員會	林祐仲技正	電話	臉部辨識於通訊產業之應用	電子郵件	提供臉部辨識發展趨勢資料一份。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

107/5/30	時報資訊	陳怡靜法務	電話	時報資訊是否適用GDPR	電話	因時報資訊網站為中文界面，且未提供歐盟區貨幣為付款項目，依GDPR recital 第23點規範，應認為屬偶然使用，無須適用GDPR。
107/6/7	集保公司	柯宗志先生	面訪	集保公司是否適用GDPR	面訪	說明若該公司與歐洲公司之往來間並無涉及個人資料之交換及對歐洲境內資料主體之蒐集，則無個人資料之適用。
107/6/15	富爾特科技	法務	電話	富爾特科技是否適用 GDPR	電話	協助該公司確認資料蒐集流程，若並未針對位於歐盟之資料主體蒐集個資，即不適用GDPR。
107/7/16	集保公司	周彤律師	電話	集保公司是否須設立資料保護員及歐盟境內代表	電話	集保公司因其核心業務並不符合GDPR所規定必須設立資料保護員之條件，無須設

本報告之智慧財產權歸屬於財團法人資訊工業策進會

						立資料保護員。但若因有蒐集歐盟境內資料主體之資料，則可能須指定歐盟境內代表。
107/7/17	集保公司	周彤律師	電話	應如何進行國際傳輸	電話	簡介企業自我拘束原則及標準契約條款之差別及其優劣。
107/7/31	國家通訊傳播委員會	林祐仲技正	電子郵件	有線電視業者蒐集用戶收視紀錄及行為等之商務模式及服務樣態隱私議題	電子郵件	提供相關研析一份（詳附件）。

資料來源：本研究自製

本報告之智慧財產權歸屬於財團法人資訊工業策進會

伍、研析成立個資保護專責機構之必要

一、國際間個資主管機構之趨勢觀測

國際間關於個人資料主管機關的設置模式，大概可以粗略分成分散管理及專責管理兩大模式，前者以美國為代表，後者則有包含歐盟會員過在內的許多國家採用。我國目前採取與美國相似的分散主管機關模式，但一直有人主張應改採專責機關的模式以管理個人資料相關的事務。以下，將分別以美國及英國為例，討論分散主管機關及專責主管機關兩個模式的執行方式。同時，參考日本從分散主管機關轉變為專責主管機關的經驗，希望可以提供給我國作為個人資料主管機關採擇時的借鏡。

(一)分散主管機關模式：美國

1. 美國的分散主管機關模式

承如第壹章所述，美國就個人資料保護方面，未有正式的單一特定主管機關，亦未有統一之聯邦法，而是採取個別立法的方式，因應時代變化和不同領域去制定相關個資保護規則和監管。

2. 通訊傳播領域主管機關

通訊傳播事業的個資、處理、利用或傳輸之監管，主要涉及下述兩個聯邦行政機關—聯邦通訊傳播委員會、聯邦貿易委員會，合先敘明。

通訊傳播事業主管機關為聯邦通訊傳播委員會，任務為管理及執行

本報告之智慧財產權歸屬於財團法人資訊工業策進會

美國通訊傳播法規、電信事業，因而通訊領域的個資蒐集、處理、利用之相關法律及行政命令，亦由其規管，法源係規範於通訊傳播法 151 條。該委員會係受國會監督的獨立政府機關[227]，由 5 名委員組成，係總統任命，並經參議院同意，由總統指定其中 1 人擔任主席，且資格限制皆需為美國公民，僅 3 名委員可屬同一政黨。任期包含主席在內，皆為 5 年，但遞補的委員任期則以前任者剩餘期間為其任期[228]。

另，聯邦貿易委員會則監督消費者隱私議題，法源係聯邦貿易委員會法第 5 條之規定，據以禁止商業中或影響商業的不公平競爭或欺罔行為，而對業者違反隱私保護的行為進行管制。但在電信事業個資保護的監理，其權限上聯邦貿易委員會仍應尊重前揭聯邦通訊傳播委員會之決定。聯邦貿易委員會之組織架構係同樣由 5 名委員組成，總統任命、並經參議院同意，由總統指定其中 1 人擔任主席，且資格限制僅 3 名委員可屬同一政黨，任何委員均不得從事任何其他業務、職業或工作，任期為 7 年[229]。除消費者隱私議題外，聯邦貿易委員會之業務範圍尚包含處理市場不公平競爭及反壟斷（antitrust）等[230]。

(二)專責主管機關模式：以英國為例

1. 另一種選擇：專責主管機關模式

一如前述，美國個人資料保護採取分散式的制度設計。然而，世界

---

[227] The FCC's Mission, https://www.fcc.gov/about/overview （last visited Nov. 29, 2018).

[228] 47 US Code § 154-- Federal Communications Commission

[229] 15 US Code § 41 - Federal Trade Commission established; membership; vacancies; seal

[230] FTC, What We Do, https://www.ftc.gov/about-ftc/what-we-do （last visited Nov. 29, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

上有許多其他的國家，其個人資料保護制度與美國不同，採取「於中央層級設立單一主管機關」的模式，以專責機關統籌個人資料保護事宜。舉例而言，歐盟各會員國[231]以及韓國[232]皆是採取此種專責主管機關的模式來管理個人資料保護的規範。以下，將以英國為例，說明此種模式的運作模式。

2. 專責主管機關模式概說：以英國資訊長辦公室為例

英國係以 1998 年所訂的資料保護法（Data Protection Act, DPA）規範國內所有涉及個人資料的蒐集、處理與利用之行為，規範主體包含公務機關與非公務機關，2018 年本法經修訂，加入了 GDPR 之規範條款，主要條款於 2018 年 5 月 25 日開始實施，詳如第壹章所述，合先敘明。該法第 114 條規範了設立資訊長一職[233]之依據，並透過附表 12（Schedule 12）闡明資訊長的任命和職權、資格定位、辭職和免職、薪資和退休金、組織功能、財政資金等組織規範[234]。

英國的「資訊長辦公室」(Information Commissioner's Office, ICO[235]) 原先成立於 1984 年，為英國的個資保護登記機關，1998 年資料保護法施行後，成為英國個人資料與隱私保護的獨立監督機關。除做為主管資料保護法之機關外，尚包含其他法規之業務，如資訊自由法（Freedom of Information Act）、隱私暨電子通訊指令（Privacy and Electronic

[231] Members, Europe Data Protection Board, https://edpb.europa.eu/about-edpb/board/members_en (last visited Nov. 30, 2018).

[232] Organization, Personal Information Protection Commission (South Korea), http://www.pipc.go.kr/cmt/english/organization/org.do (last visited Nov. 30, 2018).

[233] UK, Data Protection Act 2018, Section 114 " (1)There is to continue to be an Information Commissioner.(2)Schedule 12 makes provision about the Commissioner."

[234] Data Protection Act 2018, Schedule 12, at：http://www.legislation.gov.uk/ukpga/2018/12/schedule/12（last visited Nov. 29, 2018).

[235] 英國 ICO 官網，https://ico.org.uk/about-the-ico/who-we-are/。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Communications Regulations）及環境資訊法（Environmental Information Regulations）、調查權力法（Investigatory Powers Act）等[236]。

資訊長辦公室，主要任務在於維護公共利益的資訊權以及個人資料的隱私[237]，屬於半官方組織，意即「非政府部門之公共機構」（non-departmental public body, NDPB[238]）。所謂「非政府部門之公共機構」，係指在國家政府過程中發揮作用之機關，但並非政府部門或其中的一部分，其運作與部會間仍存有一定的距離，而該機關具有不同的腳色，包含為部長和其他執行行政或監管權能之人提供建議，在部會所制定的框架下進行[239]；若將之與我國相較，類似於「行政法人」之地位[240]。其中，資料保護法附表 12 中提及資訊長需經公平競爭的合法程序選出，由英國女王發布書面命令(Letters Patent)，授予其任用地位，向國會負責[241]。

又，資訊長辦公室是由數位、文化、媒體暨體育部（Department for Culture, Media and Sport, DCMS[242]）所贊助的部門(sponsoring department)[243]。針對資訊長和其職員(staff)之資格定位，參見資料保護法

[236] ICO, Legislation we cover, https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/ （last visited Nov. 30, 2018).
[237] ICO, What we do ,https://ico.org.uk/about-the-ico/what-we-do/ （last visited Nov. 29, 2018).
[238] ICO is an executive non-departmental public body, https://www.gov.uk/government/organisations/information-commissioner-s-office（last visited Nov. 29, 2018).
[239] What is an NDPB?, https://www.gov.uk/guidance/public-bodies-reform（last visited Nov. 29, 2018).
[240] 參酌我國行政法人法第 2 條，對於行政法人之定義：「I 本法所稱行政法人，指國家及地方自治團體以外，由中央目的事業主管機關，為執行特定公共事務，依法律設立之公法人。II 前項特定公共事務須符合下列規定：一、具有專業需求或須強化成本效益及經營效能者。二、不適合由政府機關推動，亦不宜交由民間辦理者。三、所涉公權力行使程度較低者。」又，依據同法第 3 條，「行政法人之監督機關為中央各目的事業主管機關，並應於行政法人之個別組織或通用性法律定之。」
[241] Data Protection Act 2018, Schedule 12, Paragraph 2, " (1)The Commissioner is to be appointed by Her Majesty by Letters Patent.(2)No recommendation may be made to Her Majesty for the appointment of a person as the Commissioner unless the person concerned has been selected on merit on the basis of fair and open competition."
[242] About As, The Department for Digital, Culture, Media & Sport (DCMS) , https://www.gov.uk/government/organisations#department-for-digital-culture-media-sport (last visited Dec. 2, 2018).
[243] ICO, Relationship with the Department for Digital, Culture Media and Sport,

本報告之智慧財產權歸屬於財團法人資訊工業策進會

中附表 12 提及，非屬官方政府的公務員或代理人[244]。而資訊長的任期部分，不得超過 7 年，且不得連任或再任[245]。資訊長應指派 1 名或多名副資訊長[246]，在指派第 2 名或 2 名以上的副資訊長時，需具體特定各名副資訊長負責執行之權能為何[247]。若遇資訊長缺位或因任何理由而不能行使職權時，由副資訊長代為執行之[248]。

資訊長辦公室內設有管理委員會（Management board），主要目的係領導、協助 ICO 履行其法定職責，側重於組織有效運作、符合法定要求和標準，提供經營、政策指導和建議、影響議題的諮詢、審查政策及程序，以期實現辦公室之宗旨[249]。目前管理委員會組織當中，除資訊長外，設有三位副資訊長，分別為首席副資訊長（Deputy Chief Executive）、營運副資訊長（Deputy Commissioner (Operations)）以及政策副資訊長（Deputy Commissioner (Policy)），除上述人員外，尚有技術政策和創新執行理事（Executive Director – Technology Policy and Innovation），以及 4 位非執行理事（Non-Executive Directors）[250]，共計 9 人。

(三)從分散到整合：以日本為例

---

https://ico.org.uk/about-the-ico/who-we-are/relationship-with-the-dcms/ （last visited Nov. 29, 2018).

[244] Data Protection Act 2018, Schedule 12, Paragraph 1, ”(2)The Commissioner and the Commissioner's officers and staff are not to be regarded as servants or agents of the Crown.”

[245] Data Protection Act 2018, Schedule 12,” (3)The Commissioner is to hold office for such term not exceeding 7 years as may be determined at the time of the Commissioner's appointment, subject to paragraph 3.(4)A person cannot be appointed as the Commissioner more than once.”

[246] Data Protection Act 2018, Schedule 12, Paragraph 5(1) (a),” The Commissioner—must appoint one or more deputy commissioners.”

[247] Data Protection Act 2018, Schedule 12, Paragraph 6(2), ” When the Commissioner appoints a second or subsequent deputy commissioner, the Commissioner must specify which deputy commissioner is to carry out which of the Commissioner's functions in the circumstances referred to in sub-paragraph (1).”

[248] Data Protection Act 2018, Schedule 12, Paragraph 6(1), ” The functions of the Commissioner are to be carried out by the deputy commissioner or deputy commissioners if—(a)there is a vacancy in the office of the Commissioner, or (b)the Commissioner is for any reason unable to act.

[249] ICO, Purpose of the committees, https://ico.org.uk/about-the-ico/who-we-are/decision-making-structure/ （last visited Nov. 29, 2018).

[250] Management board, Information Commissioner’s Office, https://ico.org.uk/about-the-ico/who-we-are/management-board/ (last visited Nov. 30, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

1. 日本經驗：從分散到整合

日本原先個人資料保護法之主管機關為消費者廳，但該法施行的監督機關，係由各行業類別的中央主管機關為之(主務大臣制)，多達 16 個（包含外務省、經濟產業省、總務省、財務省、法務省、農林水產省、國土交通省、防衛省、厚生勞動省、文部科學省、環境省、內閣府、消費者廳、金融廳、警察廳、復興廳）。但後續考量發生法律爭議時，易出現解釋意見不一或監督、執行效率不彰，及新興事業跨界經營使權責劃分模糊等情況，進行專責機關的調整[251]。

因而，日本眾議院在 2015 年 9 月 3 日透過個人資料保護法之修正，於 2016 年 1 月 1 日成立「個人情報保護委員會」（Personal Information Protection Commission, PPC[252]）作為個人資料保護法的專責監督機關，由內閣總理大臣所轄，將先前各事業主管機關各自定立之 GL，交由個人情報保護委員會統一訂出基本規則，意即，原則上將各事業主管機關原先與個資法有關的內容，統合到個人情報委員會的指導方針中[253]。除因特殊專業領域存在個資處理的特別需要時，可由個人情報保護委員會對 GL 的訂定提出意見，與該事業主管機關共管之[254]。其中，目前針對特定事業領域的監管權限委任，主要分為三大領域，包含了 1.資通訊業、

[251]宇賀克也，個人情報保護法改正について(1)，情報公開·個人情報保護， Vol.59，2015 年，頁 55。轉引自法務部「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告，2016 年 12 月，頁 64、65。

[252]個人情報保護委員會官網，https://www.ppc.go.jp/。

[253]個人情報保護委員会，個人情報保護法ガイドライン（案）について，頁 4，https://www.ppc.go.jp/files/pdf/280930_siryou1-1.pdf。（last visited Nov. 29, 2018).

[254]日置巴美、板倉陽一郎，平成 27 年改正個人情報保護法のしくみ， 商事法務，2015 年 12 月，頁 52 ~54 。轉引自法務部「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告，2016 年 12 月，頁 65。（last visited Nov. 29, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2.財務金融業、3.醫療和健康保險等，並另各自訂有相關之 GL[255]。

2. 日本個人情報保護委員會簡介

日本個人個資保護法於第 1 條揭示了立法目的，係伴隨資通訊社會發展，而使個人資料之利用顯著增加，為規範個人資料之正確處理方法、建立基本原則、方針及其他關於個人資料保護之政策等基本事項，且明確界定中央政府及地方機關之責任與義務、處理個人資料之業者應遵守的義務事項時，以適當、有效地處理個人資料，並有助於創新產業及實現活絡的經濟社會與富饒的國民生活，考量個人資料之可利用性同時，為保護個人權益，特制定本法。

關於日本的個人情報保護委員會組織、職權和執掌事務內容、委員任期等，明定於日本個資法第五章（第 59 條～第 74 條）當中。該委員會係依日本內閣府設置法第 49 條第 3 項規定設置，由 1 名委員長及 8 名委員所組成（其中 4 名委員為兼職人員），經兩議院同意後由內閣總理大臣任命之，隸屬於內閣總理大臣所管轄，並獨立行使其職權，採取合議制[256]，相當於我國中央二級獨立行政機關，如公平交易委員會、國家通訊傳播委員會、中央選舉委員會等。

委員會主要任務在於專責監督與監測政府各機關以及民間個資處理事業對於個資的傳遞、處理，並適時提出指導意見或建言[257]。其所職掌事務而言，參見日本個資法第 61 條，明列下列 9 項：(1) 制定及推行基本方針之相關事務；(2) 關於個人資料和匿名化資料之處理監督事務、

[255] 特定分野ガイドライン, https://www.ppc.go.jp/personal/legal/guidelines/#etc_gl（last visited Nov. 29, 2018).
[256]依據日本個人資料保護法第 59 條、第 62 條及第 63 條參照。
[257]日本個人資料保護法第 61 條參照。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

對當事人提出申訴必要之調解，及協助執行該業務之業者等事項；(3)個人資料保護團體之認證、監督相關事務；(4) 關於處理特定個人資料之監視、監督，或對當事人提出申訴之必要調解、及協助執行該業務之業者等事項；(5)特定個資保護評價；(6) 針對個資保護及適當、有效的活用，進行宣導及教育等相關事務；(7) 實施以上 6 項所列之事務時，所需的調查和研究相關事務；(8) 國際間合作之相關事務；(9)除前揭所列事項之外，其他依法隸屬委員會之事務。

任期部分，委員長及委員之任期為 5 年，但遞補的委員長和委員的任期則以前任者剩餘期間為其任期；得連任之。當任期結束時，規定該委員長及委員須持續執行其職務至繼任者被任命為止。

然而，需特別留意的是，承如前述，日本通訊傳播事業之主管機關為總務省，針對通傳領域之個資監管，係基於個人資料保護法第 44 條第 1 項，由個人情報保護委員會基於考量其特殊事業領域的專業技術背景，將通訊事業的個資監管權限委任予目的事業主管機關(即主管通傳領域之總務省)，來監督管理。詳細理由已於前述「第壹章研析數位匯流法規及隱私保護法規之規範—日本概述」中提及，併以敘明。

二、淺析我國之個資主管機關制度安排

(一)當前我國個資主管機關設計

我國個人資料保護法制自 1995 年制定「電腦處理個人資料保護法」起，直到 2010 年將其全文修正並修改名稱為「個人資料保護法」，乃至後續的修正為止，皆未針對個人資料保護的專責機關，而是採取分散管理的管制模式。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

1995 年制定電腦處理個人資料保護法時，並未特別設立個資保護專責機關，亦未指定單一的主管機關負責，而是由各目的事業主管機關，針對其所管之產業進行管理，並由法務部負責辦理協調、聯繫電腦處理個人資料保護法的相關事項，並負責「無目的事業主管機關」產業的管理[258]，同時制定電腦處理個人資料保護法的施行細則[259]。

2010 年電腦處理個人資料保護法翻修改為個人資料保護法後，類似的法律架構仍然維持。根據現行有效的個人資料保護法規定，仍未設有主管機關，而是在中央由各目的事業主管地方負責管理，在地方則由直轄市或縣市政府負責，法務部則仍負責施行細則之制定[260]。同時，法務部擔任個人資料保護法的法律解釋機關，針對各中央目的事業主管機關及各地方政府對個人資料保護法有疑義之處進行法律解釋。

而為解決因為設立單一主管機關、分散式管理所產生的跨部會協調整合問題，國家發展委員會在今（2018）年 7 月設立任務編組「個人資料保護專案辦公室」，統籌因應歐盟 GDPR 施行相關事宜、協調整合各機關對個人資料保護法落實的一致性[261]。行政院並於今年 7 月 25 日時將個人資料保護法的「法律主政機關」轉由國發會擔任[262]，國發會並在其個人資料保護專區上設立「個資法問與答」專區，除整理過往法務部之函釋外，也會持續針對個資法相關疑義進行更新[263]。然而，雖說個資法的法律主政機關已經轉由國發會負責，但至少截至今年 10 月為止，法務

[258] 電腦處理個人資料保護法（1995 年制定版）第 42 條第 2 項。
[259] 電腦處理個人資料保護法（1995 年制定版）第 44 條。
[260] 個人資料保護法第 55 條。
[261] 個人資料保護專案辦公室，國家發展委員會，https://www.ndc.gov.tw/Content_List.aspx?n=726A44EA5D724473 （最後瀏覽日：2018/11/30）。
[262] 國家發展委員會發法字第 1072001389 號函。
[263] 個人資料保護專區，國家發展委員會，https://pipa.ndc.gov.tw/ （最後瀏覽日：2018/11/30）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

部仍會針對個資法的法律疑慮發布函釋[264]。

簡而言之，目前我國個人資料保護法並未設有主管機關，而是由各中央目的事業主管機關及地方政府分別就其管理對象管理個人資料保護的相關事宜。目前，個人資料保護法的法律主政機關由國家發展委員會擔任，但法務部仍會針對個資法疑義發布行政函釋。

此種制度設計之方式，於我國大幅翻修電腦處理個人資料保護法為個人資料保護法時，無論官方或民間學者，皆已為文論著，認為有所缺陷，而應該設立一單一之個人資料保護主管機關[265]。而在個人資料保護法修正後，亦仍有民間團體認為「分散的主管機關，不僅造成《個資法》的適用落差與眾多爭議，更連帶使《個資法》及相關的科技政策欠缺完整、定期的監督或修訂」是個資法的重要缺失[266]，而分散的主管機關，也造成跨部會的個人資料問題，缺乏協同與負責的單位[267]。對此，國發會雖成立個人資料保護專案辦公室，但不僅在其組織之透明性與獨立性上遭受質疑[268]，國發會自己也承認這並非「個資專責機構」，而希望能持續努力[269]。

---

[264] 如 2018 年 10 月 22 日公佈的法務部法律字第 10703516250 號函，該函回覆對象是新北市政府 2018 年 8 月 28 日新北府經司字第 1071620399 號函，新北市政府發函時間在行政院更改法律主政機關之後。

[265] 如：劉佐國，〈我國個人資料隱私權益之保護－論「電腦處理個人資料保護法」之立法與修法過程〉，《律師雜誌》，第 307 期，頁 42-51（2005）；莊庭瑞，〈個人資料保護在台灣：誰的事務？〉，《國家政策季刊》，第 2 卷第 1 期，頁 66（2003）。

[266] 何明諠，〈焦點評論：恣意擴權的國發會〉，蘋果日報，2017/10/10，https://tw.appledaily.com/headline/daily/20171010/37807964/%E7%84%A6%E9%BB%9E%E8%A9%95%E8%AB%96%EF%BC%9A%E6%81%A3%E6%84%8F%E6%93%B4%E6%AC%8A%E7%9A%84%E5%9C%8B%E7%99%BC%E6%9C%83%EF%BC%88%E4%BD%95%E6%98%8E%E8%AB%A0（最後瀏覽日：2018/02/13）。

[267] 〈進退維谷的個人資料保護政策〉，臺灣人權促進會，2011/11/15，https://www.tahr.org.tw/news/192（最後瀏覽日：2018/02/13）。

[268] 何明諠，前揭註 266。

[269] 〈有關平面媒體投書針對本會個人資料評議中心之建言，本會至為感謝，唯內容多有誤解，國發會特別說明如下〉，國家發展委員會，2017/10/10，

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(二)我國適足性談判對象：歐盟 GDPR 之規範

歐盟於今年施行的 GDPR，對於個人資料的跨境傳輸採取「原則禁止、例外許可」的立場，只有在符合 GDPR 規定的特別情形下，才可進行個人資料的跨境傳輸[270]。GDPR 所包含的例外情形可以分為三個層次；首先，第三國或國際組織（或其特定領域或部門）可以取得歐盟執委會對其個資保護措施的適足性認定，若取得適足性認定，則可自由將個人資料傳輸到該國、國際組織（或其特定領域或部門）；若該國未能取得適足性認定，則傳輸目的地的企業或組織可以透過證明其符合 GDPR 規定的適當保護措施，而獲得國際傳輸的許可，這包含企業自我拘束規則、標準契約條款、行為守則以及獲得認驗證等四種手段；最後，若不屬於取得適足性認證的國家，亦未能證明其已採取適當保護措施，則僅在其他偶然性、個案性質的例外情形才可進行個資的跨境傳輸[271]。

有鑑於我國企業與歐盟有密切的商務往來，我國乃決定向歐盟尋求個人資料保護的適足性認定。行政院國家發展委員會於今年正式向歐盟申請，並計畫於未來就個資保護適足性展開後續的談判。在爭取適足性認定的標準下，我國若與歐盟 GDPR 適足性要求不同之處，則需要加以修改，以符合其要求。

歐盟在 1995 年資料保護指令的時代曾針對 GDPR 的適足性發布「適

https://www.ndc.gov.tw/News_Content.aspx?n=B3166DEAC8BA29A7&s=00935AA1DCF60A8B （最後連覽日：2018/02/13）。

[270] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 45, 2016 O.J. (L 119) 1, 61-62.

[271] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 46, 2016 O.J. (L 119) 1, 62.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

足性參考指引」(Adequacy Referential),在 GDPR 正式生效後,依據 GDPR 所成立的歐洲資料保護委員會亦繼續承認其指引。

在前述適足性參考指引中,歐盟在針對程序及執行措施的要求中,特別針對「主管監督機關」(competent supervisory authority)有詳細的要求。該準則要求第三國應具有一個或多個「獨立」的監督機關,以確保資料及隱私保護法令在該國的執行。監督機關應完全獨立且公正的履行其職務並運用其權力,不可尋求或接受指令。該國法令應給予該監督機關必要及確實可實行的權力(包含實施調查的能力),並同時考量該機關的職員、預算等是否能有效的協助其落實。這樣對於監督機關「獨立性」的要求,與 GDPR 條文內,對於歐盟成員國監督機關的規範相當類似,只是對於歐盟成員國,GDPR 有更詳盡的規範,例如要求監督機關的成員應有任期保障,最低任期長度不得低於四年等[272]。

整體而言,與其說歐盟 GDPR 要求的是「專責機關」,其實 GDPR 更強調的是監督機關的「獨立性」,因此無論對於歐盟成員國的規定,或是對第三國取得適足性上的規範,都並未要求僅設立「一個」個資主管機關,而是允許其設立多個不同的監督機關。然而,由於其對於監督機關獨立性的要求,而獨立機關往往展現出與其他機關不同的特性,例如在組織上,機關首長的任期保障;在決策上,不受其他機關(包含上級機關)的指導等,都使得要在單一層級內設立「多個」獨立機關來共同負責個人資料的保護顯得相當的困難。從結果上來看,歐盟各會員國的

[272] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art.54, 2016 O.J. (L 119) 1, 66-67.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

個資主管機關原則上都僅有單一的專責獨立機關[273]。比較特殊的案例則是德國，其除了在中央設有單一的主管機關外，因為其聯邦制的制度設計，各邦擁有獨立立法權，存在不同的個資法，因此在邦層級上，也設有各邦的個資主管機關[274]。因此，雖然說德國有超過一個的個資主管機關，但其實德國的主管機關是分布於垂直權利分立的不同層級，在中央的層級上，仍是維持單一、專責的機關設計。

如上所述，在我國希冀能取得歐盟 GDPR 適足性認證的前提下，我國的個資主管機關應具備獨立性，尤其重視其不受其他機關指揮的特質。基於行政一體的考量，我國中央行政機關組織基本法規定，上級機關對於所隸屬機關有指揮監督權[275]。故我國一般機關的建置在推論上應該認為都無法符合歐盟 GDPR 對於獨立性的要求，而須是我國法下的「獨立機關」方才符合相關規定。而所謂的獨立機關，根據中央行政機關組織基準法規定，指依據法律獨立行使職權，自主運作，除法律另有規定外，不受其他機關指揮監督之合議制機關[276]。而由於獨立機關不受其他機關指揮監督的特性，設立超過一個獨立機關負責個資保護事項，似乎也不切實際。因此，對於歐盟對於個資主管機關獨立性的要求，實際上便會造成設立或指定個資保護專責機關的效果。

(三)我國對獨立機關的規範建置

在我國，獨立機關是否符合憲法對於權力分立的要求，曾有過學術上之爭執。但自從司法院釋字 613 號解釋認為獨立機關並不違反憲法規

[273] Members, Europe Data Protection Board, https://edpb.europa.eu/about-edpb/board/members_en (last visited Nov. 30, 2018).
[274] *Id.*
[275] 中央行政機關組織基準法第 14 條。
[276] 中央行政機關組織基準法第 3 條第 2 款。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

定，但在組織及任命上有一定的限制以後，目前我國對於獨立機關的合憲性已無疑慮[277]。

目前，我國獨立機關之基本組織規範，係規範於中央行政機關組織基準法之中。根據該法規定，我國獨立機關在組織上有以下之規範要求：

(1) 獨立機關不受其他機關指揮監督[278]。但依據最高行政法院之見解，若無其他法律之特別規定，獨立機關所為之行政處分，仍可依訴願法之規定向上級機關訴願[279]。因此，雖然獨立機關不受其他機關指揮監督，但其行政處分仍可能受上級機關檢視。

(2) 獨立機關應為合議制機關[280]。

(3) 獨立機關之首長、副首長及合議制之成員，其任期應受保障，應依法規範其任命、停職、免職之規定及程序[281]。其中，相當二級機關之獨立機關，專任之合議制成員，應經立法院同意後任命，其他層級之獨立機關合議制成員，由一級機關首長任命[282]。

(4) 相當二級機關之獨立機關組織規模建置，業務單位原則以 4 至 6 處為原則，各處以 3 至 6 科為原則[283]；其為處理技術性或專門性業務需要，得設立附屬之署、局，其附屬的署、局，與其他二級

[277] 葉俊榮，〈獨立機關之獨立性：論國家通訊傳播委員會設立之憲法爭議〉，台灣行政法學會編，《行政組織與人事法制之新發展》，頁 62-63（2010）。
[278] 中央行政機關組織基準法第 3 條第 2 款。
[279] 最高行政法院 97 年 12 月份第 3 次庭長法官聯席會議。
[280] 中央行政機關組織基準法第 3 條第 2 款。
[281] 中央行政機關組織基準法第 21 條。
[282] 中央行政機關組織基準法第 21 條。
[283] 中央行政機關組織基準法第 32 條第 1 項。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

機關合計，總數 70 個（地方分支機關除外）[284]。

(5) 相當二級機關之獨立機關總數，原則以 3 個為限[285]。

目前，我國共有相當中央二級獨立機關 4 個，分別為國家通訊傳播委員會、公平交易委員會、中央選舉委員會[286]、促進轉型正義委員會[287]；相當中央三級獨立機關 2 個，即飛航安全調查委員會[288]及不當黨產處理委員會[289]。其中，促進轉型正義委員會根據促進轉型正義條例的規定，自成立後兩年內完成任務後解散（必要時得延長一年）[290]。

在機關獨立職權方面，依據有線廣播電視法[291]、衛星廣播電視法[292]、廣播電視法[293]、公平交易法[294]、促進轉型正義條例[295]、政黨及其附隨組織不當取得財產處理條例[296]之規定，我國公平交易委員會、促進轉型正義委員會、不當黨產處理委員會所為之行政處分以及國家通訊傳播委員會在適用有線廣播電視法、衛星廣播電視法及廣播電視法所為之行政處分，排除向上級主管機關訴願之規定。至於其他獨立機關，包含國家通訊傳播委員會適用電信法部份之行政處分、中央選舉委員會及飛航安全

284 中央行政機關組織基準法第 33 條。
285 中央行政機關組織基準法第 32 條第 2 項。
286 行政院組織法第 9 條。
287 促進轉型正義條例第 2 條。
288 飛航安全調查委員會組織法第 1 條。
289 政黨及其附隨組織不當取得財產處理條例第 20 條；唐筱恬，〈不當黨產委員會主委　月薪近 20 萬元〉，2016 年 7 月 29 日，上報，https://www.upmedia.mg/news_info.php?SerialNo=1226&fbclid=IwAR1Z_Wu7fXFrjT0PcktMLz23JuwsO14NQf4cmhZRwCyw1unHSu2nVkXndc4 （最後瀏覽日：2018/11/30）。
290 促進轉型正義條例第 11 條第 1 項。
291 有線廣播電視法第 75 條之 1。
292 衛星廣播電視法第 66 條之 1。
293 廣播電視法第 50 條之 2。
294 公平交易法第 48 條。
295 促進轉型正義條例第 20 條。
296 政黨及其附隨組織不當取得財產處理條例第 9 條、第 16 條、第 29 條。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

調查委員會的行政處分，則仍須受上級機關之檢視。

在首長、副首長及合議制之成員的任期及專兼任規範方面，行政院組織法所規範的三個相當中央二級獨立機關中，除中央選舉委員會有兼任的委員外，國家通訊傳播委員會及公平交易委員會皆為專任委員，委員皆為 7 人，任期 4 年任滿得連任，得連任無連任次數限制，採交錯任期制，委員中具同一政黨黨籍者，不得超過委員總數的 1/2[297]。至於中選會，其委員人數 9 至 11 人，得為兼任委員，任期 4 年得連任 1 次，採交錯任期制，委員中具同一政黨黨籍者，不得超過委員總數的 1/3[298]。至於促進轉型正義委員會，其委員 9 人，包含主任委員及副主任委員在內的 5 名委員為專任，其餘 4 人為兼任，由於該委員會預計存續時間為 2 年，並無任期之規範，委員中具同一政黨黨籍者，不得超過委員總數的 1/3，同一性別不得少於 1/3[299]。

而在相當中央三級的獨立機關方面。飛航安全調查委員會置委員 5 至 7 人，皆為兼任，任期 3 年並無連任相關規定，採交錯任期制，委員中具同一政黨黨籍者，不得超過委員總數的 1/2[300]。至於不當黨產處理委員會，則置委員 11 人至 13 人，任期 4 年並無連任相關規定，委員中具同一政黨黨籍者，不得超過委員總數的 1/3，同一性別不得少於 1/3[301]。

由上述的整理可以發現，我國實務上相當中央二級機關的獨立機關，習慣上任期規劃為 4 年，可連任 1 次，採取交錯任期制；至於委員是否為專任，則是機關業務是否繁複而定，行政院組織法所規定的獨立

[297] 國家通訊傳播委員會組織法第 4 條、公平交易委員會組織法第 4 條。
[298] 中央選舉委員會組織法第 3 條。
[299] 促進轉行正義條例第 8 條。
[300] 飛航安全調查委員會組織法第 3 條。
[301] 政黨及其附隨組織不當取得財產處理條例第 18 條。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

機關中，除主管選舉、及公投事項的中央選舉委員會外，其餘委員皆為專任。而在相當中央三級機關的獨立機關中，任期並無一定，且也無清楚的連任規範、不一定採取交錯任期制度。而在黨籍比例的規定上，如果涉及與政黨競爭或管理對象為政黨者，任一政黨比例為 1/3，其餘則為 1/2。

三、代結論：我國個資主管機關可能之模式

(一)各國個資主管機關設置模式比較

綜合上述對各國個資主管機關之耙梳，以及對我國現狀之整理，本研究發現，各國主管機關皆具有一定程度之獨立性，只是在組織上達成獨立性手段方法有所差異，日本及美國皆採取設立合議制獨立機關，而且皆類似於我國相當中央二級機關之獨立機關的模式來達成獨立性的要求，但英國則設立類似我國行政法人的獨任機關來完成。而在獨立機關的組織上，美國合議制成員皆為專職，而日本則有部份兼職之設計，這與該國對於合議制成員之組成應包含之範圍有關，我國似可依據實際需要決定是否引入兼職人員。而人員的任命上，獨立機關成員皆須由行政權提名、國會同意，任期則有 5 或 7 年兩項設計，除英國限制禁止連任與再任外，其餘皆可連任。下表將比較美、英、日三國個資主管機關與我國個資主政機關在組織上之差異。特別值得注意的是，我國的「法律主政機關」與一般所稱之「主管機關」不同，僅是負責法律之協調與統籌，根據個人資料保護法之規定，實際執行個資法相關規定的，仍為各中央目的事業主管機關以及縣、市政府，在此先與指明。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

表 8 各國個資主管機關及法律主政機關比較

國別	美國	美國	英國	日本	臺灣
機關名稱	聯邦通訊傳播委員會	聯邦貿易委員會	資訊長辦公室	個人情報保護委員會	國家發展委員會（法律主政機關）
機關性質	合議制獨立機關	合議制獨立機關	獨任機關	合議制獨立機關	非獨立機關
機關定位	類似我國相當中央二級機關之獨立機關	類似我國相當中央二級機關之獨立機關	類似我國行政法人	類似我國相當中央二級機關之獨立機關	中央二級機關
首長或合議制成員數量	5 人	5 人	首長 1 人，副手 3 人	9 人	1 人
專職與否	皆專職	皆專職	專職	5 人專職 4 人兼值	專職
任命程序	總統提	總統提	經公平競	總理提	行政院長

本報告之智慧財產權歸屬於財團法人資訊工業策進會

	名，參議院同意	名，參議院同意	爭程序選出	名，國會兩院同意	任命
任期長短	5 年	7 年	7 年	5 年	無任期保障
連任規定	可連任	可連任	不可連任或再任	可連任	無任期保障

資料來源：本研究自行整理

(二)我國個資主管機關可能之模式

承上所述，若我國希望取得 GDPR 的適足性認定，成立獨立的個資保護專責機關應是難以繞過的要件。此外，本研究於訪談階段向法律學者及業者請教對成立保護專責機構之看法。受訪談對象基本上都同意，若能成立單一的個資主管機關，則對於事權、解釋方法乃至監管力度上，都有正面的幫助。無論是國際接軌的需求，或是內國對於個資保護專責機關的期待，成立一個專責而獨立的個人資料保護主管機關，似乎成為一種共識。然而，由於目前政府組織架構的憲政，成立個人資料保護專責機關仍具有一定的難度。以下，就成立個人資料保護專責機關的四種可能方式：將現有主政機關轉型為獨立機關、另立獨立機關、由現有獨立機關處理以及其他可能方式等分別進行討論。

1. 現有個人資料保護法主政機關轉型為獨立機關

我國目前個人資料保護法的主政機關為國家發展委員會，在「最小

本報告之智慧財產權歸屬於財團法人資訊工業策進會

變動」的邏輯思考下，將其轉型為獨立機關，似乎是最為簡便之舉。然而，由於國家發展委員會的機關定位以及組成方式，將其改為獨立機關，並不切實。

國家發展委員會負責國家發展政策、國家發展計畫、經濟發展政策、社會發展政策、產業發展政策、人力資源發展政策、國土、區域及離島發展與永續發展政策、文化與族群發展政策、管制考核政策、政府資訊管理政策行政與法制革新政策以及其他國家發展政策之綜合性規劃[302]、協調、審議及資源分配以及法規影響評估、性別影響評估之協調[303]，其組織定位為「國家發展策略運籌總部」，甚至可以有「小行政院」的稱號[304]。而其委員組成，更包含各部會首長在內[305]。這個職司國家重要政策協調及審議的單位，是行政權執行行政職務的重要核心機制之一，若將其轉型為不受其他機關指揮監督的獨立機關，與其根本的組織定位顯有扞格，恐怕並沒有實現的可能性。

2. 另立獨立機關

成立個資專責機構的另一個可能性，為另外成立獨立機關。目前我國中央政府之獨立機關可分為相當中央二級機關及相當中央三級機關兩個種類，以下分別就設立該種機關的可能性進行簡要評估。

(1) 相當中央二級機關之獨立機關

[302] 國家發展委員會職權不包含文化與族群發展政策綜合規劃。
[303] 國家發展委員會組織法第 2 條。
[304] 國家發展委員會揭牌成立（103 年 1 月 22 日），國家發展委員會，https://www.ndc.gov.tw/News_Content.aspx?n=608F56E26D137607&sms=5DC1EF6FAAE15BA2&s=CD7881C092EDFEEC （最後瀏覽日：2019/12/1）。
[305] 國家發展委員會組織法第 3 條。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

個人資料保護法除對非公務機關有所規範外，亦針對公務機關有規定。是以個人資料保護法之主管機關，除要針對非公務機關進行管理外，亦應監督公務機關之落實。同時，個人資料在應用至各領域時，可能與該領域其他作用法之實行有關，有跨機關協商與討論之需要。為能有效監督公務機關對個人資料保護之落實，並能與其他中央機關平行討論相關事宜，似乎將此一新的個資主管機關定位為相當中央二級機關之獨立機關有其合理性。同時，參考美國及日本之經驗，也是以此種層級之獨立機關來管理個資事務，似乎更能讀顯此一方案的合理性。

然而，根據中央行政機關組織基準法之規定，我國相當中央二級機關之獨立機關總數為 3 個。而依據行政院組織法之規定，此 3 個相當中央二級機關之獨立機關為：國家通訊傳播委員會、公平交易委員會及中央選舉委員會；易言之，目前我國相當中央二級機關之獨立機關已經滿編。

也因為如此，當政府以促進轉型正義條例排除前述中央行政機關組織基本法獨立機關數量限制的作法，設立設有落日條款的促進轉型正義委員會，就已經不斷受到外界批評[306]。個資保護專責機關與促進轉型正義委員會不同，並無一定存續的期間，在行政機關總量管制的大原則之下，要另外設立新的相當中央二級機關之獨立機關，難度相當高。

當然，在制度採擇的思考下，其實亦可以考慮將現有的相當中央二級機關之獨立機關彼此整併，或與其中央二級機關整併後，再

[306] 如：〈風評：黃煌雄也擺不平「促轉」不正義的違憲爭議〉，風傳媒，2018 年 3 月 29 日，https://www.storm.mg/article/417300 （最後瀏覽日：2018/12/03）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

行設立新的相當中央二級機關之獨立機關作為個資主管機關。然而，我國目前行政院組織法所律定的三個獨立機關中，中央選舉委員會基於其選務獨立之需求，在我國當前社會環境中，似乎不宜取消其獨立機關之資格，併入其他機關內。而公平貿易委員會此一競爭法的重要管制機關，若要歸併進經濟部等其他部會，似乎就難以發揮其獨立機關獨立決策的功能。至於國家通訊傳播委員會，作為我國第一個法律明文規定的獨立機關，其成立有我國重要政黨間為維持通訊傳播管制中立、維護民主發展，發揮「保險」功能的背景[307]，且為通訊傳播基本法所明定要設立的機關[308]，若要將其與功能類似之其他機關整併（如文化部、交通部等），若無重大政治環境變化，恐有現實之困難與阻礙。因此，現在實無將現有之相當中央二級機關之獨立機關整併的條件與空間。

(2) 相當中央三級機關之獨立機關

成立新的相當中央二級獨立機關有行政機關總額限制之困境已如前述。由於相當中央三級機關之獨立機關並不受總量限制管制，因此以此形式成立個資保護專責機關其實也是選項之一，江耀國教授就認為，可以考慮以此形式設立個人資料主管機關。

然而，現行我國相當中央三級機關之獨立機關，包含飛航安全調查委員會及不當黨產處理委員會，前者職司飛航安全事件之調

[307] *See* Jiunn-rong Yeh, *Experimenting with Independent Commissions in a New Democracy with a Civil Law Tradition: The case of Taiwan*, in COMPARATIVE ADMINISTRATIVE LAW 260-262, 246 (Susan Rose-Ackerman & Peter Lindseth eds., 2010).

[308] 通訊傳播基本法第 3 條。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

查，後者針對政黨及其附隨組織之財產進行調查。這些獨立機關，其職權行使皆無對其他中央機關法令落實情形的管理，與個人資料保護專責機關所需負擔的任務有所差異。以此形式成立主管機關，在管理中央政府各部會個人資料落實情形上，是否能順暢執行，將是此種形式設立之主管機關能否有效運作的關鍵。

(3) 由現有獨立機關處理

設立個資保護專責機關的第三種選項，便是交給現有的獨立機關處理。在我國現有的獨立機關中，中央選舉委員會、促進轉型正義委員會及不當黨產處理委員會的職權，與個人資料保護相距甚遠，幾乎不可能合併。因此，以下將僅就國家通訊傳播委員會及公平交易委員會進行較深入的討論。

A. 由國家通訊傳播委員會負責

英國個資主管機關資訊長辦公室是由該國數位、文化、媒體暨體育部所贊助，同時數位、文化、媒體暨體育部亦負責與通訊傳播有關事項之管理，並擔任通訊傳播事業監管的「通訊局」（Office of Communications, Ofcom）的贊助機關。考慮到通訊傳播事業擁有大量個人資料，而資通訊技術的進步，亦為推動各國個資保護法制發展的重要因素，將個人資料保護的主管機關交由通訊傳播主管機關辦理，似乎並不是難以想像之事。

然而，姑且不論個人資料保護法所適用之產業規模遠較通訊傳播產業來的大，在我國若要將個人資料保護法交由國家通

本報告之智慧財產權歸屬於財團法人資訊工業策進會

訊傳播委員會主管，尚有一組織上之困難。依據中央行政機關組織基準法之規定，相當中央二級機關之獨立機關，其業務單位以四處至六處為原則[309]。目前，國家通訊傳播委員會已設有六個處[310]，達到中央行政機關組織基準法所規範之上限。誠然，此一規定並非強行規定，但在政府組織總量管制的大前提下，任意「突破」法規所定之組織原則，仍勢將遭遇反對。

B. 由公平交易委員會負責

除了由國家通訊傳播委員會負責外，陳錡雄教授則建議，可以考慮仿照美國的模式，將個資保護視為一種競爭議題，由公平交易委員會負責處理。美國目前雖無個人資料保護法制的統一主管機關，但由於聯邦貿易委員會負責消費者隱私議題，實際尚以能涵蓋大部分非公務機關處理隱私時的保護問題。當前，我國公平交易委員會共設有 5 個處，尚有增加組織編制的空間[311]，亦是優勢之一。然而，由於個人資料保護法亦規範公務機關對個人資料之蒐集、處理與利用行為，此部份是否適合由公平交易委員會管理，確實尚存疑問。

3. 其他可行方法

前述之制度安排，大體上係以於行政院下設立專責機構的方式進行

[309] 中央行政機關組織基準法第 32 條第 1 項。
[310] 本會組織架構，國家通訊傳播委員會，https://www.ncc.gov.tw/chinese/content.aspx?site_content_sn=2898&is_history=0 （最後瀏覽日：2018/12/03）。
[311] 組織與職掌，公平交易委員會，https://www.ftc.gov.tw/internet/main/doc/docDetail.aspx?uid=522&docid=12191 （最後瀏覽日；2018/12/03）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

思考。惟我國對於主管機關的安排，尚有其他少見，但仍有前例的其他模式。以下，將討論此類方法的可行性。

(1) 由行政院擔任主管機關

針對類似像個人資料保護這類具有跨部會性質的業務，我國亦有由行政院擔任主管機關的前例。舉例而言，資通安全管理法即以行政院為主管機關，並在院本部下設立「資安處」負責相關業務的推動。消費者保護雖由各中央目的事業主管機關分別負責，但行政院未收統籌之效，亦於院本部下設立消費者保護處。類似的案例上有環境基本法有永續發展委員會負責統籌等。然而，採取這樣的管理方法，仍有挑戰須面對。首先，由行政院擔任主管機關，雖然在憲法規範架構上以為最高行政機關，形式上既然為「最高」，就應該具備一定程度的「獨立效果」。然而，實質上行政院長並無任期之保障，由行政院擔任主管機關，是否能有效發揮「獨立」之實質效果，殊值懷疑。此外，就行政院本身之人力而言，是否有足夠之人力負擔個人資料保護之管理，亦存有疑問。

(2) 由監察院擔任主管機關

與由行政院擔任主管機關的構想相較，由監察院擔任主管機關雖然是一個更為罕見的作法，但其仍有其可能性。我國禁止酷刑及其他殘忍不人道或有辱人格之待遇或處罰公約施行法草案第 4 條，就規定由監察院設「酷刑及其他殘忍、不人 道或有辱人格之待遇或處罰防制相關委員會」，負責定期訪查行政機關是否落

本報告之智慧財產權歸屬於財團法人資訊工業策進會

實禁止酷刑規範、受理人民陳情、調查事件、提出建議及撰擬年度報告等工作。

監察委員由總統提名經立法院同意後任命，並有任期保障之規定，且得依憲法規定獨立行使職權。監察院之獨立性並無疑問。監察院作為憲法定位的國家最高監察機關，其憲法職權包含彈劾、糾舉及審計權，尤其作為監督政府落實個人資料保護之基督機關，並無扞格或窒礙之處。由監察院負責個人資料保護之落實，其可行性上之最大爭議在於憲法規定行政院為國家最高行政機關，行政一體亦為我國憲法所揭示的重要價值[312]。由監察院擔任個資法之主管機關，行使行政權管理非公務機關個資法令之落實，是否違反行政一體之憲法誡命，實有疑問。

(3) 由行政法人負責

另一個可能的制度安排，是參考英國資訊長辦公室的案例，設立行政法人負責個人資料的監管問題。雖然我國目前規範要求獨立機關須為合議制機關無法以獨任制機關型式存在，但由於行政法人董監事採任期制[313]，對於其組織的獨立性仍較一般機關高，有符合歐盟 GDPR 對於獨立專責機關機關要求的可能。然而，根據我國目前之規範，行政法人應僅負擔涉及公權力行使程度較低之公共事務[314]，個人資料之管理牽涉到行政罰等較高強度之公權力行使。就我國目前行政法人之定位而言，由行政法人負責個資

[312] 司法院釋字第 613 號解釋。
[313] 行政法人法第 6 條。
[314] 行政法人法第 2 條第 2 項第 3 款。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

法相關事項，恐怕並不妥適。

持平而論，以行政法人之手短管理個資事物有其優點，例如具有相對教高的獨立性，行政法人職員可以由非公務員擔任、程序上也較為靈活，可以提供行政效率與彈性[315]；但我國目前制度設計的假設上，並未預設由行政法人負擔有較高程度公權利之事務，若要由行政法人負責個資事務，除須制定行政法人設置條例外，尚須修改行政法人法，其修法難度教高，虛有高度政治意志，才有可能落實。

4. 小結

綜合上述的討論可以發現，各個解決方案各自都有優缺點，尚無一絕對妥適之方案。由於國家發展委員會在定位上幾乎不可能轉型為獨立機關，其他可能方案也都需要極高度的政治意志方有實現的可能。因此，主要可行的方案當由另立獨立機關或由現有獨立機關兩個方案之中選擇。

此外，再考慮到現有中央行政機關組織基準法對於相當中央二級機關之獨立機關在總量及組織編制上的限制，另外設立相當二級機關之獨立機關或由國家通訊傳播委員會主管等兩個選項有現行法上的實質困難。故，最後應於「成立相當中央三級機關之獨立機關」或「由公平交易委員會主管」這兩個方案中，考慮現有機關員額編制，以及行政機關層級對於其執法難易程度影響等因素，做出最後之採擇。

[315] 彭錦鵬，〈行政法人與政署之制度選擇〉，《考銓季刊》，第 53 期，頁 31-32（2008）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

陸、結論與建議

一、數位匯流法規及隱私保護法規之規範

就整體發展脈絡而言，本研究本次所觀測之國家中，英國及日本皆有因應科技進步之衝擊，而修正其個資保護法規。相較之下，美國雖尚無聯邦層級實際的法律變動，但在州層級，已經出現相關的立法，而在聯邦層級上，亦曾有立法的倡議。因此，至少可以認為，即便法制背景各異，但是各國普遍感受到技術發展對於隱私保護法規之影響。然而此一調整之方向，並非是採取「放鬆管制」的立場，而是進一步加強資料當事人權益的保障，並在不降低主要保護架構的強度情形下，適當的調整規範內容，回應技術之需求。

(一)取得各種資料類別之行為規範

我國與其他國家相較，較為明顯之差距在於：針對兒少個資保護之規範上並無特別之規定；而英國及美國皆對此有特別之規定，要求對一定年齡以下之孩童蒐集、處理、利用其個人資料時，除少數明文例外外，皆需經家長或監護人的同意；並對於後續資料保存等，也有相較該國其他資料而言更為嚴格之規定。我國目前個資法既然並無特別之規定，則應回歸民法對於未成年意思表示之規定處理，七歲以上之未成年人，除純獲法律上利益，或依其年齡及身份、日常生活所必需的情形以外，應得法定代理人之允許，才算有效。但，何謂「依其年齡及身份、日常生活所必需」終究仍相當模糊，有進一步釐清的必要。

因此，本研究建議，基於保護未成年人個人資料之權利以及降低業

本報告之智慧財產權歸屬於財團法人資訊工業策進會

者在蒐集、處理、利用未成年人個人資料的不確定性的角度而言，短期內主管機關可以依據《兒童及少年福利與權益保障法》第 46 條第 1 項的規定，召集各目的事業主管機關、委託民間團體成立內容防護機構，推動網際網路平臺提供者就兒童、少年個資之蒐集年齡、取得父母或監護人同意之標準等，先行建立自律機制。透過由業者自律、民間團體及相關政府機關參與的多元協作模式，探索出實際符合我國國情之年齡規範及技術方法。以符合具有我國內國法效力之《聯合國兒童權利公約》第 16 條對於兒童隱私權保障之意旨。

(二)個人資料保存機制

我國通訊傳播事業個人資料保存機制，雖然在個資法規範的較為寬泛，但在通訊傳播領域，因為各項法規命令及行政規則的補充下，就資料保存期限及紀錄與證據保存的相關規定而言，與其他國家並無明顯的差異。不過，就適當安全維護措施而言，觀察各國對於安全維護措施之規定，為了防止資訊處理業者內部或外部的不正當行為，導致個資外洩等，使監督責任區分更加明確化，因此往往要求資料控制者應設立具有一定職權的保護員。而我國目前之安全維護規範，並未強制要求設置此類似之保護監督管理者角色，與美國之規範較為類似。就組織上，我國僅要求應設置適當人員管理，對該人員之職權、應負責事項等，缺乏較明確之規定。

考量到通訊傳播事業掌管資料量相當龐大，建議可以參考日本及英國的規定，在國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法中，要求相關業者配置之管理人員應具有一定程度之獨立監督之職權，並應賦予其確保組織內部個資管理順暢之功能。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(三)資料釋出之授權規範

我國就資料釋出給第三人部份的規定，與本研究研究之國家而言，在共通原則上，並無明顯差異。不過就去識別化（匿名化）之規定，以及資料可攜權等部份，則有進一步深究之比要。

就資料去識別化（匿名化）之規定而言，除美國外，各國雖於法律規範中規定去識別化（匿名化）之定義，對對於實際之操作方式，並未以具有法律規範效力的形式明文規範。究其原因，正如同本研究訪談及研討會與會專家之建議，目前技術上幾乎無法確切得出清晰、明確且保證有效的去識別化（匿名化）的操作步驟與方法。有鑑於這樣技術上的限制，建議我國未來相關規範之修正時，可以考慮僅給予去識別化（匿名化）清楚之定義，並禁止將其重行識別；而不要直接規定去識別化之步驟或方法，以避免規範之步驟無法真正有效去識別而造成對人民權利的傷害。另參考本研究訪談中業者之意見，建議未來可輔導業者，以「賦予當事人參與資料釋出決策」的方式，取代去識別化之模式，平衡當事人權利與資料加值之需求。

就資料可攜權的議題而言，GDPR 規定資料當事人有權請求控管者以結構化、通常使用且機器可讀的格式，將其基於同意或契約關係所提供之資料，以及依據自動化方式處理之資料提供給資料當事人或其指定之其他資料控制者。此一權利係為反應數位匯流時代消費尋求不同資料控制者提供服務所衍生之需求，確實有其時代意義。然而，由於不同資料控制者間資料規格、格式等並不統一，目前英國個資主管機關就資料控制者間如何基於資料可攜權互通資料，並未訂定明確之內涵，僅以指引型式提供業者處理上的建議，希望業者能逐漸發展出共通之標準。以

本報告之智慧財產權歸屬於財團法人資訊工業策進會

我國電子病例的推動狀況為例，不同醫院間也需要多年時間才能逐漸制定統一的規格。考量到目前大部份領域之資料也缺乏統一之標準，資料可攜權此一新興權利型態目前可以說是尚未完全成熟，貿然以具有法律拘束力的規範引入此一權利，恐怕使權利難以落實。研究建議，短期內可以以心態上有意願、技術上有能力且同一類別業者數量較少的產業領域為主，政府以輔導、鼓勵方方式與這些業者共同討論資料互通所需的資料格式、欄位標準等議題，形成架構後，建立一先期的典範。後續在就國際規範發展、民眾需求、技術能力等條件，進一步擴散此一互通之標準，或是討論是否須於法律成面承認此一權利。

(四)隱私蒐集評估機制

就本研究所觀察之國家而言，僅英國在 GDPR 的規範下設有隱私蒐集評估機制。此一機制目的在於協助業者在採取新技術（如自動化決策處理技術）之前，透過影響評估識別出風險，並評估可採行之減輕措施。對於業者完善資料治理，建立民眾對資料使用之信任有所助益。雖然各國並未以法律規範此一評估機制，但觀察國際發展，在各國隱私主管機關間，似乎已經逐漸形成「應該引入類似之風險評估機制」之共識。建議我國可以以「鼓勵」與建議的方式，引導業者在採取應用新的技術之前，得以先採取類似之步驟，以降低技術可能帶來的風險。

(五)資料側寫議題

就本次觀測的國家而言，僅英國在 GDPR 架構下對於資料側寫技術有明確的規範；規定使用資料側寫技術處理個人資料前應進行資料保護影響評估；同時，除非是基於契約所必須、法律規定或當事人的明確同

本報告之智慧財產權歸屬於財團法人資訊工業策進會

意，否則應給予當事人拒絕單純採用側寫等自動化處理技術處理而對其造成法律效果或其他類似重大影響之個人資料處理的結果的權利。此外，無論如何資料之控制者仍應對當事人提供部份參與、意見表達及挑戰該技術產生之決策等權利。

這樣的規範有兩個主要的精神：第一是採用側寫等自動化處理技術將對當事人造成特別之風險；第二則是決策仍應以人為中心，應確保側寫等自動化處理技術產生之結果是透明、可以解釋的（如此當事人才能對其決策進行挑戰)。雖然目前僅有歐盟將其直接規定入法律之內，但類似的倡議在國際間也已經不斷出現。國際間對於採取資料側寫技術進行個資處理前應進行隱私風險評估以及對於相關技術應該具有可解釋性、透明性等，似乎已經逐漸形成共識。我們似乎可以預期，針對資料側寫技術的風險評估及對其解釋性的要求，將會在近年內逐漸加強。

而就臺灣本身通傳資料而言，目前我國業者亦有逐漸引入這類自動決策技術的傾向。這類技術的引入一方面將會降低資料控制者處理資料的成本，相對的也就可能可以使使用者能以更便宜的代價來換取服務。在國際間一方面對此一議題逐漸形成共識、漸有將其轉化為規範的趨勢；一方面對於技術的發展仍待投入的背景下；我國若能在此時，與資料當事人、業者就如何使側寫等自動決策技術具備解釋性、如何評估相關技術可能之風險等議題進行廣泛討論，逐漸形成我國之共識，並適當投入技術的研發。搭配我國相對成熟的技術環境，相信可以在國際逐漸形成規範的過程中，同步、甚至領導相關規範的形成。對於我國相關產業的發展，具有重要的意義。因此，建議我國可以一方面投入具可解釋性之側寫技術研發，一方面可以擬定側寫技術風險評估之方法，以因應

本報告之智慧財產權歸屬於財團法人資訊工業策進會

側寫技術應用可能產生之風險。

(六)資料加值應用與隱私保護之調和

就上述的規範發展而言，若從資料加值應用的角度觀察，大致上可以得出下列三項主要之結論。

- 國際間資料保護標準並未因技術進步而退讓

  在技術進步的背景下，資料加值應用的可能性大幅增加。因此有人主張或許有因此降低資料保護規範的可能。然而，就本次研究所觀察的各國規範而言，目前尚未看到各國有因此降低資料保護的規範密度。與之相較，各國目前對於新興技術反而採取比較保守與謹慎的立場，甚至有逐漸成為國際共識的趨勢。

- 去識別化標準難定義

  觀察各國之發展以透過訪談及研討會所蒐集的專家意見，本研究發現，當前對於去識別化標準與實施步驟難清楚、明確、有效的詳加規範。因此，至少短期內，要以去識別化方法最為資料加值應用的解決方案，是難度較高的。

- 利用技術協助賦權消費者，建立資料加值之信任基礎

  透過個資去識別化以促進資料加值應用雖有技術可行性上的難度，本研究建議可以透過其他技術協助消費者之賦權、建立消費者對資料加值應用之信任，以使資料經濟能妥善發展。

  過去認為資料加值最大的難題在於難以取得當事人對資料利用條件的同意，但這樣的難題困境在近年來已經有逐漸改善的跡

本報告之智慧財產權歸屬於財團法人資訊工業策進會

象，就本研究蒐集之外國案例及研討會中與會專家之經驗分享，可以發現各國開始頻繁出現以技術方法協助消費者參與資料釋出決策、建立信任基礎、促進資料加值應用的案例。

本研究建議，我國可輔導業者透過技術的方法，使資料當事人更容易行使其權利。透過這樣的方法，使其信賴資料加值應用的體系，進而可以在使當事人個資受到保障的情況下，促進資料加值應用的發展。

二、歐盟隱私及電子通訊規則（ePrivacy Regulation）草案之發展

歐盟基於數位單一市場戰略之指引，以及考量到 ePrivacy Directive 立法後，資通訊技術帶來的新的規範需求，在完成 GDPR 之制定後，進一步展開電子通訊相關規範之修法作業。其於 2017 年提出 ePrivacy Regulation 草案，原本希望與 GDPR 一起施行，但目前仍未完成相關之立法程序。

就草案本身及目前歐洲議會及歐洲理事會討論之情形歸納，大致可得出以下幾項重要結論：

- ePrivacy Regulation 擴大原先 ePrviacy Directive 的適用範圍，將該指令通過後大量發展的新型電子通訊服務提供者，包含電子郵件、簡訊、即時訊息等不同類型之服務，皆納入管理範圍。
- ePrivacy Regulation 為 GDPR 之特別法，應優先適用。無論 GDPR 或 ePrivacy Regulation 草案，皆有類似之規定。換言之，就 ePrivacy Regulaion 草案所規範之範圍，應優先考慮其規範之內容。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

- ePrivacyr Regulation 草案在處理的合法要件上，比 GDPR 更為限縮。ePrivacy Regulation 草案規定，原則上禁止蒐集、處理、利用電子通訊資料（包含電子通訊的內容及詮釋資料），依據資料類別的不同，皆僅有目的相當限縮的少數例外。即便是基於當事人同意所為的處理，往往也有額外的條件限縮（例如必須是不處理該資料便無法提供服務，或與監管機關諮詢等情形）。不過，目前審理過程中，歐洲理事會有在局部放寬處理要件的規劃。

- 就儲存時間而言，ePrivacy Regulation 草案也較 GDPR 規定更為限縮。與 GDPR 不同，ePrivacy Regulation 草案並未如 GDPR 一般規定可基於某些特定具有公共利益或學術研究目的放寬資料保存之限制，而是規定資料須在完成服務後，立刻刪除或去識別化處理，僅計費所需的詮釋資料，因為有法律爭執的可能，可保存到爭執期限結束為止。

- ePrivacy Regulation 草案對於隱私設定的方式，較 GDPR 規範的更為清楚。該草案要求提供電子通訊之軟體（包含於網路上搜索和提供訊息者）應提供防止第三方在最終使用者終端設備上儲存或處理已儲存資訊的選項，並在安裝軟體時通知使用者隱私設定的選項，在安裝過程中取得使用者相關事項的同意。

目前，由於 ePrivacy Regulation 草案在歐洲議會及歐洲理事會的審理過程中，仍有許多不同之意見。無論是本研究自行之觀察，或歐盟當地政府機關及隱私專業從業人員之見解，都認為短期之內 ePrivacy Regualtion 草案不會迅速的通過，且通過後仍會給予一定的緩衝調整期

本報告之智慧財產權歸屬於財團法人資訊工業策進會

間。因此，短期內暫時不會帶來急迫之影響。但是，由於該草案對於電子通訊業者的規定相當嚴格，建議仍應持續的觀測法案後續之發展。

三、研析成立個資保護專責機構之必要

由於我國既定政策立場希望取得歐盟 GDPR 適足性之認定，GDPR 適足性規範中，要求個資保護之機關須具備獨立性。而事實上由於獨立性之規範要求，即便並未要求須為「專責」或「單一」的主管機關，但歐盟各國及取得 GDPR 適足性認定之國家，亦都以單一、專責的主管機關管理個資保護事宜。是以，即便世界上仍有國家（如美國）以分散式管理的模式管理個資議題，但對我國而言，似乎仍有設立專責機構之必要。

就我國目前行政體制而言，雖然有：由現有個人資料保護法主政機關轉型為獨立機關、另外成立獨立機關或是由行政院、監察院或行政法人擔任主管機關等不同的可能制度安排，但考量到各機關之定位、組織編制以及憲法、中央行政機關組織基準法及行政法人法對於各機關之數量、任務類型等之規範與要求，目前應以「成立相當中央三級機關之獨立機關」或「由公平交易委員會主管」此二方案在我國較有事實上之可行性。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件一 訪談紀錄

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談紀錄	
受訪單位：	中華電信法務處
受 訪 人 ：	鍾國強協理
訪談日期：	107 年 7 月 16 日 10:00-11:00
訪 談 人 ：	資策會科法所王德瀛、林玉書研究員
紀　　錄 ：	資策會科法所王德瀛、林玉書研究員

問題（一）目前不同類型個人資料處理，受不同主管機關管轄，規範密度亦有差異，目前是否因此有所困擾？

受訪者：目前是採用同一種管理標準應對不同類型之資料，因為皆採較嚴格之標準，故並無太多困擾。

問題（二）了解貴公司目前也有計畫針對個人資料進行巨量資料應用，不知道這部份是否有一些法規上的建議？

受訪者：目前個資法的規定下並沒有給予太多的空間，除了將個人資料進行去識別化。但是個資法對於去識別化卻未給予清晰之定義，導致無法確認何種程度的處理可以達成去識別化，造成實行上的困難，有綁手綁腳之感。日前標檢局的國家標準其實也沒有實質的標準。建議政府可以明確規定去識別化的定義或標準，或是由第三方協助驗證是否達成去識別化的結果（並能確保其完成去識別化）。

問題(三)如果制定一些隱私的指引或是實務操作的建議是否會有幫助？

受訪者：對我們而言，因為都採取嚴格的方法來實施，所以不會有太多的影響。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

問題（四）對於設立個資個資主管機關是否有特定的看法？
受訪者：如果是不同目的事業主管機關管理，寬嚴標準可能會不同。所以單一的主管機關會比較好，至於是那一個單位擔任主管機關，我們沒有特別的意見。

問題（五）對於個資法的其他建議，例如對於目前實際應用的限制？
受訪者：雲端、大數據等應用目前都會因為個資法而受到限制。目前個資的處理僅用在公司內部的分析（如行為、喜好、產品開發、資費擬定等），不會對外提供。此外，個資法上有許多不確定法律概念，缺乏指引標準，例如「有利於當事人權利」的判斷標準等，目前都缺乏實質的標準可以參考。

問題（六）請教有關 MOD 收視率普查資料的應用情形。
受訪者：收視率普查結果因為考量到可能是個資的風險，所以目前沒有公開。

問題（七）請教是否有針對未成年個資蒐集做特別規定？
受訪者：認為目前並沒有蒐集未成年資料（以 MOD 為例，都是成年人申請，資料歸檔到申請人身上，尚無蒐集未成年之問題）。

問題（七）請教目前漫遊資料的交換是否有受 GDPR 影響？
受訪者：漫遊的交換上，並沒有受到 GDPR 的影響，一切照舊。因為僅交換了特定行動電話內碼通話多長、花費多少等資訊，目前大家不認為這樣有涉及個資的內容。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談記錄	
受訪單位：	中原大學財經法律學系
受 訪 人 ：	江耀國教授
訪談日期：	107 年 7 月 18 日 13:00-14:00
訪 談 人 ：	資策會科法所宋佩珊組長、王德瀛、林玉書研究員
紀　　錄 ：	資策會科法所王德瀛、林玉書研究員

問題（一）如果是想要推動民間資料的聚合，大致上討論上可以分為現有財團法人、民間公協會、公私協力、標案推動或是行政法人等模式，不知道老師對這方面有什麼樣的看法？

受訪者：這種聚合會設計「成立資料庫」，也可能會有「平台」的效果，最後才是「組織體」。要思考，平台除了聚合民間資料外，是否還有其他功能；另外還應該要釐清是否有必要委託或設立一個特定的組織體。在組織上來看，行政法人似乎較不適合，臺灣目前的行政法人大多都是有長期運作的基礎，才轉換角色，臺灣現在較缺乏新設行政法人成功的前例，且組織法設立等所需成本也較高。折衷來看，或許由現有的財團法人兼辦會較為適合。

問題（二）對個資法是否設立專責主管機關的看法。

受訪者：因為 GDPR 規定個資主管機關需有一定的獨立性，在我國要爭取適足性認定前提下，建議以設立新機關為宜。從歷史脈絡來看，法務部長期負責個資法的立法、修法以及解釋，目前就個資法的解釋、應用的專業知識主要是累積在法務部的法律事務司，因此可以考慮在法務部下面設立一個三級的獨立機關負責（因為法務部的人力及編制目前不足以因應）。不過若考慮到意願問題，也可以另外新設。這個機關不一定要是獨立在不同部會之外，可以是在部會內部；但如果由其他機關負責，可能會有專業知識難以延續或移轉的問題，應該確保人員、經驗能夠繼

本報告之智慧財產權歸屬於財團法人資訊工業策進會

受與移轉。新機關的另一個考量點在於原先「目的事業主管機關」的架構，不論是 GDPR 的適足性，或是我國實務上，都不是很理想。我國對於個資管理較為專業的，應該仍只有在原先電腦個資法八大產業的主管機關才有比較多的累積；新個資法架構下有些機關會負責本來沒有管理經驗的行業（例如因為企業在經濟部獲得營業許可，及由經濟部管理，但經濟部沒有管理此些行業的經驗，可能難以落實）這種垂直的概念有所限制，不如由統一主管機關「水平式」的管理，也不錯。

問題（三）收視率蒐集的隱私問題？

受訪者：收視率主要兩種可能，一種是抽樣；另外一種則是在可以掌握母體的前提下，以普查的方式呈現。抽樣制的公司實務上多是以取得同意的模式來進行抽樣。普查形式的收視率調查，是不是個資法的蒐集，又是不是合法的個資法蒐集，會是爭議的焦點。這個概念類似「健保資料庫」的狀況，重點有兩個：資料本身是否足夠去識別；以及管理者可否再為通知當事人的狀況下將個資去識別。如果蒐集時，仍然知道是特定用戶的收視行為，那該資料可能還會是個人資料；但技術上有討論空間的是，若「下載所有人的收視資料」，沒有「識別」任何人，也無法回推識別任何人，就不會是個人資料。要具體看行為態樣才會比較清楚。但大體來看，若是做統計用的資料，如果以非個資方法蒐集，風險程度會比較低。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談紀錄	
受訪單位：	中華電信 MOD
受 訪 人 ：	王莉貞總監
訪談日期：	107 年 7 月 19 日 14:00-15:30
訪 談 人 ：	資策會科法所王德瀛、林玉書研究員
紀　　錄 ：	資策會科法所王德瀛、林玉書研究員

問題（一）去識別的標準及資料應用上有沒有一些困擾？以及在數據資料公開與否方面，希望了解一些比較實務上的經驗？

受訪者：中華電信的收視率是一個普查的概念，針對蒐集的資料，原始碼會是自始完全去識別化的。因為大家都知道資料進來時，如果都是數字和代碼本來就是系統或 data base 的處理方式，原始資料其實一律使用代碼代表客戶，可以說是去識別化的，或者是根本沒有識別化的問題。第二個問題 比如說尼爾森收視率的資料，當向其購買收視率資料，它就公開，中華電信也是採取這種模式。在平台上的頻道有收視率，算是合作夥伴，我們須公開收視率讓它了解，但中華電信不販售這些資料，而是利用收視率來做分潤這件事情。所以中華電信的資料不會像尼爾森，比如說委託你做一個專案調查，他就拿這些資料做專案調查，中華電信不會做這件事，我們僅單就分潤的這些資訊告訴營運商，我們不會作任何的再利用。

問題（二）在個資的處理上，中華電信本身有些相關的技術，事實上沒有跟其他業者合作的需求，想請問貴公司在整個個資處理的流程，包含巨量資料的處理上是否在法規面覺得現在的解釋不夠清楚？或是規範過於嚴格？或是規範不足之處呢？

受訪者：法規規範是否過於嚴格這部分，我不太清楚公司內部有沒有考

本報告之智慧財產權歸屬於財團法人資訊工業策進會

量，回來另一個層面而言，很多人都誤認為中華電信有大量的數據資料，一定可以做一些應用；但其實距離真正去執行還有好大一段距離。
回來法規層面觀之，個資法已經行之有年，很難從大數據去更改個資法，因為個資法是世界的一個潮流，GDPR 的出現表示有更為嚴格的傾向，台灣相對其他國家法規上反而不是最嚴格的。我個人認為，每一個人的資料是要被謹慎看待及利用的，這是世界對於人權尊重的趨勢，關於如何把這些數據去做利用，又是另外一條很長的路要走。
我覺得要有人走過這些路，你才知道欠缺了什麼東西，需要有經驗去做這件事情，我個人在公司內部看到的是，數據太大使得雲端不夠承載、軟硬體的不足，在從事業務的人與做系統的人之間，其實是兩個不同的層面，我需要的東西他不一定能理解、不一定能做得出來。反觀，尼爾森可以做一些專案分析，那是因為他們在這個領域上累積了長久的經驗，以及在影視產業的深耕，他們有統計、系統的專業人員，也有模組等相關資源，去建立這件事情。
相對地，中華電信所擁有的資料其實可以變化很多，但如何變化、如何跟業務面或市場面做結合、應用上的問題又是另外一個層面；其實該怎麼做本身就是一件非常困難的事情，例如要做一個系統，其實 user site 常表達不清楚它的需求是什麼，係因 user 的作業跟寫系統是兩件事情，我認為中間要有一些所謂的中間人角色，舉凡寫系統部分，有一個系統分析師或是前端、後台設計人員，去整合大家彼此之間的落差。

問題（三）在這件事情上中華電信內部的運作流程，會需要法務方面的人進來一起參與過程嗎？還是僅單純業務和系統中間的流程呢？
受訪者：原來做大數據的人，他一定至少有基本個資的概念，法務方面的問題中華電信比較沒有牽涉到，因為電信公司基本上是遵法的單位且被高度監理，因此中華電信比較沒有這方面的疑慮。

問題（四）中華電信內部自己有一個依循個資法產生的個資保護規章政策，大致上貴公司目前是按照這樣的個資規章來運作，請問是否有遇到想做但礙於目前的政策，而不能做的類似狀況？
受訪者：公司內部不管是法律或員工教育的部門，或是對於個資的追蹤、認知等等，中華電信算是蠻完善的，有訂定一套標準去執行。至於利用上面有需要，比如說法規突破方面的問題，因為最近 GDPR 的議題，大家都有不同的解讀。
而關於數據利用上有沒有需要法律上的支持而言，像是去識別化，主管機關 NCC 其實對系統也不了解，無法去判斷去識別化是否為有效的，

本報告之智慧財產權歸屬於財團法人資訊工業策進會

他們相信中華電信不會去觸犯法規，並會去做嚴格的考量。例如收視率的部分，NCC 也有問過我們去識別化的問題，甚至提供過往的資料給 NCC，我們提供出去的都是經去識別化資料，並且還要跟 NCC 解釋是基於什麼原因，所以我們對此進行去識別化等等。因而，我在識別化上，至少我碰到的例子，沒有這方面的問題。

問題（五）關於法規上有沒有需要突破的地方？

受訪者：我認為現在法律規定蠻明確，公司的教育也傾向於嚴格，我們也付出蠻多的行政成本去建置相關因應措施，公司還希望資料不落地、對資料的管理很嚴格、公司的資安處也有既定的模式，除非政府現階段的政策有重大改變，否則暫時沒有。

問題（六）那 MOD 的這些數據資料大概還有哪些可能的應用的形式？

受訪者：用戶的資料、用戶收視率基本上對於我們 mod 來講，我們是不會使用，也不會再去利用。另，對於非收視率的其他資料，例如流量及點擊率跟個資沒有關聯性。

問題（七）mod 在其兒童專區的設計上，會不會被法務要求特別嚴格？

受訪者：mod 內容上大部份是涉及版權的問題 而且是經由鎖碼去控制，法務上的問題大部份是牽涉到訂定授權合約、合作合約；去年則因為分潤問題，我們跟頻道營運商的合約就有比較多的修改。兒童專區則沒有特別的要求。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談紀錄	
受訪單位：	景翊科技股份有限公司
受 訪 人 ：	陳奕廷總經理
訪談日期：	107 年 7 月 20 日 14:00-15:30
訪 談 人 ：	資策會科法所王德瀛、林玉書研究員
紀　　錄 ：	資策會科法所王德瀛、林玉書研究員

問題（一）在蒐集交通類別資料的時候，就資料的蒐集與整合，一些業者對資料的格式或是這中間的商業機制該如何設計？或政府是否能在商業機制上扮演一些角色，希望從交通方面的經驗，借鏡給通傳領域的主管機關做參考，進而檢視是否需要在法規上做調整？

受訪者：關於資訊整合應用部分，在通訊領域中，大家知道手機就有所謂的 SIG IN 資料，也就是透過藍芽系統感知，蒐集個人移動的所有訊息，代表了移動的模式，並從移動模式可以去推估大家對於交通方面的需求及方式。而這些資料可以讓我們變得很方便，串聯過程中會經過很多基地台，電信業者可利用這些資料做很多應用，並在符合個資保護前提之下。

而這些可被利用的數據，像日本的電信業者 Docomo 與計程車合作，提供位置資料以知道哪些地方人比較多，統計出叫車熱點，增加計程車司機收益的機會，幫助提升業績，這種異業結合的資料應用會是一種發展趨勢。然而，這樣的行為其實會使整個產業在利用上產生比較大的問題，從這些交通數據可以知悉很多資訊。例如，了解民眾的交通行為模式，進而去推展一些政策，舉凡外國旅客購買電信預付卡就能夠得知其旅遊住宿、飲食地點，追蹤這些行動軌跡，雖然即便會把個資都拿掉，但會知道國家別、性別等。

目前經由自動化的方式取得這些資料可以獲得一些有趣的事情，這件事

本報告之智慧財產權歸屬於財團法人資訊工業策進會

情在 SIG IN 資料的運用上越來越普遍，不僅在於交通方面，觀光行銷顧問這些方面利用多方蒐集的數據資料，去做進一步的運用情形也越來越多。

問題（二）在付費交換大數據的部分，台灣一些中小型業者若想要發展資料付費交換的機制，以您的視角可行嗎？
受訪者：資料鑑價其實眾說紛紜，即便釋出資料，但其商業性價值可能就沒這麼高，且這裡面也牽涉到資料鑑價的問題，很難認定等不等值。

問題（三）對於大數據交換這種形式，當然可能不是很健全，但是不知道您覺得這類像對岸公開市場的模式，會不會是一種解決方式？
受訪者：一定是一種解決方法，但他們其實是用國企的概念在經營這件事情。

問題（四）如果台灣發展資料鑑價的機制，您認為能夠如何調整？
受訪者：資料能否被交易，牽涉到大家對於資料的取得難易、價值高低、可用的程度跟價格能否被接受。

問題（五）以資料為主的經濟會是未來台灣民間或政府重視的地方，您覺得除了資料本身很難衡量其真正價值以外，為什麼這樣的機制難以妥善地建立起來？
受訪者：這件事情若它的門檻很低，那這些資料可能是沒有價值的，所以 open data 很多都是沒有價值的，許多資料還須經過處理做成 API，然後才能進而做成網站以一些報表的方式呈現、提供分析。過程中從 raw data 經過處理、轉換過程，再以客製化的方式提供，事實上這裡面真正賣的不是 data，而是這裡面所有處理過程所需的勞力、時間、費用。
我們公司在資料交易方面，是自公部門取得資料，經過資料清理、處理，轉換為高品質的乾淨資料，成為符合國際標準的資料後再售出。至於資料能否賣出的原因有：對於處理資料這件事情，當我們把資料處理成國際標準，具備更好的品質時，除了與國際大廠合作，目前也會從民間部門取得資料，透過我們公司處理後，協助他們將資料賣給國外。因此，我認為在整個資料經濟模式這件事情，同樣的資料不一定賣得出去，而是在於將資料做區隔、建立門檻及品質，自然具有市場競爭性。

問題（六）若政府協助業者建立資料的品質、標準，對業者會有影響嗎？
受訪者：我認為不是政府可以有效去做的，因為業者若不配合也沒辦法，

本報告之智慧財產權歸屬於財團法人資訊工業策進會

我覺得政府可以做的事情是「對接」，例如今天一個國際大廠需要某些資料,是否有辦法從既有的廠商這邊提供對接資源,並且在品質及 quality service 上能夠符合國際大廠需求，這件事情沒有一個共通的標準。

問題（七）目前國際上有沒有一套公認的國際標準？

受訪者：大部份領域都沒有，但像手機交通領域有國際標準，我覺得政府可以做到的是，公開資料的釋出及提升釋出資料的品質、減少廠商在做資料處理時的障礙。

問題（八）如何控制識別性障礙的風險？

受訪者：我覺得識別性不是由我們定義，而是要考量民眾的感受。蒐集資料但卻沒有經過消費者同意，做到風險管控是非常難的。在科技化的社會裡，考慮到便利安全又要避免隱私外曝，我們認為我們可以託管一些事情,假設一個中間機構 可以將個人部分的情資交由其托管,此機構可以增加便利性，甚至該個人允許機構將部分的資訊賣給別人而有所收益。

問題（九）若政府要來對個資進行管理這件事情，但因為現在資料的主管機關權責分散在不同部門，就您的經驗，例如剛剛所提到的交通部，不知道您業務上會不會接觸到其他主管機關的管理？不同主管機關間，對於個資的解釋會不會有落差？

受訪者：我覺得不管是主管機關，或是公司都一定有不夠專業的地方，在做資料的運用過程裡，常常造成很多資料都是公開的。

問題（十）貴公司針對風險管理係如何做因應，例如將資料應用到開發的 APP，但後續的一些風險管理措施您是怎麼樣去管理呢？

受訪者：針對這件事情沒有想像的太複雜，我們還是會有一些顧問 APP 去收集顧客的資料，在這過程中我們就會把所有在網路上公告的部分做加密,當這些資料傳輸到另一個端點,不會是經由明碼的方式傳輸出來，而會是經由加密再解密的方式，再去做進一步運用，我們也會用自己的防火牆去控管資安疑慮的部分。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談紀錄	
受訪單位：	交通大學科技法律研究所
受 訪 人 ：	陳錦雄教授
訪談日期：	107 年 7 月 20 日 16:00-17:00
訪 談 人 ：	資策會科法所王德瀛研究員
紀　　錄 ：	資策會科法所王德瀛研究員

問題（一）是否適合由各目的事業主管機關發布個資法的相關指引或實務建議？

受訪者：依照目前個資法的架構而言，各目的事業主管機關就所轄產業而言，就是主管機關。因此去制定相關指引或實務建議，並沒有權限上衝突的問題，不一定要去等法務部的看法。

問題（二）各目的事業主管機關是否適合以指引或實務建議的模式介入商業活動？其界線該如何界定？

受訪者：這其實是長期以來討論需要有個資主管機關的問題，因為現在許多個資主管機關是一手是促進產業發展，一手又是管制機關，所以會很尷尬。例如大數據的利用，我們可以定一個比較清楚的指引，其實是可行的。

問題（三）個資主管機關組織架構的看法。

受訪者：這可以分為兩個部份討論。在不更動整體組織架構的前提下，可以在 NCC 內部將個資管理的業務集中成一個組織（如辦公室）加以執行，並設立諮詢性質的委員會提供相關建議。這個作法應該是在未更動中央組織架構下的唯一可行作法。指引等相關部份可以由辦公室來制定；委員會可以引入更多元的參與，某種程度上算是 NCC 個資方面的內部監督機制。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

如果要改設獨立主管機關的話，可以由公平交易委員會來管理，這類似美國 FTC 的設計方式。可以一併調整公平會的委員組成以及組織內涵。這是把個資視為一種競爭法上的問題，如果不當利用個資，會是一種「不公平」的競爭行為。（依據同樣的邏輯，如果把格局拉的更大，或許可以考慮把消保處一併納入公平會內）至於未來個資的業務推廣跟監理要如何分工，可以以機關間行政協議的方式來解決。

問題（四）請教老師對於去識別化標準訂定的看法。

受訪者：因為技術不斷的在改變，實際上去識別化的標準不可能具體定的清楚，不過政府仍可以提供程序性的規定，或是提供判斷的標準，或是提供第三方的認驗證架構，來確認哪些東西是去識別的。這些東西其實是在目前的個資法架構下可以作到的。

問題（五）其他對個資法的建議。

受訪者：許多不確定法律概念應該可以有更清楚的解釋跟說明，例如對「公共利益」等的內涵。這個在未修法的方法下，可以以指引等方法來完成。雖然沒有拘束的效果，但仍能可業者更清楚的判斷標準。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談紀錄	
受訪單位：	遠傳電信
受訪人：	李和音副總
訪談日期：	107 年 7 月 25 日 10:00-11:30
訪談人：	資策會科法所宋佩珊組長、王德瀛、林玉書研究員
紀 錄：	資策會科法所王德瀛、林玉書研究員

問題（一）對通傳事業的個資管理方式、風險管理、去識別化的標準等，目前並無實質上的法律文件加以規定，請問業者認為政府是否有需要透過諸如法律文件或行政指導之方式，以不同規範密度的方法來進行管理，給予業者更多具體的遵循方向？

受訪者：首先，在去識別化方面，其法律層面的標準、以及技術規範在哪裡，對於業者操作而言頗不明確，究竟是處理到不能還原的程度？還是持有者和保管者或使用者分開即可？再者，精準行銷的界線究竟在哪裡，也會令業者感到疑惑。因而，如何將大數據資料做進一步的應用、發展數位經濟，政府沒有一套明確的區分標準，使得民間電信業者實務上在發展大數據應用時會有所窒礙難行，很難在公司業務的推展上給予一個精確的答案。因此，希望 NCC 有一套技術上的指導標準（例如以行政指導的方式規範），就個資和新創領域利用的中間區分界線在哪裡。

問題（二）以業者的觀點，是否有必要設立一個獨立的專責主管機關？貴公司目前在面對不同主管機關，處理個資議題時，是否曾遇過不同主管機關在個資的執法標準或議題的認定上面，有寬鬆不一的情形，造成在實務操作中的困擾？

受訪者：現行由各目的事業主管機關分散管理個資的方式，使得當業者發展其它附加領域、欲創造新的商業經濟模式時，所牽涉到的主管機關會有所不同，對於業務的推展時程也會造成影響，難以適時跟上該產業領域發展的速度，故期待有統一的個資專責機關解釋窗口。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

舉例而言，雖遠傳的核心業務在於電信通訊，但目前產業趨勢在於發展數位匯流，所以電信業者也在尋找、開發提供其他方面的新服務，或是促成跨產業的合作，且 OTT 服務在競爭上也有不明確之處，主管機關究竟為何？此時可能同一個服務同時涉及很多主管機關，如：金管會、經濟部、NCC 管理的模糊範疇，目前法律上亦未明確規定實際的管理機關，很可能使業者無所適從。雖然國發會目前設立了個人資料保護專案辦公室，意在介入促成協調，但機關間協調一來一往所耗費的時間，曠日廢時，直接地影響到業者在業務上的推展，效率仍有所疑慮。

問題（三）除了去識別化方面，貴公司在個資的整體其他流程上(蒐集、處理或利用)，還有哪些方面是遇到困難，需要加強的？

受訪者：在同集團之間跨平台的個資利用界線是否可以放寬或是在特定範圍內允許業者對資料加以利用（係因現行規範除非取得消費者同意，否則完全不被允許的）。也就是說，目前個資法在個資的傳遞規範上較少，希望是否能就規範內容上做些調整。

此外，私人企業若是基於公共利益的目的（例如企業社會責任、永續經營），可否對個資加以索取、利用，目前對業者而言，也是感到相當模糊的。

問題（四）有無其他相關意見，希望向 NCC 反映、建議的？

受訪者：NCC 目前固定每年來進行訪查，今年開始委外，同時也要求我們業者須自評，但我們希望建議政府考慮有一個更明確的稽核機制，並對企業的個資控管有所分級，而非每年稽核，例如當業者符合在一段年限內未發生相關個資事故，或許給予本身已控管相當嚴格的業者一些獎懲空間，係因目前業者本身也都有內部進行相關的自評、驗證機制（如 ISO 或 BSI）。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談紀錄	
受訪單位：	麟數據科技股份有限公司
受 訪 人 ：	佘志龍技術長、鄭名傑共同創辦人
訪談日期：	107 年 7 月 27 日 14:30-16:00
訪 談 人 ：	資策會科法所王德瀛、林玉書研究員
紀　　錄 ：	資策會科法所王德瀛、林玉書研究員

問題(一)我們對於現在大家如何使用通訊傳播資料的路徑不是很熟悉，所以業界操作上會有什麼樣比較困擾的法律議題？您是應用一些通訊傳播或是一些瀏覽的資料等來做分析，在這過程中您會接觸到什麼樣類型的個人資料呢？

受訪人：目前應該是接觸到個人的資料類型，除了我們在 survey 這一塊，就是問卷名單的部分，那這一塊通常都是我們的客戶所給予的；或是我們自己的 survey partner，像一些線上或是大型的問卷公司，經由他們的 panel 去進行問卷調查或市場調查。在這個區塊上，因為我們會協助客戶進行這樣的調查分析，或是跟 panel partner 合作的話，我們算是協助客戶去做資料處理或是作為資料分析的平台。

問題(二)貴公司曾提及有協助媒體公司做數據資料的分析，那大概是什麼樣類型的數據呢？

受訪人：大致上是數位廣告的分析，簡單來說就是以設備跟 cookie 做基礎，接著去分析這個設備，再跟這個廣告接觸的點，然後這當中它的瀏覽歷程。

問題(三)在不同媒體之間彼此收集到的數據的串連，但是好像有一些法規上的障礙，貴公司會面臨到什麼樣的困難面呢？

受訪人：主要還是在 google、facebook 他們的平台上面，因為我們客戶

本報告之智慧財產權歸屬於財團法人資訊工業策進會

投放在 google 上的廣告或是 facebook 廣告，廣告上面的這些 cookie 資料，ownership 還是 facebook 的廣告，但是發生資料連結的這個地方其實是在台灣的媒體網站，那這方面的資料目前就沒辦法進一步去取得和利用。

簡單一點來說，目前第三方廣告數據公司在台灣算是剛開始起步，但在國外通常是一個成熟的產業，就像電視尼爾森一樣。這裡面主要的第一個問題是媒體跟媒體之間不一定只有 facebook，就是所謂的 world garden，因為他們彼此之間可能會有絕對不會 release 的資料，再來是媒體之間的這些資料，如果能夠有效應用的話，其實對於廣告主來講能夠降低成本。

然而，目前 facebook 或 google 是現在最大的廣告投放平台，實際上市場很大一部分是被其壟斷。所以，我們想表達的概念是，目前在台灣像我們這些提供相關服務的小業者，等於是被這種國外平台幾乎是殖民的情況。

針對一個市場來講的話，台灣的法規面，應該要適時地去反托拉斯，像 GDPR 一出來，我們很快開始對 google、android 進行所謂的反托拉斯，尤其是台灣來多，我們開放接受很多外來的企業，但反過來影響到我們本土沒有自己的品牌足以與之競爭、抗衡。這個也是目前因為競爭性的關係，在市場比較小的狀況下，他們做投資的目的並非為了投資台灣，而是他整個戰略就像侵城掠地。

因此，我們想表達的一件事情就是：GDPR 目前在我們這個行業裡面是兩面刃，在歐盟的立場是想要保護隱私，但相對地某程度上這件事情，目前面臨這 google、facebook 兩大品牌，他們的競爭力已是富可敵國，尤其現在許多優勢科技上來講，他們擁有極為龐大的資料庫，遠遠超過這些各自國家可以做的。

所以，法規層面上，剩下唯一能夠制衡的就是利用法律的制定，我們的觀點認為台灣目前的立場上反而比較不是在個人隱私層次上的討論，而比較偏向整體產業的健全跟競爭力。個人隱私方面而言，我覺得台灣的個資法不斷地在演進，從上一個版本就已經規範的很深刻、嚴格，而近期 GDPR 的觀念，對台灣來講如果去配合歐盟的話，我們步調已經慢許多了，其實別人已經做了該做的事情，因而我認為這個個資法律很可能最終會限制到本國企業的發展。像 google 之前就有七天鑑賞期，不做好的話他就讓消費者的力量來反饋這件事情。

問題(四)剛剛提到 google 跟 facebook 之前是可以 mapping 的，但後來 GDPR 施行後把它阻斷掉，那麼之前是用什麼方法去 mapping 它？

本報告之智慧財產權歸屬於財團法人資訊工業策進會

受訪人：因為之前像我們這樣的平台分析業者，要先經過他們認證，我們才有權限以廣告主的名義操作，他們會要求把我們的 coding 放在他們的廣告欄位，也就是在這一波廣告曝光的同時，讓我們的程式去觸發、感知，我們就可以蒐集數據，有點像你在用 GA 的數字，協助廣告主去驗證 google 沒有灌水，我們平台扮演的角色是這樣的。
另外一個程度，是牽涉接下來的應用，我們會幫客戶把這些 raw data 存留下來，作為他們之後做資料再分析的應用。
google 比較厲害的是，他提供一個免費的平台讓所有人都去使用，然後關鍵是沒有人可取得到實際的資料，除非你付費；但其實也拿不到所有的資料，他開放給你 GAP，你卻需要付一個很高的代價，核心問題是他們拿走的東西到最後是不是應該要回到台灣？是否有權利去取得民眾自己的東西？
GDPR 施行對於我們帶來的影響在於：我們在 5/25 施行之前都可以協助廣告主去做資料取回的動作，但在 5/25 施行之後，廣告主唯一所能做的，只能付費跟他買回。

問題（五）在台灣我們對個資的定義是比較模糊的，所以像過去機器內碼這些東西一直都有一些爭議（像電話號碼），你們在這部分如何處理？貴公司目前有無這方面的困擾？
受訪人：我們把電話號碼、email、性別、身分證字號等這種列為算個資，以前機器內碼是不屬於個資的。
目前在我們這行業的認知，不太有個資這方面的困擾，簡單來說，能夠 mapping 這些個人的只有電信公司，電信公司都是高度監管，所以我們是得不到這些內碼的。我們現在唯一在幫客戶做的事情是，透過這些管道然後客戶自己再跟他們的資料庫去 mapping，且取得會員資料的同時其實已經取得個人的同意，所以對客戶而言，需要找到一個適當的館道去連結這件事。

問題（六）貴公司面對很多不同的客戶，而台灣目前個資法的架構係讓不同的主管機關彼此去管理所轄的企業，你們有遇過客戶表示他們在適用上遭逢哪些困難嗎？
受訪人：我們目前比較沒有碰到，雖然我們也有銀行業的客戶，但這種高度監管的客戶，本身對個資非常的敏感，我們是幫他們連結之後丟還給客戶，所以 data 是進到他們自己的資料庫。
我認為個資保護的重點是要把權利交給個人，但關鍵在於整體資料應用上而言，台灣是遠遠落後整個世界，應如何在可運用的範疇下去做創新

本報告之智慧財產權歸屬於財團法人資訊工業策進會

或與世界競爭，是迫切需要去檢視、因應的。

問題（七）如果是法規上障礙的話，是哪方面的法規阻擋了這方面的發展？跟台灣結構相似的個資法在亞洲也不少見，所以您認為是法律上面的問題？ 還是行政機關的問題？

受訪人：我覺得不是法律上的問題，而是整體本土企業能夠運用的資料非常有限，因此這裡面涉及的問題並非法規的關係，而是包含整個市場的承受度、對於資料的重視程度。

問題（八）貴公司有無給主管機關（主要是 NCC）一些建議？

受訪人：雖然大家都會抱怨個資法很嚴格，但台灣目前被個資法阻擋的案例目前看似較少，反倒是因為大家不了解，所以會不敢做或是沒有意識到該怎麼做。

我們反而是怕台灣又回到個資法上再去琢磨，因為近幾年才修過個資法而已，我覺得政府促進、協助台灣整體產業的升級，能與這些國外大平台競爭，為目前應重視的實際面。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制 訪談紀錄	
受訪單位：	臺灣本土 OTT 平台業者
受 訪 人 ：	數據專案經理
訪談日期：	107 年 8 月 2 日 11:00-12:00
訪 談 人 ：	資策會科法所王德瀛、林玉書研究員
紀　　錄 ：	資策會科法所王德瀛、林玉書研究員

問題（一）您剛剛提及利用觀看數據上，會面臨一些法規上比較難以實現的地方，想進一步請教大概是哪些方面會有法規上的障礙，是我們可以跟 NCC 建議的？

受訪者：我們一直很想知悉使用者外在的行為是什麼，因為希望可以透過了解他們的外在的行為，進而做一些更精準的行銷。但是每次在交換的時候，就會卡在需檢視這樣的行為有沒有符合個資的規範？如何去檢核？我們希望有一個明確的流程，可以去確認這樣的資料交換是合理、合規的，也就是資料交換到什麼程度才符合法律規定，能同時保護使用者也保護我們業者。

問題（二）上述提及關於「使用者外在行為」，希望做什麼樣的外在應用？

受訪者：希望可以透過外在的資料去了解，例如從年輕族群喜好的服務、性質去分析了解其關注的事物、生活樣貌等，希望作進一步的精準行銷。但侷限於我們這邊沒有資料去得知年輕族群是透過什麼管道去了解這些資訊，或是其他年齡層的生活樣貌是什麼，要如何接觸到這群人，例如我們目前會跟娛樂或是新聞發布相關的媒體合作，但目前沒有相關的資料去提供支持。

問題（三）使用者外在行為的部分，這樣的資料是希望可以與貴公司內

本報告之智慧財產權歸屬於財團法人資訊工業策進會

部的資料做個人，抑或是群體式的結合？
受訪者：最好的情況是有辦法對到單一的個人 。

問題（四）律師在法規上有建議什麼可突破的方法嗎？
受訪者：目前我們還沒討論到這個問題，以我們現在給使用者簽署的法條合約是可以符合交換，但還是必須以 aggregate 的方式作處理，沒辦法給予可以識別出個人的東西交換。很多媒體公司有許多使用者資料，或者是一些新創公司有在做這樣的服務，我們想知道這樣的交換可以做到多個人，在多個人的狀況下，是不違反政府規定，我們自己可以在未來進行更快速的分析。

問題（五）想要請教個資法規的遵循上面，就政府目前的規範而言，還有哪些地方可以提供業者更清楚的指引？像是資料交換到什麼程度始符合法律規定，若政府可以提供指引，會不會相對比較保全？
受訪者：我覺得應該會有所助益，但也會怕政府訂定的規定太細、過於嚴格，使業者實際操作上綁手綁腳。

問題（六）關於先前曾提及，對使用者的資料分析後，回饋到使用者身上，主要是在選材上面或大概的資料應用流程是如何？
受訪者：應用流程會分為幾個方面：我們會把使用者觀看紀錄做一個分析，例如每個月每個檔期的選片上面，亦即整個平台的服務。第二個就是針對使用者個人，比如說其戲劇偏好或是依據其用戶習慣的觀看時間，去設定推播廣告的時間，把我們的產品做到更個人化是更好的。

問題（七）在使用者資料蒐集的條款，或儲存的方法，或是類似個資的整個流程有沒有哪些地方覺得政府可以規範的比較清楚？或是建議鬆綁、可以改變的地方？
受訪者：我們當然希望保護使用者個人的隱私，到底要怎麼做才能在不侵犯個人隱私的情況下讓我們也得到這些資料，但因為我們公司是台灣比較小的 OTT 業者，倘若這些資訊可以把我們的使用者擴大的話，我們也希望可以盡量透過資料的價值，去消弭我們跟競爭對手之間的 GAP；另一個是當我們跟第三方合作的時候，到底有哪些東西需要去確認？比如彼此應該符合什麼樣的規範或是資料應該如何儲存或是檢核？

問題（八）對於 OTT 服務的主管機關為哪個部門有些疑惑，目前在主管機關的認定上會不會有模糊或是困擾的地方？

本報告之智慧財產權歸屬於財團法人資訊工業策進會

受訪者：分為兩塊，第一個是資料、資安的層面是歸誰管；第二個則是 OTT 本身的服務是 NCC 或文化部，在不同的情況下，兩個單位都會有一些想法。

問題（九）當 NCC 和文化部兩邊的想法不一致時，會不會造成困擾？
受訪者：目前暫時沒有這個狀況，但是在資料的部分，的確蠻需要一個統一的主管機關來管理，例如 OTT 服務上若有上架陸劇、陸綜，需不需要經過審核，這是過去幾個月面臨到比較大的問題。

問題（十）那麼您認為在資料面是不是需要一個主管機關？
受訪者：非常需要，因為它從資料如何蒐集、到儲存，已經是一個很專門、特定的領域，這些資料可以幫每個產業帶來什麼影響，都應該已經是個很特定的東西 ，而且變化的很快。所以如果有一個統一的管理單位，應該可以很快知道業者在想什麼，並加以互相協助。

問題（十一）關於資料的應用上，有沒有什麼政府可以提供更多的協助，或是管理上比較不足的地方？對資料面向有沒有哪些建議？
受訪者：比如說在 GDPR 而言，聽說台灣政府雖然很有可能在個資修法的方向會朝著 GDPR 去進行。但我們業者可能會遇到的問題，第一個，對於業者而言，若要符合 GDPR 的規範，我們可能有相當的成本支出，我們會先考慮在歐盟的收入，能不能 cover 這個成本，目前還在討論這些事情。然而，現在我們了解的 台灣這邊的法規很有可能跟 GDPR 一起調整，對政府的修法方向也不清楚，但我們的成本勢必會提高。

問題（十二）貴公司目前有無遇到實踐上的困難面？
受訪者：數位服務的產品在提供服務時，變化是很快速的，當我們每次的服務在變化時，要如何在變動時取得使用者的同意，希望政府能提供相關的指導服務。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件二 英國出國報告

出國報告（出國類別：考察）

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制計畫

出國報告

姓名職稱；王德瀛 法律研究員

派赴國家：英國

出國期間：107 年 4 月 16 日至 22 日

報告日期：107 年 5 月

本報告之智慧財產權歸屬於財團法人資訊工業策進會

一、目的

歐盟「一般資料保護規則」（General Data Protection Regulation，以下簡稱 GDPR）即將於今（2018）年 5 月 25 日正式施行。由於 GDPR 統一了歐洲經濟區（European Economic Area，包含歐盟及冰島、挪威及列支敦斯登，簡稱 EEA）的個人資料保護法律規範，其內容擴張了個人資料的範圍、增加並調整了當事人權利內容、調整了資料控制者及處理者之權利義務，同時對於資料傳輸出歐盟亦有限制之規定。由於 GDPR 將所有處理歐盟境內資料主體資料之行為納入管制，又有針對資料跨境傳輸之限制，我國通訊傳播產業於發展國際業務時，若有與歐盟相關之業務，將深受 GDPR 之影響。同時，我國個人資料保護法（及其前身——電腦處理個人資料保護法）之立法，受到歐盟個人資料保護影響甚深，GDPR 之發展亦可能對於我國個人資料保護法之解釋及未來資料保護法制之變化發生重要之影響。

為了解歐盟各會員國之個資主管機關、企業界及學界在 GDPR 正式施行前夕，對於 GDPR 之準備、因應及預期，此行安排參加歐洲個人資料保護重要之研討會「IAPP 2018 歐洲資料保護密集研討會」，並透過參加英國倫敦當地兩場針對當地企業之說明會、工作坊——「關於 GDPR，你需要於 5 月 25 日前知道的一切說明會」及「給企業與新創的 GDPR 工作坊」——了解當地企業之因應方向與準備程度。

二、效益

此行主要效益有下列三項：

第一，了解歐盟會員國個資主管機關因應 GDPR 施行所作之準備及

本報告之智慧財產權歸屬於財團法人資訊工業策進會

其對 GDPR 之預期。透過了解各該主管機關之立場，有助於了解我國與歐洲有往來之通訊傳播產業所可能面對之管理樣態，例如主管機關對於管理企業之態度為何，是否考慮迅速使用 GDPR 著名之高額處罰等。同時，亦可藉此了解 GDPR 中許多有待逐漸形成之實質內涵以及實踐可能發展之方向，例如 GDPR 所新出現的資料可攜權之發展等。另外，亦可藉由各主管機關所關切之重點側面了解面對新時代條件下的個資法體系，主管機關可能會面對哪些挑戰，又可以將側重之重點放在哪些議題之上。最後，可以一窺歐盟相關法領域最新之發展動態，如曾預計與 GDPR 一起施行但迄未完成立法程序之「電子通訊規則」（Regulation on Privacy and Electronic Communications，簡稱 ePrivacy Regulation）之最新動態等。

第二，了解歐洲實務界及學界對於 GDPR 發展之看法。這包含對於 GDPR 所創設或調整之權利及規範要求實務界之應對方式。例如對於新出現之資料可攜權之實質內容或是隨著 GDPR 對同意之行使有更多之要求後，實務界如何應對，使其資料之利用行為仍能順利運行等。透過此些了解，一方面有助於協助國內相關業者及主管機關了解實務層面 GDPR 之衝擊與影響，一方面也有助於對 GDPR 相關細節研究之展開。

第三，透過觀察英國倫敦在地企業因應 GDPR 施行之態度，折射出 GDPR 施行後可能之狀態。透過參與針對英國倫敦在地企業的小型活動，了解當地 GDPR 準備之程度，亦可藉此觀察 GDPR 正式施行後，當地可能的變化。

三、研習對象

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(一)IAPP「2018 歐洲資料保護密集研討會」(Europe Data Protection Intensive 2018)

由「國際隱私專業人員協會」(International Association of Privacy Professionals,以下簡稱 IAPP)所舉辦的 2018 歐洲資料保護密集研討會於今年 4 月 18 日至 19 日於英國倫敦「田莊塔橋飯店」(Grange Tower Bridge Hotel)舉行。今年度的主題為即將施行的 GDPR,透過不同分組議程以及主題演講,勾勒歐洲當前對 GDPR 各面向討論之樣貌。會議有許多於企業或政府部門中擔任隱私保護工作之專業從業人員參加。講者除有業界從業人員及來自政府個資主管機構之官員外,亦有來自學術單位之專業研究人員參與,是國際間相當重要之隱私專業會議。

IAPP 是 2000 年所成立的全球性非營利組織,其目的在協助及改進全球的隱私行業,是全球最大的資訊隱私專業社群,其提供包含資料隱私認證計畫、教育訓練,並常態舉行多個重要的個資保護相關研討會[316]。

本次會議分別於兩日上午安排主題演講,並接續有四個時段、每個時段四場之分組議程。詳細之議程請參考下表。

[316] https://iapp.org/about/mission-and-background/

本報告之智慧財產權歸屬於財團法人資訊工業策進會

表 9 IAPP Europe Data Protection Intensive 議程表

4 月 18 日議程	
時間	議程
9：15～10：30	Opening General Session
11：15～12：30	Consent and the GDPR: How Successful Organisations Tackle Consent Management
	ePrivacy Regulation: All's Well That Ends Well?
	New Controller and Processor Relationships Under GDPR - What a Show!
	The Next Generation of Privacy Professionals: Women Leading Privacy
13：45～14：45	AI Meets Privacy: How the GDPR May Impact Machine Learning
	Data Beyond GDPR
	Friends Don't Let Friends Use Legitimate Interest to Avoid Consent Requirements
	The Impact of Data Localisation on the Digital Economy
15：15～16：30	GDPR: 72-Hour Notification – Is Your Breach Response Plan Operational?
	Just Because You're GDPR Compliant Does Not Mean You Can Use Your Data
	Privacy Challenges and Solutions for Blockchain Projects in the Context of GDPR
	Snooping on Your Staff: Privacy or Prying?
17：00～18：15	Making Sense of the UK: Privacy, Brexit and More
	New Individuals' Rights Under the GDPR: Power to the People and Business Change
	PSD2: How to Balance Open Banking and Privacy Protection
	To BCR or to GDPR: That Is the Question

本報告之智慧財產權歸屬於財團法人資訊工業策進會

4 月 19 日議程	
時間	議程
9：15～10：15	Closing General Session
11：00～12：15	Accountability and Demonstrating Compliance Under the GDPR
	Are You Prepared to Address New Privacy Laws in AI Environments?
	One GDPR and Many National Implementation Regimes – How to Find Your Way Through
	Privacy in APEC: Views from Privacy Professionals
12：30～13：30	Creepy or Cool?
	Enforcing the GDPR – DPA Roundtable
	Incident Response Session: Simulated Breach
	Privacy by Design in Cars – Myth or Reality?
14：30～15：45	Data Breach Response: Tips from the Trenches
	How Your Move to the Cloud Can Accelerate GDPR Readiness
	North by Northwest: Managing Privacy Across the Value Chain
	The Future of Consent
16：00～17：00	Effective Tactics for Rallying the IT team to Your Side
	Greatest PR #Fails in U.S. Breach Response and How EU Companies Can Avoid Them
	Regulatory Obligations – Engineering Requirements
	Third-Party Privacy Risk – Beyond Your Organisation's Bounds for GDPR

資料來源：本研究整理

由於本次主要參訪主要係針對 GDPR 對我國通訊傳播產業可能有之影響以及蒐集有關 ePrivacy Regulation 之動態，故報告人參與之分組議程皆以與此較為相關之領域為之議程為主。具體而言，報告人參加之場

本報告之智慧財產權歸屬於財團法人資訊工業策進會

次及大致之介紹如下：

1. Opening General Session

英國「資訊長」（Information Commissioner）Elizabeth Denham 及暢銷書籍「The Stranger in the Woods」作者 Michael Finkel 分別發表主題演講。

Elizabeth Denham 的演講主要聚焦在英國個資主管機關「資訊長辦公室」（Information Commissioner's Office，以下簡稱 ICO）因應 GDPR 所作的準備以及未來的工作目標。她強調，雖然 GDPR 給予了 ICO 更多對於個人資料使用、處理、分享等行為監管的權利，ICO 的目標仍然是在公司（資料控管者或處理者）的權利以及法律對個人資料保護的誡命間盡量求取平衡，然而資料有關的犯罪仍然應該被當作是真正的犯罪（data crimes are real crimes）。為了有效的監管相關的行為，ICO 的預算規模及組織員額都有所增加，並新設了 6 個調查小組。而面對 GDPR 即將施行，ICO 作為主管機關，目前將重點放在協助、教育、監管、諮詢及賦權之上，透過出版一系列檢核表、指導原則等方式，協助企業應對 GDPR。

Denham 也特別澄清一般對於 GDPR 的兩個迷思。首先，在 GDPR 最常讓人驚嚇的「高額賠償」議題上，她表示 ICO 無意改變目前現行的裁罰標準。GDPR 對於主管機關而言，罰鍰並非最好用的管制工具，其他的管制工具如頒布停止處理命令等，對於主管機關而言更加有效。第二則是對於資料洩漏的通報標準上，並非所有的資料洩漏都需要通知 ICO，只有會影響到當事人權利的洩漏事件，才有通報的必要，ICO 也會協助企業判斷是否需要通報。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

而在談到 ICO 的工作重點時，Denham 揭示了 ICO 目前的三大工作重點：「資訊安全」（Cyber Security）、人工智慧以及「追蹤設備」（device tracking）對個人資料安全的影響之上。其中，針對人工智慧對於隱私的影響，英國政府規劃將於明（2019）年推出沙盒機制，預計將於今年展開公眾諮詢程序。

至於英國脫歐的相關影響，Denham 表示，英國脫歐並不會因此影響到民眾的「隱私權」（information right）保護，英國的隱私法修正草案也是以將 GDPR 完全落實為目標進行修正，除了 ICO 與歐盟其他會員國個資主管機關間的關係可能受到影響外，其他事項不不會因為英國脫歐而發生改變。

最後，Denham 總結認為，在民眾逐漸覺醒個資保護意識的時代，如何建立民眾的信心與信任，將是個資主管機關最重要的工作。

Michael Finkel 則從自身經驗出發，講述當前時代下個人身份與資料認定及保護的困難。他曾被一名逃犯假冒身份，在墨西哥以他的名義招搖撞騙。在落網後 Michael 與他聯絡時，還要求他自己證明自己的身份。Michael 發現要證明自己是自己一件相當困難的事情，也因此產生了一個疑問：在現今這個以資料為主的世界中，我們到底該如何證明自己？

2. ePrivacy Regulation: All’s Well That Ends Well?

本場次主要聚焦於 ePrivacy Regulation 的立法時程跟主要爭點。場次由 IAPP「共同主管」（co-head）Ruth Boardman 擔任主持人，英國「數位、文化、傳媒暨體育部」（Department for Digital, Culture, Media, and Sport）「歐盟資料流動及歐盟與國際資料保護」（EU Data Flows, EU and

本報告之智慧財產權歸屬於財團法人資訊工業策進會

International Data Protection）部門主管 Elisabeth Stafford 以及歐盟執委會「通訊網路、內容與科技總署」（Directorate General for Communications Networks, Content and Technology，簡稱 DG connect）政策官 Agnieszka Wawrzyk 擔任與談人。

Wawrzyk 首先介紹了 ePrivacy Regulation 的立法背景，隨著民眾使用電子服務的範圍擴大，規範的範圍也應該擴大，將「OTT」（over-the-top）也納入範圍，而在資料種類上，除了個人資料外，考慮到其他資料也有機敏性（例如企業資料也可能包含商業機密，或也會連帶的存在個人資料），所以也將非個人資料納入，因此有此次的修正。

歐盟執委會版的 ePrivacy Regulation 草案原則上認為通訊應該是機密的，通訊的內容、脈絡（包含時間、地點、頻率等等）原則上非經當事人同意不可蒐集。同理，服務提供者原則上也不可監控聯網的設備，或透過聯網設備進行監控。不過在此歐洲議會有不同見解，想要允許服務提供者監控以提供資安相關之更新。而在隱私設定上，ePrivacy Regulation 草案要求要有拒絕所有揭露的選項，歐洲議會則希望增加更多友善使用者隱私設定的規定。目前草案正等待「歐洲理事會」（European Council）的通過後展開歐洲理事會、歐洲議會與歐盟執委會的三方協商。

Stafford 接著解釋了英國目前對於 ePrivacy Regulation 的立場，她表示這些立場還會在歐洲理事會與其他國家協商。她舉例，英國對於不同類別的 cookie 管理強度還有一些意見，有六個主要的問題會在理事會與各國導論；在用戶同意服務提供者利用其資料的部份，英國則主張應與 GDPR 做一樣的規劃；同時，由於瀏覽器可以預設關閉所有 cookie，但在網站取得使用者情況下開啟，英國認為如何確保瀏覽器能辨認網站取

本報告之智慧財產權歸屬於財團法人資訊工業策進會

得的同意是合法的，會是實際要面對的問題，也需要與各國討論；此外，對於行銷電話號碼顯示的部份等等，英國也都還有所疑慮。四月份歐洲理事會將再繼續針對 ePrivacy Regulation 開會討論，目前尚無法得知何時通過。

事實上，對於哪些類型的通訊行為將納入 ePrivacy Regulation，還仍有許多地方需要進一步釐清。舉例而言，在本次會議的問答階段，有觀眾提問若是網路遊戲的遊戲商有提供聊天的功能，是否應納入 ePrivacy Regulation 管理？Stafford 認為，可能要看情況處理，如果只提供「公頻」（所有人都可以看到的對話），則可能不受此規則管轄，若是「私頻」（只有參與對話的玩家看得到），則可能受此規則管轄。但她也類似議題確實也還需要討論。

類似的狀況也發生在政治性質的通訊上，是否可以與商業性質的通訊一樣受到規範？或是與「聊天機器人」（chat-bot）的對話是否受到此規則的管理？Stafford 和 Wawrzyk 都認為還有需要釐清的空間。

3. Data Beyond GDPR

IAPP 荷蘭的國家領袖 Jeroen Testegge 針對資料未來可能的發展發表演講，主要討論巨量資料及資料驅動的新技術對於未來可能的影響。包含隨著依靠服務提供者提供資料的設備越來越多，財產權的概念是否會受到侵蝕，如何確保服務的延續性將是未來的重點。此外，在經濟、勞動層面，如何因應巨量資料促發人工智慧成長後，相關的衝擊，也需要應對。最後，則是針對資料分析技術與演算法進行討論，認為維持一定程度的透明性要求是有所必要的。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

4. Just Because You're GDPR Compliant Does Not Mean You Can Use Your Data

本場次由知名隱私保護公司 Anonos 執行長 Gary LaFever 與「南安普敦大學」（University of Southampton）資料保護與治理研究員 Alison Knight 主講。

LaFever 跟 Knight 主要針對 GDPR 所提供的兩種不同的合法處理個人資料的權源進行討論。認為 GDPR 在基於同意處理個人的規範上，對於同意的行使設下許多要件的情況下，企業可以考慮改以追求其或第三方「合法利益」（legitimate interest）的方法來處理個人資料。不過須注意的是，GDPR 要求在採取合法利益作為處理個人資料的合法權源時，亦要求須針對其處理與對資料當事人可能的損害進行損益衡量。

此時，LaFever 跟 Knight 都認為在 GDPR 中被鼓勵的「假名化」（pseudonymisation）可以成為企業降低其個人資料風險，進而減少對資料當事人可能損害，因此可以作為企業在採取合法利益此一權源時，所採用的技術。Gary 甚至大膽的主張，假名化處理個人資料事實上是為 GDPR 所鼓勵的，依照該公司目前與歐盟會員國監管機構討論的狀況來看，若採取這種假名化的手段，則原先在 GDPR 施行前可以合法利用的資料型態，在 GDPR 施行後，應該都可以透過假名化降低風險，而已合法利益作為權源合法使用。

不過 LaFever 跟 Knight 也都提醒，因為無法驗證是否真正作到完全的「去識別化」（anonymisation），因此建議企業原則尚要避免「資料係採取去識別化方式處理，而不再屬於個人資料，沒有 GDPR 適用」的主張。以免因為並未完成去識別化而造成後續的其他法遵上之風險。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

5. New Individuals' Rights Under the GDPR: Power to the People and Business Challenges

本場次由 Hogan Lovells 律師事務所「資深合夥人」（Senior Associate）Lilly Taranto 及「駿懋銀行集團」（Lloyds Banking Group）資料保護及智財法制主管 Belinda Doshi 共同主講。

兩位認為，GDPR 在個人權利部份透過增加個人對個資的掌控能力、加強暨有的權利（如拒絕權）、增加新的權利內容（如資料可攜權）以及將既存權利「法典化」（codifying）（如被遺忘權）等方式，賦權資料當事人。但同時，也對資料控制者及資料處理者增加了實行的挑展，資料控制者及處理者能需要增加新的程序、準則、整備資訊系統、更新相關契約及增加訓練等準備，才能符合 GDPR 的要求。

在拒絕受側寫或自動決策程序的拒絕權的部份，GDPR 雖然提供了三種例外（包含法律規定、合約必須及明確同意），但是講者認為明確同意的部份由於如何能證明是「明確」（explicit）可能有困難，所以還有一些值得觀察發展的空間。這種「拒絕權」不只是「權利」，對於控制者與處理者而言，仍有許多組織上的挑戰，例如需要進行個資衝擊影響評估、維持透明性、隨時監測等等。其中，講者認為最大的挑戰是，GDPR 要求側寫與自動決策需有人類介入的階段，但實務尚要如何讓這個介入是有意義的，仍有需要努力的地方。

至於被遺忘權的部份，講者也介紹樂對於組織及技術上的難處。其中講者認為最大的困難可能在於有些資料在技術上難以刪除。畢竟現在某些技術（如區塊鍊等）所儲存的資料，可能在事實上難以刪除，甚至無法刪除，已經不像以前紙本資料時那樣容易刪除。講者提醒，此時英

本報告之智慧財產權歸屬於財團法人資訊工業策進會

國個資主管機關的見解認為，資料控制者或處理者只要將資料停用，使任何人皆無法近用該資料，也符合被遺忘權的要求。

最後，在可攜權的部份，兩位講者首先提醒，資料可攜權與資料近用權兩者在範圍及申請條件上有所不同。資料近用權可以取得所有個人資料，但資料可攜權僅須提供資料使用者所提供之資料。(例如智慧手環傳遞出跑步數據，應用程式針對跑步的數據做出評估，如果使用者主張資料可攜權，要轉移資料的時候，運用數據所做出的評估資料不在轉移的範圍內)。此外，申請資格方面，無論是依據哪個合法權源處理的資料都有近用權的適用，但可攜權僅有基於同意或契約處理的資料和自動決策的資料才有適用。

在落實方面，傳遞資料出去的一方，要思考資料的結構為何，並應盡量提供機器可讀的資料格式；而接受資料的一方，則須注意仍須遵守資料最小蒐集原則，蒐集的資料也應受到利用目的的限制，不是對方提供什麼資料都可以接收。不過由於不同資料控制者、處理者對於資料的結構、型式、資料欄目的意義等都存在許多的歧異，講者認為，如何真正將資料可攜權具體落實，還有待業者及主管機關持續充實該權利的實質內涵才能比較明朗。

6. Closing General Session

知名個資保護企業 IF 執行長 Sarah Gold 發表主題演講，而英國知名電視節目主持人 Don Snow 與英國「公開大學」(the Open University) 社會史「名譽教授」(emeritus professor) David Vincent 則針對隱私的歷史發展進行對談。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Gold 就企業應該以什麼態度面對 GDPR 為中心發表主題演講。其認為在當前環境下，有許多事情開始影響人們對於資料處理的信任，而 GDPR 確實對企業提出了一些困難的問題。她建議，企業面對這些問題的時候，有幾個方法可以處理：首先，企業要了解自己服務提供的內容。同時，要對於第三方提供的服務加以監管。企業還需要學習一些新的技能，並學習以「人類可以理解」（human readable）的方式將其應用資料的方式解釋給使用者聽。她認為最重要的應該就是企業應對自己處理哪些資料及為何處理資料。最後，Gold 總結認為「信任」是這個時代企業最需要重視的部份。

至於 Snow 與 Vincent 的對談，則從 1341 年開始，談論隱私概念的變化。他們提醒，隱私權最為一個區隔內與外的權利，會不斷隨著科技的變化而有所演化。企業與主管機關都應該隨著科技的發展不斷辯證隱私的內涵，逐步調整對於隱私的態度。

7. Privacy in APEC: Views from Privacy Professionals

本場座談由全球諮詢公司「海峽金融集團」（Promontory Financial Group）隱私與個資實務主管 Simon McDougall 擔任主持人，由紐西蘭航空公司的資訊長 Jacqueline Peace、「施耐德電機」（Schneider Electric）主任 Mak Joshi 以及 Rajah &Tann Singapore 律師事務所合夥人 Steve Tan 針對亞太經合會地區的個資保護進行討論。

三位與談人最主要強調的是亞洲的多樣性，不說有許多亞洲國家迄今仍沒有個人資料保護法，就算有個人資料保護法的國家，其個資法的內含有很大的不同。以菲律賓為例，其規定每一次的資料洩漏事件，都可能需負擔刑事責任，這在其他國家是很難想像的。而在新加坡，在當

本報告之智慧財產權歸屬於財團法人資訊工業策進會

時立法時，考察了各國的個資法後，決定自行擬定適合新國國情的個資法，因此有許多地方與一般國家不同。例如新加坡就並未區分一般個資與特種個資。而在企業是否需要設立資料保護員、資料保護員是否需要項政府機關登記註冊上，亞洲各國也呈現了很大的歧異性，這都會造成在亞洲開展業務的公司在適用上的困擾。

而在 APEC「跨境隱私保護規則」（Cross Border Privacy Rules，簡稱 CBPR）的發展前景上，長期研究亞洲個資法，在新加坡執業的 Steve Tan 認為，考慮到 CBPR 發展許久卻沒有太多國家加入，CBPR 短期內要發揮巨大的影響力有實質上的困難。報告人在會後詢問 Tan 新加坡加入 CBPR 後的發展，與先前所公布的不同，Steve 表示就他了解，新加坡應該不會以其個資監管機關加入成為「問責機構」（Accountability Agent，簡稱 AA），而是應該會像日本、美國一樣，選擇一個非政府組織成為問責機構。Steve 表示，新加坡政府應該會在六月份時就細節提出更多的資訊。

8. Enforcing the GDPR – DPA Roundtable

本場座談會係邀請歐盟境內個資主管機針對 GDPR 施行進行討論，會議由海峽金融集團「資深總監」（Senior Principal）John Bowman 擔任主持人，英國資訊長辦公室負責營運的「副資訊長」（Deputy Commissioner）James Dipple-Johnstone、法國「資訊與自由國家委員會」（Commission nationale de l'informatique et des libertés，簡稱 CNIL）執行部門副首長 Mathias Moulin、愛爾蘭「資料保護長辦公室」（Office of the Data Protection Commissioner）「副資料保護長」（Deputy Commissioner）John O’Dwyer 以及「歐盟資料保護監督機關」（European Data Protection

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Supervisor，簡稱 EDPS）「歐盟資料保護委員會聯絡協調員」（EDPB Liaison Coordinator）Isabelle Vereecken 參與與談。

此次座談會主要討論了各會員國主管機關就 GDPR 施行的準備情形、對於歐洲經濟區內各國主管機關間合作的預期、GDPR 銜接期的處理、資料可攜權以及若發生解釋歧異時該如何處理等問題的等議題。

就各會員國準備的情形來說，法國、英國、愛爾蘭等國主管機關以及 EDPS 都表示他在組織及員額上都有相應的擴增，並針對 GDPR 的施行制定相關的指引守則供企業界遵循。

對於歐洲經濟區內各主管機關間彼此合作上，許多主管機關代表對於最早面對的案件為何表示難以預期，不過愛爾蘭主管機關似乎頗為確定的預估，最早使用 EDPB 協調機制的將會是資料的洩漏案件。

在 GDPR 銜接其可能面對的問題上，英國主管機關認為最大的挑戰會在新權利的落實上，但是他也表示所謂「GDPR 調適期」應該是 GDPR 通過到施行的這段時間，所謂的銜接期已經將要結束，主管機關會即刻依照 GDPR 規範進行管制。但英國主管機關代表再次重申，ICO 認為比起採取高額的罰鍰，其他 GDPR 的管制措施更為有效，也會是主管機關優先考慮的選項之一。對於這個看法，法國主管機關的代表也呼應指出應該注意到除了罰鍰外，GDPR 第 58 條也賦予主管機關許多的管制工具，主管機關將會妥善使用這些權利。法國主管機關代表認為，由於事前已經提供了許多指引，企業界應該已經對此做好準備。愛爾蘭主管機關的代表則從另一個角度討論此一議題，他認為對於從 GDPR 施行前已經開始而持續進行到 GDPR 施行後的處理行為究竟應該適用新法還是舊法，或許是未來需要注意跟解決的問題。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

針對資料可攜權內涵不清影響運作可行性的問題，愛爾蘭主管機關的代表認為難以藉由主管機關制定標準的方法解決，應該鼓勵同類型企業彼此討論與合作，對於該行業類別內的資料結構訂定標準，如此較能妥善的解決問題。

至於若發生解釋歧異的問題，法國主管機關的代表認為這並不會造成太大的困擾，若真的出現主管機關與受管制對象對於資料解釋的歧異，「歐洲法院」（European Court of Justice）的訴訟應該就可以解決這類的問題了。

9. The Future of Consent

本場座談由 IAPP 英國國家領袖 Giles Watkins 擔任主講人、個資保護公司 Citric Data Protection 資料保護顧問 Matt Anslow、獨立歐盟隱私與 GDPR 專家 Chiara Rustici、隱私與技術公司 JLINC Labs 資料保護員 John Wunderlich 等人參與座談，雖然本場次主題是「同意的未來」，但實質上這個場次主要討論的內容還包含了 GDPR 施行前就已存在的「遺澤資料集」（legacy dataset）的使用等問題。

在「同意」未來的發展上，Anslow 企業要提昇對於同意管理的能力，可能要建立一個中央資料庫來記錄使用者對於同意權行使的內容，可能可以成立一個同意的確認表單，讓人們自由選擇想要同意的內容。Anslow 認為，未來「同意」的概念可能變成類似「意圖」（intend）的概念，也就是使用者想要什麼樣的處理，這會是根本概念的改變。而 John 認為未來同意的內涵可能會逐漸的「標準化」，區塊鍊技術則可能可以有助於儲存同意的內容。（至於區塊鍊與被遺忘權間的緊張關係，Wunderlich 認為可以透過解釋的方法來加以調和）同意要件變得更加嚴

本報告之智慧財產權歸屬於財團法人資訊工業策進會

格，Wunderlich 認為如果換個角度討論，或許就不是壞事。舉例而言，嚴格的同意對於廣告商而言或許是種挑戰，但對廣告主而言，可以讓目標群更加精準，反而是好事，而且「主動告知」的行為，有助於民眾建立信任感。而 Rustici 認為「同意」概念的改變，最主要的是要「讓使用者思考」，同意變得更嚴格的意義並非要禁止人們使用資料，而是要透過設計讓使用者可以思考資料可能被使用的方式。

所謂「遺澤資料集」，一般來說指的是以老舊格式儲存或除存在老舊資訊系統中，而難以近用與處理的資料。在本場次則特別指的是在 GDPR 施行前已經蒐集、處理的資料。因為 GDPR 對於資料合法利用的權源與之前的指令或各國內國法有差異，這類資料是否——或應該如何——可以繼續使用，成為討論的焦點。針對 GDPR 施行前已經存在的遺澤資料集使用問題，由於其或許係奠基於傳統的同意型式，因此可能不符合 GDPR 對同意的標準，造成使用上的困擾。Rustici 特別指出歐盟「第 29 條工作小組」（Article 29 Working Party）的指導原則對此有所處理，一般而言，資料不能任意轉換合法權源，但針對遺澤資料集的部份，可以例外的轉換其合法權源。

至於同意更加嚴格是否會使「合法利益」作為資料合法使用之權源變得更常被使用，Rustici 提醒「合法利益」一詞的解是在 GDPR 與指令的解釋有出入，如果資料使用者基於合法利益處理個人資料，發生與資料當事人權利的衝突應該如何處理？其處理方式尚不明瞭，資料控制者或處理者可能會面段爭訟的風險，可能需要暫時停止利用該資料並證明自己具有使用該資料的合法利益，對於資料使用者跟利用者而言，不見得更加有利。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

10. Third-Party Privacy Risk – Beyond Your Organisation's Bounds for GDPR

本場次座談由「寶隆洋行」（Santa Fe Group）資深總監 Tom Garrubba、Bird & Bird 律師事務所合夥人 Gabe Maldoff 以及軟體開發商 InterSystems 資料保護員 Ken Mortensen 共同主講。

兩位講者強調資料控制者與資料處理者的概念並非截然二分，而是更接近光譜的概念。在資料控制者與處理者間資料傳遞上，可以大致上分為四種不同的型態，包含：資料控制者傳給資料處理者、資料處理者傳給資料處理者、共同作為資料控制者，以及資料控制者傳給資料控制者。前三者在 GDPR 中都可以找到相關的規定，然而資料控制者傳遞給資料控制者的情形，在 GDPR 中沒有相關規定，不過現實生活中卻真實存在，例如 Facebook 與劍橋分析公司之間就是這樣的關係。

在此狀況中，講者整理了第 29 條工作小組、愛爾蘭個資主管機關以及美國國會的意見後，認為在這種狀況下確保過程的透明性，而資料提供者應該要主動的監控相關程序的運作，確保資料保護的有效性；同時，資料分享的範圍應有所限制、也應該確認該資料能被確實的刪除。Mortensen 特別建議這種情形其實與美國「健保可攜與責任法」（Health Insurance Portability and Accountability Act，簡稱 HIPAA）兩個「受管制實體」（covered entity）間的資料傳遞類似，此時 HIPAA 的「資料分享協議」（Data Sharing Agreement）或許可以作為這部份企業的參考。

(二)「關於 GDPR，你需要於 5 月 25 日前知道的一切」（Everything you need to know about GDPR before 25 May 2018）說明會

本報告之智慧財產權歸屬於財團法人資訊工業策進會

關於 GDPR，你需要於 5 月 25 日前知道的一切說明會是由 Nccgroup 公司於 4 月 20 日上午於倫敦的「醫院俱樂部」（Hospital Club）所舉行的一項活動，該活動主要目標係針對倫敦當地之企業介紹 GDPR 相關事宜。當日與會之觀眾有來自當地之小型企業或醫院等不同單位之個人資料處理人員。

在本次活動中 Nccgroup 公司人員介紹之內容主要有二：其一為 GDPR 之內容及其可能對其業者造成之影響。另外，則特別針對 GDPR 中有關於資料外洩通報之部份做詳細之說明。

(三)「給企業與新創的 GDPR 工作坊」（Workshop-GDPR for Entrepreneurs and Start-ups）

給企業與新創的 GDPR 工作坊係大英圖書館（相當於我國國家圖書館）於其自有之會議室所舉辦的針對新創企業 GDPR 調適之工作坊。參加者除當地小型企業及新創企業外，亦有部份大型企業員工或律師參與討論。

工作坊中除介紹 GDPR 大致之規定外，另針對小型公司或新創產業如何在合理成本下符合 GDPR 相關規定特別加以著墨，提出實際可行之建議。

四、重要議題討論

(一)歐洲各個資主管機關應對 GDPR 之作法

從歐洲各主管機關在本次會議中的發表可以發現，各國主管機關面

本報告之智慧財產權歸屬於財團法人資訊工業策進會

對 GDPR 的施行，在組織與員額上都有所擴充，並投入相當資源擬定適用的指引供大眾遵循。同時，從英國資訊長以及愛爾蘭個資主管機關代表的發言可以發現，資料外洩通報的運作或許是其中一個特別受到重視的要素。在未來，歐洲許多主管機關計畫持續進行教育與輔導各個企業符合 GDPR 的規範。在管理方式上，與臺灣輿論上普遍強調 GDPR 的高額罰鍰不同，各國主管機關其實並不特別強調高額罰鍰，而是更實際的強調 GDPR 中其他的管制措施或許會更常被主管機關使用。換言之，各國主管機關可能會透過 GDPR 賦予的權利，透過各種管制手段直接介入資料控管者或處理者處理資料的內容，而非消極的僅以處罰的方式來處理。

(二)ePrivacy Regulation 之動態

ePrivacy Regulation 的發展仍為會場許多參與的人士所關心，不過從英國政府及歐盟執委會代表的發言來看，歐盟理事會內部對於 ePrivacy Regulation 的內涵尚有許多需要討論，可能不會迅速的通過。而 ePrivacy Regulation 在歐盟理事會通過後，仍需要經過歐盟理事會、歐盟議會與歐盟執委會三方協商，才能正式通過。因此，我們可以很篤定的認為 ePrivacy Regulation 勢必不可能在 GDPR 前正式實施。

從另外一個角度來說，ePrivacy Regulation 此前所通過的歐盟執委會及歐盟議會兩個版本已經有所歧異，在歐盟理事會討論後，勢必會有另一版本的出現，未來三個版本的差異，如何調整值得繼續觀察。而如同前述，在本次會議討論的過程中，已經可以發現 ePrivacy Regulation 草案中擴張適用範圍後，仍有一定程度的模糊地帶，對於這些範圍定義的釐清，以及各種 cookie 如何管制，或許將是未來討論的重點。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(三)拒絕權、被遺忘權與資料可攜權等新興權利之發展

在 GDPR 加強、成文化或新增的各種資料當事人權利中，拒絕權與被遺忘權雖然在落實上尚有許多挑戰需要克服。但與會的專業人士與講者普遍認為實行上可能面對的最大困難應該是資料可攜權的內涵。包含應該如何統一資料格式、資料欄目如何對應等問題，在 GDPR 即將施行的現在，其實還沒有清楚的答案。而主管機關似乎無法，也不可能直接擬定相關的細節。因此，對於資料可攜權的實質內涵以及實務做如何進行，仍有待持續相關行業類別內部，持續討論與合作，才能逐步形成實質的內涵，也更值得我們繼續加以觀察。

(四)個人資料處理合法權源之轉向：同意及「合法利益」（legitimacy interest）之爭

隨著「同意」的要件在 GDPR 內變得更加的嚴格，在本次會議的多場討論中，與會者紛紛討論到未來資料控管者與處理者可能將更重視「以合法利益為由處理個人資料」的途徑。部份學者與隱私相關的業者認為，若搭配假名化技術降低對當事人可能的隱私衝擊，以合法利益作為合法處理個人資料的權源可能作為許多企業在為來處理個人資料的方法。然而，也有部份講者認為，由於合法利益須與資料當事人的隱私權利加以權衡，這種權衡的損益過程存在一定程度的不確定性，因此在實務上考慮可能面臨的訴訟或爭議，這種處理方式仍然存在一定的風險，值得業者加以注意。

(五)APEC 地區個人資料保護之發展

本報告之智慧財產權歸屬於財團法人資訊工業策進會

亞洲地區或許因為文化背景的關係，或是發展程度的差異，個人資料保護制度存在高度的歧異性。這種的差異將使在亞洲地區展開跨國營運的業者增加實務工作的困難性。

目前 APEC 雖然有 CBPR 的制度，但此一制度發展已久東南亞許多國家仍未能加入，能發揮的功能或許仍然有限。我國目前正積極想要加入 CBPR 體系，新加坡做為最近一個加入 CBPR 的國家，其處理方法值得我們注意。未來，新加坡將要決定要以哪個單位申請成為 CBPR 的 AA。與此前傳出的消息不同，新加坡可能不會以個資主管機關申請，而會以非政府組織加入。新加坡的相關動態，可能在六月時會有更多資訊出現，值得留意與重視。

(六)GDPR 未竟之處：資料由控管者轉移至控管者

如同前面的討論，GDPR 對於資料控管者間資料的轉移並未有所規範。然而，當前討論的沸沸揚揚的 Facebook 與劍橋分析公司間的爭議，就是資料控管者間的轉移。透明性與資料傳遞者對於傳遞對象的監管這兩個項目，是目前討論中認為在這種資料移轉關係中最需要的條件。未來歐盟各主管機關會如何填補 GDPR 在這裡的規範空白，是否會參考 HIPAA 資料分享協議的相關規定，值得我們繼續加以觀察。

(七)當地企業準備狀況與新創因應之道

本次報告人特別參與兩個當地針對小型企業所作的 GDPR 說明會或工作坊。從會議中與會者的討論來看，許多小型業者對於 GDPR 的施行仍然感到焦慮，甚至尚未因應 GDPR 的施行進行工作流程的改變。因此，即便許多歐洲的個資主管機關認為已經做了許多的宣導與指引，應該可

本報告之智慧財產權歸屬於財團法人資訊工業策進會

以順利的過渡到 GDPR，但短時間內許多業者應該尚無法完全符合 GDPR 的要求，一定程度的混亂與銜接應該是可以預期的。

此外，從這類小型座談會中，我們也可以發現歐盟內部對於 GDPR 的了解還存在差異。例如其中一場的主講人在說明 GDPR 的適用範圍時，就認為 GDPR 的判斷標準應該是資料當事人的「國籍」(nationality)；然而 GDPR 強調的其實是針對「在歐盟境內的資料主體」，國籍應該不是重點。從這種小地方的差異可以佐證上判斷，在 GDPR 正式施行後，這些誤解或認知上的差距才會逐漸突顯，因此短期間內歐盟境內應該還是會有一段逐漸適應的過程。

最後，這類小型最談會也提供了小型業者實際的因應手段。大英圖書館的講者特別建議小型或新創業者可以利用大型雲端企業提供之服務，如 Google 或 Dropbox 等服務來管理自己所保有的個人資料，因為這類大型企業提供的服務已經符合 GDPR 的規範要求。這種處理的方法對於歐盟個資數量不多的一些臺灣企業而言，也具有一定的參考價值。

五、心得及建議

(一)針對 GDPR 施行，國內企業應調整作法，但不須太過慌張

GDPR 的施行確實會很大程度的影響個人資料的使用與管制，國內企業若有與歐盟有所往來，會保有或處理歐盟境內公民的個人資料或是會有將個人資料從歐盟境內轉移出去的行為，都應該盡速的調整相關的內容。

但與此同時，企業也無須因為 GDPR 高額的罰鍰感到恐慌。許多歐

本報告之智慧財產權歸屬於財團法人資訊工業策進會

盟個資主管機關已經表明比起高額的罰鍰，更可能採取其他的管制手段來促使企業能符合 GDPR 的要求。英國 ICO 更表明，其不會改變現行的裁罰基準。

(二)臺灣企業或可積極參與資料可攜權的內涵形成

資料可攜權如何具體落實是本次會議中許多場次共同關心的問題。目前較為主流的意見應該是資料可攜權的具體內涵會由各行業內部合作討論形成。由於這將牽涉到資料架構的設計、資料欄目內容以及資料格式標準等問題，這類標準一旦形成，可能就會成為該行業內部共同遵循的標準。我國相關企業或許可以積極參與此一規範形成的過程，與歐洲的同行展開合作，以免未來相關標準難以適用。

(三)ePrivacy Regulation 及 GDPR 都有須持續觀察之處

ePrivacy Regulation 仍有待歐盟內部立法程序的完成，有許多改變的內容仍待持續的追蹤。而 GDPR 雖然即將要施行，但其許多新增的規範要求或權利內涵，在未正式實施之前，仍然無法完全明朗，我國宜持續就此二領域持續觀察。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

六、附錄

(一)行程表

時間	行程內容
4 月 16 日(一)	自桃園國際機場前往英國倫敦希斯洛國際機場
4 月 17 日(二)	(中停荷蘭阿姆斯特丹)
4 月 18 日(三)	參與 IAPP「2018 歐洲資料保護密集研討會」(Europe Data Protection Intensive 2018)
4 月 19 日(四)	參與 IAPP 2018 歐洲資料保護密集研討會
4 月 20 日(五)	上午：參與「關於 GDPR，你需要於 5 月 25 日前知道的一切」(Everything you need to know about GDPR before 25 May 2018) 說明會 下午：參與「給企業與新創的 GDPR 工作坊」(Workshop-GDPR for Entrepreneurs and Start-ups)
4 月 21 日(六)	自英國倫敦希斯洛國際機場返回桃園國際機場
4 月 22 日(日)	(中停荷蘭阿姆斯特丹)

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(二)研討會照片紀錄

資料來源：報告人自行拍攝

圖 1 英國資訊長 Elizabeth Denham 發表演說

本報告之智慧財產權歸屬於財團法人資訊工業策進會

資料來源：報告人自行拍攝

圖 2 歐洲各國個資主管機關圓桌論壇

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(三)攜回資料

1. Are You Prepard to Address New Privacy Laws in AI Environments 簡報資料
2. To BCR or to GDPR: That Is the Question 簡報資料
3. Greatest PR #Fails in U.S. Breach Response and How EU Companies Can Avoid Them 簡報資料
4. Privacy Challenges and Solutions for Blockchain Projects in the Context of GDPR 簡報資料
5. Creepy or Cool?簡報資料
6. Data Beyond GDPR 簡報資料
7. Data Breach Response: Tips from the Trenches 簡報資料
8. The Future of Consent 簡報資料
9. GDPR: 72-Hour Notification – Is Your Breach Response Plan Operational?簡報資料
10. Incident Response Session: Simulated Breach 簡報資料
11. Just Because You’re GDPR Compliant Does Not Mean You Can Use Your Data 簡報資料
12. New Controller and Processor Relationships Under GDPR - What a Show!簡報資料
13. New Individual’s Rights Under the GDPR: Power to the People and Business Challenges 簡報資料
14. North by Northwest: Managing Privacy Across the Value Chain 簡報資料
15. One GDPR and Many National Implementation Regimes – How to

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Find Your Way Through 簡報資料

16. Privacy by Design in Cars – Myth or Reality?簡報資料
17. Privacy in APEC: Views from Privacy Professionals 簡報資料
18. PSD2: How to Balance Open Banking and Privacy Protection 簡報資料
19. Regulatory Obligations – Engineering Requirement 簡報資料
20. Snooping on Your Staff: Privacy or Prying?簡報資料
21. Third-Party Privacy Risk – Beyond Your Organisation's Bounds for GDPR 簡報資料

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件三 美國出國報告

出國報告（出國類別：考察）

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制計畫

出國報告

姓名職稱；施弘文 法律研究員

派赴國家：美國

出國期間：107 年 10 月 2 日至 8 日

報告日期：107 年 10 月 22 日

本報告之智慧財產權歸屬於財團法人資訊工業策進會

一、目的

為執行「研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制」案，研議國家通訊傳播產業資料加值及個人資料隱私保護相關之法制規範或相關政策等議題，須蒐集他國目前之資料加值創新應用及隱私保護相關法制資訊及作法，針對目前世界各國對於隱私保護之趨勢，以及歐盟「一般資料保護規則」(General Data Protection Regulation，以下簡稱 GDPR）於今年（107 年）5 月施行後所產生之影響，瞭解目前國際上之隱私保護趨勢，以研議我國未來可行之政策與推動措施參考，故擬訂本次行程，於 107 年 10 月 2 日起赴美國為期 7 天之考察。

本次考察行程安排參加美國「隱私與安全論壇（Privacy + Security Forum）」，論壇之內容包含隱私保護之法律政策與實務作法、目前國際所關注之隱私議題與發展趨勢，以及目前新興科技應用下所衍生之隱私保護等相關議題，並透過參與論壇第一日舉辦的座談會（Workshop），瞭解美國聯邦貿易委員會（Federal Trade Commission, FTC）對於隱私保護所採取之相關政策與措施，作為我國相關政策之參考。

二、效益

GDPR 自今年 5 月實施以來已有數月時間，歐盟各國多已對於 GDPR 之遵法措施已預備多時，而國際上各國如何與之接軌，其相關作法或經驗，可作為我國相關法制政策之參考。此外，GDPR 就個資保護之規範詳盡，為目前國際隱私法制上之標竿，部分國家亦逐步配合調整其隱私法規，故本次考察之效益，即為瞭解目前國際上 GDPR 相關遵法之經驗，並藉此瞭解目前美國、歐盟及其他國家相關隱私或資安法規領域最新之

本報告之智慧財產權歸屬於財團法人資訊工業策進會

發展動態。

在產業部分，因企業型態之不同，相關 GDPR 之遵法措施亦有不同之作法，本次考察亦可瞭解目前各國產業界因應 GDPR 以及準備相應遵法措施之經驗，並瞭解目前國際上對於隱私保護及資安之趨勢以及所面臨之困境。另於新興科技之發展上，人工智慧的應用日趨普遍，本次考察亦可瞭解其所衍生新的隱私或資安風險，以及可能面臨的相關法制問題，藉此汲取各界隱私與資安專家之經驗，作為未來我國政策規劃之借鏡。

三、研習對象

(一)隱私與安全論壇（Privacy + Security Forum 2018）

「隱私與安全論壇」於 2015 年起至今年已連續舉辦四屆，由國際知名隱私法學者 Daniel Justin Solove 教授及 Paul M. Schwartz 教授所籌備主辦，Daniel Justin Solove 教授是美國喬治華盛頓大學法學院的法律研究教授，主要研究領域為隱私法，為該領域之知名學者，同時也是 TeachPrivacy 公司的創辦人，該公司主要為企業、醫療機構、大學或其他組織提供相關之隱私與網路安全之培訓及諮詢[317]。Paul M. Schwartz 教授是美國加州大學柏克萊分校法學院的法律教授，研究領域為資訊隱私法、智慧財產權、電信及資訊法等，同為美國知名之隱私法領域專家[318]。

其籌辦隱私與安全論壇之目的是希望藉由匯集國際上不同領域之專業人士，共同討論目前國際上隱私與安全的發展趨勢等議題，分享與交

[317] https://www.law.gwu.edu/daniel-justin-solove
[318] https://www.law.berkeley.edu/research/bclt/research/law-tech-research-portal/paul-m-schwartz/

本報告之智慧財產權歸屬於財團法人資訊工業策進會

流彼此經驗，該論壇並提供隱私與資安相關的線上課程與實作教學等，為一在隱私法制領域具有相當專業性之論壇。參加人員包含隱私專業人士、安全專業人員、資訊（隱私）主管、律師、政策制定者、學者、非政府組織之研究人員及技術專家等。

本次論壇共舉行三日，第一日分別於上午及下午安排不同主題之專題研討，第二日及第三日自上午至下午共安排接續 9 場之不同議題演講，由參加學員挑選適合的主題參加。本次論壇總計邀請超過 200 位包含學界、實務界及產業界等不同領域之講師，並安排近 80 場不同之議題，供參加學員參與。今年隱私與安全論壇之議題焦點，主要集中在歐盟隱私保護之議題，如歐盟「一般資料保護規則」（General Data Protection Regulation，以下簡稱 GDPR）的影響衝擊、各國之因應措施、法規適用，新興科技議題之隱私保護，如區塊鏈、人工智慧（Artificial Intelligence, AI）的隱私保護，以及目前國際上關於網路安全（Cybersecurity）之相關議題等，表 1 僅列本次考察所參加與本計畫有關之議題議程，詳細議程請參考附件。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

表 1 Privacy + Security Forum 2018 議程表

10 月 3 日研討會議程（Workshop）	
時間	議程
9:00~10:15	Understanding the FTC on Privacy and Security (Part 1)
10:45~12:00	Understanding the FTC on Privacy and Security (Part 2)
13:30~14:45	Blockchain (Part 1)
15:10~16:30	Blockchain (Part 2)
10 月 4 日論壇（Forum）議程	
時間	議程
8:50~9:50	Session1: ISO 27001 & The GDPR: Identifying Overlap and Streamlining Efforts
10:10~11:10	Session2: GDPR Compliance 2.0
11:30~12:30	Session3: The Intelligent Future: A legal Framework for Artificial Intelligence
14:30~15:30	Session4: Managing Consent Headaches in the EU: Best Practices in Obtaining a GDPR-Compliant Consent
16:00~17:00	Session5: The GDPR’s First Four Months: What

本報告之智慧財產權歸屬於財團法人資訊工業策進會

	Happened and What is Next?
10 月 5 日論壇議程（Forum）	
時間	議程
8:50~9:50	Session6: The ePrivacy Regulation: The Next EU Frontier
10:10~11:10	Session7: How Will the GDPR Affect the Application and Development of Artificial Intelligence?
11:30~12:30	Session8: The Data Protection Officer in the EU
14:30~15:30	Session9: Data and Privacy in the Autonomous Car: What New Questions Might We Face?

資料來源：本研究整理

(二)Pre-Conference Workshops

1. Understanding the FTC on Privacy and Security

第一日上午的研討會主題，挑選 Understanding the FTC on Privacy and Security 參加，藉以瞭解美國聯邦貿易委員會在消費者隱私保護上所採取之相關作法。該研討會內容主要針對美國聯邦貿易委員會對於消費者隱私保護之工作內容進行相關介紹，並討論聯邦貿易委員會的職責及管轄範圍，以及其對於消費者之隱私保護相關政策等。本主題邀請到聯邦貿易委員會隱私與身份保護部門（Division of Privacy and Identity Protection）的資深律師 Jamie Hine 為主講人。Jamie Hine 首先簡介了該部門主要負責之工作內容，包含監管消費者隱私保護、信用徵信、身份

本報告之智慧財產權歸屬於財團法人資訊工業策進會

盜竊和資訊安全等業務，並於其管轄範圍內執行相關法律規範，拓展服務範圍和政策制定，並向消費者和企業宣導新興科技所帶來的隱私、信用徵信或資料保護之相關影響，並提供身份竊之盜預防及協助等。

Jamie Hine 並表示，美國聯邦貿易委員會從 1990 年代即開始關注消費者隱私與安全保護之議題，然而美國未具有單一之隱私或資料保護法規，而是依據職掌法規監管消費者保護及市場競爭。以隱私與身份保護部門而言，該部門所職掌之法規，包含聯邦貿易委員會法第 5 條（Section 5 of the FTC Act），禁止對消費者為不公平或詐欺行為；公平合理信用報告法（The Fair Credit Reporting Act），要求相關信用機構確保消費者資料之正確性及尊重其隱私，並賦予消費者有權知悉其何種資訊經債權人、保險公司或雇主知悉。The Gramm-Leach-Bliley Act，亦稱為金融服務現代化法（Financial Services Modernization Act of 1999），要求金融機構須確保顧客資料的保密與安全，並使消費者得以確保其資料不會分享至不相關之第三方；兒童在線隱私保護法（Children's Online Privacy Protection Act），使家長得以掌控企業利用網路所蒐集有關其孩童的資訊及如何利用；有害健康通知規則（The Health Breach Notification Rule），要求未受健康保險可攜性及責任法案（The Health Insurance Portability & Accountability Act, HIPAA）規範的企業，如發生可識別個人身份的電子健康資料洩漏之情況，應通知該用戶。

隱私與身份保護部門除監管上述法規外，亦提供隱私保護相關的指引手冊及報告，供企業或消費者參考，並提供受害者相關的隱私保護協助。而該部門除受理消費者之申訴外，亦主動從新聞、報章媒體或網路等管道，瞭解相關之資料洩漏或隱私侵害等案件，並進行相關之調查。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

該部門受理案件後，將先進行相關資料的蒐集，進而開啟後續的民事調查，並對案件的事實進行分析，決定是否進行訴訟或調解，最後持續進行後續的追蹤監管。該部門目前約有 600 名員工，大部分具有律師資格，負責處理上述之業務。

2. Blockchain

第一日下午的研討會，參加區塊鏈（blockchain）的主題，討論區塊鏈的運作及運用，以及區塊鏈可能涉及的隱私、安全問題與目前法規的影響等。主講人為 James M. Aquilina，James M. Aquilina 是 Aon Cyber 公司的總裁，並為旗下 Stroz Friedberg 公司執行管理團隊的成員，負責該公司的全球數位鑑識相關業務。Stroz Friedberg 公司為一專業的風險管理公司，主要為協助企業解決網路安全、數位鑑識、事件應變、調查等問題。James M. Aquilina 具有豐富的數位鑑識及電腦、網路犯罪等實務及諮詢經驗，並曾擔任美國加州刑事助理檢察官，承辦過美國第一個對於殭屍網路攻擊事件提起訴追之案件[319]。

James M. Aquilina 首先介紹了區塊鏈的含意及運作方式，而由於區塊鏈技術具有分散式資料庫（Distributed database）、不可改變（Immutable）、共享（Shared）及安全（Secure）等優點，故多適用在多數人間不具有信任關係的交易中，如加密貨幣。然而加密貨幣的應用（如比特幣），僅為區塊鏈技術應用之一環，區塊鏈技術尚可運用在各領域，如醫療紀錄資料、政府保有之民眾資料等。而在資安風險部分，James M. Aquilina 表示區塊鏈技術雖有上述優點，但仍有其風險，並舉出下列區塊鏈技術上可能面臨之資安風險，如 51%攻擊（51% Attack）的風險，

[319] https://www.strozfriedberg.com/professional/james-aquilina/

本報告之智慧財產權歸屬於財團法人資訊工業策進會

即當有人掌控超過 50%的網路運算能力，攻擊者則有能力造成區塊鏈的網路系統停止運作；此外，如於客戶端、智慧合約（smart contracts）或電子錢包（wallets）存有病毒或弱點時，亦有可能造成加密貨幣被竊取之情形。而在法律面上，因比特幣交易網路中的各節點，均會擁有網路內比特幣交易的相關紀錄，James M. Aquilina 認為此種交易方式，會有侵害隱私保護之疑慮。

(三)Privacy + Security Forum

第二日及第三日的會議，主要挑選與歐盟 GDPR 及隱私保護相關之議題參與，參加之場次及內容整理如下：

1. ISO 27001 & The GDPR: Identifying Overlap and Streamlining Efforts

本場次之內容主要針對 ISO 27001 資訊安全管理系統國際標準與 GDPR 的規範進行討論，主講人為 Brian Philbrook。Brian Philbrook 為 OneTrust 公司的隱私顧問，負責提供全球之隱私法規指導，協助企業建置隱私法遵措施。OneTrust 公司是隱私管理系統軟體平台業者，提供不同類型的隱私管理軟體或諮詢訓練協助客戶建立企業之隱私保護制度，使企業得以遵循不同區域或管轄範圍的資料隱私保護規範（如歐盟 GDPR 或 ePrivacy），該公司超過 1,500 名客戶，為全球隱私管理系統的領導業者。

Brian Philbrook 表示，ISO 27001 主要用於資訊安全管理機制的建立，目的在保全資料的機密性、完整性及可用性。而 GDPR 則是著重於個人資料隱私的保護，兩者具有部分之相同處，如 ISO 27001 與 GDPR 均著重於降低資料外洩之風險，並要求企業投入資源、人力與層級在法

本報告之智慧財產權歸屬於財團法人資訊工業策進會

遵措施上。而企業如欲減少重複資源之投入，在導入 GDPR 相關規範時，首先應盤點相關措施與 ISO 27001 的重疊處，考量如何利用專業人員的現有工作或企業內部機制來達到 GDPR 之要求，進而思考如何利用 ISO 27001 的管理框架與 GDPR 的政策、目標與要求進行接軌，節省法遵之成本。

Brian Philbrook 並歸納出 ISO 27001 與 GDPR 之六項可共同協力執行之措施，包含安全措施、通知義務、委外廠商管理、文件軌跡保存、資料保護設計（Data Protection by Design）及資料主體權利等，並舉出企業於 ISO 27001 與 GDPR 合作銜接之具體方式。

(1) 在安全措施上，ISO 27001 要求組織須考量內外部之安全議題，並規劃、構建相關之安全措施計劃以及建立風險評估機制。而 GDPR 同樣將安全訂為隱私原則的核心，並要求組織採用相關技術或措施，以確保其安全水平得以因應其風險。此外，Brian Philbrook 並強調組織內部合作之重要性，組織內部之隱私團隊與資安團隊兩者間之溝通、合作，在法律遵循上才能發揮出最大之效益。

(2) 在通知義務上，ISO 27001 要求組織應訂定識別資安事件及通報應變的機制或方式。而 GDPR 亦規定業者負有向監管機構的通知義務，以及於知悉個資洩漏事件後 72 小時內，應對受影響之個人進行事件之通知。故在組織內，原有 ISO 27001 之相關通報應變機制及文件，則可納入 GDPR 之規範內容，使兩者機制進行整合，以簡化通報流程。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(3) 在委外管理上，ISO 27001 在委外之監管可視組織之需求，對委外廠商採取相關符合組織資料保護要求之措施，而 GDPR 對於資料處理者則具有較為詳細之要求，如要求業者僅能委託能提供適當安全性證明之廠商、委外契約之內容等，而組織則可設計相關之檢核表來進行委外廠商資格之檢視。故 ISO 27001 與 GDPR 在組織內之調和上，可共同確認委外廠商是否具有符合兩者要求之安全性措施，並將安全保證納入委外合約中。

(4) 文件軌跡保存為因應資料主體行使權利時之重要資料，ISO 27001 要求須識別並將資料標記（如資料所有人、存取人或用途等）、分類及分級，並應訂定資料存取控制規範。而 GDPR 在資料保存上，則要求資料控制者和處理者必須保留資料處理之軌跡紀錄，包含如資料類別、資料主體類型、保護措施、國際傳輸等。因此在 ISO 27001 與 GDPR 協調上，透過跨部門之溝通協調，並利用組織內資安小組的資產盤點建立資料清單，並於資料使用時通知隱私小組建立軌跡紀錄，共同建置適合組織之文件軌跡保存機制。

(5) 在資料保護設計（Data Protection by Design）上，ISO 27001 提供一彈性之框架，要求組織需制訂並定期審查其安全政策及進行風險安全評估。而 GDPR 則由資料管理之角度出發，要求組織從一開始即應將安全和隱私原則融入產品和流程中。故在 ISO 27001 與 GDPR 之協調上，Brian Philbrook 認為資料保護設計的關鍵在於生產階段和系統設計，組織可於這兩部分將相關之安全和隱私原則納入流程或系統中，並可參考 GDPR 對資料最小化

本報告之智慧財產權歸屬於財團法人資訊工業策進會

的要求納入現有的安全政策。

(6) 在資料主體權利上，ISO 27001 要求對於資料應進行分類及存取控制，而 GDPR 則具體列出資料主體的權利，如刪除權、更正權、限制處理權等，並要求對於當事人之權利行使，應有相關之作為。故於現階段，Brian Philbrook 建議可利用組織內現有的處理程序，來因應當事人之要求，而組織內部則應同時使內部資料處理程序透明化，並使資安小組參與當事人權利行使之處理程序，以調和 ISO 27001 與 GDPR 之規範。

2. GDPR Compliance 2.0

GDPR 於今年 5 月實施後至今已近半年時間，產業界多已開始進行相關之因應作法，並訂定新的法遵流程或執行措施，本場次邀請到四位於實務界從事隱私保護法遵工作之專業人員，其中三位分別為擔任旅遊公司、教育單位及雲端服務產業之隱私保護顧問或主管，分享其建置有關 GDPR 法遵措施之經驗。

Mikaela Karlsson 為旅遊公司 KAYAK 的隱私顧問，處理公司隱私相關之法律問題，其表示為因應 GDPR 之實施，公司成立了一個團隊來處理相關之法遵事務，該團隊首先從法遵開始，將 GDPR 條文進行逐條的釋義與釐清，進而組成執行團隊進行相關措施之實施。而在實施中，因資料保護需透過不同部門之協力，故必須經各部門間之協調及合作（如 IT 部門、人力資源部門等），而當各部門均能瞭解法遵之影響及衝擊後，開始建置相關之資料處理流程及程序時，各部門將較有意願配合。而為因應 GDPR 的實施，該公司前後歷經了一年的準備時間。此外另有與談

本報告之智慧財產權歸屬於財團法人資訊工業策進會

者表示，其單位係將部分業務委託外部諮詢（顧問）公司來進行相關之法遵作業，此亦為一有效率之方式可供參考。

本場次之討論主要重點可彙整如下：(1）為使企業或組織內部因應GDPR 的相關規範，企業內部各部門應先充分瞭解其衝擊與影響，並應就相關事項進行協調；(2）公司內部應建立清楚的流程，使第一線的工作人員或委外廠商均能知道應如何進行各項流程的步驟，而資料主體亦能知道如何行使其擁有之相關權利。(3）企業應特別重視於隱私保護政策、產品以及委外廠商之管理是否符合 GDPR 之規範要求，相關之文件、合約規範，是否一併調整。

3. The Intelligent Future: A Legal Framework for Artificial Intelligence

隨著人工智慧逐漸應用於各行各業，國際上開始討論對於人工智慧之管理，相關之監管機關與業界正在思考如何使人工智慧技術納入目前之法律框架中。本場次會議即針對此議題為討論，並以隱私保護為焦點，來探討建構人工智慧技術法律框架之可能性。會議邀請到三位產業界的隱私專業人員來討論目前人工智慧的趨勢、應用、法律框架及相關風險等。

本場會議邀請到 Lindsey Tonsager，首先針對目前人工智慧之定義及於發展上所應具有之功能為闡述。Lindsey Tonsager 於 Covington & Burling LLP 事務所負責人工智慧之相關計畫，Lindsey Tonsager 表示，目前人工智慧尚處於發展階段，而最終目標係希望人工智慧有能力與人一樣進行相同之行為，如在視覺部分，有能力辨識圖片或影像的內容；在聽覺部分，則能理解對方所說的內容；在語言部分，則能瞭解詞義；在認知上，則能夠通過理解人、事、物、地點及事件等之間的關係來推

本報告之智慧財產權歸屬於財團法人資訊工業策進會

理；在學習能力上，則可透過自行學習提升能力而無須藉由程式編碼；在決策上，則能夠在多數選擇中建議或採取特定行動。而目前人工智慧的應用逐漸廣泛，並將影響各行業原來之運作方式，進而可能衍生相關之法律問題，如人工智慧的運作方式，即可能對於個人之隱私與安全產生影響或侵害等。

在法律規範部分，Derek Smith 與 Elaine Call 兩位專家表示，人工智慧的法律框架可從消費者保護出發，對於消費者保護目前可從三個面向思考，並舉出目前相關之參考法規，即考量隱私保護（如歐盟 GDPR）、透明性（如聯邦貿易委員會法第 5 條禁止詐欺行為）及公平性（如聯邦貿易委員會法第 5 條禁止不公平行為）。

此外，因人工智慧應用的多元化，故將來在法律規範上，則可從監管規範、商業應用、責任及社會等層面思考法律框架之建構。如相關法律規範上，尚可考量其他的監管規定，如競爭/反壟斷、數位健康、金融服務、運輸服務、就業、政府採購及貿易管制和禁運等相關之監管法規。商業面則可考量如智慧財產權、服務提供的程度或等級、人工智慧本身之安全風險等。責任上則可考量安全性、過失/侵權、刑事責任、保險範圍等。而社會面則可考慮勞動力、監督、責任歸屬及社會福利或價值等。最後會議並舉出幾個案例討論，並從上述因素思考可能之法律規範。

4. The ePrivacy Regulation: The Next EU Frontier

歐盟近年來除 GDPR 外，亦對於 2002 年頒布之「隱私與電子通訊指令」（Directive on privacy and electronic communications, Directive 2002/58/EC）進行重大修正。本場次會議主要在討論歐盟將隱私與電子通訊指令修正為「隱私與電子通訊規則」（Regulation on Privacy and

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Electronic Communications，簡稱 ePrivacy Regulation）之立法背景與現況，以及與 GDPR 之關聯。本場次邀請到歐洲資料保護委員會（European Data Protection Board）副主席 Willem Debeuckelaere 為主講人。

Willem Debeuckelaere 首先簡述了隱私與電子通訊規則的立法背景及內容，Willem Debeuckelaere 表示，在歐盟數位單一市場戰略（The Digital Single Market Strategy）下，為達到歐盟境內對於數位服務的信任與安全性之目標，歐盟通過了 GDPR 之規定，並針對原來的隱私與電子通訊指令（Directive on privacy and electronic communications, ePrivacy Directive）重新進行評估，希望能提升電子通訊服務的隱私保護，並使其能符合數位單一市場戰略之目標以及能與 GDPR 之規範一致。評估之結果認為，雖然隱私與電子通訊指令的規範原則仍符合目前的隱私保護框架，但指令卻未能跟上科技的發展，如互聯網的應用、OTT 通訊服務等。歐盟在經過政策與效益的評估及市場民意調查後，歐盟執委會提出了隱私與電子通訊規則。隱私與電子通訊規則依循 GDPR 之規範，並同屬規則（Regulation）之法律位階，並適用於視為個人資料之電子通訊資料（如 cookie, OTT 通信服務等）。因此，在法規適用上，隱私與電子通訊規則屬 GDPR 的特別法，就涉及個人資料的部分，可能適用 GDPR 與隱私與電子通訊規則，而就電子通訊資料部分，則適用隱私與電子通訊規則。

雖然隱私與電子通訊規則曾預計與 GDPR 同時實施，但目前仍於討論中，Willem Debeuckelaere 表示，隱私與電子通訊規則目前於歐盟理事會已有新的版本提出，其中在第 6 條（Permitted processing of electronic communications data）與第 10 條（Information and options for privacy

本報告之智慧財產權歸屬於財團法人資訊工業策進會

settings to be provided)，有較大幅度之修改，並於第 8 條（Protection of end-users' terminal equipment information stored in terminal equipment of endusers and related to or processed by or emitted by end-users' terminal such equipment）提出了部分法律爭議，主要在於電子通信設備透過無線網路（wifi）連線時，廠商利用連線時所取得之資料進行利用之爭議。

對於隱私與電子通訊規則正式通過之時程，目前尚未有一明確的時間點，Willem Debeuckelaere 表示，隱私與電子通訊規則因各方有不同之意見，歐盟內部尚未能形成共識，就個人資料保護部分，目前已有 GDPR 及相關規範可資適用，而明年（2019）又適逢歐洲議會選舉等因素，其立法進程可持續追蹤觀察。

5. How Will the GDPR Affect the Application and Development of Artificial Intelligence?

本場次主要在討論 GDPR 對於人工智慧在應用上及發展的影響，並邀請到三位隱私與安全之法律、技術專家前來進行討論。Neil Chilson 目前為一研究機構之技術與創新資深研究員，首先對於人工智慧的運作原理及內涵進行概述。相關內容整理如下：目前人工智慧是藉由大量資料之蒐集、分析及演算，使程式進行深度學習，藉由輸入相關之訓練資料進行分析、比對，使程式得以對事件形成判斷或預測模型，並得以透過該模型識別新資料而進行自動決策。由於預測模型將來所處理之資料不見得會與所輸入之訓練資料相同，故在形成預測模型的學習過程中，輸入學習的資料應具有概括性，故會刪除部分偏離的資料。

人工智慧在應用上涉及資料的處理，故亦適用 GDPR 之規範，而在 GDPR 之規範中，部分資料保護原則對於人工智慧的運作則會產生挑

本報告之智慧財產權歸屬於財團法人資訊工業策進會

戰。Neil Chilson 指出，人工智慧與 GDPR 的衝突，主要會出現在公平原則、目的限制原則、資料最小化原及透明性原則等。舉例而言，公平原則要求所有之個人資料處理都應尊重資料主體的權益，並依據資料主體可預期之方式來使用。公平性原則亦要求資料控制者應採取相關措施，以防止對於個人之歧視。然而如於人工智慧形成預測模型的過程中，輸入的訓練資料有所偏差或與所欲形成的模型主題無關，則模型的結果可能產生不正確或具有歧視性，而將違反 GDPR 的公平原則。此外，在資料最小化原則上，GDPR 要求資料利用應適當，並限於與處理目的相關、必要之資料。而此原則與人工智慧之開發則有所相違，因預測模型的形成通常需要大量的個人資料，而哪些資料係屬必要，判斷上則有困難。此外，在學習過程中，亦難以預測人工智慧將學習到什麼，而預測模型之目的亦可能因學習過程而改變，故與最小化原則有所違背。

對於上述之影響，Nancy Libin 與 Jules Polonetsky 則做了部分的回應，Nancy Libin 為 Davis Wright Tremaine 事務所負責隱私與安全及技術的高階主管，提供資料隱私與網絡安全的法律和監管諮詢。Jules Polonetsky 則為未來隱私論壇（Future of Privacy Forum）的執行長，該論壇主要研究隱私保護之相關議題。其表示人工智慧在 GDPR 的資料處理規範下，較為可行的方式應為取得資料主體的同意，可考量透過與資料主體以合約作約定來解決上述問題。而在資料最小化上，則可限縮於僅輸入所必須的關鍵性資料，以符合資料最小化之要求。

6. The Data Protection Officer in the EU

依據 GDPR 第 37 條之規定，部分企業應於歐盟設置資料保護官（Data Protection Officer, DPO），故本場次則針對資料保護官之工作內容

本報告之智慧財產權歸屬於財團法人資訊工業策進會

進行分享與討論，簡述 DPO 之工作內容及於企業中扮演之角色等。本場次邀請到 Anna Zeiter 前來分享其工作經驗，其目前為 eBay 公司的首席隱私保護官。

Anna Zeiter 表示由於 GDPR 的規定，歐盟境內對於隱私保護的專業人才需求增加，連帶 DPO 的薪資水平也大幅提升，而在工作內容上，DPO 之職責具有相當之獨立性，但於工作上仍必須同時兼顧企業的發展與隱私保護兩個層面，因其必須同時面對公司內部的管理高層以及歐盟各會員國內的資料保護機關（Data Protection Authorities, DPA），故須具備充分的協調與隱私專業能力，並需對於企業之運作能充分了解。且 DPO 之任用上，並無法隨意免職，因此企業在任用 DPO 上，多會充分考量其是否與企業文化相符。此外，由於企業其分支機構可能設置於歐盟境內各處，而 DPO 需顧及企業內部整體的隱私保護水平，故語文溝通能力對 DPO 而言則為一挑戰，大多 DPO 多兼具一種以上之外文能力。雖 GDPR 之規範上僅要求企業應設置一名資料保護官，但 Anna Zeiter 表示，為求效率與分工，大規模企業多於歐盟會員國內設置不只一位 DPO，如依照業務區域來設置 DPO，而企業內如有數名 DPO，其內部則應建立相同標準的隱私保護程序，DPO 間亦須有良好的溝通及程序措施，使企業內部的隱私保護標準及作法得以一致。

而就目前企業設置 DPO 之情形，GoncaGökgöz-Dhont 則提供了部分意見，其為 DPO 網絡歐洲（DPO Network Europe）公司的董事總經理，該公司為一家專門招聘 DPO 的人力資源公司。GoncaGökgöz-Dhont 表示，目前 DPO 設置有分為企業內部或外部兩種方式，企業內部係由企業自行聘任 DPO，而外部則係透過委託專業事務所或人士，協助處理企業

本報告之智慧財產權歸屬於財團法人資訊工業策進會

之隱私保護事項。兩種方式各有優缺，可視企業經營之方式採用，依目前實務而言，較小規模之公司，多採取外部之方式為之。

四、心得及建議

綜整此次參與論壇之心得，目前國際上關於隱私保護之議題，主要仍聚焦在 GDPR 相關制度或措施之接軌或因應，而對於隱私保護之新興議題，則圍繞在 AI 人工智慧的應用上。

(一)隱私法制部分

歐盟 GDPR 雖於已於今年 5 月實施，然各國仍然處於調適之階段，企業部分亦嘗試不同之新興作法（如資料大使館），以達到 GDPR 之相關要求，故在此趨勢下，隱私相關之顧問諮詢企業（如 DataGuidance、OneTrust、 NYMITY、radar 等），亦依據法規之規範發展出不同之法遵流程措施提供參考，而相關隱私法規資料庫的建立及法遵系統，亦相當詳盡豐富，可見目前國際上對於個人資料隱私保護之趨勢，已朝向建立系統流程化之法遵管理方式。

在法規面上，各國之隱私法制有漸進調整之趨勢，GDPR 之部分內容逐漸為國際間所採納，故本屆論壇部分內容即針對目前各國之隱私法制為討論主題，如美國加州於今年 6 月所通過之加州消費者隱私法（California Consumer Privacy Act，CCPA）、韓國、加拿大之隱私法規等。整體而言，國際上對於隱私保護之法制架構，因 GDPR 之影響，產生了漣漪之效應，各國企業雖不見得適用 GDPR 之規範，然卻逐漸提升了其隱私保護之水平。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

此外，論壇之另一討論重點在於各國隱私法制間之調和，目前國際上部分國家係參考 GDPR 之相關規定而調整國內之隱私法規（如日本、韓國），並希望藉由取得歐盟之適足性認定，使其得以自由地與歐盟進行個人資料之跨境傳輸，部分國家則以協議之方式為之（如美國隱私盾協議）。而企業因應國際間不同之隱私監管法制，多以尋求隱私顧問諮詢企業或專業協助之方式為之，透過隱私專業人員之協助，以遵循當地之隱私保護法制措施。故可以想像，將來對於隱私保護之專業人才之需求將大幅提高，而我國則可考慮對於隱私專業人員進行有計畫之培訓，以因應將來隱私保護之趨勢。

(二)隱私新興議題

在新興科技的隱私議題上，人工智慧為目前較為熱門之討論，特別是人工智慧應用之部分，如自動駕駛、健康資料等所衍生之隱私保護問題。目前雖已開始討論人工智慧相關之法制建置、隱私保護及風險預防等面向，但就法制而言仍未能有一全面之架構，相關之法律框架及責任規範仍於討論中，本次論壇雖有多場議題與人工智慧有關，但多為提出可能之思考方向或可採行之建議或作法，具體架構及內容則尚未成形。然於人工智慧的深度學習過程中，涉及與隱私保護之衝突與挑戰，相關之思考方向及討論，仍可作為我國人工智慧發展之參考。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

五、附錄

(一)行程表

時間	行程內容
10 月 2 日（二）	臺北至華盛頓航程（舊金山轉機）
10 月 3 日（三）	參加「隱私與安全論壇座談會」（Privacy+Security Forum Workshops） 上午主題:「瞭解 FTC 的隱私與安全」(Understanding the FTC on Privacy and Security） 下午主題：「區塊鏈」（Blockchain）
10 月 4 日(四)-10 月 5 日（五）	參加「隱私與安全論壇」（Privacy+Security Forum）
10 月 6 日(六)-10 月 8 日（一）	華盛頓至臺北航程（舊金山轉機）

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(二)研討會及論壇照片紀錄

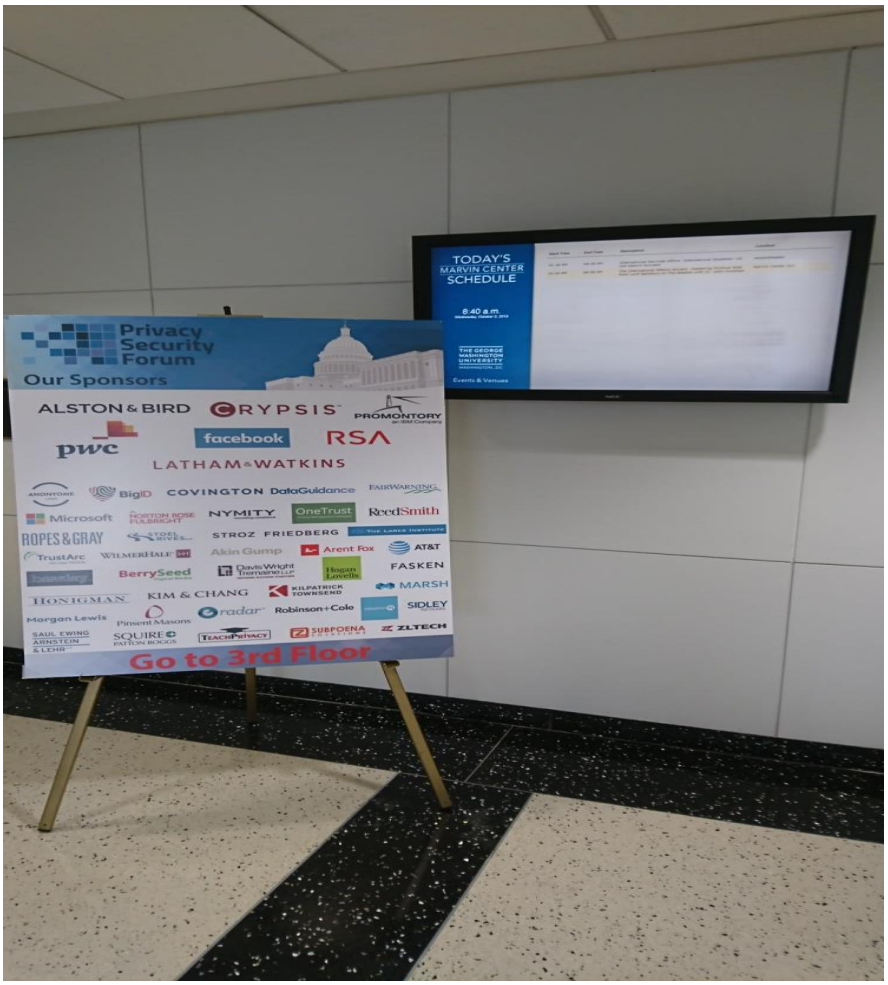


圖 1 Privacy+Security Forum 參與廠商

資料來源：報告人自行拍攝

本報告之智慧財產權歸屬於財團法人資訊工業策進會

圖 2 Workshop: Understanding the FTC on Privacy and Security 現場

資料來源：報告人自行拍攝

圖 3 Workshop: Blockchain 現場

資料來源：報告人自行拍攝

本報告之智慧財產權歸屬於財團法人資訊工業策進會

圖 4 ISO 27001 & The GDPR: Identifying Overlap and Streamlining Efforts 現場

資料來源：報告人自行拍攝

圖 5 The Intelligent Future: A Legal Framework for Artificial Intelligence 現場

資料來源：報告人自行拍攝

本報告之智慧財產權歸屬於財團法人資訊工業策進會

圖 6 Keynote: The US and EU: Areas of Convergence, Areas of Divergence?現場

資料來源：報告人自行拍攝

(三)攜回資料

1. Understanding FTC: Careful Connections Building Security Internet of Things 會議提供資料
2. Understanding FTC: Data Breach Response Guide for Business 會議提供資料
3. Understanding FTC: FTC Privacy and Data Security Update 2017 會議提供資料
4. Understanding FTC: Start With Security 會議提供資料
5. Governing the Blockchain How to Determine Applicable Law 會議提供資料
6. Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty 會議提供資料
7. ISO 27001 & the GDPR: Identifying Overlap and Streamlining Efforts 簡報資

本報告之智慧財產權歸屬於財團法人資訊工業策進會

料

8. California Consumer Privacy Act vs GDPR What You Need To Know 會議提供資料
9. Future Proofing Privacy 會議提供資料
10. The Intelligent Future: A Legal Framework for Artificial Intelligence 簡報資料
11. Leveraging GDPR Initiatives to Comply with the CCPA and Other Privacy Laws 簡報資料
12. Korean Data Privacy Law Post-GDPR and Pre-Adequacy 簡報資料
13. Less Than 20Weeks to the European Union GDPR—What to Do Now? 會議提供資料
14. GDPR Ante Portas : Compliance Priorities for the Impending EU Data Protection Regulation 會議提供資料
15. Representatives under Art.27 of the GDPR IAPP 2018 會議提供資料
16. ePrivacy Regulation Consolidated Austrian compromise text of the draft ePrivacy regulation 9.20.2018 會議提供資料
17. ePrivacy Regulation COM 會議提供資料
18. ePrivacy Regulation Report 會議提供資料
19. Should your company appoint a data protection officer(DPO) under the GDPR? 會議提供資料
20. Artificial intelligence and privacy 會議提供資料
21. Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Models 會議提供資料
22. Unfairness by Algorithm: Distilling the Harms of Automated Decision Making 會議提供資料
23. General Data Protection Regulation The Official Text 會場廠商提供資料

本報告之智慧財產權歸屬於財團法人資訊工業策進會

24. CCPA Accountability Handbook 會場廠商提供資料

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(四)Privacy+Security Forum 全部議程

Forum Day 1 – Thursday, October 4, 2018

Session 1
Thurs, Oct 4 8:50 AM – 9:50 AM

ISO 27001 & the GDPR: Identifying Overlap and Streamlining Efforts
Level 201, Room 301
- Leon Ravenna, Chief Information Officer, KAR Auction Services Inc.
- Dr. Barbara S. Walker, Sr. Director, Global IT Operations and Security, PolyOne Corporation
- Brian Philbrook, Privacy Counsel, OneTrust

Protecting Knowledge Assets: An International Perspective on Cybersecurity
Level 201, Room 302
- Jon Neiditz, Partner, Kilpatrick Townsend & Stockton
- Alison Howard, Assistant General Counsel, Microsoft
- Niko Härting, Partner, HÄRTING (Berlin)

A Compare and Contrast on the U.S. and Canada Privacy Law
Level 201, Room 311
- Kurt Wimmer, Partner, Covington & Burling LLP
- Alex Cameron, Partner and Chair, Privacy and Cybersecurity Group, Fasken

Biometrics in Global Digital Identity Programs
Level 201, Room 403
- Brenda Leong, Senior Counsel & Director of Strategy, Future of Privacy Forum
- Andrea Hackl, Research Analyst, Ranking Digital Rights, Open Tech Institute, New America
- James Loudermilk, Senior Director Innovation & Customer Solutions, IDEMIA National Security Solutions

Leveraging Transactional Data
Level 201, Room 307
- Elizabeth Canter, Partner, Covington & Burling LLP
- Kimberly Wong, Senior Counsel, Data & Technology Practice Group, McDonald's Corporation
- Zoe Sharp, Deputy General Counsel, Optoro

Managing Privilege and Related Concerns in Incident Response
Level 201, Room 308
- Gerard M. Stegmaier, IP, Tech & Data, ReedSmith LLP
- Megan Gabriel, LEVICK Communications
- Sam Rubin, Vice President, Crypsis
- Dawn-Marie Hutchinson, Executive Director, Office of the CISO, Optiv

continued

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Session 1, Thurs, Oct 4, 8:50 AM – 9:50 AM (continued)

The California Consumer Privacy Act: Our First "Federal" Privacy Law?
Level 201, Room 309
- Alfred Saikali, Chair, Privacy & Data Security Practice, Shook Hardy & Bacon
- Debra Farber, Senior Director, Privacy Strategy, BigID
- Travis LeBlanc, Partner, Boies Schiller Flexner LLP

AI and Health Information and Technology
Level 201, Room 405
- Dominique Shelton, Partner, Privacy & Security, Perkins Coie LLP
- Venora Hung, Manager, Clinical, UnitedHealth Group
- Nandita Guha, Senior Legal Counsel, Roche Diagnostics
- Kori Kelley Meehan, Senior Privacy Counsel, Google

Break
Thurs, Oct 4 9:50 AM – 10:10 AM
Grand Ballroom

Session 2
Thurs, Oct 4 10:10 AM – 11:10 AM

Has the Time for Baseline Privacy Legislation in the US Come at Last?
Level 201, Room 301
- Cameron Kerry, Senior, Counsel, Sidley Austin LLP
- Julie Brill, Corporate Vice President and Deputy General Counsel, Microsoft
- Nuala O'Connor, President & CEO, Center for Democracy & Technology
- Eric Einhorn, Chief Counsel to Senator Brian Schatz
- Michelle Ash, Chief Minority Counsel, Subcommittee on Oversight & Investigations, House Energy & Commerce Committee

Medical Device Security and Privacy: Risks, Liability, and Recommendations
Level 201, Room 302
- Elliot Golding, Partner, Squire Patton Boggs LLP
- Seth Carmody, Ph.D., Cybersecurity Program Manager, Food and Drug Administration
- Teri Campbell, Global Privacy Officer, Permobil

Legal vs Forensics: What Attorneys Should Know About Digital Forensics in Incident Response Management
Level 201, Room 307
- Donna McPartland, Counsel, Arent Fox LLP
- Ann Marie Barry, Chief Privacy & Records Management Officer, Johnson Controls Inc.
- James Aquilina, President, Aon Global Cyber Solutions, Stroz Friedberg

continued

Session 2 Thurs, Oct 4, 10:10 AM – 11:10 AM (continued)

Developing an Advanced Workforce Training Program
Level 201, Room 311
- Debra Bromson, Assistant General Counsel, AAA Club Alliance Inc.
- Margaret Gloeckle, Vice President, Privacy and Compliance Counsel, A&E Networks
- K Royal, Senior Director, West Region, Privacy Consulting, TrustArc
- Ashley Slavik, Data Protection Officer & Lead Data Counsel, Veeva Systems Inc.

Vulnerability Management
Level 201, Room 308
- David Sheidlower, CISO, Turner Construction
- Larry Whiteside, Greenway Health, Chief Information Security Officer

Designing a Global Employee Privacy Program
Level 201, Room 310
- David Longford, CEO, DataGuidance
- Bonnie Yeomans, VP, Assistant General Counsel and Privacy Officer, CA Technology
- Addison Brown, Privacy Specialist, Allegis Group

All Your Network Interfaces Belong to Us: Managing Privacy Risk at the Level of Network Traffic
Level 201, Room 403
- Steven Roosa, Head of NRF Digital Analytics & Technology Assessment Platform, Norton Rose Fulbright
- Mira El Sonbaty, VP and Group Privacy Officer, 21st Century Fox

Buying and Using Alternative Data Sources: Best Practices
Level 201, Room 405
- Marc Zwillinger, Founder, ZwillGen
- Sara Cable, Director, Data Privacy & Security & Assistant Attorney General, Massachusetts
- Sam Fraenkel, President, Co-Founder, TOMAHAWK

GDPR Compliance 2.0
Level 201, Room 407
- Bret Cohen, Partner, Hogan Lovells
- Michael Hamilton, Senior Corporate Counsel, Privacy, Salesforce
- Andy Bloom, Chief Privacy Officer, McGraw-Hill Education
- Mikaela Karlsson, Corporate & Privacy Counsel, KAYAK

Break
Thurs, Oct 4 11:10 AM – 11:30 AM
Grand Ballroom

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Session 3
Thurs, Oct 4 11:30 AM – 12:30 PM

The Intelligent Future: A Legal Framework for Artificial Intelligence
Level 201, Room 301
- Lindsey Tonsager, Partner, Covington & Burling LLP
- Derek Smith, Senior Counsel, Airbnb
- Elaine Call, Senior Privacy Counsel, LinkedIn

Leveraging GDPR Initiatives to Comply with the CCPA, the LGBD and Other Privacy Laws
Level 201, Room 307
- Teresa Troester-Falk, Chief Privacy Global Strategist, Nymity
- Andy Bloom, Chief Privacy Officer, McGraw-Hill Education
- Kimberly Bubnes, Director, Global Data Privacy, General Motors
- Jennie Hargrove, Global Data Privacy Manager, HID Global

Hot Topics in TCPA Litigation
Level 201, Room 308
- Ian Ballon, Shareholder, Greenberg Traurig LLP
- Eulonda Skyles, Assistant General Counsel, Privacy, Capital One
- Debra McGuire Mercer, Of Counsel, Greenberg Traurig, LLP

Cybersecurity Federalism: Privacy and Cybersecurity at the State and Municipal Level
Level 201, Room 309
- David Husband, Senior Attorney, Board of Governors of the Federal Reserve System
- Kelsey Finch, Policy Counsel, Future of Privacy Forum
- Emily Shaw, Monitoring and Evaluation Officer, GovEx, Johns Hopkins University

Anonymous Trust, Blockchain Models for Consumer Identity, Security and Privacy
Level 201, Room 310
- Steve Shillingford, CEO, Anonyome Labs
- Robert Hackett, Senior Writer, Fortune Magazine

Legislative Changes to the California Consumer Privacy Act and a Federal Pre-emption: How to Become Involved in the Process
Level 202, Room 302
- Natasha Kohne, Partner, Akin Gump
- Justin Brookman, Director, Consumer Privacy and Technology Policy
- Greg Guice, Senior Counsel, Akin Gump Strauss Hauer & Feld

Canadian Privacy Law for Global Companies: What You Need to Know
Level 201, Room 403
- Karen Eltis, Professor of Law, University of Ottawa
- Julie Himo, Partner, Norton Rose Fulbright (Montreal)
- Chantal Bernier, Counsel, Dentons (Ottawa)
- Nancy Cleman, Partner, Lapointe Rosenstein Marchand Melançon LLP (Montreal)

本報告之智慧財產權歸屬於財團法人資訊工業策進會

continued

Session 3 Thurs, Oct 4 11:30 AM – 12:30 PM (continued)

Effective Risk Management: Engaging the C-Suite
Level 201, Room 405
- L. Elise Dieterich, Information Security & Privacy Counsel, Kutak Rock LLP
- Craig Howser, Executive Vice President, ProQuest
- John Verry, Managing Partner, Pivot Point Security

Lunch
Thurs, Oct 4 1:30 PM – 2:30 PM
Grand Ballroom

Keynote (Plenary)
Thurs, Oct 4 1:30 PM – 2:30 PM
Grand Ballroom

Big Data, Big Responsibilities: The Data Challenges Inherent in GDPR Implementation, from a Big Data Scientist's Perspective
- **Jeff Jonas**, CEO and Founder, Senzing Inc.

Session 4
Thurs, Oct 4 2:30 PM – 3:30 PM

Best Practices for Using and Securing Connected Vehicle Data: What Are They Now and What Should They Be?
Level 201, Room 301
- Steven M. Wernikoff, Partner, Co-Leader, Autonomous Vehicle Practice, Honigman
- Peder Magee, Senior Staff Attorney, Federal Trade Commission
- Chris Murphy, Lead Counsel, Cybersecurity and Privacy & Chief Privacy Officer, General Motors
- Dana Sade, Senior Attorney, National Highway Traffic Safety Administration

Digital Health Privacy: FTC and OCR Perspectives
Level 201, Room 302
- Reece Hirsch, Partner, Morgan Lewis & Bockius LLP
- Cora Han, Senior Attorney, Federal Trade Commission
- Linda Sanches, Senior Advisor, Health Information Privacy at U.S. Dept. of Health & Human Services

Privacy+Security Forum 2018 Wed Oct 3 – Fri Oct 5 Washington, DC

continued
Session 4, Thurs, Oct 4, 2:30 PM – 3:30 PM (continued)

Privacy Impact Assessment: The Most Powerful Tool in Your Privacy Program Toolbox
Level 201, Room 307
- Jocelyn Aqua, Principal PwC
- Justin Antonipillai, Founder & CEO, WireWheel
- Alyssa Senzel, Deputy General Counsel, Blackboard
- Kim Shur, Vice President, Assistant General Counsel, Marriott

Managing Consent Headaches in the EU: Best Practices in Obtaining GDPR-Compliant Consent
Level 201, Room 308
- Michelle Perez, Head of Privacy, Samsung Electronics America Inc.
- Aruna Sharma, Assistant General Counsel, Turner Broadcasting System, Inc.
- Amanda Witt, Partner, Kilpatrick Townsend & Stockton LLP

How Can a US Company Comply with GDPR in Germany? What Should My EU Representative/DPO Be Doing for Me?
Level 201, Room 309
- Amy Carlson, Of Counsel, Stoel Rives LLP
- Volker Wodianka, Partner, SKW Schwarz
- Mahmood Sher-Jan, CEO, RADAR Inc.

Don't Acquire Your Next Breach: Assessing Cyber Security Before, During and After the Transaction
Level 201, Room 310
- Steve Bergman, General Manager Risk and Cybersecurity Practice, RSA
- Evan Wolff, Partner and Co-Chair of the Privacy and Cybersecurity Practice Group, Crowell & Moring

Korean Privacy Law Post-GDPR and Pre-Adequacy
Level 201, Room 311
- Juhyun Park, Kim & Chang
- Gail Crawford, Partner, Latham and Watkins (London)
- Michael H. Rubin, Partner, Latham & Watkins LLP

Power to the Consumer: The Reality of Managing Individual Rights Under the GDPR
Level 201, Room 407
- K Royal, Sr. Privacy Consultant, TrustArc
- Maggie Gloeckle, VP, Privacy Compliance, A + E Networks

Ice Cream Break
Thurs, Oct 4 3:30 PM – 4:00 PM
Grand Ballroom

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Session 5
Thurs, Oct 4 4:00 PM – 5:00 PM

Drafting Privacy Policies – US-Style and European-Style
Level 201, Room 301
- Niko Härting, Partner, HÄRTING (Berlin)
- David Keating, Partner, Alston & Bird
- Kimberly Wong, Senior Counsel, Data & Technology Practice Group, McDonald's Corporation

The GDPR's First Four Months: What Happened and What is Next?
Level 201, Room 302
- Lothar Determann, Partner, Baker & McKenzie
- Ellen Grant, Corporate Counsel, Thermo Fisher Scientific
- Anne-Kathrin Kroemer, Senior Director, Legal, Rubrik Inc.
- Paul Schwartz, Professor, Berkeley Law School

Carpenter v. US and What that Might Mean for Future National Security Surveillance
Level 201, Room 307
- April Falcon Doss, Partner, Saul Ewing Arnstein & Lehr LLP
- Matthew Tait, Adjunct Professor, University of Texas at Austin School of Law
- Laura Donohue, Professor and Director of the Center on National Security and the Law, Georgetown Law, and Director of the Center on Privacy & Technology
- Justin Danilewitz, Partner, Saul Ewing Arnstein & Lehr LLP

Data Privacy Issues Across the Digital Ad Ecosystem
Level 201, Room 308
- Matt Savare, Partner, Lowenstein Sandler LLP
- Michael Hahn, General Counsel, IAB
- Daniel Shore, Privacy Counsel, Conversant LLC
- Travis Davis, Counsel, Hearst
- Anjali Shenoy Dahiya, Senior Director, Deputy Counsel & Privacy, AppNexus

Managing Risk for the Internet of Things
Level 201, Room 309
- Katie Boeckl, Privacy Risk Strategist, National Institute of Standards and Technology (NIST)
- Naomi Lefkovitz, Senior Privacy Policy Advisor, NIST
- Katerina Megas, Program Manager, Cybersecurity for IoT Program, NIST

Beyond Breach Insurance: What's Next with Cyber Extortion, Cyber Business Interruption, Data Destruction, Supply Chain Issues and Other Systemic Risks?
Level 201, Room 310
- Marcello Antonucci, TMB E&O Claims Focus Group Leader, Beazley
- Dave Wong, Managing Director, Mandiant
- Troy Harris, Sr. Director, National Leader, Business Continuity Planning, RSM US LLP
- Tobias Gebhardt, Corporate Underwriter/Loss Engineer for Cyber Security Issues, Munich Re

continued
Session 5, Thurs, Oct 4, 4:00 PM – 5:00 PM continued

Cyber Extortion: Doing Business with Crooks
Level 201, Room 403
- Bart W. Huffman, Partner, Reed Smith LLP
- Elizabeth Cookson, Senior Cyber Investigator, Kivu Consulting Inc.
- Sheraun P. Howard, FBI

Privacy and Security by Design in the IoT
Level 201, Room 405
- Randy Sabett, Special Counsel, Cooley
- Aarti Soni, Cyber Coverage Leader, Marsh
- Kristin M. Grimes, Corporate Counsel, Leidos

Reception
Thurs, Oct 4 5:00 PM – 6:00 PM
Grand Ballroom

Forum Day 2 – Friday, October 5, 2018

Session 6
8:50 AM – 9:50 AM

Chinese Cybersecurity Law
Level 201, Room 301
- Edward McNicholas, Partner, Sidley Austin LLP
- Hugo Teufel III, Chief Privacy Counsel, Raytheon Company

The ePrivacy Regulation: The Next EU Frontier
Level 201, Room 302
- D. Reed Freeman Jr., Partner and Co-Chair, Cybersecurity and Privacy Practice Group, WilmerHale
- João Rodrigues, Legal Adviser, European Parliament
- Willem Debeuckelaere, President, Belgian Data Protection Authority, and Deputy Chair, European Data Protection Board

Global Enforcement Update 2018
Level 201, Room 307
- Andrew Serwin, Partner, Morrison & Foerster LLP
- Ann Henry, Partner Commercial Litigation, Pinsent Masons (Ireland)

continued

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Session 6, 8:50 AM – 9:50 AM (continued)

A Next Tidal Wave of U.S. Privacy Law?
The California Consumer Privacy Act and What's to Come
Level 201, Room 308
- Anwesa Paul, Chief Privacy Counsel, American Express
- Michael Nonaka, Partner, Covington & Burling LLP
- Ryan Smyth, Senior Principal, Promontory

New Developments in Data Breach Response and Liability
Level 201, Room 309
- Jeffrey Schultz, Partner and Co-Chair, Privacy and Data Security, Armstrong Teasdale LLP
- Neil Chilson, Senior Research Fellow for Technology and Innovation, Charles Koch Institute

Cybersecurity – Board Oversight and Emerging Trends
Level 201, Room 310
- Phyllis Sumner, Partner and Chief Privacy Officer, King & Spalding LLP
- Sean Joyce, Principal, US Cybersecurity & Privacy Practice Leader, Americas Cybersecurity & Privacy Leader, and a member of PwC's Global Cyber Strategy Team, PwC
- Richard Walker, Partner, King & Spalding LLP
- Matthew H. Baughman, Office of the Deputy Attorney General, Associate Deputy Attorney General

Is Cyber Product Liability the Next Big Litigation Wave?
Level 201, Room 311
- Brian Finch, Partner, Pillsbury Winthrop Shaw Pittman LLP
- Katherine Gronberg, Vice President of Global Public Policy andGovernment Affairs, ForeScout Technologies, Inc
- Christopher Porter, Chief Intelligence Officer, FireEye Inc

The New Wave of Cybersecurity Regulations: NYDFS and Beyond
Level 201, Room 403
- Kim Peretti, Partner, Alston & Bird, Co-Lead Cybersecurity Preparedness and Response
- Joel Lutz, Chief Privacy Officer, Lincoln Financial Group
- Erez Liebermann, Chief Counsel, Cybersecurity & Privacy; Vice President and Senior Counsel, Regulatory Law, Prudential Financial Inc.

Break
Fri, Oct 5 9:50 AM – 10:10 AM
Grand Ballroom

Session 7
Fri, Oct 5 10:10 AM – 11:10 AM

Cybersecurity Risk Assessment: The Roles of Legal and IT
Level 201, Room 301
- Robin Campbell, Partner, Co-Chair, Data Privacy & Cybersecurity, Squire Patton Boggs
- Tony Scott, Senior Advisor (Former CIO, U.S. Government) Squire Patton Boggs
- Michelle Beistle, Counsel and Chief Compliance Officer, Privacy and Ethics, Unisys
- Mathew Newfield, Chief Information Security Officer, Unisys
- Mike Tibodeau, Data Protection Operations Manager, Cisco

Reconciling the Importance of Data Sharing and Individual Privacy Concerns under HIPAA and GDPR
Level 201, Room 302
- Deborah L. Gersh, Partner, Ropes & Gray LLP
- Marc Berger, Sr. VP and General Counsel, Verana Health
- Andrew Kopelman, IP Counsel and Chief Privacy Officer, Medidata

EU E-Commerce Reforms: The Impact on Privacy and Beyond
Level 201, Room 307
- Kai Westerwelle, Partner, Bird & Bird
- Alfredo Della Monica, VP & Senior Counsel, U.S. Privacy, American Express
- Rob Corbet, Partner, Head of Technology & Innovation, Arthur Cox
- Dr. Anna Zeiter, Chief Privacy Officer, eBay Inc. (Switzerland)

The "Alternative Data" Market: Strategies for Buying and Selling Data on the Marketplace
Level 201, Room 308
- Heather Sussman, Partner, Ropes & Gray LLP
- Kelsey Finch, Policy Counsel, Future of Privacy Forum
- Peter Lefkowitz, Chief Privacy & Digital Risk Officer, Citrix
- Mark Eichorn, Assistant Director, DPIP, FTC

Current and Future HHS Initiatives in Health Privacy
Level 201, Room 309
- Adam Greene, Partner, Davis Wright Tremaine LLP
- Roger Severino, Director, Office for Civil Rights, U.S. Department of Health and Human Services

Vendor Privacy Diligence and Negotiation
Level 201, Room 310
- Michael Hamilton, Senior Corporate Counsel, Privacy, Salesforce
- Ami Patel, Chief Legal Officer, Sharecare Inc.
- Dan Guggenheim, Deputy General Counsel, Hill Physicians Medical Group/PriMed Management Consulting
- Bret Cohen, Partner, Hogan Lovells
- Gerard Stegmaier, Partner, Reed Smith
- Matthew Karlyn, Partner, Foley & Lardner LLP

本報告之智慧財產權歸屬於財團法人資訊工業策進會

continued
Session 7, Fri, Oct 5, 10:10 AM – 11:10 AM (continued)

How Will the GDPR Affect the Application and Development of Artificial Intelligence?
Level 201, Room 403
- Nancy Libin, Co-Chair, Privacy & Security + Technology Practice, Davis Wright Tremaine
- Neil Chilson, Senior Research Fellow for Technology and Innovation, Charles Koch Institute
- Jules Polonetsky, CEO, Future of Privacy Forum

Navigating Incident Response in a Rapidly Changing World
Level 201, Room 405
- Seth P. Berman, Partner, Nutter McClennen & Fish LLP
- Eric Friedberg, Co-President, Stroz Friedberg
- Chuck Brooks, Principal Growth Strategist in Cybersecurity and Emerging Technologies, General Dynamics Mission Systems

Break
Fri, Oct 5 11:10 AM – 11:30 AM
Grand Ballroom

Session 8
Fri, Oct 5 11:30 AM – 12:30 PM

Government Hacking and Vulnerability Disclosures
Level 201, Room 301
- Eric Wenger, Director, Cybersecurity & Privacy Policy, Cisco
- Angela McKay, Director, Cybersecurity Policy and Strategy, Microsoft
- Ari Schwartz, Managing Director, Cybersecurity Services & Policy, Venable
- Harley Geiger, Director, Public Policy, Rapid7

The Data Protection Officer in the EU
Level 201, Room 302
- Gonca Gökgöz-Dhont, Managing Director, DPO Network Europe
- Dr. Anna Zeiter, Chief Privacy Officer, eBay Inc. (Switzerland)

Trust: How to Overcome Blockchain Privacy and Security Challenges
Level 201, Room 307
- Marsali Hancock, President and CEO, EP3 Foundation
- Cristina Cardenas, General Coordinator, @prende.mx
- Sandra Elliott, Chief Education Officer EP3 Foundation
- Gözde Erbaz, Cybersecurity Expert | President & Founder of Cyberrobin.com and Robincode.org
- Adewale O Omoniyi, Senior Managing Consultant, IBM GBS Cybersecurity and Blockchain Services

continued

Session 8, Fri, Oct 5, 11:30 AM – 12:30 PM (continued)

What to Do if Both Inside and Outside HIPAA? Managing Compliance Complexities
Level 201, Room 308
- Ann Waldo, Principal, Waldo Law Offices PLLC
- Iliana Peters, Shareholder, Polsinelli, former Deputy Director and Senior Advisor for HIPAA Compliance and Enforcement, HHS Office for Civil Rights

Preventing the Next Digital Black Swan: The DPO, The CISO, & The C-Suite
Level 201, Room 309
- Jeffrey Welgan, Executive Director and Head of Executive Training Programs, CyberVista
- Tony Urbanovich, President, Cyber Insight

Data Ethics: Building a Practicable Methodology for Responsible Data Processing
Level 201, Room 310
- H. Leigh Feldman, Managing Director, Privacy & Data Protection, Promontory Financial Group
- Nicolas Economou, CEO, H5; co-Chair, Law Committee, IEEE Global Initiative
- Ben Zevenbergen, Visiting Specialist, Princeton University's Center for Information Technology Policy
- Yoomi Lee, Head of Enterprise Data Partnership Strategy, American Express

Initiating Outreach to Patients: What Privacy Risks Loom?
Level 201, Room 403
- Nancy Perkins, Counsel, Arnold & Porter Kaye Scholer
- Cora Tung Han, Senior Attorney, Division of Privacy & Identity Protection, FTC
- Adam Peltzman, Director, BCBS Legal Department Cooperative, Senior Associate General Counsel, Legal & Governance, Blue Cross Blue Shield Association

Privacy in Security Research: How to Answer Your Engineer's Question, "How Do We Code for Data Minimization and Other Privacy Requirements?"
Level 201, Room 405
- Lourdes Turrecha, Senior Privacy Counsel, Palo Alto Networks
- Jason Cronk, Privacy and Trust Consultant, Enterprivacy Consulting Group
- Luk Arbuckle, Chief Methodologist at Privacy Analytics

Lunch
Fri, Oct 5 1:30 PM – 2:30 PM
Grand Ballroom

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Keynote (Plenary)
Fri, Oct 5 1:30 PM – 2:30 PM
Grand Ballroom

The US and EU: Areas of Convergence, Areas of Divergence?
- **Rebecca Kelly Slaughter**, Commissioner, Federal Trade Commission
- **Willem Debeuckelaere**, President Belgian Data Protection Authority
Deputy Chair, European Data Protection Board

Session 9
Fri, Oct 5 2:30 PM – 3:30 PM

Data Profiling and Augmentation
Level 201, Room 301
- Jennifer Archie, Partner, Latham & Watkins
- Gail Crawford, Partner, Latham & Watkins (London)
- Alice Lincoln, Vice President, Data Policy & Governance, MediaMath

Integrating Risk Assessment into Privacy Breach Investigations for Health Care
Level 201, Room 302
- Keith Cheresko, Principal, Privacy Associates International LLC
- Cheryl Canfield, Privacy Officer, Roswell Park Comprehensive Cancer Center
- Doris Patrick, Manager Cybersecurity & Privacy Advisory Practice, Ernst & Young LLC

Smart Cities and the Internet of Things
Level 201, Room 307
- Ami Rodrigues, Privacy and Cybersecurity Counsel, The Coca-Cola Company
- Michelle Ramsden, Attorney-Advisor, U.S. Department of Justice, Office of Privacy & Civil Liberties
- Julie C. Grundman, Senior Associate, Kilpatrick Townsend & Stockton LLP

Practical Third-Party Information Security Risk Management: More Than Questionnaires, Less Than Full-Blown Audits
Level 201, Room 308
- Soleil Dolce, Vice President, Technologies Risk Management, Wells Fargo
- Sarah E. Statz, Vice President, Senior Information Security Counsel, American Express
- Cody Wamsley, Cybersecurity & Privacy Attorney, Dorsey & Whitney LLP

Customer Data Platforms (CDP): Technological, Legal, and Ethical Issues of Managing Massive Marketing Data Sets
Level 201, Room 309
- Andy Dale, General Counsel & VP Global Privacy, SessionM
- Pedro Pavón, Managing Counsel, Oracle
- Mark Kahn, Head of Legal, Segment.io, Inc.

continued

Session 9, Fri, Oct 5 2:30 PM – 3:30 PM (continued)

Data and Privacy in the Autonomous Car: What New Questions Might We Face?
Level 201, Room 310
- Tim Tobin, Partner, Hogan Lovells
- Lauren Smith, Policy Counsel, Future of Privacy Forum
- Michael Dolan, CISO, Element Fleet Management
- David Schwietert, Executive Vice President, Federal Government Relations & Public Policy, Alliance of Automobile Manufacturers

Ice Cream Break
Fri, Oct 5 3:30 PM – 4:00 PM
Grand Ballroom

Conference Ends
Fri, Oct 5 4:00 PM

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件四 日本出國報告

出國報告（出國類別：考察）

研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制計畫

出國報告

姓名職稱；宋佩珊 組長

派赴國家：日本

出國期間：107 年 11 月 11 日至 15 日

報告日期：107 年 11 月

本報告之智慧財產權歸屬於財團法人資訊工業策進會

一、目的

為執行「研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制」案，研議國家通訊傳播產業資料加值及個人資料隱私保護相關之法制規範或相關政策等議題，須了解以資料為基礎之科技應用發展與趨勢，以研議我國未來可行之政策與推動措施參考，故擬訂本次行程，於 107 年 11 月 11 日起赴日本東京，進行為期 5 天之考察。

本次考察行程安排參加 Gartner 於東京舉辦的研討會與 IT 應用展示（SYMPOSIUM/ITXPO），該研討會之內容包含未來的關鍵科技趨勢與策略，可作為我國相關政策之參考。

二、效益

近年來，提倡「開放資料」之風氣在國際上日益蓬勃，已成為許多國家發展之重點戰略，希望透過巨量資料等新興之技術，將資料附加之價值最大化，造就以資料為基礎之資料經濟。根據全球知名的管理諮詢公司——艾森哲（Accenture）估計，預計全球的資料經濟產值將在 2020 年時成長至 24.6 兆美元，約占全球 GDP 的 25%，並且持續看漲。而我國也自 2012 年開始推動資料開放，並在 2015 年起，連續兩年在世界開放資料指標單位「開放知識基金會」（Open Knowledge Foundation）所編纂的「開放資料指標」（Open Data Index）中，資料開放程度排名世界第一，政府開放資料已有一定程度之成果。此一開放資料之風潮，不僅只於政府之資料，「科技、媒體及通訊」（Technology, Media, Telecom，簡稱 TMT）產業作為數位經濟發展的基礎，其資料之開放，也在數位經濟發展中扮演重要之角色。通訊傳播產業一般來說保有大量資料，若能妥善加值，其蘊藏之價值將會對相關科技之發展、商業模式之突破有相當大的助益。本次赴日參加 Gartner 所舉辦的研討會，不只可了解以資料經濟為基礎之科技趨勢，同時也能就重點科

本報告之智慧財產權歸屬於財團法人資訊工業策進會

技進行深入的探討，對於我國未來通傳產業資料加值應用的實務運作，能有更清楚的架構跟研析方向。

三、研習內容

(一)2019 年的 10 項科技趨勢

此次研討會特別針對 2019 年的 10 項科技趨勢進行介紹，簡略概述如下：

1. 自動化物品（Autonomous Things）

自動化物品從形式上可區分為機器人、車輛、無人機、家電與媒介平台，這些自動化物品將涵蓋路、海、空與數位領域，但是依據其技術的核心內容又可區分為三個不同的層次，包括性能、協作與智慧。

其中性能的強度由弱到強，分為人類協助者、部份自動化、有條件的自動化、高度自動化與全自動化。而協作的部份，由弱至強則分為隔離性質、具有獨立性、可連線的與共同運作。最後在智慧化的部份，由弱至強分為靜態的、半智慧化與動態的、獨立智慧化與動態的以及透過多工智慧化模式的動態蜂巢式互動。

2. 人工智慧（Artificial Intelligence, AI）導向的發展

依據 Gartner 的專家報告，預估到了 2022 年，至少有 40%的新應用發展計畫會納入人工智慧，來進行合作開發的任務。目前人工智慧分為四種型態，分別是人工智慧服務、人工智慧平台、人工智慧架構、人工智慧基礎建設。人工智慧服務包含了影像處理、語言處理、對話、知識服務、顧客型態等;人工智慧平台則主要為機器學習,諸如 Amazon、Microsoft、Google 與 IBM 都有進行研發;人工智慧架構則是以協助開發程式為主,諸如 Google 的 TensorFlow、Facebook 的 Torch 等，都屬於此種類型；而人工智慧基礎

本報告之智慧財產權歸屬於財團法人資訊工業策進會

則重點在於去伺服器化的開發，例如 AWS Lambda、IBM 的雲端功能、Google 的雲端平台以及 Microsoft 的 Azure AI。

3. 數位雙胞胎（Digital Twin）

數位雙胞胎意指物件或系統的多元軟體模型，借助感測器來理解標的物件或系統的真實處境，讓使用者能精準快速地反應各種變動情況，從而改善物件或系統的的操作，或增添其附加價值[320]。數位雙胞胎的核心功能在於模式建立、資料蒐集、監控、分析與模擬，這些功能建立在資產資料、運作資料、控制的基礎上，尤其對於製造業的影響甚大。

4. 加強的邊際運算（Empowered Edge）

儲存、運算及進階的人工智慧與分析能力，將會在 2028 以前增進邊際運算設備的能力。另外，Gartner 的專家也指出，當邊際運算設備與 5G 這樣的基礎網路設施結合後，未來 5-6 年之間將創造出更快的速度、更少的遲延與更大的密集度，有利於邊際運算設備的發展。

5. 實境體驗（Immersive Experience）

實境體驗將會促進互動模式的改變，並且加強系統對人類，人類對系統的學習與適應能力。尤其可用在訓練與模擬、行銷、零售、虛擬設計、工作場合等，目前的智慧音箱也是實境體驗的一種模式。未來虛擬體驗的開發將不限於視覺，甚至包含聽覺、味覺、觸覺與冷熱感等。

6. 區塊鏈（Blockchain）

專家預估到了 2030 年，區塊鏈技術可創造 3.1 兆的商業利益。區塊練主要有兩個主要能力，一是區塊鏈帳本，另一則是選擇性的特色。

---

[320]「妙用 Digital Twin 加速驅動智慧轉型」，DigiTimes，2017.09.06. available at https://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&cat2=10&id=0000510929_m19llbtk1778a9lkqa178 (last visited Nov. 17, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

區塊鏈帳本的功能在於分享數位資產、加密化與分散式、不可改變及可追溯的紀錄以及去中心化的運作機制。而選擇性的特色在於智能合約、中央式管理、控管存取與更新、替代的共識機制。目前區塊鏈技術主要應用在貨物運送、電子健康紀錄、數位貨幣與不受限制的交易市場等。

7. 智慧空間（Smart Spaces）

智慧空間可以是實體或數位的環境，主要在於促進人機在互動、智能、自動化的科技上的結合。智慧空間的模式主要有四個階段，第一階段為獨立的無互聯的系統，侷限於團隊的共用；第二階段則是連結的系統，適合部門內部使用；第三階段則為共同運作的系統，具有半人工智慧的特點，適合組織內部使用；第四階段為人工智慧環境，是一個開放、互聯、共同合作、人工智慧的環境，適合生態系統模式。智慧空間未來對於連結工廠與數位供應鏈有很大的幫助，甚至可擴大為智慧城市模式。

8. 數位倫理與隱私（Digital Ethics and Privacy）

有鑑於未來將有上億的端點在蒐集資料，包括識別個人（臉部辨識、語音辨識、DNA、虹膜、指紋）、個人位置（GPS、行動電話追蹤、授權的多功能盤測儀、IP 位置、建築物保全）、個人行為（活動、心律、睡眠、血壓、血糖、行車偏好）及個人想法（搜尋引擎、社群網站、超級 cookies、智慧麥克風、電子郵件）。

與會專家認為，在數位倫理的議題下，應該從法遵導向轉為倫理導向，並據此做出對的決定並且創造價值。這樣的轉變分為內部導向與外部導向。內部導向包含了追求你的價值與創造特殊性，其中價值包含了自我詢問這是否是對的事情？如果這樣的事情可行與被允許，但是是否是我們所想要的？另外在特殊性的部份則是數位倫理是否為價值主張的一部分？這是否可使自身有特殊性？外部導向的部份，則在於減輕風險與法遵的部

本報告之智慧財產權歸屬於財團法人資訊工業策進會

份。風險的部份在於是否有聲譽上的風險？或是所創造的產品或服務會傷害其他人？而法遵的部份則在於自身是否違反了相關法規？

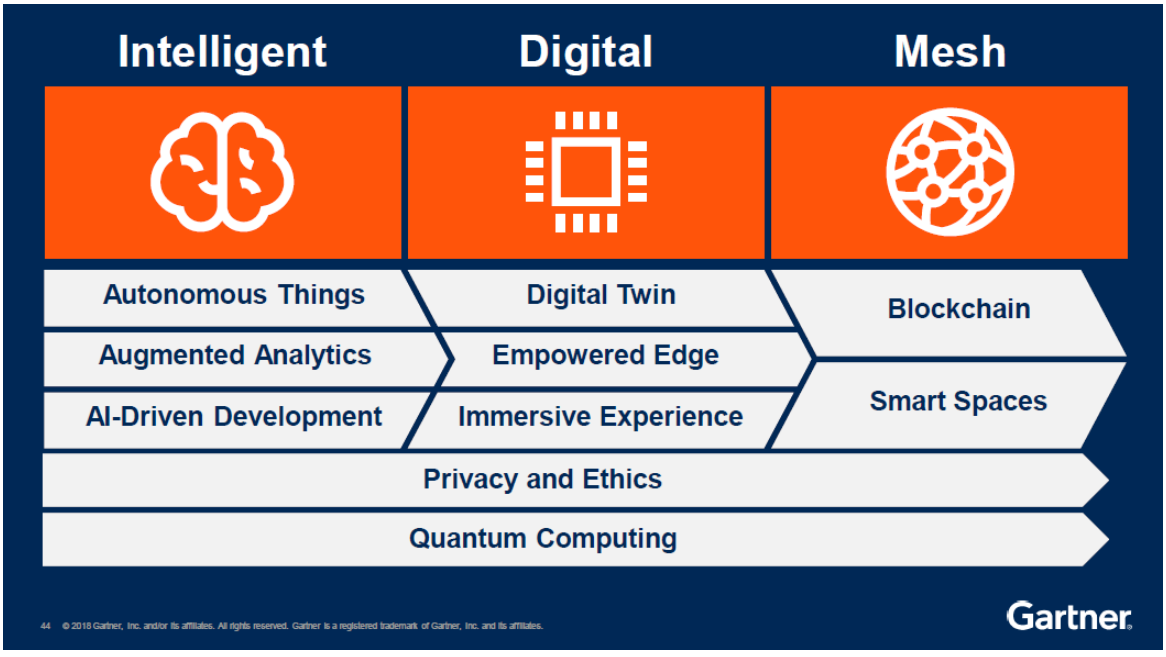
9. 量子運算（Quantum Computing）

量子運算是一種非典型的運算型態，能夠大量增加運算能力，主要目前運用的案例在於優化問題、材料科學、化學、個人化醫療以及生技。

10. 秒速間找到同時發生之資料的不知名連結（Finding Unknown Correlations for Crop Yield-In Seconds）

透過人工智慧、資料聚集與操作，從大量資料中擷取到所需要的資料來進行分析，以色列的 SparkBeyond 公司即以此技術為主要產品與服務。

這十項科技趨勢的分類與關聯主要如下圖所示：



(二)2019 年十大基礎架構與營運（I&O）趨勢與技術衝擊

2019 年與基礎架構與營運相關的趨勢與技術衝擊，包含無伺服器的運算、人工智慧衝擊、資料中心的終結、網絡的敏捷度、邊際運算、數位多

本報告之智慧財產權歸屬於財團法人資訊工業策進會

元化的管理、基礎架構與營運的新角色、SaaS 技術的抵制、人才管理成為核心任務與全球化基礎建設之可行性。

其中在人工智慧的部分，根據每日新聞調查，121 個接受調查的日本公司中，有一半已經推出或計劃進行將人工智會導入他們的一些操作中。

三菱電機集團和麒麟控股將開始使用人工智慧進行研究，計畫將經驗豐富的員工的商業知識作為學習對象，未來人工智慧可能會負責複製精密光學零件的技能和任務，或是用於掌握啤酒釀造工藝。另外，人工智慧最主要的影響在於工作機會的減少，以日本為例，主要保險提供商表示，人工智慧可以取代數十名員工的工作，日本三井物產（Mitsui＆Co。）表示，人工智慧有削減少數人的工作的效果。許多接受調查的公司沒有表是人工智慧的引入是否會導致員工人數減少。但是有兩家公司透過人工智慧的導入，提出了減少人工負荷的具體數據。大日本印刷公司導入人工智慧後，相關用來檢查打印缺陷和其他任務得以移轉到人工智慧系統上，相關的員工人力大約減少 20 名員工，因此讓公司人力資源盈餘。日本保險公司 Fukoku Mutual Life Insurance 導入 IBM 的 Watson Explorer AI，因而多出 34 名員工的員額，員工勞力被機器取代即將成為未來趨勢。

(三)管理人工智慧的風險

依據 Gartner 的調查，人工智慧未來會成為重要核心技術的原因在於促進能力、顧客體驗、因自動化所省下的成本等。然而，針對人工智慧的挑戰調查，其中占最高比例的疑慮在於資安與個資保護的議題上。

從資訊技術組織的層面切入，人工智慧可能會透過以下方式損害企業系統：

- 缺乏可稽核性：黑盒算法使企業無法追踪或解釋為什麼人工智慧應

本報告之智慧財產權歸屬於財團法人資訊工業策進會

用的結果。

- 管理不善：人為疏忽導致對客戶或其他人的傷害。
- 不可預測性：人工智慧應用程序被編程或進行學習和適應環境後，在開始後以不可預見的方式發生變化，產生有害影響。
- 互動：不同的人工智慧應用程式進行互動並改變彼此的編程，而帶來有害後果。

從企業的觀點來看，人工智慧可能會透過以下方式損害企業品牌或其他資產：

- 不倫理的活動：人工智慧應用程序的編程沒有符合人類的目標和社會規範。
- 技術依賴：人工智慧應用程序的故障影響商業營運。
- 從環境的觀點來看，可能從外部的因素造成損害：
- 經濟影響：由於自動化取代高科技人力，因此將造成大規模失業。
- 監控：可以不斷調整對策的人工智慧應用程序，可收集有關個人和公司的資訊。
- 惡意人工智慧：可以對應用程序進行編程以執行破壞性操作，例如，發動永久性網絡攻擊的程式。
- 超級智慧：人工智慧應用程序達到人類智慧和自治水平，此將使人工智慧無法受到控制。

基本上 Gartner 提供的人工智慧風險對策包括投資控制措施以管控風險、進行保險以轉移風險與選擇接受風險。專家特別將風險管理視為支持人工智慧創新的關鍵要求。允許接受風險是一個合法的商業決策，但是只

本報告之智慧財產權歸屬於財團法人資訊工業策進會

有在做出理性決定時才能接受風險。另外，利用相對成本和風險緩解的可預測性來平衡風險，同時也要在評估中考慮風險規模。

(四)人工智慧與倫理議題

人工智慧出現後，相關的倫理議題陸續出現，包括失業、不平等、人性、人工智慧故障、偏見、安全、不可預測的結果以及控制等問題。與會專家提出了人工智慧應該被思考的治理原則，分述如後。

1. 機器學習悖論

人工智慧學習的最佳狀態，是使用現實世界的資料去創造有彈性的模式，但是這個前提是建立在這個彈性是在現實世界中所需要的功能。

2. 準確性困境

先進的學習科技應該會產生更準確的結果，但是如果過程不透明，所產生的結果也會難以解釋。

3. 接受的難題

人工智慧只有在了解或運算出人類想法時才會被接受，但是這樣的結果可能是充滿與吊詭的。

Gartner 專家建議，可以在資訊治理、分析治理與人工智慧治理帶入不同的要素。在資訊治理的層次，建立信認識最重要的，而在分析治理的層次，則是信賴加上透明度，至於在人工智慧的層次，則是信賴、透明度加上多樣性。

我們目前並非在人工智慧的時代，而是處在學習的時代，一個新興數位的社會。相較於設定許多的原則，訂定自我的人工智慧倫理較為實際，尤其是將數位倫理運作立於設計的基礎。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

四、心得及建議

綜整此次參與研討會之心得，人工智慧是目前國際上最關心的議題，其也牽涉相當多的法律爭議。近年人工智慧（Artificial Intelligence, AI）領域再次引領潮流，近期最引人注目的新聞即是 2016 年 3 月，人腦與人工智慧的世紀圍棋大戰，最後由 Google 旗下 Deep Mind 公司所打造的人工智慧系統「AlphaGo」，在連續三次的圍棋對奕中擊敗南韓天才棋手李世乭[321]。此次的對戰再次讓全世界感受到目前人工智慧技術進步程度驚人，然而同時間也引起各界熱烈討論人工智慧未來可能對人類社會造成何種影響。

目前人工智慧並無單一特定的定義[322]，不過一般而言，人工智慧被認為是受到人類神經系統、身體感知、學習、推理以及行動能力等所啟發的電腦技術與科學[323]。近年人工智慧發展快速，各界再度正視人工智慧領域的發展與相關議題。世界經濟論壇（World Economic Forum）將人工智慧稱之為「第四次工業革命」（The Fourth Industrial Revolution）[324]；英國政府認為人工智慧技術對英國的影響，將是自從瓦特發明蒸汽機並由英國帶起世界第一次工業革命以來，下一個有機會讓人類生活脫胎換骨的技術[325]；日

---

321 *Artificial intelligence: Google's AlphaGo beats Go master Lee Se-dol*, BBC NEWS, Mar. 12, 2016, http://www.bbc.com/news/technology-35785875 (last visited Nov. 17, 2018).

322 EXECUTIVE OFFICE OF THE PRESIDENT NATIONAL SCIENCE AND TECHNOLOGY COUNCIL COMMITTEE ON TECHNOLOGY, *Preparing for the Future of Artificial Intelligence* 6 (2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (last visited Nov. 17, 2018).

323 Peter Stone, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg, Shivaram Kalyanakrishnan, Ece Kamar, Sarit Kraus, Kevin Leyton-Brown, David Parkes, William Press, AnnaLee Saxenian, Julie Shah, Milind Tambe, and Astro Teller, STANFORD UNIVERSITY, "*Artificial Intelligence and Life in 2030*." *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel* 4 (2016), https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf (last visited Jan. 21, 2017).

324 Klaus Schwab, WORLD ECONOMIC FORUM [WEF], *The Fourth Industrial Revolution: what it means, how to respond* (2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (last visited Nov. 17, 2018).

325 GOVERNMENT OFFICE FOR SCIENCE, *Artificial intelligence: opportunities and implications for the future of decision making* 2 (2016),

本報告之智慧財產權歸屬於財團法人資訊工業策進會

本政府在 2016 年 6 月 2 日正式提出「日本再興戰略 2016」，將人工智慧視為日本能否跟上第四次工業革命的關鍵技術之一[326]；美國政府同樣強調未來人工智慧所扮演的角色，認為人工智慧將持續促進經濟發展，並成為改善醫療、交通、環境、司法以及經濟等多領域的重要工具[327]。

人工智慧技術發展的同時，對於人類生活的改變以及可能帶來的影響也有非常多的討論。近期以來，日本、美國、英國及歐盟等官方或智庫相繼做出與人工智慧相關的研究報告，包括日本總務省在 2016 年 6 月 20 日發表了《人工智慧網路檢討會議報告書》（AI ネットワーク化検討会議報告書 2016）[328]；美國白宮在 2016 年 10 月發布了《為人工智慧的未來做好準備》（Preparing For The Future of Artificial Intelligence）[329]，緊接在 2016 年 12 月白宮再度發表報告《人工智慧，自動化以及經濟》（Artificial Intelligent, Automation, and The Economy）[330]；英國「商業、創新暨技能部」（Department for Business, Innovation and Skills）底下的「政府科學辦公室」（Government Office for Science）則在 2016 年 11 月發表《人工智慧：未來決策過程的機會與影響》（Artificial intelligence: opportunities and implications for the future

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf (last visited Nov. 17, 2018).

[326] 首相官邸，〈日本再興戦略 2016-第 4 次産業革命に向けて-〉，頁 2（2016），http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/2016_zentaihombun.pdf （最後瀏覽日：2018/11/17）。

[327] Ed Felten and Terah Lyons, *The Administration's Report on the Future of Artificial Intelligence*, (Oct. 12, 2016, 6:02 a.m.), The White House Blog, https://obamawhitehouse.archives.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence (last visited Nov. 17, 2018).

[328] 総務省情報通信政策研究所，〈AI ネットワーク化検討会議 報告書 2016 の公表〉(2016)，http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000050.html （最後瀏覽日：2018/11/17）

[329] 前揭註 322。

[330] EXECUTIVE OFFICE OF THE PRESIDENT NATIONAL SCIENCE AND TECHNOLOGY COUNCIL COMMITTEE ON TECHNOLOGY, *Artificial Intelligence, Automation, and the Economy* (2016), https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF (last visited Nov. 17, 2018).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

of decision making）[331]；歐盟議會智庫（European Parliament Think Tank）同樣在 2016 年 10 月公佈一份人工智慧議題的簡報（Briefing），名為《人工智慧：潛在益處與倫理思考》（Artificial Intelligence: Potential Benefits and Ethical Considerations）[332]。

上述這些報告中提出到許多相類或相關的法律與政策討論，足見人工智慧技術發及其應用領域皆帶來許多值得深思的議題，包括最基本但也是最根本的資料保護與隱私討論，此外人工智慧更多討論的是發展過程以及應用層面的倫理議題，以及人工智慧應用帶來的社會經濟等領域的改變[333]。

人工智慧相關應用目前看來加強了「個人行為側寫」效果，歐盟最新施行的 GDPR 相關指引文件針對「側寫」有一系列的說明，其中包括說明側寫必須由以下三個要素組成：

- 它必須是一種自動化的處理形式；
- 必須對個人資料進行處理；
- 分析的目標必須是評估關於自然人的私人面向。

從廣義上講，分析意味著收集有關個人（或個人群體）的訊息並評估他們的特徵或行為模式，以便將他們置於某個類別或小組，特別是分析和/或預測，例如，資料主體的：

- 執行任務的能力；
- 喜好；

[331] 前揭註 325。.

[332] Francesca Rossi, EUROPEAN PARLIAMENT THINK TANK, *Artificial Intelligence: Potential Benefits and Ethical Considerations* (2016), http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf (last visited Nov. 17, 2018).

[333] 陳譽文，人工智慧規範性議題綜觀，頁 44，第 29 卷第 4 期，科技法律透析，2017 年 4 月。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

- 可能的行為[334]。

依據 GDPR 第 22 條之規定，資料主體有權拒絕這樣自動化決策系統所產生的側寫[335]。

有關側寫的行為在我個人資料保護法中並未明文規定。但透過第 2 條第 1 項第 5 款有關利用之規定[336]，似可將側寫視為個人資料的利用，因此只要符合個人資料保護法第 16 條前段[337]或第 20 條前段[338]之規定，亦即在

[334] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p.6-7, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, (last visited Nov. 6. 2018)

[335] 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

[336] 個人資料保護法第 2 條：「本法用詞，定義如下：一、個人資料：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。二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。三、蒐集：指以任何方式取得個人資料。四、處理：指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。五、利用：指將蒐集之個人資料為處理以外之使用。六、國際傳輸：指將個人資料作跨國（境）之處理或利用。七、公務機關：指依法行使公權力之中央或地方機關或行政法人。八、非公務機關：指前款以外之自然人、法人或其他團體。九、當事人：指個人資料之本人。」

[337] 個人資料保護法第 16 條前段：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。」

[338] 個人資料保護法第 20 條前段：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。」

本報告之智慧財產權歸屬於財團法人資訊工業策進會

特定目的範圍內的利用即屬合法。然而，人工智慧龐大的運算與資料處理能力，可能遠超過現行特地目的的想像範圍，舉例來說一個資料主體願意透過會員卡折扣的優惠，提供本身的基本資料與消費模式，日後此等的資料將用來作為會員消費喜好的判斷基礎，也就是以「行銷」為目的。然而，透過人工智慧來處理相關的資訊，即有可能側寫出資料主體本身的性格特徵、心理狀況等資訊，再行堆疊出可行的行銷模式。

這些透過人工智慧相關應用所得到的資訊，雖然最終所得之資料還是符合特定目的的涵攝範圍，然而在人工智慧之演算過程中所產生的側寫資料，是否也符合我國特定目的的範圍，確有值得商榷之處，也是未來續行研析的重點之一。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

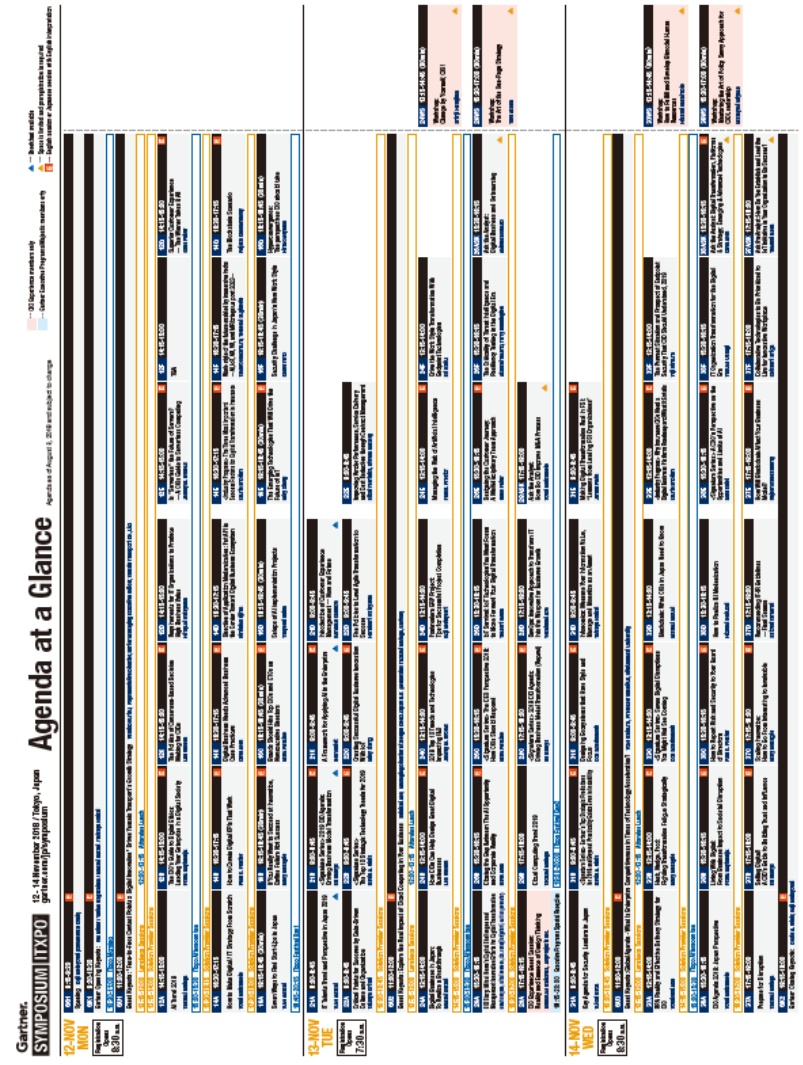
五、附錄

(一)行程表

時間	行程內容
11 月 11 日（日）	臺北至東京
11 月 12 日（一） -11 月 14 日（四）	參加 Gartner 於東京舉辦的研討會與 IT 應用展示（SYMPOSIUM/ITXPO）
11 月 15 日（四）	東京至臺北航程

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(二)研討會議程



本報告之智慧財產權歸屬於財團法人資訊工業策進會

(三)攜回資料（PDF 電子檔）

25. Explore the Real Impact of Cloud Computing in Your Business　Shinichi Abe, Managing Director at Google Cloud Japan G.K (Moderator: Tadaaki Mataga, Gartner)
26. What Is Enterprise Competitiveness in Times of Technology Acceleration?　Yoko Ishikura, Professor Emeritus, Hitotsubashi University
27. Tadaaki Mataga-AI Trend 2019
28. Frank Buytendijk-The CIO's Guide to Digital Ethics: Leading Your Enterprise in a Digital Society
29. Lee Weldon-The Politics of Consensus-Based Decision Making for CIOs
30. Hiroyuki Katayama-Requirements for IT Organizations to Produce High Business Value
31. Jeffrey M. Brooks-Is "Serverless" the Future of Servers?−A CIOs Guide to Serverless Computing
32. Gene Phifer-Superior Customer Experience−The Winner Takes It All
33. Yusuke Uesugi-IT Organization Transformation for the Digital Era
34. Yoshi Matsumoto-How to Make Digital / IT Strategy From Scratch
35. Paul E. Proctor-How to Create Digital KPIs That Work
36. Dave Aron-Digital Business Needs Advanced Business Case Practices
37. Kimihiko Iijima-Direction of Application Modernization: Put API in the Center Toward Digital Business Ecosystem
38. Laurie Shotton-<Industry Program> The Three Most Important Success Factors for Digital Transformation in Insurance
39. Takuro Nakamura, Tomoaki Sugimoto-Work-style of the future enabled by immersive techs ～AI, IoT, AR, VR, and MR brings us post 2023～
40. Rajesh Kandaswamy-The Blockchain Scenario
41. Yuko Adachi-Seven Ways to Find Start-Ups in Japan
42. Mary Mesaglio-If You Really Want to Succeed at Innovation, Dene Failure Not

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Success

43. Mark Raskino-Boards Should Hire Top CIOs and CTOs as Nonexecutive Directors
44. Tsuyoshi Ebina-Setups of AI implementation Projects
45. Milly Xiang-The Emerging Technologies That Will Drive the Future of IoT
46. Kaoru Yano-Security Challenge in Japan's New Work Style
47. Hiroko Aoyama-Hyperconvergence: The perspectives CIO should take
48. Tatsuya Ichishi-Critical Points for Success by Data-Driven Culture and Organization
49. David A. Willis-The Top 10 Strategic Technology Trends for 2019
50. Milly Xiang-Creating Successful Digital Business Innovation With IoT
51. Harutoshi Katayama-Five Policies to Lead Agile Transformation to Success
52. Eiichi Yoshihira, Steven Buckley-Improving Vendor Performance, Service Delivery and Cost Reduction through Contract Management
53. Masaki Suzuki-Digital Business in Japan: To Realize a Breakthrough
54. Lee Weldon-How CIOs Can Help Design Great DigitalBusinesses
55. Jeffrey M. Brooks-2019 Top 10 Trends and Technologies Impacting I&O
56. Koji Motoyoshi-Postmodern ERP Project: Tips for Successful Project Completion
57. Paul E. Proctor-Managing the Risk of Articial Intelligence
58. Eri Hariu-Drive the Work Style Transformation With Endpoint Technologies
59. Dave Aron-Closing the Gap Between The AI Opportunity and Corporate Reality
60. Mark Raskino-The CEO Perspective 2018: How CIOs Should Respond
61. Takeshi Ikeda-IoT Survival: IoT Technologies You Must Focus to Move Forward Your Digital Transformation
62. Gene Phifer-Designing the Customer Journey: A Multidisciplinary Team Approach
63. Atsushi Takano, Terry Bebbington-The Criticality of Threat Intelligence and Resiliency Testing in the Digital Era
64. Tadaaki Mataga-Cloud Computing Trend 2019
65. Yoshifumi Abe-DevOps: Innovative Approach to Transform IT Into the Weapon for

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Business Growth

66. Shunsuke Ishikawa, AnyProjects Inc.-CIO Experience Guest Session:Reality and Essence of Design Thinking
67. Yoshifumi Abe-RPA Reality and Effective Delivery Strategy for CIO
68. David A. Willis-Gartner's Top Strategic Predictions for 2018 and Beyond: Practicality Exists Even in Instability
69. Don Scheibenreif-Designing Ecosystems that Have Style and Focus
70. Tatsuya Ichishi-Infonomics: Measure Your Information Value,Manage and Monetize as an Asset
71. James Plath-Making Digital Transformation Real in FSI:"Lessons from Leading FSI Organizations"
72. Yuichi Isoda-Key Agenda for Security Leaders in Japan
73. Mary Mesaglio-Hack, Nudge, Prod: Fighting Transformation Fatigue Strategically
74. Masaki Suzuki-Blockchain: What CIOs in Japan Need to Know
75. Katsushi Shiga-Collaborative Technologies to Be Prioritized to Use for Innovative Workplace
76. Yoshi Matsumoto-CIO Agenda 2019: Japan Perspective
77. Frank Buytendijk-Living With Digital:From Business Impact to Societal Disruption
78. Paul E. Proctor-How to Report Risk and Security to Your Board of Directors
79. Hideaki Horiuchi-How to Realize BI Modenization
80. Tadaaki Mataga-Prepare for Disruption
81. Ed Gabrys-Selling Digital! A CIO's Guide to Building Trust and In-uence
82. Mary Mesaglio-Scaling Innovation: How to Go From Interesting to Invaluable
83. Satoshi Yamanoi-Recommending IT-IR Guidelines
84. Rajesh Kandaswamy-How Will Blockchain Affect Your Business Model?
85. Yoji Kimura-The Present Situation and Prospect of Endpoint Security That CIO Should Understand, 2019

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件五 歐盟執委會版 ePrivacy Regulation 草案中譯版

布魯塞爾，2017 年 1 月 10 日
COM （2017） 10 最終
2017/0003 （COD）

歐洲議會與理事會

關於在電子通訊領域尊重私人生活與保護個人資料，及廢止 2002/58/EC 指令 （隱私與電子通訊規則）之規則草案

（歐洲經濟區相關正文）

{SWD （2017） 3 最終}
{SWD （2017） 4 最終}
{SWD （2017） 5 最終}
{SWD （2017） 6 最終}

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2017/0003 （COD）

歐洲議會與理事會

關於在電子通訊領域尊重私人生活與保護個人資料，及廢止 2002/58/EC 指令 （隱私與電子通訊規則）之規則草案

（本文適用於歐洲經濟區）

歐洲議會與歐盟理事會，根據

歐盟運作條約，特別是其第 16 與 114 條，
歐盟執委會的草案，
經傳送該立法草案給各成員國議會後，根據
歐洲經濟與社會委員會[339]的意見，
歐洲區域委員會[340]的意見[2]，
已考慮歐洲資料保護監管者[341]的意見，
依據通常立法程序辦理，
茲因：

（1）歐盟基本權利憲章（下稱「憲章」）第 7 條保護每個人有關尊重其私人與家庭生活、住家與通訊的基本權利。尊重每個人的通訊隱私，是本權利的重要要素。電子通訊的保密，是為了確保當事人間所交換的資訊，及該通訊的外部元素（包括資訊傳送時間及來源與去處等）不致洩露給涉入通訊當事人以外的任何其他人。保密原則應適用於現在與未來的通訊工具，包括呼叫、網際網路接入、即時通訊應用、電子郵件、網際網路電話與社交媒體所提供的個人訊息等。

（2）電子通訊的內容會洩露與該通訊有關的自然人之高度敏感資訊，其範圍從個人經驗與情緒到醫療狀況、性傾向與政治觀點；洩露該資訊會造成個人與社會的傷害、經濟損失或難堪。同樣地，電子通訊所衍生的詮釋資料也會洩露非常敏感與個人的資訊。這些詮釋資料包括，當個人進行呼叫時，被呼叫的號碼、訪問的網站、地理位置、時間、日期及持續期間等，以致能對與該通訊有關的人員之私人生活作出準確的結論(例如其社會關係、其習慣與日常生活活動，其興趣、品味等)。

339 OJ C , , p. .
340 OJ C , , p. .
341 OJ C , , p. .

本報告之智慧財產權歸屬於財團法人資訊工業策進會

（3）電子通訊資料也會洩露有關法人的資訊，例如商業秘密或其他具有經濟價值的敏感資訊。因此，本規則的條文應同時適用於自然人與法人。另外，本規則也應確保歐洲議會與理事會[342]的（EU） 2016/679 規則亦適用於法人的最終使用者。這包括（EU） 2016/679 規則中對同意的定義。當*（按：本規則）*提及最終使用者（包括法人）之同意時應適用本定義*（按：（EU） 2016/679 規則中之定義）*。另外，法人就有關監管機關方面，與自然人最終使用者具有相同權利；同時，本規則中的監管機關亦應負責監督本規則有關法人的適用。

（4）依據該憲章第 8 條第 1 項及歐盟運作條約第 16 條第 1 項，每個人都享有保護其個人資料的權利。（EU） 2016/679 規則制定有關個人資料處理時保護自然人的規定，以及有關個人資料自由流通的規定。*（按：本規則）*電子通訊資料得包括（EU） 2016/679 規則所定義的個人資料。

（5）本規則的條文，就有關個人資料的電子通訊資料方面，闡明與補充了（EU） 2016/679 規則所制定的個人資料保護一般原則。因此，本規則並不降低自然人在（EU） 2016/679 規則項下所享有的保護程度。電子通訊服務提供者的電子通訊資料處理應只能在本規則所允許的狀況下為之。

（6）歐洲議會與理事會[343]2002/58/EC 指令的原則與主要條文就一般而言仍屬健全，但該指令並未完全跟上科技演變與市場現實的腳步，以及不符合或不足以有效保護電子通訊中隱私與祕密。這些進展包括一些從消費者角度已能取代傳統服務的電子通訊服務進入了市場，但這些服務不一定需要*（按：與傳統服務）*符合同一套規定。另一項進展是能追蹤最終使用者線上行為的新技術，這是 2002/58/EC 指令所未涵蓋的。因此 2002/58/EC 指令應被廢止並以本規則取代之。

（7）應允許各成員國在本規則範圍內維持或制定內國規範，進一步指定與闡明本規則的規定之適用，以確保這些規定的有效適用與解釋。是故，各成員國在此範圍內，應為了在私人生活、個人資料保護與電子通訊自由流通兩者間的平衡而為裁量。

（8）本規則應適用於電子通訊服務提供者、公眾可近用之目錄提供者，以及允許電子通訊之軟體提供者（包括在網際網路上搜索與提供資訊者）。本規則亦適用於利用電子通訊服務、傳送直接行銷商業通訊或

[342] 歐洲議會與理事會 2016 年 4 月 27 日關於處理個人資料的自然人保護及該資料的自由流通，及廢止 95/46/EC 指令 (一般資料保護規則)的(EU) 2016/679 規則 (OJ L 119, 4.5.2016, p. 1–88)。

[343] 歐洲議會與理事會 2002 年 7 月 12 日關於電子通訊業處理個人資料與保護隱私的 2002/58/EC 指令 (隱私與電子通訊指令) (OJ L 201, 31.7.2002, p.37)。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

蒐集最終使用者終端設備相關或該終端設備所儲存資訊的自然人與法人。

（9）本規則亦適用於在歐盟境內提供與使用電子通訊服務中所處理的電子通訊資料（不論該處理是否在歐盟境內進行）。另外，為不使歐盟境內最終使用者喪失其有效保護，本規則亦應適用於歐盟境外提供給歐盟境內最終使用者的電子通訊服務中所處理的電子通訊資料。

（10）投放在歐盟內部市場的無線設備及其軟體，必須遵循歐洲議會與理事會[344]的 2014/53/EU 指令。2014/53/EU 指令所要求的任何適用性，或歐盟執委會依據 2014/53/EU 指令所制定之授權法（包含要求特定類別或等級的無線設備含有保護措施、確保最終使用者的個人資料與隱私受到保護的權力），均不受本規則影響。

（11）使用於通訊的服務及其傳遞的技術手段皆已有相當大的進展。越來越多的最終使用者偏愛以功能類似的線上服務，如網路電話、訊息服務以及網路電子郵件等，以取代傳統的語音電話、文字訊息（SMS）、及電子郵件傳送服務。為確保最終使用者使用功能上類似的服務時，受到有效與同樣的保護，本規則使用「歐洲議會與理事會制定歐洲電子通訊法之指令[345]」中對電子通訊服務的定義。該定義不僅包含網際網路接入服務、全部或部分傳送訊號的服務，也包含人際通訊服務，而後者不一定是以號碼為基礎（例如網路電話、訊息服務與網路電子郵件服務）。對附屬於其他服務的人際通訊服務而言，通訊祕密的保護也是相當重要的；因此具有通訊功能的這類服務應被包含在本規則中。

（12）越來越多的聯網裝置與機器，會透過電子通訊網路互相通訊（即物聯網）。機器對機器通訊的傳送，涉及透過網路的訊息轉換，並因此，通常構成電子通訊服務。為確保通訊隱私與祕密的權利能有充分的保護，並且推動數位單一市場中被信賴與安全的物聯網，有必要闡明本規則應適用於機器對機器通訊的傳送。因此，本規則所規範的祕密原則，亦應適用於機器對機器通訊的傳送。特定保護也可在產業別法律項下制定，例如 2014/53/EU 指令。

（13）快速與有效的無線技術發展促進了公眾在公共和辦私人空間透過無線網路接取向公眾提供之網路的可用性（例如在城市、百貨公司、購物中心與醫院等不同地方的「熱點」）。若該通訊網路是提供給不特

344 歐洲議會與理事會 2014 年 4 月 16 日關於各成員國適用無線設備市場的法律調合及廢止 1999/5/EC 指令的 2014/53/EUC 指令 (OJ L 153, 22.5.2014, p. 62)

345 歐洲議會與理事會制定歐洲電子通訊法指令(修改)的歐盟執委會草案 (COM/2016/0590 最終 - 2016/0288 (COD))。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

定最終使用者的群體時，在此範圍內，透過該網路所傳送的通訊，其祕密應受到保護。無線電子通訊服務可能附屬於其他服務的事實，不應妨礙通訊祕密的確保以及本規則的適用。因此，本規則應適用於使用電子通訊服務以及公共通訊網路中的電子通訊資料。相反地，本規則不適用於封閉的最終使用者群體（例如公司網路，其接入者只限於該公司成員）。

（14）電子通訊資料應以充分寬廣及技術中立的方式定義，使其能涵蓋所有關於傳送或交換內容（電子通訊內容）的資訊，以及所有因為傳送、分發或啟用電子通訊內容交換之目的而處理之電子通訊服務最終使用者資訊（包括追蹤與識別通訊來源與去處的資料、通訊的地理位置與日期、時間、持續期間與種類）。不論該訊號與相關資料是透過有線、無線、光纖、或電磁方式所傳送者（包括衛星網路、有線網路、固定（線路與封包交換，含網際網路）與移動地面網路、電纜系統等）有關該訊號的資料都應視為電子通訊詮釋資料，並因此應受本規則條文的約束。若訂購服務相關的資訊是為了傳輸、分發或交換電子通訊內容而進行處理的，則電子通訊詮釋資料得包括該資訊。

（15）電子通訊資料應視為祕密。這表示對電子通訊資料傳送的任何干擾（包括透過直接人為干預或透過機器自動處理的介入）若未經通訊當事人同意，應被禁止。傳送通訊資料時應禁止攔截該資料（亦即至預定收件人收到電子通訊內容時之前）。電子通訊資料的攔截可能包含，例如：通訊當事人以外的人竊聽通話、讀取、掃描或儲存電子通訊內容或相關的詮釋資料（當其以交換通訊以外的目的取得詮釋資料時）。當第三方未經相關最終使用者同意而監視其訪問網站、訪問時間、與他人互動時，攔截也可能發生。隨著技術的演進，從事攔截的技術方法也大為增加。該方法的範圍，從安裝蒐集目標地區終端設備資料的設備（例如所謂的 IMSI （國際移動用戶識別）搜集器）到偷偷監視瀏覽習慣以建立最終使用者檔案等的程式與技術。其他的攔截例子，包括截取未加密無線網路或路由器中的載荷資料或內容資料（包括未經最終使用者同意的瀏覽習慣等）。

（16）禁止通訊的儲存，並非意圖禁止基於執行電子通訊網路傳送目的而對該資訊進行的任何自動、中途與暫時性的儲存。為確保電子通訊服務的安全與持續性而處理電子通訊資料者（包括檢查安全威脅，例如存在惡意軟體等），或為確保服務所需品質要求而處理詮釋資料者（例如延遲、跳動等）都不應被禁止。

（17）處理電子通訊資料，對企業、消費者與整體社會都有幫助。相對於 2002/58/EC 指令，本規則增加電子通訊服務提供者在基於最終使用者

本報告之智慧財產權歸屬於財團法人資訊工業策進會

同意的基礎上，處理電子通訊詮釋資料的可能性。然而，最終使用者相當重視其通訊的祕密（包括其線上活動），並且他們希望對使用電子通訊資料於傳送通訊以外目的者進行管制。因此，本規則應要求電子通訊服務提供者在處理電子通訊詮釋資料時，應取得最終使用者的同意；該詮釋資料應包括為允許與維持接入與連接至該服務所產生的裝置位置資料。但在提供電子通訊服務以外情況下所產生的位置資料，不應視為詮釋資料。電子通訊詮釋資料被電子通訊服務提供者用於商業用途的例子包括提供熱度地圖；其係利用顏色表示出現個人資料的地理圖示。為顯示特定期間特定方向的交通流量，需有一個辨識碼以在特定期間連結個人位置。若使用去識別化資料，則該辨識碼將會遺失，並且不能顯示流量。電子通訊詮釋資料的使用優點，比如：它有助於公共機關與公共運輸營運者，根據既有結構的使用與壓力，而界定在何處開發新的基礎建設。若電子通訊詮釋資料的處理方式（特別是使用新技術時），在考量該處理的性質、範圍、背景與目的後認為其可能對自然人的權利與自由帶來高風險時，則在進行該處理前，應依據（EU） 2016/679 規則第 35 條與第 36 條，進行資保護影響評估、以及與監管機構的協商（視其適用）。

（18）使用者得同意處理其詮釋資料以收到特定服務，例如防止詐欺活動的保護服務（透過即時分析使用資料、位置與顧客帳戶）。在數位經濟中，服務經常是憑金錢以外的對等物供應（例如使最終使用者曝露於廣告）。就本規則目的而言，最終使用者的同意，不論其為自然人或是法人，均與（EU） 2016/679 規則規定之資料當事人的同意有相同意義，且受其條件約束。基本寬頻接入與語言通訊服務，被視為能使個人進行通訊與參予數位經濟利益的重要服務。對處理網際網路或語音通訊使用資料所給的同意，若資料當事人沒有真正與自由的選擇，或不能無害地拒絕或撤銷同意者，將為無效。

（19）電子通訊內容屬於憲章第 7 條所保護的尊重私人與家庭生活、住家與通訊等基本權利的要素。對電子通訊內容的任何干擾，只有在明確定義的條件且具有特定目的、有防止濫用的充分保護等情況下，方得為之。本規則提供電子通訊服務提供者，經所有相關最終使用者知情同意後，處理傳輸中電子通訊資料的可能性。例如，提供者得提供涉及到掃描電子郵件的服務，以刪除預先設定的資料。由於通訊內容的敏感性，本規則所建立的假設是，該內容資料的處理將會對自然人的權利與自由帶來高風險。在處理該類資料時，電子通訊服務提供者應在處理前持續諮詢監管機關。該諮詢應依據（EU） 2016/679 規則第 36 條第 2 項與第 3 項辦理。若內容資料的處理是為提供最終使用者所

本報告之智慧財產權歸屬於財團法人資訊工業策進會

請求的服務，且該最終使用者已同意該處理，並且該處理是為該服務目的、於絕對必要與合比例的期間內所為者，則前述假設不包含之。電子通訊內容經最終使用者送出且由預定最終使用者收到後，得由最終使用者或其委託記錄或儲存該資料的第三方記錄與儲存之。該資料的任何處理必須遵循（EU） 2016/679 規則。

（20）電子通訊網路最終使用者的終端設備，及有關使用該終端設備的任何資料，不論是儲存在該設備或該設備所發送者，或為使其能連接至其他裝置或網路設備而請求或處理者，均屬於歐盟基本權利憲章與歐洲保護人權與基本自由公約規定中需要保護的最終使用者隱私範圍的一部分。由於該設備含有或處理，可能洩露個人情緒、政治、社會等綜合詳情的資訊（包括透過存取該設備的 GPS 功能、連絡名單所取得的通訊內容、圖像、個人位置等，以及已儲存在該裝置的任何其他資訊），故有關該設備的資訊，需有加強的隱私保護。另外，所謂的間諜軟體（spyware）、網蟲（web bugs）、隱藏識別碼、cookies 追蹤、及其他類似的多餘追蹤工具等，會在最終使用者不知道的情況下，進入其終端設備，以存取資訊、儲存隱藏資訊、及追蹤活動。有關最終使用者裝置的資訊，也可能透過所謂「裝置指紋」的技術，經常在最終使用者不知道的情況下，在遠端蒐集、進行識別與追蹤目的，並且可能嚴重侵入該最終使用者的隱私。偷偷監視最終使用者活動的技術，例如追蹤其線上活動或其終端設備位置，或破壞最終使用者終端設備作業等，對最終使用者的隱私有嚴重威脅。因此，對最終使用者終端設備的任何干擾，只有在最終使用者同意且基於特定與透明之目的，方得為之。

（21）為使用終端設備的處理與儲存功能，或存取終端設備所儲存的資訊，而需取得同意的義務，唯有在不涉及或只有有限度侵入隱私的情況下，方得免除。例如，為使最終使用者能夠使用其明確請求的特定服務，則就合法目的為絕對必要與合比例之技術儲存或存取，不需請求其同意授權。這可能包括：當最終使用者填寫數頁的線上表格時，於一定的期間內在網站上儲存 cookies，以便保存追蹤最終使用者的輸入。Cookies 也可以是合法與有用的工具，例如用於衡量網站的網路流量。從事配置檢查以提供符合最終使用者設定服務的資訊社會服務提供者，以及單純登入裝置但最終使用者裝置不能收到其所請求的內容者，均不構成存取裝置或使用該裝置的處理功能。

（22）為提供資訊及取得最終使用者同意所使用的方法，應儘可能對用戶友善。由於追蹤 cookies 與其他追蹤技術的普遍使用，最終使用者愈加被請同意在其終端設備儲存追蹤 cookies。因此，最終使用者因被請

本報告之智慧財產權歸屬於財團法人資訊工業策進會

求提供同意而感到負擔。使用提供同意的技術手段，例如透過透明與用戶友善的設定，可處理這問題。因此，本規則應提供、利用瀏覽器或其他應用軟體的適當設定、表示同意的可能性。最終使用者在建立其瀏覽器或其他應用軟體的一般隱私設定時所作出的選擇，應對任何第三方具約束力且可對該第三方執行。網路瀏覽器是一種應用軟體，它允許在網際網路上搜尋與呈現資訊。其他種類的應用軟體，例如允許呼叫、傳送訊息、或提供路徑指引者，也有相同的功能。網路瀏覽器可以調解最終使用者與網站間所發生的許多內容。從這角度來看，它們有特權地位，扮演主動角色來幫助最終使用者控制終端設備的進出資訊流。更特別的是，網路瀏覽器可當作守門員，因此幫助最終使用者防止其終端設備（例如智慧型手機、平板或電腦）的資訊，被存取或儲存。

（23）從設計與預設包含的資料保護的原則業已規定在（EU） 2016/679 規則第 25 條中。目前，在多數目前的瀏覽器中，cookies 的預設值被設定為「接受所有 cookies」。因此，能在網際網路上搜尋與呈現資訊的軟體提供者，有義務配置該軟體，使其能提供選項，防止第三方儲存終端設備的資訊；這通常呈現為「拒絕第三方 cookies」。最終使用者應被提供一組設定選項，範圍從較高（例如「絕不接受 cookies」），到較低（例如「永遠接受 cookis」），以及中等（例如「拒絕第三方 cookies」或「只接受第三方 cookies」）。該隱私設定應以易見與易懂的方式呈現。

（24）為使網路瀏覽器能取得（EU） 2016/679 規則所定義的最終使用者同意，例如：在儲存第三方追蹤 cookies 時，除其他事項外，需有終端設備之最終使用者明確肯定的動作，表示其有自由、有受清楚告知、且明確地同意該 cookies 對該終端設備的儲存與存取。若，例如，最終使用者在已被給予作選擇所需資訊的情況下被要求主動選擇「接受第三方 cookies」以確認其同意，則該動作應視為有效的。為達此目的，能夠接入網際網路的軟體提供者，必須告知最終使用者在各種選項中選擇隱私設定的可能性，並要求他們作出選擇。所提供的資訊不應勸阻最終使用者選擇較高的隱私設定，並且應包含有關允許第三方 cookies 儲存在電腦中的相關風險的資訊（包括編纂個人瀏覽歷史長期記錄，與使用該記錄送出目標廣告等）。網路瀏覽器宜提供簡易方法給最終使用者，使其能在使用中的任何時間變更隱私設定，並且允許該使用者排除某些網站或列於白名單網站，或指定那些網站（第三方）的 cookies 是被永遠或絕不允許。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

（25）電子通訊網路的接入，需要固定發出某些資料封包，以便能發現或保持連接到網路或網路上的其他裝置。另外，裝置必須有單一的編配地址，使其能在該網路上被識別。無線與行動電話標準，同樣涉及含有單一識別碼的主動訊號發送，例如 MAC 地址、IMEI （國際移動設備辨識碼）、IMSI 等。單一無線基地站（亦即發射站與接收站），例如無線存取點，有捕捉該資料的特定範圍。已有服務提供者藉由掃描設備相關資訊的基礎提供追蹤服務，其具有多項功能，包括計算人數、提供在線等待人數的資料、查明特定區域的人數等。該資訊可能被用於更多的侵入目的，例如當最終使用者進入商店時，發送個人化的商務訊息給該最終使用者。雖然某些功能並不具有高度隱私風險，但其他可能有高度隱私風險，例如涉及長期追蹤個人者，包括重複到訪特定位置。從事該實務的提供者應在最終使用者進入該技術作業區域特定邊界內的定義區域前，在其邊界的位置張貼顯目通知，告知最終使用者該追蹤之目的、其負責人、以及有終端設備最終使用者為減少或停止蒐集可採取的措施。若依據（EU） 2016/679 規則第 13 條蒐集個人資料時，亦應提供其他資訊。

（26）當電子通訊服務提供者對電子通訊資料的處理是屬於本規則之範圍時，本規則應提供歐盟或成員國可在特定條件下以法律限制某些義務與權利的可能性，若該限制係構成民主社會保護特定公共利益而為必要與合比例的措施者，包括：為國家安全、國防、公共安全與預防、調查、偵查或起訴犯罪、或執行刑事處罰等目的（包括防護與預防公共安全威脅）；與歐盟或成員國一般公眾利益有關的重要目的（特別是歐盟或成員國的重要經濟或金融利益）；或公務機關基於上訴目的所行使的監督、檢查或管制職能。因此，若其為保護上述公共利益而為必要與合比例、且依據歐盟基本權利憲章及歐洲保護人權及基本自由公約（依據如歐盟法院及歐洲人權法院所解釋）所為之，則本規則不應影響成員國進行合法監聽電子通訊或採取其他措施的能力。電子通訊服務提供者應提供適當程序以執行主管機關的法定請求，若相關時，亦應考量第 3 條第 3 項所規定之代表的角色。

（27）關於發話號碼，發話方保留發話號碼顯示的權利，以及收話方拒絕接受未顯示號碼來電的權利，皆必須受到保護。某些最終使用者，（特別是求助號碼，與類似組織）在保證其來電者去識別化方面擁有利益。關於連接號碼，收話方保留顯示發話方實際連接號碼的權利與法定利益，必須受到保護。

（28）在特定情況下，有正當理由時應停止遮蔽顯示發話號碼。最終使用者有關發話號碼的隱私權利，若為追蹤騷擾呼叫而有必要時應受到限

本報告之智慧財產權歸屬於財團法人資訊工業策進會

制；並且，有關發話號碼與位置資料的權利，若為緊急服務所需（例如 eCall），亦應受到限制，以便能儘可能有效的執行其任務。

（29）有技術能使電子通訊服務提供者，得以以不同的方式減少最終使用者收到不想要的呼叫（包括阻隔靜音呼叫與其他詐欺與騷擾的呼叫）。公共可用之以號碼為基礎的人際傳播服務提供者，應配置這類技術，並且應免費提供，以保護最終使用者，防止騷擾的呼叫。提供者應確保最終使用者知悉該功能的存在，例如在其網頁上公佈該事實。

（30）電子通訊服務最終使用者的公眾可近用之目錄被廣為發布。公眾可近用之目錄是指包含有最終使用者資訊，例如電話號碼（包括行動電話號碼）、電子郵件地址連絡資料等的任何目錄或服務，並且包括查詢服務。基於自然人隱私及個人資保護的權利，要求在將其個人資料納入目錄前，先取得自然人最終使用者的同意。基於法人的法定利益，則規定該法人最終使用者有權拒絕將其相關資料被納入名錄中。

（31）若自然人的最終使用者同意將其資料納入該目錄時，他們在同意的基礎上應能夠決定那些類別的個人資料可被納入該名錄（例如姓名、電子郵件地址、住家地址、用戶名稱、電話號碼）。此外，公眾可近用之目錄提供者應在將其納入該目錄以前，告知最終使用者該目錄之目的及該目錄的搜尋功能。最終使用者在同意的基礎上應能夠決定其連絡資料中哪些類別的個人資料可被搜尋。納入該目錄中的個人資料類別與最終使用者連絡資料中可被搜尋的個人資料類別，不一定相同。

（32）在本規則中，直接行銷是指自然人或法人利用電子通訊服務，將直接行銷通訊直接送至一位或多位已識別或可識別的最終使用者的任何形式的廣告。除提供商業目的之產品與服務外，也包括政黨所傳送的訊息，其透過電子通訊服務連絡自然人以推廣其政黨。其他非營利組織傳送支持該組織宗旨的訊息亦同。

（33）應提供防護以確保最終使用者不受以直接行銷為目的、侵入最終使用者私人生活的未經請求通訊。不論是使用自動呼叫與通訊系統、即時通訊（IM）應用軟體、電子郵件、簡訊（SMS）、多媒體簡訊（MMS）、藍芽等方式，其隱私侵入與騷擾的程度，被視為相對類似的，且與用於進行該些電子通訊的各種技術與通路無關。因此，有正當理由要求在傳送直接行銷目的商務電子通訊給最終使用者前，先取得該最終使用者的同意，以便保護個人使其私人生活免受侵入之權利，及保護法人的合法利益。由於法律明確性的需要及確保防止未經請求的電子通

本報告之智慧財產權歸屬於財團法人資訊工業策進會

訊之規定的需要，定義單一一套不會因因傳送這些未請求的通訊所使用的技術而有不同，並同時保證整個歐盟的所有公民都有等同的保護水準的規定，仍有不過時的合理性。然而，在既有客戶關係中提供類似產品或服務的條件下，仍可合理的允許使用電子郵件連絡資料。該可能性只適用於已依據（EU） 2016/679 規則取得電子連絡資料的同一公司。

（34）當最終使用者已同意收到未經請求的直接行銷目的通訊時，他們仍可在任何時間以簡易的方式撤銷其同意。為使歐盟關於未經請求的直接行銷訊息的規定能更有效地執行，有必要禁止在傳送直接行銷目的之未經請求商業通訊時，掩蔽身份、使用虛假身份及虛假回覆地址或號碼。因此，未經請求的行銷通訊應可被清楚辨認其性質，並且提供傳送該通訊或代為傳送該通訊的法人或自然人身份，以及提供其他必要資訊給收受人,使其能行使其反對再收到書面與/或口頭行銷訊息的權利。

（35）為使同意能被簡易地撤銷，透過電子郵件進行直接行銷通訊的法人或自然人應呈現連結或有效的電子郵件地址，使最終使用者能輕易利用以撤銷其同意。透過語音對語音之呼叫或透過自動呼叫與通訊系統呼叫，進行直接行銷通訊的法人或自然人，應顯示顯示其身份線路，以供回撥該公司之用；或呈現特定編碼，以識別該呼叫為行銷呼叫的事實。

（36）語音對語音之直接行銷呼叫未涉及自動呼叫與通訊系統的使用，因為耗費傳送方相當大的成本，且不會使最終使用者負擔財務成本。因此各成員國應能夠建立與/或維持其國內系統,允許該呼叫送至未表示反對的最終使用者。

（37）提供電子通訊服務的服務提供者應告知最終使用者其對通訊安全可採取的措施（例如使用特定種類的軟體或加密技術）。告知最終使用者特定安全風險的要求，並不因此免除服務提供者以自己的成本採取適當與立即的措施以矯正任何新的、未預見的安全風險並恢復該服務的正常安全水準的義務。應免費提供給購買者安全風險相關的資訊。安全應依據（EU） 2016/679 規則第 32 條評估。

（38）為確保與（EU） 2016/679 規則充分的一致性，本規則條文的施行應由負責（EU） 2016/679 規則條文施行的同一機關負責；並且本規則適用（EU） 2016/679 規則的一致性機制。各成員國應能有一個以上的監管機關以反映其憲法、組織與行政架構。監管機關亦應負責監督本規則有關法人的電子通訊資料的適用。這些其他任務不應影響監管

本報告之智慧財產權歸屬於財團法人資訊工業策進會

機關在（EU） 2016/679 規則及本規則規定下保護個人資料的職能。應提供各監管機關必要的其他財務與人力資源、處所及基礎設施，使其能有效履行本規則規定下之任務。

（39）各監管機關應有資格在其本身成員國領域內行使本規則中規定之權力及履行其中任務。為確保本規則在整個歐盟的一致性監督與施行，各監管機關在各成員國應有相同的任務與有效的權力，但不影響其在成員國法律規定下之的檢察權力，亦不影響將違反本規則事件移交司法機關並參與法律程序之權。各成員國及其監管機關在適用本規則時，宜考量微型、小型與中型企業的特定需求。

（40）為加強本規則規定的施行，各監管機關應有權力對違反本規則之事件科以處罰，包括行政罰鍰，科或併科本規則中任何其他適當之處置。本規則應闡明違法事件及訂定相關行政罰鍰的上限與標準，其在各別案件中應由主管監管機關經考量違法的性質、程序與持續期間、後果、其確保符合本規則規定之義務所採措施及防止或減輕該違法後果所採取之措施等所有相關情況後決定之。就訂定本規則規定之罰鍰的目的而言，企業一詞應解讀為歐盟運作條約第 101 與 102 條所定義的企業。

（41）為達本規則的目標，亦即保護自然人的基本權利與自由，特別是保護其個人資料的權利，並確保歐盟境內個人資料的自由流通等，依該歐盟運作條約第 290 條制定法律的權力應授權給歐盟執委會以補足本規則。特別是應就有關應呈現的資訊制定授權法（包括標準化圖標的方式），以便能輕易接收並且容易瞭解到蒐集終端設備所發送資訊的概況，以及其蒐集目的、負責人、及終端設備最終使用者為減少蒐集可採取的任何措施等資訊。授權法亦必須指明識別直接行銷呼叫的規則（包括透過自動呼叫與通訊系統所為者）。由歐盟執委會進行適當的諮詢，以及依據 2016 年 4 月 13 日[346]機關間關於更佳立法的協議中所制定的原則進行該諮詢，尤為重要。特別是，為確保在草擬授權法中的公平參與，歐洲議會與理事會及成員國專家應同時收到文件，並且專家應有系統的進入歐盟執委會專家群組處理授權法草擬的會議。另外，為確保本規則執行的統一條件，當本規則有規定時，該執行權力應賦予歐盟執委會。這些權力應依據（EU） 182/2011 規則行使。

（42）由於本規則的目標（亦即確保自然人與法人的同等保護程度以及電子通訊資料在整個歐盟的自由流通等）不能由各成員國有效達成，但

[346] 歐洲議會、歐盟理事會、及歐盟執委會 2016 年 4 月 13 日機構間關於更佳立法的協議 (OJ L 123, 12.5.2016, p. 1–14)。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

所涉行為的規模或效力，可在歐盟位階達成；故歐盟得依據歐盟條約第 5 條所規定之輔助性原則採取措施。依據該條所規定的比例原則，本規則不超出為達成該目標所必須之範圍。

（43）2002/58/EC 指令應被廢止。

已通過本規則：

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第一章
一般條款

第 1 條
主旨

1. 本規則制定有關提供與使用電子通訊服務時保護自然人與法人基本權利與自由的規定，特別是關於尊重私人生活與通訊的權利，以及處理個人資料時對自然人的保護。

2. 本規則確保歐盟境內電子通訊資料與電子通訊服務的自由移動，不應因尊重自然人與法人的私人生活與通訊及處理個人資料時對自然人保護等理由，而受到限制與禁止。

3. 本規則的條文透過制定關於第 1 項與第 2 項所述目的之特定規定，闡明與補充（EU） 2016/679 規則。

第 2 條
實體適用範圍

1. 本規則適用於有關提供與使用電子通訊服務的電子通訊資料處理，以及有關最終使用者終端設備的資訊。

2. 本規則不適用於以下範圍：

(a) 歐盟法律管轄範圍外的活動；

(b) 歐盟條約第 5 篇第 2 章所述範圍內的成員國活動；

(c) 不向公眾開放的電子通訊服務；

(d) 主管機關為防止、調查或起訴刑事犯罪，或執行刑事處罰，包括保護與預防公共安全威脅等目的之活動；

3. 歐盟機構、組織、辦公室與機關所為的電子通訊資料處理，由（EU）00/0000 規則 [新規則取代 45/2001 規則]規範之。

4. 本規則不影響 2000/31/EC 指令[347]的適用，特別是該指令第 12 條至第 15 條中調解服務提供者的責任原則。

[347] 歐洲議會與理事會 2000 年 6 月 8 日關於資訊社會服務，特別是內部市場電子商務法律面的 2000/31/EC 指令（「電子商務指令」) (OJ L 178, 17.7.2000, p. 1–16)。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

5. 本規則不影響 2014/53/EU 指令的條文。

第 3 條
領域適用範圍與代表

1. 本規則適用於以下範圍：

(e) 在歐盟境內提供電子通訊服務給最終使用者者，不論最終使用者是否必須付費；

(f) 該服務的使用；

(g) 位於歐盟境內的最終使用者終端設備相關資訊的保護。

2. 若電子通訊服務提供者未在歐盟境內設立，其應書面指定其在歐盟境內的代表。

3. 該代表應設立於該電子通訊服務最終使用者所在地成員國之一。

4. 為確保遵循本規則，該代表應有權力，在其所代表的提供者之外，另外或代替其回覆問題及提供資訊；特別是就有關電子通訊資料處理的所有問題，回覆與提供給監管機關與最終使用者。

5. 針對從歐盟境外提供電子通訊服務給歐盟境內最終使用者之自然人或法人處理電子通訊資料所提出之法律訟訴，不應因第 2 項所述代表之指定，而受到影響。

第 4 條
定義

1. 就本規則目的而言，應適用下述定義：

(h) （EU） 2016/679 規則中之定義；

(i) 分別列示於「歐洲電子通訊法制定指令」第 2 條之第 1 點、第 4 點、第 5 點、第 6 點、第 7 點、第 14 點與第 21 點所規定之的「電子通訊網路」、「電子通訊服務」、「人際通訊服務」、「基於號碼的人際通訊服務」、「無關號碼的人際通訊服務」、「最終使用者」與「呼叫」等的定義。

(j) 執委會 2008/63/EC 指令[348]第 1 條第 1 點鎖定「終端設備」之定義。

2. 就第 1 項第 b 點之目的而言，「人際通訊服務」之定義應包括使人際與互動通訊僅連結至另一服務之微小輔助特性服務。

[348] 歐盟執委會 2008 年 6 月 20 日關於電信終端設備市場競爭的 2008/63/EC 指令 (OJ L 162, 21.6.2008, p. 20–26)。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

3. 另外，就本規則目的而言，應適用下述定義：

(k) 「電子通訊資料」是指電子通訊內容與電子通訊詮釋資料；

(l) 「電子通訊內容」是指透過電子通訊服務工具所交換的內容，例如本文、音訊、視訊、圖像與聲音；

(m) 「電子通訊詮釋資料」是指在電子通訊網路中所處理的資料，其目的在於傳送、分發或交換電子通訊內容；包括用於追蹤與識別通訊來源與去處的資料、在提供電子通訊服務時所產生的裝置位置、以及通訊的日期、時間、期間與種類；

(n) 「公眾可近用之目錄」是指電子通訊服務最終使用者的目錄，不論是印刷或電子格式，或其是公佈或提供給公眾或公共部分（包括透過名錄查詢服務的方式）；

(o) 「電子郵件」是指透過電子通訊網路傳送，含有本文、音訊、視訊、聲音或圖像等資訊的任何電子訊息，其可儲存在網路或相關電腦設備或其收件人終端設備中者。

(p) 「直接行銷通訊」是指任何形式的廣告，不論是書面或口頭，其係傳送至一位或多位已識別或可識別的電子通訊服務最終使用者者，包括自動呼叫、有人際互動或無人際互動的通訊系統、電子郵件、SMS*（按：簡訊服務）*等；

(q) 「直接行銷語音對語音之呼叫」是指現場呼叫，其不涉及自動呼叫系統與通訊系統的使用；

(r) 「自動呼叫與通訊系統」是指能根據系統指示自動呼叫一位或多位接聽者，並傳送非現場講話音訊的系統，包括利用自動呼叫與通訊系統的呼叫，其透過被呼叫人員轉接至個人者。

第二章
保護自然人及法人電子通訊及儲存於其終端設備之資訊

第 5 條
電子通訊資料的保密

電子通訊資料應保密。最終使用者以外任何人對電子通訊資料的任何干擾，例如電子通訊資料的聆聽、竊聽、儲存、監聽、掃描、或其他種類的攔截、監控或處理等，除本規則所允許者外，應被禁止。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第 6 條

被允許的電子通訊資料處理

1. 在下述情況下，電子通訊網路與服務提供者得處理電子通訊資料：

(s) 若為完成通訊的傳送而有必要時，於該目的之必要期間內為之；或

(t) 若為維護與恢復電子通訊網路與服務的安全，或為偵測電子通訊傳送中的技術缺失與/或錯誤，而有必要時，則於該目的之必要期間內為之。

2. 在下述情況下，電子通訊服務提供者得處理電子通訊詮釋資料：

(u) 若為符合「歐洲電子通訊法制定指令」或（EU） 2015/2120 規則[349]所定之強制性服務品質要求而有時必要時，則於該目的之必要時間內為之；或

(v) 若為記帳、計算互連款項、偵測或停止詐欺、濫用或購買電子通訊服務而有必要時；或

(w) 相關的最終使用者已同意為一個或多個特定目的處理其通訊詮釋資料（包括為提供特定服務給該最終使用者），但以該目的或相關目的不能以去識別方式處理資訊達成者為限。

3. 電子通訊服務提供者只得在下述情況下處理 電子通訊內容：

(x) 若以提供特定服務給最終使用者為唯一目的，而最終使用者或相關的最終使用者已同意處理電子通訊內容，且若未處理該內容則無法提供該服務時；

(b) 若所有相關最終使用者已同意為一個或多個特定目的處理其電子通訊內容，而該目的不能透過處理去識別化資訊達成，並且提供者已諮詢監管機關時。*（按：在此情形下，）*（EU） 2016/679 規則第 36 條第 2 點與第 3 點應適用於監管機關的諮詢。

第 7 條

儲存與刪除電子通訊資料

1. 在不影響第 6 條第 3 項第 b 點及第 6 條第 3 項第 a 點與第 b 點的情況下，電子通訊服務提供者應於預定收件人收到電子通訊內容後，

[349] 歐洲議會與理事會 2015 年 11 月 25 日關於公開網際網路接入所制定的措施，及修訂關於通用服務及用戶有關電子通訊網路及服務的權利的 2002/22/EC 指令，及關於歐盟境內公共移動通訊網路漫遊的(EU) No 531/2012 規則的(EU) 2015/2120 規則 (OJ L 310, 26.11.2015, p. 1–18)。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

刪除電子通訊內容或使該資料去識別化。該資料得由最終使用者或受其委託記錄、儲存或處理該資料之第三方，依據（EU） 2016/679規則記錄或儲存之。

2. 在不影響第 6 條第 1 項第 b 點與第 6 條第 2 項第 a 點與第 c 點的情況下，電子通訊服務提供者應在電子通訊詮釋資料不再為通訊傳送目的所需時，刪除或使其去識別化。

3. 若電子通訊詮釋資料是為第 6 條第 2 項第 b 點所規定之記帳目的而處理時，則相關詮釋資料得保存至國內法律規定可依法爭執帳單或追索款項的期間結束時止。

第 8 條

儲存在最終使用者終端設備的資訊及其相關資訊的保護

1. 相關最終使用者以外的其他人，對終端設備處理與儲存功能的使用，及最終使用者終端設備的資訊蒐集，除基於下述理由外，應被禁止：

(y) 若以透過電子通訊網路進行電子通訊傳送為唯一目的而有必要時；或

(z) 若最終使用者已同意時；

(aa) 若為提供最終使用者所請求的資訊社會服務而有必要時；或

(bb) 若為最終使用者所要求之資訊社會服務之提供者所進行之必要網路受眾測量網路訪客測量而有必要時。

2. 為連接其他裝置與/或網路設備而對終端設備所釋放的資訊進行的蒐集，除下述情況外，應被禁止：

(cc) 若其只是為必要時間內建立連接目的所進行者；或

(dd) 若已顯示清楚與明顯的通知，其內容至少包含告知該蒐集之方式、目的、負責人、以及終端設備最終使用者為停止或減少該蒐集可採取的任何措施。（若係蒐集個人資料者，亦包括（EU） 2016/679規則第 13 條所要求的其它資訊）

蒐集該資訊的前提是，已採取 （EU） 2016/679 規則第 32 條所述適當的技術與組織措施，以確保該風險相應的安全等級。

3. 依第 2 項第 b 點所提供的資訊得連同標準化圖標一併提供，以便能以易見、易懂、易讀的方式全面瞭解該蒐集。

4. 執委會有權依據第 27 條制定授權法案，訂定標準化圖標應呈現的資訊，以及提供標準化圖標的程序。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第 9 條
同意

1. 應適用（EU） 2016/679/EU 規則第 4 條第 11 項與第 7 條中對同意的定義與條件。

2. 在不影響第 1 項的情況下，若技術上可能與可行時，就第 8 條第 1 項第 b 點目的而言，該同意得利用接入網際網路的應用軟體之適當技術設定表達。

3. 對於已同意第 6 條第 2 項第 c 點及第 6 條第 3 項第 a 點與第 b 點所述之電子通訊資料處理的最終使用者，應給予機會於任何時間依（EU）2016/679 規則第 7 條第 3 項規定撤銷其同意，並且在該處理繼續進行期間，應每 6 個月定期提醒該機會。

第 10 條
應提供的隱私設定資訊與選擇

1. 在市場上提供電子通訊的軟體（包含在網路上搜索和提供訊息者），應提供選項以防止第三方在最終使用者終端設備上儲存或處理以存在資訊。

2. 經安裝後，該軟體應告知最終使用者有關該隱私設定的選項，並且在繼續安裝時，要求最終使用者同意該設定。

3. 若是在 2018 年 5 月 25 日以前已安裝的軟體，在該軟體進行第一次更新時應符合第 1 與第 2 項項下的要求（但至遲以不超過 2018 年 8 月 25 日為限）。

第 11 條
限制

1. 歐盟或成員國的法律得透過立法措施限制第 5 條至第 8 條所述之義務與權利，但該限制應尊重基本權利與自由的本質，並且應是民主社會為保護（EU） 2016/679 規則第 23 條第 1 項 a 至 e 款所述之一項或多項公共利益所必需、適當與成比例的措施，或是公務機關行使該利益的相關監督、檢查或規範功能。

2. 電子通訊服務提供者應訂定內部程序，以因應基於第 1 項所制定的立法措施，而對最終使用者電子通訊資料的近用請求。經要求後，其應提供有關該程序的資訊給監管主管機關。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第三章
自然人與法人控制電子通訊的權利

第 12 條
發話號碼與連接號碼的顯示與不顯示

1. 若依據「歐洲電子通訊法制定指令」第 107 條提供發話號碼與連接號碼的顯示時，公共可用之以號碼為基礎的人際傳播服務提供者應提供：

(ee) 發話之最終使用者應有機會，在每次呼叫、每次連線或永久性地阻止發話號碼顯示；

(ff) 收話之最終使用者應有機會阻止來電的發話號碼顯示；

(gg) 若發話號碼顯示已被發話之最終使用者阻止顯示時，收話之最終使用者應有機會拒絕來電呼叫；

(hh) 收話之最終使用者應有機會阻止將連接號碼顯示給發話之最終使用者。

2. 第 1 項第 a 點、第 b 點、第 c 點與第 d 點所述機會應以簡單及免費方式提供給最終使用者。

3. 第 1 項第 a 點亦應適用於歐盟境內發話至第三國的呼叫。第 1 項第 b 點、第 c 點與第 d 點亦適用於來自第三國的來電呼叫。

4. 若提供發話號碼與連接號碼顯示時，公共可用之以號碼為基礎的人際傳播服務提供者應提供有關第 1 項第 a 點、第 b 點、第 c 點與第 d 點所述選擇的資訊給公眾。

第 13 條
發話號碼與連接號碼的顯示與不顯示之除外事項

1. 不論發話之最終使用者是否已阻止發話號碼顯示，若呼叫緊急服務時，公共可用之以號碼為基礎的人際傳播服務提供者應停止遮蔽發話號碼顯示，並且在處理緊急通訊組織（包括公共安全回應點等）每條線路基礎上，不理會最終使用者對處理詮釋資料的拒絕或不同意，以便因應該通訊。

2. 各成員國應制定各特定之規範，規定於何者情形下最終使用者得請求追蹤惡意或騷擾呼叫，及應以何種程序請求公共可用之以號碼為基礎的人際傳播服務提供者暫時停止遮蔽發話號碼顯示。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第 14 條
來電阻隔

公共可用之以號碼為基礎的人際傳播服務提供者應以當前最佳科技措施，避免最終使用者接收不想要的呼叫，並且亦應免費提供收話之最終使用者下述機會：

(ii) 阻隔特定號碼或去識別化來源的來電呼叫；

(jj) 停止第三方至最終使用者終端設備的自動轉接。

第 15 條
公眾可近用之目錄

1. 公眾可近用之目錄提供者將自然人最終使用者個人資料納入目錄應徵求其同意，並且當這些資料與該目錄提供者認定的分類相關時，應獲得該等最終使用者之同意，以便在每個類別的個人資料中，將其資料納入。提供者應提供自然人最終使用者有關確認、改正與刪除該資料的方式。

2. 公眾可近用之目錄提供者應告知自然人最終使用者，其個人資料被納入具搜尋功能的名錄中，並且在有關其本身資料的搜尋功能啟用前，取得最終使用者的同意。

3. 公眾可近用之目錄提供者應讓法人最終使用者有機會拒絕將其相關資料納入名錄中。提供者應提供該法人最終使用者確認、改正與刪除該資料的方式。

4. 應免費提供最終使用者不被納入公眾可近用之目錄的機會，或確認、改正與刪除其相關資料的方式。

第 16 條
未經請求的通訊

1. 自然人或法人得以傳送直接行銷通訊給同意的自然人最終使用者為目的使用電子通訊服務。

2. 若自然人或法人在銷售產品或服務的情況下，依據（EU） 2016/679 規則取得其客戶電子郵件的電子連絡資料時，該自然人或法人得使用這些電子連絡資料，進行其本身類似產品或服務的直接行銷，但以客戶被清楚與明顯的給予機會得以免費與簡易方式拒絕該使用為限。該拒絕的權利，應於蒐集及每次傳送訊息時給予。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

3. 在不影響第 1 項與第 2 項的情況下，使用電子通訊服務於直接行銷電話的自然人或法人應：

(kk) 顯示其可被連絡的號碼；或

(ll) 顯示能識別該呼叫為行銷電話事實的特定編碼或字首。

4. 除第 1 項規定外，成員國得以法律規定，只有在自然人最終使用者未表示拒絕接收該通訊時，方得對自然人最終使用者所為的直接行銷語音對語音之呼叫。

5. 成員國在歐盟法及適用之國內法的架構下，應確保充分保護自然人最終使用者享有依第 1 項所述方式傳送未經請求的通訊之合法利益。

6. 使用電子通訊服務於傳送直接行銷通訊的任何自然人或法人，應告知最終使用者有關該通訊的行銷性質，以及所傳通訊所代表的法人或自然人的身份，並且應提供必要資訊，以便接收者能以簡易方式行使其撤銷同意再收到行銷通訊之權利。

7. 執委會有權依據第 26 條第 2 項規定制定執行措施，指定第 3 項第 b 項下識別行銷呼叫的編碼或字首。

第 17 條
有關偵測到之安全風險的資訊

若網路或電子通訊服務安全存在特定風險時，電子通訊服務提供者應告知最終使用者該風險；並且若該風險處於服務提供者可採措施範圍外，應告知最終使用者任何可能的補救措施，包括說明其可能涉及的成本。

第四章
獨立監管機關及執行

第 18 條
獨立監管機關

1. 負責監督（EU）2016/679 規則施行的獨立監管機關亦應負責監督本規則的施行。準用（EU） 2016/679 規則第六章與第七章。監管機關應對相關最終使用者行使其職權與權力。

2. 第 1 項所述監管機關於適當時應與依「歐洲電子通訊法制定指令」設立的國家管理機關合作。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第 19 條
歐洲資料保護委員會

依（EU） 2016/679 規則第 68 條設立的歐洲資料保護應有權確保本規則的一致施行。為此目的，歐洲資料保護委員會應行使（EU） 2016/679 規則第 70 條所述職權。該委員會亦應有下述工作：

(mm) 向歐盟執委會建議本規則的任何修訂草案；

(nn) 依據其任一成員或歐盟執委會的請求，主動審查本規則施行的任何問題，並制定準則、建議及最佳實務，以鼓勵本規則的一致適用。

第 20 條
合作與一致程序

各監管機關應致力於本規則在整個歐盟的一致適用。為此目的，各監管機關應依據（EU） 2016/679 規則第七章之規定就本規則所涵蓋事項，彼此及與歐盟執委會合作。

第五章
補償、責任與處罰

第 21 條
救濟

1. 在不影響任何其他行政或司法救濟的情況下，每位電子通訊服務最終使用者應享有（EU） 2016/679 規則第 77 條、78 條與 79 條所述相同之救濟。

2. 最終使用者以外的任何自然人或法人，其受本規則侵權負面影響，且有合法利益停止或禁止該侵權者（包括電子通訊服務提供者保護其合法商業利益者），應有權提起有關該侵權的法律程序。

第 22 條
賠償權利與責任

任何電子通訊服務最終使用者因違反本規則而遭致重大或非重大損害者，應有權獲得該違反所致損害的賠償，但違反人證明其依據（EU） 2016/679 規則第 82 條不需以任何方式負責導致該損害的事件者除外。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第 23 條
行政罰鍰的一般條件

1. 就本條目的而言，（EU） 2016/679 規則第七章應適用於違反本規則的事件。

2. 違反本規則下述規定者，應依據第 1 項，處以最高 1 千萬歐元的行政罰鍰；若為企業，則最高為其前一會計年度全球年度總營業額 2%，其中兩者以較高者為準。

(oo) 第 8 條所定處理電子通訊資料的任何法人或自然人之義務；

(pp) 第 10 條所定含電子通訊之軟體提供者之義務；

(qq) 第 15 條所定公眾可近用之目錄提供者之義務；

(rr) 第 16 條所定使用電子通訊服務的任何法人或自然人之義務。

3. 違反第 5 條、第 6 條與第 7 條所定通訊保密原則、被允許的電子通訊資料處理、刪除期限之規定者，應依據本條第 1 項，處以最高 2 千萬歐元的行政罰鍰，若為企業，最高為前一會計年度其全球年度總營業額 4%，其中兩者以較高者為準。

4. 各成員國應制定違反第 12 條、第 13 條、第 14 條與第 17 條之罰鍰原則。

5. 不遵守第 18 條所述監管機關命令者，應處以最高 2 千萬歐元的行政罰鍰，若為企業，最高為其前一會計年度全球總營業額 4%，其中兩者以較高者為準。

6. 在不影響第 18 條鎖定監管機關之矯正權力的前提下，各成員國得制定是否對該成員國境內設立的公共機關與機構處以行政罰鍰及其處罰範圍之規定。

7. 監管機關行使其在本條項下權力時，應依據歐盟及成員國法律，採取適當的程序保護，包括有效的司法救濟及正當程序。

8. 若該成員國法律體系未規定行政罰鍰，得按下述方式適用本條：由主管監管機關提出該罰鍰，並由管轄國家法院處罰之，同時，應確保該法律救濟為有效，並且與監管機關所處行政罰鍰具同一效力。在任何情況下，所處罰的罰鍰應為有效、按比率、與懲誡性的。 [xxx] 依本項所制定的法律條文，各成員國應通知歐盟執委會並且應及時告知任何後續修訂法律或影響該法律的修訂文。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第 24 條
罰則

1. 各成員國應制定適用於違反本規則的其他罰則規定，特別是不受第 23 條項下行政罰鍰約束的違法行為，並且應採取所有必要措施以確保其執行。該處罰應為有效、按比率、與懲戒性。

2. 依第 1 項所制定的法律條文，各成員國應於第 29 條第 2 項所述日期後 18 個月內通知歐盟執委會，並且應及時告知影響該條文的任何後續修訂。

第六章
授權法與施行法

第 25 條
授權的行使

1. 歐盟執委會被賦予制定授權法的權力，但應受本條所述條件約束。

2. 第 8 條第 4 項所述制定授權法的權力，應於[本規則生效日]起的不定期間內，賦予歐盟執委會。

3. 第 8 條第 4 項所述授權得由歐洲議會或理事會隨時撤銷。撤銷決定應終止該決定所述之授權。其應於歐盟公報公告該決定之次日，或公告所述日期生效。其不影響已生效的任何授權法。

4. 在通過授權法以前，歐盟執委會應依據 2016 年 4 月 13 日機關間關於更佳立法的協議中所訂立之原則，諮詢各成員國所指定的專家。

5. 一旦通過授權法，歐盟執委會應盡快同時通知歐洲議會與理事會。

6. 第 8 條第 4 項所通過的授權法，在歐洲議會或理事會在收到該法的通知後兩個月期間內未表示反對，或在該期間屆滿前歐洲議會與理事會均告知歐盟執委會其將不會反對時，方為有效。該期間得由歐洲議會或理事會提出延常 2 個月。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

第 26 條
委員會

1. 依據「歐洲電子通訊法制定指令」第 110 條設立的通訊委員會，應協助歐盟執委會。該委員會應為（EU）182/2011 規則[350]所定義的委員會。

2. 於本項情形，（EU）182/2011 規則第 5 條應適用。

第七章
最後條款

第 27 條
廢止

1. 2002/58/EC 指令自 2018 年 5 月 25 日起廢止。

2. 凡引述廢止的指令者，應解釋為引述本規則。

第 28 條
監督與評估條款

最遲在 2018 年 1 月 1 日以前，歐盟執委會應訂立監督本規則效力的詳細計劃。

在本規則施行日起 3 年內及以後每 3 年，歐盟執委會應對本規則進行評估，並且向歐洲議會、理事會、及歐洲經濟與社會委員會提出其主要發現結果。若基於法律、技術或經濟的演進，該評估應適當提出修訂或廢止本規則的法案。

第 29 條
生效與適用

1. 本規則應於歐盟公報公告日起第二十天後生效。

2. 其應於 2018 年 5 月 25 日起施行。

本規則全部具有約束力，並且直接適用於所有成員國。

350 歐洲議會與理事會 2011 年 2 月 16 日關於制定歐盟執委會各成員國行使執行權力的控制機制之規則與一般原則的(EU) No 182/20110 規則 (OJ L 55, 28.2.2011, p.13-18)。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

於布魯賽爾作成

代表歐洲議會
主席

代表理事會
主席

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件六 歐盟執委會版 ePrivacy Regulation 草案英文原文

EUROPEAN
COMMISSION

Brussels, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

(Text with EEA relevance)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2017/0003 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee[351],
Having regard to the opinion of the Committee of the Regions[352],
Having regard to the opinion of the European Data Protection Supervisor[353],
Acting in accordance with the ordinary legislative procedure,
Whereas:

(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the parties involved in a communication. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media.

(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their

351 OJ C , , p. .
352 OJ C , , p. .
353 OJ C , , p. .

本報告之智慧財產權歸屬於財團法人資訊工業策進會

social relationships, their habits and activities of everyday life, their interests, tastes etc.

(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council[354], also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.

(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data may include personal data as defined in Regulation (EU) 2016/679.

(5) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation.

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[355] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of online behaviour of end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.

(7) The Member States should be allowed, within the limits of this Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. Therefore, the margin of discretion, which Member States

[354] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

[355] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

have in this regard, should maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.

(8) This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing commercial communications or collect information related to or stored in end-users' terminal equipment.

(9) This Regulation should apply to electronic communications data processed in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union.

(10) Radio equipment and its software which is placed on the internal market in the Union, must comply with Directive 2014/53/EU of the European Parliament and of the Council[356]. This Regulation should not affect the applicability of any of the requirements of Directive 2014/53/EU nor the power of the Commission to adopt delegated acts pursuant to Directive 2014/53/EU requiring that specific categories or classes of radio equipment incorporate safeguards to ensure that personal data and privacy of end-users are protected.

(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. In order to ensure an effective and equal protection of end-users when using functionally equivalent services, this Regulation uses the definition of electronic communications services set forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code[357]]. That definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.

(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a

[356] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).

[357] Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.

(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.

(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.

(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others,

本報告之智慧財產權歸屬於財團法人資訊工業策進會

etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.

(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats such as the presence of malware or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc.

(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, based on end-users consent. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to obtain end-users' consent to process electronic communications metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.

(18) End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users

本報告之智慧財產權歸屬於財團法人資訊工業策進會

being exposed to advertisements. For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment.

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.

(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device’s GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user’s device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called ‘device fingerprinting’, often without

本報告之智慧財產權歸屬於財團法人資訊工業策進會

the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes.

(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example,

本報告之智慧財產權歸屬於財團法人資訊工業策進會

‘always accept cookies’) and intermediate (for example, ‘reject third party cookies’ or ‘only accept first party cookies’). Such privacy settings should be presented in a an easily visible and intelligible manner.

(24) For web browsers to be able to obtain end-users’ consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select ‘accept third party cookies’ to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.

(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.

(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law

本報告之智慧財產權歸屬於財團法人資訊工業策進會

certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).

(27) As regards calling line identification, it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. Certain end-users, in particular help lines, and similar organisations, have an interest in guaranteeing the anonymity of their callers. As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected.

(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. End-users' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services, such as eCall, to carry out their tasks as effectively as possible.

(29) Technology exists that enables providers of electronic communications services to limit the reception of unwanted calls by end-users in different ways, including blocking silent calls and other fraudulent and nuisance calls. Providers of publicly available number-based interpersonal communications services should deploy this technology and protect end-users against nuisance calls and free of charge. Providers should ensure that end-users are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users

本報告之智慧財產權歸屬於財團法人資訊工業策進會

that are legal entities have the right to object to the data related to them being included in a directory.

(31) If end-users that are natural persons give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories should inform the end-users of the purposes of the directory and of the search functions of the directory before including them in that directory. End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the end-user's contact details can be searched should not necessarily be the same.

(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

(33) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, emails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for all citizens throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.

(34) When end-users have provided their consent to receiving unsolicited communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person transmitting the

本報告之智慧財產權歸屬於財團法人資訊工業策進會

communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages.

(35) In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called or present a specific code identifying the fact that the call is a marketing call.

(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems only allowing such calls to end-users who have not objected.

(37) Service providers who offer electronic communications services should inform end-users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679.

(38) To ensure full consistency with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.

(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty.

(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[358]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

(42) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural and legal persons and the free flow of electronic communications data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(43) Directive 2002/58/EC should be repealed.

HAVE ADOPTED THIS REGULATION:

[358] Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ L 123, 12.5.2016, p. 1–14).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.

2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data.

3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.

Article 2
Material Scope

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.

2. This Regulation does not apply to:

(ss) activities which fall outside the scope of Union law;

(tt) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;

(uu) electronic communications services which are not publicly available;

(vv) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC[359], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

[359] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal

本報告之智慧財產權歸屬於財團法人資訊工業策進會

5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.

Article 3
Territorial scope and representative

1. This Regulation applies to:

(ww) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;

(xx) the use of such services;

(yy) the protection of information related to the terminal equipment of end-users located in the Union.

2. Where the provider of an electronic communications service is not established in the Union it shall designate in writing a representative in the Union.

3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.

4. The representative shall have the power to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from outside the Union to end-users in the Union.

Article 4
Definitions

1. For the purposes of this Regulation, following definitions shall apply:

(zz) the definitions in Regulation (EU) 2016/679;

(aaa) the definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in points (1), (4), (5), (6), (7), (14) and (21) respectively of Article 2 of [Directive establishing the European Electronic Communications Code];

(bbb) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC[360].

aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).

[360] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20–26).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2. For the purposes of point (b) of paragraph 1, the definition of 'interpersonal communications service' shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

3. In addition, for the purposes of this Regulation the following definitions shall apply:

(ccc) 'electronic communications data' means electronic communications content and electronic communications metadata;

(ddd) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;

(eee) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;

(fff) 'publicly available directory' means a directory of end-users of electronic communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service;

(ggg) 'electronic mail' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;

(hhh) 'direct marketing communications' means any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;

(iii) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems;

(jjj) 'automated calling and communication systems' means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, including calls made using automated calling and communication systems which connect the called person to an individual.

CHAPTER II
PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT

Article 5
Confidentiality of electronic communications data

Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or

本報告之智慧財產權歸屬於財團法人資訊工業策進會

processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.

Article 6
Permitted processing of electronic communications data

1. Providers of electronic communications networks and services may process electronic communications data if:

(kkk) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(lll) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

2. Providers of electronic communications services may process electronic communications metadata if:

(mmm) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120[361] for the duration necessary for that purpose; or

(nnn) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(ooo) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

3. Providers of the electronic communications services may process electronic communications content only:

(ppp) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or

(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

[361] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Article 7

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

Article 8

Protection of information stored in and related to end-users' terminal equipment

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

(qqq) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(rrr) the end-user has given his or her consent; or

(sss) it is necessary for providing an information society service requested by the end-user; or

(ttt) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.

2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

(uuu) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

(vvv) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security

本報告之智慧財產權歸屬於財團法人資訊工業策進會

appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

Article 9
Consent

1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.

2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.

3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.

Article 10
Information and options for privacy settings to be provided

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.

3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.

Article 11
Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

CHAPTER III
NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS

Article 12
Presentation and restriction of calling and connected line identification

1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of publicly available number-based interpersonal communications services shall provide the following:

(www) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis;

(xxx) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;

(yyy) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user;

(zzz) the called end-user with the possibility of preventing the presentation of the connected line identification to the calling end-user.

2. The possibilities referred to in points (a), (b), (c) and (d) of paragraph 1 shall be provided to end-users by simple means and free of charge.

3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1 shall also apply to incoming calls originating in third countries.

4. Where presentation of calling or connected line identification is offered, providers of publicly available number-based interpersonal communications services shall provide information to the public regarding the options set out in points (a), (b), (c) and (d) of paragraph 1.

Article 13
Exceptions to presentation and restriction of calling and connected line identification

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall

本報告之智慧財產權歸屬於財團法人資訊工業策進會

override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.

2. Member States shall establish more specific provisions with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of malicious or nuisance calls.

Article 14
Incoming call blocking

Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge:

(aaaa) to block incoming calls from specific numbers or from anonymous sources;

(bbbb) to stop automatic call forwarding by a third party to the end-user's terminal equipment.

Article 15
Publicly available directories

1. The providers of publicly available directories shall obtain the consent of end-users who are natural persons to include their personal data in the directory and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.

2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.

3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.

4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.

Article 16
Unsolicited communications

1. Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons that have given their consent.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.

3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:

(cccc) present the identity of a line on which they can be contacted; or

(dddd) present a specific code/or prefix identifying the fact that the call is a marketing call.

4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.

5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications.

7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.

Article 17
Information about detected security risks

In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.

CHAPTER IV
INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT

Article 18
Independent supervisory authorities

1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the

本報告之智慧財產權歸屬於財團法人資訊工業策進會

application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.

2. The supervisory authority or authorities referred to in paragraph 1 shall cooperate whenever appropriate with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code].

Article 19
European Data Protection Board

The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have competence to ensure the consistent application of this Regulation. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679. The Board shall also have the following tasks:

(eeee) advise the Commission on any proposed amendment of this Regulation;

(ffff) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation.

Article 20
Cooperation and consistency procedures

Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation.

CHAPTER V
REMEDIES, LIABILITY AND PENALTIES

Article 21
Remedies

1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679.

2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation and having a legitimate interest in the cessation or prohibition of alleged infringements, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.

Article 22
Right to compensation and liability

Any end-user of electronic communications services who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered, unless the infringer proves that it is not in any way responsible for the event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Article 23
General conditions for imposing administrative fines

1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation.

2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(gggg) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;

(hhhh) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;

(iiii) the obligations of the providers of publicly available directories pursuant to Article 15;

(jjjj) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.

3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17.

5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Article 24
Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than 18 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.

CHAPTER VI
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 25
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].

3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 26
Committee

1. The Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic

本報告之智慧財產權歸屬於財團法人資訊工業策進會

Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011[362].

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VII
FINAL PROVISIONS

Article 27
Repeal

1. Directive 2002/58/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation.

Article 28
Monitoring and evaluation clause

By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.
No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.

Article 29
Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

[362] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件七 有線電視業者蒐集用戶收視紀錄及行為等之商務模式及服務樣態隱私議題分析

一、蒐集用戶收視紀錄及行為，應認為屬於個人資料之蒐集

按《個人資料保護法》（以下簡稱個資法）第 2 條第 1 款之規定，凡能直接或間接識別個人之資料，及屬於個人資料。有線電視業者蒐集用術數收視紀錄或行為，得以透過機器之內碼或用戶之編號得知該用戶之身份，故應認為對有線電視業者而言，該資料具有識別個人之特性，屬於個資法所稱之個人資料。而蒐集該資料之行為，即屬於個資法中對個人資料之蒐集。

二、有線電視業者應依個資法規定取得蒐集之合法基礎，並踐行告知

如前述，該行為既屬對個人資料之蒐集，依據個資法第 19 條之規定，非公務機關對於個人資料之蒐集，及應有特定目的，並符合該條第 1 項各之合法條件。期中，以有線電視業者而言，最有可能取得之合法基礎應為第 2 款「與當事人有契約或類似契約之關係，且以採取適當之安全措施」或第 5 款「經當事人同意」。具體而言究竟如何取得合法性基礎，應依個別業者狀況逐一檢視。

此外，由於有線電視業者蒐集用戶收視紀錄及行為，應係透過用戶回傳之訊號或用戶使用之機器等加以蒐集，故應認為屬於所謂「直接對當事人蒐集」之行為。因此，有線電視業者應依個資法第 8 條之規定，項當事人告知其名稱、蒐集目的、個人資料類別、利用之期間、地區、對象及方式、權利行使之方式及不提供資料時之影響。

三、蒐集後利用之商務模式及服務樣態之定性，應視其蒐集時「特定目的」之範圍，以及其利用之資料是否仍屬於個人資料而定

本報告之智慧財產權歸屬於財團法人資訊工業策進會

(一)仍屬個人資料，屬於特定目的內之處理或利用

若業者利用仍具有個人資料性質之資料，於原特定目的內處理、利用，依據個資法第 19 條之規定，可以合法利用。

至於是否特定目的內之利用，應視個別業者蒐集時所告知之「特定目的」範圍以及其實暨使用之樣態而定。舉例而言，依法務部公告之「個人資料保護法之特定目的」，若業者當時所告知之特定目的為「（152）廣告或商業行為管理」或「（153）影視、音樂與媒體管理」，則業者依此而做的相關管理、利用行為，應可初步認為尚屬原蒐集時之特定目的範圍內。

(二)仍屬個人資料，屬於特定目的外之處理或利用

若業者處理、利用個人資料已經逾越其蒐集時之特定目的，則屬於特定目的外之處理、利用（個資法並未規定特定目的外之處理，目前法院實務見解認為得類推適用個資法目的外利用之規定），應有個資法第 20 條第 1 項所列之 7 款事由中之任一款，方可合法進行處理或利用。

(三)已經非屬個人資料

1. 個人資料經統計等處理，可能不再具個人資料性質

若個人資料經處理後已經無法直接或間接識別特定個人，依據個資法對個人資料定義之反面解釋，及法務部之函釋，可認為其以非屬個人資料（法務部 2014 年 11 月 17 日法律字第 10303513040 號函參照）。

舉例而言，若有線電視業者蒐集用戶之收視資料，作為收視率調查（或普查）之用，由於該調查或普查之結果，通常僅表示特定地區、年齡區段之用戶於特定時間段收看某頻道之比例，於一般情形下，此類統計性質之資料應可認為其無法直接或間接識別特定個人，故不屬於個人資料。

2. 使用已不具個人資料性質之資料，不適用個資法

將前述已不具個人資料性質之資料，再做其他處理或利用者，因非利用個人資料，沒有個資法的適用。

舉例而言，若有線電視業者將前述之收視率調查（或普查）資料做其他應用，因其非個人資料，自然無個人資料保護法之適用。

本報告之智慧財產權歸屬於財團法人資訊工業策進會

附件八 臉部辨識法制議題簡析

一、臉部辨識之特性

臉部辨識屬於所謂「生物識別技術」（biometric technology）的範疇，係利人體生理學上具有個體間獨特的特徵進行人別的區辨。由於臉部辨識所依靠的特徵點在成長過程中幾乎不會改變，因此具有「人人不同、終身不變」的特性。這與指紋辨識有相當類似的性質。

二、大法官解釋釋字 603 號對於生物識別技術的立場

大法官在釋字 603 號解釋中認為，由於指紋人各不同、終身不變得特性，具有「高度人格識別功能」，可以被視為為「得以監控個人的敏感性資訊」。因此，大法官認為若要「強制」蒐集相關資料，將侵犯人民的資訊自主權，政府機關應以「法律明定蒐集目的」，蒐集的範圍與方式應與「重大公益目的之達成」具有「必要性與關聯性」，並「禁止目的外之使用」。照樣的規定，與我國個人資料保護法相比，是更為嚴格的規定。

而由於臉部辨識技術與指紋技術在性質上相當接近，因此，大法官對於指紋的法律見解，在臉部辨識上，亦應有所適用。

三、目前我國臉部辨識資料蒐集之標準

依照我國目前的個人資料保護法規定，人體的外觀、骨骼等臉部辨識所用以識別個人的資訊，屬於個資法規定的一般個資。因此，我國公務機關與非公務機關，可以依照個人資料保護法第 15 條、第 16 條及第 19 條、第 20 條的規定，蒐集、處理及利用相關資料。然而，若政府機關有意以其強制手段大規模蒐集個人資料，則應適用司法院大法官釋字第 603 號解釋之標準，亦及其蒐集目的應以法律明定，其蒐集範圍與方式英語重大公益目的達成有必要性與關聯性，同時禁止目的外之利用。

本報告之智慧財產權歸屬於財團法人資訊工業策進會