出國報告（出國類別：開會）

出席 2018 年「APEC 跨境隱私保護規則（CBPR）體系研討會」暨「全球隱私高峰會（Global Privacy Summit）」會議報告

服務機關：國家通訊傳播委員會

姓名職稱：鄭美華科員

派赴國家：美　　國

出國期間：107 年 3 月 25 日至 30 日

報告日期：107 年 6 月 15 日

摘要

本次共參加 2018 年「APEC 跨境隱私保護規則（CBPR）體系研討會」暨「全球隱私高峰會（Global Privacy Summit）」兩場會議。前者由美國商務部舉辦，目的在擴大產業對 APEC 跨境隱私保護規則（CBPR）及其認證制度的瞭解；後者則是由國際隱私專家協會（International Association of Privacy Professionals）所舉辦的年度隱私盛會，主要就各項時下熱門的隱私議題進行意見分享與討論。

本次會議係由法律事務處鄭美華科員參加，特別感謝國家發展委員會提供本次會議報名資訊，讓本會有機會共同參與交流。本次獲得寶貴收穫包括：（一）瞭解 APEC CBPR 體系的運作，並向已加入的經濟體借鏡實務面的相關經驗；（二）瞭解 GDPR 未來的執法方向，以及其他國家的觀察重點，以協助我國企業因應 GDPR 的施行；（三）瞭解各國隱私保護主管機關對於個人資料保護的執法策略，以作為未來政策或法規研擬的參考。

目　錄

壹、前言……5

貳、行程安排與參與人員 7

一、3/26(一) APEC 跨境隱私保護規則（CBPR）體系研討會 7

二、3/27(二) 「全球隱私高峰會（Global Privacy Summit）」Day1....9

三、3/28(三) 「全球隱私高峰會（Global Privacy Summit）」Day2...12

參、研討會議題紀要 15

一、APEC 跨境隱私保護規則（CBPR）體系研討會 15

Session 1: APEC CBPR 管制者討論會議.....16

Session 2: CBPR 運作討論會議 19

Session 3: CBPR 的下一步：CBPR 對於貿易的重要性、PRP、與 GDPR 其他法律架構的架接，及公司或國家參與的提升.....20

附件：資料處理者之隱私承認（PRP）之目的與背景說明.....23

二、全球隱私高峰會（Global Privacy Summit）.....25

(一) GDPR 2.0 26

(二) GDPR：個別成員國具體執法與豁免之討論.....28

(三) 專訪法國國家資訊自由委員會主席 Isabelle Falque-Pierrotin.....32

(四) 打破 GDPR 的迷思.....36

(五) 對結果管制：有效利用胡蘿蔔與棒子 38

(六) 隱私與競爭：大數據時代的重要議題 41

(七) GDPR 與 e-privacy 對於廣告科技與歐洲互動廣告局指引的影響 ……...43

(八) 管制全球化的資料流通：來自三大洲的觀點 44

肆、心得與建議 45

壹、前言

隨著電子商務、物聯網技術的蓬勃發展，個人資料已經成為企業重要資產之一，個人資料保護法制也因此與電子商務等重要產業之發展密切相關。其中最受矚目的要屬在 2018 年 5 月 25 日正式施行的歐盟「一般性個人資料保護規則（General Data Protection Regulation，GDPR）」，其率先突破以往法律適用以內國領域為原則的地域範圍限制，將非設立於歐盟、但針對歐盟市場提供商品或服務的個人資料控制者，納入規範對象，並且將備受爭議的「被遺忘權（Right to be forgotten）」、資料可攜權，及從設計著手保護隱私的概念等等，順應網際網路與科技發展所誕生，加強個人對於其個人資料自主控制的新興權利，均明文入法，同時一舉將罰鍰金額大幅提高，因此造成許多國際企業惴惴不安。我國屬於外貿出口導向的國家，與歐盟之間並有密切的貿易往來，故有必要積極瞭解相關法規規範及其未來落實方式，以期協助降低我國企業與歐盟貿易間之障礙。

於此同時，由亞洲太平洋經濟合作會議（Asia-Pacific Economic Cooperation，APEC）」所倡議的「跨境隱私保護規則（Cross-Border Privacy Rules System，CBPRs）」，亦不容忽略。隨著新興經濟模式逐漸發展以資料驅動為基礎，APEC 也意識到資料的跨境自由流通已成為現代經濟發展的命脈，而個人資料保護則攸關消費者對於資料跨境傳輸的信心，因此對於資料自由流通之促進至關重要。我國為 APEC 的正式成員，向來積極參與 APEC 各式議題的討論與發展，以促進亞太地區經濟體的共同繁榮，目前亦已向 APEC 提出申請加入 CBPR 體系。

綜上，本次透過兩大國際主要隱私架構討論會議—「APEC 跨境隱私保護規則（CBPR）體系研討會」及「全球隱私高峰會（Global Privacy Summit）」的參與，將有助於我國瞭解目前世界各國所關注的隱私保護議題，評估 APEC CBPR 及 GDPR 實施後對企業所產生的影響，俾利並作為未來研擬政策及規劃因應方式的重要參考。

貳、行程安排與參與人員

本次參加 2018 年「APEC 跨境隱私保護規則（CBPR）體系研討會」暨「全球隱私高峰會（Global Privacy Summit）」會議，由法律事務處鄭美華科參與，目標在瞭解 APEC CBPR 及 GDPR 實施後將如何運作，以評估對企業所產生的影響，俾利及早因應並作為未來研擬政策之重要參考；同時並與其他隱私主管機關交流，瞭解各國所關注的隱私保護議題及因應策略。

「APEC 跨境隱私保護規則（CBPR）體系研討會」於 3 月 26 日舉辦，本會代表均全程參與；「全球隱私高峰會（Global Privacy Summit）」則自 3 月 27 日至 28 日止，每日均設定多場主題活動，因同時舉行超過 10 場以上會議，故本次以瞭解歐盟對於 GDPR 未來執法之立場及方向為目標參與會議，並盡可能將於會中所獲得內容重點摘錄於本報告，期能與本會同仁分享。以下為本次行程及研討會主題重點：

一、3/26(一) APEC 跨境隱私保護規則（CBPR）體系研討會

時間	議程
1:00p.m.- 1:20 p.m.	**開幕致詞** 美方說明會議主題 美國商務部部長 Wilbur Ross 美國聯邦貿易委員會 代理主席 Olhausen 女士
1:20 p.m.- 2:30 p.m.	**Session 1: APEC CBPR 管制者討論會議**

	主持人：美國聯邦貿易委員會 Hugh Stevenson 美國聯邦貿易委員會 國際消費者保護法律顧問 Melinda Claybaugh 日本 個人情報保護委員會 國際學術交流委員 Fumio Shimpo
2:30 p.m.- 3:45 p.m.	**Session 2: CBPR 運作討論會議**
	主持人：TrustArc 代表 Josh Harris Cisco 全球資料保護暨隱私顧問 Harvey Jang IBM 代表 Anick Fourtin-Cousens CA Technologies 副總裁 Bonnie Yeomans
3:45 p.m. -4:45 p.m.	**Session 3: CBPR 的下一步：CBPR 對於貿易的重要性、與 GDPR 其他法律架構的架接，及公司或國家參與的提升**
	主持人：ITI 副總裁 John Miller 日本經濟產業省國際事務辦公室處長 Shinji Kakuno 美國貿易代表處電信政策副助理代表 Johnathan McHale 加拿大工業部處長 Mark Schaan 美國資訊政策領導中心副主席與資深政策顧問 Markus Heyder 美國商務部服務副助理次長 Jim Sullivan 美國國家經濟委員會的科技、電信與網路安全政策首長特別助理 Abigail Slater
4:45 p.m. -5:00 p.m.	**閉幕致詞**

二、3/27(二) 「全球隱私高峰會（Global Privacy Summit）」Day1

時間	議程	
9:00a.m.- 10:15a.m.	開幕大會	
10:15a.m.- 11:00a.m.	休息 時間	*10:20a.m.-10:50a.m. IAPP 隱私核心線上教學展示 即興對等式圓桌討論會議 「透過隱私及資安訓練減輕人為風險因素」 之迷你演講
*11:00a.m.- 12:15p.m.	結合邊境之隱私與安全 美國聯邦貿易委員會首席技術官員：對使用者選擇、安全及課責之觀點 GDPR 2.0 Microsoft 公司能現在就能協助您達成 GDPR 之法遵 厚顏無恥地搜刮網路世界：從公開個人檔案（public profiles）談蒐集資料之倫理倫理界線 供應商之風險 2.0—確定瞭解您的資料位於何處？ 彌補隔閡：在隱私保護主管與安全主管間建立有效率的關係 會學習的機器人：他們是否也能學會人性價值？ 資料在地化對於數位經濟的影響 成為企業隱私長的途徑及方法 企業隱私長們談在中國及自中國邁向全球之商業	
12:00p.m.		12:15p.m.-12:35p.m.

<table>
<tr><td rowspan="4">2:00p.m.</td><td rowspan="4">午餐時間</td><td>從資料主體近用權至第 30 條規定之紀錄保存：談 GDPR 法遵之迷你會議</td></tr>
<tr><td>*12:30p.m.-13:30p.m.</td></tr>
<tr><td>美國法之資料規範與全球資料保護法制間之衝突
被挾持的資料人質：瞭解勒索軟體之威脅與因應
GDPR：個別成員國具體執法與豁免之討論
隱私與資安之立法最新發展
資料倫理與人工智慧之迷你會議</td></tr>
<tr><td></td></tr>
<tr><td>*2:00p.m.-3:15p.m.</td><td colspan="2">專訪法國國家資訊自由委員會主席 Isabelle Falque-Pierrotin
違反 GDPR：在 72 小時內損失全球總營收百分之四
於聯邦政府內找到一份隱私工作
拉丁美洲的最新管制發展
隱私科技的操作化：來自實務工作者的觀點
資料主體的近用權利：GDPR 實施之指引
隱私專家如何看待資料倫理
健康保險隱私與責任法(HIPAA)2.0—優化隱私與安全規範
遠東之旅：亞洲資料保護及隱私發展之初介
GDPR 實施後之「隱私盾」
從民事調查需求程序(CID)到同意，與聯邦貿易委員會協力進行隱私或安全調查</td></tr>
<tr><td rowspan="2">3:00p.m.-4:30p.m.</td><td rowspan="2"></td><td>3:30p.m.-3:50p.m.</td></tr>
<tr><td>運用科技建立以證據為基礎的 GDPR 法遵路</td></tr>
</table>

	休息時間	徑
		3:55p.m.-4:15p.m.
		追隨資料：達到 GDPR 第 30 條規定之最佳實踐方式與訣竅
*4:15p.m.-5:30p.m.	人工智慧：永遠傾聽與永遠開啟的利與弊 可以重新來過嗎？10 大違反資料安全事故通報之案例 打破 GDPR 的迷思 區塊鍊將如何轉化隱私與身分 如何將客戶隱私植入市值 300 億的跨國企業 事故通報 3.0—處理新的個別法律責任議題 利用演算法偵錯與減輕損失的產業最佳典範 趕上 E-Privacy：永不落幕的戲曲 巨量資料是封致未來的情書（且將協助你遵循 GDPR！） 公開資料的隱私：政府部門如何走在底線之內 在 GDPR 之外的全球隱私優先關注	

※時間經標註「*」者表示多場會議同時舉行。

三、 3/28(三) 「全球隱私高峰會（Global Privacy Summit）」Day2

時間	議程
*8:00a.m.- 9:00a.m.	◆ 關於生物識別科技的消費者使用與顧慮 ◆ 從新加坡到西雅圖：智慧城市的最佳典範 ◆ 資料治理策略到授權法遵 ◆ 如何展開隱私之職涯生活 ◆ 如何移動至雲端將促進你面對 GDPR 的準備工作 ◆ 我是律師：我該如何在資安議題上給予建言？ ◆ 用 GDPR 思維管理雲端人資系統以創造價值並節省時間 ◆ 隱私在拉丁美洲—多重司法管轄下解決跨時代議題的務實途徑 ◆ 對結果管制：有效利用胡蘿蔔與棒子 ◆ GDPR 與第三方、第四方及第 N 方—雖然還有時間，但剩下不多
9:00a.m.- 9:30a.m.	休息時間
*9:30a.m.- 10:30a.m.	◆ 一間聰明又安全的教室—隱私與教育科技 ◆ 設定好你的優先事項了嗎？演示 5 月 25 日的 GDPR 法遵…甚至更多！ ◆ 差異化：這不止是一個 checkbox！透過你的隱私計畫支援多樣化與包容性 ◆ 金融論壇：銀行隱私長討論金融隱私中的熱門話題 ◆ 健康保險隱私與責任法對於受規範主體與商業夥伴的執法

	◆ 我的特殊資源—女性（及男性）如何推銷自身的隱私專才 ◆ 隱私顧問的播客現場：為數位時代的青少年做決策 ◆ 隱私與競爭：大數據時代的重要議題 ◆ 隱私律師在聯邦執法機關中的角色
10:30a.m. 11:15a.m.	茶點時間
11:15a.m.- 12:30p.m.	閉幕大會
12:30p.m.- 12:50p.m.	資料隱私的民主化— 即時隱私風險智慧與同意管理之迷你會議
12:30p.m.- 1:30p.m.	離別午餐
1:30p.m.- 2:30p.m.	◆ 加州隱私法：對於美國及非美國企業的法遵要求 ◆ 美國司法部代表對於關鍵監控爭議的看法 ◆ 將「從設計著手保護隱私」工程技術植入安全發展的生命週期 ◆ GDPR 法遵與您的雲端服務供應商：最佳實務案例研析 ◆ GDPR 將改變您的網路使用經驗：擁抱它並取得優勢 ◆ GDPR：坐而言不如起而行 ◆ 從國際隱私監理機關之觀點看網路名聲爭議 ◆ 隱私執法與跨境資料流通：第一代施雷姆斯到第

	二代施雷姆斯 ◆ 創新的倫理：隱私如何與資料發展共存共榮 ◆ GDPR 與 e-privacy 對於廣告科技與歐洲互動廣告局指引的影響
2:30p.m.- 3:00p.m.	休息時間
3:00p.m.- 4:00p.m.	◆ 資料外洩該怎麼辦！（談企業在面對亞太地區的隱私法規落差下，如何發展出一套可普遍適用的隱私政策規範） ◆ 在（產品）不斷傳輸資料並改變軟體模型的環境下如何「從設計著手保護隱私」 ◆ 管制全球化的資料流通：來自三大洲的觀點 ◆ 學校不應該恐慌：兒童線上隱私保護法、家庭教育權利及隱私法與教育科技。

※時間經標註「*」者表示多場會議同時舉行。

參、研討會議題紀要

一、APEC 跨境隱私保護規則（CBPR）體系研討會

本次會議由美國商務部舉辦，目的在擴大產業對 APEC 跨境隱私保護規則（CBPR）及其認證制度的瞭解。

會議開始，首先由美國商務部部長 Wilbur Ross 以錄音方式致詞。Ross 部長表示，從近來的 FTC 已著手調查的臉書（Facebook）與劍橋分析（Cambridge Analytica）事件，以及美國政府與微軟（Microsoft）目前繫屬於最高法院的訴訟案件等重要事件可以發現，資料跨境流通已為數位經濟不可或缺的一環；在亞太地區的各個經濟體，有的已經訂定了嚴格的個人資料保護規範，有的則完全沒有相關規定，在這樣的法規落差的客觀環境下，如何有效建立安全自由的跨境資料流通機制以保護個人資料，同時確保國家主權不被犧牲，對於數位時代的全球經濟發展至為關鍵。

美國聯邦貿易委員會（Federal Trade Commission, FTC）代理主席 Maureen Olhausen 女士也接續補充，在資料跨境流通的時代，為企業、消費者及管制者都帶來了許多嚴峻的挑戰，而自「APEC 跨境隱私規則體系（Cross-Border Privacy Rules System，CBPRs）」建立以來，FTC 即持續扮演相當重要的角色，除了督促取得標章的業者信守承諾，也成功地與其他經濟體的隱私執法機關互助合作，例如在 2015 年的 AshleyMadison.com 資料外洩案，FTC 即與加拿大、澳洲的隱私執法機關合作進行國際調查，最終並以 160 萬美金與該公司達成和解，即為一國際合作處理跨境資料外洩事故的成功案例。顯示由 CBPRs 所建立的機制，將更有助於各經濟體互相回應彼此的調查需求。

美方認為對於國際性企業而言，具備跨境傳輸資料的能力相當關鍵，而 CBPRs 為隱私保護提供了全球性的可執行標準，確保消費者對於企業所進行的跨境資料傳輸活動能有所信賴。將 CBPRs 納入全球法遵計畫的企業，除了可以對外展示該公司致力於隱私保護的決心，對內並可簡化其全球法遵的程序與降

低相關成本，為企業帶來至少以下五個好處：

(一) 簡化跨越數個亞太地區經濟體的法遵程序與成本

(二) 由第三方提供具有對外證明效力的認證標章

(三) 符合為全球消費者與商業夥伴所承認的國際隱私標準

(四) 可提供管制機關相當的可信賴度

(五) 可彈性選擇被涵蓋的資料與經濟體

CBPRs 的認證係由被認可的問責機構（Accountability Agent）所執行，通過認證的企業可被證明符合 APEC 跨境隱私規則體系的相關要求。目前已經參與的 APEC 經濟體包括美國、墨西哥、日本、加拿大、南韓及新加坡；澳洲、中華臺北及菲律賓也正在申請加入，在各該經濟體中，並至少有一家認證機構提供相關的服務。

Session 1: APEC CBPR 管制者討論會議

本節會議邀請美、日兩國的隱私執法機關代表說明各機關在 CBPRs 中的角色，會議並由 FTC 國際事務辦公室副處長 Hugh Stevenson 擔任主持人。主持人首先說明 CBPRs 的角色中主要有問責機構（AA）及隱私執法機關（PEA）作為政府的代表。

AA 的任務包括：

1. 負責透過法律或契約條款來執行 CBPRs 的要求
2. 對相關消費爭議提供爭端解決的機制
3. 與其他 AA 合作以處理消費者申訴問題
4. 受到該所屬經濟體隱私執法機關的司法管轄

PEA 的任務則有：

1. 依據內國法執法，並使該個人資料保護效果與 CBPRs 要求一貫。
2. 在執法事項上與其他跨境隱私執法協議中的夥伴合作。

目前 CBPRs 中已有來自 10 個經濟體的 12 個 PEA，包含澳洲、加拿大、中國香港、日本、韓國、墨西哥、紐西蘭、菲律賓、新加坡及美國，其中澳洲及

韓國各有兩個 PEA，其他經濟體則各有一個 PEA 作為代表。

FTC 國際消費者保護法律顧問 Melinda Claybaugh 說明，美國是第一個加入 CBPR 體系的國家（2010 年），在加入以後即一直致力於促進國際隱私執法，FTC 對於國際隱私的隱私執法扮演關鍵的角色，一方面對取得認證但未信守承諾的企業採取行動；另一方面，對於未取得認證卻謊稱已取得的企業也會加以取締，執法重點在於要求企業必須信守對於消費者的承諾。

日本個人情報保護委員會國際學術交流委員 Fumio Shimpo 說明，日本在 2011 年 11 月加入 CPEA(Cross-border Privacy Enforcement Arrangement)；在 2014 年 4 月再加入了 CBPRs；2016 年 12 月 JIPDEC 成為問責機構(AA)，並於 2016 年 12 月給予 Intasect Communications, Inc 認證，該公司為第一個取得 CBPRs 認證的日本企業。此外，新修正的日本個人情報保護法第 24 條，也認可 CBPR 驗證具有法律上的效力，亦即除了當事人同意等合法事由外，企業亦得以位於國外的第三方（資料接受者）已取得 CBPRs 的驗證，作為個人資料國際傳輸的合法事由。

此外，日本個人資料保護情報委員會(PPC)成立於 2016 年 1 月；2017 年 5 月，原本分屬於各部會的個人資料保護權責均歸屬於 PPC，此後 PPC 為具有高度獨立性的個人資料保護專責機關，**並為 CBPRs 中唯一的日本 PEA**。PPC 有如下的主要功能：

1. 規劃並草擬相關法令
2. 監管個人資料處理活動
3. 為相關申訴提供必要的調解，並與企業合作
4. 促進相關國際合作

在全球化方面，日本個人情報保護法第 75 條與第 78 條分別規定有域外適用及與其他隱私執法機關分享必要資訊的規範；PPC 也已加入全球隱私執法網路(Global Privacy Enforcement Network，GPEN)，持續致力於與其他隱私執法機關進行國際合作。而在 CBPRs 方面，對於取得認證的公司，除了在必要時予以

監控、處理相關申訴，及施以額外的審查（根據情況給予停權或取消認證的措施）等項目由 AA 負責外，現場檢查、發布相關指引與建議、推薦相關取得認證的企業，都屬於 PPC 的任務；另外，在日本要擔任 AA 之前，必須先取得官方許可。在推動 CBPRs 作為方面，PPC 除了發散相關的宣導手冊以外，並已舉辦 103 場的研討會，有約 14,000 名參與者，並將在國際隱私會議上舉辦 CBPRs 工作坊。

Claybaugh 女士補充，CBPRs 並非取得認證企業的安全港（按：非加入即免責），但在執法機關在做相關決定時的考量因素上，取得 CBPRs 會是一個潛在的加分項目。因為 CBPRs 與各國個人資料保護規範具有相當的重疊性，例如告知、選擇等要求因此企業取得認證便可以迅速向執法機關展示其維護消費者隱私的能力，進而讓後續調查程序得以更為簡便的進行，同時也能增加消費者對於企業的資料安全信賴。

圖 1: APEC CBPR 管制者討論會議

Session 2: CBPR 運作討論會議

本節會議由前身為 Truste 的 TrustArc 國際管制事務處長 Josh Harris 擔任主持人，邀請已取得 CBPR 的企業分享取得 CBPRs 驗證的經驗與獲益。

IBM 是第一個取得 CBPRs 認證的企業，其代表 Anick Fourtin-Cousens 認為，在資料生態系統日趨複雜之際，企業如何向客戶提高可信賴度，並且說服相關利害關係人個人資料國際傳輸是以可被信賴的方式達成，是相當重要的課題。另外 IBM 也注意到了資料處理者之隱私承認（Privacy Recognition for Processor，PRP）的需求，並會在近期提出申請，IBM 認為 CBPRs、PRP 等制度可以為合作的生意夥伴具有一定的個人資料保護水平提供證明，因此可以為企業帶來加入的誘因。

Cisco 全球資料保護暨隱私顧問 Harvey Jang 則表示，對於企業來說最重要的是如何在不同的法規範要求中尋找其間的共通性，而 CBPRs 採納了受全球普遍認可的九大個人資料保護原則，同時又為各個經濟體保留形塑各自內國法的彈性，藉以滿足不同消費者的期待，並讓取得 CBPRs 驗證的企業可以更有效率的完成法遵的作業。同時問責機構也提供定期查核機制可以確保服務維持可信賴的品質；更重要的是，依照 Cisco 的經驗，相較於歐盟 BCR 的制度需耗時 6 個半月，通過 CBPRs 的認證只需要 8-10 週的時間，且有助於後續更快進入美歐之間的「隱私盾（Privacy Shield）」，

CA Technologies 副總裁 Bonnie Yeomans 亦認同企業要達成 CBPRs 的法遵上不若 GDPR 費時，而且相較於 GDPR 必須聘請個別的專業律師作為法律顧問，CBPRs 有問責機構(Accountability Agency，AA)的機制協助企業完成法遵，因此對企業來說提供了相當便利與幫助。

至於對是否要求合作的夥伴必須要先取得 CBPRs 的認證？Cisco 及 IBM 均表示在此議題上，不同於 GDPR，它們保持彈性的立場， 但也確實期待合作夥伴有這樣的標章；亦即雖非強制性要求合作夥伴必須具備，但認同 CBPRs 可以作為一個可信賴的機制。此外，由於企業的角色會不時轉變（按：資料控制者

與資料處理者的角色），因此未來 Cisco 也計畫會申請取得 PRP 的認證。

圖 2: CBPR 運作討論會議

Session 3: CBPR 的下一步：CBPR 對於貿易的重要性、PRP、與 GDPR 其他法律架構的架接，及公司或國家參與的提升

本節會議邀請日本、美國、加拿大的產業主管機關討論 CBPRs 對貿易的重要性、APEC 資料處理者之隱私承認（PRP）、與其他如歐盟一般個人資料保護規範（General Data Protection Regulations，GDPR）等其他法律制度的接軌，以及如何提升各經濟體或企業的參與，並由 ITI 副總裁 John Miller 擔任主持人。

日本經濟產業省國際事務辦公室處長 Shinji Kakuno 表示，CBPRs 為貿易帶來了許多好處，包含提升消費者對於企業的信賴、使國外的資料接受者能符合日本個人情報保護法的規範、以及促進與其他國際架構的接軌。另一方面，CBPRs 可以增資料的自由流通，因此可以解決許多社會議題，並刺激經濟發

展，這些好處都已經在去年的 G7 及 G20 會議上獲得共識。

美國貿易代表處電信政策副助理代表 Johnathan McHale 也附和，資料自由流通對於促進線上交易活動的發展至關重要，從 WTO 服務貿易總協定到 TPP 都一直被視為相當重要的原則，而 CBPR 以更有創意、提供更多空間的方式，促進資料自由流通的實現。

加拿大工業部處長 Mark Schaan 表示，在隱私的議題上，如同過去處理垃圾電子郵件的案例一樣，如何與國內的公民溝通，並與國際間維持對話都是相當重要的課題，而 CBPRs 為隱私保護劃定了最佳的底線。

美國資訊政策領導中心副主席與資深政策顧問 Markus Heyder 表示 CBPRs 可以為個人、企業乃至管制機關都帶來益處，例如：透過全球結盟的隱私保護措施及認證課責機制促進資料自由流通、協助企業符合當地的法律要求、讓企業可以向其潛在的商業夥伴及執法者展示其法遵能力、透過創造一個刺激組織主動實行有效隱私保護的機制以提高企業對於執法的可預見性、提高公眾及執法者對於組織的信賴、使組織能夠適用以風險為基礎的隱私原則參與資料活動；對於中小企而言，能夠藉由正式的課責方案於其組織內部落實相關課責機制等等。不過由於 CBPRs 採取的是自願課責的機制，因此必須盡可能地提高相關企業加入的誘因，才能將前述效益發揮至最大，對此 Markus 向隱私執法機關提出下列建議：

1. 正式展現對 CBPRs 的支持
2. 將該機制納入相關調查與執法中
3. 將該機制納入處罰金額的評估項目
4. 將該機制作為企業隱私承諾的證據
5. 將該機制作為企業已善盡善良管理人義務的證據
6. 將該機制作為認可企業已具備個資保護適足性，可為個人資料國際傳輸的條件

美國商務部服務副助理次長 Jim Sullivan 認為，CBPRs 與 PRP 可以為個人

資料國際傳輸提供最佳的安全保證，並期待 APEC 所有經濟體都能加入 CBPRs，同時也鼓勵自己國內的產業加入。

美國國家經濟委員會的科技、電信與網路安全政策首長特別助理 Abigail Slater 則強調此一議題主要有三個重點：

1. 資料自由流通可以帶來實際與潛在的利益

2. 資料自由流通應該是預設的選項

3. 各國法律也許不盡相同，但應該持續保持對話

此外，也許未來也能考慮擴大納入 APEC 以外經濟體的可能性。

圖 3:各產業主管機關及政府代表表達對 CBPR 的看法

附件：資料處理者之隱私承認（PRP）之目的與背景說明

APEC 資料處理者之隱私承認（Privacy Recognition for Processor，PRP）PRP 一方面可以協助個人資料處理者展現其能有效履行資料控制者關於個人資料處理義務的能力；另一方面也能幫助資料控制者識別出具備資格且可課責的資料處理者。

由於 APEC 隱私架構僅適用於資料控制者，所以 2011 年根據該架構所確立的 APEC 跨境隱私規則體系（CBPRs）亦僅限於資料控制者方有適用。對於 CBPRs 如此限縮的適用範圍，資料控制者因此呼籲必須發展另一套機制，以協助其找出具有資格且可課責的資料處理者來締結契約。同樣地，APEC 經濟體中擔任資料處理者角色的企業也對於此一機制表達了高度的興趣，因為如此將可顯示它們具備有效履行資料控制者隱私要求的能力，包含可以協助在其經濟體以外默默無名的中小企業，因此能成為全球資料處理網絡的成員之一。

PRP 代表著資料處理者為了取得 APEC 問責機構認證所應符合的最低要求，同時也為資料處理者的隱私政策及執行提供相關的保證。

因為 APEC 隱私架構中的隱私原則不適用於資料處理者，PRP 並不會直接履行隱私架構的原則。一般而言，PRP 可以被資料處理者用於展現其履行個人資料處理活動的能力，但也被設計成可以確保個人資料處理活動，與 CBPRs 中對於資料控制者的相關要求具有一致性。

PRP 不影響隱私架構、CBPRs 或相關法律對於資料控制者與處理者間的責任分配。依據隱私架構及 CBPRs 的課責原則，資料控制者必須對資料處理者受委託所進行的相關活動負責，未來即使與 PRP 所認可的處理者締約，此一原則仍不會改變。

因此，資料處理者的活動仍會因為對於資料控制者的執法而間接受有拘束，亦即，為 CBPRs 所認證的資料控制者在選擇其資料處理者時必須負起「善良管理人」（due diligence）的注意義務，並且適當監督其資料處理者，不論該等資料處理者有否取得 PRP 的認證。必須注意的是，取得 CBPRs 認證的資料

控制者並未被要求一定要和取得 PRP 認證的資料處理者締約，始能符合隱私架構及 CBPRs 的課責原則。

二、　全球隱私高峰會（Global Privacy Summit）

全球隱私高峰會是由國際隱私專家協會（International Association of Privacy Professionals）所舉辦的年度隱私盛會，在兩天的會議期間舉行超過 80 場的大、小型會議，邀請包含世界各國的隱私執法機關代表、產業界取得隱私專家證照的專業人士，以及各大企業中的資料保護長，就各項時下熱門的隱私議題進行意見分享與討論；此外，會場並有許多提供隱私保護服務的廠商，擺設超過 50 個攤位，提供相關產品及服務的諮詢。

圖 4:全球隱私高峰會攤位現場

(一)GDPR 2.0

主持人

Ruth Boardman

Co-head, International Data Protection Practice, Bird & Bird

與談人

Helen Dixon

Commissioner, Office of the Data Protection Commissioner of Ireland

本場會議主要想傾聽自歐盟的各個資料保護主管機關的計畫，以瞭解：GDPR 中是否有哪些具有優先性的條文？主管機關是否會進行現場調查？對於達成新法要求有困難者，他們是否會給予相當寬容？主管機關有足夠的資源嗎？以及他們計畫將如何用運這些強大的新權力來課處罰鍰？

來自愛爾蘭隱私執法機關的代表 Helen Dixon 表示，據瞭解現在對於企業最主要的壓力在於資料事故發生後通知資料主體的義務；而由於資源的有限，執法機關必然需要將其任務作優先性的規劃。她認為對於愛爾蘭隱私執法機關，**最重要的是有關「透明化」義務的規範**，因為透明化是最基本的義務，是資料主體行使權利的前提，如果資料控制者沒有向資料主體揭露足夠的資訊，資料主體不能知悉其被蒐集的個人資料有哪些？資料被如何處理？如此將妨礙資料主體其他權利的行使，因此會是執法者最優先關切的規定。

此外，在處罰方面，不是所有申訴案件都會被處罰，愛爾蘭隱私執法機關會參考過去歐盟競爭法上的先例，特別是歐盟過去對於 Facebook、Google 等公司裁處的案例，但對於什麼樣的案件將科處多少金額的處罰，並無一定答案，必須視個案情節與比例原則等因素綜合決定，而且相關決定嗣後還必須受到法院的檢驗與確認，因此很難在現在就給予明確的答案；另外由於在雇主與員工之間存在有大量的個人資料蒐集行為，因此這部分也會是執法機關未來關注的焦點之一。

GDPR 很重要的是調合了各歐盟成員國不同的法律系統，並提供一站式

（one stop shop）的架構，讓企業不需要同時面對數個隱私執法機關；另一個重點是明定「假名化（pseudonymization）的個人資料。至何謂「假名化」的個人資料，非常仰賴具體個案情況作判斷，無法一概而論。

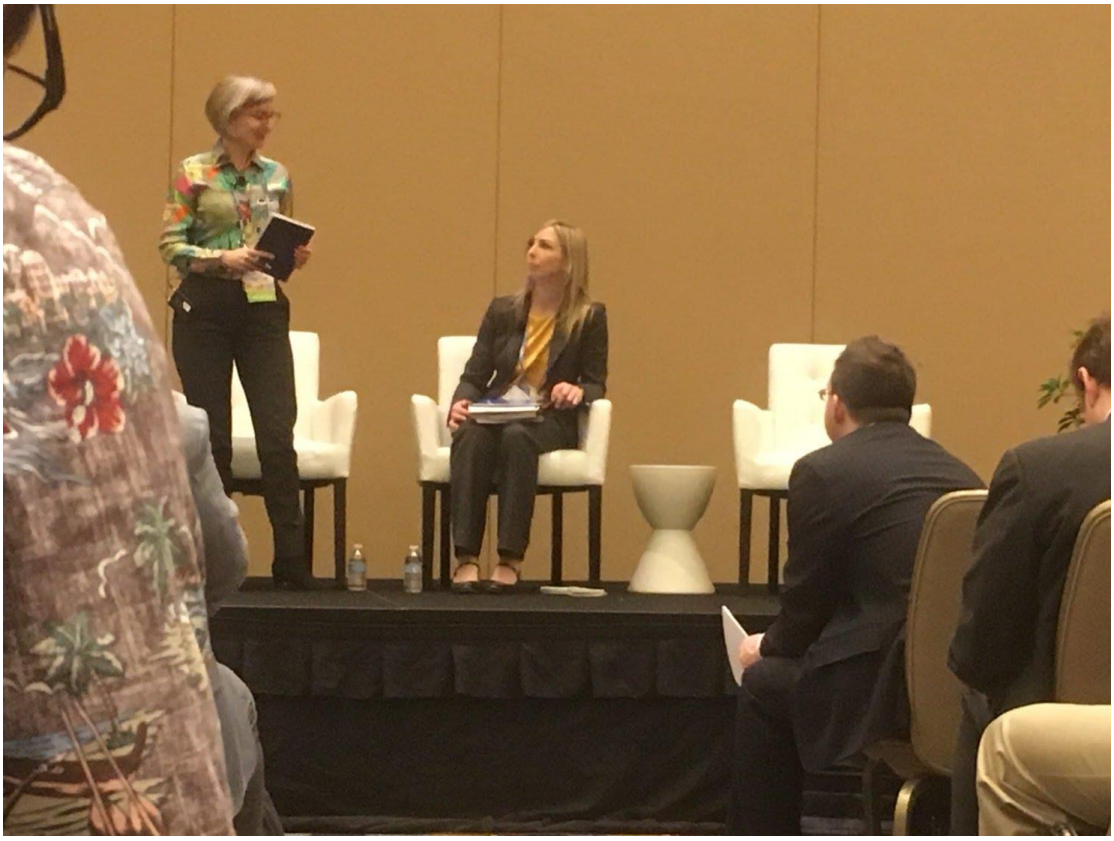

圖 5:主持人 Boardman（左）與愛爾蘭隱私執法機關代表 Dixon（右）

(二)GDPR：個別成員國具體執法與豁免之討論

講者

Erica Kitaev

CIPP/US, Managing Editor, Privacy and Data Security, Practical Law Thomson Reuters

Kimberly Wong

CIPP/US, CIPT, FIP, Senior Counsel, Data and Technology Practice Group, McDonald's

Theodore Kobus III

CIPM, Leader, Privacy and Data Protection Team, BakerHostetler

本場會議，講者們深入探討 GDPR 中每一條授權各會員國得制定自己豁免規定的條款，檢視各種施行法規的狀況及要求，找出其中的相異處，並為必須採取的相應措施提供指引及最佳典範。

GDP 是歐盟資料保護規則 20 年來第一次的全面性改造，並將會取代過去的歐盟個人資料保護指令(95/46/EC)，2018 年 5 月 25 日並將直接適用所有歐盟會員國，取代所有依據指令所制定的內國法。GDPR 目標提供一致適用於全歐盟的資料保護規則，但同時也允許歐盟會員國立法補充 GDPR 的部分規範。

GDPR 重點鳥瞰

寬廣的適用範圍	新增的關鍵義務	加強資料主體權利	強化執法及責任
✓ 規範適用於資料控制者及資料處理者 ✓ 增加適用於非歐盟企業 ✓ 處理未滿 16 歲孩童的個人資料必須取得父母的同意	✓ 隱私影響評估 ✓ 預設隱私及從設計著手保護隱私 ✓ 資料外洩的通知義務 ✓ 課責及法遵的展現 ✓ 新增關於同意的規範 ✓ 側寫(profiling)規範 ✓ 在特定條件下必須設置資料保護官(Data Protection Officer)	✓ 強化告知義務 ✓ 資料可攜權 ✓ 被遺忘權 ✓ 限制資料處理權	✓ 最高 2000 萬歐元或前一年度全球總營收 4%的行政罰鍰（取較高者） ✓ 隱私執法機關擁有更大的執法權限 ✓ 私人可提起訴訟

資料來源：GPS18

GDPR 允許各會員國為不同規範的重點條文

GDPR 條文	會員國可為不同規範的內容
第 6 條	得依第 6 條第 1 項 c 款或 e 款處理個資的特別規定
第 8 條	孩童得為有效同意的年齡（不得低於 13 歲）
第 9 條	處理特定類型敏感性個資（基因、生物特徵或健康資料），及以同意作為合法事由處理敏感性個資的條件與限制
第 10 條	有關處理涉及刑事追訴及犯罪個資的授權
第 23 條	對於資料主體權利範圍及資料控制者義務的限制
第 36 條第 5 項	要求基於公共利益處理個人資料必須向隱私監理機關事前諮詢及取得其核准
第 37 條第 4 項	額外要求設置資料保護專責人員(DPO)
第 58 條第 6 項	強化隱私保護機關的權力
第 83 條第 7 項	得對公務機關處以行政罰鍰

第 84 條	對於不適用第 83 條行政罰鍰違法行為的其他處罰
第 87 條	對於處理國家身分識別號碼的規定
第 88 條	對於基於僱傭關係處理個資的規定
第 89 條第 2 項	基於檔案、科學或歷史研究、統計目的處理個資時，對於資料主體的權利限制

資料來源：GPS18

目前已經根據 GDPR 重新訂定、通過內國個人資料保護法的國家包括奧地利、比利時、德國、斯洛伐克；已經公布草案的國家則有：捷克、丹麥、愛沙尼亞、芬蘭、法國、愛爾蘭、拉脫維亞、立陶宛、盧森堡、荷蘭、波蘭、羅馬尼亞、斯洛維尼亞、西班牙、瑞典以及英國；尚未公布任何草案的是：保加利亞、克羅埃西亞、賽普勒斯、希臘、匈牙利、義大利、馬爾他及葡萄牙。

對於這些不同國家在細節上寬嚴不一的內國法制未來應如何調和仍有不明，勢必需要未來的個人資料保護委員會發佈相關的指引加以釐清。不過一般而言，預期的關鍵差異大概會在「孩童有效同意的年齡」、「處理敏感性個資的限制」、「有關處理涉及刑事追訴及犯罪個資的授權」、「基於僱傭關係處理個資」、「對於資料主體權利的額外限制」、「額外要求設置資料保護專責人員」、「有關設置內國隱私保護機關的規定」、「課予公務機關的罰鍰」，以及對於「違法行為不適用 GDPR 行政罰鍰所為的其他處罰」等事項。

此外，由於 GDPR 第 3 條只規範其適用情形，GDPR 卻未規範如何適用歐盟會員國各內國法，目前看起來在各會員國內國法的適用上會有下面兩種可能：

適用資料處理者或控制者所在的歐盟會員國內國法；

若為非歐盟的資料處理者或控制者，則適用受影響資料主體所在的歐盟會員國內國法。

在內國法的適用範圍上，部分國家於其內國法中複製 GDPR 第 3 條規定（例如：荷蘭），但其他國家則似乎擴大了適用範圍（例如德國、英國）。例如

英國草案明定，該草案對於資料主體居住於英國境內，而資料控制者非設立於英國但設立於歐盟其他會員國的情形，亦有適用；相反地，依照 GDPR，資料控制者必須設立於歐盟，才有該特定會員國法律的適用。因此即便是在適用範圍上，各會員國內國法亦有差異，導致企業可能同時必須適用多個會員國的內國法。

雖然各國的管轄權如何行使與調和仍有不明，但講者則認為，依照一般法律原則，各國應該沒有將其內國法延伸至境外（其他會員國）的打算，而歐盟個人資料保護工作小組(WP29)也已經表明，未來將會針對此一議題再發布相關的適用指引。

圖 6:本場會議講者

(三)專訪法國國家資訊自由委員會主席 Isabelle Falque-Pierrotin

主持人

Eloïse Gratton

Partner and National Co-leader, Privacy and Data Protection, Borden Ladner Gervais

來賓

Isabelle Falque-Pierrotin

President, National Commission on Informatics and Civil Liberties (CNIL)

Isabelle Falque-Pierrotin 擔任法國國家資訊自由委員會主席超過 6 年、4 年的歐盟第 29 條資料保護工作小組主席，主導法國及歐洲資料保護法的轉型與成長。她發布過無數的意見與指引，主導對大型跨國企業的跨境調查與執法，並目睹資料保護主管機關在數位時代成為一個強大的管制者。

本場會議將著名的加拿大律師 Eloïse Gratton 專訪主席 Falque-Pierrotin 女士，議題包含隨著 GDPR 生效日期的逼近，ePrivacy 草案的立法進度？歐美之間隱私盾的執法問題？未來歐洲資料保護委員會(EDPB)又將與過去的第 29 條資料保護工作小組有什麼不同？執法是否會集中針對美國的跨國企業，或歐洲的中小企業也會受到影響？當貿易及資料流通至欠缺全面性資料保護法規的中國及印度兩大市場時，該如何維持原來的資料保護標準？促進網路經濟發展的廣告科技公司面對嚴格的同意要求，又應該如何調適？隱私在面對如人工智慧、連網汽車、智慧城市等目不暇給的科技發展，又該如何回應？

Falque-Pierrotin 女士表示，GDPR 的誕生是為了解決數位網路時代所產生的信任危機問題，希望讓資料控制者負起更多的責任、讓資料主體擁有更多可以行使的權利、統整並調和歐盟境內的隱私保護規範，以及確保境外能夠尊重歐盟的隱私架構。此外，GDPR 也賦予各國隱私保護機關更多的權力，並提供「一站式(one-stop shop)」的監理方式，讓企業只需要面對一個隱私保護機關，而不需要因為應付多個會員國的隱私保護機關而疲於奔命。

關於 GDPR 的資料保護委員會，是由指令時代的非正式歐盟資料保護小組

(WP29)轉變而來，過去的歐盟資料保護小組 WP29 只是由專家組成的咨詢小組，其意見沒有拘束力，未來的資料保護委員會則是由歐盟各會員國代表組成，將可共同作成具有法律效力的決定，有統一對外的聲音，與過去有很大的不同。

GDPR 並沒有應該被優先執法的選項，所有條文都應該被遵循，即使罰鍰額度提高，但過去已經存在許多已經成為共識的指引，因此應該不需要過度焦慮。此外，對於管制者而言，目的在於督促資料控制者與管理者瞭解並落實 GDPR 的規範，處罰是手段並非目的，除了處罰以外，監理機關還有其他許多可能的作法來促進 GDPR 的落實，會視具體個案情形而定，例如行為人是否為善意（good faith）、是否已盡其善良管理人的注意義務（due diligence）等等，不一定非處罰不可。而中小企業因為相對於大企業擁有的資源確實較少，因此可能受到較多的寬容。

在個人資料的國際傳輸上，GDPR 提供了許多不同的工具，其中並沒有特別受到主管機關偏好者，而是要視個別資料控制者或處理者各自的需求而定，例如對於大型跨國企業而言，「共同拘束條款（Binding Corporate Rules，BCR）」可能可以提供更多的適用彈性。GDPR 的出發點在於確保個人資料的安全，不只考量貿易，對於國際傳輸的適足性評估，GDPR 也非要求其他國家必須複製 GDPR 的規定，而是希望必須在重點上具有一致性，亦即實踐個人資料保護的手段可以不同，不過所達成的結果必須大致相同。談到歐盟與美國之間的「隱私盾」協議，目前還有待法院作出做後的決定，但該協議也只是劃定一個最低的個人資料保護界線，未來在個人資料國際傳輸議題上，必須透過國際會議的場合，與不同國家的隱私保護主管機關保持持續的對話、相互學習與交流，而這當中也包括傾聽一般民眾對於個人資料保護規範的期望，如此亦有助於形成全球性的個人資料保護原則及最佳的行為典範，

關於 GDPR 目前一些比較受到討論的爭議，由於 GDPR 目的是確保在歐盟活動的人民都能遵循該法律，因此以瞄準歐盟市場的資料控制者與處理者為規

範對象，至於如何定義「瞄準(target)」？有一些具體的案例可以提供參考，解釋上會著重在該資料控制者的「意圖(intention)」上。另外，對於資料處理者來說，其義務主要是透過契約而形成，最重要的義務是確保資料的安全(security)。

而如「被遺忘權」、「資料可攜權」等新的資料主體權利也經常被質疑將如何被實踐，對此，Falque-Pierrotin 女士表示這些新的權利都是順應社會發展下新的公民需求而產生的權利，而在 GDPR 增加該兩者之後，日本與新加坡也各自於其最新的個人資料保護法中加以明定，更顯見這兩個權利的訂定有其需要及合理性。此外，面對複雜的數位生態系統，為了更適當地平衡隱私保護與經濟發展，從設計著手保護隱私的概念以及當事人同意、透明性的確保，都是不可或缺的。

關於 GDPR 的法遵(compliance)，Falque-Pierrotin 女士強調這並非只是法律技術層面的問題，而是企業整體都必須投入，將個人資料保護的意識內化成企業運作的一部分。即便一時沒有辦法「完全達成」GDPR 的要求也不需要太過緊張，因為 GDPR 對於所有人來說都是一個「學習曲線(learning curve)」，即使是主管機關也是持續的在學習、研究因 GDPR 所發展出來的各種議題，對於不同國家法律之間的衝突，也必須透過國際會議場合持續的對話與溝通。

最後，關於何時會公布 e-privacy 規則，由於各界對於是不是要採取「選擇同意(opt-in)」的機制還有相當大的爭議（Falque-Pierrotin 女士表示，該機制其實在 2009 年已經實施的版本就已經有所規範，因此對於現在還會有如此爭議她感到相當吃驚），因此目前也無法提供明確的時間表。

圖 7: 法國國家資訊自由委員會主席 Falque-Pierrotin（左）
與主持人 Gratton（右）

(四)打破 GDPR 的迷思

講者

Jocelyn Aqua

CIPP/G, Principal, Cybersecurity and Privacy, PwC

Christian D'Cunha

Policy and Consultation Unit, European Data Protection Supervisor

Gabriela Zanfir-Fortuna

Fellow, Future of Privacy Forum

本場會議聚焦在與 GDPR 有關的公共領域中，最有趣且極富爭議—但也最模糊的一些議題，邀請來自歐洲管制機關頂尖的專家，及產業中居於領導地位的實務工作者提供其洞見。延續英國資訊委員辦公室的倡議，會議逐一探討以下迷思：

1. GDPR 適用於…身處世界各地歐洲公民的個人資料？又，GDPR 不適用於設立於歐盟境內的資料控制者或處理者，處理歐盟境外人民個人資料的情形？

對於 GDPR 適用範圍的解釋，資料保護小組將會在近期發佈相關的指引說明，但 GDPR 所瞄準的主要是歐盟境內，因此如果是境外企業聘僱歐盟公民，不必然就會適用 GDPR，除非該企業在歐盟有相關的招募活動，亦即在歐盟境內有個人資料的蒐集行為才有適用。另外，GDPR 對於資料處理者所規範的義務只有二項：資料安全及國際傳輸。

2. 取得有效的當事人同意是 GDPR 法遵的關鍵？

當事人同意並非唯一的工具，在許多情形下，當事人同意並非必要，重點在於透明化與課責，對於資料控制者而言，最重要的在於對於個人資料的蒐集處理能否有相關的合法事由存在。

3. 個人資料專責人員在企業當中不能負責其他工作？

擔任企業的資料保護專員並不必然即不能擔任公司其他的職位，與其說是角色上的衝突，不如說是本質上的衝突，重點在於是否能夠「獨立」執行其業務。

4. 資料製圖(mapping)是 GDPR 一個重要的要求？

資料製圖並非一個法定要求，但對於個人資料保護的落實，是一個好的措施(good practice)，因為對於資料控制者而言，知道自己所掌有的個人資料位於何處，是有效管理的前提。

5. 要達成 GDPR 法遵只需要說你已經將個人資料匿名化(anonymized)及累積性(aggregated)處理了？

談到資料去識別化，資料控制者必須要留意「再識別(re-identification)」的問題，如果資料可再識別，則仍然屬於個人資料而須受到 GDPR 的規範，因此資料控制者必須要確保經過去識別處理後的資料已經確實達到「匿名化」（按：即無法再識別特定個人）的要求，才能稱該等資料為「匿名化資料」。

6. 「具體」與「明確」同意是同一件事？

當事人同意的具體(specific)與明確(explicit)不同，前者指讓當事人了解資料將如何被處理，後者則有關如何取得當事人的同意。

7. GDPR 是歐洲的資料帝國主義(imperialism)？

GDPR 的目的是確保個人資料安全不會因跨境、跨國傳輸而有所減損，增進個人對於整體數位生態系統運作的信賴，進而促進資料的流通。

(五)對結果管制：有效利用胡蘿蔔與棒子

講者

Bojana Bellamy

CIPP/E, President, Centre for Information Policy Leadership, Hunton & Williams

Müge Fazlioglu

CIPP/US, Westin Fellow, IAPP

Andrea Jelinek

Austrian Data Protection Authority

Yeong Zee Kin

Deputy Commissioner, Personal Data Protection Commission of Singapore

本場會議，由來自兩大洲的隱私保護主管機關，與最近甫發表論文「對結果管制—給領導者與參與者的策略與優先建議」的資訊政策領導者中心總裁 Bojana Bellamy，及剛公布對於資料保護主管機關預算及人事調查的 IAPP 成員 Muge Fazlioglu 共同討論管制者的策略。

Bellamy 女士表示當被賦予眾多任務、被寄予高期待，但資源卻相對有限時，管制者必須以風險基礎（risk-based）為考量來設計適當的策略與優先計畫，包括與被管制者間建立有建設性的來往，以作最佳的資源分配。而要進行更有效率的管制，應採取結果導向（results-based）的方法，其論文歸納出的原則如下：

1. 要對數位世界中的結果進行管制，需要具有策略、效率、協調且透明的獨立資料保護機關。
2. 隱私保護主管機關的目標應為產生具有成本效益的結果，以有效率的保護個人，確保有責任的資料使用，並促進繁榮與創新。
3. 隱私保護主管機關應該優先確保個人的資料安全。
4. 各個獨立的隱私保護主管機關都應該具備可問責的透明性，詳細說明其所

欲達成的特定目的、優先任務，以及其將在日常監理工作中將採取的途徑。

5. 所有的隱私保護主管機關都應該盡可能的具有協調性、一貫性及互補性。
6. 隱私保護主管機關在管制態度上應維持一致，跨產業、領域都應該採取相同的管制途徑，而不考慮被管制的組織所屬的類型或區域。
7. 各個隱私保護主管機關都應該以風險基礎為考量，將焦點放在將造成個人、民主或社會價值最大危害的行為上。
8. 一個採取強調與領導者之間架構建設性協議，且具有資訊性、建議性的對話與支持的管制途徑，將遠比只倚靠豁免與處罰等手段來得更有效率。
9. 在資料保護的領域中，著重於給予資訊與建議更是特別重要，因為其影響遍及無數組織，且相關規範在本質上既無由精確，更須視具體脈絡及個案判斷而定。
10. 在個人資料處理上與組織間保有開放且具有建設性的關係。此關係構築在誠實對話及相互合作之上，但在課責上必須毫不模糊，如此對於整體法遵的結果將能有所改善。
11. 受管制機關在法律遵循上所展現的善意與已善盡查核責任的努力，應該被特別納入評估。
12. 當組織展現負責任的行為與試圖將事情做正確時，應當受到鼓勵。例如對外透明呈現其課責機制、隱私及風險管理程式、其隱私專責人員的影響、驗證標章機制、標準契約條款、CBPR，以及其他課責機制等等。
13. 懲罰性裁處應該針對基於故意或重大過失的違法行為，或有屢犯、特別嚴重情節的情形上。
14. 儘管處理民眾申訴可能是保護個人的重要因素之一，但要處理大量的申訴將消耗相當的資源，且可能會影響其他策略目標，因此應該運用清楚的基準決定發動調查與否，並將個案申訴是否富有重要參考價值的因素納入考量。

在實證研究上，經過調查，各國隱私執法機關(DPA)的預算主要與各國的國產內毛額(GDP)與人口等國情因素密切相關，但也有少數情形例外。例如英國GDP 較西班牙高近 2 倍，但兩國隱私執法機關的預算卻相去不遠。然而，Fazlioglu 也提醒，必須注意各國的隱私執法機關的架構可能有所不同，例如美國 FTC 同時肩負促進競爭與消費者保護（按：即隱私執法）的任務，因此該機關究竟確實分配多少預算至隱私保護部分，實際上不得而知。

奧地利隱私執法機關代表 Jelinek 表示，隨著數位時代個人資料保護意識的高漲，歐洲各隱私保護主管機關的預算及人力都有持續增加的趨勢。GDPR 中大部分是延續指令時代就存在的規範，順應數位時代的發展帶來新的隱私保護形式，賦予資料主體更多的權利，以及企業更多的責任，也因此促使隱私執法機關必須要不斷精進，並與其他國家的隱私執法機關有更密切的合作。

新加坡個人資料保護委員會副主席 Yeong 表示，新加坡的隱私執法計畫重點包括：提供私人組織資料保護專員(DPO)相關協助;對於個人提出的申訴擇具有本質上重要性者予以處罰，其他則盡可能以調解方式處理爭端；將法律觀念轉化為政策與實際的案例指引，並公開委員會所做成的相關決定，以協助企業進行法遵。

Jelinek 女士表示，新加坡的作法非常有趣，但由於資料隱私權屬於基本人權，不能因受規範的組織大小而有差異；且歐洲與新加坡在法律體系上有本質上的不同，因此新加坡的個人資料保護模式恐怕不適合歐洲。

Yeong 副主席補充，新加坡在隱私執法上不會憑空想像，他們認為釐清究竟個案中具體的「公共利益」為何非常重要，因此都是以個案為基礎作思考；會以是否具有公共利益，或只是單純存在於私人雙方間的爭議，來決定是否投入資源來進行更進一步的調查或處罰。

(六)隱私與競爭：大數據時代的重要議題

講者

Giovanni Buttarelli

European Data Protection Supervisor

Edith Ramirez

Former Chairwoman of the U.S. Federal Trade Commission; Partner, Hogan Lovells

Peter Swire

CIPP/US, Law and Ethics, Georgia Tech Scheller College of Business; Senior Counsel, Alston & Bird

本場會議中，由曾經發表關於隱私與反壟斷交叉點的 Peter Swire 教授，主導與曾經負責同時管理該兩個領域的前美國貿易委員會主席 Edith Ramirez，與來自歐盟資料保護監理機關 Giovanni Buttarelli 的討論。

2016 年 3 月，德國競爭主管機關(GCA)基於懷疑臉書(Facebook)透過服務條款中有關使用者資料蒐集的規定，濫用其於社交網路市場的市場主導者地位，發動對臉書的調查。GCA 聲明指出，為了使用社交網路，使用者必須先同意該公司的個人資料蒐集服務條款，但從服務條款中，使用者難以瞭解及評估這些協議的影響範圍，因此國家法律是否容許這樣的過程，特別是從資料保護法的角度而言，即存在相當大的疑慮；如果服務條款會誤導消費者，則甚至會構成濫用市場地位的行為。

GCA 認為，因為臉書擁有大量的使用者，且競爭對手產品的替代性有限，使該公司在德國的社群網路市場具有準獨占(quasi-monopoly)的地位。臉書利用市場主導者地位，在近用使用者資料上取得優勢，為了確保並加強此優勢，臉書將使用服務的條件構築在使用者對於個人資料蒐集的廣泛同意上；此外，臉書也會蒐集使用者利用臉書帳號登入第三方網站時的資料，並利用這些資料來優化其服務，並讓更多使用者「綁定」在其網站上，即使使用者應該對於他們在第三方網站所產生的個人資料將被如何處理，會有某程度的預期，但這個程

度不包含預知這些資料會被加入到他們在臉書的帳戶之內。因此，GCA 認為在這方面，資料保護法與競爭法係有相同目標，亦即保護使用者之個資免於被市場相對方所利用，而臉書的條款對於不論是從競爭法或資料保護的角度而言，都是無法被接受的。

但這樣的初步看法也引起了一些爭議，是否所有的隱私侵害結果都會自動構成市場地位的濫用？但 GCA 後來又再度對外說明，表示臉書的使用條款即使沒有侵害隱私，也是不公平的。該機關試圖在隱私以外，建立一個單獨可成立的反競爭行為，只是同時具有隱私侵害的「特色」。

從上述隱私保護與競爭法交錯的指標性案件出發，Peter Swire 教授詢問歐、美競爭法主管機關代表的看法。FTC 前主席表示，FTC 對於資料交易的看法，關鍵是資料是否能創造或加強市場力量？資料是否具有獨特的價值？資料庫的結合是否如同創新與服務品質等非價格因素一樣會加強市場力量？管制者能否正確適當的評估資料的價值在此一議題上是具有決定性的前提。

而當前備受討論的爭議在於，讓新進、小型業者能夠近用並分享資料有助於競爭，但卻不利於隱私。

但歐盟資料保護監理機關代表認為，競爭與隱私保護是相輔相成，反競爭手段可以確保消費者對於其個人資料能保有自主控制權利，並有利於民主的發展。

FTC 前主席表示，相關的理論基礎確實存在，但究竟應該在具體案例中如何實踐，仍有相當困難，這是當前面臨的最大挑戰。站在 FTC 的立場，不會單純為了隱私而禁止結合，只有在結合可能導致隱私方面反競爭的結果出現，進而可能傷害消費者時，才會禁止結合。

(七)GDPR 與 e-privacy 對於廣告科技與歐洲互動廣告局指引的影響

主持人

Peter Swire

CIPP/US, Law and Ethics, Georgia Tech Scheller College of Business; Senior Counsel, Alston & Bird

講者

Matthias Matthiesen

CIPP/E, Director, Privacy and Public Policy, IAB Europe

Ghita Harris-Newton

CIPP/E, CIPP/US, CPO, Deputy General Counsel, Quantcast

Alice Lincoln

CIPP/US, VP, Data Policy and Governance, MediaMath

Noga Rosenthal

CIPP/US, CPO, Epsilon

如 Cookies ID 等網路識別碼、位置資料均屬於個人資料，假名化資料在 GDPR 中也已被確認屬於個人資料，而促使企業進行假名化措施的誘因包括：可以進一步的利用、資料安全因素等考量。

Epsilon 代表表示，關於資料主體的近用權，如何確認請求者的身分？必須非常謹慎，否則反而會侵害他人隱私。如果資料處理者的身分不能獨立回應資料主體的請求，除非已經獲得控制者清楚的指示，否則必須由資料控制者來回應。而 Mediamath 代表表示，同意不一定必要，在正當利益的合法事由上，有利益權衡的機制來決定是否有合法事由存在。至於如何進行利益權衡則完全仰賴個案判斷，在此情形下，假名化有助於資料控制者通過利益權衡的測試。

E-privacy 指令在 2002 年頒布，自 2009 年開始要求儲存或近用使用者的裝置必須取得一般性同意。而新的 E-privacy regulation 可能還要花上許多時間才會公布，在此之前很難預測細節會是什麼，也無法確知其與 GDPR 之間將會如何調和。

(八)管制全球化的資料流通：來自三大洲的觀點

主持人

Omer Tene

VP, Chief Knowledge Officer, IAPP

與談人

Julie Brill

Corporate VP and Deputy General Counsel, Microsoft

Helen Dixon

Commissioner, Office of the Data Protection Commissioner of Ireland

Stephen Wong

Privacy Commissioner, Office of the Privacy Commissioner for Personal Data, Hong Kong, China

本場會議由來自亞洲、歐洲及美國的政策主導者討論影響著全球資料流通的最新法律及管制方向的發展。

愛爾蘭隱私執法機關代表表示，在 GDPR 之下，企業只要面對單一的主管機關，讓資料可以在歐盟境內自由的跨境流通，更重要的是讓個人資料保護的執法能有一貫性。

Microsoft 代表表示，就其向相關執法機關作的了解，在今年 5 月 25 以後的個人資料處理活動就會適用 GDPR，但沒有很明確的執法期限，執法機關應該會採取以風險及事實為基礎導向的執法態度。而 Microsoft 非常嚴謹地面對自己在個人資料生態系統的角色，重視使用者的信任，因此為 GDPR 投入相當的法遵成本。

香港個人資料私隱專員公署專員表示，香港的個人資料保護法 PDPO 主要參考 1998 年的 OECD 原則及歐盟 1995 的個人資料保護指令所訂定，因此與 GDPR 有相當程度的相似性。歐盟是香港的第二大貿易夥伴，因此香港企業非常關注 GDPR 的公布，但目前香港的中小企業對於 GDPR 的地域適用範圍仍然感到相當的不確定。

肆、心得與建議

當資料自由流通已經成為國際自由貿易的重要原則時，瞭解如何在達成該目標的同時，並確實維護個人資料的安全，已成為我國邁向數位國家階段必須積極面對並準備的課題。本次藉由參加「APEC 跨境隱私保護規則（CBPR）體系研討會」暨「全球隱私高峰會（Global Privacy Summit）」兩場會議，除了觀察世界兩大主要隱私架構規範的最新發展外，並得以進一步瞭解各國隱私主管機關及企業，在面對資料經濟所帶來的機會與對個人隱私的挑戰時，所各自提出的因應策略與規劃。相關會議重點及可供參考的建議，一併臚列如下：

一、關於 APEC 架構下的跨境隱私保護規則（CBPR）體系，我國目前已提交相關申請加入的文件，但值得注意的是，新加坡在申請加入 CBPR 的同時，亦一併申請加入資料處理者之隱私承認（Privacy Recognition for Processor，PRP）體系。在企業已紛紛提出對於資料處理者認證機制的需求之際，我國也應積極將申請加入 PRP 的必要性納入評估，以更貼近產業面的需求。

二、關於歐盟於今年 5 月 25 日施行的一般性個人資料保護規則（GDPR），從觀察此次會議中相關隱私主管機關的態度可以發現，在相關規範的解釋與未來的執法面上，歐盟仍維持相當開放且彈性的立場，並不以處罰為唯一手段。因此我國企業在評估上，雖應有所準備，但不需過於恐慌而急於在法規遵循上尋求要「一步到位」。如同法國國家資訊自由委員會主席 Isabelle Falque-Pierrotin 所強調的，GDPR 的施行只是學習的開始，而我國個人資料保護法主要參考歐盟過去指令時代的規範所訂定（除了關於個人資料國際傳輸部分，應特別注意 GDPR 採取原則禁止、例外許可之規定係與我國完全相反），企業應先從檢視對於我國個資法的落實情形做起，再持續觀察 GDPR 施行後，歐盟個人資料保護委員會對於包含適用範圍等相關爭議所公布的各該解釋或指引，並依據該等官方資料加以調整法規遵循的準備，相信是最能達成事半功倍效果的最佳路徑。

三、 最後，由於本會所掌理的通訊傳播事項，與 E-Privacy Regulation 的適用範圍係密切相關，因此該規則未來將如何發展，亦值得我們密切注意，以在未來修法時加以納入考量，俾將我國有關通訊傳播產業的隱私規範與國際規範接軌，以協助降低企業在經營上的法遵成本，以利其開拓國際市場的商機。