調　查　報　告

壹、案　　由：113年9月，美國聯邦貿易委員會（FTC）發布報告揭露科技公司大規模蒐集個人資訊隱私之嚴峻情勢，而國內公私部門亦屢傳資訊隱私與個人資料相關爭議及隱憂，究我國資訊隱私之保障及規範是否適足？111年憲判字第13號判決之續處情形及與先進國家之接軌情形各為何？均有深入瞭解之必要案。

貳、調查意見：

本案經調閱行政院個人資料保護委員會籌備處（下稱個資會籌備處）、人權及轉型正義處(下稱行政院人權處)、數位發展部(下稱數發部)、交通部及國家發展委員會(下稱國發會)、國家通訊傳播委員會(下稱通傳會)等機關卷證資料，已調查完畢，臚列調查意見如下：

一、我國個人資料保護法(下稱個資法)規定，「可直接或間接識別個人」之資料，始為個資法所規範之個資；惟現今網路資通訊技術發達，諸多用戶行為數據等數位資料如Cookies[1]或Tracking pixel[2]等，雖然並非以直接或間接識別個人為主要目的，惟其蒐集、追蹤使用者行為活動，並傳輸伺服器及第三者分析之特性，實有侵害個人資料自主控制權等隱私權之虞，更可能淪為業者商業行銷、營利甚至認知操作使用。歐盟、美國等先進國家有鑒於此，已建置「電子隱私指令」

[1] 按Google Chrome瀏覽器定義；「您造訪過的網站會建立稱為Cookie的檔案。Cookie會儲存造訪過程的相關資訊，提供更便捷的上網體驗。舉例來說，網站可以讓您保持登入狀態、記住網站偏好設定，並提供與當地相關的內容。」

[2] 按照Meta定義，「您可以使用 Meta像素來追蹤網站訪客的動作，也就是所謂的廣告轉換追蹤。追蹤的轉換會出現在Facebook廣告管理員和Facebook事件管理工具中，可用來分析轉換漏斗的有效性，並計算廣告投資報酬率。」https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking/

(EPD)及「加州消費者隱私權法案」(CCPA)及其他複式規範構成之完整治理環境，並有「無效同意」及「退出權」等維護個人資料自主控制權之制度設計。然而，我國近期雖已推動籌設個人資料保護委員會及修訂個資法，用戶行為數據等資訊隱私權之治理卻尚未納入研議範疇，機關權責亦未臻明確，難以充分保障資訊隱私權，亟需行政院協調並督同個資保護及相關目的事業主管機關檢討改進。

(一)根據美國聯邦貿易委員會(Federal Trade Commission，下稱FTC)於2024年[3]9月發表的「A Look Behind the Screens」報告[4]指出，社群媒體和影音串流服務(Social media and video streaming services，下稱SMVSSs)業者普遍進行大規模的用戶行為數據收集、追蹤與利用，其收集範圍不僅限於平臺內部，還擴及平臺外部及數據代理商(Data Brokers)，同時缺乏足夠的隱私保護措施，已形成資訊隱私權的威脅及風險，茲將報告內容摘要如下；此外，捷克眾議院副議長Jan Bartošek受邀於2025年臺灣資安大會演說時亦表示：「**我們不是社群媒體的客戶，我們是商品；它們監視我們的行為，數位平臺利用我們更甚於我們利用它們**」，並指出用戶行為數據遭武器化而威脅民主法治社會，對該等威脅及風險的描述更為明晰。

1、SMVSSs的主要業務模式依賴於向其他企業銷售廣告服務，雖然對終端用戶而言通常是免費的服務，但消費者實際上是透過個人數據和資訊來付費。

---

[3] 我國事務以民國年表示，外國事務則以西曆紀元表示。

[4] FTC.2024.*"A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services"*，網址：https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services

該等業者實現「數據變現」的核心在於收集和彙整大量的用戶和非用戶數據，其來源及內容包括：

（1）用戶直接輸入的資訊（例如個人檔案資訊）。

（2）被動收集的資訊，例如IP地址、設備資訊，以及用戶在平臺上的互動（如按讚、搜尋、觀看紀錄）。

（3）平臺外活動： 透過將廣告技術（如Tracking pixel[5]、SDKs[6]）嵌入廣告商的網站或應用程式，收集用戶在平臺外的詳細活動和行為。

（4）Cookies技術：FTC將Cookies視為「個人資訊」的持續性識別碼(Persistent Identifier)，為用戶數據的一部分，其內容可能包括設備ID、IP位址、瀏覽器設定、設備元數據(Meta Data)以及位置資訊等。

（5）第三方數據：許多擁有數位廣告服務的業者會從數據代理商（Data Brokers）和其他第三方購買數據集，該等數據可能涉及家庭收入、地理位置和興趣等屬性。

2、FTC報告認為該「數據變現」模式對用戶的隱私權構成嚴重的威脅，理由如下：

（1）持續追蹤的規模與不透明性：業者進行大規模數據收集，追蹤用戶在平臺內外的行為。許多用戶可能不知道他們的每一次點擊、搜尋和行動都被收集、記錄和儲存，或被用於廣告目的。

（2)敏感資訊的收集：追蹤技術(如Tracking pixel)

[5] Tracking pixel：像素追蹤代碼通常為1x1像素的透明圖像，可放置在廣告、電子郵件或網頁中。當顧客到訪網站或開啟電子郵件就會觸發這些像素追蹤代碼，把相關數據傳送到廣告平臺（詳閱https://www.fimmick.com/online-ads/online-ads-types-of-tracking-cookies-pixel-utm-blog/）。

[6] Software Development Kit，指軟體開發套件，可將用戶資訊收集功能嵌入套件內，使應用程式(App)具備用戶資料收集功能。

能夠在用戶不知情或未經同意的情況下，傳輸包括健康狀況、敏感網站搜尋和問卷回應等敏感的個人數據。

（3）預設同意使用數據：業者傾向於預設使用用戶和非用戶的資訊來驅動演算法，而非要求用戶明確選擇同意（opt-in）。

(二)茲將各國現行治理模式盤點如下：

1、有關Cookies之規管，歐洲聯盟(下稱歐盟)主要透過「電子隱私指令」(ePrivacy Directive，下稱EPD)治理：

（1）EPD指令第5條第3項規定被稱為「Cookies法」，規範該技術使用之相關具體規則(不論是第一方或第三方Cookies)，且因EPD指令提供更具體的規則，故與歐盟一般資料保護規則(General Data Protection Regulation，下稱GDPR)相較，符合特別法優先一般法之原則而優先適用。

（2）在權責方面，有別於GDPR由司法總署提案，EPD指令之修訂係由「通訊網路、內容和技術總局(Directorate General for Communications Networks，Content and Technology，下稱DG CONNECT)」負責提案，目前已於2017年提送「電子隱私規則(ePrivacy Regulation)」至歐盟議會與理事會審議中。

2、英國於脫離歐盟前，亦因適用上開EPD指令，而於英國個人資料保護法（Data Protection Act 2018，下稱英國個資法）外，另行制定「隱私與電子通訊條例(The Privacy and Electronic Communications Regulations，PECR)」，該條例

第6條規範有關Cookies技術。

3、美國「加州消費者隱私法案」(California Consumer Privacy Act，下稱CCPA)[7]：

（1）**CCPA明確將「Cookies」定義為「唯一標識標誌」(Unique identifier)或「唯一個人識別碼」(Unique personal identifier)的一種**。

（2）「唯一識別碼」或「唯一個人識別碼」是指一種持久性的識別碼，可用於識別某位消費者、一個家庭，或一個與消費者或家庭有關聯的裝置，其識別效力可跨時間及不同服務持續存在。

（3）除**Cookies外**，識別碼尚包括但不限於：裝置識別碼、網際網路協定位址（IP位址）、網頁信標、像素標籤、行動廣告識別碼或其他類似技術；客戶編號、唯一化的假名或使用者別名；電話號碼，或其他可用於識別特定消費者、裝置、或與消費者或家庭有關聯之實體的持久性或機率性識別工具。

（4）消費者則有知情權(right to know)、存取權(right to access)、刪除權(right to delete)和拒絕販售權(right to opt-out of sale)等種種權利。

4、在韓國廣播通訊委員會主管之《資訊通信網利用促進及資訊保護法》及韓國個人資料保護委員會

[7] “Unique identifier” or “unique personal identifier” means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, “family” means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

(PIPC)主管之《個人資料保護法》(PIPA)，雖未明定Cookies為個資，但對Cookies仍有「存取權限」、「告知」、「使用者同意」及「行政調查」等等設計。

5、至於加拿大、澳洲、巴西、日本及中國等國家，對Cookies之規範多數係以「與其他用戶行為數據結合進行剖繪」及「定向廣告」之角度切入治理。

(三)個人資訊隱私權於憲法第22條之保障內容：

1、司法院釋字第603號解釋理由書肯認隱私權為憲法第22條所保障之基本權：「……隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第22條所保障」，其中就個人資訊隱私權進一步闡明：「個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權，惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第23條規定意旨之範圍內，以法律明確規定對之予以適當之限制」。

2、林子儀大法官於司法院釋字第603號解釋之協同意見書表示：

（1）將資訊隱私權所欲保護之對象限於個人私密之資訊，毋寧過分限縮，而不能因應現今資訊科技發展所可能對個人造成之侵害……隱私權

保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。

（2）人民面對國家資訊蒐集的無奈之一是，一旦個人資訊脫手，個人其實已經很難再有控制之可能。且除非具體問題發生，否則人民對於機關內部的資訊保管及運用情形，實則一無所悉，也無從確認國家是否良好地保護其資訊安全並予以正當使用。

3、憲法法庭111年憲判字第13號判決(全民健康保險資料庫案)進一步闡明資訊隱私權如下：

（1）資訊隱私權之保障核心既在於保護個人對資料之自主控制權，則個資之蒐集、處理及利用，即應以取得當事人同意為原則。

（2）憲法第22條個人資訊隱私權保障當事人原則上應有事後控制權，且當事人就獲其同意或符合特定要件而允許未獲當事人同意而經蒐集、處理及利用之個資，仍具事後控制權，不因其曾表示同意或因符合強制蒐用要件，當事人即喪失請求刪除、停止利用或限制利用個資之權利。

（3）**<u>個資若經處理，依其資料型態與資料本質，客觀上仍有還原而間接識別當事人之可能時，無論還原識別之方法難易，若以特定方法還原而可間接識別該個人者，其仍屬個資</u>**。當事人就此類資料之自主控制權，仍受憲法資訊隱私權之保障。反之，經處理之資料於客觀上無還原識別個人之可能時，即已喪失個資之本質，當事人就該資訊自不再受憲法第22條個人資訊隱私權之保障。個資法第2條第1款以「得直接或間接識別該個人」為是否屬個資之標準，即在

表彰上開憲法對個人資訊隱私權保障界限之意旨。

（4）由個資法或其他相關法律規定整體觀察，欠缺個人資料保護之獨立監督機制，對個人資訊隱私權之保障不足，而有違憲之虞，相關機關應自本判決宣示之日起3年內，制定或修正相關法律，建立相關法制，以完足憲法第22條對人民資訊隱私權之保障。

(四)前開運用Cookies等新興科技工具對用戶行為數據等個人資訊之蒐集、處理與利用行為，係不同程度及規模侵害資訊隱私權等基本權利。若為公務機關所為之行為，縱然認定非屬個資法所規範之個資而不受該法規範，惟依憲法法庭111年憲判字第13號判決意旨，至少該等個人資訊之取得，應以當事人同意為原則，或至少應盡告知義務，俾利當事人得選擇退出權，若為對個人之重大侵害，應符合法律保留原則，自不待言。現今法規範密度嚴重不足，主管機關宜有更積極之法制作為，以維護個人資訊隱私權等憲法及國際公約[8]保障之基本權利。

(五)無論是公務機關或私人業者運用前開科技工具所為個人資訊之蒐集、處理與利用行為，恐衍生相關威脅及風險，前文業已敘述，我國憲法學者劉靜怡教授於「網路時代的隱私保護困境」[9]亦多有著墨，茲摘述如下：

1、例如類似Cookies之類資訊科技的運用，乃是透過拼湊種種有關網路使用者個人枝微末節的方式，勾勒出網路使用者自己根本無從預見的剖面

[8] 公民與政治權利國際公約第17條。

[9] 劉靜怡。2021年9月。網路時代的隱私保護困境。元照出版。P165-167。

圖。在面對侵害個人隱私的質疑與挑戰，使用這些資訊科技的廠商總是嘗試描繪出一幅「雙贏」(win-win situation)圖像，甚至使用網路科技從事行政行為的政府機關，也喜歡以這種雙贏說詞，例如提高行政效率、促進競爭力，甚至便利人民取得資訊等說法，來掩飾其侵犯個人資訊隱私的潛在缺陷。

2、1979年，美國聯邦最高法院在Smith v. Maryland此一判決中指出，只要是個人「自願公諸於世」(voluntarily made public)的資料，基本上便無個人隱私遭受侵犯的問題可言。但是，身處今日資訊時代，「自願」向政府提供個人資訊，或是透過「自願」撥接網路的動作，進而在網路上所從事的絕大部分活動，或許都可以解釋成是出於「自願」的。例如，在上述Cookies在與網路其他技術(如user authentication)結合之後，使用cookies的網站，對於該使用者「出於自願」的網路旅行經驗瞭如指掌；**網路使用者在網路上循何種路徑移動、從事那些網路行為，已在不知不覺中暴露無遺。這種即使是屬於「自願」，但卻根本「不知」自己相關資料正以各種形式被納入不同資料庫的情形，本質上是否違背個人尊嚴與意願的核心價值，毫無「自願」可言**，所謂「自願提供個人資訊」的定義，是否應該重新釐清，在法律論證上應該是不無討論空間的。

(六)經查，Cookies等用戶行為數據於資訊隱私權之威脅及風險已臻明確，用於商業行銷及認知操作更是氾濫，先進國家已針對資訊隱私風險制定各種法制及機制進行管理；個人資訊隱私權雖為我國憲法保

障的基本權之一，但目前唯一可用的法律工具-個資法，卻採取由目的事業主管機關「分散式管理」的制度設計，導致當**肇生任何資訊隱私疑慮時，首先就沒有機關能夠出面界定是否「得直接或間接識別該個人」而適用個資法，遑論更廣泛的用戶行為數據規管議題**。以Cookies為例，目的事業主管機關認為應通案解釋或訂定參考指引，而個資主管機關則認為須就具體個案情形而定，已形成我國在資訊隱私權保障方面的困境，相較於歐美國家已建置複式治理環境，尚持續力求精進，易言之，我國對用戶行為數據之規管及態度顯得十分落後，無異於任憑民眾隱私為業者所宰制。茲將相關機關對於Cookies及資訊隱私權之界定權責看法臚列如下：

1、個資會籌備處稱[10]:「Cookies是否為我國個資法第2條第1款所定義之個人資料，須就具體個案情形而定，尚未能一概而論」、「目前本國網站Cookies內容、同意範圍或退出權等事項，仍係由各網站設置事業之目的事業主管機關予以監管，個資會籌備處為個資法之法律解釋機關，尚無直接掌握網站監管情形等相關資訊」、「不代表對本國網站Cookies立法規範政策只能依個資法」等語。

2、數發部則稱[11]:「各機關網站Cookies管理可能衍生個資法遵之疑義，宜由個資法主管機關釋疑」，以及「有關Cookies之個資屬性、管理強度/密度、同意範圍或Opt-in/Opt-out機制等事項，數發部相關單位近年尚無與個資會籌備處進行協調溝

[10] 個資會籌備處114年4月14日個資籌法字第1140000382號函。
[11] 數發部114年4月11日數位策略字第1140006208號函。

通」等語。

3、通傳會則稱[12]:「為發展國家數據經濟之法規調適規劃，針對通案實例之適法及適用情形，應通案進行解釋或訂定參考指引」、「有關Cookies或因科技進步所涉個人資料保護等爭議，涉及我國人民個資保護之重大權益,且屬多機關之權責事項，宜由未來個人資料保護委員會滾動檢視，順應科技趨勢審慎考量是否儘速納入個資法或相關子法之修法範疇，或提出參考指引」等語。

4、交通部則稱[13]:「目前對於網站Cookies尚無相關法令明確規定與解釋,爰就航空公司網站Cookies政策與內容未有強迫性規範」等語。

(七)至於Cookies及其他資訊隱私權與現行個資法在法制上如何調和，以及短期或中長程策略等課題，相關機關於114年6月30日本院約詢時說明如下，顯示初步共識為中長期朝專法方向推動，而在短期策略方面，目的事業主管機關仍希望個資會籌備處能先以行政指導方式訂定通案性規定或指引，以利各目的事業主管機關遵循。

1、個資會籌備處鄭其昀副主任：

(1) Cookies只是一種技術，將文字檔存入終端設備，但文字檔可能是包括個資，也可能僅有非個資。國外比較法上來看,如果是能識別個人，當然適用個資法；但非個資部分如何管控，以歐盟作法，是以EPD電子隱私指令，不區分個資或非個資，採專法方式，而非個資法。就立法政策解決，日韓歐盟均是以訂立專法處理。

[12] 通傳會114年6月30日本院詢問前電子郵件查復資料。
[13] 交通部114年4月11日交科字第1145005219號函。

（2）個資會籌備處主要是針對可識別自然人資料去做規範，但是Cookies裡面是有非個資部分，所以個資會籌備處與世界各國作法一致，都是建議要有專法處理，於專法未立法前，有關個資部分，個資會成立後或能以個資法或是行政指導先行處理。

2、數發部陳怡君副司長：

（1）Cookies議題是新興議題，該政策在國外主要是由個資主政機關研議，無論未來是立專法或修正個資法，數發部都會配合辦理，通盤檢討權責範圍內業務。

（2）建議個資會籌備處可以行政指導先行，各目的事業主管機關配合辦理。

3、通傳會黃天陽副處長:電信業者是扮演郵差角色，透過網路實體層傳輸封包到終端，至於封包承載的Cookies內容為何，已經是資訊服務層上的應用。目前並沒有全面規定各網站應如何規範Cookies，至於三大電信業者網站，電信業者都有盡到告知、說明的義務，如果有通案性規定，各電信業者會配合辦理。

(八)此外在機關職權方面，「個人資料保護委員會組織法」第1條雖明定:「行政院為落實資訊隱私權保障，健全個人資料保護法制，並促進個人資料之合理利用，特設個人資料保護委員會」，惟在該會正式成立並推動資訊隱私法制之前，我國對資訊隱私權之保障僅能侷限於個資法範疇之內，對於資訊隱私及個資難以界定之灰色地帶缺乏規管，實有檢討改進之必要，均有賴個資會成立後，由行政院督同相關機關積極推動。

(九)另查，郭戎晉教授於「從個人資料保護立法談Cookies之定位、應用爭議與規範課題」[14]一文指出目前我國在Cookies的規管問題如下，益證我國個資法對於廣泛的資訊隱私權風險管理力有未逮：

1、無法強令Cookies使用以取得當事人的**有效同意**為必要，並非個資法設計存在缺漏，而是其**已逾越個資法作為個人資料保護事務普通法此一基線**。如何有效掌握並因應資訊通訊科技的進步，類型化可能侵犯個資的利用態樣，並於法制政策層面擇定合適的管理模式及明確規範，將是後續無可迴避的另一課題。

2、**有效同意相關判斷要件尚待建立**：……國內目前並未明訂(以取得當事人之)同意以明示同意為必要，**當解釋上存在默示同意之可能時，自無法要求同意表示必須達到自主性、具體且明確之程度**。合適作法當是後續於評估修正個資法同意規定時，除考量有無提升為明示同意之必要外，在決意修改為明示同意時，一併將有效同意的判斷要件納入個資法或其施行細則。

(十)以國籍航空公司網站為例，部分業者採「不同意就無法使用」之Cookies牆策略(如中華航空股份有限公司)、部分業者採預設同意(如台灣虎航股份有限公司)，亦有部分業者比照歐美規範由使用者自行設定(如長榮航空股份有限公司及星宇航空股份有限公司)，均與歐盟、英國及美國航空公司網站Cookies政策普遍符合EPD及CCPA有相當差距，顯示我國在Cookies等資訊隱私權方面全無規則可循；

[14] 郭戎晉。109年4月。從個人資料保護立法談cookies之定位、應用爭議與規範課題。東吳法律學報32:1 70-104。

交通部雖稱中華航空網站預計於115年第2季改版強化Cookies政策，然而該部也坦承：「目前對於網站Cookies尚無相關法令明確規定與解釋，爰就航空公司網站Cookies政策與內容未有強迫性規範」。

(十一)綜上，在網路資通訊技術衝擊下，單純以個資法狹隘個資定義為保護範疇的法規及制度，已不足以充分保障憲法第22條所保障之個人資訊隱私權，其威脅及風險均有FTC報告及歐美國家資訊隱私規管制度可證。然而，政府卻怠於建構資訊隱私權之治理環境，任憑民眾的網路行為數據受平臺及數據收集業者宰制，此由國內網站Cookies政策紊亂即為明顯例證，實有檢討必要，亟需行政院積極協調及督同個資保護機關及目的事業主管機關確實檢討改進。

二、歐盟「一般資料保護規則」(GDPR)是當前對資料跨境傳輸、加重企業相關責任及賦予個資當事人完整權利之最完整規範，行政院雖於107年5月24日第3601次院會已責成國發會統籌推動「適足性認定」，期使我國個資保護水準相當於歐盟而得以互相承認，進而促進數位經濟發展，惟迄至114年10月已逾7年，進度遙遙無期；反觀韓國早在2020年即設立個資獨立機關並積極修法，旋於2021年完成GDPR適足性認定，不僅凸顯我國個資保護制度之落後，亦有影響數位經濟發展之虞，核有違失，行政院責無旁貸，允應協調及督同相關部會積極檢討改進。

(一)根據行政院107年5月24日第3601次院會報告事項，國發會向時任行政院賴院長清德報告「因應歐盟『一般資料保護規則』生效之措施」，經作成決議，茲摘述如下：

1、數位經濟下，資料之價值即是商機之展現，大數據流通與資源分享也是不可逆之趨勢，除國內應做好個資保護外，全球化下個人資料流通之保護也同等重要。

2、歐盟一般資料保護規則（GDPR）即將施行，已引發全球高度關注，由於歐盟為我第五大貿易夥伴，第一大外資來源，雙邊經貿往來一向密切，GDPR之施行，將對我國在歐盟營運或從事對歐業務之企業產生相關影響，政府部門應密切關注後續發展，妥為因應。

3、我國個資法與GDPR就個資保護基本原則均有相關規範，但我國個資法未設單一主管機關而採分散管理制度，後續請**國發會儘速成立個資保護專案辦公室**，以作為部會間協調整合之平臺，**積極整合**各部會辦理GDPR相關因應事宜，並研議個資法之主管機關。

4、協助企業因應GDPR施行後可能造成之衝擊，對內部分，請各部會積極協助提供所轄產業相關輔導與諮詢服務；對外部分，**請國發會統籌相關部會儘速與歐盟洽商適足性認定事宜**，期藉由各部會之分工合作，早日完善我國公私部門有關GDPR之準備工作。

(二)次查，時任國發會副主任委員鄭貞茂於108年Taiwan FinTech產業策略論壇說明略以：「**國發會與歐盟談判進展順利，希望在2020年獲得GDPR適足性認定**」，並稱：「一旦臺灣通過歐盟GDPR適足性認定，就可以讓臺灣境內企業，自由與歐盟間進行個資跨境傳輸。這對臺灣企業來說，就不用各別與歐盟申請符合GDPR規範，可以降低許多企業的成本」等語。

(三)再查行政院112年12月5日新聞稿[15]，時任行政院院長陳建仁表示：「……期許籌備處儘速推動建置個人資料保護委員會的法制主管機關，全力維護民眾個資權益，讓臺灣的個資保護**符合國際水準**」。

(四)另查，國發會109年委託「達文西個資暨高科技法律事務所」研究「韓國個人資料保護法制因應GDPR施行之調適」報告[16]摘要如下，顯示該國在推動GDPR適足性認定及個資保護之積極情形:

1、韓國政府為通過歐盟GDPR之適足性認定，於2020年1月由韓國國會通過新修正之「個人情報保護法」、「信用情報法」及「情報通信網法」，並於2020年8月5日正式施行。此次修法以「個人情報保護法」作為明定個人資料之具體判斷基準，並將個人情報保護委員會提升為中央行政機關，使其具有獨立監督個人資料色彩的地位，藉此達到GDPR對於個資監管機關獨立性之要求，再參考GDPR假名化而引進「假名情報」的概念，特別的是無須當事人同意之「假名情報」得被運用於科學研究中，韓國各界認為此次修法將有助於促進新技術之開發，使韓國商業發展更加活絡。

2、本次修法整合了韓國過去對於個資保護過於混亂的現象,預期未來韓國對個資的保護更具有效性、統一性。鑒於我國現正積極申請通過歐盟GDPR適足性認定，有必要深入了解正在申請適足性認定之國家的作法。

(五)惟查，我國GDPR適足性認定之推動，前由國發會主

[15]https://www.ey.gov.tw/Page/9277F759E41CCD91/fec13417-8b26-466f-a59d-cc1aaee75a25

[16] 達文西個資暨高科技法律事務所(國發會委託)，2020，〈韓國個人資料保護法制因應GDPR施行之調適〉，網址https://www.ndc.gov.tw/nc_1871_34458

責，並於108、109年及110年與歐盟召開諮商及視訊會議研商，但當時無法滿足個人資料保護獨立機關之條件，復為因應憲法法庭111年憲判字第13號判決，行政院於112年3月2日第3845次會議決定設立個資保護獨立監督機關，續於112年7月31日召開「研商個人資料保護委員會籌備處籌設事宜」會議，要求國發會及相關單位儘速成立籌備處[17]。至114年3月27日，行政院第3945次會議通過「個人資料保護委員會組織法」草案，始於組織法第2條明定「跨境傳輸個人資料保護之評估、研析、協調、限制及執行」為該會職掌之一，然迄114年10月為止，個資會組織法尚未通過立法院審議，距行政院於107年5月宣示推動GDPR適足性認定已逾7年，仍遙遙無期，足見政府態度消極，未來應有更積極作為：

1、行政院於114年6月30日本院約詢時表示，個資會籌備處現階段主要任務為推動個資會成立的總體規劃事宜，俟未來個資會成立後，後續將通盤修正研議隱私權及個資保護涉及之修法議題。行政院並洽國發會說明，該會已完成GDPR及適足性諮商相關業務移交。

2、個資會籌備處另於114年6月30日本院辦理約詢前查復表示：

（1）韓國個資保護獨立機關-個人資料保護委員會（PIPC）是於2020年8月成立，而歐盟執行委員會是於韓國個人資料保護委員會成立並有效運作後，於2021年6月始啟動關於韓國適足性認定的審批程序，並於2021年12月始通過韓國適足性認定之決定。

[17] 112年12月5日正式成立。

（2）依國發會過往洽商過程可知，歐盟最為關切我國有無設立個資保護獨立機關。蓋依歐盟GDPR第45條第2項第(b)款規定，歐盟執委會於評估第三國保護程度適足性時應考量之因素，包含該第三國國內有1個以上獨立監管機關之存在且須有效運作，以確保及執行資料保護規則之遵守，包括充足之執行權，以協助及建議資料主體行使其權利,並與會員國之監管機關合作，此為最關鍵之條件。

（3）在賡續洽商GDPR「適足性認定」前，我國須先籌設個資會，至於有關我國是否繼續推動GDPR「適足性認定」及其計畫、期程，因涉及國家整體之重大政策，允宜俟未來個資會成立及賦予相關職權有效運作後，由該會以個資法主管機關地位會商相關機關評估後續推動事宜。

(六)綜上，歐盟「一般資料保護規則」(GDPR)是衡量一個國家的個人資料保護及資訊隱私權保障是否符合先進國家水準的量尺之一，相較韓國於GDPR施行後2年完成個資保護獨立機關籌設，再於隔年即完成GDPR適足性認定，總計約3年半即趕上先進國家水準；反觀我國於107年宣示推動，迨至114年10月仍未完成個資保護獨立機關籌設，違失至臻明確，行政院責無旁貸，應協調及督同相關部會積極檢討改進。

三、為兼顧資訊隱私權保障及資料加值運用需求，「隱私強化技術」已然成為確保資料使用安全性的重要工具。經查數發部雖已完成「隱私強化技術應用指引」，惟其在明確性、合規性、標準化等均有不足，難以促使公私部門積極導入，並有造成後續數位經濟及資料運

用困境及隱私爭議之虞。行政院允宜協調技術面及法制面所涉相關部會，強化「隱私強化技術」之標準及合規性。

(一)依據數發部研擬「隱私強化技術應用指引」[18]已指出，隨著資通訊科技的進步，資料的數量及複雜度迅速增長，政府公部門或民間企業在兼顧隱私保護及資料合理利用之前提下，不可避免地須導入隱私保護措施或隱私強化技術，以增進資料當事人之信任，降低資料利用之風險。顯見「隱私強化技術」將成為未來具隱私疑慮資料進一步加值應用所必須具備的技術，茲將其要旨摘述如下：

1、隨著人工智慧、巨量資料探勘等技術之高速發展，傳統隱私強化技術，如直接刪除辨識碼方法或k-匿名化等方式，正面臨隱私保護有效性的挑戰。有鑑於此，國際上陸續推動新興隱私強化技術之政策與法規制定，如聯合國於 2020 年成立聯合國隱私強化技術實驗室（UN PET Lab），並與美國人口普查局(US Census Bureau)、荷蘭中央統計局（Statistics Netherlands)、義大利國家統計局（Italian National Institute of Statistics)以及英國國家統計局(UK's Office for National Statistics）共同合作，展開測試計畫，藉由隱私強化技術的導入，促進資料共享並同時兼顧資料之安全性與合規性。

2、廣義上隱私強化技術可泛指所有用於保護資料隱私或資料機敏性之技術方法。較為傳統的技術包括抑制/編修、遮罩、記號化、雜湊化等，而近

[18] https://hackmd.io/@petworks/rJ-UOh9Rn/https%3A%2F%2Fhackmd.io%2F%40petworks%2FSyE8LXbd6

期較具指標性的技術則包括差分隱私、合成資料、聯合學習、同態加密等，更強化保障資料在使用階段(in use)的隱私安全，也更著重於為時下資料應用場景所面臨之隱私挑戰，衡平隱私保護與資料運用需求，透過技術方法降低直接利用原始資料所衍生之風險，同時保有資料可用性。

(二)有鑑於資訊隱私權之法遵要求日益具體而繁複，「隱私強化技術」之導入，勢將成為組織保障資料安全及資訊隱私權的重要法遵證明；惟查，我國目前尚未將「隱私強化技術」法制化，而數發部所研擬之「隱私強化技術應用指引」僅屬指引性質，在明確性、合規性、標準化等均有不足下，難以促使公私部門積極導入，數發部雖曾向個資會籌備處提出「個資法」修法意見，惟未見於114年3月27日行政院第3945次院會通過之個資法部分條文修正草案(立法院業於114年10月17日三讀)，有賴行政院協調技術面及法制面相關部會，強化「隱私強化技術」之標準及合規性：

1、數發部說明，按照「隱私強化技術應用指引」，個資法第2條第1款規定，個人資料係指各種得以直接或間接方式識別個人之資料，為避免個資當事人人格權受侵害，其蒐集、處理及利用過程皆受個人資料保護法規範。因此，如將個資進行去識別化等技術處理，使資料無法用於直接或間接識別當事人，即非受個資法所保護之客體（111年憲判字第13號判決參照）。

（1）歐盟GDPR個人資料處理之安全性（第25條、第32條）及英國Data Protection Act 2018皆規範有關個人資料處理之權利及自由之保護，須

採取適當之技術性或組織性措施，亦即，控管者應採取符合「設計（by design）與預設（by default）資料保護」之規則與措施。而**隱私強化技術之採用即可作為組織遵從GDPR及Data Protection Act 2018之佐證**。

（2）現行具指標性之隱私強化技術歸納為以下3類：第1類為「改變原始資料以減少或移除個人識別資訊」，如差分隱私、合成資料；第2類為「對原始資料進行保密性處理後進行操作」，如同態加密、安全多方運算（包含私有集合交集）、零知識證明；第3類為「透過設計系統運算機制達到資料保護效果」，如聯合學習、可信執行環境。

（3）然而經隱私強化技術處理後之個人資料，未必能與去識別化之資料劃上等號，例如：經差分隱私處理後之個人資料，若設定之「隱私預算」較高，所含可識別個人之資訊亦可能較高，因而再識別之風險較高；因此，導入隱私強化技術是否就符合111年憲判字第13號判決所稱「……無論還原識別之方法難易，若以特定方法還原而可間接識別該個人者，其仍屬個資」，仍待進一步研析。

（4）依據數發部查復，綜觀國際歐盟、日本等立法例，例如歐盟GDPR就去識別化係依資料加工程度之高低，區分為匿名化及假名化；日本個資法則已規範匿名加工資料處理等程序及措施。現行**我國個資法並未就匿名化及假名化予以解釋或規範，因此實務上各界難以具體界定去識別化之合規情境**，進而影響侵害行為之發現

及認定。

（5）同時，部分隱私強化技術屬於新興科技，尚未發展統一之技術標準、國際規範或得以驗證其隱私保護效力之機制，有賴技術面之機關持續研議強化。

2、根據數發部函復，該部於113年12月及114年3月向個資會籌備處提出個資法修法意見，建議明定去識別化、假名化或匿名化或可資識別之規定，以使個資法規框架趨於完備。惟查，相關內容未見於114年3月27日行政院第3945次院會所通過之個資法部分條文修正草案(立法院於114年10月17日完成三讀程序)。

(三)另查，「台灣人權促進會」(下稱台權會)於113年5月30日發表「位置足跡就是隱私，應釐清電信資料利用要件」[19]指出電信信令之利用涉及隱私權爭議。經查通傳會雖已要求行動寬頻服務業者修訂服務契約條款，惟該契約條款有關「隱私強化技術」之技術規範，僅空泛說明「包含但不限於抑制、泛化、擬匿名化、隨機、彙集等等」，並未針對不同資料特性指定適當技術或最佳實踐(Best practice)。換言之，目前電信資料的「隱私強化技術」尚欠技術性的合規（Compliance）規範，以致於難以確保電信資料在經過某種「隱私強化技術」處理後，即符合111年憲判字第13號判決「……無論還原識別之方法難易，若以特定方法還原而可間接識別該個人者，其仍屬個資」之要求，益證國內目前僅以指引型式推廣「隱私強化技術」，尚有值得精進之處，

[19] 台權會，2024，〈位置足跡就是隱私，應釐清電信資料利用要件〉網址：https://www.tahr.org.tw/news/3537

析論如下：

1、茲將台權會訴求摘述如下：

（1）台權會建請電信主管機關、數位廣告與行銷業者之主管機關、政黨，應釐清及說明包含手機信令分析、基地台位置分析、Beacon室內定位等資料蒐用現況、法律依據等，並檢視其已否落實消費者的知情同意與退出權利。

（2）本次事件[20]凸顯臺灣不少資料蒐用者長期存在「只要資料不是個資，就能愛怎麼用就怎麼用」的邏輯，既無視於移除姓名或身分證字號本身，並不等於讓資料變成「不是個資」，也無視於「去識別」本身也是一種需要取得合法基礎的一種資料處理方法。

2、對此，通傳會查復說明，該會因應立法院第11屆第1會期交通委員會第15次全體委員會議委員質詢，已於113年6月18日以行政指導並邀集三大行動寬頻服務業者研商修正事宜，經三大行動寬頻服務業者分別於同年7月上旬檢送變更契約條款作業，且於同年8月12日核准在案。該會復於同年8月29日以通傳平臺字第11300300680號函復三大行動寬頻服務業者修正其服務契約條款內容，以及督促業者保護個資措施。

3、然而，通傳會經研析數發部公告之「隱私強化技術應用指引」內容，考量去識別化技術及適用驗證標準與機制甚多，擬修正通傳會安維辦法部分條文，其修正重點為「處理無從識別用戶個人資料應揭露其處理方式」、「處理無從識別用戶個

[20] 民進黨政策會執行長王義川113年5月27日在政論節目上表示，透過電信資料能比對國會濫權抗議現場民眾與519民進黨部前集會、今(113)年初總統大選前晚造勢活動參與者群眾屬性之異同。

人資料應取得國內或國際相關標準管理驗證機制(如CNS29100-2)」等規定，以督促業者落實個資料法遵義務，並利配合國家數據經濟發展。惟按「國家通訊傳播委員會委員會議審議事項及授權內部單位辦理事項作業要點」第15點規定，**通傳會因目前委員人數未達委員總額過半數，暫難執行授權審議之事項**，將待委員人數確定後，續行辦理後續法制作業程序。

(四)綜上，「隱私強化技術」是在保障資訊隱私權的前提下仍能充分發揮資料價值的重要配套，惟目前數發部所研擬的「隱私強化技術應用指引」僅屬指引層級，法律位階與管制強度明顯不足，在明確性、合規性及標準化等方面更不足以提供公私部門導入時遵循，以行動寬頻服務業者所收集的電信資料為例，其對「隱私強化技術」的技術規範條款過於空泛，難以確保所採取之技術可充分保障用戶資訊隱私權。爰此，如何使「隱私強化技術」成為展現資料價值及發展資料經濟的護身符，有賴行政院協調技術面及法制面所涉相關部會並積極推動。

參、處理辦法：

一、調查意見，函請行政院督同個人資料保護委員會籌備處、數位發展部、國家通訊傳播委員會及交通部等有關部會確實檢討改進見復。

二、調查意見，送請國家人權委員會參處。

三、調查報告經委員會討論通過後公布調查意見。

四、檢附派查函及相關附件，送請交通及採購委員會處理。

調查委員：賴鼎銘

高涌誠