

# 行政院及所屬各機關因公出國人員出國報告書

(出國類別：開會)

## 出席 2019 年秋季 Line 及 Intertrust 隱私高峰會

( Line X Intertrust Privacy Summit Fall 2019 )

服務機關：國家發展委員會

職稱／姓名：副主任委員／鄭貞茂

職稱／姓名：高級分析師／楊耿瑜

出國地區：法國巴黎

出國期間：108 年 10 月 26 日 - 108 年 10 月 31 日

報告日期：108 年 12 月 25 日

## 公務出國報告提要

出國報告名稱：出席 2019 年秋季 Line 及 Intertrust 隱私高峰會

( Line X Intertrust Privacy Summit Fall 2019 )

頁數 33 含附件： 是  否

出國計畫主辦機關/聯絡人/電話

國家發展委員會/楊耿瑜/02-2316-5300 分機 6806

出國人員姓名/服務機關/單位/職稱/電話

鄭貞茂/國家發展委員會/副主任委員/02-2316-5300

楊耿瑜/國家發展委員會/資管處/高級分析師/02-2316-5300 分機 6806

出國類別： 1 考察 2 進修 3 研究 4 實習  5 其他：開會

出國期間：108 年 10 月 26 日 - 108 年 10 月 31 日 出國地區：法國巴黎

報告日期：108 年 12 月 25 日

分類號/目：資訊管理/資訊政策

關鍵字：Data Economy、Digital Economy、Data Protection、Privacy Protection

## 內容摘要

Line 股份有限公司與 Intertrust 科技股份有限公司( Intertrust Technologies ) 合作，訂於 2019 年 10 月 29 日於法國巴黎舉辦 2019 年秋季 Line 及 Intertrust 公司隱私高峰會 ( Line X Intertrust Privacy Summit Fall 2019 ) ，會議主題為「以資料驅動經濟發展的隱私保護作為」( Protecting the integrity of the data-driven economy ) 。國家發展委員會鄭貞茂副主任委員應邀出席高峰會擔任與談貴賓，向國際說明臺灣推動數位經濟的政策方向與相關因應措施。

另安排拜訪法國興業銀行總部及兆豐商業銀行巴黎分行，並參觀巴黎新創基地 Station F ，藉以了解歐洲地區經濟發展趨勢、金融服務現況，以及協助新創業者的服務環境與相關措施。

## 目錄

壹、目的.....	1
貳、過程.....	2
參、2019年秋季 Line X Intertrust 隱私高峰會 .....	2
一、計算機科學與隱私.....	2
二、個人資料的擁有權.....	5
三、歐盟「一般資料保護規則」的公私組織衝擊與因應 .....	9
四、健康照護與隱私保護.....	15
肆、拜會活動.....	20
一、法國興業銀行.....	20
二、兆豐國際商業銀行巴黎分行.....	21
三、法國巴黎新創基地 Station F.....	23
伍、心得及建議 .....	25
一、取得歐盟「一般資料保護規則」適足性認證.....	25
二、推動資料經濟新模式-個人資料自主使用(My Data) .....	25
陸、附錄.....	27

## 壹、目的

近年來政府、學者及民間團體對於數位時代可能侵犯個人隱私權之研究與討論範圍，多數聚焦於政府、企業應用數位科技監看、蒐集民眾日常行為的相關舉動，例如巨量資料分析、人臉辨識、指紋辨識等。過去，數位科技尚未普及至日常生活時的隱私保護措施，現在已完全無法發揮效果，數位科技完全破壞過往日常生活中保持的隱匿性作法。縱然應用數位科技監看民眾隱私的爭議值得各界投注心力關心，現在，更需要重視數位科技與數位經濟發展趨勢下，民眾隱私保護的作為必須更深入的檢討與設計更有效率的保護作為。

Line 股份有限公司(以下簡稱Line)為全球即時通訊軟體上市公司，在臺灣、日本、泰國等亞洲國家具有相當大的市占率。根據 Line 官方資料指出，該公司雖然以即時通訊軟體起家，現在正以數位化多元服務方式，進軍線上遊戲、電子支付、電子商務，在臺灣甚至取得純網銀執照，揮軍進攻數位金融產業。有鑑於數位科技衍生的隱私權保護之衝擊可能限制 Line 的發展契機，Line 自 2017 年起與美國知名資安與隱私保護的科技公司 Intertrust Technologies 合作，辦理資訊安全與隱私保護的國際高峰會議，廣邀國際專家、學者共商資訊安全與隱私保護的倫理、法制、管理與技術等相關議題。

2019 年秋季隱私高峰會議地點安排於法國巴黎，高峰會主題為「以資料驅動經濟發展的隱私保護作為」( Protecting the integrity of the data-driven economy )，邀請二十餘位來自臺灣、日本、美國的產、政、學領域專家出席高峰會發表專業意見，並與現場出席者交流數位經濟時代下的隱私保護議題。我國為 Line 業務的重要市場，且臺灣推動數位經濟發展具有顯著成果，Line 總公司特別邀請國家發展委員會鄭貞茂副主任委員擔任與談貴賓，向國際說明臺灣推動數位經濟的政策方向與各項因應措施。

本次出國行程安排除參加 2019 年秋季 Line 及 Intertrust 公司隱私高峰會外，另拜訪法國興業銀行總部交流討論國際經濟發展趨勢；另由我國駐法代表

處經濟組同仁安排，拜訪兆豐商業銀行巴黎分行了解國銀在歐洲地區經營情形，並參觀法國巴黎規模最大的新創基地 Station F，藉以了解法國協助新創業者的服務環境與相關措施。

## 貳、過程

2019 年 10 月 28 日(星期一)

由鄭貞茂副主任委員率隊拜訪法國興業銀行總部全球銀行與資訊部副主管 Alvaro Huete 先生，訪談國際經濟發展趨勢。下午在我國駐法代表處經濟組同仁協助下，拜訪兆豐商業銀行巴黎分行，並參觀巴黎市規模最大的新創基地 Station F。

2019 年 10 月 29 日(星期二)

出席「2019 年秋季 Line 及 Intertrust 公司隱私高峰會」，會議聚焦於資料驅動經濟發展之隱私保護具體作為，鄭副主任委員擔任高峰會與談人，並發表臺灣推動數位經濟之政策方向與具體作為，報告主題為「數位經濟時代下臺灣政府擔任的角色與使命」( The role and mission of Taiwanese Government in the digital economy age )。

## 參、2019 年秋季 Line X Intertrust 隱私高峰會

本次會議座談議題圍繞在數位經濟發展過程中，個人隱私保護的威脅與解決問題的方案、隱私保護法規、管理與技術層面的創新研究，以及最新的實務案例分享。

### 一、計算機科學與隱私

因應數位科技為國家與社會整體帶來民眾隱私的變化衝擊，並且尋求資通訊產業創新發展的契機，參與座談之技術專家 Maher 先生在高峰會上分享有關區塊鏈技術在隱私保護應用的研究情形，他認為保護民眾隱私的第一步，必須要識別「當事人身分」，亦即金融機構最重視的工作之一

「瞭解你的客戶」(Know Your Customer)。Mather 先生認為區塊鏈技術的「零知識證明」(Zero-Knowledge Proofs)以及去中心化信任機制，可以避免過往要識別當事人身分而獲取太多身分以外的個人資料(例如金融機構辨識當事人只需要知道「當事人」即為眼前之人，不需要拿身分證知道當事人的統編字號、住址、生日等個人資料)，進而保護客戶的機敏性資料安全性和隱私性。

普廉斯頓大學 Tarjan 教授從密碼學基礎介紹近兩年在資安界研究的「白箱加密」(White-box Cryptography)資料加密技術。Tarjan 教授解釋，過去網際網路尚未普及的年代，駭客大多由外而來，所以資料加密方式主流為採「黑箱加密」，外界無法探知黑箱加密的運作方式，因此黑箱加密具有效果。然而，現在駭客經由網際網路，更容易駭入資訊系統內部，一旦探知黑箱內部加密運作方式即可輕易竊取資訊。有鑑於此，資安界傾向採用「白箱加密」，透過複雜的數學演算法讓資料竊取者拿到了加密資料，仍舊無法解讀資料內容，他更鼓勵軟體開發公司公布加密機制，集眾人力量一起檢驗白箱加密的安全性。

明尼蘇達大學數學學院 Odlyzko 教授從資安風險的角度陳述他獨到的見解。他認為資安事件可以是由駭客攻擊造成，也有可能是自然事件(例如讓地球上的電子設備損壞的太陽日冕物質拋射)，更有可能是因為人為非過失的疏忽而導致風險，例如資訊系統程式編碼邏輯失誤、操作錯誤或資訊系統複雜的運作過程而產生非預期的預作異常。要全面預防所有資安事件帶來的災害是不可能的任務。因此，Odlyzko 教授指出，目前政府與企業大量使用的舊式防護技術已經逐漸失去原有的功效，如防火牆面對越來越多加密的封包而難以辨識封包特徵，另一個原因企業的整體數位環境已經大幅度變化，企業的資訊系統與服務供應商、合作夥伴和客戶的資訊系統，以及員工自己擁有的資通訊設備交雜在一起，傳統「在組織內部建立層層資安防護」的概念，已無法滿足雲端化服務的現況。政府或企業在資安

防護上，不應該只重視「數位空間安全」，不應該持續大量投入資源在採購資安防護設備，應該回歸本質，從現實世界中檢視資訊系統可能被外界影響而造成物理性破壞的風險，進而建立具備高回復能力的資訊運作基礎建設及管理能力。

總結與會人士對於科技應用於個人隱私保護之看法，凝聚以下數點共識。

#### (一) 隱私保護的心態要融入組織文化

科技保護隱私的各項相關作為，應該是建立在政府、企業自身的隱私保護政策與心態中之上，在組織運作的任何環節都將隱私保護納入考量，並建立管理機制督促組織內的成員依循政策執行隱私保護作為，最後藉助科技力量協助組織更有效率的完成資料保護的作為。

#### (二) 數位時代下隱私保護措施必須與時俱進

有鑑於數位科技突飛猛進地發展，導致既有隱私保護各項防護措施無法因應科技變遷引發的隱私侵害風險，例如物聯網科技協助組織即時監控空間變化，偵測環境異常；然而，物聯網感測器蒐集的資料可能是民眾日常生活的各項舉動，逾越了設置的目的。與會人士建議組織面對、使用新興科技之前，必須瞭解該項科技對於隱私保護衍生的衝擊。歐盟已針對資料應用訂定資料保護衝擊評估( Data Protection Impact Assessments ; DPIA )規範，協助組織已將營運過程面臨的資料應用情境，以系統化方式分析、識別和最小化資料保護風險，如果做得正確，可以評估和證明該組織遵守所有資料保護義務。



### (三) 物聯網資料保護有待加強

物聯網科技已發展得相當成熟，隨著第五代行動寬頻通訊網路逐漸普及，將再次推升物聯網應用範圍。在物聯網的環境中，每個人身邊充滿許多感測裝置，隨時監看、蒐集各種資料類型，進而引發民眾隱私權侵害的疑慮。例如，影像監控科技將特定人選的行蹤掌握無疑，使用行動載具與電子票證等，都有留存個人數位足跡在網際網路上難以避免存在個資遭到濫用的風險。此類資料若未經適當處理，即很有可能造成個人隱私權之侵害。歐盟要求成員國採納「自設計著手保護隱私」之概念，即在構思設計階段就將隱私權保護的概念納入設計中。

## 二、個人資料的擁有權

2013 年 12 月聯合國大會一致通過由巴西和德國共同提出的題為「數位時代的隱私權」決議。該決議強調隱私權是民主社會的基礎之一，非法或任意監控通信以及蒐集個人資料，是侵犯隱私權和言論自由權的行為，背離民主社會的信念。隨著數位科技日新月異，各種強調個人化精準服務、使用者體驗式服務、主動化服務不斷的推陳出新，這些服務背後隱藏的動能即為民眾個人隱私。換句話說，今天民眾享受許多相當「便利」的數位服務，亦即表示民眾被「瞭解」的更徹底，越沒有隱私。

2018 年 Facebook 創辦人 Mark Zuckerberg 在美國國會聽證會多次表示：Facebook 的使用者擁有自己的全部資料。與談貴賓 Niimi 先生表示，外界討論資訊隱私權經常表達的概念是「資料屬於誰？」。2019 年 5 月 Insights Network 顧問公司進行資料擁有權的調查研究，發現有 79% 的消費者表示他們認為「跟自己有關的資料」被共享時應該獲得補償。這表示消費者已意識到資料擁有權的問題，並萌生個人資料被利用的實質補償概念。Niimi 先生另舉例，美國藝人 William Adams 在 2019 年 1 月的「經濟學

人」雜誌的社論上公開呼籲科技巨頭必須支付使用個人資料的費用，他認為世界各國必須建立比「擁有權」更強烈的「資料權」，讓資料的蒐集與利用均在可控制的過程中進行，即便民眾同意與他人共享資料，資料權仍持續有效。Niimi 先生認為「資料權」與「擁有權」最大的差異在「治理」，資料權賦予人們對其個人資料治理的權利，包括個人資料被取用、更改、移動、刪除的權利，以及知道誰在蒐集我的個人資料，資料在哪裡，資料去哪裡，誰有權使用，以及因為什麼目的而蒐集、使用我的個人資料。其實上世界各國已經開始重視民眾對其個人資料的治理權利，透過法制規範要求企業必須遵守，最受國際矚目的歐盟「一般資料保護規則」( General Data Protection Regulation )在 2018 年 5 月正式實施，它試圖解決資料壟斷問題，賦予民眾具備資料可攜權，允許消費者從既有的企業中取出個人資料，並轉移到另外一家企業，藉以突破資料壟斷並進一步創造良性的競爭環境。另外，Niimi 先生對於「資料貨幣化」的概念感到遲疑，就「個人資料」本身的價值性可能不大，但是綜整整個資料市場的各项資料後，就有可能產生相當可觀的利益，劍橋分析公司 ( Cambridge Analytica ) 蒐集個人資料影響美國總統大選就是最好的例證。劍橋分析公司支付每一位選民 0.75 美元蒐集該選民的姓名、性別、所在地，以及分析該選民政治支持傾向的資料，0.75 美元看似價值不高，但是綜整串聯之後產生的綜效社會衝擊，卻遠遠無法以金錢衡量。現在，法律規範已經賦予民眾資料治理權利，但這些權利並非萬靈丹，最重要的是將這些規定易於使用且廣泛採用。

與談貴賓 Manning 先生表示，美國政策制定者已經認真考慮數位時代資料擁有權的議題。參議員 John Kennedy 提出了「2019 年擁有自己資料法案」( Own Your Own Data Act of 2019 )，該法案的核心精神是「每個人都擁有自己在網際網路上產生的資料之擁有權」，要求數位社交媒體公司使用消費者資料錢必須獲得消費者同意。參議員 Mark Warner 及 Josh

Hawley 提出法案，要求 Facebook 、 Google 和其他大型資料蒐集者必須揭露他們蒐集的消費者個人資料而衍生的價值。在加利福尼亞州長 Gavin Newsome 希望推行「資料紅利」的政策，期望民眾的資料被企業使用而產生利潤時，必須回饋給消費者。以上這些政策上的發展方向，明確的指出「個人資料是消費者的財產」之概念，這個概念更深刻的意涵，與隱私權專家 Alan Westin 提出的概念一致：民眾有權利控制、編輯、管理與「個人」相關的資料，並且具備將個人資料在「個人同意」的程度上資料傳達給他人使用之權利。消費者無法掌握個人資料在市場上被流通、使用的情形，但是應用資料的企業卻因分析個人資料而提升銷售利益，進而讓消費者衍生對這類不對稱市場經濟模式的反感。

與談貴賓 Naman 先生認為，我們在數位時代產生的資料，不僅只有狹義與「資料產生者」相關(如消費者使用Facebook 而產生的資料)，更有廣義的「涉及各類資料增值利用」的各項作為，尤其數位經濟推波助瀾的發展浪潮中，民眾的資料被廣泛流通於資料共享生態圈中，最明顯的案例是我們在金融機構的交易，除了「完成金融交易」的原始目的之外，更拿消費者的資料進行各項監理措施，例如詐欺監控、防制洗錢等監理作為，而這些使用個人資料進行監理的工作在許多法制規定中已被明確許可，例如 1970 年的美國第一部聯邦隱私法「公平信用報告法」( Fair Credit Reporting Act )，到近期的歐盟「一般資料保護規則」和「加州消費者隱私法」( California Consumer Privacy Act )。簡單的說，大量資料共享是有助於促進公共利益和經濟價值，任何資料使用付費機制或使用限制，都有可能破壞公共利益和經濟價值，進一步思考，這些資料共享付費機制與使用限制，對於個人隱私保護幾乎沒有好處。相反的，應該著眼於保護消費者個人隱私的前提下，建構個人資料共享使用對於社會、經濟、國家發展的方式，就像消費者的金融交易資料被使用於防止詐騙。

律師 Wheeler 先生補充醫學研究與促進就業等個人資料分享而創造公共利益的案例。在醫學研究和涉及人體實驗的研究中，個人資料共享與隱私保護作為可以兼顧，進一步因醫療資料共享利用而為社會帶來重大效益。美國大多數醫學研究受到 1996 年「健康保險的可攜性和責任法」(Health Insurance Portability and Accountability Act) 以及美國衛生與公共服務部 (Department of Health and Human Services) 的「隱私權規則」(Privacy Rule) 的規範，該規則明確訂出多種個人資料的定義與範圍，並限制了醫療研究資料的揭露和共享方式；而人體實驗研究在衛生與公共服務部的「通用規則」(Common Rule) 規定醫療研究機構審查委員會評估受測者的隱私衝擊風險，包括隱私權及因應風險的方式。在就業方面，美國平等就業機會委員會 (Equal Employment Opportunity Commission) 要求雇主提報被雇用者的普查資料，因為沒有這些資料將無法發現就業歧視的現況，據以訂出合理的促進公平就業的政策。這些普查資料鉅細靡遺蒐集美國境內各企業雇用員工的各類敏感性個人資料(性別、種族、族裔、宗教、政治傾向等)，但是美國透過法律規定這些敏感資料的使用目的、範圍及使用限制，違反這些規定是刑事犯罪，根據這些法規規定，政府對就業普查資料進行個人資料去識別化，避免發布的資料顆粒度太小進而關聯出資料與該民眾的關係。然而，人口普查資料是各類社會科學研究的基礎資料，可為政府政策、學術研究、商業規劃和市場研究提供必要的資訊。美國人口普查的文件可免費取得，這是公共政策創造的資料共享空間，這種運作方式與大眾「沒有歧見」的價值觀一致，因為政府兼顧個人隱私保護與個人資料增值利用劃出基準線。反諸求己，企業執行商業行為蒐集、利用個人資料，應該也要做到兼顧隱私與利益。

本次高峰會議主辦人 Shmoon 先生總結與談人的意見，包括美國在內的工業化社會中，民眾對「擁有權」有一致的共識。小時候媽媽曾告誡我不可以拿別人的玩具，就像我們也不喜歡別人拿我們的東西一樣。然而

，上大學之後，我從教室返回宿舍後，發現室友穿著我的外套準備出門。室友聳肩說：我以為我可以穿你的外套，我們不是室友嗎？大學宿舍中「個人財產」的定義顛覆了小時候的教育。當我逐漸成長，接觸到更複雜的財產擁有權的樣態，例如汽車所有權和房屋契約，這些法律文件證明我們擁有所描述的內容，並給予我們法律保護。我的所有權帶來了兩個重要的好處：我可以控制自己認為合適的資產，並在其他人不知情的情況下做自己想做的事情，這就是「隱私權」，即便我向別人租房或在飯店的房間，房東授予我在租用的空間中使用房屋，而不會受到房東干擾與監視。很不幸的，我們當前的法律體制無法明確定義個人資料屬於我個人資產的保護範圍。如同 Naman 先生與 Wheeler 先生提到的金融、醫療、公平就業的案例，雖然都有訂定法規或管理機制，但只著重在民眾與資料蒐集者之間的權利義務，而傳遞給第三方的資料，就像是在馬路上丟置一箱個人文件一樣，任何一位拾荒者撿走之後都可以聲稱他具有這些文件所有權，即便這些文件載明的內容與他無關。我們的金融交易資料、醫療健康資料被企業蒐集之後，都可以聲稱資料屬於它們，甚至可以將其出售給其他第三方。2018 年 5 月 25 日歐盟開始實施「一般資料保護規則」，要求企業對從歐盟境內蒐集的任何資料都必須獲得民眾同意，它擴大了個人資料的定義，涵蓋「可識別當事人」的任何資料，包括計算機 IP 地址、照片與信用卡消費資訊。加強個人資料保護措施，建立個人主張個人資料擁有權的機制，將可補強民眾個人隱私的重大衝擊，並提升民眾拒絕將個人資料揭露在公共空間的權利。

### 三、歐盟「一般資料保護規則」的公私組織衝擊與因應

隱私權是 Samuel Warren 和 Louis Brandeis 發表在 1890 年「哈佛法律評論」( Harvard Law Review )上撰寫的法律評論文章，是美國法律史上最具影響力的論文之一。這篇文章被廣泛認為是美國倡導隱私權的第一篇研究

，最大的貢獻是將隱私權視為獨立的權利，兩位作者認為個人權利必須隨著環境變遷與生活改變，持續檢視、定義個人對其人身和財產的保護的確切性質和範圍，隱私權則是賦予民眾獨處權利。

與談來賓 Benhamou 先生指出，資通訊技術與私人生活之間的衝突早在工業化時期已經發生，例如報紙刊載政治人物、社交名人的生活情形，並且大量複製散布到整個國家，自此民眾就很難享受到私人通信。數位時代中，我們面臨的隱私權挑戰比起工業時代更為嚴峻。為因應數位時代下的隱私保護責任，幾乎每個國家都頒布了資料隱私法律或類似的管理規定，規範資訊的蒐集方式，資料主體的知情方式以及資料主體轉移後對資料控制方式。以美國為例，它沒有全面性的聯邦法律來規範資料隱私相關權責，但在特定領域因應個別管制目的而訂定資料隱私的權利義務，例如「聯邦貿易委員會法」( Federal Trade Commission Act )、「兒童線上隱私保護法」( Children' s Online Privacy Protection Act )、「健康保險可攜與責任法」、「公平信用報告法」等。

截至目前為止，國際上已頒布的資料保護中，屬歐盟的「一般資料保護規則」最全面，它要求世界上每一個組織，從歐盟 28 個國家(地區)的居民蒐集、使用、傳輸和安全性必須遵守「一般資料保護規則」規定，重點包括：

#### (一)行使同意權

蒐集個人資料前，必須賦予資料主體用明確同意其資料被蒐集的機會。包括網站使用 cookie 技術蒐集瀏覽者的瀏覽偏好，另外在美國通常不被視為個人資料的資料（例消費者瀏覽網站時的電腦 IP 地址），在「一般資料保護規則」中被視為「個人資料」，因為它可以串聯消費者在網際網路上的足跡，進而追蹤、分析該消費的生活習性。

## (二)資料洩漏通知

如果組織蒐集的個人資料不慎遺失、洩露，則該組織必須在 72 小時內通知隱私保護監理機構和資料主體。

## (三)資料主體治理個人資料的權利

組織必須提供資料主體治理其個人資料的能力，包括取用、更正、刪除資料的權利。

歐盟「一般資料保護規則」保護對象僅為歐盟會員國地區的民眾，為民眾提供個人資料高度控制權。由於「一般資料保護規則」適用範圍包括任何針對歐洲市場或提供服務，並持有歐盟居民的個人身份資料的組織，對該組織管理與處理資料提出了相當高門檻的規定，包括設計資料保護的機制，並且記錄所有資料處理的過程，其影響性遍及全世界。從以上三項規範重點，Benhamou 先生指出科技產業面對歐盟「一般資料保護規則」的挑戰及因應措施，必須要盡早實施。

### (一)對技術平臺的影響

由於「一般資料保護規則」對資料管理與處理的要求相當高，因此組織必須全面檢視及評估其技術平臺和資料處理架構，包括資訊系統、網站、資料庫及資料處理平臺，確實掌握組織搜集了哪些個人資料以及其存在何處。在進行內部評估後，組織必須更改其技術平臺和資料處理架構，才能滿足「一般資料保護規則」的要求。再者，「一般資料保護規則」要求組織向歐盟居民提供強大的資料治理權利，例如被遺忘權、取用權，可攜權和自動決策解釋權，如果民眾想知道組織蒐集了哪些個人資料以及蒐集目的，則該組織必須及時回應民眾的要求。另外，組織掌有有居住於歐盟民眾資料，或來自歐盟受雇者的個人資料，組織必須提

供民眾、員工取用其個人資料的要求，並依據請求有效地從系統中刪除其個人資料。具體而言，組織首先需要從所有資料來源管道中識別與民眾或員工的個人資料。再者，組織需實施整體搜索工具，全面搜尋內部所有技術平臺，系統，檔案，以找出所有相關個人資料。

為了滿足「一般資料保護規則」的要求，組織必須投入大量的人力和資源來升級技術平臺，更新隱私政策，以及調整資料存儲和流程。由於美國和中國這兩個經濟大國擁有許多與歐盟業務相關的公司，因此「一般資料保護規則」對兩國企業的影響尤其重大。根據 PricewaterhouseCoopers 調查研究機構公布資料，預計 68% 的美國企業將花費 100 萬美元至 1,000 萬美元來改變企業技術平臺來滿足 GDPR 要求，而 9% 的公司預計將花費超過 1,000 萬美元，如此高的成本最終將轉嫁給消費者，從而削弱中美企業的競爭優勢。此外，「一般資料保護規則」拉高阻擋歐盟與外國企業之投資和合併的門檻，成為美、中企業壟斷歐洲市場的有力工具。

## (二)對網路安全的影響

「一般資料保護規則」預估對組織的網路安全政策和實施程序產生重大影響，它要求組織實施合理的資料保護措施，以保護歐洲民眾個人資料遺失和隱私侵害的問題。「一般資料保護規則」提出關鍵性的隱私和資料保護要求，例如需徵得資料主體同意才能處理資料、資料處理過程必須匿名化以保護隱私、資料洩漏後 72 小時內通知資料主體、跨境資料傳輸安全管理，以及要求企業任命資料保護長來監督組織有確實遵守「一般資料保護規則」。因此，組織必須加強網路安全保護力道，以防止個人資料受到威脅和破壞，並最大限度地降低法律責任。



雖然「一般資料保護規則」對保護個人資料高標準要求為組織帶來壓力，也為組織帶來了新的機遇。近年個人資料安全漏洞的負面消息以及組織不當使用和銷售從民眾蒐集的資訊案例引起了國際關注，並給消費者信任帶來了負面影響。若組織在資料安全與隱私保護贏得民眾的信任，可以為組織帶來更多的收入，組織應抓住機遇增強其保護個人資料的能力，不僅可大幅降低「一般資料保護規則」課予組織的法律責任，還可以贏得消費者的信任，並與無法完全遵守「一般資料保護規則」的國家建立獨特的競爭優勢。

### (三)對新興科技的影響

由於新興科技如人工智慧、區塊鏈及雲端運算等均與資料密切相關，因此「一般資料保護規則」將對新興技術的發展產生重大影響。大家都清楚新興科技是提高組織運作效率和提升生產力的有效方式，是促進全球經濟發展的關鍵，且為各國最強大的競爭因素之一。這些新興科技運用巨量資料和資料演算法實現了公共或商業利益價值，而「一般資料保護規則」要求極為嚴格的資料處理與保護規定可能會壓制新興技術的開發和使用，並且不可避免地會增加技術開發成本。例如「一般資料保護規則」要求人工智慧的資料分析決策，必須要有人為審查和解釋，除了衍生大量人工成本外，更打破循證式決策過程的透明性與準確性。在區塊鏈技術應用上，每個節點的資料都會影響後續的紀錄資料，如果民眾有權刪除和更正資料，那麼區塊鏈的效率和效力將不存在。而雲端運算方面，「一般資料保護規則」要求雲端運算服務提供商負責向資料主體說明資料被如何處理的義務，這無疑是增加雲端運算服務之運營困難，因為雲端運算的效率來自於最佳運算資源分配，資料被蒐集與使用前無法完全確定資料會如何被處理。

歐盟成員國所屬組織主要處理歐盟居民的個人資料，所以歐盟所

屬公、私組織在新興科技的研發與應用方面將面臨重大挑戰，若歐盟新興技術產業無法升級技術而有效地解決上述限制，那麼歐盟內部新興科技開發和應用的進度將大為趨緩。應用新興科技的相關行業，例如金融科技，電子商務、智能化應用等將受到重大影響，相較歐盟成員國，美、中、日、韓、臺等科技能力領先國家處理非歐盟地區民眾資料，不受「一般資料保護規則」的規範要求，在新興科技發展與應用方面受到較少的阻礙，可以更快創造更新、更好、更快的公共及商業服務予非歐盟地區使用。不過，從長遠發展來看，歐盟依循「一般資料保護規則」提供資料主體治理其個人資料，可以打下兼具隱私保護與新興科技發展的平衡基礎，相較於其他地區更具競爭優勢。

有鑑於「一般資料保護規則」對全球各國的影響性，而且隱私保護是未來發展的必然要求，也是維持國家競爭力的方式之一，Benhamou 先生建議各國要勇於接受該法規的挑戰，並提出兩項建議：

#### (一)改善個人資料與隱私保護的方法

科技能力先進國家應利用新興科技優勢，探索安全有效的資料處理方法，以增強其保護個人資料的能力。例如，運用科技改善隱私和個人資料保護方法，優化匿名化方法和資料驗算法，以解決透明性和效率之間的矛盾。除了科技手段外，更需要從組織日常運作實踐資料與隱私保護的管理措施。例如，找出組織現況與「一般資料保護規則」要求的差距、評估組織實施「一般資料保護規則」的成本。從另外的角度來說，「一般資料保護規則」規定的資料保護影響評估是測試組織隱私保護相關措施有效性的好方法。

## (二)建立信任

各國組織與歐盟有商業、科學合作的組織導入「一般資料保護規則」相關因應措施，可增強民眾對組織的信任度；此外，向民眾顯示資料使用之透明度和誠實揭露隱私保護情形，是提高民眾對組織信任度和聲譽的有效方法。為了在歐盟市場中保持競爭力，世界各地與歐盟往來的組織需要加強在隱私風險管理和個人資料保護方面的努力。

## 四、健康照護與隱私保護

健康照護是指與個人健康與疾病治療的相關作為，個人健康照護過程中產生的個人資料在多數國家的隱私保護政策中，均屬敏感等級的特種個資，並且受制於特別嚴格的規則，並且只能由受保密義務約束的醫護專業人員處理。此外，組織應採取必要的安全措施以確保健康照護資料受到保護，並且避免未經任何授權的揭露資料的行為。

與談貴賓 Bouchet 先生在美國健康照護領域擔任營運長，他認為隱私在醫療照護領域涵括的概念相當豐富，應該有以下四個面向必須注意。

### (一)身體隱私 (Physical Privacy)

從字意解釋，身體隱私表示免於與他人接觸。民眾將社會、企業和政府的聯繫行為視為侵犯隱私，例如測謊、酒測、路口監視器等。政府因公共利益的公共治理手段，對個人隱私產生威脅而引發爭議，尤其是在國際情報蒐集、國內犯罪偵查等方面。醫療照護方面，完全的身體隱私與現代醫療照護行為要求不一，現代醫療照護服務需要讓病患與醫護人員相互觸碰與診療，大多數病患願意犧牲對身體隱私的權利以獲得更好的醫療照護機會。

## (二)資訊隱私 (Information Privacy)

醫療照護領域中，對資料隱私的關注焦點集中在醫病關係的機密性及限制醫療照護和保險紀錄的取用。醫療照護的資訊隱私不僅是保護個人資訊的問題，更包括因家庭遺傳、基因研究等先天或人為因素，導致病患的家屬被推測出可能具有相同的生理特徵或疾病，更讓健康照護資訊之隱私成為民眾關切的議題。醫療照護機構必須具備限制病患健康照護資料被取用的安全管控機制，除了在實體環境中對病歷文件上鎖之外，電子化健康照護資料被傳輸、使用的過程，都需對資料進行加解密、去識別或代碼化。在安全考量外，資訊隱私另一個關注焦點在於資料被「合理使用」的議題，組織必須在最小資料取用限制下為病患進行醫療照護、病理檢查、保險理賠等工作。

## (三)專有隱私 (Proprietary Privacy)

根據美國多數州承認，未取得對方同意的情形下，使用對方的名字、肖像、身份是侵犯隱私的行為。依循此觀念，未經病患同意而拍攝患者的行，應為以保護個人隱私為由而反對。此外，人們普遍認為人類的基因資料是一把識別個人身分，甚至可控制個人健康的生物鑰匙，未經同意擅自使用他人基因資料可能觸犯民眾隱私權。

## (四)決策隱私 (Decisional Privacy)

決策隱私的意涵是人類具有為個人生活與私人事務自主選擇的權利，表示人類能做出自己的決定，並根據決定採取行動，而不受政府或其他不必要干擾。健康照護領域的決策隱私涉及啟動治療、終止治療及稀少性醫療資源分配的重要決策，誰擁有醫療照護行為的決定權，是病患？家屬？醫護人員？還是研究人員？在美國，決定隱私的概念已成為政府對人工流產、嚴重殘疾、絕症或長期處於人狀態的病患

執行健康照護行為的討論焦點，例如在代理生孕的案例，不育夫婦的決定隱私意味著在第三方的協助下訂立具有法律效力的生殖自由、父母有時會稱「家庭隱私」有權決定子女撫養、教育、醫療方式的自由等。

Bouchet 先生認為隱私的效果是促進自由社會和政治制度來創造、增強人類人格，例如隱私權可促進整體幸福感。現在正值數位科技劇烈變革健康照護模式之際，善用科技充分發揮健康照護資料提升醫療品質，已經是全世界不可擋的趨勢，當外界把健康照護隱私討論範圍擴及到醫病雙方之外的第三者時，必須建立健康照護資料流通的四個支柱，期望建立病患隱私保護，並積極促進醫療照護品質的基本要求。

- (一) 為了保護病患隱私，必須建立具有公信力的資料應用審查機制，在未確認侵犯隱私風險前，任何資料都不應該被流通使用。
- (二) 病患的同意其個人資料被使用之後，在任何時間可以撤銷同意，也就是尊重病患的意願，並可以隨時更改使用條件。
- (三) 健康照護資料產生的收益應回饋給資料主體。由於病患可能只獲得極低的回饋金，建議將回饋金轉入公共衛生體系，或是承擔醫療風險的醫事機構，提升全體國民健康或改善病患的醫護品質。
- (四) 在資料產生的源頭使用資料，最具價值和最新醫護資料通常來自臨床診斷與門診現場治療，可避免醫護資料被過度去識別化導致資料失真的問題。

與會貴賓 Abramson 先生認為，健康照護資料包含個人健康狀況相關的個人資訊，包括醫療行為過程產生的資料(例如醫生處方、醫療檢查報告、實驗室病理檢驗、病理影像等)，還有行政和財務資料(醫療預約、醫療服務發票、醫療證明)等，所以組織應採取必要的安全措施以確保健康照

護資料受到保護，防範任何未經同意的個人資料揭露行為。不僅在醫療機構保存民眾的健康照護資料，歐盟成員國的企業、團體亦應多種不同的目的而蒐集、處理其雇員之健康照護資料，例雇用前的體檢紀錄，年度醫療檢查紀錄，病假資料，兼職工作以照料重病或殘疾家庭成員之員工紀錄等。在法制面上，廣為全世界討論與遵循的歐盟「一般資料保護規則」相關法律規定，健康照護資料有幾項必須注意的管理措施。

#### (一)蒐集資料最小化

個人資料保護的基本要求是在蒐集資料的階段，依據特定目的取得「最小化的資料」，不要取得與目的無關的個人資料。組織蒐集、處理其雇員之健康照護資料(例如醫療證明和其他醫療資料)，應由組織的醫療服務部門進行，不可假手人力資源部門或其他部門，人力資源部門應僅搜集、處理雇員病假所需的行政資料（例如病假天數）。

#### (二)知情權

組織必須告知其雇員因為何種目的搜集、處理雇員的健康照護資料，在內部公開管道中揭露前項資訊，確保員工依其需要隨時可以取得。

#### (三)取用權

組織的雇員有權取用留存於組織之健康照護資料與其他與健康相關的資訊，以利雇員驗證資料正確性與完整性，組織必須清楚交代個人行使權利的相關訊息。

#### (四)資料保留期限

組織必須保證與雇員相關健康照護資料之保留時間不會超過必要的時間。由於雇員的健康及醫療情形隨時不同，過往搜集的資料不見

得能呈現現況，所以組織必須為雇員的健康照護資料訂定明確的保留期限，並徹底執行資料保存工作。

Abramson先生指出，多數組織會忽略組織蒐集雇員健康照護資料之管理措施，亦須配合國家隱私權的規定辦理各項因應作為，以前述歐盟地區組織面臨之敏感性資料管理之挑戰，亦為全世界各公、私團體必須指係思考與因應的課題。

與會來賓中央研究院吳全峰副研究員表示，臺灣早在 1995 年實行「電腦處理個人資料保護法」，要求公、私團體使用電子化程序處理數位資料必須遵守的權利與義務；因應各國落實個人資料保護風潮，臺灣於 2015 年實行「個人資料保護法」，規範個人資料之蒐集、處理及利用相關權責；2018 年因應歐盟實施「一般資料保護規則」，讓臺灣警覺個資保護規定與歐盟的規範存在明顯的差距，可能嚴重影響臺灣對歐盟業務推廣、學術研究之跨境合作，必須檢視與調整「個人資料保護法」相關規定。吳副研究員指出，臺灣「個人資料保護法」架構矛盾、體例不一的問題，起源於臺灣參考美歐個資保護立法例時，摻雜不同基本概念之結果便導致「個人資料保護法」在適用時出現扞格。例如，「無從識別特定個人」可分為無從「直接」識別或無從「間接」識別。美國之去識別假名化概念通常指前者，亦即將與個人可識別因素排除即可，但歐盟之匿名化概念卻兼具不得直接及間接識別之概念，且去除識別因子的資料仍可對照回推，故被認仍屬可識別個資。而臺灣「個人資料保護法」之「無從識別當事人」，在法條用語、法務部函釋、法院判決中卻無統一定義與內涵，甚至直接混用美歐法規用語，未考慮概念與實務上的差異。2018 年臺灣最高行政法院對健保資料庫案作出判決，認為衛福部未經民眾同意而釋出健保資料，已限制民眾自主權利，法院主張除非衛福部釋出資料具有「公共利益」時，才能「例外」不需取得資料主體同意，否則就是對資訊自主權的不正當侵害，而「產業發展」或「商業應用」之目的明顯不在「公共利益」之範疇，所

以法院判決表示衛福部若沒有取得個人同意，便不能違法將其健康資料釋出作「產業應用」或「商業用途」，此判決亦符合個人資料保護法第六條第一項第四款之規定，亦與美國、歐盟對個人資訊自主權保障之規範相似。

## 肆、拜會活動

### 一、法國興業銀行

地點：法國巴黎興業銀行(Societe Generale)總部

時間：108年10月28日(星期一)9點至11點。

我國參加人員：鄭貞茂副主任委員、楊耿瑜高級分析師

興業銀行接待人員：全球金融與諮詢副總裁 Alvaro Huete 先生

訪談內容：

法國興業銀行（Société Générale）是歐洲歷史悠久，且在全球金融界占有一席之地的金融服務。本次拜訪興業銀行副總裁 Huete 先生，主要為了解全球經濟發展情形與展望。談話重點摘錄如下：

- (一)全球經濟動能已呈現趨緩現象，預計在 2020 年至 2021 年將持續惡化。世界經濟大國將持續採取寬鬆貨幣政策，各國維持低利率的時間會拉得更長。經濟大國採取低利率政策應該有助於讓資本往新興市場流動，但是全球性經濟動能低迷是主要的阻力。
- (二) 中國與美國之間的貿易戰緊張情勢，加深中國出口成長的限制，預期持續影響中國 2020 年至 2021 年的經濟成長，有鑑於中國資產階級債務水準持續提高，中國對採取貨幣寬鬆政策採取謹慎態度，因此匯率有可能會波動。



(三)在美國方面，近兩年經濟持續成長，美國逐漸降低財政支持而侵蝕企業的利潤。美國聯邦儲備系統在全球經濟成長動能趨緩的環境下，持續寬鬆的貨幣政策，造成對外貿易的不確定上升，並且影響全球經濟成長。美國經濟的主要風險是對外貿易持續升級的緊張局勢和企業財務狀況趨緊，而且 2020 年總統大選之前，財政政策轉換的空間不大。

(四)全球貿易趨緩帶來的不利因素嚴重影響歐元區製造業，2019 年出口增長率已降至 1.1%，並將在 2020 年至 2021 年將持續下降至 0.4%，連帶影響失業率持續攀升。面對前景暗淡出口狀況，歐盟中央銀行採取了刺激措施，包括重新開始購買淨資產。有鑑於歐國脫歐可能讓歐元區出口動能持續放緩，後續將隨著英國脫歐的不確定性逐步消失之後，2022 年之後歐元區經濟發展動能將持續回復。

(五)亞洲新興國家(不包括中國、印度)整體出口成長率也受到全球經濟發展趨緩的影響，GDP成長力道持續減緩，但總體表現是全球最好的地區。以亞洲為主的半導體需求情形，受到日本與韓國的貿易緊張關係、全球消費性電子及國家戰略性產品需求較低等因素，讓半導體產業成長前景較具不確定性，而臺灣是唯一在製造業投資上成長的經濟體，這要歸功於國家政策上的支持。

## 二、兆豐國際商業銀行巴黎分行

地點：兆豐國際商業銀行巴黎分行

時間：108 年 10 月 28 日(星期一) 14 點至 16 點。

我國參加人員：鄭貞茂副主任委員、駐法代表處經濟組梅碧琦組長、楊耿瑜高級分析師

兆豐國際商業銀行接待人員：巴黎分行經理邱進偉先生

兆豐國際商業銀行(簡稱兆豐商銀)前身為中國國際商業銀行，2006年8月合併交通銀行而改名為兆豐商銀，業務專注於國際貿易與匯兌業務，截至2019年12月，兆豐商銀國內分行有108家，海外分行23家，行員數超過5,500人，資本額逾新臺幣853億元，為我國大型行庫之一。本次拜訪兆豐商銀巴黎分行經理邱進偉先生，主要為了解兆豐商銀在巴黎地區的業務運作情形。談話重點摘錄如下：

- (一)兆豐商銀海外分行主要任務係協助臺商辦理經商匯兌與融資業務，以巴黎分行服務範圍來說，主要往來對象為法國地區之臺商企業。由於在法地區臺商企業數量並未有顯著提升，所以巴黎分行的業務項目與營收無顯著增加。
- (二)兆豐商銀配合推動新南向政策，近年海外重點發展區域鎖定東南亞國家，包括泰國、菲律賓、越南、緬甸等地，近期更準備新臺幣一千億元的新南向專案融資額度，提供至新南向國家之臺商融資需求，依據其是否有擔保品、有無提供保證、個人或企業等不同條件的案件給予不同的優惠利率。
- (三)由於2016年8月紐約分行被紐約州金融服務署因違反反洗錢防制法處以罰款1.8億美元，造成母公司兆豐金控全年獲利減少2成以上。自此，兆豐商銀成立具有百人以上規模的法令遵循處及反洗錢暨金融犯罪防制處，專職各項洗防與法遵改善、制度建立，初估每年花費約計新臺幣11億元。
- (四)巴黎分行配合歐盟反洗錢防制相關規定辦理各項法遵作業，由於巴黎分行在非臨櫃金融交易方面的配套措施尚未完善，目前未辦理金融卡、網路銀行、信用卡等非臨櫃交易服務。近期巴

黎分行評估臺商或國人在法國地區的非臨櫃交易服務交易需求不高，多數為臨櫃辦理外匯、融資、授信等，故尚無推出非臨櫃交易服務之規劃。

(五)由於臺商與國人在法國地區之企業數與人數持平，巴黎分行營業收益遇到瓶頸，兆豐商銀在 2019 年 4 月要求加拿大、巴拿馬、巴黎分行調整營運模式，由批發零售轉向以國際聯貸案為主，因預期英國脫歐效應將使國際聯貸業務從倫敦轉向歐陸，巴黎分行更有機會拓展歐陸商機。

### 三、法國巴黎新創基地 **Station F**

地點：Station F

時間：108 年 10 月 28 日(星期一) 16 點至 18 點。

我國參加人員：鄭貞茂副主任委員、駐法代表處經濟組梅碧琦組長、楊耿瑜高級分析師

位於巴黎第 13 區的 STATION F 是目前全球最大的數位新創孵化中心，自 2017 年啟用至今已吸引 Microsoft、Facebook、UBISOFT、zendesk、THALES DIGITAL FACTORY、Arts & Métiers Acceleration、Schoolab、IMPULSE LABS，和以 LINE 和 NAVER 團隊組成的 SPACE GREEN 等國際數位巨擘進駐。由於本會參訪行程為臨時決定，Station F 主辦方未能及時安排解說，因此本報告僅就書面資料與實體環境觀察法國新創育成基地之特色，參訪結果摘錄如下：

(一) Station F 基地原為法西奈車站 (La Halle Freyssinet) 翻修改造，占地 3,4000 平方公尺，為全球最大的創新育成中心。除了新創育成區，另依據法國的時尚生活風格，設立有結合購物、休閒和生活的未來轉運站。無論新創業者、遊客、巴黎居民都喜

愛在 Station F 享受自由舒適的生活體驗。

(二)整個 Station F 的空間採用開放式設計，設置超過 3,000 張工作桌，60 個會議室，8 座會議中心，每個工作區域均以玻璃帷幕營造整體通透與開放的氛圍。Station F 向每位新創者索取每張桌子的費用為每個月 195 歐元（約新臺幣 6,600 元），2019 年 8 月提供 600 人居住的新創宿舍區，讓新創者落腳巴黎。

(三)相較於臺灣創業育成中心配有創業導師，協助創業者提供開業輔導和發展方向，Station F 沒有為新創者配置導師，期望讓新創者之間彼此交流合作，創造全新服務或產品，創業過程中有什麼問題，就去問隔壁桌的夥伴，例如新創者的生醫科技創業計畫需要數值分析的技術，但是自有團隊人員沒有適合的人才，這時候可以跟鄰近辦公桌進行人工智慧專案的新創者交流，一起解決問題。

(四)同時期法國里爾市積極響應「法國科技」（La French Tech）計畫，自 2016 年起於市郊廢棄工廠改建新創園區Plaine Images，新創園區宗旨在培育音樂、3D動畫、線上遊戲、虛擬實境、數位出版與設計等創新技術的發展，提供新創者共享工作空間、相關軟硬體設備、技術與商業資源、資金挹注等，也與不少知名企業、學校、研究單位合作，共同培育數位內容設計人才，將創意能量向下扎根，預計於 2020 年落成啟用。

## 伍、心得及建議

### 一、取得歐盟「一般資料保護規則」適足性認證

隨著網路數位科技蓬勃發展，資料保存與傳輸過程衍生之個人資料保護與使用的相關議題逐漸受到關注。商業數位服務的使用者常因取用各項數位服務，自願將個人資料釋出予該企業使用；同時在當事人不自覺的情況之下，該企業將個人資料進行目的外處理與利用。為因應數位經濟蓬勃發展，並兼顧民眾個人資料保護，歐盟自 2018 年 5 月全面實施「一般資料保護規則」，該規則之重點是擴大資料保護範圍，除了在歐盟境內設立據點的企業外，增列對歐盟境內人民提供產品、服務，或監測歐盟境內民眾網路行為的境外企業。其次，在個資跨境傳輸的部分，由於歐盟是採「原則禁止、例外允許」模式，只有在符合例外條件下，歐盟地區民眾的個人資料才能跨境傳輸，而例外獲得許可的情形包括由企業自主採行符合規範的適當保護措施。

我國為數位科技應用程度相當普及且產業全球化程度高的國家，運用數位科技、網路傳輸與電子化資料處理協助企業運作的機制相當成熟。而「一般資料保護規則」之跨境個資傳輸規定，直接衝擊我國企業與他國企業具備之個資共有、移轉的情形。為協助企業之個資保護措施合規辦理，降低「一般資料保護規則」對我國國際發展之衝擊，我國自 2018 年起由國家發展委員會與歐盟啟動「一般資料保護規則」適足性認定協商作業，並配合雙方諮商程序研議我國「個人資料保護法」的修法事宜，2019 年我國已向歐盟遞交適足性認定申請，預期於 2020 年獲得認定。

### 二、推動資料經濟新模式-個人資料自主使用(MyData)

「個人資料自主使用」(MyData)的核心理念是由民眾自主決定個人資料之管理與運用，讓資料當事人取得所屬個資的知情與同意授權的權力，

進一步對個資的運用發展創新作法，讓數位服務更貼近個人需求，其中個資的來源包含政府與民間組織。為在合規的前提下使用個人資料，提供民眾對數位服務全新體驗，賦予個人資料全新的數位經濟價值，國際上如美國、英國與芬蘭等國已積極推動民眾「個人資料自主使用」(MyData)與個人化服務，借鏡各國推動經驗，發展適合我國國情之MyData需要持續深度探討法規、作業、技術上的相關議題，包括跨部門溝通的資料規格、個資授權規範、相關法規調適與行政流程搭配。

我國推動MyData之濫觴自 2014 年衛生福利部推出「健康存摺」線上服務，在民眾通過身分確認之後，自行下載當事人之門診、用藥、體檢等醫療照護紀錄。有鑒於善用民眾個人資料可簡化民眾申辦政府業務複雜度，更可依據民眾資料分析需求，設計精準的數位服務，進而推升資料經濟、數位經濟發展，國家發展委員會自 2015 年著手規劃 MyData 機制，將政府業務掌握之個人資料，依據資料當事人需求提供自行下載個人資料，或是透過線上服務同意方式，由民眾同意政府機關或民間業者取得其個人資料，提供民眾所需的個人化服務，截至目前已完成健保、地政、戶政、教育、交通等 10 大業務領域的 17 類個人資料，提供資料當事人自主應用。未來除持續擴大個人資料自主使用項目，將深化個人資料合規使用的情境，包括申辦政府業務免檢據證明文件、政府業務線上申辦，進一步研議公私協力之「資料市集」，讓民眾自己的個資自己賣，自主決定誰有權用個資。

## 陸、附錄

### 一、2019年秋季 Line 及 Intertrust 隱私高峰會議程

Time	Duration	Salon des Aigles	Salon des Batailles
8:00 – 9:00am	1 hr	Welcome and registration	
9:00 – 9:30am	30 mins	<p>Welcome speeches</p> <ul style="list-style-type: none"> <li>• Takesh Nakayama, Executive Officer/CISO/DPO/CPO, LINE Corporation</li> <li>• Talal G. Shamon, CEO, Intertrust</li> </ul>	
9:30 – 10:00am	30 mins	<p>Privacy, Confusology, Price Discrimination, and the Seeds of Capitalism's Destruction</p> <ul style="list-style-type: none"> <li>• Andrew Odlyzko, Professor, School of Mathematics, University of Minnesota</li> </ul>	
10:00 – 10:15am	15 mins	<p>Privacy: A Key to Avoiding Dystopia</p> <ul style="list-style-type: none"> <li>• Lizzie O'Shea, Founder and Board Member, Digital Rights Watch (by video)</li> </ul>	
10:45 – 11:30am	45 mins	<p>Computer Science and Privacy</p> <ul style="list-style-type: none"> <li>• Dave Maher, EVP and CTO, Intertrust</li> <li>• Milan Petkovic, Head, Data Science Department, Phillips</li> <li>• Robert E. Tarjan, Chief Scientist, Intertrust and Professor, Princeton University</li> <li>• Andrew Odlyzko, Professor, School of Mathematics, University of Minnesota</li> <li>• Talal G. Shamon, CEO, Intertrust (Moderator)</li> </ul>	<p>Energy, Climate and Privacy</p> <ul style="list-style-type: none"> <li>• Thomas Birr, SVP, Innovation and Business Transformation, E.ON (opening presentation)</li> <li>• Stephen Comello, Director, Energy Business Innovations, Stanford Graduate School of Business (Moderator)</li> <li>• Cameron Briggs, General Manager of Future Energy, Origin Energy</li> <li>• Andreas Schlayer, Member, Facultative &amp; Corporate Cyber Team, Munich RE</li> </ul>
11:30am – 12:20pm	50 mins	<p>Panel Session: Cross Cultural Norms on Privacy and Data Ownership</p> <ul style="list-style-type: none"> <li>• Toru Niimi, Privacy Strategy Lead, LINE Corporation</li> <li>• Nawaf Naman, President and Founder, The Bridge of Cultures Association</li> <li>• Nathaniel Manning, Co-Founder Ushahidi and Director of Business Development, Intertrust (Moderator)</li> </ul>	
12:20 – 1:00pm	40 mins	<p>Conversation: Should There Be a Legal Right to Privacy?</p> <ul style="list-style-type: none"> <li>• Talal G Shamon, CEO, Intertrust</li> <li>• Ron Wheeler, Attorney</li> </ul>	

Time	Duration	Salon des Aigles	Salon des Batailles
1:00 – 2:00pm	1 hr	Networking lunch	
2:00 – 2:30pm	30 mins	<b>European Perspectives on Privacy and Security Regulations for the Tech Industry</b> <ul style="list-style-type: none"> <li>• Bernard Benhamou, Secretary-General, Institute of Digital Sovereignty</li> </ul>	
2:30 – 2:45pm	15 mins	<b>The Right to Privacy in the Digital Age from a Human Rights Perspective</b> <ul style="list-style-type: none"> <li>• Nawaf Naman, President and Founder, The Bridge of Cultures Association</li> </ul>	
2:45 – 3:00pm	15 mins	<b>The Role and Mission of the Taiwanese Government in the Digital Economy Age</b> <ul style="list-style-type: none"> <li>• Cheng-Mount Cheng, Deputy Minister, National Development Council, Taiwan</li> </ul>	
3:00 – 3:45pm	45 mins	<b>Healthcare and Privacy</b> <ul style="list-style-type: none"> <li>• Philip Bouchet, COO, Tilak Healthcare</li> <li>• Paul Abramson, Founder and Medical Director, My Doctor Medical Group</li> <li>• Milan Petkovic, Head, Data Science Department, Philips</li> <li>• Chuan-Feng Wu, Associate Research Professor, Academia Sinica</li> <li>• Tomas Sander, DPO, Intertrust (Moderator)</li> </ul>	<b>Latest Developments in International Privacy Policy</b> <ul style="list-style-type: none"> <li>• Kaori Ishii, Professor, Chuo University</li> <li>• Elaine Harwell, Senior Counsel, Procopio, Cory, Hargreaves &amp; Savitch</li> </ul>
3:45 – 4:15pm	30 mins	Afternoon tea break and networking	
4:15 – 4:45pm	30 mins	<b>Rethinking Human-Technology Interaction</b> <ul style="list-style-type: none"> <li>• Anne Flanagan, Data Policy Lead, World Economic Forum Centre for the Fourth Industrial Revolution</li> </ul>	
4:45 – 5:45pm	1 hr	<b>Closing Panel Session: Cross Sector Views on Data and Privacy</b> <ul style="list-style-type: none"> <li>• Andreas Schlayer, Member, Facultative &amp; Corporate Cyber Team, Munich RE</li> <li>• Florian Kolb, Managing Director, innogy New Ventures</li> <li>• Alberto Sigismondi, CEO, Tivù</li> <li>• Naohisa Ichihara, Head of Cyber Security Dept., LINE Corporation</li> <li>• Talal G. Shamoan, CEO, Intertrust (Moderator)</li> </ul>	
5:45 – 5:50pm	5 mins	<b>Closing Remarks</b> <ul style="list-style-type: none"> <li>• Talal G. Shamoan, CEO, Intertrust</li> </ul>	
6:00 – 7:00pm	1 hr	Cocktail reception	



## 二、2019年秋季 Line 及 Intertrust 隱私高峰會與談人



Lizzie O'Shea



Florian Kolb



Dave Maher



Elaine Harwell



Kaori Ishii



Ron Wheeler



Bernard Benhamou



Anne Flanagan



Cheng-Mount Cheng



Milan Petkovic



Nawaf Naman



Thomas Birr



Chuan-Feng Wu



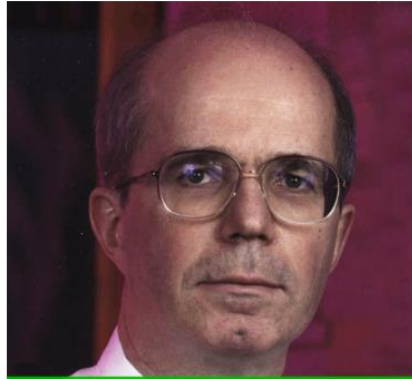
Naoshia Ichihara



Toru Niimi



Tomas Sander



Andrew Odlyzko



Robert E. Tarjan



Alberto Sigismodi



Andreas Schlayer



Paul Abramson



Nathaniel Manning



Takeshi Nakayama



Cameron Briggs



### 三、2019年秋季 Line 及 Intertrust 隱私高峰會活動照片



國發會鄭貞茂副主任委員介紹臺灣數位經濟發展方向  
照片來源：自行拍攝



與會來賓聆聽鄭貞茂副主任委員之專題演講  
照片來源：自行拍攝

#### 四、拜會行程照片



鄭副主任委員與興業銀行接待人員合照  
照片來源：自行拍攝



鄭副主任委員與兆豐商銀巴黎分行經理、駐法代表處同仁合照  
照片來源：自行拍攝





鄭副主任委員與駐法代表處同仁於 Station F 合照  
照片來源：自行拍攝