數位時代下的國民身分證與身分識別政策建議書

中央研究院法律學研究所

資訊法中心

109 年 11 月 2 日

版本	
V1.1	P.157 第八行誤植，改移至 P.164 第十五行

目錄

中央研究院法律學研究所資訊法中心
數位時代下的國民身分證與身分識別

政策建議書研議小組

召集人

邱文聰 本院法律學研究所研究員兼資訊法中心主任

院內成員（姓氏筆畫序）

王大為 本院資訊科學研究所研究員兼副所長
王柏堯 本院資訊科學研究所研究員
何建明 本院資訊科學研究所研究員
吳介民 本院社會學研究所研究員
吳全峰 本院法律學研究所副研究員兼資訊法中心副主任
吳齊殷 本院社會學研究所研究員兼副所長
李育杰 本院資訊科技創新研究中心研究員
李德財 本院院士、資訊科學研究所客座講座
莊庭瑞 本院資訊科學研究所副研究員
陳舜伶 本院法律學研究所副研究員兼資訊法中心副主任
劉靜怡 本院法律學研究所合聘研究員
蔡文軒 本院政治學研究所副研究員

院外成員（姓氏筆畫序）

王仁甫 財團法人資訊工業策進會資安科技研究所策略總監
沈伯洋 國立臺北大學犯罪學研究所助理教授
查士朝 國立臺灣科技大學資訊管理系教授
黃東益 國立政治大學公共行政學系教授

總結與建議

本報告針對目前內政部所規劃之晶片身分證及國家發展委員會提出的智慧政府方案，進行事實調查與問題盤點後，發現上述政策存在以下三大問題：
第一，規劃中的晶片身分證將對臺灣的自由民主體制帶來立即而重大威脅；
第二，在現行條件下，強制發行晶片身分證欠缺符合憲法的法制基礎；
第三，與晶片身分證同步推動的跨機關業務資料共享與整體智慧政府計畫，欠缺符合可課責性的設計與作法。

本報告進一步提出解決上述問題的三大政策建議：
第一，建立身分證晶片化與數位化的法制基礎、提供個人權利保障；
第二，立法確保晶片身分證的資安與國安；
第三，建立跨機關資料交換與智慧政府的可課責性及社會信賴。

本報告並建議，在解決上述問題之前，應立即暫緩晶片身分證之換發。

A. 事實調查與問題盤點

一、規劃中的晶片身分證將對臺灣的自由民主體制帶來立即而重大威脅

（一） 晶片身分證之資訊安全性嚴重不足

1. 晶片身分證之資訊安全除了晶片安全外，還包括其他硬體安全、整體系統安全、軟體安全與管理安全。但以下三者卻使未來使用晶片身分證的國人處於極大的資訊安全風險當中：
   (1) 內政部目前只強調「晶片製造」上的安全，卻無視「晶片設計」、「晶片作業系統與應用程序開發」、「晶片寫入設備」、「資訊應用軟體」等均為外包，因此存在系統與軟體安全風險；
   (2) 內政部也不在乎各種可輕易取得的「讀卡裝置」因欠缺安全驗證而存在硬體安全風險，誤認只要晶片資料已加密，讀卡機即使外洩資料亦不致造成危害，卻忽略若加密資料大量外洩，不僅外洩之覆水難收，更將大幅提高加密系統遭破解的風險；

(3) 個人、私部門與政府目前均欠缺妥適管理資訊安全與維護資訊隱私所需的習慣與文化。

2. 資安漏洞所涉及的外洩利益遠大於賞金的前提下，無法期待透過賞金獵人即完全發現晶片身分證存在的資訊安全漏洞；對漏洞擁有實質利益的敵人，不會輕易對外揭露所發現的漏洞。
3. 後量子密碼標準將於兩年後問世，內政部急於此時全面換發一張採用即將過時之加密技術的晶片身分證，其必要性有待商榷。

（二） 晶片身分證的晶片設計、設備生產製造與應用軟體存在嚴重國安風險

1. 資訊戰的攻擊鍊基本上是以取得大量對象國之國民個資為始，透過對其國民的人格剖析，建立能隨時精準投送各類假新聞/假資訊的名單，最終達到控制其公眾意見與民主之目的。晶片身分證因擁有完整國人身分個資，並可在未來使用時留下國人生活行動的大量數位足跡，成為新一波資訊戰的戰場，但依目前晶片身分證委外設計製造的模式，未來晶片身分證一旦正式發行使用，恐將成為國安破口。
2. 承包「晶片系統設計、空白晶片卡製造」與負責提供「晶片資料寫入設備」給中央印製廠的兩家國外廠商，疑似與中國安全部門存在合作關係。內政部雖強調晶圓由台積電生產，且兩家廠商也承諾提供給臺灣的空白晶片卡與資料寫入設備均不在中國製造。但因「晶片模組設計」、「晶片作業系統及應用程序設計」、「資料寫入設備生產」均仍外包給和中國政府關係曖昧的國外廠商，其中存在後門或共用系統元件而產生的風險，並不因為晶圓本身由台積電生產而改變。
3. 負責開發晶片身分證相關應用軟體的臺灣公司，在中國亦承包多家中國公營金融機構的資通業務，除了同樣存在共用系統元件而產生的風險外，更因該公司進入中國從事業務即受中國國安法令規範，其人員在中國境內有被迫交出臺灣資通系統參數、數位身分證專案或其他機敏資料的巨大危險，但目前我國並無法令限制該等人員進出中港澳。
4. 目前對承包我國資通安全業務廠商之最終資金來源、股東適格性，也欠缺相關法令規範可據以進行國家安全管控。

（三） 數位化與晶片化增加人民被監控之風險

1. 晶片第四區自然人憑證的「數位身分驗證」雖由需用機關透過下載憑證廢止清單的方式離線進行，使內政部憑證中心不能藉由身分驗證而即時監視

個人。

2. 但無論身分證有無「數位身分驗證」功能，個人在臨櫃或虛擬環境使用晶片身分證的過程中，仍不可避免地因提供晶片中儲存的各種數位身分個資進行「數位身分識別/資料驗證」，而留下精確的數位足跡。
3. 晶片身分證因創造紙本身分證所無的數位足跡，大幅增加個人被持續記錄、分析，進而在不同目的下被監視與控制的風險。
4. 發行晶片身分證之其他民主法治國家，多定有專法禁止、限制身分數位足跡之蒐集、處理利用，或建立制度化的機制使國民可有效反向監督政府或企業對個人數位足跡的蒐集、處理與利用，以降低晶片身分證對個人所帶來的數位監控風險。目前《戶籍法》或《個人資料保護法》，則均未針對身分數位足跡，制定特別的保護規範。
5. 晶片的資訊安全並非對抗數位監控與保護個人隱私的充分手段。

（四） 資通安全法、電子簽章法、個資法等現行法均不足以因應數位化/晶片化後帶來的挑戰

1. 內政部宣稱目前已有《資通安全管理法》、《電子簽章法》與《個人資料保護法》，無須另定專法規範晶片身分證可能對自由民主體制帶來的威脅。然而：

(1) 《資通安全管理法》僅要求「公務機關」以及「經指定為關鍵基礎設施提供者之特定非公務機關」應訂定資通安全維護計畫，並未從涉密人員之出境管制、外包廠商之最終資金來源、股東適格性與系統元件共用風險等角度進行全面規範。且即使僅為目前安全維護計畫的低度管制模式，也不適用於承包設計與製造晶片身分證的國外廠商，以及開發相關晶片身分證應用軟體的國內廠商（因為均非被指定之關鍵基礎設施提供者）。

(2) 《電子簽章法》僅規範「用以辨識及確認電子文件簽署人身分、資格及電子文件真偽之方法」得以成立與生效的條件，並未規範電子簽章過程所遺留之數位足跡，其蒐集、處理與利用的限制。

(3) 《個人資料保護法》目前並未針對數位身分足跡的蒐集、處理與利用，制定禁止或限制的規定，僅適用個資法第 16 條、第 19 條及第 20 條針對一般個資可廣泛蒐集並供目的外利用的現行規定，任令身分證數位化/晶片化帶來監控風險。

2. 因應數位化/晶片化對自由民主體制威脅的一個必要機制是獨立且權責相

符的個人資料保護專責機關。但到目前為止，專責機關的設立仍無具體進展。

二、強制發行晶片身分證欠缺符合憲法的法制基礎

（一） 《戶籍法》第 51 條規定身分證的全國性身分辨識效用，不足以做為法定強制身分辨識目的下，強制晶片化的依據

1. 《戶籍法》第 51 條雖規定國民身分證有於全國辨識個人身分之效用，但並非因此即謂個人負有無條件以國民身分證向全國各地之公務機關或私人證明自己身分的義務**。《戶籍法》第 51 條並未創設不限目的之身分證明義務**。國民身分證的全國性身分辨識效用，仍**應依其究為個人權利或義務，區分為「法定的強制身分辨識義務」，與事實上提供予個人的「任意性身分證明方法」**。
2. 《戶籍法》所規定的「強制身分辨識」以戶政機關的戶籍管理，以及公務機關為國家與人民間權利義務關係確認身分所需者為限。換言之，人民雖可在符合其需要時，依其自由意願，利用國民身分證所具有的身分辨識功能，向他人證明個人身分；卻只有在為了達成戶籍管理，或公務機關配賦權利義務予個人為確認身分所需的目的範圍內，人民才有配合國家申領國民身分證，並以之接受身分辨識的法律上義務。
3. 強制人民申領並接受身分辨識的手段，既然僅在達成戶籍管理或機關配賦權利義務時身分確認之目的必要範圍內，始符合《憲法》第 23 條法律保留與比例原則之要求，則身分證的「晶片化」，無論是否較紙本對個人自由權利帶來更高的侵害風險，理當只有為了達成上述目的之必要範圍內，才有強制為之的正當基礎。
4. 然而，國家的戶籍管理與機關配賦權利義務時身分確認之目的，一般並不以身分個資的數位化與證件的晶片化為必要之手段，完全可依賴傳統非數位化之個資與非晶片化的身分證件，即滿足單純戶籍管理或機關配賦權利義務時身分確認之目的。以強制晶片化做為達成戶籍管理或機關配賦權利義務時身分確認之手段，不僅欠缺法律依據，也不符合比例原則。

（二） 《戶籍法》第 52 條賦予主管機關的格式決定權，不足以做為國民身分證由紙本轉為數位與晶片化所需的法制依據

1. 主管機關對身分證之格式決定權，應以達成《戶籍法》授權國家建立身分證制度，所欲達成目的之必要範圍內為限，並不得對人民之自由權利增加

法律所無的限制。因此原則上不得藉由格式的決定，實質增加人民在原有紙本身分證下自由權利所面臨的侵害風險。

2. 《戶籍法》授權國家建立強制身分證制度之原意，一方面是為了在戶籍管理上發揮與戶籍登記簿相互證明之功能，另一方面也是公務機關配賦權利義務時，由機關用以辨識人民身分之用。在上述立法目的下，人民才有義務接受以身分證為形式的強制身分辨識；主管機關對身分證的格式決定權，也只應在達成上述立法目的之必要範圍內為之。
3. 內政部雖主張只要新身分證具有「便攜性」與「可辨識性」，就是合法的格式決定權行使。但「便攜性」與「可辨識性」是所有身分識別證件的共通特性，是國民身分證的必備格式，卻不是主管機關對身分證之格式決定權已合法行使的擔保。
4. 即使晶片身分證仍維持「便攜性」與「可辨識性」，並不等於身分證的晶片化確實是達成前開立法目的之必要手段，也不等於身分證晶片化並未實質增加人民在原有紙本身分證下自由權利所面臨的侵害風險。
5. 如Ａ一（三）所述，晶片化不可避免地讓身分證在使用過程中留下數位足跡，因而增加個人被監控/被剖析的風險。相較於紙本身分證，晶片化對個人自由權利帶來更高的侵害風險，已超越《戶籍法》在身分證格式的決定上對主管機關所為的授權。

（三） 為提供任意性身分證明方法而強制身分證晶片化，違反法律保留與比例原則

1. 《戶籍法》第 51 條雖規定國民身分證具有全國性身分辨識效用，但除非另有強制身分辨識的規範依據，否則國民身分證充其量僅是供個人自由選擇的一種任意性身分證明方法。
2. 內政部在晶片身分證的晶片上除規劃專供執行「法定業務」之公務或非公務機關，於獲得授權使用「安全應用程式介面 (Secure API)」後，得取用儲存於「加密區」之資料者外，尚規劃可供任何人、不限目的，於自由下載「開放應用程式介面 (Open API)」後即能取用的「村里鄰戶籍」與「公開區」資料。「村里鄰戶籍」與「公開區」之規劃雖意在提供便利的「任意性身分識別方法」，但強制要求個人不得拒絕於國民身分證上登載可供任意取用之戶籍與公開區資料，在欠缺明確法律授權下，已違反法律保留原則。其僅為促進任意性身分證明方法的普及利用，即以強制手段為之，限制人民資訊自決權，也違反比例原則。

（四） 強制蒐集高解析度相片並錄存於身分證晶片，欠缺法律依據，並已超越戶籍管理與配賦權利義務所需

1. 高解析度（300 dpi 以上）相片在人臉辨識技術逐漸成熟的今日，已具有個人單一獨特識別性，而成為一種生物特徵。相較於同樣具有個人單一獨特識別性的指紋，甚至蘊含更多與個人有關的生物資訊。
2. 依據司法院大法官釋字 603 號解釋，以強制方法大規模蒐集國民生物特徵資料，應以法律明定蒐集目的，其蒐集應與重大公益目的之達成具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。
3. 《戶籍法》授權內政部發行身分證，並不包含強制蒐集高解析度相片並錄存於身分證之晶片中。
4. 身分證上的相片若僅為臨櫃身分識別之用，並不需儲存於晶片中，亦無儲存高解析度相片之必要；若專為非臨櫃之網路環境中使用，則網路環境中之身分識別或驗證既不可能仰賴相片為之，則儲存高解析度相片之必要性即不存在。
5. 儲存高解析度相片所欲達成之不明確目的，相較於在欠缺法律明確禁止法定目的外使用，而可能被用來發展與利用人臉辨識的風險，不符合比例原則。

三、 同步推動的跨機關業務資料共享與整體智慧政府計畫均欠缺符合可課責性的設計與作法

（一） T-Road 僅著重公部門間資料介接的技術工程，輕忽資料串接交換所需的法制基礎與管理規範

1. 行政院於 2019 年通過以晶片身分證 New eID 及跨機關資料交換網路通道 T-Road 做為打造「智慧政府」的兩個主要基礎架構，以達成政府的數位轉型。然而依據目前的 T-Road 規劃，國發會僅負責建置跨機關資料交換的網路與傳輸平台；關於資料交換得以合法且正當進行的法制基礎與管理規範，則仍歸各部會負責，並號稱為「去中心化」與保留「機關資料自主權」。
2. 然而，政府建置 T-Road 事實上存在兩個不同的目的：一方面，T-Road 被塑造為個人在智慧政府中實現「個人資料自主利用」的必要工具，因為個人從公部門下載自己的資料或者同意他機關取用其個人資料，除了透過晶片身分證提供使用 MyData 前的身分驗證外，還需要有跨機關資料交換網路通

道，個人才能取得資料或授權資料交換。另一方面，規劃中的智慧政府也暗示可透過跨機關間包含個資在內的資料交換共享，達成以「資料驅動」為核心的「優化決策」目的，而這並非必要以個人同意或 MyData 的使用為前提。

3. T-Road 目的多重卻曖昧隱身的結果，使真正需要的課責機制難以建立。倘若 T-Road 之目的單純僅在協助個人實現資料自主利用，則目前分散由各部會自理的資訊隱私治理模式，尚勉足以因應。但倘若 T-Road 的目的也包含促進跨機關資料共享，使政府能進行「資料驅動」的決策，則在欠缺有效外部監理與專責監理機關的現狀下，「去中心化」的治理模式只會導致破碎而無效的監理結果，無力管理公部門在不經個人同意下，就能透過 T-Road 快捷而便利地共享國人個資所帶來的風險。
4. 此外，目前國發會的 T-Road 建置計畫針對目的不明確的跨機關間資料交換，卻僅流於「流程數位化」而未觸及「流程再造」，僅將數位轉型理解為由「國發會」提供新的技術工具給「各機關」執行原有的任務，而忽視「各機關」應重新檢討原有流程在數位化後是否產生過去未有的新挑戰。

（二） 混淆意在限制機關資料蒐集權限的「資料一次性原則」，與破壞目的外利用禁止原則的跨機關資料流用

1. 部分歐盟國家在保護個人免於政府過度擾民的精神下，規定政府機關向個人蒐集資料應以一次為原則；其他有權蒐集個資之機關在他機關已蒐集過相同個資的情況下，若非經個人同意，不得再向個人蒐集。但歐盟各國採用「資料一次性原則」其目的在進一步節制政府蒐集個資的權力，並未因此即放寬「目的外利用禁止原則」的要求。
2. 然而，國發會在數位政府的策略與跨政府資料交換的規劃中雖均提及「資料輸入一次到處可用」，卻未釐清究竟是要賦予資料當事人有權拒絕政府過度的個資蒐集，或是便利資料當事人可將其在 A 機關之個資授權 B 機關取用的作法，又或者是政府機關欲打破「目的外利用禁止原則」、建立超級（虛擬）資料庫的藉口。

（三） 智慧政府的規劃因欠缺可課責性的內涵而無法建立社會信任所需的制度基礎

1. 智慧政府的推動既以跨機關資料利用為核心，則資料利用的治理即為建立可課責性的關鍵。但依目前智慧政府的規劃，負責建置 T-Road 的國發會並

未提供個人對「未經其同意的跨機關個資交換」，可查詢其次數與所交換個資內容的途徑，使人民無從對政府利用其個資進行必要的民主監督控制。另一方面，在智慧政府的規劃當中，對於未來可能利用跨機關資料進行資料驅動決策的各部會，也未要求應建立資料治理機制，以確保政府決策所依據之資料並無偏誤、演算法之應用正當。凡此均無助於建立智慧政府所需的社會信任基礎。

2. 臺灣社會普遍欠缺良好的資訊安全管理意識與資訊隱私維護文化，目前平均每年有四十餘萬張身分證遺失，而過去以來公部門與私部門個資外洩也幾乎成為常態。但政府對源自於公部門之個資外洩卻未能表現出坦然面對與積極負責的態度，任令大量遭駭的身分個資漫流於暗網，亦不認為有需要通知並盡力協助每一位受害個人採取補救措施，迥異於被其標舉為智慧政府標竿的國家：愛沙尼亞；對於私部門的個資外洩也同樣未予有效的監理。在**政府未能帶頭建立資訊安全管理與隱私維護的社會規範**的現狀下，單方面強推全面換發晶片身分證政策，除了智慧政府的虛名外，難以贏得真正的社會信任。

B. 具體政策建議

一、建立身分證晶片化與數位化的法制基礎、提供個人權利保障

1. 針對**戶籍管理或依法配賦權利義務**予個人為確認身分所需的目的範圍內，國家雖有強制要求國民申領/換發身分證以進行強制身分辨識之權限與正當性，但晶片化與數位化是否為達成此等目的之必要手段，仍應再予釐清：
   (1) 若晶片化與數位化雖有利於「戶籍管理」或「依法配賦權利義務時身分識別」目的，但並非絕對必要之手段，則**應允許個人選擇保留不含晶片之紙本/單純塑膠卡形式身分證**，**或至少允許人民選擇關閉其晶片功能**。
   (2) 若晶片化或數位化確為達成「戶籍管理」或「依法配賦權利義務時身分識別」目的之必要手段，除應對外說明其理由並以法律明文規定外，並應以法律規定目前內政部所規劃之晶片第三區（加密區），僅供戶籍管理或依法配賦權利義務予個人為確認身分之用，**不得開放予非上述目的之使用**。

2. 為戶籍管理或依法配賦權利義務予個人以外之目的，專為提供人民便利之**「任意性身分識別方法」**，並無強制為之的合法性與正當性。目前內政部所規劃之晶片第一區（村里鄰戶籍）、第二區（公開區）及第四區（自然人憑證區），均**應允許個人在含晶片之身分證上自由選擇是否開啟使用，或根本選擇不含晶片之紙本/單純塑膠卡形式身分證，不應強制為之**。
3. 不應為了換發身分證而蒐集高解析度相片。若認為確有蒐集之必要性，亦應以法律明定蒐集目的，說明蒐集高解析度相片與何種重大公益目的之達成具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。
4. 應立法規定原則禁止數位足跡的蒐集、處理、利用。
5. 於國家能依上述原則提供合憲之身分識別制度前，為免侵害人民權利，不應強制個人換發晶片身分證並宣告舊證失效。

二、立法確保晶片身分證的資安與國安

1. 應立法禁止建立可用於多重目的之單一數位身分識別/驗證方法（開啟所有服務的同一把鑰匙），改為不同目的使用不同數位身分識別/驗證方法的分散式設計，降低雞蛋放一籃的風險。身分證應與自然人憑證二者採實體分離模式：若為增加自然人憑證發卡覆蓋率，可於身分證換證時同步配發自然人憑證，但由個人自行決定是否開卡。
2. 若欲發行晶片身分證，則應以法律規範晶片身分證之晶片系統設計、空白晶片卡製造、資料寫入設備製造、作業系統與應用軟體等廠商，均須揭露最終資金來源、接受廠商適格性審查，以避免在中國具利益者成為承包廠商，其涉及機敏資訊之人員亦應受到限制赴中之出境管制，並應立法規定關鍵設施之關鍵元件以專用為原則。
3. 應於資通安全處下設立各類資安技術委員會，針對包括晶片身分證及相關應用系統在內的資通安全產品與服務（包含資訊系統、資安防護），建立資安標準，並由適當機構完成測試與驗證。
4. 應立法要求晶片身分證發行前先進行資安風險評估，其內容不應侷限於晶片端，應及於以晶片身分證為媒介的整體智慧政府應用，並應包括評估轉換為後量子密碼標準的成本，以決定是否應於此刻換發採取舊密碼系統的晶片身分證。
5. 應建立完善的資安防護環境與作為，包含培養專職/專責的資訊/資安人員，編列合適的經費預算，以厚植發展智慧政府及數位國家的基礎。

三、建立跨機關資料交換與智慧政府的可課責性及社會信賴

1. 應於發行晶片身分證與推動跨機關資料交換前，**立法設立專責個資保護之主管機關**；其組織層級、人員配置應有規制主要個資需用機關的相應能力與實力，以達成有效監理公務機關與非公務機關的任務。
2. T-Road 提供跨機關資料交換前，應盤點比對各機關保有之個人資料檔案、檢討相關資料蒐集流程，以確保跨機關資料交換之必要性與資料提供最小化原則。
3. 應以法律確保「資料一次性原則」不得架空「目的特定原則」。
4. 應完整記錄公部門各機關蒐集人民數位足跡之政府足跡，以供個人查核。
5. 應建立各機關之外部資料治理機制，確保資料驅動決策之妥適性與公平性。
6. 智慧政府所對應各機關的行政作業流程並必須重新檢討，以符合數位化政府的數位應用服務。

在解決上述關乎臺灣自由民主體制、國家安全與人權保障的問題之前，本報告建議應立即暫緩「晶片身分證」之換發。

本報告以內政部對外公開之各項 New eID 招標資料及國家發展委員會的智慧政府行動方案為分析對象，探討晶片身分證對臺灣自由民主體制的可能衝擊影響，檢討強制發行晶片身分證與推動數位身分識別制度的法制基礎，並針對跨機關業務資料共享與整體智慧政府規劃的可課責性進行分析。

第一章 New eID 對臺灣自由民主體制的可能衝擊影響評估

一、 晶片身分證欠缺整體資訊安全性

1. 「晶片製造」的安全性不足以擔保晶片身分證整體的資訊安全

內政部推行 eID 政策，最常被大眾談論的就是晶片身分證的資訊安全議題。資訊安全所涉及的層面相當廣，可以包含硬體安全、軟體安全、系統安全，甚至是管理安全等，這些都非常重要。不過，目前為止內政部雖不斷保證晶片身分證的資安絕對沒有問題，一再強調晶片非常安全，甚至已達軍規等級，但卻完全沒看到內政部對於讀卡機具相關安全管理規劃與機制，也沒有看到針對身分證當事人隱私保護有進一步的管理規劃，令人憂心。

晶片可能涉及的資安問題，通常是「晶片製造」過程中可能存在私密金鑰的外洩風險。但影響晶片整體資訊安全的還包括「晶片設計」、「晶片作業系統與應用程序開發」、「晶片寫入設備」、未來實際應用時所使用的「資訊應用軟體」等。如果「晶片設計」本身就隱藏了後門，則即使「晶片製造」交由有信譽的公司代工，也無法確保晶片實際的資訊安全。同樣地，如果無法對「晶片作業系統與應用程序」的原始碼進行檢驗，也同樣會使身分證晶片的資安陷入危機。「晶片寫入設備」是未來將個人資料寫入空白晶片卡的機器設備；其資訊安全性也同樣必須經過驗證，才能確保在寫入過程中沒有產生額外的資安風險。

此外，採用非接觸式的通訊介面 NFC 讀取晶片身分證，可能造成卡號、無讀取碼保護的資料外洩，因為 NFC 等同在他人面前輸入 PIN 碼，在使用的過程中，相關資料即直接曝光。另外，當身分證遺失而憑證尚未被列入廢止清單前，身分證的自然人憑證功能很可能被有心人士拿來偽裝電子身分。

除晶片可能存有潛在的資安風險之外，跟晶片身分證最相關的，就是讀取身分證的讀卡設備。有關讀卡設備的潛在資安風險，大抵可分為讀卡設備本身的資安風險，及與讀卡設備連接之運算裝置的資安風險。讀卡設備本身的資安風險，可能起因於讀卡設備被安裝惡意側錄的元件，所以在使用讀卡機時，資料就已經外洩了；或者是讀卡機出場時，讀卡機本身或甚至公司裡面的員工可能就有問題；或即便讀卡機沒有問題，但當保護機制沒做好，讀卡機就很容易

就成為駭客攻擊的弱點。與讀卡設備的連接裝置也是另外一個需要注意的地方，連接裝置可能被植入惡意程式或木馬，這時也可能造成資料外洩；或是受到 MAN-IN-THE-MIDDLE－中間人的攻擊，從資料傳輸時擷取資料。以上為讀卡設備常見的潛在的資安風險。

目前針對讀卡機的流通，並無任何的上市許可管制，很難避免藏有惡意測錄元件的產品，潛入臺灣的日常生活而成為資安破口。從個人消費習慣的角度來看，一般人如果有新臺幣 80 元的中國製讀卡機可買，就不會去花 550 元買臺灣製有驗證的讀卡機。但檢視內政部最近一次的招標文件，完全沒有提到讀卡設備的資安風險。內政部 New eID 的簡易問答集內，也沒有看到與讀卡設備相關的規範與機制。

2. 身分個資數位化增加外洩風險，卻更難發現資料外洩

晶片身分證的採用，勢必使資料數位化。資料經過數位化後當然會很方便，但值得注意的是，在數位化的同時，資料也更容易取得、更容易編輯、更容易散佈傳播。

日常生活使用晶片卡非常普遍，你我身上可能有幾張類似的晶片卡，例如：悠遊卡、自然人憑證都是晶片卡。悠遊卡和自然人憑證其實都是通過一連串的安全認證的晶片卡，悠遊卡公司也一直號稱絕對不可能被破解，晶片卡看似應該是很安全的，但並不全然。舉例來說，2010 年臺大鄭振牟教授在駭客年會上展示以監聽的方式有篡改悠遊卡餘額的可能性；2011 年一位臺北某科技大學畢業的工程師，就直接拿破解的加值加密系統去消費且盜刷成功；2013 年臺大鄭振牟教授再次證明破解自然人憑證金鑰系統的漏洞。

那麼，或許有人會提問，悠遊卡既然這麼不安全，為什麼還在使用？這個問題，悠遊卡公司總經理受訪時已有回復過，悠遊卡具有相關配套機制，讓悠遊卡更安全。因為悠遊卡所有的消費記錄是可以稽核的，帳如果對不起來，公司就知道系統可能有一些問題，這時就可以開始追蹤。當悠遊卡被盜刷的時候，公司早就知道了。總經理說，發生問題時沒有馬上處理，反而讓卡片繼續使用的原因，是公司想要知道盜刷的手法。而且，就算有人盜刷，也很容易被發現，現時對於盜刷者也有相關的法律責任規範。所以，悠遊卡雖然可能有資安風險，但是發行數量龐大，如果為了一個可能的風險、小漏洞，要把卡片全部收回，可能不符合成本效益，經與資安問題容易偵測的權衡之下，還是可以繼續使用。

但是，將悠遊卡與即將推行的 eID 相比較，目前內政部所規劃的數位身分證，並有沒有這些特性。所以，當晶片身分證不具與悠遊卡類似的相關特性與機制時，以悠遊卡為例說明晶片卡的安全性，比較基礎與說服力道是顯不足夠的。

舉一個很簡單的例子，錢掉了，馬上看得到。個人資料被偷了，你知不知道？大概在 2016 年左右，第一銀行 ATM 發生問題，錢一不對，大家就開始找問題，所以很快地發現，還有機會把這錢追回來。但是，如果外洩的是個人資料，外洩好幾年後，才被發現在暗網販售，政府還可以說這是舊資料。

當然，資料即使加密後還是可能「外洩」。「加密狀態下」的外洩資料一般雖仍無法直接獲知資料內容，但加密資料一旦「大量」外洩，就大幅增加「密碼被破解」的風險。重點在於，當駭客破解了密碼，往往並不會對外張揚。在模仿者遊戲電影裡面也曾經提到，當 Alan Turing 破解德軍密碼後，雖然知道德軍即將轟炸英國艦艇，但他們選擇犧牲這些艦艇，也不將已破解德軍密碼一事讓德軍知道，目的是希望繼續獲得更多的情報。所以，資料真實可能存在的風險與威脅，應該是十分容易想像的。Alan Turing 告訴我們，當敵國或他國的駭客國家隊，一旦破解了密碼通常不會張揚，以便繼續竊取資料。

就目前可得的資料所知，單在 2014 年就有 44 萬張身分證遺失。未來一張用途更廣更便利的 New eID 是不是更容易遺失？再加上，數位身分證使數位化的資料更容易取得、更容易編輯、更容易散佈傳播的特性，會不會有更多外洩的個資在外面流傳？再者，當身分證遺失的數量多到一個程度後，是不是讓駭客更容易知道背後的系統該如何破解？

駭客圈裡面有一件事叫撞庫與拖庫，基於不少人習慣直接以自己或家人的個人資料，例如出生年月日，來設定帳號密碼，所以當 New eID 資料洩露的時候，駭客或是中共可以用來撞庫，他們可以用這些資料重新排序，不斷去試出當事人其他的帳號密碼，把這些資料全部拖出來，然後開始洗庫。所以外洩後的資料，我們最後能看到的是洗庫後的資料，就是中共把資料拿去重新堆疊過的資料，而政府卻因為格式不同否認這不是從政府資料庫中外洩的資料。最後，中共就利用這些資料，進行社交工程的 APT 攻擊 (Advanced Persistent Threat)。

3. 量子密碼標準將使目前的加密技術過時

現在很多人都在談量子電腦，量子電腦具有的快速運算能力，使目前的密碼技術可能被輕易破解。雖然量子電腦何時問世仍不確定，但因應量子電腦而

開發的「量子密碼標準」已預計在兩年後發佈。為何政府要在量子密碼新標準問世前，在這個時候仍採用舊的、可能成為潛在量子電腦威脅的密碼系統，令人十分不解。

資訊安全的研究者都知道，新的資訊技術永遠有發現新資安漏洞的潛力，發現漏洞之後再透過更新的資訊技術加以補強；因此攻擊技術的發展，一般均先於防禦技術的發展。所以，資訊安全是沒有辦法永遠保證的。資安公司與資安研究學者所能做的，是在資安防禦技術面上做偵測、阻絕，並設法延後系統被攻破的時間。更重要的是，系統雖沒有 100%安全，但當系統被攻破時，必須具備控管風險的能力，甚至是要求迅速地復原系統。這是目前提供資安服務、資安研究等，一個非常重要的思考方向。因此，資安雖無法絕對保證，但資安風險卻應該是「要可控管」的。當防禦技術即將進入新一世代（量子密碼）時，內政部卻以資安系統沒有絕對安全為由，堅持採用舊加密技術並無不當，而未積極儲備足以因應新攻擊技術的資安風險控管能力，令人費解。

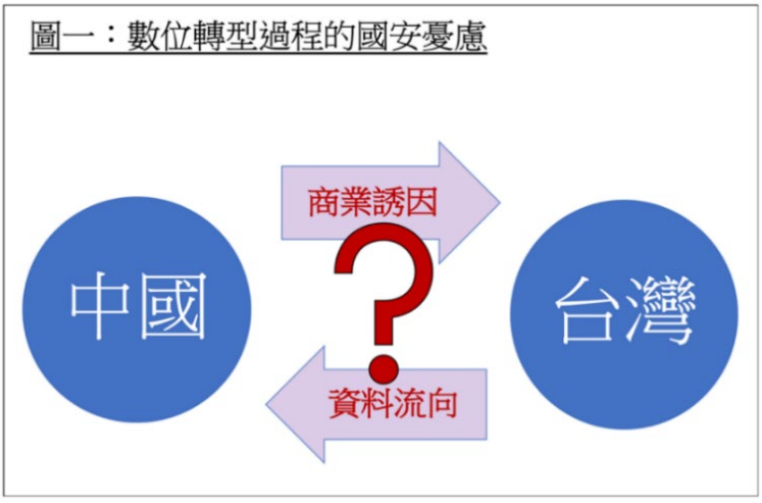
二、晶片身分證的晶片設計、設備生產製造與應用軟體存在嚴重國安風險

1. 晶片身分證的中國因素與臺灣國安的管制缺漏

數位身分個資與國家安全的關係，源自近年數位轉型的過程。數位轉型已經是當代全球政治經濟的一個趨勢，很少人會反對數位轉型，但是數位化的過程卻經常帶來資訊安全與國家安全的疑慮。

尤其是，中國政府善於使用「以商業模式做統戰」做滲透，在跨海峽的交易過程中，中國提供臺灣廠商商業誘因，就可能產生臺灣個人資料流向中國的疑慮（參見圖一）。因此，我國數位轉型過程中最重要的議題，就是兼顧現代化的效率、人權，更重要的是同時要兼顧國家安全，這三者間平衡的問題。中國

圖一：數位轉型過程的國安憂慮



因素是臺灣在從事數位轉型的過程當中，我們必須非常嚴肅討論的國安議題，更何況中國因素已經成為全球的關注焦點。

國家安全的破口，在這一次的數位身分證爭議當中大概可以歸納為三個，也就是，相對於中國對臺灣的政治戰跟資訊戰，第一個是包商的破口，第二個是營運商的破口，第三個就是中共對臺的資訊戰。

1.1 中國式監控資本主義

監控資本主義在最近一年，因為 Shoshana Zuboff 所著《監控資本主義時代》的出版得到比較多的關注。不過，中國式的監控主義，相比於 Zuboff 所稱的監控資本主義，其實結合了兩個很不同的元素。Zuboff 談的是「巨大的他者」（Big Other），所謂的 Big Other 指的是，人們的個資通過極為密集的網路數位連結之後，同步發生商品化的過程，然後這個「個資商品化」的過程，變成廠商追求利潤的一個核心動力，這是所謂監控式資本主義的核心命題。

但是中國是用國家巨大的極權力量控制這個監控資本主義，所以中國的監控資本主義必須在 Big Other 上面再加上一個「老大哥」 (Big Brother)，就是喬治歐威爾早在《1984》這本書提出的觀點：「老大哥正在監控你」(big brother is watching you)，而且是隨時隨地、無所不在的極權監控。所以中國式監控資本主義的要點，就是集合了老大哥的監控，加上「巨大的他者」這個監控資本主義模式的數位監控。中國共產黨的國家機器一直在駕馭資本，它的一個核心動力就是利用經濟誘因來驅動政治目標。就中共的監控政策而言，從最早的網路防火長城，之後建構中國社會信用系統，一直到現在強調網路主權，都是一貫的政策目標。這種數位極權主義的中國式監控資本主義，它不斷地精進監控技術、累積監控廠商的資本，舉比較大家耳熟能詳的案例就是，對新疆維吾爾族（東突厥斯坦）的監控，包括數位的工具乃至各種人體生物特徵的採集辨與識，都是結合了龐大的商機與國家監控標的。

2019 年 10 月，美國商務部將 8 家中國科技公司，包括海康威視 (Hikvision) 和浙江大華技術（這兩家公司掌握全球三分之一監視器市場），列入黑名單，這些公司牽涉對中國新疆維吾爾族等穆斯林少數民族違反人權的待遇。商務部發布的聯邦公報指出：「具體來說，這些實體牽涉違反和迫害人權，實施中國對維吾爾族、哈薩克族和其他穆斯林少數族群的壓迫、大規模任意拘留、高科技監控。」（經濟日報 2019/10/08 https://udn.com/news/story/6813/4092139；聯邦公報相關網頁：https://reurl.cc/v16XrL）海康威視大有來頭，在臺灣也有代理商，並宣稱「海康威視是目前全球安全監控產業的領導品牌」（https://www.digifocus.com.tw/about/brand-hik/）。

從全球監視器的密度排名來看，前 10 名城市之中，中國有 8 個，除了亞特蘭大跟倫敦之外，其他 8 個都集中在中國（https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/）。除了新疆等地，最近中國在香港實施國安法，很可能使用這些監控技術。

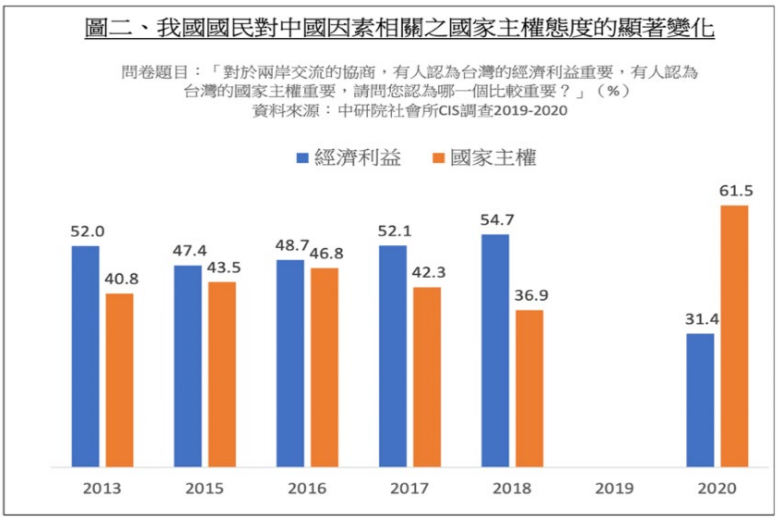
1.2 數位極權輸出

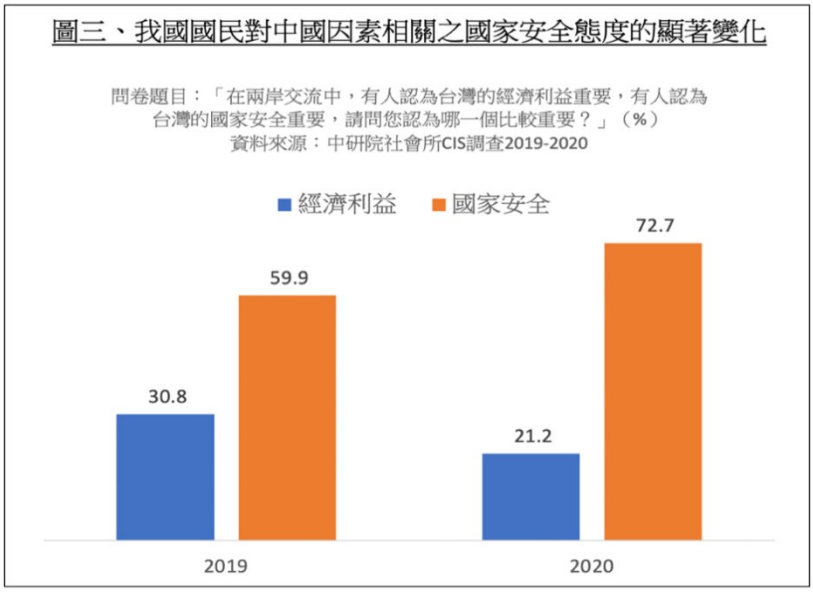
當前在香港或是新疆對人民的監控技術，透過一帶一路被輸出至其他國家，包括白俄羅斯、辛巴威、厄瓜多等等。大約三年前中國政府開始進行維吾爾族語的語音辨識，一直到前年底，開始針對東突厥斯坦人（新疆）的步態辨識。今天如果一個人過馬路稍微快一點，那他就可能被認定為恐怖份子。因為大家知道步態辨識，就是一個人走路的姿勢基本上不太會改變，其實跟人臉辨識是一個類似的系統。用此種方式將人的危險等級劃分成不同的九個種類，然後再根據這個種類，去把人送到所謂的再教育營，基本上跟集中營並沒有什麼太大的差別。

這些技術的對外輸出，會使民主國家在混合戰裡的外交戰上，處於非常不利的地位。例如願意譴責中國對維吾爾族暴行的國家共有 29 個，但相對地反對譴責的國家總共有 55 個。為何這 55 個國家反對譴責中國？其主要原因就是這些與中國結盟者在外交戰上的策略考量。

1.3 我國國民國家安全意識的變遷

我國的國民，對中國因素相關的國家安全態度，近年有著非常顯著的變遷。從 2013 年到 2018 年，關於兩岸交流協商的議題，在 2018 年以前經濟利益永遠都高過國家主權，而且高過的差距是蠻顯著的。但 2018 年至今，發生了巨大變化，從 2020 年 4-5 月的中研院社會所 CIS 調查來看，認為國家主權更重要者已逆轉高達 61.5%，相對地認為經濟利益較重要者僅為 31.5%，國民態度已發生很大的變化。同一調查亦顯示，問卷題目若改以國家安全替代國家主權，支持國家安全更重要者更高達 72.7%（參見圖二、圖三）。故政府應認知到，我國國民已認為國家安全，在跟中國大陸交流時是一個非常重要的議題。





1.4 中國對臺操作「以商業模式做統戰」分析

中國政府對臺統戰，包括銳實力滲透、資訊戰，在各個社會經濟領域當中的政治影響力操作，是不分時空地無所不在，相關案例及研究非常多。而在臺灣的數位轉型過程中，中國政府非常可能操縱臺灣的廠商，利用臺商的商業利益，做為它的載具跟平臺，然後造成臺灣個資的外洩，進一步變成國安危機。

臺灣廠商可能受中國影響力操作存在幾種不同樣態：第一個就是臺灣公司同時在臺灣跟中國兩地承包同類標案，然後在兩岸都有利益關係；第二種樣態為臺灣公司承包臺灣政府的數位標案，但在中國則從事其他的經濟利益行為，例如，一家臺商雖然在兩岸並非做同樣的生意，在臺灣做 A 生意、在中國做 B 生意，但是中國一樣可以透過利益關係操縱這家臺商；第三種樣態是臺商在中

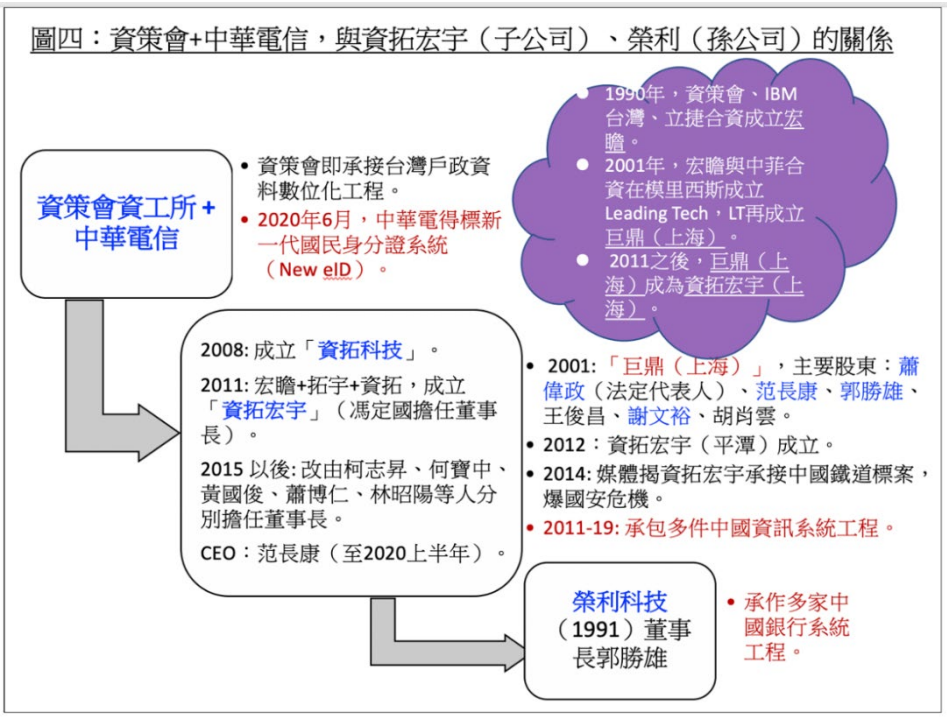
國從事數據資訊相關產業，反過頭回來臺灣投資並且承包標案。這三個樣態我們都必須同時注意，但是就 New eID 的具體問題而言，第一類特別值得注意。

這種「以商業模式做統戰」的操作模式，不僅限於資訊業，而是普遍存在。臺灣過去最常見的中國影響力的一個領域是媒體業，而且中國是全球性的操作，例如，美國政治學者 Larry Diamond 與 Orville Schell 在專書《中國影響力與美國利益》(Chinese Influence & American Interests, 2018)中點名《聯合報》，因該報老闆有興趣在中國發展事業，因此該報業集團所屬的美國《世界日報》，在最近這些年在許多議題上轉為親中立場。

New eID 個案分析：中華電信與資拓宏宇

中華電信的個案分析。今（2020）年 6 月，中華電信得標新一代國民身分證（New eID）系統，中華電信轉投資一家公司叫做「資拓宏宇」(IISI)，資拓宏宇的副總經理同時擔任它的子公司榮利的董事長，榮利承作多家中國銀行系統工程。資拓宏宇公司頂層的幾位關鍵高階經理人，長期是這個企業集團的核心經營團隊網絡（參見圖四）。而從其官方網站可以看出，資拓宏宇的子公司榮利，它從事金融業務，承接中國多家銀行的案子（參見圖五）。

圖四：資策會+中華電信，與資拓宏宇（子公司）、榮利（孫公司）的關係



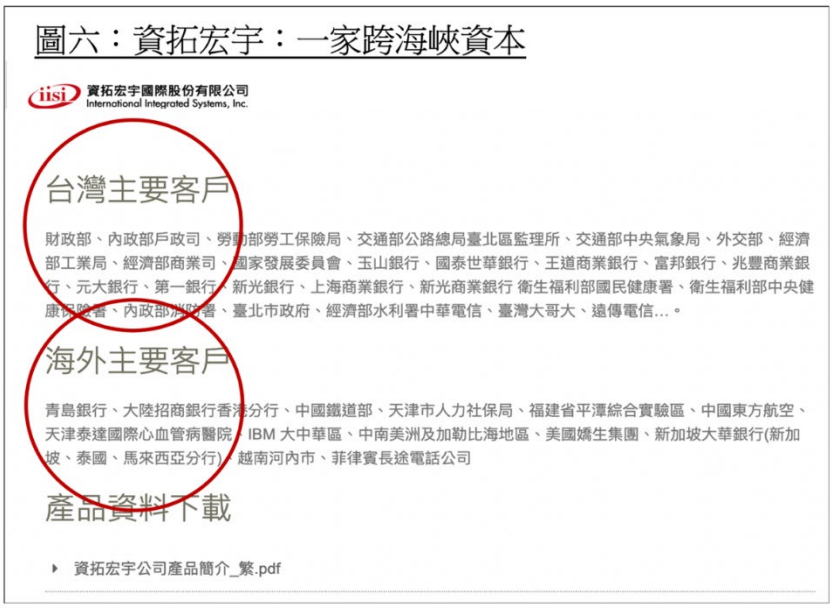
以下說明中華電信、資拓宏宇及榮利間母公司、子公司跟孫公司複雜的交叉持股跟轉投資關係。資策會的資工所，最早於 2008 年跟中華電信合組資拓科技，到了 2011 年宏瞻、拓宇、資拓三家公司合併為資拓宏宇，其門神董事長為

馮定國。馮定國四年董事長任內曾爆發嚴重國安危機新聞，當時 2014 年新聞報導很多。這個事件後，2015 之後資拓宏宇就改由不同人擔任董事長，幾乎每年都換一位，但長期擔任 CEO 職位的都是范長康（最近離職）。資拓科技最初是資策會資工所 spin off 出來，榮利科技是孫公司，榮利原本是拓宇的子公司，因合併才變成資拓宏宇的子公司，榮利董事長就是郭勝雄。這就是目前從中華電信、資拓宏宇、到榮利的公開資料中，整理出來的母公司、子公司、孫公司的關係網絡。

圖五：榮利承接中國銀行系統工程
（2020年7月官網資料：https://www.e-utc.com.tw/about.html）

再仔細看這些關係，已知在 2020 年 6 月，中華電信已經得標 New eID 系統，那我們再看這些投資關係。1990 年時，資策會跟 IBM 臺灣還有立捷就合資成立了宏瞻公司，然後到了 2001 年宏瞻跟中菲這兩家公司合資在模里西斯成立一家 Leading Tech，Leading Tech 在短期間內成立 Leading systems（一樣在模里西斯登記），然後 Leading systems 再成立巨鼎上海，之後因為公司合併的關係，巨鼎很自然就變成是資拓宏宇集團旗下的公司，所以 2011 之後就變成「資拓宏宇上海」，然後資拓宏宇在 2012 年又成立「資拓宏宇平潭」。從 2011 年到 2019 年，資拓宏宇就承包多件中國資訊系統工程，然後榮利科技根據它現在的網站，也承包多家中國銀行系統工程。

必須說明：此次得標 New eID 系統的中華電信，它整體企業集團在從事資訊業務的人事網絡，所承包或承作的資訊工程業務，呈現了跨足臺灣跟中國的模式，而且是現在進行式。根據資拓宏宇自己官網顯示，它是一家典型的「跨海峽資本」（參見圖六）。



1.5 臺灣目前欠缺對承包跨海峽資通業務之企業的國安規範

數位戶籍資料交給中華電信、或中華電集團的相關公司處理，將來可能發生層層轉包，並可能造成國安破口。以下幾個環節都值得仔細評量：

A. 臺灣的資通公司同時承作臺灣與中國政府和中國國營企業的工程，會不會共用或採取類似系統元件？開發人員是否屬於同一批人員？是否會讓臺灣資安與國安出現破口？
B. 中華電這家集團公司以及它的子公司、孫公司，會不會成為中國施壓的對象？是否會成為中國獲取我國人民個資的破口？
C. 最後，臺灣公司是否會成為中國對臺灣進行資訊戰的切入點？

中華電承包 New eID，只是諸多臺灣公司承包政府標案的其中一個案例，其他公司也應該嚴格檢驗。政府資訊工程標案中，衍生的許許多多資安與國安疑慮，主管機關須要嚴肅面對，謹慎行事。此次數位身分證標案，牽涉如此重大資安與國安的政策，在疑慮完全解除之前，政府不應貿然執行。

2. New eID 的資安破口恐成為中國對臺資訊戰攻擊鍊的起點

我們可從 New eID 在資訊戰攻擊鏈中的位置，來思考資安與國安風險這件事。目前 New eID 系統後面綁定的除了戶役政系統外，未來也可能連結財稅系統、出入境資料，還有健康保險資料、社福弱勢資料，甚至是公投領票資料。

如果民眾去參加某一場公投，往往很容易辨識出他的政治立場。中國政府若想掌握每個人的社經狀況、政治立場，破解 New eID 將是一條方便的路徑。而這樣一個攻擊型態之所以成為可能的原因，在於 New eID 整個系統從晶片設計、作業系統、寫入設備、讀卡機、應用程式等，都存在中國因素的問題。當 New eID 晶片卡一插進去，可能所有的資料就被中共蒐集走了。從之前付錢讓小吃店撥放特定頻道的前例來看，未來 New eID 上路以後，中國政府非常有可能以第三人名義去發展一個免費軟體、免費的 New eID 登錄系統，提供給我們的保全業、公寓大樓乃至各行各業使用（取代換證登記）。卡片只要插進去就做相關紀錄，做完紀錄後就遠端送到中國，進而完整掌握我們民眾個人的電子足跡。但目前內政部對此卻完全沒有任何風險意識。

但中國政府對臺的個資蒐集，並不一定顯現為直接的監控。目前最主要的管道反而可能透過民間公司來做，例如日前臺灣很多人在看愛奇藝等影音串流平臺。愛奇藝透過大量獨占內容來吸引民眾訂閱，這些版權獨占須要花不少錢，因此愛奇藝其實可能是虧損的。但為什麼愛奇藝之前還可以持續不斷地營運下去？其真正目的或許並非藉由提供影音串流服務營利，而是個資蒐集。若觀眾在手機上安裝觀賞用的 APP，那它將可取得位置定位、viewing preferences、作息時間等等的資訊。又如果透過安裝應用程式於第四台電視盒的方式，當第四台在契約中要求提供身分證字號與戶籍地址才能安裝時，一旦這些資料與愛奇藝的 APP 串接時，等於可將基本個資連同個人偏好資訊，全部外流。這些都是目前已經可以做到的事，而現在政府推動的 New eID 不幸地會讓上述這件事情變得更容易。就這個層次而言，如果大家有興趣可以多看 ASPI (Australian Strategic Policy Institute) 的報告，中國從翻譯的軟體或是影音串流的媒體，大量地在全世界蒐集個資。

北京蒐集臺灣國人個資的目的，基本上在於「分眾」，而這點必須從資訊戰或假新聞攻擊的觀點說明。最有效的假新聞攻擊，並不是今天丟一個假新聞給全體的民眾，這種做法是完全不會有效果的，因為其面臨的反作用力會變得很強。最有效果的做法，是要將訊息丟給特定的群眾，亦即要對這種陰謀論會有心裡的洞可以被填補的對象，相關的假新聞才會有用。舉例而言，一個很有名的中國政府在背後極力傳播的假新聞是「蔡英文墮胎」，就是蔡英文跟李登輝有姦情。這個訊息如果同時對全臺灣 2300 萬人投放，在反作用力下可想而知並不會有效果，由此可見分眾攻擊的重要性，而分眾的有效性就倚賴個資蒐集的完整度。以 2016 年來講，臺灣人民就已被歸類成大約 60 種不同的分群，到現在 2020 則已演變為好幾萬種，所以如果我們把身分個資全部交出去，搭配其他私部門外洩的資料，其實就可以輕易的對臺灣的民眾來做分眾，然後做不同類型的假新聞，或者是陰謀論的攻擊，進而影響到民眾的認知領域。

中共戰略支援部隊有兩三萬人專門負責發動假新聞的攻擊。他們偷臺灣人的個人資料，偽造個人行為，然後透過買公關公司來炒作，搭配公廟系統，扶植特定政治人物，也可冒用小林新村的資訊，或冒用某個賣花椰菜的阿伯，然後在 FB 抱怨政府不重視農產品的價格，害花椰菜堆了整山，接下來透過地方新聞分享，造成輿論的不滿。香港解密也是另一個血淋淋的例子。當一個國家開始控制人民，就會實施恐怖主義，實施思想改造和教育。之前香港發生恐怖的抗議意外事件，前一天一個小女孩去抗議反送中活動，坐電梯回家的監視器影片還說說笑笑，隔了三個小時後，她的屍體在河裡面出現，讓媽媽在哭泣。這件事的原因在於，中共結合黑道鎮壓香港相關抗議，而「香港解密」將抗議反送中參與者的個資都上傳上去，指控這些人是暴徒，號召港民（黑道）殺他，甚至有懸賞獎金。臺灣人也受到影響，例如基進黨及其他人士就在反送中活動後，被公佈了八個人名，甚至連護照號碼都有。這些都是身分資料被惡意人士掌握後的危害。

而 New eID 中更令人擔心的是在開放區居然有個人 300 dpi 的相片，在加密區更有 600 dpi 相片，這些高解析度照片一旦被不當蒐集，搭配中共人臉辨識 AI 系統，將能掌握當事人本人與身邊所有人的私人行蹤，其風險不可謂不大。

同樣嚴重的是暗網的問題。很多外洩資料目前都放在暗網上販售，很多暗網也疑似由中共在背後經營。針對臺灣兩千萬筆戶政資料在暗網被販售一事，臺灣政府回應這些格式與政府資料庫內資料格式不符，因此並非由政府外洩。這個回應令人擔憂。臺灣面對的並不是單純的駭客組織，而是中國政府，它們可以偷完資料，過幾年更新完後再丟上暗網，以很低的價格販售，只為了讓臺灣政府難堪。這麼做除了可以製造臺灣的社會混亂與人民對國家的不滿，將臺灣的資安漏洞或個資公佈讓全球駭客攻擊，或許比起中共網軍自己進行攻擊，可造成更大的危害。

有人認為未來 New eID 的資料外洩不可能發生，因為晶片已達軍規等級。但 New eID 最終雖在中央印製廠內寫入資料完成印製，但包括空白卡、晶片作業系統、印製設備等都委外給國外廠商，而從目前透露出的資料顯示其與中國黨政軍均有相當密切的關係。委外合作的廠商之一，更曾在 2017 年因違約將他國的 eID 拿到中國製造，被 IMF 制裁停權。這些根植於晶片系統內的資安/國安風險，既不可能由負責晶圓代工製造的台積電來擔保晶片沒有後門，也不可能交由最後僅負責操作機器將身分資料寫入晶片的中央印製廠來把關。

當臺灣的主權面臨被中共消滅的現實威脅下，如果沒有一個完善的資安與國安維護機制，就急著換發 New eID，等於為中共網軍竊取臺灣所有人的資料，開啟方便之門。

三、資料數位化與卡片晶片化增加人民被監控之風險

1. 「拒絕成為設定好的公民」是抗拒監控的規範性理由

一個社會何以應擔憂監控並保障隱私權？ 有三個規範上的理由來說明，第一個是匿名生活的確保；第二個是自主權的尊重，最後就是獨立人格的追求。

第一個理由－匿名生活的確保，每一個人都有匿名生活的需要，在日常生活中不希望處於被監看及窺視的狀態。所以，即使名人也希望其與配偶或伴侶間家庭生活是否和諧的狀態，不會被他人窺視或公眾議論，這就是所謂匿名生活的確保。

但有時在意隱私權與是否匿名沒有關係，換句話說，就算匿名性沒有被侵害，還是可能會在意隱私權，這裡要談的就是第二個理由 - 自主權的尊重。即使不涉及可識別資料，仍然可能會存在隱私權的保障問題。舉例來說，使用公共廁所時，如果有人偷拍，雖然不見得會偷拍到可識別資料，但是多數人在這種情況下，會認為這個行為已經構成對於隱私權的侵犯，而其背後的理由，應該與自主權尊重有關。

第三個在意隱私權的理由，其實是為了追求獨立的人格，拒絕國家或社會製造已設定好的公民 (programmed citizens)，不希望每一個人都被政府塑造成同一個或者有限的樣子。

個人在數位生活中留下大量而零散的數位足跡，可透過專屬個人的持續識別碼加以串連而整合成個人剖繪，個人剖繪則提供各種不同監控目的之用（參見 Box 1-1）。一方面，個人剖繪技術已在中國的社會信用體系中運作供政治監控之用（參見 Box 1-2）。另一方面，個人剖繪亦可為了精準商業行銷，在蒐集個人資料後將個人加以分類，形成各種不同的人物誌或角色設定 (persona)。無論是哪一種目的，監控對獨立人格的追求，都會產生某程度的緊張關係。但每個人對於追求獨立人格所需的空間並不完全一樣，有些人需要比較多的獨立人格追求空間，有些人覺得好像多少都無所謂，而這又牽扯到每個人對於隱私的品味，或者說各個社會文化對於獨立人格追求空間的品味及需求，每個社會都可能有所差異。所以，獨立人格的追求對臺灣、美國、日本跟歐洲社會而言，確實可能存在不一樣的重要性。

Box 1-1 監控、剖繪、持續識別碼與數位足跡

Surveillance 通常譯為監控，含有控制的意義，但有時監控以比較微妙、非直接的方式控制被監控者的行為。監控有時不是視覺或偏向實體空間，而可以透過資料的掌握，以對監控或監察對象有比較全面的了解。

監控，這個詞通常會有全面性的意涵在裡面，當講到監控時，通常含有時間與空間的要素，換句話說，這個行為已經進行了一段時間，而且在空間上沒有迴避的可能性。比如一個空間若只有一台監控攝影機，則有避開監控範圍的可能；但是如在城市裡有幾十萬個監控攝影機的話，那幾乎是很難避開。另外，監控，可能是針對大規模人口所進行，資料記載的精細程度可能到匪夷所思的地步，且資料將會被儲存，保存期間可能為永久或不特定。通常情況是不知道保存期間；日後如果有需要，已蒐集的資料就隨時拿出來分析。監控就是一個這樣的概念。

監控可以是對一個群體、一個地區的人口所為之的行為，比如現在新疆就是整個地區的人口，在一個被全面監控的狀況下生活。監控也可以是針對特定的人，對其行為做一個掌握。但監控也可能對不特定人所為，因為監控者還不知道要對誰監控。這時，監控的目的是要先蒐集資料或影像，事後如有需要再來查找可能會感到興趣的人。雖然這聽起來好像有點不可思議，但卻是事實上一直發生的事情。這種不特定目的下的監控，在政府部門、商業部門、個人等，其實都有能力可以做到。

另外，還有一種相互監控。比如 Amazon 的電子門鈴，住戶將電子門鈴安裝在門口，當有人來按門鈴時，攝影機就會啟動，然後將影像傳到綁定的手機。所以，不論在家裡或在外面，屋主都可以看到是誰在按門鈴，然後，再決定要不要跟他通話。裝電子門鈴的原始目的其實大部分是為了住家安全，但是很有趣的是，如果社區內每戶都裝了電子門鈴，那可能會變成
彼此監控，因為會來按門鈴的人恐怕大部分是鄰居或送貨員等。

有趣的是，Amazon 也跟政府部門間相互合作，例如警察局參與 Amazon 給社區住戶的折扣方案，讓社區裡多數住戶都裝有類似的電子門鈴。但如果整個社區都裝電子門鈴，那將是一個蠻有趣的畫面。Glenn Harvey 為 NBC News 新聞網站做了社區相互監控報導的示意圖。當住戶都裝有電子門鈴時，只要走進社區都可能被住戶的電子門鈴拍到。因為電子門鈴並不是只有按門鈴才會啟動，在風吹草動的時候也會啟動。所以，如

果裝有電子門鈴的話，入鏡的應該大部分都還是家人，譬如說在戶外烤肉的或遛狗時的影像，然後，這些影像其實由 Amazon 公司保存，住戶再經由雲端調閱這些影片。

以資料做為基礎的監控稱做資料監控(data surveillance)。在此可引用美國國安局 Keith B. Alexander 所說過的話來說明，資料監控就是先把資料通通收起來，為了日後容易查找，先做好標記及相關後設資料的分類，比如時間、地點、關鍵詞、人名等。先大規模收集資料，日後如有需求，再去查找，這就是資料監控的現況。

監控下的資料蒐集與分析往往是在權力不對等的情況所進行。對於大量資料的蒐集，一般人並沒有資訊能力進行資料處理及分析。更重要的是在大部分的情況下，個人並沒有強制的權力進行大規模的資料蒐集、處理與分析，但國家或政府至少在某些情形下卻有權這樣做。被蒐集資料的這一方，其實也沒有多少管道了解其個人資料被蒐集、處裡及利用的情形，所以這裡就產生了非對稱的權力關係。

當個人察覺其個人資料、行為資料一直被蒐集、處理，而且不知道會被保存多久，會被怎樣分析的時候，會不會導致行為上有甚麼樣的改變呢？ Mary Hui 這位記者於 2019 年 6 月 12 日紀錄並報導香港的示威活動，提到參與示威者寧願用投幣買單程地下鐵車票，也不用八達通（類似臺灣悠遊卡的電子票證），因為使用電子票證時，如為記名的交通票證，持卡人的交通歷程資訊都留存在經營交通運輸的公司手中；即使是不記名的交通票證，事後也可能透過串接勾稽出持證者的可能身分。所以，示威者如不想讓自己陷入那樣的風險，就必須要改變原本的行為模式，例如寧願用零錢買車票，或改變原本計畫不參與示威，改採其他方式參與。從這個事件可以看出，當個人察覺其資料被蒐集、處理利用時，可能會改變原本的行為和意念。

與監控有關的一個技術是所謂的持續識別碼，意指識別碼與其所連結的物件、人物、或活動將會持續一段時間不變，且通常以電子方式存在個人的數位足跡裡。透過識別碼可以去拼接不同屬性的個人資料。有些物件，比如電話，除了電話號碼本身，手機有其唯一的號碼、SIM 卡也有其唯一的號碼：IP address、e-mail address、車牌號碼、電子票證號碼都是。然後，關於人物，比如臺灣人民終生一號的身分證字號、信用卡卡號、銀行帳號、跟消費紀錄相關的會員卡號，以及登入網站的 login name、在 social media 上的名稱等均屬之。雖然有些持續識別碼可能會

隨著時間更動，但是至少仍持續用一陣子。活動也是可有持續識別碼，例如交通紀錄、etag 紀錄等等，都是活動的紀錄。持續識別碼可以被機器讀取，處理上也非常方便，因此普遍存在於日常生活的各處。持續識別碼雖然可能不一定是唯一的（比如說網頁瀏覽器 Browser 的 cookie 也是持續識別碼，但當清理 cookie 或無痕瀏覽時，可能就沒識別碼了），但即使識別碼不是終生唯一，但還是可以在一段時間內有效的串接個體與活動紀錄間的關係。

剖析、描繪 (profiling)，剖繪是透過已鎖定特定群體或非特定個體的資料所推演出的額外資訊。比如政府有時候為了社會福利制度、措施等，有時會對少數民族或某社會經濟地位層級的群體進行剖繪，了解政府資源有沒有被好好使用。日常生活的剖繪，常見於消費行為的分析。在社群媒體張貼照片等，其實就是個人自願告訴社群媒體公司，張貼照片的時間，而且往往伴隨著地點、跟誰在一起等內容以及背景資訊，這些資料也常一併被蒐集。

將監控與剖繪相比較，一般認為監控是全面的，剖繪是比較破碎的。例如使用悠遊卡雖然資料留存散佈在不同的公司（悠遊卡公司、手機公司或電信公司、或車牌監理單位等），但是因為有持續識別碼，所以使散佈在各資料來源間的資料，能夠很容易再串接在一起。而在數位時代提供剖繪的破碎資料多半就是數位足跡 (digital footprint)。數位足跡裡通常含有持續識別碼，因此即便資料散佈於不同來源，還是可以透過持續識別碼把資料串在一起。當很多數位足跡串連在一起時，就可以變成一個非常精細的剖繪。如果是做一個大規模、很精細的剖繪，這個就成了監控。

在上述的認知下將很容易理解，目前國民身分證字號的使用方式，即讓它成為一個功能強大的超級持續識別碼，因為其他的持續識別碼，例如車牌號碼、手機等，最終都註冊在同一個身分證字號下。身分證字號因此能串接各個資料、串接數位足跡，剖繪就變得分外容易，分外精細。

Box 1-2 數位監控系統：中國社會信用體系的殷鑑

中國存在數個監控體系，近年推動的社會信用體系僅是威權國家全面監控體系之一環。社會信用體系本質上與商業信用體系相關，只不過中國將商業信用體系的商業指標替換成政治指標，成為更徹底的社會監控。

一、 強化社會控制的嘗試

大規模監控之所以存在於中國，要從威權國家一直很想知道人民或幹部到底在做什麼事情，並付諸實現開始。過去沒有電子媒體的時代，主要靠著非常類似臺灣早期人二室的人事檔案系統進行追蹤。直到現在，中國的人事檔案系統仍存在且運行著。人事檔案系統的運作主要依附在機構單位，每個人必須歸屬於一個機構單位，才會有一份人事檔案。而目前只有幹部仍保有人事檔案系統。依據人事檔案系統，若大學畢業後並非擔任幹部，就不會繼續在人事檔案內追蹤；但如果擔任幹部，人事檔案將會透過機要專線轉到所屬的部門。大部分被記錄的人，終其一生都無法看到人事檔案系統的紀錄。凡屬學校的操行及各種政治評價都被紀錄在人事檔案裡面。但是，人事檔案系統並不是全面的，而且主要透過人工的書寫，所以，就主政者所獲取的資訊量來說，相較於電子或數位的社會監控，人事檔案系統的資料相對較少。

職是之故，中國當局一直在思考如何在保留人事檔案系統的前提下，進行更廣泛更具規模的監控。螞蟻金服下的芝麻信用與商業信用體系的概念與運作模式，給中國當局很好的啟發。芝麻信用是與顧客進行交易時，一種給顧客信用評比的積分指標。在芝麻信用體系裡，每個人都有一個分數，如果信用極好，進行交易時會比較方便。同時，中國當局借用芝麻信用的評分機制，導入商業信用體系的概念，只是把商業信用指標換成政治信用指標，再結合網際網路與行動個人裝置，於是產生了社會信用體系。

雖然過去人事檔案某種程度扮演黨管社會的一個角色，但因為對象與運作模式的限制，所能發揮的功能有限。然而，當黨管社會與科技網路結合，全面性的效果就出來了。社會信用體系可說是黨管社會與科技網路的一個邂逅。

中國社會信用系統的概念與運作模式在何種條件下可以複製或輸出到中國以外的國家，必須進一步檢視該國是否具有類似中國的操作環境。這

個系統在中國得以得天獨厚的順利運作，由幾個因素加乘而得。

首先，中國是全世界虛擬交易最蓬勃的國家。在大部份的其他國家，例如美國跟日本，大部分交易其實則仍然使用現金或信用卡。依據觀察，中國的虛擬交易從 2010 年到 2012 年的間突然暴增成長，雖然現在仍在尋求直接證據，但論者均高度懷疑背後可能有國家機器的推動。中國讓人民靠著習慣虛擬交易過生活，當人民的日常生活離開不了虛擬交易，而進行虛擬交易必須要有信用評分，人民從日常生活開始就必須一直仰賴政府提供所謂的信用指標。

二、 社會信用體系的建置

2014 年中國頒布社會信用體系的計畫與建構綱要，開始與商業公司合作，透過商業公司的協助，逐步完善這套社會治理的架構。同時，各地開始進行試點，並成立「社會信用體系建設領導小組」，由各級發改委負責牽頭。

社會信用政策推動的表面理由，是為了讓民眾維持好的信用，以推進社會主義的先進文明。但若進一步觀察，即能瞭解社會信用體系是一種獎懲措施：信用太低不能購買火車票，不能申請好學校，子女不能申請學校，不能申請好工作等。信用評比低，將成為個人一生的恥辱、標誌，永遠跟著走。社會信用體系懲罰信用評比低的人，其背後之目的為何？這意味人民必須追求政府所規定的良善，因為黨教你怎麼做好人。

當商業指標提升為政治指標，表面上看起來沒什麼差異，但後者卻蘊含維穩的思維。例如，不贍養老人扣五十分，其目的是為了促使人民可以贍養老人，為政府分憂解勞，國家就得以穩定。網路言論詆毀他人扣一百分，目的就是言論控制，禁止造謠，不要攻擊別人，以維持社會的穩定和諧。圍堵黨政機關的鬧訪扣五十分，意味就算有冤屈，也不要到機關鬧訪，為了顧全大局，繼續維持表面的和平。酒駕扣五十分，因為中國有許多社會不穩定事件是酒駕引起的，而這些由警方處理事情的背後，常會涉及一些人事關係等，所以常有很多社會不穩事件其實是警方處理不當造成。

社會信用體系的真正用意是由黨設定怎麼做好人的指標，以控制個人，這已經和商業交易沒有太多關連。符合黨的期待，指標分數就會高。一個人的分數太低，也會影響其交友，因為與低分者交友，分數會因此被

拉低。一旦被黨或被社會唾棄，就自然會被孤立。這是讓異議份子被孤立的方法。

事實上，中國正全面在各級政府推動社會信用體系，雖然各地的作法不一，但都宣稱在 2020 年完成。然而，因為體系的運作會牽涉到諸如牽頭部門的國務院發改委（國家發展和改革委員會）和其辦公廳、地方的經信委（經濟和信息化委員會）以及中央的工信部（工業和信息化部）等許多不同機關單位，各單位間的整合仍然有許多待解決的問題。例如當分數低不能買火車票，這時會牽涉到交通部門；分數低的子女不能申請好學校，就涉及教育部門；分數低的人不能買房子，這時則涉及城市住建部門。因為背後所涉及的條條塊塊太過於複雜，目前各地還在整合中，再加上疫情的關係，進度稍微緩和，目前還未見很明確的作法。

社會信用體系的特徵是每一個人都被配賦一組獨特的識別代碼，像是身分證字號的社會信用代碼。進行虛擬交易時，包含借書、租房、買房等，都可透過這個代碼進行。當輸入信用代碼時，系統會串連很多部門的資料，最後總結出一個整合性的評比。簡單來說，每一個人民都有一組代碼，代碼背後都有一個分數；分數高者被允許做很多事情，甚至租房可以不用繳租金；分數低的人連買車票都不行，特別是如果你曾經闖訪機關。

對社會治理或政治學而言，中國的社會信用體系的特殊之處在其與西方先進國家的信用評比相較，有兩個最大的差異。第一，西方先進國家的信用評比 (credit scoring system, CSS) 基本上只用於融資信貸，主要是商業銀行核發貸款或涉及商業、工作的一個依據；但中國的社會信用評比卻深入至各個領域，其本質上是一項政治評比，並非單純的商業信用評比；社會信用評比對人民而言已是一個全面的控制。第二，在資料保障方面，銀行信用評比基本上只在金融機關或當事人所知悉的單位才能取得，而中國的社會信用評比是公諸於大眾，亦即無論相關與否，都可以知道他人的評比，完全沒有隱私權的保障。

三、 社會信用體系與當代中國的社會治理

中國社會信用評比體系對於威權國家的治理而言，大幅降低治理、監控的成本。以邊沁或傅柯的圓形監獄概念來理解，中國社會中的每個人都在這個圓形監獄裡面，自己對自己進行自我審查，達到社會控制的目的，因此降低了國家監控的成本。

中國社會信用評比系統是一種受歡迎的科技威權主義，也就是這種信用

評比體系與過去傳統威權體系相較，常受到人民的歡迎與擁戴。中國人民多數認為政府透過社會信用體系，幫大家把持住信用，因此並不覺得有什麼問題，反而認為是西方國家想太多了。到底是慣於自由民主與人權的社會錯了，還是民主國家的憂慮是對的？中國人民多數並不認為其已被控制，這反而是最恐怖的地方。過去的威權體制，人民多半會知道被控制，知道鬧訪時被打壓，被限制居所，甚至其他親戚朋友也都被監控；但社會信用評比是個受歡迎的威權控制體系，是人民心悅誠服的接受、喜歡這個系統，然後甘願被監控。

此外，中國的社會信用評比系統也透過一些被中國管控的市場機制運作。當政治跟科技還有商業的結合，大幅降低威權國家管控社會的成本，而且這是種讓人民心悅誠服的管控方式，人民不知道自己被監控，反而會為威權國家說話，所以運作成本是低的，控制風險也是低的。這是一種人類全新的管制方式，一開始可能是跟商業公司學的，但是透過中國智庫的轉換，現在變成一種全新的控制方式。

中國的社會信用評等制度在其他國家是否有實踐與複製的可能性，端視其他國家是否已建立起一套相類似的數位基礎建設，使虛擬交易的社會實踐得以存在。此外，由國家主導的評等標準雖也是中國社會信用評等的特色，但即使非由國家主導，受歡迎的科技威權主義仍可能以私部門的形貌出現。

2. New eID 的數位足跡與監控風險

內政部雖宣稱 New eID 的卡片有效性驗證程序是由使用端下載「憑證廢止清單」的方式進行，因此使用 New eID 時並不需要與內政部連線，所以內政部對身分證的使用過程並無資料可以掌握，無從記錄使用者使用 New eID 的足跡，也不可能對 New eID 的使用過程進行監控。

然而，內政部的說詞混淆了兩個不同的問題。內政部所規劃 New eID 的晶片分區中涉及晶片的使用行為其實可分為兩類：第一類為使用自然人憑證的第四區，稱為數位身分驗證；內政部再三強調，自然人憑證區可以由民眾自主選擇開啟／關閉。第二種使用類型則與第一至第三區塊（戶籍地區、公開區與加

密區）有關；這三區的功能是單純的「數位身分識別」，因為不涉及以憑證進行身分驗證，僅透過晶片識別你到底是誰，或至多在臨櫃或虛擬環境中進行晶片「資料的驗證」。「數位身分驗證」（第四區）的功能如內政部所稱，可由個人選擇關閉。但「數位身分識別」或「資料驗證」（其餘三區）的功能則無法關掉，每個人都被強制要求在 New eID 上有這三區的晶片資料（此與德國允許個人關閉晶片身分證上全部的晶片功能，保留單純無晶片功能的塑膠卡，在保障個人自主權上有很大的差異）。

區分「數位身分驗證」與「數位身分識別／資料驗證」的目的在於，前者在身分驗證過程中確實不會在內政部留下任何紀錄，且憑證功能也可依個人的選擇而關閉；但後者在每一次使用時，都會在需用機關留下包含有數位身分識別資料的數位足跡，比如為了門禁安全管制，由保全人員插卡或感應進行數位身分識別，這時身分證當事人的身分資料，就被紀錄且留存下來。所以，即使關掉 New eID 的自然人憑證功能，僅使用晶片身分證前三區的識別資料，也仍然會在使用過程中留下紀錄，這就是所謂的數位足跡。

固然「數位身分識別/資料驗證」類型中的「加密區」，依目前規劃僅限依法授權的需用機關（包括公務、金融、醫院等）才可藉由 secure API 讀取，讓加密區的數位足跡蒐集似乎具備法令的依據。然而，身分證持有人往往無法掌握哪些機關是法律授權的需用機關、所謂的需用機關究竟讀取了哪些資料、需用機關蒐集數位足跡資料後又將如何使用、需用機關是否在蒐集後將資料儲存再隨時依其需求使用、如何審視需用機關使用資料的法律依據及可讀取蒐集的資料種類、內政部將如何控管需用機關及是否具有相關機制。更大的挑戰在於，「戶籍區」與「公開區」的數位足跡蒐集，並不以需用機關有法律授權為必要，無形中擴大了濫用的可能。

數位足跡究竟會造成什麼問題？當大量國民日常生活的數位足跡被留存下來，就有可能被用來進行分類、分析，並形成前述所提到的人物誌或角色設定 persona。Persona 就是針對不同類型的人，會有甚麼樣的特性，加以模組化。Persona 在某些情境或對特定需求可能具有用處，例如，進行市場行銷時可更精準地瞄準目標客群，分析各種類型的人群可能會喜歡的產品或需求。當然 persona 也可以用在其他用途，比如上次美國大選時，競選團隊利用劍橋分析所做的 persona，類型化與標記人群，並對其個別使用不同手法做政治宣傳，針對立場比較偏向民主黨支持者的意識型態，或思想比較偏向自由派，就以投其所好的特定方式，對其進行政治宣傳。

New eID 當事人一旦留下數位足跡而未予規範，一方面可能被拿來形成 persona 做各類應用；另一方面也可能隨時以公共利益之名被拿來利用。以陳其

邁副院長 COVID-19 論文中所揭露的事實為例，政府透過電信公司的個人手機訊號擷取的移動軌跡，進行所謂的疫情調查。原本電信資料並不在政府手中，但只要資料被產出並且被留存，一旦有需要，政府就可能以公共利益之名蒐集與利用。

簡言之，數位足跡的存在離未來可能隨時被取用後進行監控，其實有時候只是一步之遙。只要留存了數位足跡，就有可能被拿來使用的一天；如果數位足跡沒有被留存，基本上就不可能發生後續的監控問題。

3. 因應數位足跡監控的外國法制規範模式

為了因應公私部門蒐集、利用數位足跡可能帶來的問題與疑慮，各國在推展晶片化與數位化過程中，也負責任地提出對抗數位足跡的法制規範模式。以日本、德國、愛沙尼亞及比利時為例，可歸納出兩種規範模式。

第一種類型，以法律直接禁止或限制數位（身分）足跡的蒐集。日本法律即限定蒐集個人編號 My Number 的數位（身分）足跡，僅限公務機關或受託行使公務的機關，為社會福利、稅務或者災害對策目的。所以，日本是在非常限定的目的下，才能做數位（身分）足跡的蒐集及利用，其他與前述無關的目的都不可以蒐集。德國也採取此一模式，原則禁止串連並限定留存數位（身分）足跡，如非有權確認身分的機關要蒐集數位身分資料前，必需經過主管機關的事前許可，始得為之。德國透過前端事前管制的方式，要求僅於相關主管機關許可下才可以蒐集數位身分資料，而且不得蒐集含生物特徵的資料，甚至，身分證影本也不能隨意再使用，並禁止使用自動化的方式取用身分證個人資料。德國同樣是以法律明文禁止使用身分證做資料庫間的資料串連，除非具有法律明定的其他例外情形。比利時也採取限定蒐集與限定留存的規範模式，規定敏感性身分個資（比如照片或身分證字號）需另有法律或法規命令為依據，才可進行蒐集、處理利用。若非以身分識別之目的而讀取身分證，及為進行身分識別目的後的資料留存，都需另外取得主管機關的事前授權許可，始得為之。

對抗數位監控的第二種規制模式則採「反向監控」sousveillance 的策略。當政府或商業公司在蒐集數位足跡時，由個人反過來對政府及商業公司取用資料的足跡進行監控。例如，日本透過資訊提供等紀錄開示系統，允許個人可一次調閱完整的數位足跡被調用/使用的日誌，確保個人對於其個人編號 (My Number) 有控制權。另一個反監控的例子則為愛沙尼亞，其個人資料獨立專責機關 (Data Protection Inspectorate, DPI)，負責監管其他政府部門取用資料的行為是否符合個人資料相關法律、法令規定及機制的要求。所以，政府部門蒐集

數位足跡的行為受到 DPI 的管制，同時 DPI 對於私部門之個資利用也同樣有規制的權力及監管的權限。除了 DPI 的監管之外，愛沙尼亞還有資訊系統管理局，提供個人資料追蹤服務 (data tracker)，要求政府在資料庫的使用必須要留下足跡，且提供個人查詢。所以，當事人可透過資料追蹤服務系統，清楚地知悉政府部門取用個資的時間、目的等，可以反過來追蹤政府，希望藉此能讓政府在個人資料的取用，符合民主課責的原則。

以上這兩種法制的規範模式，都可用來對抗數位足跡廣泛使用的情況。但對照臺灣目前 New eID 的規劃，內政部僅再三強調憑證的使用過程中不會蒐集個人的數位足跡，卻避重就輕刻意不提「數位身分識別功能」仍將遺留數位足跡，拒絕立法進行規範，坐實以晶片身分證進行數位監控的懷疑。

四、現行法無力因應數位化/晶片化帶來的挑戰

針對各界質疑 New eID 的發行將對臺灣的自由民主體制帶來威脅，呼籲應另定專法以便因應，內政部則不斷宣稱目前已有《資通安全管理法》、《電子簽章法》與《個人資料保護法》，強硬回應沒有另定專法規範晶片身分證的必要。

然而，內政部所提到三部法律當中，資通安全法由行政院（資安處）主管，電子簽章法由經濟部主管，個資法則由各目的事業主管機關與國發會進行相當分散的管制。此一破碎化的管制體系，能否因應身分證晶片化與身分個資數位化帶來的挑戰，已有疑義。若進一步檢視三部法律之實質內容，即可發現三者事實上均未針對上述發行 New eID 所涉及的資安、國安與人權威脅風險，有任何規範。

首先，《資通安全管理法》（簡稱資通安全法）的規範對象是「公務機關」以及「經指定為關鍵基礎設施提供者之特定非公務機關」，並課予訂定資通安全維護計畫的義務。該法在面對 New eID 的問題上，存在兩個規範困境：第一，資通安全法並未從資通安全設施之涉密人員的出境管制、外包廠商之最終資金來源、股東適格性與系統元件共用風險等角度進行全面規範；第二，資通安全法並不適用於承包設計與製造晶片身分證的國外廠商，以及開發相關晶片身分證應用軟體的國內廠商（因為均非被指定之關鍵基礎設施提供者），因此即使僅為安全維護計畫的低度管制模式，也完全不適用於目前承包 New eID 發行的各類軟硬體廠商。

其次，《電子簽章法》的立法目的雖在確保電子交易安全，促進電子化政府及電子商務之發展，但其實質內容僅在規範「用以辨識及確認電子文件簽署人

身分、資格及電子文件真偽之方法」得以成立與生效的條件，並未針對電子簽章過程所遺留數位足跡之蒐集、處理與利用，有特別之限制規定。
內政部僅仰賴《個人資料保護法》（簡稱個資法）做為管制數位足跡的規範依據，但個資法目前並未針對數位身分足跡的蒐集、處理與利用，制定特別禁止或限制的規定，僅適用個資法第 16 條、第 19 條及第 20 條針對一般個資可廣泛蒐集並供目的外利用的現行規定，任令身分證數位化/晶片化帶來監控風險。相較於整體數位化程度極高的愛沙尼亞、德國、比利時，與近年亦極力發展數位化的日本，均在其國內一般的個資保護法制之外，特別制定專法規範晶片身分證使用過程所產生數位足跡的蒐集、處理與利用，審慎因應數位化可能對其自由民主體制的威脅，內政部以我國已有個資法為由，拒絕正視數位化/晶片化產生的新威脅，並非妥適。

最後，因應數位化/晶片化對自由民主體制威脅的一個必要機制是獨立且權責相符的個人資料保護專責機關。但到目前為止，專責機關的設立仍無具體進展。

第二章 強制發行晶片身分證的法制基礎檢驗

內政部宣稱，晶片身分證的換發已具有相關法律規定，主要法律依據是戶籍法第 51 條、第 52 條及第 59 條。按其主張，戶籍法第 51 條規定「…身分證用以辨識個人身分，其效用及於全國…」，即可推知身分證可提供公、私部門間個人身分辨識之用，因此，內政部可以強制發行身分證。另外，戶籍法第 52 條及第 59 條之規定，亦分別授權內政部有身分證格式決定權。

對於內政部所持的法律主張，應進一步思考兩個問題：第一，戶籍法第 51 條真的可作為強制換發不限定目的及對象、供全國公私部門使用，且任其取用第一區戶籍區、及第二區公開區資料的晶片身分證？第二，從紙本到晶片身分證，真的只是格式的改變嗎？

一、 《戶籍法》第 51 條身分證的全國性身分辨識效用

回顧歷史，戶籍法最早出現在民國 20 年，當時法條文字既無身分證也沒有身分證字號。「身分證」一詞最早出現在民國 33 年的戶籍法草案中。爾後，35 年戶籍法才正式將身分證制度納入。不過，按當時法律規定，得由政府發行的身分證，是作為人民享有權利與履行義務時，主管機關查驗身分之用。

值得注意的是，35 年戶籍施行細則有個與現行法第 51 條有關的條文：「…身分證的效用及於各地，無庸隨地換發。」因當時各省縣可發行各自身分證，在推行時發生爭議，例如在 A 地發行的身分證拿到 B 地可不可以使用等問題，所以，施行細則訂定所謂「及於各地」的條文，即便處於不同省分，身分證仍然有效，不需隨地另行換發，所以，「及於各地」的原始用意為此。

「及於各地」的文字一直到民國 87 年，戶籍法才將文字修正為「及於全國」，並移除後面「無庸隨地換發」等字，而成為今日第 51 條規定。換言之，戶籍法第 51 條有關身分證辨識身分的效用「及於全國」，並非指個人負有以國民身分證「向全國各地之公私部門證明自己身分的義務」，而僅指身分證可供全國各機關依法確認個人身分之用。這可由民國 37 年動員戡亂時期發行國民身分證的實施辦法得知，發行身分證的目的是為了管理人口遷徙跟敵我識別，及作為機關配賦權利義務，人民身分證明之用。

在此，可得到一個初步的結論：戶籍法授權主管機關發行國民身分證的目的，是以國家與人民之間的關係為範疇，作為機關配賦權利義務時，人民身分證明之工具。雖然，在日常生活中，身分證已經被廣泛地使用在國家與人民間關係以外之其他的場合，但戶籍法本身仍只在國家與人民之間關係的目的與範疇內，才授權主管機關強制發行身分證。換言之，戶籍法第 51 條所稱國民身分證的全國性身分辨識效用，應依其究為個人權利或義務，區分為「法定的強制身分辨識義務」，與事實上提供予個人的「任意性身分證明方法」；前者是戶籍法授權強制發行身分證的目的，後者則欠缺強制為之的法律基礎。

是以，前述晶片身分證第 1 區（村里鄰戶籍區）及第 2 區（公開區），如開放允由當事人自由選用，勉強可認為仍未違背法律保留原則。但倘依內政部目前強制登載第 1 區及第 2 區之規劃，恐已超越戶籍法授權的範圍。

二、《戶籍法》第 52 條身分證格式決定權的授權範圍

內政部在推動晶片身分證政策時，經常提到以德國、愛沙尼亞為師。而臺灣本身的戶籍制度則與日治時代臺灣的戶口制度有關聯性。基於以上理由，以下即以德國、愛沙尼亞、日本為對象，與目前政府對於 New eID 的規劃與法律制度進行比較與研析。

德、愛、日三國雖均有身分證，但其實質內涵與使用規範，與臺灣有諸多不同之處。德國雖規定強制領證，但替個人編派統一編號在德國被認定為違憲，所以德國並沒有像臺灣一樣一人一號的統編；日本雖規定每人應配賦一人一號的 My Number，但並未規定強制領身分證，個人仍可自由決定領卡與否；愛沙尼亞既有一人一號的身分證統編，也有強制領證的規定，但愛沙尼亞仍沒有像臺灣定有強制攜帶證件的規定。臺灣在學習其他國家成功發行晶片身分證經驗的時候，必須理解各國在制度上的背景條件。

晶片身分證外國與台灣法制比較 I

	德國	愛沙尼亞	日本	台灣
終身一人一號	X	●	●	●
強制領證	●	●	X	●
強制攜帶證件	X	X	X	●
基本的個人資料保護法	●	●	●	●
專法規範晶片身分證	●	●	●	X

德、愛、日雖有上述差異，但其共通之處在於，三者均於基本的個人資料保護法之外，再制定規範晶片身分證的專法。三國的專法除了針對晶片身分證的發行給予法律的授權基礎，界定個人選擇晶片化程度的權利與義務，主要也是更嚴格地規範晶片身分證產生「數位資料」後的蒐集、處理與利用。

德國雖強制發行晶片身分證，但專供身分驗證及電子簽章的憑證（自然人憑證）功能則屬選擇加入 (opt-in)，僅於當事人決定購買時，身分證上才會附加憑證，強制發行的身分證本身並不預設置入憑證。此外，當事人也可選擇整個關閉晶片身分證上的晶片功能。換言之，德國雖強制發行晶片身分證，個人仍可自行選擇完全關閉晶片功能，讓身分證成為一張單純的塑膠卡。

日本在領卡上並非強制，因此晶片卡的身分識別、驗證或簽章功能可說全部由個人選擇加入 (opt-in)。

愛沙尼亞雖可自由選擇退出 (opt-out) 憑證功能，但卻強制規定晶片身分證必須要有數位身分識別功能。這樣的設計表面上與臺灣目前的規劃相似，但愛沙尼亞身分證的數位化與晶片化程度，卻是建立在其獨特的制度與文化條件之上。首先，愛沙尼亞設有個資保護的專責監理機關（而臺灣現在還沒有），負責對公私部門蒐集處理利用個資的行為，進行管制。其次，愛沙尼亞政府過去針對資安事件均展現出負責任的態度，在資安攻擊之後，政府除承認錯誤外，也積極尋求改善之道，使人民對政府產生信任感。再者，愛沙尼亞在法律上高度保障個人資訊自主權；早在 1997 年的個資法中，即以優於當時歐盟個資指令的標準保障個人的資訊自主權。最後，愛沙尼亞所在的北歐社會具有極強的社會連帶傳統，個人不僅較願意與他人共享權利，也願意共擔義務。凡此均是愛沙尼亞得以成功推動身分證晶片化及數位化政府的真正原因。

晶片身分證外國與台灣法制比較 II

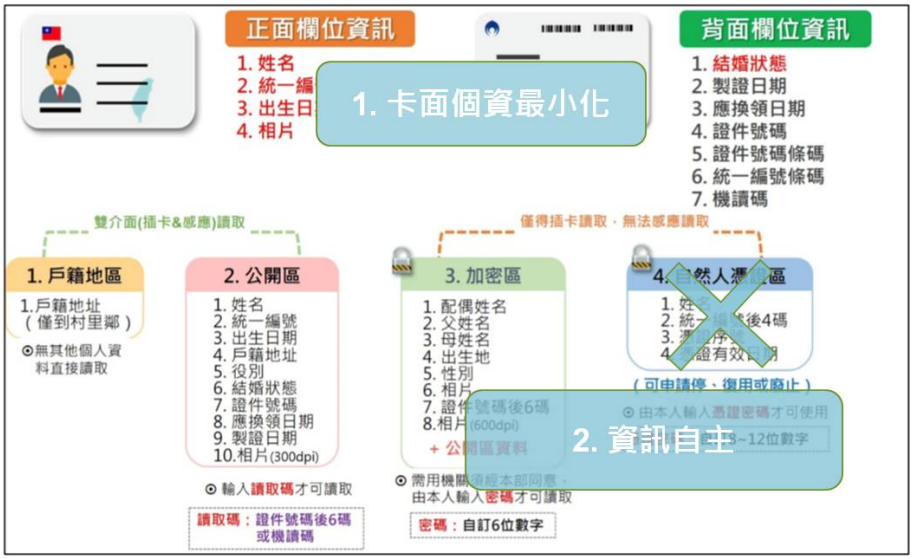
<table>
<tr><th></th><th>德國</th><th>愛沙尼亞</th><th>日本</th><th>台灣</th></tr>
<tr><td>數位身分識別</td><td>Opt-out</td><td>●</td><td>Opt-in</td><td>●</td></tr>
<tr><td>數位身分驗證</td><td rowspan="2">Opt-in</td><td rowspan="2">Opt-out</td><td>Opt-in</td><td rowspan="2">Opt-out</td></tr>
<tr><td>近用授權（電子簽章）</td><td>Opt-in</td></tr>
<tr><td>身分資料取用限制</td><td>●</td><td>X</td><td>●</td><td>X</td></tr>
<tr><td>身分資料串連限制</td><td>●</td><td>X</td><td>●</td><td>X</td></tr>
<tr><td>個資專責保護機關</td><td>●</td><td>●</td><td>●</td><td>X</td></tr>
<tr><td>個人對政府足跡之監督</td><td>●</td><td>●</td><td>●</td><td>X</td></tr>
</table>

從德國、愛沙尼亞、日本的比較研究後可以得知，身分證的晶片化因為涉及數位時代資料的蒐集、處理與利用，對於「誰」可以「為了什麼目的」使用身分證「蒐集甚麼資料」等，均須以專法予以規範。而身分證專法起碼必須將內政部對 New eID 的規劃加以法制化，而不可僅以招標文件的方式隨意為之。

三、 New eID 限制個人資訊自主違反法律保留原則

內政部宣稱，其所規劃的 New eID 與原紙本身分證相較，具有「卡面資料最小化」及「資訊自主」兩個優點，因為部分的紙本卡面資料將轉存在晶片，未來晶片卡的卡面資料將比現在的紙本身分證減少，符合卡面個資最小化的要求；同時，New eID 分別在晶片第三區（加密區），提供個人自訂密碼控制資料的近用，也允許個人決定是否關閉第四區（自然人憑證區）的功能，賦予個人資料釋出的控制權。

然而，相對於可自主選擇關閉的第四區（自然人憑證區），其他三個晶片區塊（第一區－村里鄰戶籍區、第二區－公開區、第三區－加密區）在目前內政部的規劃下仍屬強制，亦即，身分證晶片上必須具備並登載身分資料的區塊，不容個人自主選擇關閉，因此 New eID 並非如內政部所稱更能保障個人的「資訊自主」。



縱然「資訊自主」的個人權利並非絕對不得予以限制，但其限制仍必須符合「法律保留原則」與「比例原則」的要求。而依目前內政部的規劃，至多僅有第三區（加密區）可能滿足上述檢驗。

依照內政部在招標文件與對外釋出文宣品的說明，「加密區」僅限執行法定業務所需的需用機關在申請 secure API 後才可近用讀取。就此而論，目前法源資料庫系統中，法令條文明白規定應蒐集或可蒐集國民身分證的法令有 95 筆，而提到蒐集國民身分證統一編號的則有 74 筆。後者雖未直接提及國民身分證，但國民身分證統一編號的蒐集常與國民身分證資料之讀取相連結。若以相對寬鬆的標準來檢視，「加密區」若僅開放予依法令規定在執行法定業務中應蒐集或可蒐集國民身分證資料的公務或公務機關使用，形式上或可謂符合「法律保留原則」，但執行該等法定業務是否都「必要」以數位化的資料為之，因此須將身分證「晶片化」，則是「比例原則」下應予檢驗，卻從未見內政部說明與回答的問題。此外，將「加密區」的使用限定於法定業務的規劃，目前僅是隨時都可能變動內容之「招標文件」當中的敘述，並非法律的明文規定，也因此全無「法制化」的擔保。

更大的問題存在於未限定目的、無自訂密碼控制的第一區（村里鄰戶籍區）及第二區（公開區）。依內政部目前規劃，任何人只要下載 open API，都可能取用登載此二區的身分資料。第一區與第二區的用途因無限制而可包羅萬象：日常生活常見利用身分證統一編號的某個號碼或是尾數，享免費美食或折扣；或是為配合防疫採取實聯制，掃描身分證條碼，即可得到身分證字號的資料。這些沒有法令依據，理論上屬於個人自願選擇採用的「任意性身分證明方法」，因無法律限制其利用目的，事實上已到了氾濫使用的地步。然而，依據內政部目前的規劃，個人卻不被允許選擇關閉第一區與第二區的功能，形同限制「個人資訊自主」。

四、 強制蒐集高解析度相片並錄存於身分證晶片違反釋字 603 號解釋意旨

高解析度（300 dpi 以上）相片在人臉辨識技術逐漸成熟的今日，已具有個人單一獨特識別性，而成為一種生物特徵。相較於同樣具有個人單一獨特識別性的指紋，甚至蘊含更多與個人有關的生物資訊。而依據內政部之規劃，New eID 的換發將一併強制蒐集個人的高解析度相片，並在晶片的公開區中錄存 300 dpi 相片，於加密區中錄存 600 dpi 之相片。

然而，依據司法院大法官釋字 603 號解釋，以強制方法大規模蒐集國民生物特徵資料，應以法律明定蒐集目的，其蒐集應與重大公益目的之達成具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。《戶籍法》雖授權內政部發行身分證，但母法之授權並不包含強制蒐集高解析度相片並錄存於身分證之晶片中，與大法官釋字 603 號解釋所要求高度的法律保留原則不符。

另從比例原則加以檢驗，則身分證上的相片若僅為臨櫃身分識別之用，並不需儲存於晶片中，亦無儲存高解析度相片之必要；若專為非臨櫃之網路環境中使用，則網路環境中之身分識別或驗證既不可能仰賴相片為之，則儲存高解析度相片之必要性即不存在。儲存高解析度相片所欲達成之不明確目的，相較於在欠缺法律明確禁止法定目的外使用，而可能被用來發展與利用人臉辨識的風險，並不符合比例原則。

第三章 跨機關業務資料共享與整體智慧政府計畫之可課責性評估

一、 T-Road 僅著重公部門間資料介接的技術工程，輕忽資料串接交換所需的法制基礎與管理規範

1. T-Road 的去中心化設計惡化目前「個資保護治理破碎化」的困境

行政院於 2019 年通過以晶片身分證 New eID 及跨機關資料交換網路通道 T-Road，亦即建置一個類似高速公路的概念，讓資訊可在其上自由地流通跟串接，做為打造「智慧政府」的兩個主要基礎架構以達成政府的數位轉型。然而依據目前的 T-Road 規劃，國發會僅負責建置跨機關資料交換的網路與傳輸平台；關於資料交換得以合法且正當進行的法制基礎與管理規範，則仍歸各部會負責，並稱此為「去中心化」與保留「機關資料自主權」。

就跨機關個人資料交換的合法性議題，其實目前各界對此就已存有疑慮，例如是否須以作用法之授權為必要或僅有組織法已足的疑義，此類合法基礎之挑戰在 T-Road 資料共享平台建置後，將更形複雜。因為機關跟機關間的資料共享或交換，原本須通過層層紙本公文程序才得以完成，現在 T-Road 上只須一個按鍵後，資料就能快速地透過 T-Road 傳輸分享。對此，理應有更嚴密的管理機制把關，但在相關管理機制尚未完成前，仍以回到各主管機關去中心處理時，可能會產生各機關就機關間資料傳輸的合法性有標準不一致的情形。

2. T-Road 建置目的以資料自主為名隱含公權力擴權疑慮

然而，政府建置 T-Road 事實上存在兩個不同的理由：一方面， T-Road 被形塑成為個人在智慧政府中實現「個人資料自主利用」的必要工具，因為個人從公部門下載自己的資料或者同意他機關取用其個人資料，除了透過晶片身分證提供使用 MyData 前的身分驗證外，還需要有跨機關資料交換網路通道。另一方面，規劃中的智慧政府也暗示要透過跨機關間包含個資在內的資料交換共享，即除了透過當事人同意的方式，經由 MyData 或是另外的 T-Road 入口網，去介接或存取不同機關的資料之外，各機關之間也可利用 MyData 以外的其他途徑，不經當事人同意即在 T-Road 上完成資料串接交換，達成以「資料驅動」為核心的「優化決策」目的。

補充說明，個人資料自主利用可說是 OECD individual participation 原則的延伸。GDPR 其實也有類似的權利，包括資料查詢權、資料刪除與被遺忘權、資料可攜權等。為實現自主，提供資料當事人查詢及資料可攜的應用服務，是一種當事人對於其個資近用控制的概念，主要運作方式係由當事人或當事人授權第三方，將 T-Road 作為不同政府機關及單位間資料大量傳輸的渠道，以達跨政府機關資料庫之資料串連目的。

3. T-Road 目的多重卻曖昧隱身使真正需要的課責機制難以建立

倘若 T-Road 之目的單純僅在協助個人實現資料自主利用，則除了 New eID 將來可用來申請哪些服務、適用範圍如何、是否在政府服務外亦適用於委由民間提供或民間經營的金融或醫療服務、如何規範等問題，在目前公開規劃文件中並不清楚，仍有待釐清之外，目前分散由各部會自理的資訊隱私治理模式，尚勉足以因應。

但倘若 T-Road 的目的也包含促進跨機關資料共享，使政府能進行「資料驅動」的決策，則在在欠缺有效外部監理與專責監理機關的現狀下，「去中心化」的治理模式只會導致破碎而無效的監理結果，無能管理 T-Road 使公部門能快捷便利地共享國人個資所帶來的風險。

除政府跨機關資料交換之合法授權基礎疑慮外，政府若欲以資訊科技之應用——亦即資料驅動——來優化政府決策、達成數位轉型之目的，在實際運作上，仍有尚待解決之問題。例如，必須先把法令的授權事項轉譯成電腦能執行的指令，在針對個別情況作出判斷時，原本行政機關的裁量空間必須轉成資訊系統可以操作的精準規範，也因此有一種「類似立法 (Quasi-legislation)」的效果。解決此問題的一種做法是制定規範，且須提高立法技術，讓立法更精確，但並不容易，何況若規範訂得太細，導致行政僵化、縮減原有之裁量彈性空間，當未來需要因時制宜而修正時，成本將大為提高；另一解方則是要求系統有清楚易懂的文件說明，並將這些文件說明視為是類似行政機關的法規命令，讓受該系統決策之影響、受此類似立法規範效果之人民得以預見、司法機關並得加以審查，才有可能符合法治國原則下法律明確性之要求。

4. T-Road 僅流於「流程數位化」而未觸及真正需要的「流程再造」

目前國發會的 T-Road 建置計畫針對目的不明確的跨機關間資料交換，僅流於「流程數位化」而未觸及「流程再造」，僅將數位轉型理解為由「國發會」提供新的技術工具給「各機關」執行原有的任務，而忽視「各機關」應重新檢討原有流程在數位化後是否產生過去未有的新挑戰。

在缺乏整體流程再造的思維，而僅認為提供新技術工具執行業務，也就是單純地將業務流程數位化時，在法規與檢視管理規範與配套時，很容易落於既然原業務執行相關規則早已存在，繼續沿用即可的窠臼；卻忽略過往的路跟現時的路已不是同一條的關鍵事實。

非數位化系統跟數位化系統，二者有不同的問題與風險，絕對需要不一樣的管理與規範方式，而且基本上，很多系統管理上的細節，必須要對該系統上使用的新科技，加上對相關法律或規則有一定的理解，才能有效處理。

二、混淆意在限制機關資料蒐集權限的「資料一次性原則」，與破壞目的外利用禁止原則的的跨機關資料流用

部分歐盟國家在保護個人免於政府過度侵擾的精神下，規定政府機關向個人蒐集資料應以一次為原則，此即所謂「一次性原則」(The Once-Only Principle)，；其他有權蒐集個資之機關在他機關已蒐集過相同個資的情況下，若非經個人同意，不得再向個人蒐集，有若干國家直接將此原則定性為人民之權利，亦即人民有主張僅須提供一次資料給政府的權利。制度上，其為歐盟單一數位市場的一環，是為便利歐盟會員國之間共同市場中資料的跨境交換、減少文件傳遞之障礙及不便而設，因此也是實現歐盟公民遷徙自由的一個途徑。

惟此原則之具體內容，歐盟各國在實踐上尚無定論，而我國目前關於一次性原則的規劃及適用，僅見於國發會在數位政府的策略與跨政府資料交換的規劃中提及「資料輸入一次到處可用」，也就是 T-Road 及 MyData 政策規劃，然而其中並未釐清究竟是要賦予資料當事人有權拒絕政府過度的個資蒐集，或是便利資料當事人可將其在 A 機關之個資授權 B 機關取用的作法？具體規範及措施事實上並不清楚；又，我國沒有歐盟單一市場及跨境移動之需求，採用此原則的必要性為何？凡此皆未見政府具體說明。

退萬步言，縱使我國為提升政府服務效率或便民而確實有仿效歐盟採行「一次性原則」之必要，歐盟各國採用「資料一次性原則」並未因此即放寬「目的外利用禁止原則」的要求。其雖預設所蒐集之資料可能得以直接提供目的外利用，但這不應作為打破「目的外利用禁止原則」，而建置超級（虛擬）資料庫的藉口，而建置超級（虛擬）資料庫的藉口（包含以提供他機關為由而於特定目的完成後仍永久保存資料的情形），隱私權的基本權保障仍然應該優先，這也是為什麼歐盟即使採行一次性原則，其仍受 GDPR 的規範，而在我國既有的法規架構下，資料之目的外利用當然仍須遵守個資法。

三、智慧政府的規劃因欠缺可課責性的內涵而無法建立社會信任所需的制度基礎

1. 先上車後補票的智慧政府推動策略

智慧政府的推動既以跨機關資料利用為核心，則資料利用的治理即為建立可課責性的關鍵。但依目前智慧政府的規劃，內政部將 New eID 定性為「推動智慧政府關鍵的鑰匙」，但其理由何在？關鍵性何在？是否有配套措施？這些也應該告訴國民。所有科技工具都無法保證百分之百的安全性，必定有風險。那麼，目前的風險管控及課責機制為何？國民都了解嗎？另一方面，負責建置 T-Road 的國發會則同樣怯於擔負起資料治理的責任，拒絕提供個人對跨機關個資交換的次數與所交換個資之內容進行查詢的可能性，使人民無從對政府利用其個資進行必要的民主監督控制。整個 T-Road 系統若未清楚記錄各機關交換資料的內容、次數、目的、範圍、時間等（依個資法個人有獲知這些資訊的權利），個人就沒有辦法知道各機關交換了哪些個人資料、也就無從行使請求機關停止蒐集、利用、處理個資的相關權利。

再者，資料驅動 (data-driven) 的決策模式，運用大量資料分析，是否一定能優化決策、資料品質如何、資料怎麼被使用等等，這些內部過程以及結果都很難被大眾檢視。當系統發生錯誤，或既有偏見被內建在系統設計中所造成的決策偏誤，都可能更難被發現。進一步言，若人民欲挑戰行政機關之決定，過去只要具備法律知識即可，但政府實施數位轉型後，若想要挑戰系統決策偏誤，須兼具對於法律及資訊系統的了解，對人民而言門檻非常高。

在智慧政府的規劃中，對於未來可能利用跨機關資料進行資料驅動決策的各部會，並未要求應建立資料治理機制及規範。所謂資料治理，包括「政府據以做出決策之資料，其品質控管」、「究竟需要／實際取得多少以及哪些資料」、「是否因應不同決策內容而有不同資料類型的需求」等，因資料運用將影響系統判斷的結果，對以上各該事項，都應有更完整的資料治理機制與規劃，以確保政府決策所依據之資料並無偏誤，及演算法之應用正當。

政府於政策規劃初期時期必須先確認目的，以及提出明確具體的作法。在設計制度（「路」）規劃前，作為制度骨幹的規範原則（「道」），必須先行確定。此外，工序也是重點，因為就算整體目標正確，只要工序出錯，結果仍舊無法達成目標。為求亮點及先求有再求好的 KPI 文化，在欠缺跨機關資料治理機制也無個人資料保護專責機構的監督真空下，將可能帶來荒誕的後果。

例如，MyData 及 T-Road 等服務目前已試營運或接近啟用，New eID 也已箭

在弦上，政府卻一直要等到出現輿論壓力，才表示願意開始考慮設立個人資料保護專責機關的可能。個人資料保護專責機關理應在各項數位智慧政府政策開始推動前就先建立，而非待各項數位政策上路之後，才急就章式地要成立，迫使該機構必須遷就現狀去解決問題。這樣不但無法從根本解決問題，且將使一個獨立監管機關淪為錯誤政策的遮羞布。

再者，個資當事人必須知道各機關基於哪些目的蒐集了哪些個人資料，使個資當事人至少能預想資料經調用後進行串連可能的結果與範疇。例如，美國要求各機關必須符合 SORN (System of Records Notices) 的規定，亦即機關單位須公告其所蒐集的資料欄位清單，以及各資料蒐集的目的等。

在當事人無法得知（資料提供）機關及（資料接收）機關或單位持有哪些個資的狀況下，（資料接收）機關或單位可能透過與其固有的資料進行串聯，這資料的串聯可能超越當事人授權資料時所預想範圍，此時，即便當事人同意資料傳輸，此種情況下之同意本身仍有瑕疵。

欠缺完備資料治理機制之現狀下，縱使個資法賦予資料主體各種權利，包括同意權、申請閱覽權、申請刪除權等，也將形同具文。人民權利保障幾乎被完全架空；又，在個資保護專責機構尚未立法設置、尚未有明確的組織架構與職掌規範之際，T-Road 計畫已先上路。如果個資保護專責事務與 T-Road 皆在同一個部會（國發會或數發部）職掌範圍內，且個資法修法及專責機構設置等重大法規變動，已在近期政府議程中，為何急著發包由外部廠商來制定 T-Road 的管理規則，而非由主管機關依職權來訂定？凡此種種，均無助於建立智慧政府所需的社會信任基礎。

2. 政府未能帶頭建立資訊安全管理與隱私維護的社會規範

臺灣社會普遍欠缺良好的資訊安全管理意識與資訊隱私維護文化，目前平均每年有約 40 餘萬張身分證遺失，而過去以來公部門與私部門的個資外洩，也幾乎成為常態。但政府對可能源自於公部門之個資外洩卻未能表現出坦然面對與積極負責的態度，除任令大量遭駭的身分個資漫流於暗網之外，亦不認為有需要通知並盡力協助每一位受害個人採取可能的補救措施（例如更換身分證字號），迥異於被其標舉為智慧政府標竿的國家：愛沙尼亞；對於私部門的個資外洩也同樣未予有效的監理。愛沙尼亞政府除肯認個人資料歸屬於個人資料當事人，政府亦承擔起保護其所持有之個資的責任；當民眾與政府形成良好關係，信任政府時，自然較願意提供資料給政府。

相較於愛沙尼亞透過良性互動所形成的智慧政府成功經驗，反觀我國在各

項政策的設計理念上通常只單向地強調「增強使用者的安全意識」，卻完全忽略政府本身應該扮演的積極角色。在此條件下強推全面換發晶片身分證政策，除了智慧政府的虛名外，難以贏得真正的社會信任。

附件一

研議小組成員意見書

國民身分證晶片化的資安威脅與個資隱憂

李育杰

中央研究院資訊科技創新研究中心　研究員

談到內政部預計推行的 eID 政策時，最常被談到的就是晶片身分證的資訊安全議題。但是，資訊安全所涉及的層面相當廣，可以包含硬體安全、軟體安全、系統安全，甚至是管理安全等，這些都非常重要。不過，到目前為止，內政部僅一直保證晶片身分證的資安絕對沒有問題，一再強調晶片非常安全，甚至是軍規等級，但卻完全沒看到內政部對於讀卡機具相關安全管理規劃與機制，也沒有看到針對身分證當事人隱私保護有進一步的管理規劃，令人憂心。

本篇文章將就晶片身分證的晶片與身分證使用時潛在的資安風險作觀念釐清與舉例說明，同時再度強調資訊安全無絕對保證，但資安風險卻是可控管的觀念。

一、　晶片潛在的資安風險

先簡單整理晶片可能涉及的資安風險，通常包含晶片製造的過程，可能會有私密金鑰的外洩；採用非接觸式的通訊介面讀取晶片身分證，可能造成卡號、無讀取碼保護的資料外洩；以及當身分證遺失時，身分證的自然人憑證功能很可能被有心人士拿來偽裝電子身分。

二、　讀卡設備潛在的資安風險

除晶片可能存有潛在的資安風險之外，跟晶片身分證最相關的，就是讀取身分證的讀卡設備。有關讀卡設備的潛在資安風險，大抵可分為讀卡設備本身的資安風險，及與讀卡設備連接之運算裝置的資安風險。讀卡設備本身的資安風險，可能起因於讀卡設備被安裝惡意側錄的元件，所以在使用讀卡機時，資料就已經外洩了；或者是讀卡機出場時，讀卡機本身或甚至公司裡面的員工可能就有問題；或即便讀卡機沒有問題，但當保護機制沒做好，讀卡機就很容易就成為駭客攻擊

的弱點。與讀卡設備的連接裝置也是另外一個需要注意的地方，連接裝置可能被植入惡意程式或木馬，這時也可能造成資料外洩；或是受到MAN-IN-THE-MIDDLE－中間人的攻擊，從資料傳輸時擷取資料。以上為讀卡設備常見的潛在的資安風險。

再次檢視內政部最近一次的招標文件，完全沒有提到讀卡設備的資安風險。在內政部 New eID 的簡易問答集內，也沒有看到與讀卡設備相關的規範與機制。該文件只有提到身分證已有三個法律規範：包括資通安全管理法、個人資料保護法，自然人憑證部分則有所謂的電子簽章法。即便如此，但是，臺灣仍然沒有像日本、德國、愛沙尼亞，就晶片卡有專法規範。

三、　對身分證當事人潛在的資安風險

談到身分證當事人潛在的資安風險時，最主要是要談資訊自主。按目前內政部在 eID 所規劃的第 3 區 - 加密區，主張因為身分證當事人可以決定是否要開啟自然人憑證功能，符合當事人自主。不過，就個人所知，按內政部在第 3 區加密區與第 4 區自然人憑證區的規劃，兩者是結合在一起的。即便當事人可提出申請關閉自然人憑證功能，但如果沒有提出請求關閉就是預設開啟。所以，事實上，當事人並沒有辦法做到完全的資訊自主。

再者，雖然，內政部表示第 3 區為加密區僅限依法授權的需用機關（包括公務、金融、醫院等），加上使用 secure API 才可讀取，而就內政部的回應，確實，第 3 區加密區的需用單位是可以得到身分證使用的數位足跡。但是，當身分證當事人根本無法控制或掌握哪些為法律授權的需用機關、所謂的需用機關讀取了哪些資料、需用機關讀取蒐集資料後將如何使用資料、需用機關是否可於讀取後將資料儲存隨時依需求使用、內政部將如何審視需用機關使用資料的法律依據及可讀取蒐集的資料種類、內政部將如何控管需用機關及是否具有相關機制、是否有專法規範等，對於需用機關還有非常多的疑問。

但是，到目前為止，內政部僅回復：將於政策推行後，才會推出更細部規劃。因為目前針對身分證的使用者、使用細項等，完全沒有法律規定，這也是為什麼筆者主張要有專法的主因。試想看看，當需用機關只需要出生年月日，但是需用機關輸入密碼後，卻可取得加密區全部的資料。這時，加密區給的資料比需用機關需求還多時，內政部要怎麼處理這個問題？

在愛沙尼亞、德國、和日本，因為有專法，民眾可以大抵知道機關將會如何使用這些數位化的資料。雖然內政部戶政司一直在強調學習愛沙尼亞的作法，但

是，卻沒有類似的規範。當沒有身分證專法時，身分證當事人無法知悉與了解需用機關將如何使用身分資料，也無從知悉資料是否有轉給第三人。

筆者建議，當向先進國家學習成功經驗時，他國成功經驗成就的必要條件也應該備齊後，才能推行 eID 政策。

四、 資訊安全無法保證但可得管控

談到資訊安全時，可以知道的，是資訊技術永遠可發現資安漏洞，然後在發現漏洞之後再補強，所以攻擊技術的發展，往往先於防禦技術的發展。所以，資訊安全是完全沒有辦法永遠保證的。資安公司與資安研究學者所能做的，是在資安防禦技術面上做偵測、阻絕，還有延後系統被攻破的時間。更重要的是，系統沒有 100%安全，當系統被攻破時，必須具備控管風險的能力，甚至是要求迅速地復原系統。這是目前提供資安服務、資安研究等，一個非常重要的方向。

李德財院士在擔任國安會諮議委員時，極力主張資安即國安的觀念。簡單來說，其實只有在利大於弊時才能做。一個有資安概念的國家政策，應當想辦法把資安風險最小化，同時，因為有新技術的採用，公共政策也需要隨之調整，除非這個公共利益大過背後的風險時，才可以來實施。

五、 通過安全認證不表示絕對安全 - 以自然人憑證、悠遊卡為例

確實，日常生活使用晶片卡非常普遍，你我身上可能有幾張類似的晶片卡，例如：悠遊卡、自然人憑證都是晶片卡。悠遊卡和自然人憑證其實都是通過一連串的安全認證的晶片卡，悠遊卡公司也一直號稱絕對不可能被破解，晶片卡看似應該是很安全的，但並不全然。舉例來說，2010 年鄭振牟教授在駭客年會上 demo 用監聽的方式篡改悠遊卡的餘額；2011 年就有一位臺北某科技大學畢業的工程師，就直接拿破解的加值加密系統直接去消費且盜刷成功；及 2013 年台大鄭振牟教授曾經破解自然人憑證的金鑰系統。

那麼，或許有人會提問，悠遊卡既然這麼不安全，為什麼還在使用？這個問題，悠遊卡公司總經理受訪時已有回復過，悠遊卡具有相關配套機制，讓悠遊卡更安全。因為悠遊卡所有的消費記錄是可以稽核的，帳如果對不起來，公司就知道系統可能有一些問題，這時就可以開始追蹤。當悠遊卡被盜刷的時候，公司早就知道了。總經理說，發生問題時沒有馬上處理，反而讓卡片繼續使用的原因，是公司想要知道盜刷的手法。而且，就算有人盜刷，也很容易被發現，現時對於

盜刷者也有相關的法律責任規範。所以，悠遊卡雖然可能有資安風險，但是發行數量龐大，如果為了一個可能的風險、小漏洞，要把卡片全部收回，可能不符合成本效益，經與資安問題容易偵測的權衡之下，還是可以繼續使用。

但是，將悠遊卡與即將推行的eID相比較，目前內政部所規劃的數位身分證，並有沒有這些特性。所以，當晶片身分證不具與悠遊卡類似的相關特性與機制時，以悠遊卡為例說明晶片卡的安全性，比較基礎與說服力道是顯不足夠的。

另外相信各位應該有注意到，前一陣 2000 多萬筆個資外洩事件，事實上是已經外洩多年後，被置於暗網販售。對此事件，內政部第 1 次的說法是否認資料為內政部資料外洩，後來，內政部又改口說這個資料是舊的。筆者不確定，這是政府對於資料外洩時，該負責任的態度？

舉一個很簡單的例子，錢掉了，馬上看得到。個人資料被偷了，你知不知道？大概在 2016 年左右，第一銀行 ATM 發生問題，錢一不對，大家就開始找問題，所以很快地發現，還有機會把這錢追回來。但是，如果外洩的是個人資料，外洩好幾年後，才被發現在暗網販售，政府還可以說這是舊資料？

六、 加密後資料仍有外流風險

從前述所舉案例可知，資料即使加密後還是可能外洩。重點在於，當駭客破解了密碼，往往是不會張揚，也不會講的。在模仿者遊戲電影裡面也曾經提到，當 Alan Turing 破了密碼後，就知道德軍即將要轟炸英國的艦艇，但是他們選擇寧可犧牲這些艦艇，也不會說出來。所以，資料真實可能存在的風險與威脅，是十分容易想像的。

另外，現在很多人都在談量子電腦，也不知道是不是已經有量子電腦了，但兩年後，後量子密碼的標準也許會發佈，為什麼政府要在量子密碼新標準問世前，在這個時候仍採用舊的、可能成為潛在量子電腦威脅的密碼系統，令人十分不解。

七、 資料數位化使資安風險提高

接續，晶片身分證的採用，勢必使資料數位化。資料經過數位化後當然會很方便，但值得注意的是，在數位化的同時，資料也更容易取得、更容易編輯、更容易散佈傳播。所以，當個人的隱私可能變成是別人的方便，是不是要強制換發晶片身分證，是值得再三思考的。

事實上，就目前可得的資料所知，單在 2014 年就有 44 萬張身分證遺失，那未來那張更便利的 eID，是不是更容易遺失？然後，再加上，數位身分證使數位化的資料更容易取得、更容易編輯、更容易散佈傳播的特性，會不會有更多外洩的個資在外面流傳？再者，當身分證遺失的數量多到一個程度後，是不是讓駭客更容易知道背後的系統該如何破解？

八、 新技術=進步？以人臉辨識系統為例

再來，新技術是不是就代表進步？以人臉辨識系統為例，舊金山市去年即禁止使用人臉辨識系統；微軟最近也剛刪除所謂最大的、公開的，約有 1000 萬筆的人臉資料庫；前一陣子的 Black Lives Matter 之後，IBM 也宣稱要退出人臉辨識系統；IBM CEO 甚至寫公開信，說明這個技術可能淪為種族歧視的幫兇，所以，對於新技術的使用，其實是需要去反思的。當新技術具備有一定的便利性時，可能要去檢視是否同時具有管理的配套機制，才能使問題減緩或風險降低。

九、 結語

最後，再次強調資安是絕對無法保證的，但資安風險卻是可控管的。透過分散式的設計本身就是一種安全機制，Alan Turing 告訴我們，當敵國或他國的駭客國家隊，一旦破解了密碼通常不會張揚，就繼續取用資料。

就目前推動 eID 政策而言，法律規範與管理機制尚未整備前，臺灣政府還沒獲得人民眾的信任以前，臺灣是不是準備好了？

T-Road 的資料庫串連與數位身分證的近用控制

查士朝

國立臺灣科技大學資訊管理系　教授

一、 T-Road 與 X-Road

從相關資料可以發現，T-Road 其實本身是參考愛沙尼亞 X-Road 的機制，比較起來兩者確實十分相似，但目前看來 T-Road 還是比較針對民眾的近用控制，而沒有處理到有關於不同單位之間的存取。其實我們有時在參考國外的制度或工具，常會與國外的實際狀況產生齟齬。像是新聞上面提到，T-Road 參考 X-Road 會加入區塊鏈的應用，但是以 X-Road 來說，它本身沒有區塊鏈的機制，甚至在我們智慧政府推動的一個策略計劃裡面，也有提到會用到區塊鏈的技術。但是愛沙尼亞的 X-Road，實際上就是沒有用到區塊鏈。另一個例子是，在一些愛沙尼亞談到它們 X-Road 經驗的文章中提到，愛沙尼亞政府非常重視「資料是屬於人民」的一個看法，政府必須要好好保護資料，保護資料民眾才會信任政府、才會提供資料，不然民眾不會提供資料給政府。這樣子的說法，很明顯地與我國在 T-Road 的設計理念上提到的「增強使用者的安全意識」的想法有所差距。這會讓人懷疑，我國政府是否在面對資安事件時，僅會單方面要求使用者要加強資安意識，而沒有要努力保護民眾的資訊安全。

二、 MyData

其實我們在談近用控制的時候，可以發現 MyData 和近用控制非常相關。以歷史發展角度來講，近用控制可說是從 OECD 的 individual participation 原則的延伸。而從 OECD 八原則到 GDPR，其實有相當多類似的權利，包括本人資料查詢權、資料安全性、資料刪除與被遺忘權、資料可攜權等。MyData 跟近用控制，主要在於查詢跟資料可攜的概念。回到 X-Road 的架構裡面，如果說是以個人的近用控制來看，T-Road 與 X-Road 其實也類似，就是核心上是以 MyData 的角度來去驅動資料交換。

以下說明對於 MyData 平台的相關議題與建議。首先，在近用控制面來講，美國有提供 SORN(System of Records Notices)的要求。所以到一般美國政府的網站上時，都會有一個專頁在談有關 SORN 的資料，點進去之後就會看到，到底這個單位蒐集了哪一些資料，以及為了哪一些目的蒐集。我們的個資法也有這樣子的要求，只是我們很多時候到政府網站上面都找不太到相關資料，而其實我們政府在網站上面如果有這樣一個資訊公開的設計會比較好。相關單位的遵法程度，可能需要國發會來做一些整理，而且可能也需要成立一個專責的、個人資料保護的機構。

其次，資料交換的部分，以 MyData 或 T-Road 來說，其實比較專注在針對特定機關，去邀請它們做資料交換。然而像是剛才提到的 SORN 等個資相關的規範，理論上其應能涵蓋整個我們國家政府機關的範圍，而不是僅限於願意參與 T-Road 的部分單位。因為事實上存在部分單位，該單位發覺 T-Road 有些機制不能符合單位本身的要求，於是就自行來做資料分享機制。此時相關的個資規範，是否能涵蓋到該單位自行創建的資料分享機制，就成為一個必須關切的問題。

而在資料下載上，MyData 目前的功能，第一個是提供本人檔案，第二個是存到一個 storage 上面，然後由 storage 直接提供另外一個單位去存取資料。此種情況下，我們可以看到，當一次都是以一個檔案為單位的時候，本身來它就會欠缺一些資料最小化選擇的方式。舉例而言，如果我今天要去辦某個證件，它只要我健康體檢報告的結論部分就好，不需要提供完整檢查細項，但系統上只能提供完整報告，此時就有違反資料最小化原則的疑慮。

此外，若在提供資料時沒有像 SORN 的機制，則當事人並無法知道對方到底有哪一些我本人的個資，在此情形下，接收資料單位可能透過與其固有的資料串聯方式，進而超越當事人授權資料提供時所預想範圍，獲得更多個人資料。例如辦便利商店會員註冊時，可能悠遊卡消費綁電子發票並無大礙，但當紅利點數與悠遊卡投資的一些公司來做綁定之後，交通紀錄跟購物紀錄或許可以連結起來，此時再與會員資料連結，可以說資料就被完全掌握。因此，今天必須知道到底在分享時，對方已經有什麼樣的資料，才能有更好的決策可能。

最後是身分鑑別的議題，目前 MyData 在身分鑑別上，主要提供方式有二，第一種是當事人自行下載之後，以 QR code 臨櫃提供；第二種是線上直接提供。但在使用情境下，其實需要多一些考量。例如使用者臨櫃要拿實體卡片去存取時，要輸入 PIN 碼，而在現在手機都支援 NFC 的情況下，等同在他人面前輸入 PIN 碼，在按的過程裡，相關資料直接曝光，故本文建議針對類似情境，應事先設法避免。

三、 eID Card

最後是關於 eID 卡片本身的議題，首先是關於隔離環境設計的部分。未來 eID 可能要做電子投票的功能，電子投票本身是在隔離的環境底下進行，那網路不能連結要如何驗證卡片真實性？舉例來講，悠遊卡本身因為有考慮到離線的問題，所以它要用特規的讀卡機，裡面有特殊的 SM 卡。信用卡的話，它其實會直接引發連線。所以如果要做電子投票功能設計的時候，要考慮到這種隔離的環境。

另外目前 eID 本身的設計很多是參考到護照的 ICAO 卡片，這是大家常忽略到的地方。簡單就 ICAO 來講，政府單位有一個 DS signer 的部分，它簽了每一個 ePassport 的資料，放在護照裡面。此時用一般的程式去讀，其實就可以很簡單地輸入一些 PIN 碼去讀到護照裡面的資料。從 ICAO 文件，可以發現說，一般來講 eID 或者是現在的護照，需要有內建驗證的機制來防止卡片被複製，因此這也是我們在設計上面，如果考量到隔離情境的時候要注意到的。

稍微再說明一下卡片複製的問題，以信用卡或健保卡為例，相比於正常的信用卡、健保卡可以直接去讀取資料，今天如果是自行複製的白卡，假設沒有經過驗證的時候，其實讀取時會發生錯誤。因為沒有經過網路上驗證，所以永遠不會通過。所以當要考慮到臨櫃處理或離線處理的時候，必須要做好相關的規劃，要去考慮到相關應用情境。

最後，其實以資料分析面來說，當做了 T-Road 讓資料連結了之後，我們不只要考慮到自動決策要能夠自主選擇退出(opt-out)，其實我們還要做好所謂的資料保護風險評估(Data Protection Risk Assessment, DPRA)。另外剛剛也有提到，我們要能夠去要求資料蒐集者是真的能夠去保護資料，而不是說 T-Road 本身不拿資料就將責任一推了事，這個是我們應該要去注意到的。

四、 結論與建議

總結來講，基本上愛沙尼亞雖然一直不斷講說之前有受到資安攻擊，但其實它們只是受到 DDoS 攻擊，資料並未被大規模拿走。即使如此，愛沙尼亞政府還是不斷地自我檢討。所以我建議我國政府應該要多方檢討、溝通，以獲取民眾信任。另一方面，我們希望政府機關都要能夠有一些共通的、對個人資料保護的一些要求。同時，除了一般來說資料可攜之外，更進一步去滿足資料近用的相關法制要求。

個人資料、中國因素與國家安全

吳介民

中央研究院社會學研究所　研究員

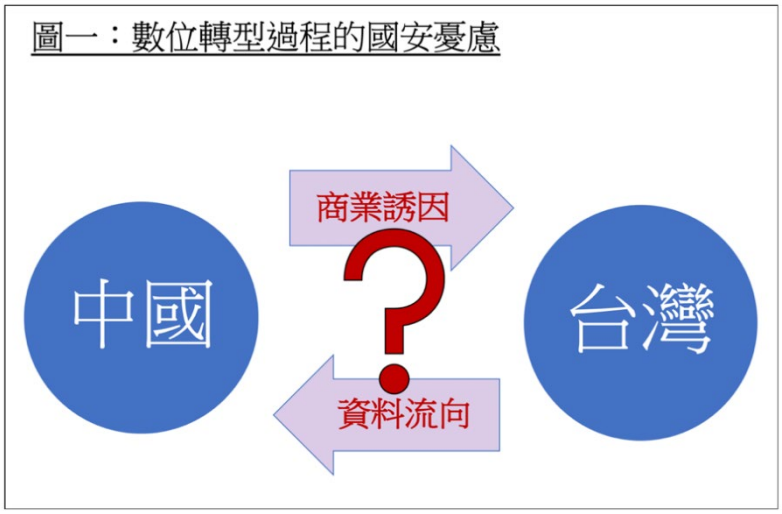
一、　數位身分個資與國家安全

數位身分個資與國家安全的關係，源自近年數位轉型的過程。數位轉型已經是當代全球政治經濟的一個魔咒，很少人會反對數位轉型，但是數位化的過程卻經常帶來資訊安全與國家安全的疑慮。

尤其是，中國政府善於使用「以商業模式做統戰」做滲透，在跨海峽的交易過程中，中國提供臺灣廠商商業誘因，就可能產生臺灣個人資料流向中國的疑慮（參見圖一）。因此，我國數位轉型過程中最重要的議題，就是兼顧現代化的效率、人權，更重要的是同時要兼顧國家安全，這三者間平衡的問題。中國因素是臺灣在從事數位轉型的過程當中，我們必須非常嚴肅討論的國安議題，更何況中國因素已經成為全球的關注焦點。

國家安全的破口，在這一次的數位身分證爭議當中大概可以歸納為三個，也就是，相對於中國對臺灣的政治戰跟資訊戰，第一個是包商的破口，第二個是營運商的破口，第三個就是中共對臺的資訊戰。

圖一：數位轉型過程的國安憂慮



二、 中國式監控資本主義

監控資本主義在最近一年，因為 Shoshana Zuboff 所著《監控資本主義時代》的出版得到比較多的關注。不過，中國式的監控主義，相比於 Zuboff 所稱的監控資本主義，其實結合了兩個很不同的元素。Zuboff 談的是「巨大的他者」(Big Other)，所謂的 Big Other 指的是，人們的個資通過極為密集的網路數位連結之後，同步發生商品化的過程，然後這個「個資商品化」的過程，變成廠商追求利潤的一個核心動力，這是所謂監控式資本主義的核心命題。

但是中國是用國家巨大的極權力量控制這個監控資本主義，所以中國的監控資本主義必須在 Big Other 上面再加上一個「老大哥」(Big Brother)，就是喬治歐威爾早在《1984》這本書提出的觀點：「老大哥正在監控你」(big brother is watching you)，而且是隨時隨地、無所不在的極權監控。所以中國式監控資本主義的要點，就是集合了老大哥的監控，加上「巨大的他者」這個監控資本主義模式的數位監控。中國共產黨的國家機器一直在駕馭資本，它的一個核心動力就是利用經濟誘因來驅動政治目標。就中共的監控政策而言，從最早從網路防火長城，之後建構中國社會信用系統，一直到現在強調網路主權，都是一貫的政策目標。這種數位極權主義的中國式監控資本主義，它不斷地培育監控技術、累積監控廠商的資本，舉比較大家耳熟能詳的案例就是，對新疆維吾爾族的監控，包括數位的工具乃至各種人體生物特徵的採集跟辨識，都是結合了龐大的商機與國家監控標的。

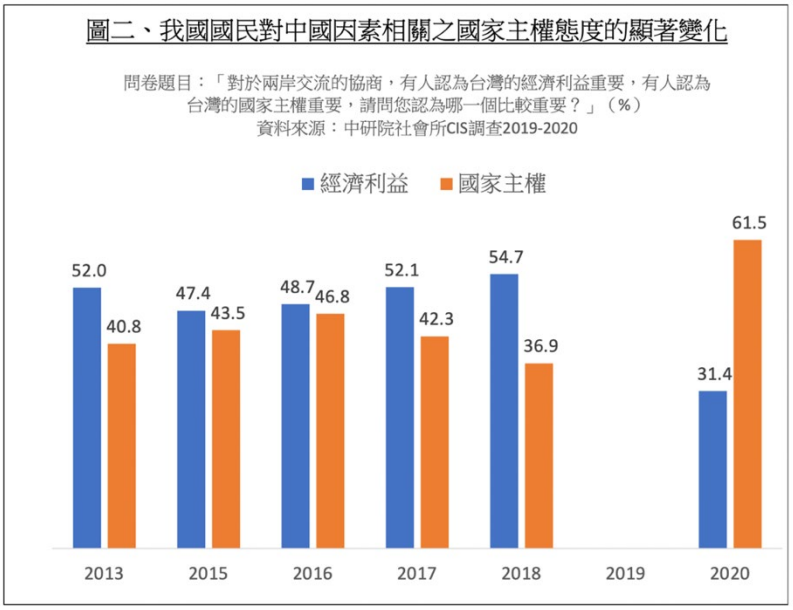
2019 年 10 月，美國商務部將 8 家中國科技公司，包括海康威視(Hikvision)和浙江大華技術（這兩家公司掌握全球三分之一監視器市場），列入黑名單，這些公司牽涉對中國新疆維吾爾族等穆斯林少數民族違反人權的待遇。商務部發布的聯邦公報指出：「具體來說，這些實體牽涉違反和迫害人權，實施中國對維吾爾族、哈薩克族和其他穆斯林少數族群的壓迫、大規模任意拘留、高科技監控。」（經濟日報 2019/10/08 https://udn.com/news/story/6813/4092139；聯邦公報相關網頁：https://reurl.cc/v16XrL）海康威視大有來頭，在臺灣也有代理商，並宣稱是「海康威視是目前全球安全監控產業的領導品牌」（https://www.digifocus.com.tw/about/brand-hik/）。

從全球監視器的密度排名來看，前 10 名城市之中，中國有 8 個，除了亞特蘭大跟倫敦之外，其他 8 個都集中在中國（https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/）。除了新疆等地，最近中國在香港實施國安法，很可能使用這些監控技術。

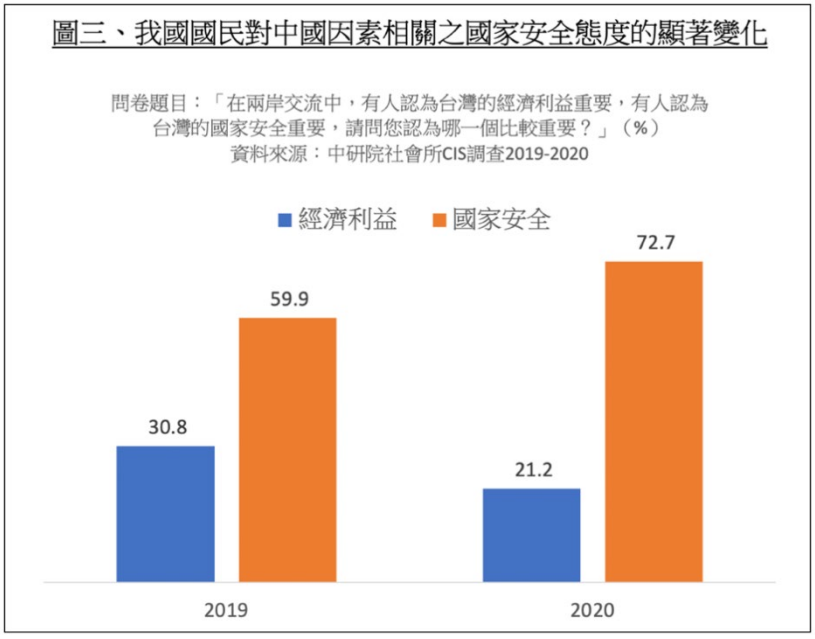
三、 我國國民國家安全意識的變遷

我國的國民，對中國因素相關的國家安全態度，近年有著非常顯著的變遷。從 2013 年到 2018 年，關於兩岸交流協商的議題，在 2018 年以前經濟利益永遠都高過國家主權，而且高過的差距是蠻顯著的。但 2018 年至今，發生了巨大變化，從 2020 年 4-5 月的中研院社會所 CIS 調查來看，認為國家主權更重要者已逆轉高達 61.5%，相對地認為經濟利益較重要者僅為 31.5%，國民態度已發生很大的變化。同一調查亦顯示，問卷題目若改以國家安全替代國家主權，支持國家安全更重要者更高達 72.7%（參見圖三、圖四）。故政府應認知到，我國國民已認為國家安全，在跟中國大陸交流時是一個非常重要的議題。

圖二、我國國民對中國因素相關之國家主權態度的顯著變化



圖三、我國國民對中國因素相關之國家安全態度的顯著變化



四、 中國對臺操作「以商業模式做統戰」分析

中國政府對臺統戰，包括銳實力滲透、資訊戰，在各個社會經濟領域當中的政治影響力操作，是無所不在、無處不在，相關案例及研究非常多。而在臺灣的數位轉型過程中，中國政府非常可能操縱臺灣的廠商，利用臺商的商業利益，做為它的載具跟平台，然後造成臺灣個資的外洩，進一步變成國安危機。關於臺灣廠商可能會受中國影響力操作的幾種樣態。

第一個就是臺灣公司同時在臺灣跟中國兩地承包同類標案，然後在兩岸都有利益關係。

第二種樣態為臺灣公司承包臺灣政府的數位標案，但在中國則為其他的經濟利益行為，例如，一家臺商雖然在兩岸並非做同樣的生意，在臺灣做 A 生意、在中國做 B 生意，但是中國一樣可以通過利益關係操縱這家臺商。

第三種樣態是臺商在中國從事數據資訊相關產業，反過頭來回來臺灣投資並且承包標案，這三個樣態我們都必須同時注意，但是就我們今天研討的主題，第一類特別值得注意。

這種「以商業模式做統戰」的操作模式，不僅限於資訊業，而是普遍存在。臺灣過去最常見的中國影響力的一個領域是媒體業，而且中國是全球性的操作，例如，美國政治學者 Larry Diamond 與 Orville Schell 在專書《中國影響力與美國利益》(*Chinese Influence & American Interests*, 2018)中點名《聯合報》，因該報老闆有興趣在中國發展事業，因此該報業集團所屬的美國《世界日報》，在最近這些年在許多議題上轉為親中立場。

五、 個案分析：中華電信與資拓宏宇

中華電信的個案分析。今（2020）年 6 月，中華電信得標新一代國民身分證(New eID)系統，中華電信轉投資一家叫做「資拓宏宇」(IISI)，資拓宏宇的副總經理同時擔任它的子公司榮利的董事長，榮利承作多家中國銀行系統工程。這個資拓宏宇公司頂層的數位關鍵高階經理人，長期是這個企業集團的核心經營團隊網絡（參見圖四）。而從其官方網站可以看出，資拓宏宇的子公司榮利，它從事金融業務，承接中國多家銀行的案子（參見圖五）。

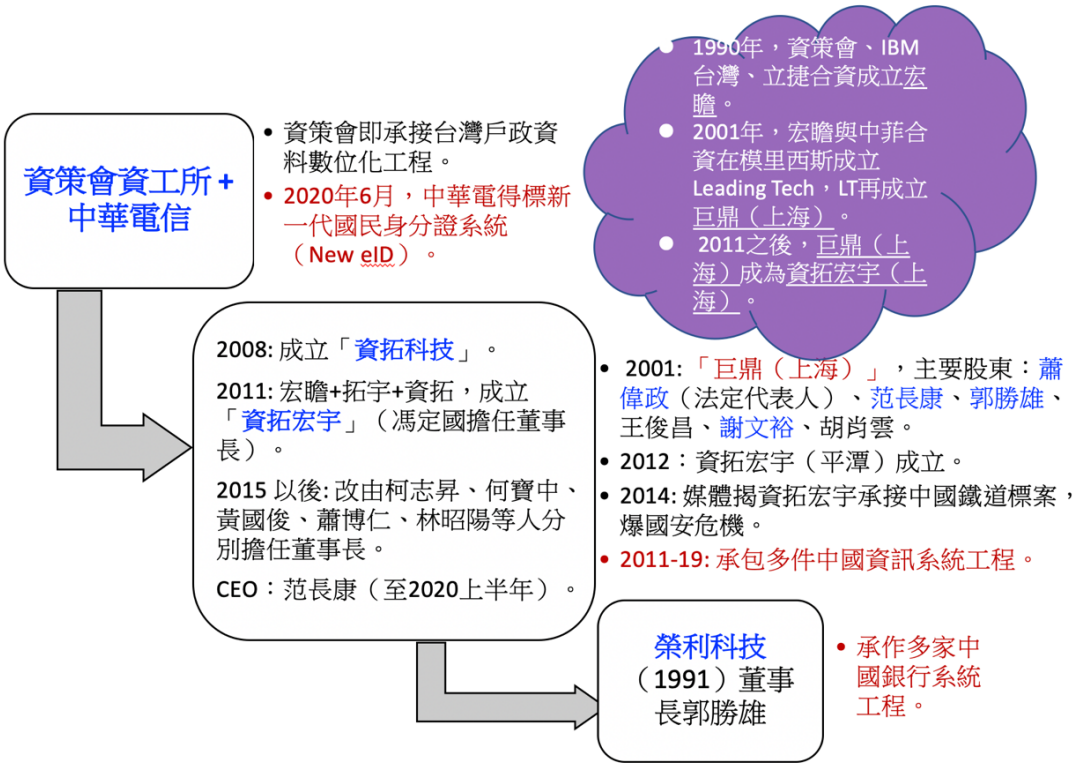
以下說明中華電信、資拓宏宇及榮利間母公司、子公司跟孫公司複雜的交叉持股跟轉投資關係。資策會的資工所，最早於 2008 年跟中華電信合組資拓科技，

到了 2011 年宏瞻、拓宇、資拓三家公司合併為資拓宏宇，其門神董事長為馮定國。馮定國四年董事長任內曾爆發嚴重國安危機新聞，當時 2014 年新聞報導很多。這個事件後，2015 之後資拓宏宇就改由不同人擔任董事長，幾乎每年都換一位，但長期擔任 CEO 職位的都是范長康（最近離職）。資拓科技最初是資策會資工所 spin off 出來，然後榮利科技是孫公司，榮利原本是拓宇的子公司，因合併才變成資拓宏宇的子公司，榮利董事長就是郭勝雄。這就是目前從中華電信、資拓宏宇、到榮利的公開資料中，整理出來的母公司、子公司、孫公司的關係網絡。

然後再仔細看這些關係，已知在 2020 年 6 月，中華電信已經得標新的 eID 系統，那我們再看這些投資關係。1990 年時，資策會跟 IBM 臺灣還有立捷就合資成立了宏瞻公司，然後到了 2001 年宏瞻跟中菲這兩家公司合資在模里西斯成立一家 Leading Tech，Leading Tech 在短期間內成立 Leading systems（一樣在模里西斯登記），然後 Leading systems 再成立巨鼎上海，之後因為公司合併的關係，巨鼎很自然就變成是資拓宏宇集團旗下的公司，所以 2011 之後就變成「資拓宏宇上海」，然後資拓宏宇在 2012 年又成立「資拓宏宇平潭」。從 2011 年到 2019 年，資拓宏宇就承包多件中國資訊系統工程，然後榮利科技根據它現在的網站，也承包多家中國銀行系統工程。

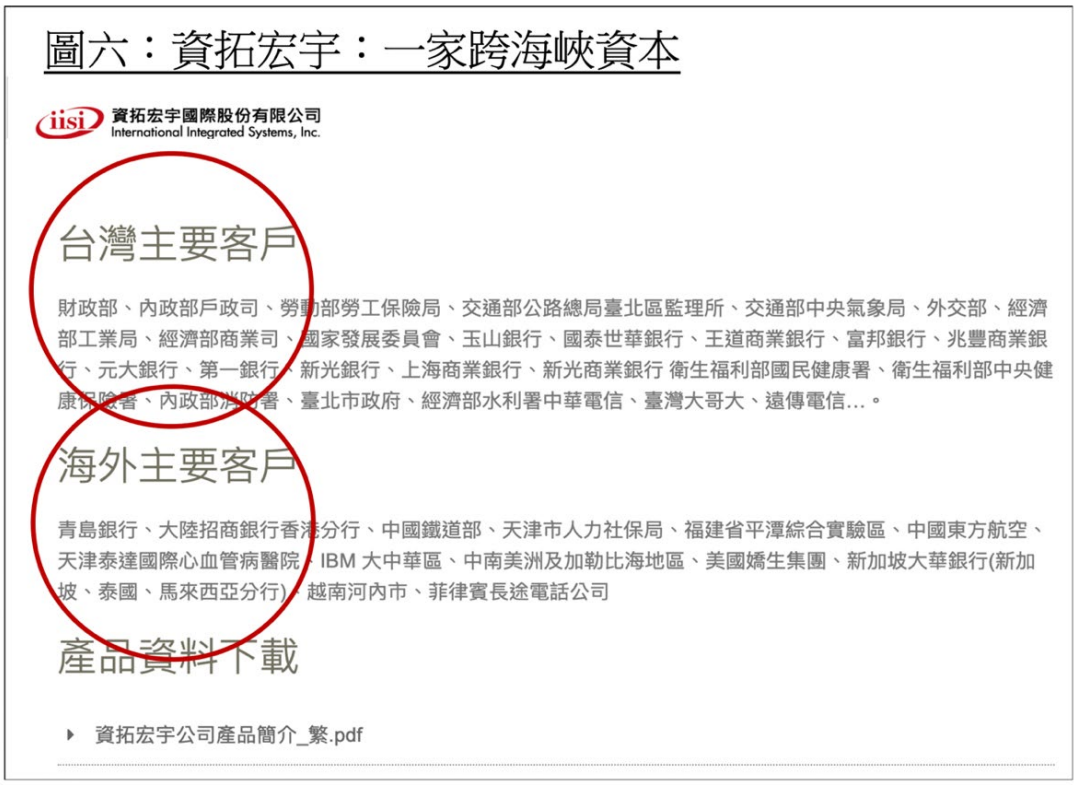
必須說明：此次得標 New eID 系統的中華電信，它整體企業集團在從事資訊業務的人事網絡，所承包或承作的資訊工程業務，呈現了跨足臺灣跟中國的模式，而且是現在進行式。根據資拓宏宇自己官網顯示，它是一家典型的「跨海峽資本」（參見圖六）。

圖四：資策會+中華電信，與資拓宏宇（子公司）、榮利（孫公司）的關係



圖五：榮利承接中國銀行系統工程

（2020年7月官網資料：https://www.e-utc.com.tw/about.html）



六、　小結

數位戶籍資料交給中華電信、或中華電集團的相關公司處理，將來可能發生層層轉包，並可能造成國安破口。以下幾個環節都值得仔細評量：

- 臺灣的資訊公司同時承作臺灣與中國政府和中國國營企業的工程，會不會採取類似系統，開發人員是否屬於同一批人員？是否會讓臺灣資安與國安出現破口？
- 中華電這家集團公司以及它的子公司、孫公司，會不會成為中國施壓的對象？是否會成為中國獲取我國人民個資的破口？
- 最後，臺灣公司是否會成為中國對臺灣進行資訊戰的切入點？

最後必須強調：中華電承包 New eID，只是諸多臺灣公司承包政府標案的其中一個案例，其他公司也應該嚴格檢驗。政府資訊工程標案中，衍生的許許多多資安與國安疑慮，主管機關須要嚴肅面對，謹慎行事。此次數位身分證標案，牽涉如此重大資安與國安的政策，在疑慮完全解除之前，政府不應貿然執行。

個資與國家安全

沈伯洋

國立臺北大學犯罪學研究所　助理教授

一、　數位時代下的中國威脅架構

以下將從中國威脅的大架構來介紹 eID 帶來的風險，主要有三個層次。首先須說明者，雖然俄羅斯跟伊朗理論上也可能造成類似的威脅，但是畢竟二者未與我們有直接敵對關係，故以下論述還是以中國架構為主。

（一）數位極權輸出

關於數位極權輸出，簡而言之就是當前在香港或是東突厥斯坦（新疆）對人民的監控技術，輸出到其他國家，像是一帶一路各國，或是白俄羅斯、辛巴威、厄瓜多等等。早期大概三年前開始做維吾爾族語的語音辨識，然後一直到前年年底，開始做所謂東突厥斯坦，就是新疆的走姿辨識，今天如果一個人過馬路稍微快一點，那他就可能被認定為恐怖份子。因為走姿辨識，亦即一個人走路的姿勢基本上不太會改變，其實跟人臉辨識是一個類似的系統。用此種方式將人的危險等級劃分成不同的九個種類，然後再根據這個種類，去把人送到所謂的再教育營，基本上跟集中營並沒有什麼太大的差別。

這些技術的輸出，會（對反數位極權國家）造成一般所謂混合戰裡面的外交戰上，非常大的不利益。像現在說要譴責中國對維吾爾族暴行的國家共有 29 個，但相對地，目前反對譴責的國家總共有 55 個。為何這 55 個國家反對譴責？主要原因就是基本上在外交戰，一般所謂的人權外交是非常弱勢的，這是第一個層次。

（二）個資蒐集

第二個層次為個資蒐集，而此蒐集行為不是以監控為目的。它最主要是會由私部門來做，可能透過公司的威脅蒐集個資，例如現在臺灣很多人在看的愛奇藝

等影音串流平台。愛奇藝透過大量獨占內容，像是夫婦的世界等韓劇來吸引民眾訂閱，這些版權獨占需要花不少錢，所以愛奇藝其實基本上是虧損的。那為什麼它還可以持續不斷地一直營運下去？簡單來講它的目的根本就不是提供影音串流服務，而是個資蒐集。更有甚者，今天如果是在手機上安裝愛奇藝的應用程式，那它將可取得位置定位、viewing preferences、作息時間等等的資訊。而如果是透過安裝應用程式於第四台電視盒的方式，當第四台在契約中要求提供身分證字號還有戶籍地址才能安裝，因一般人不會拒絕，則當這些資料再跟愛奇藝的應用程式串接時，等於是將包含我們的個資，也包含我們偏好的資訊，全部傳回北京。這些都是目前已經可以做到的事，而現在政府要推動的 eID 制度就是讓這件事情變得更容易。所以就這個層次而言，如果大家有興趣可以多看 ASPI 的報告，中國從翻譯的軟體或是影音串流的媒體，大量地在全世界來蒐集做個資。至於蒐集個資的目的為何，其實就是以下第三層次的問題。

（三）分群

北京蒐集我們個資的目的，基本上在於「分眾」，而這點必須從資訊戰或假新聞攻擊的觀點說明。最有效的假新聞攻擊，並不是今天丟一個假新聞給全體的民眾，這種做法是完全不會有效果的，因為其面臨的反作用力會變得很強。最有效果的做法，是要將訊息丟給特定的群眾，亦即要對這種陰謀論會有心裡的洞可以被填補的對象，相關的假新聞才會有用。舉例而言，一個很有名的中國愛打的假新聞叫「蔡英文墮胎」，就是蔡英文跟李登輝有姦情。這個訊息如果同時對全臺灣 2300 萬人投放，在反作用力下可想而知並不會有效果，但特定某一群具有相同特徵的人民可能非常相信這是事實，由此可見分眾攻擊的重要性，而分眾的有效性就倚賴個資蒐集的完全度。以 2016 年來講，臺灣人民就已能被歸類成大概有 60 個種類不同的分群，到現在 2020 則已演變為好幾萬種，所以如果我們把個資全部交出去的話，搭配其他公司外洩的資料，其實就可以輕易對臺灣的民眾來做分眾，然後做不同類型的假新聞，或者是陰謀論的攻擊，進而影響到我們認知領域。

二、 eID 帶來的系統風險

以上三個完全不同層次的中國影響力，係從網路世界來看，而每一個層次其實都會跟我們現在推行的 eID 系統會有高度的關聯性，以下則為 eID 系統的三個風險。

（一）個人鎖定

第一個風險如王仁甫前述，就是個人鎖定。西藏的維權人士，或東突厥斯坦的維權人士目前是被鎖定的非常嚴重，過往是用釣魚信件的方法，現在則可直接透過加密通訊軟體鎖定。舉例而言，像是提供可疑的記者訪問內容或連結，當點擊相關資訊時整支智慧型手機就遭到駭入。造成此種攻擊方法可以成功的原因，最主要就是個資外洩的問題。

而如以臺灣為例，2019 年 9 月的挺香港反送中運動，遊行下午 5 點剛結束不久，7 點在香港解密網站臺灣參與的幾個重要人物的個資，包含照片跟人臉辨識資訊，就全部放在網站上面，另外還有出生年月日、身分證字號等，而其實他們可以公布的當然更多。依被洩漏個資的層級，以及該等資料會被留存的情境，基本上洩漏行為推測應是中國公安部所為，此為其打擊異己或壓制人權的威脅手段。此種威脅手段，目前會利用現行身分證上面本來就會有配偶欄等資訊，但是 eID 所能串聯的資料其實更多，所以當未來能夠取得這樣的資料的時候，能夠做到的社群相關的社交威脅，會變得更容易。更遑論以後在無人機攻擊上，是否能取得相關的資訊，會變得非常重要。

另一方面，臺灣與香港狀況類似，就是在地協力者的問題。以上所提針對異議人士的社交威脅，其實可以跟在地協力者，例如當地黑道合作。像臺灣不少黑道除與中國有淵源外，很多也在中國有高山茶獨占利益。那這些利益來源為何？是否有交換條件？這些都是風險要素。當然這些都是既存且進行中的風險，eID 的問題在於，它會把這些既有風險放得更大。

（二）精準廣告投放

第二個問題就是精準廣告投放。精準廣告問題，源自民粹主義的崛起，以及淺碟文化帶來的注意力下降跟注意力稀缺。一個人的注意能力，已經從大概二十秒下降到現在大概七秒而已，所以如果今天可以掌握一個人七秒或者是十五秒之內他所接受的資訊，基本上就掌握到他的認知，那這種認知是鋪天蓋地的，它不一定會直接只針對注意力來做攻擊。例如說現下非常流行的抖音，抖音的優點在於它是非常短的影片，因為像 YouTube 之類有時過長的影片很多人並不願意花時間看。抖音本身的呈現形式，其實對我們的大腦的傷害非常大，因為它讓人習慣要在很短的時間裡面，去接收非常簡單化跟片面的資訊。那更不要忘記其實在抖音上，人民日報的追蹤達到千萬，是非常重要的中國資訊作戰的一個場域，目前臺灣 14 歲以下的年輕人，使用抖音的頻率其實非常非常高。

關於精準廣告投放的效果，以 2017 年發生，2020 年才被起訴的 Equifax 案為例。Equifax 是一間美國消費者信用公司，2017 年時解放軍總參謀部第五十四研究所的三位成員針對該公司發動了資訊攻擊。解放軍當時取得的資料為該公司所保有的美國公民的姓名、出生年月日、地址、社會安全號碼跟駕照資料，換句話說，就是我們現在 eID 要整合的資料。取得這些資料的意義，就在於該等資料於混合戰中的高度軍事價值。事實上單純威脅個人，以 APT 攻擊即可，不必蒐集如此完整的資料，全面取得上述資料的最大目的為分眾。除了解放軍是不斷地在蒐集這些資料，俄羅斯的網軍先前也是不斷地想要去取得這些資料，然後因為不容易取得，所以他們還直接派 KGB 的探員到美國來做田野，直接觀察像是在某個區域內大家的作息為何？該區域內大家最喜歡在什麼時候閱讀新聞？在這個區域裡面誰可能是意見領袖？然後在這個區域裡面講什麼議題最容易打動民眾的心？KGB 探員做了三個月的田野調查為的都是這些資訊。

而若把這些資料做整合，會有非常嚴重的後果。此處再以愛奇藝為例，假設愛奇藝今天開始經營成人網站，為確認使用者年齡是否已滿 18 歲，它可以合法地要求身分驗證。此時如果可以跟 eID 做串連，愛奇藝將可以非常容易地取得 log 資訊，然後再根據當事人在平台上面的 viewing preferences 去跟其他的個資做結合，這其實是非常容易的事情。今天把這些資料整合做了一個聖杯之後，其實讓資料取得的成本降得非常非常地低。諷刺的是，當時解放軍是很辛苦地從不同的地方，還要找到一家有整合這些資料的第三方公司來偷，結果我們現在做出一個 eID 聖杯，就是告訴敵人說我們自己都已經把資料整合好了，攻擊一次就夠，不用攻擊兩百次。

2016 年的時候，persona 的建立大概 60 種，以下是我們組織在分析中國的內容農場到粉絲專頁的投放，它可以分成很多種類。通常一個類型的內容平均來講可以投放給臺灣不同的三到四種人格的人，每一個粉專代表的其實是一種人格。我們在做分析時發現，它們其實是非常精準地去挑選主題，然後寫手在內容農場製造特定內容後，再投放到相關的粉絲專頁，所以針對不同的人群它可以投放不同的議題，進而再去影響其對政府的信任，或對美國的不信任，或對中國的嚮往等態度，每一種人會有不同的觀點或態度，然後讓讀者在短短的時間之內，吸收這些資訊，進而深信不疑。

這些力量不容小覷，因為這些力量未必都會是假新聞。以俄羅斯為例，它們去做跨性別人士的訊息投放時，會成立專頁大量分享暴力行為，對於有色人種就不斷地強調出生就是一種不平等，對於白人的勞工階級去主打大學教育的歧視，對中產階級就主打全球化，更不要說俄羅斯打過三年整整的疫苗論，這個疫苗論

的陰謀論大家可能沒有聽過，但是數以百萬的人在美國是相信這個陰謀論的，為什麼？就是因為它分眾做得很好，這些人心裡的洞剛好就可以用疫苗論去填補。疫苗論就是說，其實政府打疫苗都是騙人的，它只是要打疫苗讓民眾變笨，變笨之後政府好控制，學校的教授等等都是這個陰謀論的一環，大家都在騙人。地平說大家應該比較熟悉，就是地球是平的，這個是稍微比較弱的一個陰謀論。最新的陰謀論則是在講蜥蜴人，就是講川普是蜥蜴人，有一個 deep government 有很多蜥蜴人，眼睛長得是直的，沒有脊椎等等。陰謀論的重點是，不管該陰謀主張的是什麼論點，真正主要的目的其實就只有一個，就是要形成社會的分化跟對政府的不信任，告訴民眾說身邊的人是不可信的、政府是不可信的、世界是不可信的，所以要去用別的方式讓政府或既有結構被推翻。

所以它為什麼可以做到不同的分眾精準投放？就是因為投放目標對象的個資被掌握地太過於清楚，川普在競選廣告時就可以把美國人分成 20 萬種不同的人，然後進而透過改變廣告的字型、字體的底色還有語氣，吸引不同群眾閱讀，企圖影響其認知。我們可以想像，如果相類的資料大量地被敵國掌握時，能夠造成的效應到底有多大？更不要講最可怕的其實是戶籍地址，因為可以藉由戶籍地址取得區域的整體資訊，譬如保守派自由派分別在此地區佔比有多少。攻擊者之後可以針對該區域進而再做投放來影響，讓該區域特定傾向的投票率變高。比如說我希望國民黨贏，所以我就在一個支持的國民黨的群眾勢力比較多的區域，在當地來投放廣告讓投票率變高。當然不只敵國，Facebook 跟 Google 也做過同樣的事情。

當然，既有的技術已可以做到分眾，像是 7-11 櫃檯上面的攝影機跟人臉辨識，它可以針對人臉、針對性別、針對購買喜好去分析；加拿大的研究指出，光是看成人網站的 viewing preferences 就可以知道對象是自由派還是保守派，且準確率高達九成。eID 帶來最大的問題，是它透過整合讓資料取得成本大幅降低。

（三）協力模式

最後一個是協力模式，就是所謂的在地協力者。此處與前述社交威脅時所提的在地協力者問題所不同的地方，在於 eID 影響到的是在地協力者冒充。亦即，假設今天找不到在地協力者時，可以透過 eID 串接取得資料來偽造身分。當有心人士成功冒充某個在地人士的身分後，比如說某一個阿伯，或是某個小政黨，再以其社交網路為起點去投放訊息，因為大家已經被它們鋪天蓋地的訊息淹沒之後，對主流媒體產生不信任，所以不會去查證，而只會在自己的群組裡面傳的時候，對民主政治來講是一個非常大的威脅。

駭客行為、數位身分證與國家安全

王仁甫

資訊工業策進會資安科技研究所　策略總監

一、　eID 的資安風險

（一） 晶片與讀卡機漏洞

我們可以從 eID 的攻擊鏈來思考資安風險這件事，目前 eID 系統後面綁定的可能是有戶役政系統、財稅系統跟出入境資料，還有我們健康資料、弱勢資料，甚至是公投資料。換言之，如果我們民眾去參加一場公投，對岸就知道該民眾的政治立場是什麼，可以辨識特定個人的政治立場。那這樣一個攻擊型態成為可能的原因，在於 eID 整個系統可能有晶片卡的漏洞，有中國製造的問題，然後讀卡機亦有同樣的問題。從個人消費習慣的角度來看，一般人如果有新臺幣 80 圓的中國製讀卡機可買，就不會去花 550 圓買臺灣製有驗證的讀卡機。前者當 eID 晶片卡一插進去，所有的資料就被中共蒐集走了。從之前付錢讓小吃店撥放特定頻道的前例來看，未來 eID 上路以後，對岸非常有可能去發展一個免費的軟體、免費的eID登錄系統，給我們保全業、公寓大樓乃至各行各業使用(取代換證登記)。卡片只要插進去就做相關紀錄，做完紀錄就遠端送到中國，進而完整掌握我們民眾個人的電子足跡。

（二） 資料庫委外問題

另一個更嚴重的問題是，我們的戶役政資料庫、出入境資料庫、財稅地政資料庫，都是委外建置。如果發生大規模資料的洩漏，第一會有詐欺的問題，第二因為中共知道民眾個人身份，它就可以偽冒個人特徵來製造假身分，最後達成監控跟擾亂臺灣民主的目標。

有人認為資料庫外洩不可能發生，但雖然 eID 是由中央印製廠印製，可是它可能會委外給他國廠商做，而該被委託的外國廠商可能再轉委託。舉例來講，目

前傳言的委外合作公司，就是 2017 年被 IMF 制裁的公司，當初它被停權的原因之一，就是該公司違約將他國的 eID 拿去中國製造。換句話說，臺灣的 eID 號稱在臺灣製造，但會不會有一天在中國製造？這是應該注意的風險。

二、 身分個資洩漏與國家安全

（一） 暗網交易風險

接下來要思考的是關於暗網的問題。很多資料都被放在暗網上面販售，甚至我們懷疑很多暗網都是中共在經營的。臺灣兩千萬筆的戶政資料被販售這件事，我們臺灣政府的解釋是說這些格式不是政府資料庫裡的，這種說法十分令人存疑。今天我們面對的不是只有駭客組織，我們面對的是中共，它們可以偷完資料後，過了幾年，更新完再丟上暗網，用很低的價格販售，只為了給臺灣政府難堪。理由在於，這麼做可以製造社會混亂、製造國家混亂。更甚者，中共用網軍攻擊，不如將漏洞或個資公布出來，讓全球的駭客攻擊。大量個資的洩漏會造成很多的風險，第一個就是會擾亂我們整個社會安全。以電商詐騙舉例來講，有一個阿公想買巧克力給孫子，讓他轉送給女朋友（一千兩百塊），結果他最後被騙了一百五十萬。因為駭客組織不僅掌握他的個資，還掌握他孫子的個資，所以駭客騙阿公說，因為程式設定錯誤而買了十二盒，所以要阿公去 Atm 依指示解除分期付款，然後一百五十萬就轉出去了。可是關於 eID 我們更擔心的是什麼？在開放區居然有人民 300 dpi 的照片，然後在加密區居然有 600 dpi 照片，當這些高解析度的照片被洩露時，搭配對岸 AI 技術，透過人臉辨識系統，掌握當事人本人跟身邊所有人的私人行蹤，這種風險不可謂不大。

（二） 拖庫、撞庫與洗庫

駭客圈裡面有一件事叫撞庫與拖庫，基於不少人習慣直接以自己或家人的個人資料，例如出生年月日，來設定帳號密碼，所以當 eID 資料洩露的時候，駭客或是中共可以用來撞庫，它們可以用這些資料重新排序，去 try 當事人其他的帳號密碼。它們會一直去 try，把這些資料全部拖出來，然後開始洗庫。所以外洩後的資料，我們最後能看到的是洗庫後的資料，就是中共把資料拿去重新堆疊過的資料，而政府卻因為格式不同否認這不是從政府資料庫中外洩的資料。最後，中共就利用這些資料，進行社交工程的 APT 攻擊(Advanced Persistent Threat)。

（三） 身分偽冒及輿論操作

為什麼假新聞可以騙到人？因為假新聞可以以假弄真。道理非常簡單，如果今天我可以完整抓到某人的特徵，一般人通常都會以為這個人是真的，特別是在沒有其他訊息之下。例如說很久沒有見的老朋友，突然成立了臉書帳號，對方突然加你了，上面就是他本人的名字，相關學經歷及其他特徵都對，一般人通常就會加好友了。會加他因為他是現實上的朋友，可是這些網路上的身分資料代表的是他嗎？不是，當有心人偽冒到這個身分，可以做很多事，他可以詐騙，他可以作假新聞等。所以如果我們的資料掉了，甚至衛福資料都掉了，每次選舉的時候就開始會在生理特徵上挑戰對方，模糊政策焦點和干預民主選舉程序。

而被拿走身分資料這種戰略資源後，我們可能要面對的是中共戰略支援部隊的一個攻擊，他們有兩三萬人在做這件事情。他們偷臺灣人的個人資料，還偽造個人行為，然後透過買公關公司炒作，搭配宮廟系統等，以扶植紅的政治人物，如說某政治人物，天將降大任於斯人也，他的八字就是生出來要當總統。也可以炒作很多事情，舉例來講，他可以冒用小林新村的資訊，或者是冒用某個賣花椰菜的阿伯，並在社群媒體抱怨政府都不重視農產品的價格，害花椰菜堆了整山，接下來透過地方新聞去分享，造成輿論的不滿。第二個案例更可怕，就是香港解密。一個國家開始控制人民，就會實施恐怖主義、思想改造和教育。舉例來說，之前香港發生恐怖的抗議意外事件，前一天一個小女孩去抗議反送中活動，坐電梯回家的監視器影片還說說笑笑，隔了三個小時後，她的屍體在河裡面出現。這件事的起因在於，有中共結合黑道在鎮壓香港相關抗議行動，而香港解密把抗議反送中的關係人個資都上傳上去，然後說這些人是暴徒，號召全部人（黑道）殺他，甚至有懸賞獎金。臺灣人也有受到影響，像基進黨人士就在反送中活動後，被公佈了八個人名，甚至連護照號碼都有。這些都是身分資料被惡意人士掌握後的危害。

三、　小結與建議

最後我的建議是，當我們臺灣所有人都在譴責中共壓迫港人自由的當下，如果沒有一個完善的措施就去換發晶片卡 eID，簡直就等於送給中共一個最大的好處，留給中共網軍竊取臺灣所有人資料的機會。今天任何人都可能當反對黨，任何人都可能上街頭，不是你、就是你的小孩，或是你的親人，不會有人希望這些人的個人資料隨意被他人、中共或黑道公布，說因為你曾經反對中共，結果一踏上香港，就被抓走之類的憾事發生。所以我跟各位建議，我們一定要好好思考這些政策。

（數位）足跡、剖繪、與監控

莊庭瑞

中央研究院資訊科學研究所　副研究員

本文主要目的是與各位分享數位足跡(footprint)、剖繪(profiling)，及監控(surveillance)幾個用語的基本概念，以及數位足跡、剖繪以及監控間的關係。

首先，將會先談到 Surveillance，這用語通常是翻譯為監控，有一個控制的層面在內，但有時候這個控制是比較微妙的，並不是透過直接的方式去控制被監控人的行為。監控有時也不是視覺面、或偏向實體空間，而可能是透過資料的掌握，以對監控或監察對象有比較全面的了解。最後，我會提到 persistent identifiers (PIDs)「持續識別碼」的概念，而這其實是讓資料監控變得更有效率的一個關鍵。

一、　監控 (Surveillance)

監控，這個詞通常會有全面性的意涵在裡面，當講到監控時，通常含有時間與空間的要素，換句話說，這個行為已經進行了一段時間，而且空間面是沒有避開的可能性。比如在一個空間只有一台監控攝影機，那是有避開監控範圍的可能性；但是如在城市裡有幾十萬個監控攝影機的話，那幾乎是很難避開。另外，監控，可能是針對大規模人口所進行，資料記載的精細程度可能到匪夷所思的地步，且資料將會被貯存，保存期間可能為永久，或者不知道保存期間。通常的情況，是不知道保存期間，而且日後如果有需要，已蒐集的資料就隨時拿出來分析，監控就是一個這樣的概念。

監控可以是對一個群體、一個地區的人口所為之的行為，比如現在新疆就是整個地區的人口，在一個被全面監控的狀況下生活。監控也可以是針對特定的人，對其行為做一個掌握。但是，監控有可能是對不特定人所為，但只是因為監控者不知道要對誰監控。這時，監控者只是要先收資料或影像，事後，如有需要再來查找可能會感到興趣的人。雖然這聽起來好像有點不可思議，但卻

是事實上一直發生的事情。前述這種對 unknown 的監控，在政府部門、商業部門、個人等，其實都有能力可以做到。

另外，還有一種是相互監控，這也蠻有趣的。比如 Amazon 的電子門鈴，住戶將電子門鈴安裝在門口，當有人來按門鈴時，攝影機就會啟動，然後將影像傳到綁定的手機。所以，不論在家裡或在外面，屋主都可以看到是誰在按門鈴，然後，再決定要不要跟他通話。裝電子門鈴的原始目的其實大部分是為了住家安全，但是很有趣的是，如果社區內每戶都裝了電子門鈴，那可能會變成彼此監控，因為會來按門鈴的人恐怕大部分是鄰居或送貨員等。

有趣的是，Amazon 竟然跟政府部門間相互合作，例如警察局參與 Amazon 給社區住戶的折扣方案，讓社區裡多數住戶都裝有類似的電子門鈴。但如果整個社區都裝電子門鈴了，那將是一個蠻有趣的畫面。Glenn Harvey 為 NBC News 新聞網站做了社區相互監控報導的示意圖。當住戶都裝有電子門鈴時，只要走進社區都會可能被住戶的電子門鈴拍到。因為電子門鈴並不是只有按門鈴才會啟動，在風吹草動的時候也會啟動。所以，如果裝有電子門鈴的話，入鏡的應該大部分都還是家人，譬如說在戶外烤肉的或遛狗時的影像，然後，這些影像其實由 Amazon 公司保存，住戶再經由雲端調閱這些影片。

另外，以資料做為基礎的監控稱做資料監控(data surveillance)，這裡引用美國國安局 Keith B. Alexander 所說過的話來說明，資料監控就是先把資料通通收起來，為了日後容易查找，先做好標記及相關後設資料的分類，比如時間、地點、關鍵詞、人名等。先大規模收集資料，日後如有需求，再去查找，這就是資料監控的現況。

接下來要討論的是，在權力上不對等的情況所進行的資料蒐集與分析的議題。對於大量資料的蒐集，一般人並沒有資訊能力進行資料處理及分析。最重要的是在大部分的情況下，個人也沒有權力進行大規模的資料蒐集、處理與分析這樣做，而通常國家或政府至少在某些情形下有權力這樣做。被蒐集資料的這一方，其實也沒有多少管道了解其個人資料被蒐集、處理及利用的情形，所以這裡就產生了非對稱的權力關係。

那當個人察覺其個人資料、行為資料一直被蒐集、處理，而且不知道會被保存多久，會被怎樣分析的時候，會不會導致行為上有甚麼樣的改變呢？接下來舉例 Mary Hui 這位記者 2019 年 6 月 12 日在香港紀錄示威活動的相關報導，參與示威者寧願用投幣買單程地下鐵車票，也不用八達通（類似臺灣悠遊卡的電子票證），因為使用電子票證時，如為記名的交通票證，持卡人的交通歷程

資訊在經營交通運輸的公司都有留存；如為不記名的交通票證，事後也可能會可以串接勾稽出來。所以，示威者如不想讓自己落入那樣的風險，就必須要改變原本的行為模式，例如寧願用零錢買車票，或改變原本計畫不參與示威，改採其他方式參與。從這個事件可以看出，當個人察覺其資料被蒐集、處理、利用時，可能會使其在行為和意念上產生改變。

二、 持續識別碼 (persistent identifier, PIDs)

接續要說明的是所謂的持續識別碼，意指識別碼與其所連結的物件、人物、或活動將會持續一段時間不變，且通常以電子方式存在個人的數位足跡裡。透過識別碼可以去拼接不同屬性的個人資料。有些物件，比如電話，除了電話號碼本身，手機有其唯一的號碼、sim 卡也有其唯一的號碼：IP address、e-mail address、車牌號碼、電子票證號碼都是。然後，關於人物，比如臺灣人民終生一號的身分證字號、信用卡卡號、銀行帳號、跟消費紀錄相關的會員卡號，以及登入網站的 login name、在 social media 上的名稱等均屬之。雖然有些持續識別碼可能會隨著時間更動，但是至少仍持續用一陣子。活動也是可有持續識別碼，例如交通紀錄、etag 紀錄等等，都是活動的紀錄。持續識別碼可以被機器讀取，處理上也非常方便，日常生活到處。持續識別碼雖然可能不一定是唯一的，比如說網頁瀏覽器 browser 的 cookie 也是持續識別碼，但當清理 cookie 或無痕瀏覽時，可能就沒識別碼了。但即使識別碼不是唯一，經常還是可以有效地串接一段時間內，個體跟活動紀錄間的關係。

三、 剖析、描繪 (profiling)

接下來談到剖析、描繪(profiling)，剖繪是透過已鎖定特定群體或非特定個體的資料所推演出的額外資訊。比如政府有時候為了社會福利制度、措施等，有時會對少數民族或某社會經濟地位層級的群體進行剖繪，了解政府資源有沒有被好好使用。日常生活的剖繪，常見於消費行為的分析。在社群媒體張貼照片等，其實就是個人自願告訴社群媒體公司，張貼照片的時間，而且往往伴隨著地點、跟誰在一起等內容以及背景資訊，這些資料也常一併被蒐集。

將監控與剖繪相比較，一般會認為監控是全面的，剖繪是比較破碎的。比如說個人使用悠遊卡的行為，雖然資料留存散佈在不同的公司（悠遊卡公司、手機公司或電信公司、或車牌監理單位等），但是因為有持續識別碼，所以使散佈在各資料來源間的資料，能夠很容易再串接在一起。

四、 數位足跡 (digital footprint)

最後回到數位足跡(digital footprint)，剛才提到數位足跡裡很多持續識別碼，即便資料散佈於不同來源，還是可以透過持續識別碼把資料串在一起，那當有很多數位足跡串在一起時，就可能變成一個非常精細的剖繪。如果是做一個大規模、很精細的剖繪，這個就成了監控。

本人在這議題所要強調的是，國民身分證字號是一個很強的持續識別碼，比如當車牌號碼、手機等都是註冊在同一個身分證字號下，那用身分證字號來串接各個資料、串接數位足跡，剖繪就可能會變得分外容易，分外精細。

中共推動社會信用體系之發展與研析

蔡文軒

中央研究院政治學研究所　副研究員

本文主要簡介關於中國推動社會信用體系的監控過程，其實，監控是更為全面的體系，社會信用體系僅為威權國家在處理監控過程的個案，中國就有好幾個不同的監控體系。以下將介紹的社會信用體系，本質上與商業信用體系相關，只不過中國把商業信用體系的商業指標撤換成政治指標，做成更徹底的監控。

一、　強化社會控制的嘗試

監控這件事情，可能要從中國一直很想知道人民或幹部到底在做什麼事情開始。在過去沒有電子媒體的時代，主要是靠著非常類似臺灣早期人二室的人事檔案系統來追蹤，直到現在，中國人事檔案系統都還存在且運行著。人事檔案系統的運作問題，在於過去中國是單位制，每個人都一份所謂的人事檔案，目前其實只有幹部還保有人事檔案系統。依據人事檔案系統，若大學畢業後不當幹部的話，就不會繼續在人事檔案內追蹤；但如果有當幹部，人事檔案將會透過機要專線轉到所屬的部門。大部分被記錄的人終其一生都無法看到人事檔案系統的紀錄，凡屬學校的操行及各種政治評價都被紀錄在裡面。但是，人事檔案系統並不是全面的，而且主要透過人工的書寫，所以，就主政者所獲取的資訊量來說，相較於電子的社會監控，人事檔案系統的資料可以說是相對地少。

因為這個緣故，中國當局一直在思考，如何在保留人事檔案系統的前提下，進行更廣泛更具規模的監控。螞蟻金服下的芝麻信用與商業信用體系的概念與運作模式，給中國當局很好的啟發。芝麻信用是與顧客進行交易時，一種給顧客信用評比的積分指標。在芝麻信用體系裡，每個人都有一個分數，如果信用極好，進行交易時會比較方便。同時，中國當局借用芝麻信用的評分機制，導入商業信用體系的概念，只是把商業信用指標換成政治信用指標，再結合網際網路與行動個人裝置，於是就產生了社會信用體系。

雖然過去人事檔案某種程度扮演黨管社會的一個角色，但因為對象與運作模式的關係，所能發揮的功能有限。然而，當與黨管社會與科技網路結合，全面性的效果就出來了，所以，社會信用體系可以說是黨管社會跟科技網路的一個邂逅。

至於，中國社會信用系統的概念與運作模式是否可輸出到中國以外的國家，可能要進一步檢視該國是否具有類似中國的操作環境。這個系統在中國得以得天獨厚的順利運作，是有幾個因素加乘才得以展現這麼好的效果。

首先，中國是全世界虛擬交易最蓬勃的國家，在大部份的國家，例如美國跟日本，大部分的交易其實還是使用現金跟信用卡。依據觀察，中國的虛擬交易從 2010 年到 2012 年的間突然暴增成長，雖然現在仍在尋求直接證據，但個人高度懷疑其背後可能有國家機器的推動。中國讓人民靠著習慣虛擬交易過生活，當人民的日常生活離開不了虛擬交易，而進行虛擬交易必須要有信用評分，人民從日常生活開始就必須一直仰賴政府提供所謂的信用指標。

二、 社會信用體系的建置

2014 年中國頒布社會信用體系的建劃、建構綱要，開始與商業公司合作，透過商業公司的協助，逐漸完善這套社會治理的架構。同時，各地的試點正逐步進行，成立了「社會信用體系建設領導小組」，由各級發改委負責牽頭。

當然政策推動表面的理由，是為了讓民眾維持好的信用，然後推進社會主義的先進文明。但是，進一步觀察社會信用體系，其實也是一種獎懲措施。例如信用太低不能購買火車票、不能申請好學校，子女不能申請學校，不能申請好工作等。信用評比很低的紀錄，將變成人生的恥辱、標誌，永遠跟著走。所以，這套體系根本上是懲罰信用評比低的人，但這背後意味著什麼呢? 這意味著人民必須要追求政府所規定的良善，因為黨教你怎麼做好人。

當商業指標提升到政治指標後，雖然這些指標表面上看起來好像沒什麼，但背後卻有維運的思維。例如說不贍養老人扣五十分，如果人民都可以贍養老人，為政府擔憂分勞的話，國家就穩定了。網路言論詆毀他人扣一百分，目的就是要求不要到處造謠，不要攻擊別人，要維持這個社會的穩定和諧。圍堵黨政機關的鬧訪要扣五十分，意思就是說就算有冤屈，也不要機關去鬧訪，為了顧全大局，繼續維持和平。酒駕扣五十分，中國有很多社會不穩定的事件是酒駕引起的，而這些由警方處理事情的背後，常會涉及一些人事關係等，所以，常有很多社會不穩事件其實是警方處理不當或怎麼樣。

所以，黨教你怎麼做好人的指標，可以提升個人，已經跟商業交易沒有太直接的相關。做好人之後，指標分數就會很高。另外一方面，如果分數太低，就很難交朋友，因為可能分數會因此被拉低。所以，這意味著如果是被黨唾棄或者被社會唾棄的，就會被孤立不能有朋友，這將導致所謂的異議份子更為孤立。

事實上，中國大陸正全面在各級政府推動社會信用體系，雖然各地的作法不一樣，但都預計在 2020 年完成。然而，依據個人估計因為體系的運作還會牽涉到許多單位，比如牽頭部門的發改委，還有辦公室、經信委、還有像中央的工信部一樣的機關等，在各單位間的整面合，仍然有多待解決的問題。例如當分數低不能買火車票，這時會牽涉到交通部門；分數低的子女不能申請好學校，就涉及教育部門；分數低的人不能買房子，這時則涉及城市住建部門。就是因為背後所涉及到的條條塊塊太過於複雜，所以，目前各地還在行整合中，再加上疫情的關係，進度大概也稍微緩和，目前還沒看到有很明顯的作法。

最後就是，社會信用的特色就是每個人都有一組代碼，像是身分證字號的社會信用代碼。當進行虛擬交易時，包含借書、租房、買房等，都可以透過這個代碼去進行。當輸入信用代碼時，系統會連結到很多部門後將總結一個整合性的評比。簡單來說，每位人民都會有一組代碼，代碼背後都有一個分數，分數高的人可以做很多事情，甚至租房可以不用繳租金；分數低的人連買車票都不行，特別是如果你曾經鬧訪機關。

對於社會治理或政治學來講，有趣的地方在於中國的社會信用評比其實跟西方先進國家的所謂信用評比相較，有兩個最大的差異，第一個就是在西方先進國家的信用評比(credit scoring system, CSS)基本上只用於融資信貸，主要是商業銀行核發貸款或者涉及商業、工作的一個依據；但中國的社會信用評比卻深入至各個領域，其本質上是一相政治評比，已經不是單純的商業評比，社會信用評比對於人民是一個全面的控制。第二個則是在資料保障方面，銀行信用評比基本上只在金融機關或當事人所知悉的單位才可知悉，而中國的社會信用評比是公諸於大眾，亦即非相關人或單位也都知道個人的評比，這個是比較沒有隱私權保障的。

三、 社會信用體系與當代中國的社會治理

最後，也是最重要的。個人以為，中國社會信用評比系統對於威權國家的治理，大幅地降低了所謂的治理、監控的成本。用邊沁或傅柯的圓形監獄或者是後來有提到的圓形監獄的概念來看，中國每個人都在這個圓形監獄裡面，然後自己進行自我審查，這降低了很多監控的成本。

個人稱中國社會信用評比系統是一種受歡迎的科技威權主義，也就是說這種信用評比體系跟過去的傳統威權體系相比較，是受到人民歡迎、擁戴的。在中國的朋友認為是政府幫大家把持住信用，並不覺得有什麼問題，反而是覺得是不是西方國家想太多了。到底是我們想錯了，還是他們講對了？因為中國人民並不認為其已被控制，這反而是最恐怖的地方。過去的威權體制，當事人會知道被控制，知道鬧訪時被打壓，被限制居所，甚至其他親戚朋友也都被監控了。但是社會信用評比是個受歡迎的威權控制體系，是人民心悅誠服的，喜歡這個系統，然後甘願被監控。然後，社會信用評比系統也透過一些被中國管控的市場機制運作著。

當政治跟科技還有商業的結合，大幅降低威權國家管控社會的成本，而且這是種讓人民心悅誠服的管控方式，人民不知道自己被監控，反而會為威權國家說話，所以運作成本是低的，控制風險也是低的。這是一種人類全新的管制方式，一開始可能是跟商業公司學的，但是透過中國智庫的轉換，現在變成一種全新的控制方式。

目前個人不認為這個制度在其他國家有可實踐、可仿造的空間及可能性，因為如果其他國家沒有仰賴虛擬交易的社會習慣的話，其實這系統是很難推行下去。這種體系很難輸出到南美、拉美或者是非洲這些威權國家，這是一種具有中國特色受歡迎的科技威權主義。

Road to Digital Totalitarianism

劉靜怡

中央研究院法律學研究所　合聘研究員

一、　為何在意隱私權

在談數位足跡、剖繪還有監控的問題之前，可能要先確認一個社會何以應該保障隱私權？我借用邱文聰的觀點，提出三個規範上的理由來說明，第一個是匿名生活的確保；第二個是自主權的尊重，最後就是獨立人格的追求。

第一個理由－匿名生活的確保，每一個人都有匿名生活的需要，在日常生活中不希望處於被監看及窺視的狀態。所以，即使名人也希望其與配偶或伴侶間家庭生活是否和諧的狀態，不會被他人窺視或公眾議論，這就是所謂匿名生活的確保。

但有時在意隱私權與是否匿名沒有關係，換句話說，就算匿名性沒有被侵害，還是可能會在意隱私權，這裡要談的就是第二個理由－自主權的尊重。即使不涉及可識別資料，仍然可能會存在隱私權的保障問題。舉例來說，使用公共廁所時，如果有人偷拍，雖然不見得會偷拍到可識別資料，但是多數人在這種情況下，會認為這個行為已經構成對於隱私權的侵犯，而其背後的理由，應該與自主權尊重有關。

第三個在意隱私權的理由，其實是為了追求獨立的人格，拒絕國家或社會製造已設定好的公民(programmed citizens)，不希望每一個人都被政府塑造成同一個或者有限的樣子。

目前很多業者為了做精準商業行銷，常在蒐集個人資料後將個人加以分類，並形成很多不同的人物誌或角色設定(persona)。這種作法其實對獨立人格的追求，會產生某程度的緊張關係。但每個人對於追求獨立人格所需的空間並不完全一樣，有些人需要比較多的獨立人格追求空間，有些人覺得好像多少都無所謂，而這又牽扯到每個人對於隱私的品味，或者說各個社會文化對於獨立人格追求空間的品

味及需求，每個社會都可能有所差異。所以，臺灣、美國、日本、跟歐洲對於獨立人格追求，存在不一樣的評價或是配予不同的重量。

二、 New eID 與監控及數位足跡

對何以應保障隱私權的規範上理由有初步了解之後，回到本篇文章的主題 - New eID 會不會有監控的問題？請參考內政部的資料（圖一），內政部在這張簡報要表達的主張是，因為使用 New eID 時須透過使用端下載憑證廢止清單來確認憑證及卡片是否有效的驗證程序，所以，使用身分證時並不會連回內政部，所以內政部對身分證的使用過程並無資料可以掌握，是以，內政部不會記錄使用者使用 eID 的足跡，也不會對 New eID 的使用過程進行監控。

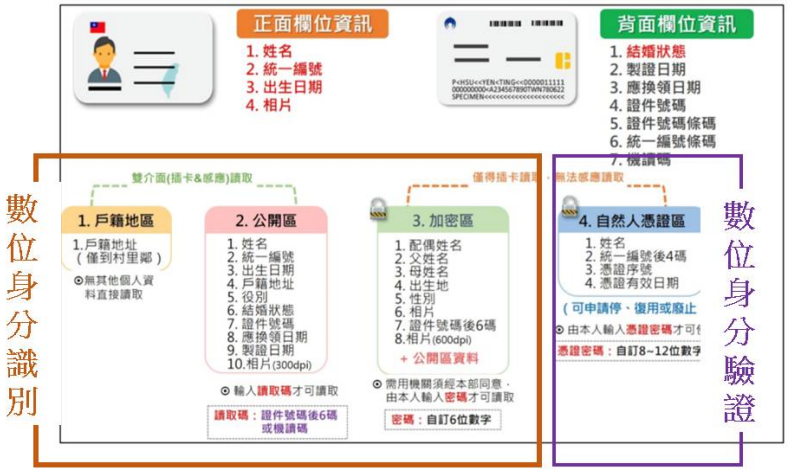
New eID與監控及數位足跡

然而，內政部的主張可能混淆了兩個不同的問題。請參考內政部所規劃 New eID 的分區與簡圖（圖二），涉及晶片的使用行為其實可分成兩大類：第一類為使用自然人憑證的第四區，稱為數位身分驗證。內政部再三強調，自然人憑證區是可以由民眾自主選擇開啟／關閉。另外一個使用類型，則為左邊三區（戶籍地區、公開區與加密區）區塊，這三區的功能，是單純的數位身分識別，因為不涉及以憑證進行身分驗證，僅透過晶片識別你到底是誰，或至多在臨櫃或虛擬環境中進行晶片資料的驗證。

「數位身分驗證」（第四區）的功能如內政部所稱，可由個人選擇關閉。但

「數位身分識別」或「資料驗證」(其餘三區)的功能則無法關掉，每個人都被強制要求在 New eID 上有這三區的晶片資料(此與德國允許個人關閉晶片身分證上全部的晶片功能，保留單純無晶片功能的塑膠卡，在保障個人自主權上有很大的差異)。

New eID與監控及數位足跡



區分「數位身分驗證」與「數位身分識別／資料驗證」的目的在於，前者在身分驗證過程中內政部確實不會留下任何紀錄，且憑證功能也可依個人的選擇而關閉，但後者在每一次使用時，都會在需用機關留下包含有數位身分識別資料的數位足跡，比如為了門禁安全管制，由保全人員插卡或感應進行數位身分識別，這時身分證當事人的身分資料，就被紀錄且留存下來。所以，即使關掉 New eID 的自然人憑證功能，僅使用晶片身分證前三區的識別資料，也仍然會在使用過程中留下紀錄，這就是所謂的數位足跡。

那麼，數位足跡會造成什麼樣的問題呢？當大量國民日常生活的數位足跡被留存下來，就有可能被用來進行分類、分析，並形成前述所提到的人物誌或角色設定 persona。Persona 就是針對不同類型的人，會有甚麼樣的特性，加以模組化。Persona 在某些情境或對特定需求可能具有用處，例如，進行市場行銷時可更精準地瞄準目標客群，分析各種類型的人群可能會喜歡的產品或需求。當然 persona 也可以用在其他用途，比如上次美國大選時，競選團隊利用劍橋分析所做的 persona，類型化與標記人群，並對其個別使用不同手法做政治宣傳，針對立場比較偏向民主黨支持者的意識型態，或思想比較偏向自由派，就以投其所好的特定方式，對其進行政治宣傳。

所以，New eID 當事人一旦留下數位足跡而未予規範，一端可能被拿來形成 persona 做各類應用，於此同時，另一端也可能在有需求時，隨時以公共利益之名被拿來利用。以陳其邁副院長 COVID-19 論文中的圖片為例，政府透過電信公司的個人手機訊號擷取的移動軌跡，進行所謂的疫情調查，原本電信資料並不在政府手中，但只要資料存在而面臨需要時，政府就可能以公共利益為名加以蒐集與利用。

簡言之，數位足跡的存在離未來可能隨時被取用後進行監控，其實有時候只是一步之遙。只要留存了數位足跡，就有可能被拿來使用的一天；如果數位足跡沒有被留存，基本上就不可能發生後續的監控問題。

三、 因應數位足跡監控的法制規範模式

當確認數位足跡的存在與可能的應用模式後，要怎麼因應公私部門蒐集、利用數位足跡可能帶來的問題與疑慮？以下將介紹數種可能對抗數位足跡的法制規範模式，並舉日本、德國、及比利時為例加以說明。

第一種類型，以法律直接禁止或限制數位（身分）足跡的蒐集。以日本為例，日本法律限定蒐集個人編號 My Number 的數位（身分）足跡，僅限公務機關或受託行使公務的機關，為社會福利、稅務或者災害對策目的。所以，日本是在非常限定的目的下，才能做數位（身分）足跡的蒐集及利用，其他與前述無關的目的都不可以蒐集。

第二個例子是德國，德國原則禁止串連並限定留存數位（身分）足跡，如非有權確認身分的機關要蒐集數位身分資料前，必需經過主管機關的事前許可，始得為之。德國透過前端事前管制的方式，要求僅於相關主管機關許可下才可以蒐集數位身分資料，而且不得蒐集含生物特徵的資料，甚至，身分證影本也不能隨意再使用，並禁止使用自動化的方式取用身分證個人資料。德國同樣是以法律明文禁止使用身分證做資料庫間的資料串連，除非具有法律明訂的其他例外情形。

比利時是限定蒐集跟限定留存的另一個例子，對於所謂的敏感性身分個資，比如說照片或身分證字號，需另有法律或法規命令為依據，才可進行蒐集、處理利用。若非以身分識別之目的而讀取身分證，及為進行身分識別目的後的資料留存，都需另外取得主管機關的事前授權許可，始得為之。

對抗數位監控的第二種規制模式則採反向監控的策略，一般稱做 sousveillance，中譯為反監控。當政府或商業公司在蒐集數位足跡時，反過來對

政府跟商業公司取用資料的足跡來加以監控。例如，日本透過資訊提供等紀錄開示系統，允許個人可一次調閱完整的數位足跡被調用/使用的日誌，確保個人對於其個人編號(My Number)有控制權。另一個反監控的案例為愛沙尼亞，愛沙尼亞個人資料獨立專責機關(Data Protection Inspectorate, DPI)，負責監管其他政府部門取用資料的行為是否符合個人資料相關法律、法令規定及機制的要求。所以，政府部門蒐集數位足跡的行為受到 DPI 的管制，同時 DPI 對於私部門之個資利用也同樣有規制的權力及監管的權限。除了 DPI 的監管之外，愛沙尼亞還有資訊系統管理局，提供個人資料追蹤服務(data tracker)，要求政府在資料庫的使用必須要留下足跡，且提供個人查詢。所以，當事人可透過資料追蹤服務系統，清楚地知悉政府部門取用個資的時間、目的等，可以反過來追蹤政府，希望藉此能讓政府在個人資料的取用，符合民主課責的原則。

以上所提出來這兩種法制的規範模式，都是足以用來對抗數位足跡廣泛使用的情況。

最後，對照臺灣目前 New eID 的規劃，應提醒注意的是，雖然內政部再三強調不會蒐集個人的數位足跡，確實也許憑證的驗證不會連回內政部，可是這並不代表個人不會因為使用 New eID 而到處留下數位（身分）足跡。

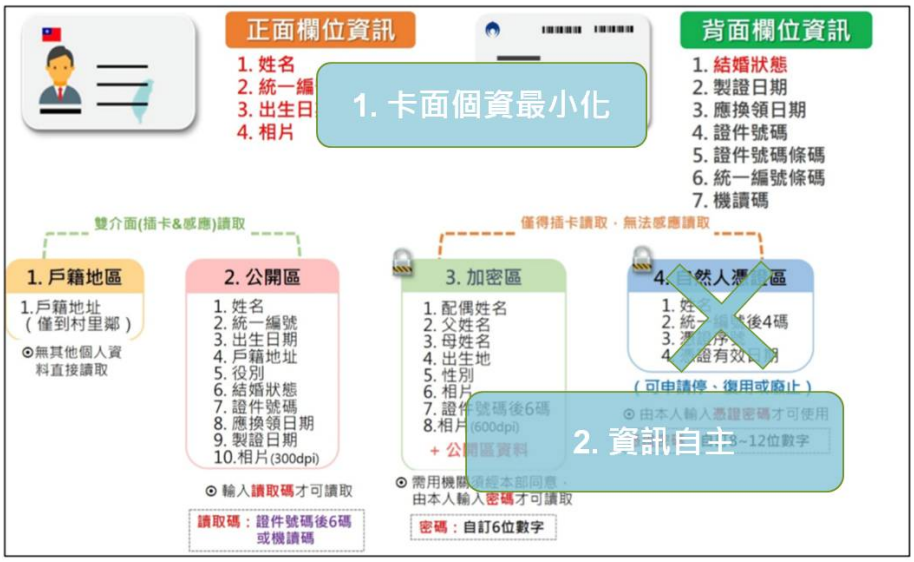
當因使用 New eID 而到處留存數位足跡，卻欠缺必要的監管模式（不管是限制蒐集使用，還是透過反向監控的方式），其實就很難確保這套系統不會走向數位極權主義 Digital Totalitarianism。

國民身分識別、戶籍管理與身分證的晶片化及數位化

邱文聰

中央研究院法律學研究所　研究員

本報告將以內政部對外公開招標資料中提及之 New eID 規劃為分析對象(如下圖一)，探討國民身分識別、戶籍管理與身分證的晶片數位化等相關議題。依據內政部的規劃，New eID 將包含卡面資料，亦即身分證塑膠卡本身正面與背面印製的資料，以及分別儲存於晶片中 4 個區塊的身分資料。



內政部宣稱，其所規劃的 New eID 與原紙本身分證相較，具有「卡面資料最小化」及「資訊自主」兩個優點，因為部分的紙本卡面資料將轉存在晶片，未來晶片卡的卡面資料將比現在的紙本身分證減少，符合卡面個資最小化的要求；同時，New eID 分別在晶片第三區（加密區），提供個人自訂密碼控制資料的近用，也允許個人決定是否關閉第 4 區（自然人憑證區）的功能，賦予個人資料釋出的控制權。

然而，相對於可自主選擇關閉的第 4 區（自然人憑證區），其他三個晶片區

塊（第 1 區－村里鄰戶籍區、第 2 區－公開區、第 3 區－加密區）在目前內政部的規劃下仍屬強制，亦即，身分證晶片上必須具備並登載身分資料的區塊，不容個人自主選擇關閉，因此 New eID 並非如內政部所稱更能保障個人的「資訊自主」。

縱然「資訊自主」的個人權利並非絕對不得予以限制，但其限制仍必須符合「法律保留原則」與「比例原則」的要求。而依目前內政部的規劃，卻存在諸多違反上述二原則的情形。

依照內政部在招標文件與對外釋出文宣品的說明，「加密區」僅限執行法定業務所需的需用機關在申請 secure API 後才可近用讀取。就此而論，目前法源資料庫系統中，法令條文明白規定應蒐集或可蒐集國民身分證的法令有 95 筆，而提到蒐集國民身分證統一編號的則有 74 筆。後者雖未直接提及國民身分證，但國民身分證統一編號的蒐集常與國民身分證資料之讀取相連結。若以相對寬鬆的標準檢視，「加密區」如果僅開放予執行法定業務中依法令應蒐集或可蒐集國民身分證資料的公務或公務機關使用，形式上或可符合「法律保留原則」；但執行該等法定業務是否都「必要」以數位化的資料為之而須將身分證「晶片化」，則是「比例原則」下應予檢驗，卻從未見內政部說明與回答的問題。此外，將「加密區」的使用限定於法定業務的規劃，目前僅是隨時都可能變動內容之「招標文件」的一段敘述，並非法律的明文規定，也因此並無「法制化」的擔保。

更大的問題存在於未限定目的、無自訂密碼控制的第 1 區（村里鄰戶籍區）及第 2 區（公開區）。依內政部目前規劃，任何人只要下載 open API，都可能取用登載此二區的身分資料。第 1 區與第 2 區的用途因無限制而可包羅萬象：日常生活常見利用身分證統一編號的某個號碼或是尾數，享免費美食或折扣，或是為配合防疫採取實聯制，掃描身分證條碼，即可得到身分證字號的資料，未來均可能以讀取該晶片區塊的方式更快速（但也可能更隱匿）地進行。這些沒有法令依據，理論上屬於個人自願選擇採用的「任意性身分證明方法」，但因沒有法律限制其利用目的，事實上已到了氾濫使用的地步。然而，依據內政部目前的規劃，個人卻不被允許依「個人資訊自主」選擇關閉第 1 區與第 2 區的功能。

究竟在執行法定業務之目的已可被充分滿足的情況下，另外強制要求人民接受一張包含非法定且不限目的功能的國民身分證，是否確實是戶籍法對主管機關的授權而符合「法律保留原則」？

一、 身分證（換）發行的法律依據

內政部宣稱，晶片身分證的換發已具有法律規定之依據，所指之法律依據主要是戶籍法第 51 條、第 52 條及第 59 條。按內政部之主張，戶籍法第 51 條規定「...身分證用以辨識個人身分，其效用及於全國...」，即是身分證可提供公、私部門間個人身分辨識之用的依據，因此，內政部可以強制發行供公、私部門不限目的使用的身分證。另外，戶籍法第 52 條及第 59 條之規定，亦分別授權內政部有身分證格式決定權，可作為「晶片化」的依據。

對於內政部所持的法律主張，應進一步檢驗兩個問題：第一，戶籍法第 51 條真的可作為強制發行可供全國公私部門不限定目的使用，且任其取用第一區戶籍區、及第二區公開區資料的身分證？第二，從紙本到晶片，真的只是身分證格式的改變嗎？

以下將先從歷史的角度，考察身分證制度的起源與身分辨識功能的原始法律設定，藉以回答戶籍法第 51 條的本意與其授權範圍，再從比較法的觀點切入，討論其他國家在國民身分識別與身分證晶片化與數位化上的作法，以瞭解由紙本到晶片可能產生的影響。

二、 國民身分證之「身分辨識」功能的歷史考察

回顧歷史，戶籍法最早出現在民國 20 年，當時法條文字既無身分證也沒有身分證字號。「身分證」一詞最早出現在民國 33 年的戶籍法草案中。爾後，35 年戶籍法才正式將身分證制度納入。不過，按當時法律規定，得由政府發行的身分證，其功能是作為人民享有權利與履行義務時，主管機關查驗身分之用。

值得注意的是，35 年戶籍施行細則有一個與現行戶籍法第 51 條有關的條文：「...身分證的效用及於各地，無庸隨地換發。」因當時各省縣可發行各自身分證，在推行時常發生爭議，例如在 A 地發行的身分證在 B 地被要求重新申領的問題，施行細則乃訂定「效用及於各地」的文字，明白規定不同省分依法發行之身分證對彼此而言均有效，不需隨地另行換發。「效用及於各地」的原始意義，即在於此。

「效用及於各地」的文字一直到民國 87 年，戶籍法才將文字修正為「效用及於全國」，並移除後面「無庸隨地換發」等字，而成為今日第 51 條規定之文字。換言之，戶籍法第 51 條有關身分證辨識身分的效用「及於全國」，並非指個人負有以國民身分證「向全國各地之公私部門證明自己身分的義務」，而僅指身分證

可供全國各機關依法確認個人身分之用。民國 37 年動員戡亂時期發行國民身分證的實施辦法也再次確認，發行身分證的目的是為了國家管理人口遷徙跟敵我識別，及作為機關配賦權利義務，人民身分證明之用。

在此可得到一個初步結論：戶籍法授權主管機關發行國民身分證的主要目的，是以國家與人民之間的關係為範疇，作為機關配賦權利義務時，人民身分證明之工具。雖然，在日常生活中，身分證事實上已被廣泛地使用在國家與人民間關係以外的其他場合，但戶籍法本身仍只在國家與人民之間關係的目的與範疇內，才授權主管機關強制發行身分證。換言之，戶籍法第 51 條所稱國民身分證的全國性身分辨識效用，應依其究為個人權利或義務，區分為「法定的強制身分辨識義務」，與事實上提供予個人的「任意性身分證明方法」；前者是戶籍法授權強制發行身分證的目的，後者則欠缺強制為之的法律基礎。

是以，前述晶片身分證第 1 區（村里鄰戶籍區）及第 2 區（公開區），如開放允由當事人自由選用，勉強可認為並未違背法律保留原則。但倘依內政部目前強制登載第 1 區及第 2 區之規劃，恐已超越戶籍法授權的範圍，並因欠缺其他可限制個人資訊自主的法律授權基礎，而違反法律保留原則。

三、　晶片身分證外國與臺灣法制比較

接下來將分析身分證從紙本轉為晶片，是否僅為格式的改變。過去在紙本身分證時代，確曾存在很多不同格式。但從紙本轉變為晶片，真的只是「格式」的問題嗎？

內政部推動 eID 政策常提到以德國、愛沙尼亞為師；而臺灣本身的戶籍制度則與日治時代臺灣的戶口制度有關聯性。基於這樣的理由，以下即以德國、愛沙尼亞、日本為對象，與目前政府對於 New eID 的規劃及法律制度的建置狀況進行比較與研析。

德、愛、日三國雖均有身分證，但其實質內涵與使用規範，與臺灣有諸多不同之處。德國雖規定強制領證，但替個人編派統一編號在德國被認定為違憲，所以德國並沒有像臺灣一樣一人一號的統編；日本雖規定每人應配賦一人一號的 My Number，但並未規定強制領身分證，個人仍可自由決定領卡與否；愛沙尼亞既有一人一號的身分證統編，也有強制領證的規定，但愛沙尼亞仍沒有像臺灣訂有強制攜帶證件的規定。臺灣在學習其他國家成功發行晶片身分證經驗的時候，必須理解各國在制度上的背景條件。

德、愛、日雖有上述差異，但其共通之處在於，三者均於其個人資料保護法之外，再制訂規範晶片身分證的專法。三國的專法除了就晶片身分證的發行給予法律的授權基礎、界定個人在晶片化與數位化程度上的權利與義務之外，主要目的是在更嚴格地規範晶片身分證產生「數位資料」後的蒐集、處理與利用。

晶片身分證外國與台灣法制比較 I

	德國	愛沙尼亞	日本	台灣
終身一人一號	X	●	●	●
強制領證	●	●	X	●
強制攜帶證件	X	X	X	●
基本的個人資料保護法	●	●	●	●
專法規範晶片身分證	●	●	●	X

在晶片化與數位化的程度上，三國亦有差異。德國雖強制發行晶片身分證，但專供身分驗證及電子簽章的憑證（自然人憑證）功能則屬選擇加入(opt-in)，僅於當事人決定購買時，身分證上才會附加憑證，強制發行的身分證本身並不預設置入自然人憑證。此外，德國雖強制發行晶片身分證，但個人也可選擇整個關閉晶片身分證上的晶片功能，讓身分證成為一張單純的塑膠卡，完全保障個人選擇不接受數位化風險的自由。

日本在領卡上並非強制，因此晶片卡的身分識別、驗證或簽章功能可說全部由個人選擇加入(opt-in)，同樣保障個人在面對數位化風險時的選擇自由。

愛沙尼亞雖可自由選擇退出(opt-out)憑證功能，但卻強制規定晶片身分證必須具備數位身分識別功能。這樣的制度設計表面上與內政部目前的規劃相似，但愛沙尼亞身分證的數位化與晶片化程度，卻是建立在其獨特的制度與文化條件之上。首先，愛沙尼亞設有個資保護的專責監理機關（而臺灣現在還沒有），積極對公私部門蒐集處理利用個資的行為，進行法遵管制。其次，愛沙尼亞政府過去針對資安事件均展現出負責任的態度，在資安攻擊後，除主動承認錯誤外，也積極尋求改善之道，贏得人民對政府的信任。再者，愛沙尼亞在法律上高度保障個人資訊自主權；早在 1997 年的愛沙尼亞個資法中，即以優於當時歐盟個資指令的標準保障個人的資訊自主權。最後，愛沙尼亞所在的北歐社會具有深厚的社會

連帶傳統，個人不僅較願意與他人共享權利，也願意與他人共擔義務。凡此均是愛沙尼亞得以成功推動身分證晶片化及政府數位化的真正原因。

晶片身分證外國與台灣法制比較 II

	德國	愛沙尼亞	日本	台灣
數位身分識別	Opt-out	●	Opt-in	●
數位身分驗證	Opt-in	Opt-out	Opt-in	Opt-out
近用授權（電子簽章）			Opt-in	
身分資料取用限制	●	X	●	X
身分資料串連限制	●	X	●	X
個資專責保護機關	●	●	●	X
個人對政府足跡之監督	●	●	●	X

從德國、愛沙尼亞、日本的比較研究後可以得知，身分證的晶片化因為涉及數位時代資料的蒐集、處理與利用，對於「誰」可以「為了什麼目的」使用身分證「蒐集甚麼資料」等，各國均以專法予以規範，而非僅將之視為與紙本身分證的格式轉變。內政部欲以現行戶籍法第 52 條身分證格式決定權作為身分證晶片化的依據，卻無視身分證晶片化將帶來與紙本身分證全然不同的數位風險，並非妥適。

On T-Road

王大為

中央研究院資訊科學研究所　研究員

一、　「道」與「路」－T-Road 的管理問題

從當前已公開關於政府骨幹網路 GSN 劃設資料交換通道（T-Road，下同）的政府文件來看，我國政府僅聚焦於 T-Road 的資料串接功能暨預期成果，但對 T-Road 的管理問題的實質內容幾乎可說是未置一詞。國發會在〈智慧政府行動方案〉第 6、7 頁中提到，國發會要為 T-Road「建立一致性的介面、規範及管理平台」，還要「協調各部會進行跨機構機關資料法規調適」，可見規範建立仍是重點，問題在於我們看不到政府在此目標上有何具體明確的作為。例如，同一國發會文件第 21 頁提到，管理平台要確保「交換紀錄可溯」，但對何謂交換紀錄可溯並無明確定義。從 T-Road 服務建議書徵求文件(Request For Proposal, RFP)來看，機關之間交換資料的次數應該包含在內，因為該交換次數是 KPI，但被調用資料的民眾是否可以查詢其資料被政府機關調用的紀錄？這點因為 RFP 沒寫，所以其實是不明確的。重點是，在設計任何制度(「路」)前，作為制度骨幹的規範原則(「道」)，必須先行確定。

至於所謂「整體目標」應該要做到的事情，可以類比政府的流程再造，而非流程數位化，二者有根本上的差異。流程數位化失敗，全世界都深受其害，才會有流程再造。一開始大家的思維很簡單，有了新的資訊技術，就單純地把過往的流程改為數位化執行，等到後來發現做出來覺得不大對勁，才會有流程再造。這邊存在一種常見的思維就是，相關規則早已存在，繼續沿用即可。問題是，過往的路跟現在的路不是同一條。舉例來說，騎馬在泥土路上想要讓人家不能追蹤，就自己跳下馬來把馬的足跡擦掉幾個以後就可以處理，但是有 eTag 系統的高速公路，一路就是追蹤到底，除非像是做一個鐵盒子然後把 eTag 放到裡面來阻止被偵測，不過這樣繳費就比較麻煩。

基本上，很多系統管理上的細節，必須要對該系統上使用的新科技，加上對

相關法律或規則有一定的理解，才能有效處理。這件事非常困難，不是任何人都有能力處理，但一件很清楚的事就是，非數位化系統跟數位化系統，二者絕對是需要不一樣的管理方式。

二、 對管理缺陷的呼籲與建議

再強調一次，現行管理有著規範內容不明確的問題。RFP 裡所謂的相關查調紀錄歷程同步上傳至中央控管系統，其具體內容究竟為何？又，何謂交換資料可溯？這些都是重要的、原則性的細節，但相關政府文件中並無清楚解釋。而為提高行政效率，MyData 透過安控伺服器提供大量資料檔案或二進位檔案，亦即能傳輸大量資料，但相關事務由誰管理、如何管理的問題，除了一句回到各主管機關外，實質內容並不清楚。文件中著墨到的對管理的議題，「協助盤點各機關資料供需情形及各機關資料傳輸現況」、「協助本會（編註：國發會）訂定 T-Road 管理規範及資安管理規範」，在系統（路）已經在開的情形下，恐怕進度稍嫌緩慢。

當然，國發會也有值得讚許的地方，就是其有提到要設計以 Privacy by Design 為原則的隱私保護機制，然後還要檢視相關的規範技術等等，亦即在事情的源頭就開始把 privacy 當回事，而不是等到出事後才買一塊布把它遮起來。然而問題在於，實際在建置系統時，是否能有效落實事先規劃的隱私保護設計，而非等系統大致完成後，才開始追加設計相關隱私保護機制。

因此，我的建議是政府應該以 TW-Way，Trust-Worthy Way toward Smart-Society 取代 T-Road，其具體工序如下：一、建立隱私保護專責機構；二、建立 TW-Way 原則，例如以告知同意、紀錄查詢等方式確保個人對其個資的可控性，以及系統應保持透明與開放溝通等；三、盤點跨部會資料需求及其授權基礎（注意：此非資訊部門工作）；四、流程再造；五、資通工程實現上述原則。此時，工序是重點，因為就算整體目標正確，只要工序出錯，其結果仍是負面的。例如專責保護機構應在一開始建立，而非等整條 T-Road 都完成後，才要求其遷就系統現狀，淪為遮羞單位。

T-Road 與個人隱私保障

王柏堯

中央研究院資訊科學研究所　研究員

一、　安全與隱私概念的異同

很多人會誤解安全跟隱私是同一件事情，但事實上不是。有一個非常簡單的方法可以區別兩者，首先，安全通常是指說我要保護我的資料，不要給不該看的人看到。相對地，隱私通常是說我的資料經過授權，給某個人看，但是我希望那個人不要因為我授權的資料去推論一些我不想讓人家知道的東西。簡單比喻來說，安全就是買一把很好的鎖把東西鎖起來，沒有人看到就安全。隱私是東西我要給你看，所以買鎖沒有用，我心甘情願給你看，但是我希望你不要看到不該看的東西。所以光靠安全的技術是沒有辦法解決隱私的問題。所有跟 eID 相關的討論或是跟 T-Road 相關的討論，當在談隱私的時候，事實上很多問題要重新去看，而不是說就買一把很好的鎖，用國防規格的安全晶片就可以有隱私保障。

過去的研究顯示，安全事實上是一個很老的問題。一個很有名的例子就是密碼學上的 Caesar cipher，就是羅馬共和末期的獨裁官 Julius Caesar 發明的編碼方式，這代表著兩千年前就有安全的問題。另一方面，通常在法律上提到隱私問題時，會以 Warren and Brandeis 在十九世紀末時，為回應相機出現導致的入鏡問題所發表的文章，作為隱私權起點。兩千年來安全問題其實沒有完全解決，這個是做任何資安的專家都認同的。相對而言，隱私問題僅誕生一百年多一點，所以解決的前景是非常看好的，因為還有兩千年可以努力。

隱私問題困難的原因，在於隱私在定義上牽扯到文化、族群等，各個不同的非技術層面。這讓我們不知道隱私到底要什麼，到底什麼叫做保障隱私？今天不同國家的人會有不同的看法，不同文化的人會有不同的看法，甚至不同性別的人都會有不同的看法，我們很難去設計一個技術幫所有人達到他們的願望。事實上，直至今日在很多社會科學──哲學、法學、還有政治學、社會學上，都對隱私有各種各樣的討論，從隱私是什麼，到什麼叫做保護隱私，都有各式各樣的理論。

隱私沒有像安全一樣，就是買一把好的鎖，關起來不讓人家看，這種這麼乾淨的定義，所以這不會是個單純的技術問題。它牽扯到法律、牽扯到文化，今天找做資訊的人來做隱私保護，基本上就是錯誤的、不可能的事情。另外就是，過去二十年來的經驗，只是明白的告訴我們──就算只把隱私當作一個純技術問題，都還是太複雜，現在也解決不了，此容後詳述。

二、 隱私保障應有的要件

雖然隱私其實沒有一個技術或是一個普遍性的定義，但是無論如何，還是要繼續討論如何保護。以下是我認為，一個好的隱私保障大概要有的一些條件：第一，隱私保障不應仰賴他人的善意。這是從安全保護借來的概念，就是安全不能是立基於某人不做壞事，隱私也是同樣的道理。第二，所有隱私保障的方式都必須符合法律要求，像是台灣有個資法、歐盟有 GDPR、加州有 CCPA 等，要有法律統一規定隱私保障的方式。第三，隱私保障應該要可以滿足每個人的基本期望，就是雖然每個人對隱私的要求及定義不太一樣，但是有些最基本的要求仍是所有人共通的，而對這種最基本期望的侵害絕對不能發生。以下將以這三個條件為中心，檢討 MyData 平台的問題。

三、 Mydata 平台的問題

MyData 數位服務個人化平台重點是以「民眾隨心同意、資料隨手可得」為核心理念，我在看這段話時，第一個想的是說，任何個人資料的電子傳輸，它都有相當的安全跟隱私的風險，這段話裡完全沒講。然後，如果我把個人資料自己保存，事實上我要承受更多安全跟隱私的風險。

我們可以看到平台上的個人資料使用同意條款，最後一句話寫得非常好聽：「透過您當次的同意，便可在 MyData 平台中取得政府機關單位所保存您的個人資料，並可當次將這些資料提供給政府機關或您信賴的政府企業使用」。以技術人的觀點來看，最後一句話應該寫的是說，「透過您當次的同意，便可在 MyData 平台中取得政府機關單位所保存您的個人資料，並可當次將這些資料提供給政府機關或您信賴的政府企業『重複』使用」。換言之，此處資料不可能只會使用一次，這件事之後將以間接證據證明。

接下來是 MyData 使用規則的問題。從 MyData 數位服務個人化首頁，按「資料下載」、按「財稅」、按「財產資料」、再按「我要下載」，後面就列出長長一大堆使用規則。其第三條，關於「資料保管及使用」明文：「當您使用本平台取得

個人資料後請妥善保管，其下載資料後續的保管、使用方式及其所造成之影響，本平台不負任何保管、管理及損害賠償責任。」換言之，我如果去 MyData 下載我的資料，MyData 很友善地告訴我說，它不負任何的保管、管理及損害賠償責任。而對任何資安專家來說，妥善保管個人資料，意指要定期更新系統、要安裝防毒工具、要改密碼、不要用同一個軟體、不要上可疑網站等等二十幾點注意事項，亦即正常一般人不發生資料外洩的情況，可能性接近於零。所以 MyData 平台真正的意思應該是，「民眾隨心同意、資料隨手可得、後果自行負責、自行承擔」，政府很明白地告訴我們這些事情。而我認為這樣的隱私保障並沒有符合我的個人期望。

另外就是數位個人資料其實非常容易複製，畢竟是以電子檔案形式存在。問題是，今天不管是機關或機構，當它擅自取用個人資料並大量重製，當事人本人基本上無從得知。所以這邊的隱私保障，完全是仰賴他人的善意。

當然這時候政府機關會說，所有的事情都回到個資法，由個資法提供隱私保護。然而當我們檢視 MyData 的隱私保障條款中，對於資料使用之「特定目的」的敘述，包含了「行銷、網路購物及其他電子商務服務」，或是在另一個例子中，包含「其他金融管理業務、其他經營和於營業登記項目或組織章程所定之業務、其他諮詢與顧問服務」，就令人產生很大的疑問。「特定」目的的內容竟然可以如此包山包海，而且這些目的內容顯然也不是只須使用一次個人資料即可達成，則此時使用者恐怕並未受到保護。

四、　隱私保護的技術上困境

另外補充有關隱私保護的技術上困境。關於隱私，一個著名的歷史事件是，1997 年美國 Massachusetts 的團保委員會要幫州政府員工和家屬買保險，團保委員會就蒐集了 135,000 位員工的資料，經過去識別化，刪除包含名字在內的一些資訊後，就把資料提供給研究人員，之後賣給產業界。去識別化後的資料大概有一百個欄位，包含性別、種族、出生年月日、郵遞區號五碼、就診日等。當年有一位女士，她發覺只要根據性別、出生年月日還有五碼郵遞區號，就可以分辨不同的個人，雖然可能無法特定出某筆資料是誰的資料，但可以知道某筆資料和另一筆資料是兩個不同的人。根據這位女士的論文內容，她就花了二十塊美元，買了一本麻州的選舉人登記名冊，名冊中包含了姓名、地址、出生年月日、五碼郵遞區號。然後她便根據性別、出生年月日、五碼郵遞區號，特定出州長的保險資料，之後將該資料寄給了州長。這位女士叫做 Sweeney，她那個時候是 MIT 的學生，現在是哈佛教授，她在 2001 年提出的 K-匿名機制，現在很多地方都在使用，

包含我們的健保資料庫。

在二十年前 K-匿名機制被提出之後，二十年來專家學者們提出了大量的新的隱私保障機制。之所以會「大量」提出，是因為當大家發現前一個方法不能解決問題時，就再提出下一個，但直到目前為止，光就技術上而言，其實都還沒有人可以說有一個完美的隱私保障機制，而且不同的資料庫須用不同的技術去保護隱私。這告訴我們的是，保護隱私這件事情，就算這只是一個技術問題，二十年來的經驗告訴我們，這是一個困難到現在還是解決不了的技術問題。

五、 T-Road 的問題

最後是關於 T-Road 的問題，T-Road 將來很重要的目的，是希望串連政府之間的資料庫。簡單的理解就是，MyData 允許個人向政府取得自己或是政府的資料，透過自行負責確保資料安全，然後 T-Road 是不同的政府機構、單位之間可以傳送大量資料的通道。這裡有疑義的是關於 T-Road 傳輸機制失靈時，例如在保管或傳輸時爆發大規模資料外洩事件，相關的責任追究問題。整個系統是否有保留詳細紀錄，能幫助事後確認事件狀況與責任所在？

不過，更根本的問題是，二十年來的隱私研究告訴我們，隱私跟資料的價值就像是魚與熊掌不可兼得，沒有什麼又有價值又有隱私的資料。當資料越有價值，我們的隱私風險就越高。然後不同機關間蒐集的資料，因為不同機關間有不同的特性，所以它的隱私風險還有隱私保障其實也都不一樣。在不同機關保有的資料，在保護隱私上就要有不同的方法，而不同的機關資料如果串在一起之後，又會變成另外一個不同特性的資料，所以它的隱私保障機制還有隱私風險評估也必須重新來做。選舉人名冊跟保險資料，分開看沒什麼問題，一串起來就能拼湊出新的資訊。所以將來如果 T-Road 要在政府機關間大量串接資料，甚至是讓 Google 或 Facebook 這種知道民眾大量私人秘密的非公務機關使用時，如何避免資料被任意串接一事，是要特別注意的。

六、小結

隱私事實上同時兼及法律跟技術，它比安全問題要複雜非常非常多。而隱私跟安全一樣，逃避不會解決問題，我們只有先了解並正視：隱私保護就是非常困難、就是需要窮盡所有的方法去保護，才有可能找到比較合適的解決方法。

T-Road 之管制困境

吳全峰

中央研究院法律學研究所　副研究員

一、　T-Road 資料傳輸架構概述

臺灣 T-Road 規劃方向，是類似資訊高速公路的概念，藉由 T-Road 串接不同資料庫並使資訊可在 T-Road 上自由流通與介接。運作上，可透過 eID 或其他方式介接，在 T-Road 上完成資料串接與交換，可能包括以下兩種模式：（1）當事人可透過同意方式，經由 MyData 或是其他 T-Road 入口網，由自己或透過第三人介接或存取不同機關間的個人資料（目前經當事人同意透過 MyData 可取得之資料大約有 100 多項）；（2）機關間亦可利用 T-Road 去直接交換各機關所保有之當事人個人資料。

雖然 T-Road 建置之基本概念是參考愛沙尼亞 X-Road 而來，但 X-Road 在規範上需依循歐盟 GDPR 規範（因愛沙尼亞為歐盟成員國，故須受 GDPR 規範），惟臺灣政府對 T-Road 規劃之規範架構與運作模式，是否完全依循 X-Road 在 GDPR 規範下對個人資料之保護，卻不無疑問。

二、　T-Road 之規範挑戰

（一）管制之碎裂化

基本上並沒有人會否認「資訊為材料，技術為工具」這個概念，也多會同意透過技術有效運用資訊，將能對產業、經濟或社會產生龐大效益；而爭執之核心往往在於，作為資訊運用之工具，社會對於技術是否應該適當規範，而規範之密度為何。在 T-Road 之政策規劃中，也面臨同樣的技術規範挑戰。詳言之，T-Road 本身是一個資訊運用之有效工具，藉由資訊高速公路之建置，不同部門之資訊可以在 T-Road 上更有效率、更廣泛地進行傳輸、串接、交換與流通；但在 T-Road 運用上，卻不難發現技術與規範是不能、亦不應完全加以切割。因為若僅重視材料與技術

而忽略規範，就如同建房子時僅有水泥與機器，但卻沒有建築法規，房子安全性將無法確保，亦可能危及公共安全；同理，若僅有機關保存之個人資訊（材料）與 T-Road（技術），雖然資料利用之效能大幅提升，但若沒有針對 T-Road 之適當、完整規範，個人資料保護—包括資訊自主與資訊隱私—亦將無法確保，而可能對社會造成更大傷害。

但在目前 T-Road 之討論上，卻不難發現大多仍集中在技術問題之解決，規範問題卻相對被忽視，甚至將後者單純視為既有規範下各機關應個別解決之管制事項，而忽略 T-Road 作為新興資訊工具之應用與建立可能對個人資料保護規範形成之根本性挑戰；其實，許多學者在討論 T-Road 時，多要求需要建立專法或專責機構，便是嘗試解決新興技術引起之規範問題。換句話說，在討論 T-Road 時，如何解決技術問題並確保資訊安全，的確是重點；但這卻並不代表資訊安全的技術問題解決後，規範性問題便一併解決，個人資料保護之重要要素，包括合法性（lawfulness）、資料最小化（data minimization）、告知後同意之衡平、監管與申訴等課責機制（accountability），均需進一步檢視是否因 T-Road 之建立而受到影響，以及檢視因 T-Road 建立而使大量資料統整與快速流通成為可能時，是否有建立統一規範加以管制之必要性。但在 T-Road 之討論中，這些規範性問題卻明顯到忽視。

詳言之，不管是 T-Road、作為 T-Road 入口之 MyData、或是利用 T-Road 進行之機關間資料傳輸，對這些不同技術所架構起之完整個人資料流通並串接之架構，在管制規範上卻是「碎裂化」的，便有可能導致個人資料保護出現矛盾、甚至無從界定可論責對象與範圍之困境。以機關與機關間透過 T-Road 傳輸個人資料而言，目前之規畫方向便是由各機關確定其資料傳輸之合法性基礎，T-Road 相關規範僅限於資料傳輸之技術（如 log 之建立），但完全不管資料傳輸是否具備合法性；但這就像是在高速公路上對於速限、超速車輛之攔查完全沒有統一規範，而要求回到各縣市主管機關個別處理該縣市註冊之車輛一樣，會使得作為資料整合之 T-Road 成為個人資料保護碎裂化下的空白。換言之，雖然各機關在資料傳輸時仍須確保合法性基礎，但這並不代表 T-Road 主管機關便應完全信任各該主管機關之判斷而沒有任何確認或稽核機制，即令 T-Road 主管機關無法就合法性內容進行判斷（權責可能仍在各該主管機關），但 T-Road 仍須就合法性進行實質審查，確認無侵害個人資料保護之虞方能進一步允許資料傳輸。舉例而言，若 B 機關（或個別公務人員）在缺乏合法授權基礎下向 A 機關提供個人資料之傳輸，T-Road 是否可在完全不確認其合法性要件是否形式上齊備情況下，仍允許此資料之傳輸？雖然有論者可能主張，針對違法提供個人資料之機關或個人仍有相關

處罰機制，但該機制僅是事後之處罰與賠償，對於個人資料釋出所可能造成之傷害卻已無從避免；因此，如何從事前預防機制之概念出發，建立在 T-Road 上傳輸資料合法性之基本規範要求，便有其重要性。再舉一例，若個人對於 B 機關進行其個人資料傳輸之合法性有所質疑，並要求 T-Road 暫停資料傳輸，T-Road 是否能以合法性判斷屬各機關權責，而忽視或拒絕當事人之主張？

在資安保護上也有類似管制碎裂化之狀況。目前在 T-Road 下所串接之各機關資料庫，是否應有統一之資安認證要求，政府似乎採肯定見解，而仍回到各主管機關自行認定；但若 T-Road 已建立一條資料傳輸與串接之管道，在資安上卻仍各行其是，甚至導致資安要求不一致之情形，對於在 T-Road 上流通、甚至將進行串接之各類個人資訊之安全保護，並不適當。

簡言之，在傳統資料傳輸的架構下，資料傳輸的數量與次數還是某種程度受到限制，因此即使管制規範呈現碎裂化之情況，對民眾權利雖有影響，但程度可能有限；但在 T-Road 之建置卻使資料傳輸之數量與頻率大幅度增加（這也是建置 T-Road 之目的），其對個人資料保護之影響也顯然與傳統資料傳輸技術不同，如大量資料傳輸與串接可能增加功能蠕變(function creep)之風險，而 T-Road 管制規範碎裂化之情況，不僅忽略 T-Road 對個人資料與隱私保護可能產生之新興風險，也忽略了規範整合對於規範此類新興技術之必要性。

（二） 資料處理合法要件之確認

1. 法定職務

在個人資料傳輸之正當性與合法性要求上，個資法之規範本就存在爭議，而這個爭議在 T-Road 下可能會更為複雜。以公務機關對個人資料之蒐集、處理與利用為例，其應於執行法定職務必要範圍內為之（第 15 條及第 16 條，敏感性個資則為第 6 條），但所謂法定義務應該要依「作用法／行為法」或是「組織法」界定，便是健保資料庫乙案在法院爭訟之重點；而類似爭議在 T-Road 下，是否可能因為對資料傳輸或串接之效率要求，使主管機關在檢視行為法是否足以作為行使職權之授權依據，或是檢視組織法是否實質上兼具行為法功能時，被迫壓縮判斷空間與時程，從而使主管機關在無從充分檢視個人資料釋出合法性之前提下便匆促釋出個人資料，不無疑問。且因為 T-Road 本身對資料傳輸之合法性要件並未有規範要求，而仍是回到各主管機關自行判斷（管制碎裂化），則主管機關對於資料合法釋出之要件是否已善盡檢視之責，T-Road 亦無從要求，從而導致個人資料可能已經釋出，但合法要件是否被充分滿足仍處於不明狀態（尤其涉及不

同機關之判斷）之矛盾狀況。

2. 告知後同意

另外一個例子是告知後同意，依據個資法規定，經當事人同意亦被視為公務機關或非公務機關蒐集、處理與利用對個人資料之重要合法要件之一。但須注意者為，當事人同意並非形式上滿足「告知」與「同意」這兩個要件即可，

告知後同意要件能正當成立須滿足「充分告知、非強制、無操控」等內涵，亦即當事人必須要能夠「充分理解」資料流通串接之相關資訊（如特定目的）、在「不被強迫」下同意（如雙方議價能力必須充分相當），才能夠滿足經當事人同意在T-Road架構下進行資料傳輸串接之正當性與合法性。但問題在於，僅少數機構對於經當事人同意訂有特定要件，多數機構多仍僅將此要件視為形式上之要求，而若T-Road對此又不訂定具體之最低規範標準，仍任由各主管機關決定，則不啻在未經當事人充分理解之前提下，便允許公務與非公務機關在T-Road上任意傳輸串接個人資料，勢必對當事人權利將造成嚴重影響。舉例來說，檢視目前各銀行透過MyData要求客戶同意其向主管機關申請蒐集並利用相關個人資料時，銀行所提供之告知後同意說明書往往是非常廣泛的同意，前述應有之告知後同意要件往往未能得到滿足。以某銀行在MyData 數位個人資料服務網頁中所提供告知後同意說明書為例，其中法定告知事項對於蒐集、處理、利用個人資料之特定目的便包括「信用卡、轉帳卡業務、人身保險、外匯業務、存款與匯款、行銷、金融服務業依法令規定及金融監理需要，所為之蒐集處理及利用、金融爭議處理非公務機關依法定義務所進行個人資料之蒐集處理及利用、保險代理業務、契約、類似契約或其他法律關係管理之事務、借款戶與存款戶存借作業綜合管理、核貸與授信業務、消費者、客戶管理與服務、消費者保護、財產保險、帳務管理及債權交易業務、授信業務、資（通）訊服務、資（通）訊與資料庫管理、資通安全與管理、網路購物及其他電子商務服務、徵信、調查、統計與研究分析、其他金融管理業務、其他經營合於營業登記項目或組織章程所定之業務及其他諮詢與顧問服務」[1]，幾乎所有事項均含括在其中（甚至包括「調查、統計與研究分析」），而成為允許銀行得恣意使用該個人資料之概括同意(broad consent)。在此情況下—當事人並無議價空間要求銀行僅得就當事人申請之業務取得必要資訊（資料最小化原則）—若銀行之主管機關並未就此廣泛授權之告知後同意做出限制，T-Road 主管機關卻仍繼續接受此明顯違反當事人資訊自主權保障之告知後同意形式，並允許個人資料透過其所提供之技術與服務流通並串接，顯然有違個人資

[1] 請參考 https://www.taishinbank.com.tw/eService/loanmydata/（最後連覽日：2020 年 10 月 27 日）。

料保護之精神。

而且在前述所舉銀行所使用 MyData 告知後同意之例子，因為在特定目的範圍內包括「調查、統計與研究分析」之概括條件，故即令當事人已終止銀行業務，銀行仍得以此目的為理由繼續使用當事人個人資料，當事人資料幾乎等於由銀行永久保存，而使得個資法所規範「個人資料蒐集之特定目的消失…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」、或其同意書所載資料保存期限為「特定目的存續期間」，成為不具意義之規範。

再舉一例，在 MyData 平台入口網上亦載明，假設資料蒐集之範圍與處理之條件有「重大變更」，便應以合理方式通知當事人，但何謂「重大變更」卻沒有定義，民眾因此無從得知主要規則為何；則若發生重大變更（如變更特定目的內容），但主管機關未有要求通知，則 MyData 或 T-Road 是否仍將允許在未通知當事人此重大變更之前提下持續進行資料之傳輸與串接，目前亦未有規範。理論上，這些告知後同意要件均屬資料得以在 T-Road 上合法傳輸之重要前提，並應該要有標準化規範或形式上要求，而不應任由各銀行、或各主管機關自行決定，導致應經當事人同意方得以在 T-Road 上傳輸之個人資料，但若 T-Road 連最低限度之一致性要求都沒有相對應之規範，將很難期待對資料傳輸合法性要件之確認或監督。且現實之情況往往是，各主管機關對於告知後同意之要件並沒有規範與要求（如前述銀行之例子），MyData 與 T-Road 又將確認告知後同意之責任委予各主管機關負責，則個人資料便在當事人同意內涵模糊與混亂之前提下，已展開或預計展開大規模之傳輸與串接。

3. 資料最小化原則

若從前述銀行之案例，不難發現不僅在告知後同意上可能出現問題，其概括之資料蒐集目的所蒐集之廣泛個人資料亦與資料最小化原則相違背，亦即銀行所蒐集之資料已超越其所欲達成特定目的所必要者。暫且不論資料最小化之判斷應由各主管機關或 T-Road 主管機關判斷之問題，在 MyData 與 T-Road 機制之設計上亦沒有可供當事人選擇同意傳輸資料範圍之選項，亦即若銀行要求 X、Y、Z 哪種資料，當事人可以選擇僅願意提供蒐集 X 與 Y 資料之授權，而拒絕銀行透過 T-Road 取得 Z 資料；目前在 MyData 與 T-Raod 之設計上，對於同意機關存取資料之範圍，呈現一個全有全無的概念，亦即當事人只能選擇同意機關存取所有列舉之個人資料，或是選擇不要申請該項服務，並沒有中間之選項，而類似對個人資料取得全有全無之制度設計，便可能使實務上操作資料最小化原則更形困難，更遑論當事人與機關間議價能力之差距，將使前者無從拒絕同意授權機關要求之所有個人資料。因此，T-Road 主管機關在此處勢必要扮演把關之角色，否則相對

處於弱勢之資料所有者便可能在「形式上同意」之狀況下，被強迫釋出個人資料。

4. 實務操作

最後則是實務操作上之問題。近年許多研究均已在討論，民眾在資訊年代透過電腦、手機或 app 進行告知後同意時，往往忽略系統出現之告知後同意說明之內容，而使得當事人同意流於形式，並無法真正保障當事人知情同意之權利；也因此，對於告知後同意從紙本或口頭轉變成為透過電子方式進行時，如何透過流程設計確保當事人充分理解必要之內容，便成為重要議題。如在告知後同意說明書之後要做一個小測驗，確定當事人針對告知後同意的重要資訊有正確的理解之後（亦即通過測驗），才能進行下一個步驟核實當事人的同意（若無法通過測驗，則重新顯示告知後同意內容並重複此程序）。而當個人資料均可透過 T-Road 傳輸時，也會產生類似之顧慮，亦即透過電子方式確認個人資料傳輸之合法性或當事人之同意時，是否可能因為操作簡便性而忽略合法性確認之審慎性（許多社會學研究或實證研究都發現，當事人對於虛擬同意與實體同意之理解與謹慎程度並不相同）；因此，如何透過不同程序設計以確認合法性要件之滿足（如同前述之小測驗），便有其意義。換言之，雖然個資法對個人資料蒐集、處理及利用之合法性本就有規範，但在使用之科技與以往不同、資料處理數量龐大、時間緊縮之情況下，T-Road 主管機關對於資料傳輸或串接之合法性確認，並非毫無意義。舉例而言，雖然個資法對於「當事人同意」作為資料傳輸合法性基礎有所規範，但 T-Road 仍可就告知後同意之方式與流程有所要求；再如「執行法定職務」同樣可作為合法性基礎，但 T-Road 仍可要求資料傳輸與接收機關，必須明確說明法定職務之具體內容與法律依據，雖然無法具體審查其內容，但仍應建立形式上與程序上之規範，而不應僅任由各主管機關自為主張。

（三） 資料傳輸之可論責性不足

前述管制碎裂化與合法性要件監督機制不足之挑戰尚未解決前，若便貿然執行 T-Road 計畫，顯然無法確保 T-Road 在個人資料保護上之完備。以歐盟為例，GDPR 要求會員國成立獨立個資保護之專責機構，並且在有效相關法律已完備且確實執行後，方能進行合法之資料傳輸與處理；但以臺灣目前狀況，在專責機關尚未建立、管制碎裂化狀況沒有改善時，便貿然將大量個人資料透過 T-Road 傳輸與串接，不免將面臨規範上本末倒置之質疑。

雖然個資法已有基本之規範，但如本文稍早主張，T-Road 之技術將使個人資料傳輸與串接之數量與效率大幅增加，而不同於傳統之資料處理技術，而仍單純

以傳統個人資料保護之管制模式、或是分散式管理(各主管機關分別獨立規範),是否足以解決 T-Road 新技術所帶來個人資料保護之挑戰,不無疑問。因此,在 T-Road 之架構下,專責獨立之個資保護機關與協調一致之管制規範,對於個資保護與機關行為可論責性之建立,更有其重要性。

除獨立個資保護機構外,就違反個資保護規定而於 T-Road 上違法傳輸個人資料者,除個資法之規定外,在 T-Road 上是否有適當之懲處機制,亦未見適當討論。舉例而言,若非公務機關(如銀行)違反合法性要求傳輸個人資料時,是否仍允許其繼續使用 T-Road,或是有適當之停權機制(如健保資料庫之規範)禁止該機關繼續使用 T-Road?若係公務機關違反規定,就機關整體為停權處置可能會影響行政效率,但仍可思考是否就個別行政機關有停權之機制。但目前規劃仍將歸責(accountability)規範回歸各主管機關處理,T-Road 本身之監督機制卻是欠缺的;只是,僅將 T-Road 視為資料傳輸之「工具」,而完全不過問透過這個工具傳輸資料是否違規及違規後之處置(建立適當之監督與懲處機制,在技術上並非不能達成),就 T-Road 本身可以處理個人資料之能量而言,似乎並不適當。

(四) 資料傳輸之透明性有限

即令相關個資保護原則均能在 T-Road 規範中被確保,資料傳輸之透明性仍是另一個需要被重視的挑戰,因為民眾需要透過此機制理解究竟有哪些攸關其自身之個人資料被哪些機關在何種目的下進行蒐集、處理與利用。

就目前 T-Road 之規劃,資料之傳輸是會留下傳輸紀錄,以確保民眾可以查詢或瞭解其資料流向;但問題在於,該傳輸紀錄之內容僅包括是哪些機關進行資料傳輸、傳輸資料概括內容、與傳輸時間,但對於傳輸之個人卻沒有留下紀錄。但就愛沙尼亞之 X-Road 規劃而言,操作 X-Road 進行資料傳輸之個別人員(如公務員)必須以其 ID 進行操作,並留下該個人操作之紀錄;此做法之優點是,若個人資料有非法傳輸之情況,雖然機關仍須負行政督導之責,但僅知道是哪個機關違法將無助於究責,亦無法在執行層面達到有效管理之目的,若能要求實際執行資料傳輸、串接作業之個人亦能留下紀錄,則對於個人資料之有效保護將有很大之助益。

(五) 資料蒐集一次性之濫用

就透過 T-Road 所取得之個人資料,能否由取得機關永久保存,是 T-Road 採行後可能出現之另一個問題。就目前討論中,可以發現有論者主張,在資料蒐集

一次性之原則下，應允許個資蒐集機關（主要是公務機關）得永久保存該次所取得之個人資料，以避免就同一個人資料反覆要求他機關提供，以促進資料利用之效率。但類似之說法實際上已逾越資料蒐集一次性之範圍。

以愛沙尼亞在建置 X-Road 時所主張之資料蒐集一次性而言，主要是針對民眾之權利保障，亦即 A 機關為 X 目的向民眾蒐集α資料後，B 機關為 Y 目的需要蒐集相同之α資料時，為避免重複向民眾蒐集相同資料並造成民眾困擾，遂允許 B 機關得透過 X-Road 向 A 機關請求傳輸α資料;但因為該方便性係針對民眾，而非創造政府機關之方便性，故 B 機關在 Y 目的消滅後仍須刪除α資料，之後若 B 機關因 Z 目的需要使用α資料時，仍需再次透過 X-Road 向 A 機關請求傳輸α資料。加拿大國會在討論愛沙尼亞 X-Road 機制時，隱私委員會委員長亦直接說明，類似 X-Road 機制之建立，並不應擴張至公務機關間平行傳輸之權力，機關蒐集、處理與利用個人資訊還是需要回到既有之個人資料保護規範。

問題在於，類似愛沙尼亞或加拿大就個人資料保護機制在 X-Road 下所應扮演角色之討論，在 T-Road 中並未見到較為細緻之討論或規範；而公務機關仍嘗試藉由資料蒐集一次性之擴張，擴張其對民眾資料蒐集之範圍與保存時間，此顯然與 X-Road 之基本精神相違背。

eID 與社會信任

吳齊殷

中央研究院社會學研究所　研究員兼副所長

各界在討論 eID 政策推行所涉及的議題，常把焦點置於細緻的法律與資安面向的議題之上。本篇文章從社會學家在面對政府推行 eID 政策時，把整個思考拉至比較基礎的角度，進一步地觀察及嘗試理解政府致力於推動 eID 政策的目的及原因為何，以及需要怎麼做比較可能達成其所規劃的目的。

一、　社會信任的重要性

社會秩序，是社會學長久以來在談社會治理時最常被拿來討論的根本議題。不論是遠古或現代社會，只要有人群聚集之處，就一定會有社會治理的問題。不過，在討論社會治理時，有一個很重要的前題，使看不到的社會秩序持續運行著。例如：人群可以安靜無聲地共處在大型會議空間內進行大型活動，或是參與者因為防疫要求配戴口罩。這種集體行為的展現並不是一個必然，而是歸因於社會治理背後的社會秩序。

社會一直靠著社會治理而運行著，而社會治理中最重要的基礎，其實是以社會信任為基礎所維繫的社會架構。如果一個社會沒有足夠的社會信任作為基礎，這樣的社會在社會秩序的維持，將是非常困難的；在沒有社會秩序的狀態下所進行的社會治理，將使該社會一直面臨著非常混亂的狀態。

再進一步談到人類社會的發展，通常被認知為從單一到複雜化，而其所隱含的是從同質到異質的過程。在同質化社會的範疇裡，其實是信任最容易產生的地方。所以，在早期社會因為人與人之間彼此較為熟識，在熟人社會所進行的社會治理，通常比較不會遭遇到太大的困難。但是，當社會逐漸邁向工業化造成社會分工後，人類社會也從熟人社會慢慢地變成陌生人社會。若要在彼此多為陌生人的社會繼續維持社會秩序，就必須仰賴有效的社會治理。社會治理最重要的意義，其實就是要處理及降低這些複雜性，以及因為社會分工所帶來的異質化問題。

當代社會因為網際網路的緣故，使前述的情況益加複雜。原本鑲嵌於日常生活場域的社會行動者，因網際網路的廣泛使用，使其活動場域慢慢地與日常生活場域相互分離。當活動場域與日常生活場域分離之後，在各場域間人與人之間的關係就更形複雜化，這時要進行社會治理，就會變得越來越困難。

二、 社會信任狀態數據的分佈呈現

當嘗試尋求臺灣政府推動 eID 政策目的時，推測可能為了追求更為有效的社會治理，以因應與處理當代社會越來越複雜化、越來越異質化的挑戰，所以選擇在這個時點致力於推動 eID。然而，社會治理的進行，必須具備以社會信任作為基礎為前提，如此一來，在處理與降低社會異質性與複雜性時，才可能得到預期的效果。

臺灣在推行 eID 政策時經常引用愛沙尼亞作為仿效或學習的成功案例，以下將進一步探索愛沙尼亞及臺灣社會的社會信任狀態。透過 2014 年跟 2018 年歐盟具有代表性的歐洲社會調查(European Social Survey, ESS)報告，可以看到愛沙尼亞在整體社會信任狀態的數據分布是比較正向；而依臺灣社會變遷基本調查所所呈現的社會信任狀態數據分佈，其實是偏向較不信任的。接續，再以國家整體社會對於政府信任比例來看，愛沙尼亞對於政府信任的狀態雖然沒有像北歐國家超級高分，但大概也還是介乎於北歐國家與德國間偏中上的程度；而在臺灣社會重要機構的信任度調查報告可以看到，一般民眾對於地方政府的信任高於中央政府，這數據可反映出，前述日常社會裡人與人間的熟悉程度與信任度是相關的現象。

從愛沙尼亞跟臺灣的社會信任狀態的數據分佈比較，愛沙尼亞整體社會信任及對於其政府的信任度比例，還算具有一定程度的信任基礎。或許，這可以推導出，這是愛沙尼亞政府在推行 eID 的過程，並沒有面臨太多阻力的原因之一。而臺灣整體社會的信任基礎，是不是已經達到如同愛沙尼亞社會信任的程度，仍待進一步確認。

同時，觀察愛沙尼亞政府在推行 eID 政策，是採用具有彈性、透明，而且提供人民多重選擇的方式進行。最重要的是，愛沙尼亞政府並未採取強制手段要求人民必須接受且使用 eID。另外，愛沙尼亞政府進行政策推行時，特別強調要注重人民的感受，且強調 authentication、社會面向的安全與隱私保護，在多數人民願意且接受政策的情況下，才會再一步一步地推進。

從愛沙尼亞的經驗可以看出，政府要讓社會政策能夠順利推行，其實背後是累積很多建置社會信任的過程。然而，至少到目前為止，尚未見到臺灣政府推動

eID 所採取的手段、策略為何，亦尚未看到臺灣政府有很明顯的企圖，嘗試著建置社會信任。臺灣社會對於 eID 可能帶來的安全與隱私衝擊，是否已經準備好了？

三、 社會信任的建置機制

那要怎麼建置與累積社會信任呢？在討論社會信任的建置時，大抵多從公平、公正、公開三個面向切入。政府在推行政策或預計達成某種政治目的時，也常常以公平、公正、公開作為進步價值的宣傳。究竟，社會信任的建制的公平、公正、公開，各具有什麼樣的內涵呢？

公平，應該是所謂的立足點的平等。民眾和政府在問題思考上具有同等地位，以及權責對等。但權責對等的意思並不是說，政府有權力時推動政策，而人民就必須配合的責任。另一個最重要的內涵，就是政府政策必須透過一個非強迫性的方式推行，也就是說，在政策面上人民應具有自由選擇的權利。

在談到公正時，是指社會的運行必須受到法律的保障，例如：專法、資安風險的管理制度、責任對應的策略，以及當政府濫用人民資料時，應該受有被課責的機制，以及修復因濫用所造成的損害等相關策略等。政府政策的推行應該建構在這些層面之上，且必須為全面且整體顧及的。當政府表現出這樣的態度時，作為接受方的人民，對政策的信任才有可能逐漸滋生。

最後，有關公開的原則，係指政府之政策推行的訊息應該是雙向透明，應該在預計推動前，把整體政策公開地且透過各種管道，讓政策的訊息，特別是這個政策可能造成的衝擊或影響，必須讓人民知悉與了解。

四、 推行 eID 是社會治理的一環

政府進行社會治理的目的，主要為處理並試圖降低複雜性及異質性，否則將導致治理成本過高，以至於治理目的無法達成。社會秩序需要仰賴有效的社會治理來維繫，如果沒有有效的社會治理，社會信任將會有危機，政策的推動就會變得很困難。所以，處理及降低複雜性與異質性的必要機制就是社會信任，社會信任的建構需要時間，而且是無法被忽略與逃避的。

推行 eID 是社會治理的一環，從社會學家的角度檢視臺灣 eID 的政策推行，建議各方各退一步，重新思考臺灣整體社會是否具迫切的需求在非常有限的時程內推動 eID 的必要。先從構築臺灣社會的社會信任開始，把社會信任機制成功建立後，接下來的社會治理，還有各項政策目標應該是能更容易、更順利地達成。

數位轉型與智慧政府的課責

黃東益

國立政治大學公共行政學系　教授

一、　從電子化政府轉向智慧政府

過去二十年來，政府循序漸進推動了很多關於電子化政府或是數位化政府的機制，包含完備政府基礎資通環境、普及政府網路線上服務等，在國際上的排名也都相當亮眼。近年，行政院進一步提出「2017-2025 數位國家・創新經濟發展方案」，國發會也配合此方案，研擬了「服務型智慧政府推動計劃」，其中出現最多的關鍵字大概就是兩個字——「資料」，提到未來智慧政府就是要以資料為骨幹，結合相當多新的資訊通信科技，以優化決策品質、提升服務品質等，而此計畫構想及具體策略，初步就體現在最近上線的 MyData 平台機制裡，資料擁有者透過平台驗證身份，並且在線上通知後，從資料提供機關比如說內政部下載個人資料，以供服務機構藉以提供臨櫃或線上的服務。

二、　數位轉型的內涵與障礙

那麼究竟上述所謂智慧政府的數位轉型內涵為何？舉瑞典為例，約兩年前我到瑞典名為 IIS(Internet Foundation in Sweden)的機構，請教其中一位資訊通訊科技專家該國類似 MyData 平台的設置進程，這位專家實際示範使用該服務，上網輸入密碼後，分享他們家中所有資料讓我知道，包括家中有幾支電話、有幾部車、他們家的房價，甚至包含附近平均房價，兩年前國外就已經做到相當多資料都整合在一起、民眾可以輕易取得。那麼，目前我國的 MyData 機制剛上線，未來要發展到什麼樣的地步？而除了短期規劃上「服務流程」及「軟硬體設備」的改變，長期、深層的轉型，包括「組織設計」、「資安能力的提昇」，以及「人與人之間、政府與外部關係之間之改變」——即政府內部執行者以及人民心態上是否能夠接受數位轉型相關具體措施，這些層面事實上也可能面臨障礙。詳言之，組織結構上，究竟數位轉型所帶來的便利性及利益，受惠的會是哪些機關？當有究責之必要時，又是哪些機關必須扛起相關責任？常是不清楚的；又，在組織文化層面，必須在推動數位轉型之同時促進提昇政府及人民的「資安文化、資安認知」。

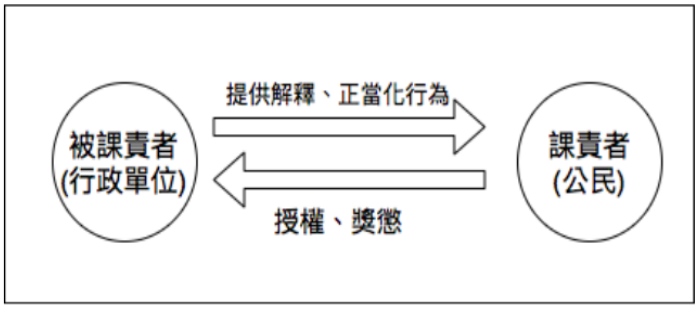
而課責機制之建立，是解決上述可能產生的轉型障礙之途徑。

三、 課責作為克服數位轉型障礙的機制

（一） 課責機制之定義及分類

若要將課責機制作為克服數位轉型障礙之道，首先必須問的是，究竟所謂「課責」之定義為何？傳統上，談到「課責」，就是「誰下台？誰負責？處罰誰？」的問題，但除此之外，參考國外學者研究，認為課責可以被視為一種社會關係，在這段社會關係中，行為者（被課責者）有義務跟重要他人（課責者）解釋與正當化其行為，必須闡明原因、並提供規範依據等，必須達到這些要求，才能算是符合課責之定義。

□課責的流程：委託-代理關係



圖一 課責流程：委託—代理關係

□課責可以依照強制力的來源、程度分為四類

類型		控制來源(Source of Agency Control)	
		內部	外部
控制程度(Degree of Control Over Agency Actions)	高	官僚課責 - 層級節制的監督	法律課責 - 法規、契約簽訂的監督
	低	專業課責 - 專業同儕間的監督	政治課責 - 選民、民意代表的監督

圖二 課責之分類

另，依強制力之來源及程度，可將課責機制分為四類：法律課責、官僚課責、專業課責、政治課責（圖二）。達成策略上，除了透過政府內部組織結構與法規的調整達到法律課責以外，從外部公民及民意代表而來的監督，即政治課責，也相當重要。

（二） 從內部組織結構來實現課責

何謂從內部組織結構來實現課責？舉例而言，德國有所謂獨立管制機關(IRAs)的360 度課責，即該機關須面對不同利害關係人，從事解釋政策、接受審核申請，及進行獨立審查等工作，但通常其管制對象為私企業，管制對象為政府（亦即違法行為者是政府），則會有不同制度設計，例如在 1970 年代，德國就成立資料保護的專責機關(Data Protection Authorities, DPAs)，早期該機關擁有與州同等級之行政權力，並且完全獨立運作，此及內部組織結構的課責。然而，近年該機構納入聯邦政府組織中，就面臨若干問題，例如資料保護專員之聘任，有別於過去遴選方式，可能有缺乏民主正當性之疑慮，或預算不足、員額不足導致監督效率不佳，或難以處理現代資訊科技與法律規範外之新興議題等，因此就導入外部課責機制來解決，比如說納入新的參與者，如公民、民間團體、跨國網絡，並應投入更多預算及人力資源，且要定義更具體的工作內容（例如具體說明要保護什麼隱私）。

（三） 從外部公民社會來實現課責

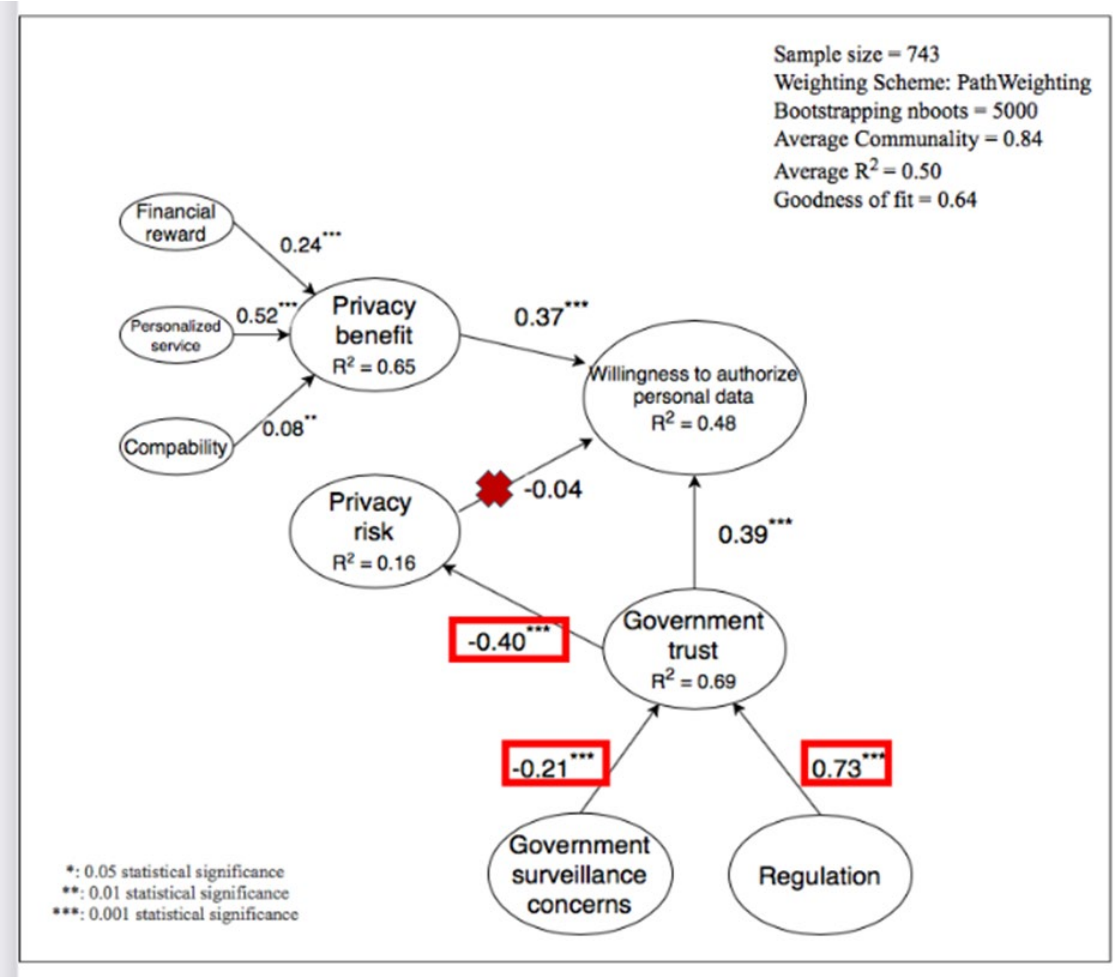
談到外部課責機制，在學理上也有幾種不同分類，包括「互動課責 (interactive accountability)」：有層次地整理政府資料、公開讓民眾得以理解，亦邀請政府官員及民眾參與座談會、聽證會等，例如紐約犯罪地圖的設置；「動態課責 (dynamic accountability)」:以開放政府資料系統做為基礎，建立動態的施政資料庫，讓公民自主針對政策績效來進行詢問跟課責，例如台北市「社會住宅戰情中心」；另外還有「公民提案課責 (citizen-initiated accountability)」，亦即由公民自主提出問題、建議與解決方法，公民不僅要求政府負責，自己也在處理社會問題上扮演主要角色，比如國發會今年開始的 JOIN 平台，就是屬於此類。

（四） 課責與智慧政府的建構：以 eID 為例

目前建構智慧政府的過程中，尤其在目前 eID 的政策推行上，似乎就面臨到上述數位轉型的障礙，「課責」則可作為用以克服此障礙的一種隱私風險管理機制，也就是說，在課責關係中，民眾可以要求被課責者提供對於以下事項之解釋，包含事前如何蒐集資料？事中如何運用資料？事後如何救濟？如果民眾感受不到管理機制時，會有三種不合

作行為，比如保留資料（拒絕提供個人資料或拒絕使用服務）、保護資料（使用某些工具以保護自身隱私），或者甚至偽造資料（提供錯誤的個人資料）。若民眾不願意透過 eID 來提供個人資料，則需要採取策略以提高民眾的信任度，策略包含上述「內部法規的修正——內部課責」以及「外部公民個人資料自主管理機制——外部課責」。

而關於政府內部管制與法規修正—內部課責—的功能及效果，今年二月我們委託政治大學選舉研究中心線上調查實驗室(Pollcracy Lab)進行調查，恰可作為一個例子。該調查的目的是要了解：什麼樣的因素會影響民眾授權個人資料之意願。實驗室總共回收了 743 份問卷，其分析結果是，民眾在考慮是否授權政府利用其資料的時候，最重要之考量因素是對政府的信任度，其次是個人利益，而個人隱私風險，似不在考量範圍之內。換言之，隱私風險考量對民眾資料授權意願影響不顯著，此結果事實上相當令人憂心，本文會針對這點提出建議，容後詳述。而從圖三中可見，民眾對於政府管制的感知，會影響其對於政府的信任程度，也間接影響個人授權隱私資料之意願。因此，若政府之行政作為有監控人民之疑慮，依常理而言，當然將降低人民對政府之信任。



圖三 民眾授權隱私資訊的考量

另外，引入外部課責之監督機制，策略上亦可參考愛沙尼亞 "Data-tracker" 作法，公民可以查詢哪些政府機關單位曾經要求存取過自己的個人資料，追蹤政府機構的數位足跡，其追蹤範圍涵蓋愛沙尼亞四個主要的政府資料庫，包含：就業登記、健康資訊、人口登記及健保基金資料庫等。過去我也曾給國發會建議，希望參考此機制，提昇政府使用人民資料的透明度，進而提昇公民對於政府機構之信任。

四、 討論與建議

以下為本文針對智慧政府數位轉型過程中的幾點建議：

（一） 提高公民的隱私風險意識與自主管理能力

從上述量化研究的結果可以看到，公民對於隱私風險的關切程度，低於對於政府信任及個人利益之關切，因此，應該增強公民（也包含公部門內部）隱私風險之意識，比如在實施身分證換發之前，應有一定期間之宣傳期。而台灣針對所謂嫌惡措施，比如核電廠，為避免事故造成危害，會舉行核安演習，那麼資訊外洩可能造成相當大的災難，政府內部也可以比照核安演習的模式，舉行資安演習。

另外，應強化公民隱私的自主管理能力。除愛沙尼亞的 "Data-tracker"機制外，建議針對不同族群制定客製化之隱私管理機制，例如針對病人或資訊素養較弱之數位弱勢族群，透過「資訊代理人」之制度，為其管理資料；又，政府透過 New eID 存取個人資料時，應主動通知。目前當其他網路或電子服務商存取個人 Google 帳號時，對於個資主體都會有所通知，那麼未來這應該可以是一個政府的著力點。

（二） 重視外部與內部之課責機制

強化內部課責機制，應針對 New eID 之授權，制定專門法規，明定公民在 New eID 使用上隱私問題之救濟及課責程序，並且設立專責機構行使獨立審查權、使其有法定行政預算，設立其具體績效指標。專責機構則可以由政府機關、國內 CSOs (Civil society organizations)、跨國機構等共同組成。外部課責機制，則可以參考愛沙尼亞的作法，將 eID 系統程式碼公布在開源軟體程式程式碼平臺，促進公眾監督，或引入瑞士對其 i-Voting 系統白帽駭客 (ethical hacker)的作法，甚至提供獎金，讓公眾來測試這個系統的安全性，爭取民眾的信任。

（三） 常任文官正向課責之可能

最後一項建議是「常任文官之正向課責」。傳統談課責機制，大多從「懲罰究責」的角度出發，是「有功無賞，打破要賠」，然而設立「正向課責」機制，除打破要處罰外，應讓有功者有賞，且針對做得好的機關單位，實施所謂標竿學習制度，讓好的案例及作法在整體政府機關中發揮影響力，如此整體政府服務及施政才能有正向循環。

邁向可課責的智慧政府

何建明

中央研究院資訊科學研究所　研究員

一、　政府數位化政策及計畫

近年我國政府各機關，包含行政院層級、部會層級（例如國家發展委員會），皆制定並推行相當多政府數位化之計畫，包含「數位國家創新經濟發展方案」、「智慧政府推動策略計畫」、「政府數位服務指引」、「智慧政府基礎建設」等。首先，以期程 2017 至 2025 的行政院科技會報數位國家組「數位國家創新經濟發展方案」為例，其目標為打造民眾有感之開放數位政府，實施智慧治理、保障數位人權、城鄉平衡發展、數位創新經濟等計畫方案，藉以提昇數位經濟價值。該計畫中也包含各部會分工、跨部會整合之相關策略及措施。再者，在國發會的智慧政府推動策略計畫中，說明「智慧政府」之概念，泛指各類改善政府對民眾、企業的服務作為，強調政府以「資料」為骨幹，應用物聯網與區塊鏈等創新科技，串聯政府服務與民眾需求，結合人工智慧雲端運算，以優化決策品質，其推動策略包含「促進公民參與及社會創新」、「資料輸入一次到處可用」等，原則上可見其中有相當好的善意設計和資訊揭露，也有部分仍有改進空間。另外，國發會也制定了「政府數位服務指引」，提供各級政府如何做好數位化工程之指引，一再提醒應確實了解使用者需求、規劃多元服務管道、確保資安隱私、以開放為優先，並遵循易用性原則等。對政府而言，new eID 跟 T-Road 是以上數位政府計畫中之基礎建設，而下一步，為因應政府或產業的數位轉型，政府亦規劃要成立一個名為「數位發展」的新部會，將由其負責資訊、資安、電信、網路跟傳播，並可能整併 NCC、科技會報辦公室、資安處、科技部，還有國發會，這將會是相當龐雜的政府組織改造工程。

二、　推行「智慧政府」之前提條件

在推動上述數位政府計畫之前，應先回答一個前提問題，亦即「台灣社會是否已經做好轉型的準備？」進一步可以劃分為三個問題：第一，政府跟民眾是否具備智慧政府所應有的資訊隱私跟資訊安全文化？第二，數位智慧政府是否真正屬於民眾所需要的？

第三，數位政府可課責性是否存在？

三、 「資訊隱私／資訊安全」文化

目前台灣民眾對於資料利用或資訊隱私保護的認知，都還不夠充分。因身分證現實用途非常廣泛，從出入機關或大樓時換取出入或停車證（如昨日研討會第一場次報告人林煜騰律師所述），以至於申請信用卡、向政府機關申辦各種手續等，甚至是將身分證交給他人影印留存。殊不知身分證（尤其是背面）有許多隱私資訊，實不宜任意交由他人影印，最起碼應註記限制其用途。也就是說，民眾普遍缺乏身分證使用風險意識、缺乏身分被盜用的憂患意識。

另外，民眾經常使用個人資料作為密碼，人民申辦自然人憑證的預設密碼，也是個人生日日期數字；而資訊學界廣為人知的「彩虹表」（Rainbow table），使個人密碼得以輕易被比對出來。故而，現實是，並非多數人所認知的，有密碼保護，資料就安全。而且，究竟除資訊專業菁英外，有多少人懂得如何設定真正有效且強度足夠的密碼？民眾對於紙本身分證的使用習慣、密碼設定方法等，使得個人資料可能很輕易地被存取或竊取，由此來看內政部規劃推動之 New eID，其中將存入民眾個人 300dpi 跟 600dpi 數位照片以及其他種類繁多之個資，相當不利於人民的資訊隱私保護。

（一） 民眾真的需要數位智慧政府嗎？政府可以保護人民隱私嗎？

進一步講，身分證的制度目的，依戶籍法之規定，係供戶政管理之用，而 New eID 依內政部規劃要載存如此繁多的個人資料，是否果真僅供法定目的之用？若是，則戶政單位早已存有人民個資，eID 中再存放人民個資的必要性，就更是有待商榷；若並非僅供法定目的之用，則 New eID 政策的推行，就逾越了法定目的，且可合理推測是為便利各方蒐集個資和數位足跡而為之。

那麼，行政院核定推行 New eID 政策後，人民只能自救嗎？昨日研討會第二場次中，面對「身為數位政委能否為保護人民隱私盡些力量」這個問題，唐鳳政委也僅能建議：應透過規範型塑（norm shaping）來教育人民如何避免各方蒐集個資與數位足跡，包含避免任意提供身分證背面影本，或未來不要開啟 eID 的自然人憑證功能，eID 與自然人憑證應分別持有，避免兩卡合一。

（二） 政府可課責性何在？

以最近 59 萬筆文官個資外洩、2000 萬筆戶政個資外洩事件為例，當面對大規模個

資侵害發生時，政府似乎缺乏積極作為。甚且，反而是政府在 Covid-19 疫情期間，大規模徵用個資，無論是民眾領取口罩、紙本振興券等，皆利用健保卡為之，此類健保卡的利用早已超越原始使用目的範圍，並委託超商作為發放或執行其他政策的中介角色，卻並未針對超商蒐集個資的各種行為發布具體行為規範。在國家因公衛緊急情事而須以公共利益為重時，全民都同意並能體諒，政府必須採行若干可能有侵害人權之虞的緊急措施或政策，但嗣後應針對法律制度或結構不足之處有所檢討。

台灣，並非中國。中國有社會信用評等制度，人民難以主張其隱私保障，然而在台灣，因過去曾經歷極權統治時代，我們都曾被長輩告誡不可隨意發表言論、以臺語說就是「囡仔人有耳無喙」那樣的時代，如今台灣社會的民主化得來不易，我們應避免再度落入那樣高度極權的社會。而政府若掌握愈多人民個資，愈容易遂行其統治意志，香港這一年來的境況，正是台灣的警惕與借鏡。

四、　智慧政府應具備之具體特徵及措施

（一） 落實資安風險管理，建立究責機制

既然唐鳳政委只能給出「人民應自行避免個資被取用」這樣的建議，更是彰顯政府可課責性之重要，而具體作法之一就是「智慧政府必須落實資安風險管理」，且重點是須「保護個人隱私權益」。

首先，政府應建立「防火牆」。目前因受限於各級政府機關資訊人員員額或技術之不足，許多政府的資訊軟體工程皆採招標委外為之，就應強化其中的資安管理，例如：不能僅依賴外部資安防護團隊及外部防火牆、敏感軟體不可下載至個人電腦、儲存國民敏感資料之資訊系統，應做好計畫開發專案管理等，包括導入專案工作分解管理架構表（Work Breakdown Structure, WBS），強化對委辦廠商及計畫之追蹤。防火牆建立後，當曾承辦政府委辦案件之台灣民間業者要往國外拓展業務，就無須懷疑這些廠商是不是帶著攸關國家安全的人民個資、國安機密等到國外而有所疑慮。再者，應設置資訊技術委員會，責成資訊技術委員會負責委外軟體資訊系統開發的技術審查，尤其是政府敏感軟體平台，包含戶役政、健保、財稅資料庫的資訊系統、台灣地形、地物、氣象相關之資料庫資訊系統之技術審查；廠商資安、開發人員，也應聘用本國人；另外，附帶一提，政府委外招標案所取得之智慧財產權，也應明定政府為智財權人，並建立機制妥為管理，不應發生有廠商成為智財權人之情形。最後，建立究責機制。前已述及，過去我國發生重大資安事件、民眾隱私權益被破壞，事實上看不到政府負起責任，也未見相關罰則，究責機制必須建立，才能真正得到民眾信任。

（二） 以增進民眾權利（empowerment）為導向

智慧政府應以增進民眾權利（empowerment）為導向，除訂定罰則主動維護民眾隱私權益外，政府智慧服務的提供，應有明確的用途、需求、規格，不應做目的外利用；另外，應有「多重身分的服務分級分流」，細節部份請參照我的簡報檔。而政府目前在推動的 T-Road 計畫，當然也同樣必須是以增進民眾權利為導向，在昨日第三場研討會中也有詳細的討論，例如個人是否有權拒絕或關閉資料在 T-Road 流通？個人有權拒絕資料再授權第三方分析或利用嗎？當人民個資在 T-Road 上傳送時，是否有管理的權限？

（三） 厚植社會信任，建立可信賴的智慧政府

智慧政府課責機制建立，才有可能厚植社會信任。前提也就是前幾場報告人都曾提過的，政府政策的制度設計，須公平、公正、公開，權責對等、自由選擇、法律保障、風險管理、課責及損害修復，且訊息要雙向透明——不是老百姓透明，更重要的是政府要透明。另外，政府需用資料最小化、政府數位足跡應透明，也就是民眾應可查詢機關使用其個資之紀錄。又，在政府掌有人民巨量個資、而資安能力不足的現實下，必須對於重大資安事件有因應能力及策略，建立風險管控與損害填補機制；政府委外營運須有適當規範，政府也應設立個資專責機構。

同時，人民對於政府的信賴，也建立在優良的政府決策品質上，因此必須有防免政府濫權的制度設計。因為決策層級愈高，事實上對於技術細節愈不清楚，而易於舉著公共利益大旗而便宜行事，則人民權益的把關，難道僅能憑藉政府官員的口頭承諾？因此，若政府決策錯誤，制度設計上一定要有補償措施，則勢必進行法規及組織調整，也必須有相當程度的社會溝通。

五、 智慧政府是政府的再造工程

更進一步說，建立可信賴的智慧政府，是政府的再造工程，進行上述的法規及組織調整，以及社會溝通時，應以「服務」作為核心價值，避免技術至上主義，且觀念必須改變：「資料屬於人民，而非屬於政府」，行政流程亦必須隨之調整，跨部會、跨部門的整合分工與合作，亦須找出共識；同時，政府資訊必須公開、強化民眾公共事務之參與、信賴及監督。

不過，究竟應由誰著手訂定這一整套智慧政府規範？昨天王大為老師的報告中提到，規則照舊將窒礙難行，責任歸屬不釐清亦很難完成目標，王老師提出了「TW-WAY」概念，即 TrustWorthy-Way，大家應共同找出能夠被信賴的作法，往這個方向來推動我們

的智慧政府。

智慧政府的承諾：數位轉型與政府可課責性

陳舜伶

中央研究院法律學研究所　副研究員

今天要談的是「『智慧政府』與政府的可課責性」這樣一個很大的題目，除了 eID 跟 T-Road 之外，智慧政府所涵蓋的範圍更廣，也是更長遠的規劃。即便是政府認為箭在弦上、甚至都已經發包動工的 eID 跟 T-Road，都還有很多規劃與設計還沒有確定，智慧政府則是更為遠程的工作，也還沒有具體詳細的規劃或內容，因此目前就只從現有可得的官方資料，提出一些觀察跟想法，跟大家討論。

一、　智慧政府運用資通技術優化決策的問題與隱憂

依照國發會 2019 年 7 月的智慧政府行動方案核定版，智慧政府希望達到的目標是「運用新進資訊與通信技術、提高施政效率效能與便利服務」，這些目標確實都很好，誰會不想要效率效能與便利、開放治理、更好的政府決策呢？但重點是如何做、做得到嗎？而且就算有這些好處，相對應的代價或風險是什麼？這些好處就足以作為非做不可的理由嗎？國內外政府在推動數位政府時經常提到要照顧不同族群，但所舉的例子常常都是數位落差，也就是要注意老年人、對上網、辦理線上服務比較不熟悉的群體的需求，從這些國內外的資料中會感覺到智慧政府這麼好，只要不是使用這些工具或服務有困難，似乎大家都應該接受這種趨勢與發展，甚至有些規範性要求的意味。然而，從這兩天來的討論我們知道，智慧政府所謂的「以資料為骨幹」、以及過程中所應用的資訊通信技術，牽涉很多隱私與安全的議題，也有很多疑慮沒有解決，在場事實上有很多人是資訊工具使用上沒有困難，而是因為各種風險、疑慮、價值觀與基本權主張的理由而不願意使用晶片身分證、不願意上 T-Road 這條路。這個族群也不小，這場研討會議題這麼硬但兩天現場都這麼多人，應該也不是疫情鬆綁後報復性報名研討會的結果，因此，智慧政府的規劃也請一定要照顧這個族群的需求。

另一方面，資訊通信技術是否一定能帶來效率效能與便利，其實也無法保證。

舉例而言，資訊系統可能增加行政效率，但某些服務流程、行政程序中承辦人原本可能有一些專業或個案判斷的空間，系統化之後這種彈性空間可能就被壓縮、甚至消失；且一旦系統建置之後，尤其是大型的系統，如果因為情事變更或法律變更而有修改、調整之必要，也可能因為成本的考量而無法及時、全面地處理，反而導致行政僵化；又，如果利用自動化系統來協助判斷申請福利給付是否符合資格、或者政府為了優化決策做出一套系統來跑大量資料，如果申請人對於結果有所疑問，承辦人可能會主張這是電腦運算的結果所以堅持沒問題，加上系統設計或資料的使用不夠透明或不容易了解，讓這些系統的決策更難被挑戰。比如說，最近因應防疫而實施的電子圍籬措施，其實就出了包，民眾分明就待在隔離處所並未離開，但系統會做出相反的判斷，認定民眾離開隔離處所，導致派出所警察一天到晚找上門來，民眾不堪其擾而反應給政府之後，1922 市警局或基地台業者，也無法處理及解決系統的問題。

再者，資訊通信技術也不保證能優化政府決策。因為，一旦系統建置完成而被採用後，行政跟管制機關受限於系統的規劃跟設計，原本沒有考慮到的資訊或分類方式等，未來就很難被考慮進去；而資料驅動(data driven)的決策模式，運用大量資料分析，是否一定得以優化決策、資料品質如何、資料怎麼被使用等等，這些內部過程都很難被大眾檢視，且當系統發生錯誤，或既有偏見被內建在系統設計中所造成的決策偏誤，都可能更難被發現，進一步講，若人民要挑戰行政機關的決定，過去只要具備法律知識即可，但如今若想要挑戰的是系統決策偏誤，須兼具對於法律及資訊系統的了解，對人民而言門檻非常高。

二、 政府數位轉型的法治思考

面對政府數位轉型，既有以上所述之疑慮及隱憂，就應該從法治面來思考。首先應釐清，數位轉型不只是技術工具的選擇或轉換而已，如果沒有訂定專法，可能會有法律零碎化的問題。國外也有學者在談政府數位轉型時提出，運用資訊系統來協助各種決定之作成，必須先把法令的授權事項轉譯成電腦能執行的指令，在針對個別情況作出判斷時，原本行政機關的裁量空間必須轉成資訊系統可以操作的精準規範，也因此有一種「類似立法(quasi-legislation)」的效果。要解決此問題的一種做法是提高立法技術，讓立法更精確，但可能很難，而且若規範訂得太細，未來修正成本也高；另一種則是要求系統有清楚易懂的文件說明，並將這些文件說明視為是類似行政機關的法規命令。而退萬步而言，假設行政機關認為數位轉型真的只是技術工具的選擇而已，那麼至少這些資訊技術的規劃也應該遵守法治的價值並且滿足法律的要求，包括紀錄並提供滿足個人依法主張權利所需之

全部資訊。

以 eID 與 T-Road 政策為例，這兩天幾位報告人已解釋過，並非單純技術選擇或變更的問題。那麼台灣既有的法律規範——數位簽章法、個人資料保護法、資通安全管理法——足夠嗎？行政部門認為已經足夠，因此毋須另訂專法，或認為就算不夠也不代表政府機關不能先推動這些政策。法律規範不充分，那麼，技術的規劃與設計能滿足現在法規要求嗎？亦是不能。何以可知？昨天第三場次有討論到，T-Road 對於跨機關的資料介接，只記錄交換次數而沒有記錄利用資料的目的、範圍、時間等，依照個資法，個人有獲知這些資訊的權利，但因系統沒有記錄，個人就沒有辦法知道其他機關持有哪些個人資料、當然也就無從行使請求機關停止蒐集、利用、處理個資的相關權利。在無法滿足目前法規要求的情形下，技術的規劃與設計能否滿足未來法規要求？此處所指的未來並非遙遠的未來，昨天提到個資專責機關的設立是國發會近期修法重點，最快下個會期立法院就會開始相關審議程序，個資專責機構之執掌跟 T-Road 所要建設的「資料串連與互通的數位環境」直接相關，但在個資專責機構尚未立法設置、尚未有明確的組織架構與職掌規範之際，T-Road 專案卻已經發包出去，如果個資專責事務與 T-Road 皆在同一個部會（國發會）職權範圍內，且可以預期近期會有如此重大的法規變動，為什麼這麼急著發包由外部廠商來制定 T-Road 的管理規則，而非由職權機關來制定？這個系統個資外洩的補救措施跟責任歸屬，目前也沒有看到充分的討論及相關的規劃。因此，政府數位轉型所應具備的法制規範，事實上仍尚未完備。

三、　國發會「智慧政府行動方案」中三項目標策略之檢討

以上談了政府數位轉型過程中可能有的疑慮及法治思考，接下來想要更為具體地檢視國發會「智慧政府行動方案」中三項目標策略，並提出一些想法及提供討論方向。

（一）「資料輸入一次到處可用」

首先是「資料輸入一次到處可用」，一般而言稱為「一次性原則」(The Once-Only Principle)，此原則常被認為是數位政府的指標措施，不過事實上其為歐盟單一數位市場的一環，是為便利歐盟會員國之間共同市場中資料的跨境交換、減少文件傳遞的障礙及不便而設，因此也是實現歐盟公民遷徙自由的一個途徑。目前各國實施的情形不一，法規用語也不太一樣（目前僅能參考英文資料，因此在討論不同國家時，跟原文相較之下可能會有些落差），例如有些國家直接規定政府

跟人民要資料僅能要一次，亦有規定政府要求人民資料前，必須先行在政府其他資料庫中搜尋是否已經持有該資料，甚至也有將此原則定性為人民之權利者，亦即人民有主張僅須提供一次資料給政府的權利。

我國目前關於一次性原則的規劃及適用，僅提及健康存摺及 MyData，未來實際上會如何實施，並未詳盡說明；又，我國沒有歐盟單一市場及跨境移動之需求，採用此原則的必要性為何？另外，歐盟針對一次性原則的實作方向也有兩種不同的討論，其一是以機關為中心，要求個人在不同平台、資料庫使用同一或者容易連結的身份識別方式，這雖然對於機關來說很方便、可以增加服務效率，但對個人來說隱私風險較高；另一種則是以公民為中心，允許個人在不同平台或資料庫使用不同（甚至是假名）且互相之間不容易連結的身份識別方式，這樣一來雖然對服務提供者而言成本較高，但對於公民來說隱私風險相對較低。

從智慧政府行動方案中關於健康存摺、MyData、eID 等政策的規劃設計來看，即使 eID 與自然人憑證並非強制結合、可以是兩張卡分別持有，目前所採取的仍是比較偏向 Government-centric 的取徑。但目前各界、包含昨天的報告中也一直有提到是否可以往多憑證、多重身分的方向走，希望相關部會能積極回應這樣的需求。

最後要強調的是，雖然有些國家在文字上把一次性原則是寫成一種權利，但這只是一個便民、表示不能過度侵擾公民的權利，該原則的具體內容，各國在實踐上其實也尚無定論，其雖預設所蒐集到的資料可能得以直接提供目的外利用，但這不應作為建置超級資料庫的藉口，隱私權的基本權保障仍然應該優先，這也是為什麼歐盟一次性原則仍受 GDPR 的規範，而在我國既有的法規架構下，資料的目的外利用當然亦須遵守個資法。剛剛在討論 T-Road 時也已經提到過，技術設計上，對於蒐集目的外的使用，如資料存取的範圍、理由、時間、次數等資訊都應有紀錄，才能滿足個資主體有效行使個資法上權利的需求。

（二）「以資料導向的運算及分析優化施政決策品質」

第二要談的策略是「以資料導向的運算及分析優化施政決策品質」，國發會智慧政府行動方案中有提及統計法 2018 年修法重點：「各部會在兼顧個資保護原則下，串接連結運用公務統計資料，優化施政決策。各級機關應善用政府業務資料、民間巨量資料，結合人工智慧等創新科技……透過數據分析，提供決策作為之參據」，據此，可知智慧政府要利用新興資訊科技、甚至是 AI 來優化施政決策品質，但，如報告一開始所提及的將有若干疑慮及隱憂，因此在此提出以下幾個

重點，以作為提醒、提供參考。

首先，關於過去已經有相當多討論的個資保護專責機關，其組織編制與權責設計、以及其裁罰權能，應能有效監督各部會之資料串接決定與個資保護措施。

另外是涉及資料倫理(Data Ethics)的問題，也就是，政府目前仍欠缺適當的資料治理機制，包括：「政府據以做出決策之資料，其品質控管」、「究竟需要／實際取得多少以及哪些資料」、「是否因應不同決策內容而有不同資料類型的需求」等，因資料運用將影響系統判斷的結果，對以上各該事項及相關規範，都應有更完整的資料治理機制與規劃。這個治理機制可能是設置機關內部或跨機關的資料治理委員會、或設置機關資料主管（chief data officer），另外也需要思考一定層級以上文官的資料素養（data literacy）問題，如果該文官職掌將需要經手資料系統、或透過資料的審核或利用來做政策判斷，應要求其有一定程度的資料素養，例如至少資料有明顯錯誤時能及時發現及反應，而非仍舊把錯誤資料直接輸入系統。

（三）「促進公民參與與社會創新」

最後要提的策略是「促進公民參與與社會創新」，政府推動數位轉型，如果只是把原有的一套運作模式建置在系統中，可能反而透過這套系統強化了原本的治理邏輯，因此，轉型過程中的「公民參與及社會創新」當然重要，也因此會強調政府之「透明性」及「可課責性」，而近年政府也極力以「開放資料」為促進政府透明性之手段。然而，開放資料的實施，如果只是政府有什麼就丟什麼出來，或選擇性地丟出來，也不能保證政府的透明與可課責性。所以，針對公民參與與開放資料這一點，我認為，應將「可課責性之要求」，理解為一種促進「政府組織學習」（institutional learning）的動機與方式。可課責性會促使傾向封閉的行政體系向外界開放、積極回應外界需求，促成行政體系去檢討原始政策目標與承諾、以及其在執行過程中的各種選擇與措施。開放資料與促進公民參與這個目標也可以提供政府新的刺激、作法與思考方向，促進行政體系的組織學習與進化，我認為是相當好的方向。這個場次的與談人高嘉良先生和 g0v 社群近年來經常性地透過各種方式與政府互動，也是希望從社群、數位世代的角度、秉持開源社群的精神，一方面協助公民重新思考政府的角色，另一方面，從小到開放資料格式、大到透過 vTaiwan.tw 或 pol.is 平台來整合公共議題的不同意見，也讓政府用不同的角度重新思考問題或解決問題的方法，有不錯的成果。

因此，很高興看到智慧政府推動策略計畫中，要求各部會應抱持開放的態度，在決策過程中，引進群眾共同協作力量及集體智慧，以貼近民意與增加透明互信，

也希望未來在更細部的規劃時，能落實資料治理與審議空間的開放，以促進政府自身的進化。

四、 總結與建議

最後，對於政府數位轉型的推進，提出幾點總結建議：首先，描繪智慧政府的願景的同時，須討論可能的弊端、風險、如何課責、及如何落實權利之行使；第二，隱私保護與資料治理等核心議題上，組織與法規仍有完善空間。未來將要設置的個資保護專責機關，層級必須夠高，才能有效監管政府各機關之間的資料交換；第三，技術其實並非中性，價值與原則的討論與可課責性的規劃應優先於技術的設計與採用，並且，技術工具之設計必須符合法規要求，包括必須能提供個人行使權利所必要之系統紀錄。而「資料輸入一次到處可用」原則之適用，亦不能凌駕於個資法之上；最後，重申一點：開放資料不只是在促進資料利用，從可課責性可促進政府組織學習的角度，期待未來智慧政府能落實資料治理與審議空間的開放，以確保人民權利不受侵害、又能實現便民之目的，成為真正「可課責的智慧政府」。

附件二

政府單位說明

鄭信偉（內政部戶政司副司長）

李所長、邱老師，李老師，吳老師，兩位知名的大律師，還有各位關心 New eID 的好朋友，大家好。今天我很榮幸，受內政部指派我來跟大家簡要的說明，有關於 New eID 大家可能仍有疑問或者是可能不是那麼清楚的地方。我必須很誠摯的講，剛才三位老師對於 New eID 的研究都非常的深入，他們也非常的關心這個案子，所以說做了很深入的研究。他們的資料，是從我們戶政司網站拿到的一些資訊。不過，我這裡先跟大家報告，戶政司網站上的資料，是我們對於 New eID 的初步規劃。當初將規劃 po 上網後，外面就有一些建議的聲音，建議有關資訊的東西要加強，有些什麼要再在提升，要做一些改變。所以，我們現在刻正進行 eID 細部規劃的調整修正。等到這些修正完成後，我們會有更新、更好的細部規劃再公開出來。就像剛才第一位報告人邱老師那邊有提到的一張圖表，那張圖表裡頭有分成好幾個區，看起來在加密區部要輸入密碼，但是其他區好像不用。但是，我跟各位報告，在那個公開區的部分，也是要輸入讀取碼，就是證件編號的後 6 碼才可讀取。但是要怎麼輸呢，用 key 的或用掃的都可以，並不是說什麼都不要就可以看得到公開區裡面的資料內容。這個部分，我們還是有加設一層所謂的個資保護的工作。

然後，我現在先跟大家做一個簡要的報告，就現在大家似乎還有疑問的部分，跟大家做個說明。

有人認為 New eID 其實已經逸脫戶籍法上的授權，這個剛才邱老師也有提到。我們現在的身分證是第六版的國民身分證，大概是每十年左右換一次。如果把時間往前推，我們第一版的國民身分證是在民國 35 年。那時發國民身分證的目的是要使戶政機關可以確認國民的身分，還有國民彼此親屬間的關係。因此，到目前國民身分證欄位，有父母、配偶，還有一些相關的記載。國民身分證最主要的目的是要具有便攜性跟可識別性，雖然我們已經換發了 6 次，但國民身分證還是要必須要具備便攜性跟可識別性，這是我們一個最基本的原則。所以，剛剛有提到，我們的 New eID 有規劃把身分證版面的一些資料放到晶片裡頭，身分證本身的還是有做所謂可識別性跟便攜性的功能。所以說，基本上我們還是依循著戶籍法第 52 條的授權來做。

下面一個部分，就是剛剛提到的自然人憑證。我想大家一定很關心自然人憑證的議題，因為原本 New eID 的規劃就含有自然人憑證，如果不要用的話，可以把它關掉，但是我們現在要改了。目前的新規劃是，當個人在申請 New eID

時,即可選擇不要自然人憑證的卡片,這樣他就不會把自然人憑證功能寫進去了。申請 New eID 之後，如果有需要，你可以自己另外再去申請一張自然人憑證。但是，有人覺得把自然人憑證放進去 New eID 會比較好用，那可以選擇申請時就把憑證放進去，如果申請後決定不想用了，後續還可以再去廢止、停用憑證。所以，在自然人憑證這一塊，我們完全尊重各位，由民眾資訊自主。也就是說，我們已經再往前跨了一步，讓民眾申請時即可做選擇。

大家所一直關心的第三個部分則是,為什麼不制定專法？有關法律這個部分，剛才老師們都有提到，我們現在從戶籍法、電子簽章法、資通安全管理法、個人資料保護法等，已有相關的規範。因為這裡面也涉及到所謂的法制作業的問題，也就是說，當你有這些相關的法律規範的時候，有沒有需要再另立一個專法，再把那些規定放進專法的問題。然後剛才老師那邊都有提到，像德國、愛沙尼亞均有所謂的專法。然後，我們也有檢視過德國跟愛沙尼亞的法。德國的身分證跟電子識別法裡面的規範，在我們的戶籍法、國民身分證還有戶口名簿製發相片的影像檔管理辦法等等，都可以看到類似的規範。然後，愛沙尼亞身分證專法是把所有的證件都納入規範，不只規範身分證，裡面還有護照等所有證件全部都涵蓋在內，因此，我們也回過頭來檢視我們的護照條例、入出國移民法等，其實也都有相關的一些規定。因此，雖然這些國家有身分證專法，但是對我們來說，各國有其法制體系及法治的方式，第一點，就相關的事項已經有法律規範，如果我再去訂一個專法，就很可能造成疊床架屋的情形。第二點，我們的法如果沒有跳脫原來已經有的法，那將來那些法修正時，這一部專法是不是也要配合修，因為這也會涉及到法律適用的問題。而且現在已經適用個資法、資通安全管理法的事項，也都是這樣子處理，並沒有什麼疑慮。所以，我們的看法是說，我們這邊不會訂專法，但會在戶籍法授權的辦法裡，做一個比較詳細的規定。現在這個辦法，我們還在討論修正中。

下一部分為資料的議題，剛剛老師也有提到，我們對於 New eID 身分資料的取用有沒有限制？因為我們在沒有專法,這議題討論就會回歸到各個法律去看。也就是說，各個公私部門還是要受到個資法的規範。另外，有關身分證的應用紀錄會不會被串，別人可以看到這資料嗎？我們每個資料庫都是各自獨立的，中間是沒有辦法去串聯的。然後，大家也很關心個資保護的專責機構，因為個資法現在是國發會主管，國發會目前針對個資專責機構也有相關的研議，後面場次好像也有提到這部分，所以，我想這部分是不是留待國發會做更詳細的說明。然後，最後就是，大家很擔心的是政府會不會監控足跡的問題。在這裡跟各位報告，eID 的使用資料是不會回到內政部來，我們永遠看不到你是怎麼用 New eID。

然後，另外有人常常講說，為什麼要強制攜帶身分證?。我們回過頭來檢視現行法律，有很多條文都有規定應攜帶的東西，事實上只是一個訓示性規定。同樣的，戶籍法第 56 條有關攜帶國民身分證，也只是一個訓示性規定。你沒有帶，我也不會罰你。

再來可能就談到安全的部分，雖然大部分剛才老師那邊都已經提到，但是我這裡可能還是需要再說明一下。有關晶片的安全，我們規劃晶片必須要符合國際安全的認證，而且本身的卡體要防偽。卡片目前是在國內設計規劃的，我們也會加強製卡監督跟管理。然後，我們還有限定原料設備的供應來源，絕對不能從中國那邊來，這是一個最大、最基本的原則。

然後，大家可能也很關心晶片的規格問題，剛才老師也有提到。我們的晶片是高要求的晶片，其晶圓是由台積電來代工。然後，有關晶片的資安防護，有外部的五層防護，及內部的四層防護，對於委外廠商也有四層管制，都有一些作法。在安全檢測部分，我們也有規劃很多種作法，包含規劃明年試行時做一個賞金獵人的活動。至於，剛才李老師提到量子電腦的部分。隨著量子電腦的發展，其所衝擊的是所有密碼學相關的理論跟應用，不是只指單純的 New eID。然後，現行晶片的加密方式，並不會因為量子電腦的出現而停止加密。將來會有後量子密碼學的一些出現，重點是，我們憑證中心每年會做金鑰安全的性能評估，然後再依據評估的結果，做必要的因應跟處置。剛提到憑證金鑰，從 100 年起自然人憑證的金鑰長度，已經提昇到 2048 了，到目前為止，還是屬於安全的。

另外，剛才有提到有一個戶政外洩 2000 多萬筆那個，那個部分可能要說明，第一個，這個資料不會是內政部的系統出去的。因為內政部系統是個封閉型的系統，根本拿不出去。然後經過我們檢視，事實上資料裡面的格式是五花八門，跟我們的格式也不一樣。但是常常有些聲音說，這個資料是戶政司外洩，但我不曉得用意是什麼，是不是這樣會比較好賣錢還是怎麼樣子？對，我們是嚴正聲明說，這個資料絕對不是內政部流出去的，這些資料看起來可能是有人去蒐集了各式各樣的資訊，然後再把它拼湊起來的。

然後，剛才有提到身分證相片，提到所謂的人臉識別的部分。這邊要說的是，身分證的相片是做臨櫃辦理識別使用，因為我們在戶政這邊，往往有時會遇到有人換身分證，櫃台人員就有需要確認相片為本人，需要辨識這張身分證是不是假冒的，或者是用那種不正當的手段換取的。

最後，事實上我們在 New eID 的推動，在很早就已經有開始做了一些的規劃：在 105 年的國發會公共政策網路參與平台有廣徵民眾的一些構想；106 年又

辦了國際研討會，還有一些座談及工作坊等；然後，我們也成立了一個換發的工作小組，一直在研議相關的妥適性。然後，戶政司網站上也有 New eID 的資訊公開專區，現在專區的資料仍是先前的細部規劃，我們將會陸續更新資訊公開專區的資料。我們還是會持續跟民間團體、社會各界，還有各位關心 New eID 的朋友們持續溝通。要強化調整 New eID 的規劃，由大家集思廣益，從多方面來的想法，才能使 New eID 能夠做得更好。

因此我們推動 New eID 的態度一定要兼顧便利性、個人隱私，還有資安保障，這是最基本的原則，然後我們會依據相關法規跟程序來推動 New eID 的換發作業。然後，最後，我們會審慎來辦理這件事情。因此，我們現在規劃明年先選擇少部分縣市，採民眾自願（不是強制）免費申請 New eID。然後，在那段時間，會同時舉辦賞金獵人的活動。我們心裡是希望大家沒有辦法破我們的資安防護，賞金獵人這筆錢最後不會發出去。我們將來規劃 New eID 要符合所謂的國安的標準，也就是剛才有提到晶片的安全等級是軍事規格以上，也就是說 New eID 的晶片比現在的金融卡、信用卡，甚至於健保卡的晶片等級更高。然後再來，我們的系統部分，是由中華電信得標後建置。中華電信有自然人憑證、還有各方面資安的經驗。卡片部分，則由中央印製廠負責。中央印廠是印鈔票的，防偽技術的專業我想是不容懷疑的。所以，不論在卡片、系統、晶片部分等，都是希望能夠達到滿足大家對於資安的相關要求。因此，我們剛才也很同意老師所提到的，資安是沒有絕對的。因此，資安面我們一定會與時俱進，並持續精進相關的資安作為。

潘國才（國家發展委員會資訊管理處處長）

主持人、各位先進大家午安。我就接續剛剛柏堯先進所提到的，隱私是一件很重要但是一個長期性的問題來接續談下去。

我也非常非常非常認同（隱私是一件很重要的問題），我講三個非常就代表非常的重要，就非常的認同。但是也提到了一件事情，就是說，隱私的保護是長期性，而且我剛剛有注意聽到說，好像是很久以來都在注意，但是到目前沒有辦法完全解決的一個問題。那我就產生了另外一個疑問，既然現在都還沒有辦法完全解決，我們是不是要等到所有問題完全解決了之後我們才開始來做我們想要做的事情呢？這個好像也不是一個做事非常好的方法。那應該要什麼方式去做呢？我們是不是在現在已知可以控制風險的情況之下，來處理我們要做的事情。這個是我們的出發點，先跟各位報告。

我本來是想要跟各位報告 T-Road 是什麼東西，可是也謝謝前面許多的先進已經做了大概的說明，不過我還是針對這兩點大概先說一下。可能是我們以前說得並不是十分清楚，所以大家並不是非常了解我們要建 T-Road 是要做哪些事情。我簡單地歸納來講，就是兩件事情，一個是政府的線上服務要重新做整理，可能原來是比較片段性的服務，我們希望能夠去把它連結起來，也就是大家可能長期以來朗朗上口，所謂叫一站式的服務。那比較早期，所謂一站式的服務，可能因為政府機關的關係，是受限在同一個政府機關裡面的所謂一站式的服務，如果是跨機關的一站式服務就非常少，我們希望未來有這樣的機制能夠比較多，等一下我會再跟各位做一個實際上的說明。第二個部分就是剛剛幾位先進提到比較技術性的，我們希望建一個資料傳輸安全性較高的通道。

我們是希望有一個服務的改造，另外有一個安全性的通道。我也非常認同前面幾位先進有提到說，現在的管制是碎裂化的，是真的是這樣沒錯，但是這也是一個很大的議題，這個可能要怎麼樣來處理，還有待大家一起來討論。那有沒有管制呢？是有管制的。因為我有點咬文嚼字，我對於前面有先進，我忘了是哪一位，說資料是在 T-Road 上面自由傳輸，我對這個並不是十分認同。因為我對於自由這兩個字並不同意，它不是自由、任意地傳輸，它還是有它的規範。

我在這邊要跟各位報告的是說，我們希望針對線上的服務做重新的整理，MyData 剛剛已經講了蠻多了，它其實將來是希望透過所謂的以人為基礎（來設計整個線上服務）。我們先試辦以人為基礎的服務設計，大致把人生的階段分成五大階段。從出生、就學、就業，可能比較年長了之後到就養，然後終老。我們

希望透過這五大階段，把一些服務能夠串連起來。

所以我在這邊跟各位舉一個例子，如果是有勞工朋友、有生育的話，他的小孩要到戶政事務所去報戶口，報戶口是一件事情，但是他也可以同時申請勞保的生育補助，然後他又可以去申請小朋友的健保卡。這原來是在三個不同的機關，一個是在戶政，健保的話你要到健保機關去，勞保的生育補助你要去勞保局。可是透過所謂我剛剛跟各位報告的一站式的服務，我們希望民眾去報戶口的時候，這三件事情能夠同時完成。那怎麼樣同時完成呢？當然要靠資訊系統，資訊系統可以把一個你報的一份的資料去分別傳送到兩個不同的機關裡面。另外兩個不同的機關接到這樣的資料，就可以處理他們後續的事情。這件事情實際上已經發生了，所以如果各位有希望（生小孩），因為現在少子化，我們也是鼓勵生育。如果有這個機會的話，如果有小寶寶的話，要去報戶口的話，可以同時處理這樣的事情。

在網路上面，政府之間傳遞的有哪些東西呢？除了我剛剛舉例有跨機關的資料以外，還有一些是符合相關法規的。我在這邊大概唸一個辦法給大家聽，叫做《外國特定專業人才申請就業金卡許可辦法》，也就是外國人士如果來台灣要申請就業金卡的話，該辦法第二條規定，申請方式以網路傳輸的方式辦理。也就是申請人要在網路上把資料 key 進去，key 進去的資料很明顯的，這就是電子式的資料、數位式的資料。可是這個申請的辦法必須透過勞動部、外交部專業的審查，然後有些專業人士可能是屬於藝術、體育、教育或者是文化專門，所以這些資料還要經過科技部、文化部、教育部、經濟部等等，看他是屬於哪一類的專長。那麼請問，這樣子已經是電子式的資料，我要再把它送到科技部或者是再把它送到文化部，不可能再把它印成紙本去傳遞，一定是要透過一個資訊傳遞的管道去傳到文化部或者是傳到科技部來處理整件事情。這就是（為什麼）我們希望透過一個比較好的傳輸通道（來做）。

剛剛我有說我不同意 T-Road 上的資料傳輸叫做自由傳輸，是因為這些傳輸的資料都是有它傳輸的規定，我必須要 follow 這些規定才能在網路上面去傳遞這些資料。那我同意的是什麼呢？我同意的是，這些規定的確目前是所謂的破碎化的。但是有沒有可能做成一個完整的（法規）？用我剛剛舉的這些例子，譬如說我舉這個出生登記的例子，（規範）它所允許傳輸的內容的規則，跟外國人申請就業金卡的傳輸規則通通合起來，抽象性的立出一個位階更高的一個傳輸法規，其實（這件事）我也同意。可是要立這樣的法規，它可能還要一段時間，可是我們現在的業務已經在推動了，那我們是不是要在現行這些已經有辦法、已經有規範的條件之下，先讓這些的資料先可以在網路上面傳遞？這個是我們在建 T-Road

最主要的一個思維。

剛剛有幾位老師提到我們 MyData 的一些文字，或者是一些用語沒有十分精確，這個我是完全接受。可能我們未來要像那個菸品的包裝上面再加上一些的警語，但是這個是不是我們想……這有點笑話啦，好像都沒有人笑，算了。這裡所謂的不負保管責任，其實指的是說，我們有一個功能是說，你存放在政府的資料，譬如說，你的親屬關係。你的親屬關係其實目前是可以下載，你可以下載到你的 USB、下載到你的硬碟、下載到你的手機、下載到你想要指定的 device 上面都沒有問題，這是目前已經有的。所以我們這裡所說的不負保管責任的意思是指，這個資料已經下載到你指定的 device 上面去了之後，你不能要 MyData 這個平台還要去負責你未來拿到哪邊去用的這樣的一個責任。

所以我們在這邊，可能用的用語並不是十分恰當，或者是（不符合）法律上面的用語，應該要用其他的文字去做說明。在這裡跟各位報告的是，像這樣你已經下載到你自己的 device 上面去，也是我們 MyData 上面提供的功能，但是你下載後的這些資料安全性，真的就像前面柏堯老師說的，就是要安全自負。但是我們將來應該也不會去直接用這四個字啦，所以未來這個文字怎麼樣調整，我們再請相關的學者、法律專家再給我們指教。

我在這邊還是謝謝許多老師給我們的一些指正，我們相信這個未來推動資訊化、政府串連這些資料，在法規的允許之下，我再強調，在法規的允許之下，所串連的資料，應該是可以給（出去），且對大家應該是有幫助的。那因為時間的關係我先報告到這邊，也許等一下還可以有交流的機會，謝謝。

李世德（國家發展委員會參事）

謝謝主持人剛剛的開場。主持人林大法官、三位報告人、兩位與談人都是我們實務經驗跟學識涵養兼具的一時之選。今天也非常榮幸能跟各位以及我們現場的來賓，還有我們線上收看我們直播的觀眾，可以來探討一下數位足跡、剖繪與監控的議題。

去年，西班牙發生了一個令大家矚目的事件，那是歐盟在 GDPR 通過後第一個裁罰事件。這可能要先勾勒一下，這件事情跟足球有關，我們都知道世界盃足球賽四年舉辦一次，讓全世界都瘋狂的球賽。在西班牙代表隊裡，我們也常常聽到非常有名的足球明星的名字，像梅西、西羅等等。他們都是出身於西班牙足球甲級聯賽的隊伍裡面，俗稱西甲。足球比賽，在西班牙國內是他們生活中非常重要的一部份。

那西班牙西甲，為了要服務廣大的國內球迷，所以就開發了一款蠻好用的 app 讓球迷下載。在比賽轉播過程，同時開啟這個 app 還可以獲得很多現場的即時資訊，讓球迷可以一邊看廣播，一邊同時看 app 接收其他的資訊。講到這邊，大家可能覺得這也沒什麼，這很很正常的科技跟生活運用的情境，這個 app 非常受到大家的歡迎，下載次數已經超過一千多萬次。。但是在這邊卻躲藏了一個問題。

去年的六月，西班牙的個人資料保護機關，認定西甲聯盟的 app 非法擷取客戶手機裡的資訊，且資訊擷取過程，並未依循 GDPR 的規定來執行。認定違反 GDPR 並裁罰歐元 25 萬（大概相當於臺幣 850 萬元）。這金額看起來或許不大，但是卻受到大家的關注。西甲聯盟受罰的原因是，因為很多人透過盜版轉播現場看球賽，西甲聯盟一直想要抓盜版，因為要經官方授權的才可以轉播球賽，所以盜版一直是他們很頭痛的問題，於是他們就想到利用球迷下載 app 後，同時會透過 app 取得授權開啟手機的收音裝置。西甲聯盟在電視轉播的時候，會加上一段人類聽不到的特定音頻，這個音頻若被手機所開啟的麥克風收錄後，app 可以將聲音送到伺服器的後端進行比對，比對後若有這個音頻就表示這是正版，若沒有的話，這可能是一個違法播放的場地，例如：餐廳或酒吧。同時，球迷手機的 app 還會再提供位置資訊，西甲聯盟就拿位置資訊去做相關違法轉播的查緝。

在這樣的過程裡面，西甲聯盟犯了一個非常大的一個忌諱，雖然當初西甲聯盟跟西班牙個人資料保護專責機關宣稱，在下載 app 都有告知當事人將會開啟麥克風、會進行現場收音，還會取得位置資訊，並取得當事人同意，但西班牙個人

資料保護專責機關認為這個理由不充分，並認為球迷並不知道下載 app 後接下來要發生什麼事情，尤其是連接現場收錄聲音資訊、以及包含取用位置資訊是要拿去抓盜版這樣的事情。球迷在毫無所悉這些資料取用的過程就下載 app，那球迷手機所提供的資訊，就完全不是在球迷所了解的狀況之下被擷取，而且用在另外一個用途 - 就是要請球迷用手機幫忙監控其他酒吧或者餐廳業者有沒有違反轉播。這個事件到現在還沒定案，西甲聯盟也提出了相關的法律救濟，目前本案還在法院審議中，但也可能因為疫情的關係，審議的速度沒那麼快。

先不管最後法律的認定是如何，這件事件的本身，跟我們今天的主題 - 數位足跡跟剖繪、監控的議題，有一個非常微妙、值得觀察的關聯。

今天三位報告人所講的內容切入點雖然不同，但是都已經大概把我們今天這個議題所要涵蓋的幾個面向都帶進來了。邱老師代劉老師所報告的數位的足跡監控的法治規範的這些模式，從各個角度來看不同國家規範模式的剖析；莊老師對於含有持續識別碼的數位足跡，經歷剖繪跟大規模監控的互動架構，這邊有非常清晰的一個架構，可以讓我們大家可以來做很多討論的運用；蔡老師把利用數位足跡非常極端的對照組 - 中國的社會信用體系，建立的過程裡面跟社會治理的緊密結合的現象，做了充分的一個描述。

那我統合來講很核心的數位足跡，如同剛剛唐鳳政委所提到，數位足跡已經變成是一種建築材料，留存在各個地方。自從有網際網路之後，我覺得這已經沒辦法走回頭路，網際網路跟電信網路結合，加上行動裝置、互聯網的出現，整個電信的基礎建設從現在 5G 邁向未來的 6G 等等速度的提升，大概已經沒有辦法讓數位足跡不存在，所以，數位足跡的存在已經變成一個事實。現在反而要從一個反向的角度來思考，當初留下數位足跡的我們 - 每個自然人，都需要加強全民資安的一個重要素養，就是認識所謂的數位足跡。

那另外一塊就是從法制面來看待，各位報告人的報告內容，剛好可以顯示出一個討論的光譜，GDPR 目前現在在法制面光譜的右邊，那中國的所謂的社會信用系統體系，正好是在光譜的左邊。二者剛好是在這個光譜的兩邊的極端，那我們如何要在這個兩邊的極端裡面取找尋到個資保護跟合理利用的一個平衡點。那我覺得這份西班牙案例的討論結構，剛好可以提供給我們，從這樣的一個例證裡面，去找尋一個適合我們目前我國社會可以運用的一個法制制度的一個內涵。

高仙桂（國家發展委員會副主任委員）

主席、各位與會的先進大家午安，很榮幸能參加這一次的會議。首先是要感謝四位報告人對於我們智慧政府的推動提供了很多建設性的建議，接下來我會針對智慧政府推動的進程，還有大家關心的資安跟個資保護的相關議題來做說明。「智慧政府行動方案」是在去年五月提出來的，主要是因應 AI、IoT，以及 blockchain 等創新科技的發展，依行政院指示，必須推動政府的數位轉型，國發會進而提出這個方案。方案當中有三個重要的目標，第一，擴大政府資料的開放跟運用；第二、第三希望能運用新興科技去優化我們政府施政的品質，提供給民眾創新智慧的服務。總結來說，其實智慧政府最終的目的是希望打造「以人為本、透明課責的開放政府」。這些願景跟目標的達成，很重要的是，絕對要強化資安的保護與確保個人隱私的保護，若缺少這兩點，那麼一切都不用再說。因此，這兩套配套措施：「深化資安縱深防禦」、「落實監督隱私保護」，與其說是配套措施，不如說是智慧政府推動的兩大基石。

在擴大政府資料的開放與運用方面，大家都知道，資料是驅動數位經濟發展很重要的動能。其實國發會在過去幾年來一直在推動政府的開放資料，目前在資料開放平台裡面，約略共有四萬五千筆的開放資料，幾乎有 75%都是符合所謂開放格式的結構化資料，同時符合機器可讀的型態。大家也知道，我們昨天開始推動個人資料平台的試營運，我們希望在民眾的自主同意與資料安全取用之下，取得民眾個人資料的自主權。因為我們會覺得，資料的開放是推動透明課責中非常重要的過程。除了我們在推動開放資料外，大家也應該知道我們的「公共政策網路參與平台」，透過這個平台，民眾可以在上面提出政策相關的點子，政府在重大政策施行前也得以利用該平台徵詢民眾意見，並且透過平台來監督事後成效。大家也知道，今年會推動台灣第一個開放政府國家行動方案，基本上就是符合 OPG 開放透明的課責精神。

我想智慧政府推動有一個非常重要的事情呢，就是我們怎麼樣利用大數據，來優化政府的決策品質。所以我們可以知道，各部會他可以運用自己擁有的巨量資料，也就是大數據，或者結合學研界的力量，在國網中心的資料平台裡面，針對攸關民眾的相關課題，在決策的過程中，應用大數據來提出更好的決策，並做出有利民眾的政策，包括食安的問題、洗錢防制、學用落差與弱勢關懷。國發會最近也跟內政部與衛福部進行跨部會資料借接，解決獨居老人的安居問題。

另外一個層面就是，如何使用所謂的創新科技機制提供民眾更多的智慧服務。像是醫療方面，我們的 AI 醫療影像分析已經運用在各個大醫院；各個縣市政府推動所謂的智慧城市、智慧交通、智慧住宅等，其實都是用創新科技來提供給民眾的智慧服務。另外，我們也有用區塊鏈來記載校園團膳的食材履歷，也是應用數位科技來提供民眾智慧服務的很好的案例。

在這兩天會議中，大家非常關心的是關於 New eID 跟 T-Road 的議題，我們希望將來政府的服務可以線上申辦，在這邊強調，在數位平權的考量下，所有的服務絕對是有線上跟線下兩種服務可供選擇，民眾不會只有一種選擇。目前 T-Road 尚在建置中，預計將來是以提供人生事件為主軸的線上服務，包括出生、就學、就業、就養等面向。民眾在個人同意之前提下，可以在線上取得相關的服務。關於 MyData，在於落實個人資料的自主運用。政府各項服務的取得，通常涉及到保存在政府機關中的個人資料，在 MyData 平台試營運的階段當中，民眾可以在 MyData 平台裡面取得 31 項的所謂個人化的資料，然後經過數位身份辨識，並經個人同意授權以後提供給第三方使用。剛有提到，在數位政府資料輸入一次可用的部分，用詞方面確實有需要釐清，其實所謂一次性的原則，意謂民眾同意當次下載資料，只有一次使用的權限，沒有所謂永久授權的問題，這部分要跟大家澄清。

剛剛講到，不管我們的願景與目標為何，很重要的就是，一定要在這個資安維護的前提之下才可以達成。行政院已經公布了資通安全管理法，要求公務機關都一定要訂定資安的維護計劃與設置資訊長，並且要求定期的稽核與監管。國發會跟內政部都是屬於資安等級 A 級的機關，所有資訊系統都是一定要透過 ISO 27001 資訊安全管理體系認證。

接下來說明大家很關心的 T-Road 傳輸管道的資安安全性。在 T-Road 的入口網中，如果民眾要取得政府相關服務，一定要先經過數位身份辨識，而且會取得當事人明確的同意。入口網會記錄所有服務使用的足跡供當事人來查驗，包括：有誰使用你的入口網、查詢資料有哪些。T-Road 入口網的身份辨識，不是只有 NEW eID 一個身分辨識機制，是採多元身分辨識的方式。至於為什麼國發會要在 GSN 上面建立 T-Road，主要係政府必須確保民眾接取服務的時候，是經由一個更安全且更可信賴的資料傳輸通道。在 T-Road 運作過程中，本會會要求各機關資料中心跟 T-Road 之介接，一定要有一次性資料傳輸的標準格式，還有符合安全標準，並且我們是採去中心化的網路架構、點對點的鏈接。第三，我們有開放程式供各界查詢或滿足安全的需要、驗證。

另外大家關心到資料交換，所有資料的提供機關，都會審核取用機關資料取得的權限，也就是一定要符合個資法的相關規定。再一次重申，其實政府數位服務中，蒐集、處理、利用個資，都要符合個資法的規定，也就是說，跨部會資料交換的時候，一定會檢視資料索取機關是否依法定職掌必要範圍蒐集個資，且在目的內利用，或是經當事人同意，方得為之。我們現在 MyData 的機制當中，你要跨機關、拿到兩個機關的資料的時候，就是分別由當事人同意下載給當事人。也有人關心，台灣個資法跟 GDPR 到底有什麼樣的差距？台灣個資法其實都是參考 GDPR 的前身——Directive 95/46/EC 的標準，兩者有很多相似的地方。不可諱言，GDPR 是近年來歐盟因應數位科技快速推展，提出的新法令，不過 GDPR 施行至今才兩年多，其具體成效還沒有被檢驗。我們目前刻正向歐盟申請國家適足性的認定，因此關於個資法要如何相應地進行修正，國發會亦已召開了幾場會議。最後，感謝大家對於智慧政府的指正，各位的批評就是政府進步的動能，謝謝。

林敏聰（科技部政務次長）

各位午安，我想從何建明研究員所提到的王大為老師說要建立一個對政府信賴的方法或是路徑開始，就是在數位轉型過程中，政府需要建立一個受信賴的路徑。其實信賴是一個結果。但是如何達到信賴？必須考慮哪些層次才能達到信賴？我想這是一個很重要的問題。今天我們整個討論到很多新科技的引入，數位科技跟其他不同的新科技，都有若干共同的特質，我嘗試從幾個角度來談，當我們談到一個新科技的引進，十年前的新科技可能今天是舊科技，對於社會的影響可能或淺或深、程度不一，但其實都類似。我嘗試把這些樣態提出來。第一個層次，要去了解新科技本身的特質。新科技本身有幾個很大的特質，第一是不確定性、也很陌生。相信科技的人，就絕對地相信，認為新科技可能帶來新的人生，很像宗教一樣，信者恆信，不信者恆不信。不相信的人，就認為它可能帶來很大的危險。那也因此在社會裡面，對新科技本身的認同也好，不認同也好，本身就是一個要去面對的複雜對話的過程，或者說是一個衝突的過程。如果我們沒有認知到，新科技在社會上會帶來一定程度的本質上的衝突的話，我們就有可能沒有辦法達到信賴。不管是贊成或者反對的那一方，尤其是具有公權力的這方，若沒有辦法得到一定社會的共識，當然就會面對社會對於這個新科技的不信賴。我們對於數位轉型，或者包括未來的 AI 都有很多的想像，正面的想像是希望去解決問題，負面則是覺得，他可能帶來在人文跟基本價值上很大的衝擊。所以就進入到第二個層次，我們必須考慮的是，新科技的應用本身與其整體影響。應用跟影響兩者是很難區分的。應用在其中一個面向，沒有被應用或考慮的面向可能會有意想不到的嚴重影響。舉例而言，產業應用對於推展新科技，是非常重要的 driving force，但當真正面對科技的應用，就好像我們剛開始在推動高科技的時候，會發現後續有污染、有勞動力的剝削，如同工業革命的時代，其實面對很多基本人權侵害的問題。在這一步一步發展進程中，其實會發現，新科技的影響是遠超過原來預期的應用範圍。如果說，一個新科技的引入，一方面我們對他陌生，也沒有透過一定的溝通過程或是理解，去理解到他可能在社會、經濟與文化面向或基本權利的影響的話，很可能就會遭遇到整個社會很大的質疑。

第三個部份，因為第一個部份跟第二個部份都很大的不確定性，我們通常希望利用新科技的可信賴性(reliability)。可是，新科技本身除了可信賴性之外，也有很強的不確定性，這就涉及第三個我想提出來的問題，也就是風險。任何新舊科技，都有一定的風險，如何面對這個風險，並對風險有一定程度的理解，進而化為公共政策，也就是我們今天必須要去面對與討論的。贊成 eID 或者贊成 AI

的人會認為，風險是可以被控制的；不贊成者則認為 eID 與 AI 某些風險應該是相當高的。風險的高低如果用一個簡單的機率來講，它跟後續深層的影響應該加以相乘、連結。簡單來說，當科技應用發生錯誤的風險很低的話，亦即假設機率很低，但是後來帶動的影響可能很大。我舉一個例子，我們現在把所有的 data 放在一起，假設一旦洩漏出去，影響層面非常大，因為個人所有資訊、身家狀況都一覽無遺；進一步說，如果把整個國家所有的 data 完全數位化，在一個比較中心化(centralized)的制度運作，當然便利性會大為提高，但是相對地風險也就會很高、相乘後影響很大。理想上，可以有很好的科技把風險的發生的機率降到比較低，但是一旦發生意外，impact 很大。因此，必須區分風險發生跟風險產生的 impact，這兩件事情是不一樣的，端看你如何去處理風險發生後所造成的影響。也因此，任何一個公共決策的作成，在面對新科技的時候，必須要去面對與建立一定程度的損害管控(damage control)機制與課責系統、管控系統。那如果不能理解這個新科技所帶來的風險，或者說相乘以後的影響，當然就無從去規劃一個好的公共政策、比較好的管控機制，或者其制度設計。

總結以上三點，所涉及之最核心問題就是核心價值。任何新科技的應用，透過政府以公權力去推動，原則上應以公共利益為重；然而另一方面，產業利益也是相當重要，因為要建立一個好的基礎設施，所以「產業的競爭力」，在新科技引入之際，也是重要的考量因素，但這兩個核心價值會有一定程度的衝突，另外可能引起衝突的，也包括基本權利的保障，例如個資保護、平等權保障等。所以在公共政策制定的過程中，有不同的核心價值。那面對核心價值之間的衝突，我們怎麼樣去訂定一個最基本的底線，並整合、理解先前提到的風險及其影響，進而達到社會共識，藉此建立可信賴與可執行的公共政策，透過這樣的決策形成過程，作成具備基本的可課責性之決定，亦即，必須具體說明「為什麼這樣做決定？在這整個社會可以容忍的風險跟風險影響是什麼？」這是一個公民社會跟民主社會中必須告知人民讓人民理解的，在此理解之下的政策，也才有一定程度的可課責性，否則其實是在資訊不透明的情況之下作成決策。這是新興科技透過政府公權力行使，化作公共政策而推動的時候，所必須面對的、我稱之為「科技基本政策的基本條件」。

對於前述幾個核心價值、風險跟應用之影響等新科技基本特質經過一定程度的辯論以後，也必須回到這個社會的 boundary condition，也就是社會條件。因為所有的科技應用，無法不考慮社會條件——亦即社會本身運作的文化及物質條件，甚至也須在社會心理層次加以理解，才有辦法形成比較好的政策。另外，就數位治理而言，所有的治理的細節，若沒有前述的討論及理解，難以訂定出比較好的

細節。因此，我要強調，在決策作成的過程當中，必須通過好的民主程序，增進民眾對於新技術本身的本質應用跟風險之理解以後，才有辦法訂定在特定政策具體施行的治理細節，也就是所謂的政策落實、政策施行相關法規的訂定，包括治理規範。簡單做個結論，第一，「價值驅動(value-driven)的科技」的發展非常重要，在一個公民社會，政府必須回答政策真正的核心價值為何？目標是要走到哪裡？是為了平權？公共利益？還是產業利益？都可以攤開來共同討論，但必須列出權利的基本底線。第二，政府之可課責性，以及如何落實平權跟控制之間的平衡？如何在決策過程中有好的公民參與程序？無論是對於 eID、或是數位轉型乃至於目前也相當重要的 AI，我想應該還有很大的努力空間，謝謝。

蕭景燈（行政院科技會報辦公室數位國家組主任）

各位與會的來賓大家好，我是行政院科技會報辦公室蕭景燈。今天討論的內容涉及很多範疇，數位轉型與智慧政府相關業務有些是在院的層級執行，有些是在部會的層級執行，這個議題很重要，過去幾年陸陸續續都有談過，並不是因為今天 eID 的案子才開始談，像網路中立性原則也是長期討論議題之一。當遇到網路霸凌事件發生，也會被外界檢視說，我們是不是注重資訊能力而忽略資訊素養。現在的客觀條件跟過往大不相同，過去我們休閒時間主要被電視佔據，現在隨時打開電腦，或手機就可以收到許多資訊，轉型已經自動發生。在這樣的脈絡(context)之下看待今天的會議，這樣比較可以想得長遠。剛剛在前面幾位老師的報告裡面，特別提到台灣目前有好幾個跟數位國家或是整體數位化、數位轉型相關的計畫在執行。把時間拉長來看，台灣開始運用網路，最早從中研院的計算中心連到 Princeton 大學，然後接下來才有教育部電算中心的 VAX 主機網路，台灣的網路是這樣發展起來。從那個時候到現在，經過了二、三十年，條件真的不一樣，所以談論議題的深度也就越來越深，也差不多到大家檢討是不是要設立一個數位發展專責部會的時機。我在行政院科技會報辦公室，是執行數位國家創新經濟 DIGI+方案，這個 DIGI+方案正是郭耀煌郭老師擔任科會辦執秘時開始啟動，一路到現在已執行了四年，未來還有五年的期程，可能此方案執行期間，專責的數位發展部會就會成立了。剛剛提到應設立個資保護專責機構，應會在成立數位專責部會過程中被充分討論。整個網路及數位化發展的過程，我有不同身分的參與，1993 年我回來台灣，以民間組織的身分推廣網路，我就已經有在各種場合談論到「網路素養(net literacy)、網路禮儀(netiquette)」這樣的概念，下班回家後是一個家長，我對我的小孩子教導網路隱私，讓他們懂得如何保護自己，像是剛剛有提到唐鳳政委所講的那樣。

回到我在行政院科技會報辦公室所執行的工作，跟國發會是一個配合的關係。整個智慧政府計畫是在「智慧國家創新經濟方案」之下，由行政院二級部會各自負責其職掌相關部份，在科技會報辦公室統籌推動下，包含：國民個人的數位轉型縮短數位落差，是教育部所執行；經濟面的產業數位轉型，大部份由經濟部主責，一部份像是金管會特定業務的主責部會也會參與。那還有一大塊就是整個政府部門的數位轉型，從以前的電子化政府到現在強調數位轉型的服務型智慧政府，電子化政府計畫共經過了四次調整，目前第五階段主要是以「服務型政府」為目標，接下來有為期五年的服務型智慧政府 2.0 推動計畫。政府部門的轉型過程有許多是因應新技術引進與外界公民期待，一路調整前進。

關於「政府可課責性」，無論政府是否數位化，都應該要建置完備的課責機制，只是因為進到了數位溝通模式的時代之後，在 cyberspace 裡面有更多的資訊流動、更多政府與國民意見溝通的管道。在這樣的情勢下，課責機制該怎麼做？目前所要解決的應是屬於這類層次的問題。那麼相關政策，像今天談的 eID，還有剛才國發會談到的 T-Road 入口網的建置，都會被大家拿出來檢視。科技會報辦公室在這過程裡面，很常討論的就是如何讓我們的公務體系能力再提升。剛剛也有一位老師提到說，行政機關內部的資安意識或是能力都不夠，所以怎麼樣讓公務部門同仁在執行公務時資安能力繼續成長、提昇，也是我們在計畫執行、預算分配時的考量項目之一。整體上，我是審慎樂觀，因為要相信，還有一些曾經在公民團體也努力過的人，現在已經進入到政府體系一起幫忙，包括唐政委與我自己，以我們過去參與網路發展的經驗，跟現有的政府計畫一起來配合、進行，我想這是我對剛才幾位報告者的回應，謝謝。

唐鳳（行政院政務委員）

好，那非常感謝三位老師的分享，我從頭到尾都有做筆記，所以待會就是用我的筆記來跟大家討論一下。不過，我看到不管是 facebook 開地球的，還是 twitter 開地球的，已經有一些觀眾在那邊推文說，我跟莊庭瑞老師會不會對戰，會如何戰呢？讓我們繼續看下去，很有意思。這個推文沒有多少人按讚，只有我們兩個人按讚。好，那很不幸喔，可能是戰不起來喔。那為什麼呢? 因為像我昨天在 RightsCon，RightsCon 就是一個叫 Access Now 的一個人權的組織辦的研討會。事實上也在討論這個題目，而且我的立場完全跟右邊三位一樣，所以事實上有點戰不起來，但是我可以稍微再幫他們再加強一下他們論述，就是由怎麼樣的講法，可以讓全世界的朋友們，更加精準地來看，不管是剛才講到的剖繪或者追蹤等等這些事情。那當然今天因為時間的關係，我沒有辦法把這個 Access Now 的 WhyID 連署的主要立場講的比較詳細，不過有空的話，歡迎大家來看這個 WhyID 的連署。

那我們可以看到不但我們的主辦方，也就是台權會、或者是開放文化基金會是連署人，我在這邊也是連署人。對，那所以啊，我想這個真的是戰不起來，那這個是合先敘明。

合先敘明之後，我們就先來討論一下剛才老師們討論的論點。那我們先從最一開始，就是劉靜怡老師的簡報，劉靜怡老師的簡報我覺得很棒，大概都沒有什麼問題，那只是有一個 point 就是說，在對於這個目的外利用是不是一定要透過兩個方式，一個是 Steve Mann 所提到的 sousveillance。當初 Steve Mann 提出 sousveillance 的時候，其實是說公民自己組成類似像剛剛講到的消費者保護等等這些組織，去時時刻刻像各位現在很多人拿起手機在拍照，就是多向地去了解一個事情發生的情況。

那如果我們現在說，以國家的力量成立一個獨立的專責機關，好比像說，像運安會之於交通部那樣，或者運安會以前叫飛安會，發生一個比較大的事故以後就也叫運安會了，這樣一個機關的話，一般來講的話不會把他叫做 sousveillance，因為他其實是體制裡面所留下來的機關。在我擔任數位政委之前，我有去法國參訪 Commission Nationale de l'Informatique et des Libertés, (CNIL)，就不是只監管個人資料，事實上重點可能也不是資料本身，而是負責去看說這個社會是不是有一些比較不平衡、不對稱的實例。不管是 Google 也好，或者是國家政權也好，這單位並沒有在管說是不是監控是資本主義還是國家主義，而只要是有影響到利

益國的根本 - libertés 的話，那這個單位就會跑出來。相信很多念法律的朋友知道，他們有裁罰 Google，這個案例我就不特別多說。

確實在臺灣我們目前只有類似像消保會，在商業交易的時候有這樣的專責機關，我完全同意說應該要有這樣的個人資料專責機關，只是覺得不應該叫做 sousveillance。大家如果了解運安會的運作的話，運安會是一個相當三級的獨立機關，但委員並不是由交通部長任命，預算也不由交通部控制。因為如果任命和經費都在交通部決定，運安會寫的報告大概也沒有人相信。運安會是由一群獨立的朋友們，去看交通部在某些事件上到底有沒有做好善後的處理。那甚至是由運安會去建議比較新的，交通部官員，不一定知道的建築方式來做大眾運輸的方式等等，來確保交通運輸的安全。這個對交通部推動很多政策有很多好處，因為如果運安會調查完一個事故，認定這其實不是公共建設的問題，而是有什麼別的問題的話，那交通部可以免除責任。那反過來講，如果運安會認定是公共建設的問題，需要換成一種新的建築材料等等，交通部就可以說，這不是交通部自己講的，而是獨立的民間專家講的，所以運安會的組成，可能就包含司法部門、立法部門，行政部門、民間專家，以及各式的朋友們所組成。

我大概在 2014 年、15 年，就是處理 vTaiwan 的題目時，就一直在倡議應該有獨立的個人資料專責機關，當然後來 GDPR 通過後其實也對此非常有幫助，所以，後來我們也建議一份建議報告，提供當時陳美伶主委拿這份建議去跟歐盟談判，目前，我們正在等歐盟技術資料的回函。我的想法其實很簡單，就是我們不應該等到發生像火車的事件再來成立運安會，我們應該要超前部署，在發生大規模資訊跟自由的侵害之前，就有一個相當於運安會，而且不是由交通部長來控制人事或預算，而是直接相當中央三級機關單位的作法。應該是下一個會期，我們就會提出這樣的想法給立法院。

至於，這個單位的組成，我覺得就需要大家來好好的討論。因為一開始我們一定會看到很多的個案，而且他成立的時候，很可能疫情還沒完全結束。所以我想在防疫過程裡面，就是以剛剛劉靜怡老師所說的，以公共利益為名進行目的外利用個人資料等等，很可能就會變成這個新成立的個資專責機關，需要處理的一些題目。這機關要怎麼處理來建立公信力，我覺得是大家非常需要關注的一件事情。尤其是像剛剛所講的，好比說電子圍籬等等這些事情，雖然當時我並沒有參與（因為那是資安處的工作），但是這個是進一步蒐集？其實他是用現有的來蒐集，但是他確實是做目的外利用，所以我們個資法裡面就是不可以合約為拋棄，請求副本等等權利，那到底應該要怎麼子去滿足呢？如果有一個獨立的專責機關說，可以這樣做就符合正當程序的話，對行政部門來講也是比較有所依循的，以

上是第一個討論。那當然這邊也有講到說日本所進行的是限定利用方式等等，不過災害對策這個解釋是很寬的，所以日本在發紓困的錢等等的時候，也都是用 My Number。所以，我覺得重點還是說，就像就是良好的建築材料一樣，我們現在有很多新興的演算法，可以好比像說 fully homomorphic encryption, federated learning, and open algorithms 等等的方法，如果用這些材料來建築的話，自然就不會產生出像碳排放那樣排放跟洩漏數位足跡。那如果有一個專業的機關，不單是給公部門或商業部門建議，也是請人民參與討論，我覺得是特別重要的一件事情。以上是對劉老師的回應，及提到 DPA and CPC 的差別。

另外一個是新疆這件事情，確實是如此。大家可能也有看到說我最近接受日經的採訪，就是說在此之前所謂的 totalitarianism 極權主義，大概都只能叫做 subtotal，就是不是很極端的極權主義，因為沒有足夠的科技去做 total totalitarianism，亦即真正完全做到每個人每時每刻每分每秒都被監控的情況。所以這個真的是非常值得注意，我也有跟日經的記者說，其實在臺灣我們只要看到他們在新疆做什麼，任何人只要提出類似於那樣子的事情，就是 non-starter，我們就不會變成討論的事情。就好像如果有人說要封網，或者斷網，那一瞬間鄉民就會群起而攻之。以至於我們在處理，好比之前假訊息危害的時候，完全沒有用行政部門的 take down 當作手段。我想這就是一直有類似新疆的 reminder 來提醒我們，我覺得這就是蠻好的一件事，其實也讓我們跨部門的共識更容易形成。

那剛才所講到的剖繪，好比說在發三倍券給中低收入戶時候，我們可以直接匯一千塊到他們的戶頭，再對他們的戶頭去給付，所以，重點還是在做處置的時候，是不是有 accountability 不斷地給交代的能力。剛剛講到 DPA 也就是去確保說我們有一個機制，能夠每一次不斷地給出交代的時候，獨立的去檢視每一個參與的部門，每位委員的人脈。透過資料的勾連或者串接，至少去做這件事情的成本就會變得很高，因為你不可能做而且不被發現。

這個時候就要回到國發會，其實已經上路的 MyData 數位服務個人化，目前還在試營運，試營運的意思就是說，就是如果你覺得這介面很爛，或者是 API 寫得不好的話，你行你來。這就是試營運的意思，那歡迎大家提出具體的建議，這邊包含可能就是大家都知道的投退保，保費繳納，健保資料或者是像各個縣市所提供的，以前沒有一個單一地方，讓大家可批次下載，你要分門別類去跟縣市政府去申請。但是如果這些縣市政府去進行剖繪或者串連等等的話，其實基本上大部分的人都不會知道。那我想在這邊是一個第一次有這樣一個 MyData 的平台，就是除了當事人自己之外，其他人都不應該能知道這些事情。所以，也歡迎大家

多使用 MyData，而且反而你行你來，覺得哪裡做得不好的話，就提醒我們要能夠增進一下。

那其他部分，我想最後這一部分是完全同意，也是我剛才就是常跟國際社會的朋友們提到說，在臺灣我們主要來考慮這件事情，並不是來讓政府的治理更由上而下，相反的，我們是希望說我們透過技術的討論，能夠讓大家都做出 privacy enhancing technology，就是能夠促進隱私的技術，這也是臺灣的特色，所謂 Taiwan Can Help。謝謝。

附件三

民間團體及個別專家意見

何明諠（台灣人權促進會副秘書長）

主持人、主講人，還有各位與談人，還有在座各位來賓大家好。我是台灣人權促進會何明諠。很開心剛剛其實聽到了我們政委跟我們做了一模一樣的連署，那我這邊先帶大家看一下，剛才政委也有參加的連署，我們其實有翻譯成中文了，所以其實大家不用很費心地去讀英文。我先花一分鐘跟大家解釋，到底那個連署的聲明在說什麼。

簡單的說，他裡面提了幾個數位身分計畫相關的風險，其中一個第一個問題在於標粗體黑字的這邊，這個計畫可能會對各國的人民造成 360 度的剖析，和監視使用者的風險。也就是說，其實非常多在建置這數位身分系統的國家，一開始是沒有身分制度的，而且沒有一個像臺灣這樣的身分制度，單一且一人一號的制度。那在建立數位身分系統的過程中，連帶把這樣的制度也建立起來。臺灣當然是已經處在身分制度基礎之上，建立一個數位身分系統。

該國際組織對於這樣的身分制度，第一個提到的風險，就是他會對個人有 360 度監視的可能，意思是你的一舉一動都會因為這個唯一的身分制度而被記錄下來，有必要的時候還會被追蹤。另外一個問題是，這個單一的制度可能會因為單點的被破解，導致整個資料的不保。那我想這個在臺灣過去這幾個月我們蒐集的資料，早上的講者也有講到，我想這應該是非常顯而易見的事情。

那國際組織也特別提到了對於弱勢族群或偏遠的人口，可能會不得不接受有風險的身分制度。舉個例子，早上的林律師其實有說過，我們現在有一個律師團，我們也在徵求原告，找一些可能會受到新身分證影響的原告。這些原告可能不想要領這個證，但是因為可能要申請補助，比如說要申請中低收入的補助，或是身心障礙的補助，被迫一定要領這個證，並承擔隨之而來的風險，但他們沒有選擇。對這些弱勢族群來說，他們會是這個身分制度推行後，最先被傷害的人。

那這大概是這整份聲明所提到的幾個問題，因為有中文翻譯了，我就不多說。請大家有興趣的話就搜尋 WhyID 台灣人促進會，就可以看的到。

因此我們其實也是很開心，看到政委有跟我們做一樣的連署，我想台權會過去很長一段時間的立場，今天在座大部分的人都知道。基本上反對這個數位身分證的政策，所以，我們很開心政委跟我們站在同一邊，我們也很希望政委可以好好地跟內政部、國發會做一些溝通。因為過去，基本上是這兩個單位在主導這個政策，卻不顧專家學者們提出的各種質疑，各種我想早上大家也聽了很多了，在

法律上需要再補強的地方、不需要補強的。那我想政委應該可以幫幫我們吧，謝謝政委。

接著可以開始進入正題了，過去幾年我們大概看過了一些數位足跡濫用、濫蒐的案例。從 2013 年 Snowden 的計畫，揭露了主要使用的科技公司，為了反恐、為了抓潛在的恐怖分子，把大家的使用網路的資料、使用平臺的資料回傳給美國國安局。到 2018 年，英國劍橋分析透過大家去 FB 的遊戲互動留下來的資料，以及朋友們的資料，去掌握大家的偏好，去推播假新聞。剛才蔡老師有介紹的中國社會信用評比制度，也是透過給你編號，透過這個編號跟各種資料的串聯，去掌控全國人民在社會的活動，應該怎麼活動。

在台灣其實還有一些資料濫搜、濫用的狀況還沒有被發現，或是比較少人注意到。比如說，大家知道我們便利商店的結帳的店員上面的那塊電視板，其實有人臉辨識的功能嗎？我想在座的大家應該不知道，但是這就是既存的事實。晶片身分證是不是有這樣子的問題，是不是會帶來資料濫用、濫蒐的問題，我等下會再跟大家仔細說明。

在科技應用的部分，過去一直在說，要平衡科技應用帶來的好處跟壞處，但其實我們應該要問的是，科技應用到底在什麼意義下，帶來什麼意義的好處跟什麼意義的壞處。在民主國家帶來了什麼樣的好處，帶來什麼樣的壞處。

接著這個是內政部目前唯一公布的數位身分證全面換發計畫，大概是檯面上比較完整的一個計畫。計畫裡面有一段文字是這樣子，他說我們發 eID 的目標是要帶動跟形塑產業的新發展，並提升國際合作。在這個段落裡面，其實它提到了非常多跟私部門間的合作，也就是說會透過這個 eID，他可以達成跟私部門之間服務的使用等等。至少從這一段說明裡可以看出，未來 eID 的使用不會只侷限在公部門，私部門需要使用 eID 的話，應該也是可讀取 eID 裡面的資料，甚至是使用電子簽章的功能去做交易。

這個圖大家今天應該看過三、四次了，再看一次，這是目前身分證的分區，前面兩區戶籍區跟公開區，是 Open API，基本上是沒有任何單位可以去讀取、或不能讀取，基本是應該是會寫 code 的，會接 API 就可以讀了。Secure API 需要經過內政部的授權，才能去 eID 裡面的資料。那當然早上內政部有提到說，在使用 Open API 公開區仍然要輸入密碼，但是輸入密碼後，並沒有限制哪些私部門或那些公部門可以讀，最後結果當然有可能就是很多公部門跟私部門都可以讀，問題只是要先輸入密碼他們才可以讀，就這樣而已。

所以，結合了剛剛前面兩張的簡報，你會發現我們有一個可能就是，我們大

概有兩種身分資料會留下數位足跡，並留存在這個使用脈絡裡面。一種是這所謂版面資料，或者是晶片裡面的 Open API 裡面這些區塊的資料。你會發現，你的身分資料如果沒有被妥善的限制使用場合，使用在哪一些私部門或公部門的服務，因為讀卡的方式變得非常的容易，變得非常的方便，不一定要以實體的方式進行，未來，身分資料可能會到處留存。

另外，這張是借用尤美女委員質詢所使用的一張圖。另外一個可能會留下的數位足跡，也就是所謂的衍生的資料，或者是說 metadata，或者是 log in 的 data。這裡舉的例子是說，某年某月某日，有一個人他去購物網消費，購物網可能要求要通過身分驗證才能使用，那會不會內政部也知道你去過購物網? 會不會他去成人網，內政部也知道？如果會，那也許內政部就有可能完全掌握每個國民的行蹤。

這個當然是我們不願意看到可能會發生的事情，因為結合了剛剛對私部門沒有限制的狀況，所以我們可能就會猜測，內政部是不是就會知道你我的數位行蹤? 今天內政部早上說不會，但剛剛也有說過了，至少企業也會留下相關的衍生的資料。因為，資料留著就有可能會被使用、會被濫用，可能會被使用的可能。那企業會把衍生資料留多久，會做怎麼使用？

過去一段時間我們常常在講德國，其實早上也有提到德國，德國的法律叫身分證及電子身分驗證法，民間司改會已經翻成中文，全文都翻譯了，所以大家其實可以去司改會或台權會的網站看。

德國的法律裡面，怎麼去避免剛剛的說的風險？其中一個在它第 10 條裡面（看紅字的地方）規定，要進行卡片驗證時，應該由服務提供者自德國內政部取回鎖卡清單，在本地端，也就是 PC home 這端，我進行鎖卡的驗證（進行卡片是不是有效的驗證），所以，其實德國內政部那邊不會知道。這個作法是寫在德國的法律裡面的，不是僅是口頭保證。那我們說私部門或者是內政部說資料不會串聯，那在德國是怎麼處理？德國雖然沒有身分證號的概念，但德國的身分證也是有身分證的序號。

同法第 16 條規定，不可以用身分證的序號去自動呼叫個人資料或自動連結檔案，意思就是說，原則上禁止使用身分證序號去串聯不同的資料庫。在私部門做了限制，這邊也開了一些例外的條款，但基本上大幅降低資料串聯的風險。這項在台灣，一樣只有給口頭保證。

同法第 17 條，紅字的部分，簡單的說，當身分證驗證完畢，相關資料應該要被刪除，不能夠被留存。意思是，一旦完成身分驗證的目的之後，那些資料就

要被刪除，所以可以大幅降低被留存的身分資料的數量。這個目前在臺灣的個資法，或其他法律裡看不到的。這項在台灣，也是只有口頭保證。

臺灣有類似的法律嗎？不知道，就我們所知目前沒有。政府的口頭保證，如果這麼堅決，能不能舉出具體的法律規定？比如說你不會留資料，你不會做人臉辨識，你不會串資料庫，這些東西到底你列不列的出是哪一條法律有明確說真的不會？

臺灣的警察，已經可以做人臉辨識，這是事實。臺灣警察怎麼做人臉辨識的？就是串接內政部的照片資料庫，內政部為什麼會有照片資料庫？因為大家的身分證上面有照片，所以身分證的照片資料庫是兩千三百萬人的照片資料庫，警察把它拿去串接了。這是現在臺灣警察就做得到的事情，那內政部早上說他不會做人臉辨識？

好，如果大家聽完之後，覺得這政策真的很有問題，我們需要立個好的法律，我們需要讓大家有選擇無晶片卡的空間，讓大家可以去建立獨立的個資專責機關之後，再來想想我們是不是應該要做這樣政策。

歡迎參加台權會連署，我的報告就到這邊，謝謝大家。

李念祖（私立東吳大學法學院暨法律學系兼任教授／總統府第一至五屆人權諮詢委員會諮詢委員）

李所長，各位在座的先進，大家早安。首先要跟各位抱歉，我大概是唯一沒有帶著 PowerPoint 來發言的，最主要原因是，我原來在想是不是帶首歌來放給大家聽，把這個時間帶過去就好了。因為我覺得，這首歌非常適合我想要表達的內容。我相信很多朋友都知道這首歌，這首歌叫做 Hotel California。但後來想想，來這邊放歌實在是不對，所以作罷。我自己承認，我是一個科技盲，所以我今天在這裡是以一個科技盲的獨白，同時還有小人之心，我是以小人之心自我提問。我帶來了 10 個自己問自己的問題，合起來我的報告題目可以稱做「無所遁形，還是不棄不離？」

我的第一個問題，就是李所長剛提到 15 年前我們一起申請大法官解釋，釋字 603 號解釋-指紋案。我第一個問題是釋字 603 號解釋以後，戶籍法改變了嗎？當時申請解釋的立法院的民進黨立委黨團，領銜的立委是賴清德立委；在我們準備過程中間，經常來幫忙我們、指導我們的是蔡英文立委；我們指責違憲的單位叫內政部，當時的部長叫做蘇嘉全先生。當時是一個很有趣景象，是國會的少數黨，對抗同黨的少數政府，而今天這三位都在同一個地方上班。我的問題是，他們都贊成 eID 嗎？今天是全面執政，誰來反對呢？我想到一個朋友，很多人都知道，大家都叫他同一個名字，叫 Peter。我也想到 Hotel California 裡面的那一句話，we ain't had that spirit here since 1969。

第一個問題的第二個部分，有關釋字 603 號解釋，當時說戶籍法第 8 條第 2 項、第 3 項強制捺指紋是違憲的。為什麼？因為立法目的不明、又缺乏配套防弊措施、違反比例原則，即日起不再適用。那今天的 eID 跟指紋一樣嗎？是蘋果跟橘子無法比較呢？還是他們都是水果呢？而指紋是政府要求交付個人資訊 - 就是指紋，給政府建立辨識系統加以使用，而 eID 是要求個人帶著自己的資訊，進入政府用新科技建立的辨識系統供追蹤使用。追蹤這兩個字，我們後續可能需要解釋，在我來看，這是自行 key in。Hotel California 裡面有一句話，We are just all prisoners here of our own device。eID 有什麼法律依據？2008 年的戶籍法跟當年的戶籍法是經過大修的，數位時代戶籍法，脫胎換骨易容整形。今天的條文剛剛文聰都已經講過了，看了這些條文，Hotel California 裡面說，this could be heaven or this could be hell。

好，我的第二個問題是，身分證制度合憲嗎？603 號解釋沒有談這個問題，

現在問這個問題會不會太晚？它不在 603 號解釋的範圍，也許不太晚。

第三個問題，強制全民換證，換成 eID 合憲嗎？剛剛聽到副司長講說，試行不是強制，是將來不打算強制嗎，還是身分證是合憲，所以強制換證是當然合憲? 這是多餘的問題嗎?

第四個問題，戶籍法的換證規定合憲嗎？我不把條文重新講一遍，我的解讀是第 51 條，每人一證，無處不用、無所不用。同樣的戶口名簿，每戶一簿。第 52 條，有關格式、資訊、內容，身分證要加什麼內容；怎麼建制；怎麼查證；誰來查證；什麼場合查證；怎麼利用，通通授權政府決定！第 59 條，換證的辦法，舊證什麼時候失效；什麼時候要限期換新；通通授權政府決定！第 77 條，可不可以用來當做處罰，我不知道，但我真的問題是，這些條文授權政府做了好幾個辦法，但事實上現在內政部正在做的就是辦法，所以說法律不需要修改。那這個辦法就可以，已經有授權，但有沒有授權不明確或過廣的疑慮？有沒有憲法問題？它有沒有符合特定目的、特定範圍，以及委任立法的基本原則？

剛剛講到身分證基本功能是辨識，戶籍法就是身分證明的功能。辨識與證明兩個詞聽起來很像，剛剛文聰講說，最早的時候，身分證是供證明之用；現在副司長講，身分證是供辨識之用，而辨識是寫在戶籍法裡頭。但證明跟辨識是否不一樣？的確不一樣。因為證明是為了執政者的需求而存在的，我需要用這個證明，我拿出來。所以，我可以用，我可以不用；我可以要，我可以不要。

但是辨識卻是為了政府的需求，所以你非有不可，非要帶不可，非要進入不可。

釋字第 603 號解釋質疑當時沒有寫立法目的，因不存在而違憲，那我現在要問的問題是，新的戶籍法寫了辨識兩個字，它就可以成為獨立的、正當的目的了嗎？企業都喜歡說 know your customers，政府現在是 know your citizens。他等不等於 trace your citizens？因為這裡面沒說什麼場合可以要求辨識？誰可以要求辨識？辨識有沒有其他的目的？譬如說追蹤。這不是空白授權嗎？違不違反法律保留原則呢？戶籍法上寫的是印製身分證，現在是發 eID，那印製身分證等於發 eID 嗎？這不違反法律保留原則嗎？

我們看到了換證辦法是溯及生效，令我好奇的是為什麼要溯及？不溯及就不合法對不對？如果不溯及就不合法，溯及就合法嗎？我覺得另外一個值得讀的解釋是釋字第 689 號解釋。因為法律可以限制私人跟追，那限不限制國家政府跟追呢？不可以全面用指紋，但是可以全面要求人民進入政府的跟追系統，這是請君入甕，還是請君出甕？政府沒有侵犯隱私權嗎？

好，下一個問題。為什麼說政府的系統是跟追系統？跟追什麼呢？我擔心的是跟追個人的即時行蹤：戶政系統會跟什麼系統聯繫？照片會不會跟街頭攝影裝置聯繫？會不會跟大家自願給的指紋系統聯繫？新的系統和稅務、健保，和其他系統會連結嗎？和將來的系統會連結嗎？譬如說將來有個支付系統的話？或者是個人加入的私人支付系統？我們是在建立臺灣版的追蹤系統的開始，還是收尾呢？

第七個問題，誰可以授權使用系統資訊？誰可以授權系統連結？我看了內政部的答客問，是內政部。那防弊措施夠不夠？請讀釋字 603 號解釋。那這違不違反個資法呢？人民有沒有知的權利，要求陽光立法？或是要求政府提供跟追自己的足跡呢？立法有沒有因為不作為的怠惰而違憲？我們的個資法，保障第三人的隱私，遇上政府要資訊的時候，永遠說，因為要維護第三人隱私不能給你。政府保護第三人隱私，保不保護當事人的隱私呢？

我是一個科技盲，問到最後的問題了。我可不可以繼續做科技盲？我有沒有拒絕政府辨識的不表述自由？我可不可以拒絕換證？不換證是什麼結果？舊證失效。舊證失效是什麼結果？失權。罰？罰不罰錢不重要。重要的是，你不能夠帶著舊證，行使憲法的權利。譬如說，投票。你可能也參加健保，會不會有困難？這是不是叫不入虎穴焉得選舉？我可不可以拒絕帶著自己的個人資訊，納入政府的資訊新系統？我們聽到所有的理由都是便利，對我們很便利，還有對政府也很便利。但是政府便利，我們便利，就可以強迫喪失基本權利？

我知道天下從來就沒有隱形人這回事，但是強迫裸奔，而無所遁形，可以嗎？

這是一個新時代，我又想起了 Hotel California。"And in the master's chambers, they gathered for the feast. They stab it with their steely knives. But they just can't kill the beast. You can checkout any time you like, but you can never leave!"

最後是一句感謝詞，承蒙政府不棄，邀我形影不離，謂之不棄不離。我的小人告白完畢，謝謝。

林煜騰（圓矩法律事務所律師／民間司法改革基金會執行委員／台權會籌措民間反 eID 律師團召集人）

大家好，我是圓矩法律事務所林煜騰律師，同時也是民間司法改革基金會，以及台權會在籌措民間反 eID 律師團的召集人。今天非常感謝中研院法律所舉辦這一次的活動，還有主講人以及與談人們精彩的介紹跟說明。聽了這些內容之後，讓我更堅定我們民間在反 eID 的這條路上，應該是沒有走錯。

剛剛主講人跟與談人談了很多 eID 會帶來的問題，可是對人民而言，最重要的問題是我今天已經知道數位身分證有這麼多的問題存在，那我的下一步是什麼？針對這個問題，我想要從人民的身分識別權這個角度切入。什麼是身分識別權？身分識別權是一個連結人民與國家之間身分關係的權利。換個白話的說法，就是今天我在國家體制下，要如何告訴別人我是誰？我在一開始的時候，跟大家介紹說我是林煜騰律師，如果你們有所懷疑時我要用什麼樣的方式證明我自己？告訴你我的身分是什麼？我家住哪裡？我跟你講的這個人，是不是真的就是我？這就是身分識別權所要處理的問題。我在這裡要問的是，到底國家有沒有義務，賦予人民一個有效認證自己身分的機制？

大家從剛剛聽到現在，應該已經很明瞭，在我國的法制底下，確實有這樣的機制存在。那就是我們的戶籍法第 51 條：國民身分證用以辨識個人身分，其效用及於全國。今天在臺灣，我不管是要跟政府或私人機構說明我的名字、我的身分，最直接的方式就是用國民身分證。這是最有實效的作法，這也是我們人民的權利。但是戶籍法同時也規定了國民身分證應隨身攜帶，所以身分識別權其實是一體兩面的，不只是人民的權利，也是義務。

不過，從現在的角度來看，戶籍法第 56 條可能會是個笑話。請問在座的各位，有誰把自己的身分證帶在身上？有每個人都帶在身上嗎？有的可以舉個手嗎？那沒有的呢？我也沒有。我今天也沒有把身分證帶在身上。但我放在哪裡？我沒有放在家裡。我放在哪裡？大家可以看我手上這樣東西，可以看的清楚嗎？這是什麼？這是我進入中研院時，在門口被要求換發的停車證。我今天開車進中研院參加這個會議，我必須把我的身分證放在中研院大門的警衛室，就為了換取這張停車證。那剛剛，戶政司副司長有提到，身分證隨身攜帶是個訓示規定。好，那我現在要請問一下，大家看一下 PowerPoint。身分證應隨身攜帶，非依法律不得扣留。那我想請問副司長，後面這句話是不是也是一個訓示規定？今天我的身分證，是不是被中研院給扣留了？

從 eID 數位身分證，推行到現在，內政部和國發會有個主打，一直強調 eID 是開啟數位政府的關鍵鑰匙。那我的鑰匙現在就在中研院大門警衛室。我想請問內政部要怎麼回應這個問題？要怎麼解決？如果依照戶籍法第 56 條第 1 項，這只是一個訓示規定，那未來我那麼重要的關鍵鑰匙，私人機構可以任意扣留，我要怎麼樣保護我的資訊安全？這麼重要的東西，到處亂放真的安全嗎？真的不需要修法嗎？

那其次，剛剛副司長也有提到，法律沒有要求隨身攜帶身分證，因為這只是一個訓示規定，不會處罰你。不過，不處罰難道就不會對生活造成任何的影響嗎？在十幾年前，司法院釋字第 603 號解釋，就已經講過這個問題，認為國民身分證已經成為我國人民經營個人及團體生活，辨識身分的重要文件。其發給與否直接影響到人民的基本權利。這些基本權利包括什麼？你今天應考試，服公職，你要選舉、罷免，對不對？你要申請任何補助，甚至說我今天要開車進中研院來這個地方與談，我都需要帶著我的身分證，不然的話，我寸步難行。那想請問一下副司長，這些算不算是對我的處罰呢？如果今天真的沒有隨身攜帶身分證也不會有任何影響，也不會受到國家的處罰，那你能不能確保我在我行使所有跟公部門以及私部門有關的權利時，也不會因為我沒有攜帶身分證，而受到任何限制呢？這個問題要是不能解決，說國民身分證隨身攜帶是訓示規定，只是一種敷衍塞責的說法。

那，好，我們今天已經確認了一個前提事實，我們國家有盡到義務，給了我們一個身分辨識的方法。但是這樣的身分辨識機制，難道就沒有任何的限制可言嗎？也早在十幾年前，大法官就已經解決這個問題。今天國家如果強制人民按捺指紋做為核發身分證的要件，這樣的身分證其實是一個有瑕疵的給付，不符合比例原則，違反憲法的規定。這時人民其實是可以拒絕受領的。所以並不是說內政部給出一個身分識別機制，人民就必須要照單全收。

綜合剛剛講的，我們從既有的釋字第 603 號解釋出發，自人性尊嚴跟資訊隱私權的角度推演，可以推導出身分識別權的存在。而身分識別權的內容，是要求國家有義務提供人民一個有效的身分識別的制度；但是，這也必須要是一個合乎憲法的身分識別制度。目前大法官已經肯認紙本身分證，可能不違憲；但是指紋身分證違憲。而我們今天所要討論的是，到底數位身分證有沒有符合憲法上的要求？從前面幾個主講人跟與談人談到現在，我們可以瞭解到，數位身分證違憲的疑慮是相當高的。

在此，我必須要再進一步去談，如果數位身分證違憲疑慮這麼高，會對人民帶來什麼樣的影響？我的看法是，戶籍法第 59 條搭配換發侵害人民憲法上權利

的數位身分證，會直接侵害到人民的身分識別權。為什麼呢？戶籍法第 59 條規定，國民身分證全面換發的期程全部由中央主管機關訂定，而且全面換發以及舊證失效的日期，也全面由主管機關訂定。領有國民身分證的人，必須要在全面換發國民身分證期間換發新證。這個條文會衍生出幾個問題來，剛剛其實李律師也稍微提到過，依照戶籍法第 59 條，內政部在什麼條件下可以發動全面換發身分證？而內政部全面換發的身分證，是不是要符合憲法的要求？如果，這個新換發的身分證侵害了人民憲法上的權利，內政部可不可以強制我接受新證，進而宣佈舊證失效？

我們來逐一來解答這三個問題。我們先來看第一個問題，在什麼條件下，政府可以發動全面換發身分證？從條文我們可以看到的是空白授權，無任何限制。試問內政部能不能依照戶籍法決定每年都要換發一次呢？還是可以決定每次政黨輪替都要換發一次？或者是說中秋節發中秋限定版的身分證？再發一個端午限定版的身分證？戶籍法有沒有規定限制內政部換發這種限定版的身分證呢？答案是：沒有。現在沒有任何的限制，也沒有任何的要求。

再來看第二個問題：當推動全面換發身分證時，是不是需要符合憲法要求呢？這樣的要求，依照現在的法律體系是很明確的。剛剛已經有提到，戶籍法第 51 條規定國民身分證只用於辨識個人身分。eID 如果有辨識個人身分之外的其他的功能，照理來講已經超出戶籍法所授權的範圍，直接違反法律保留的原則了。除此之外，今天身分證的形式跟態樣並不是沒有任何限制的。釋字第 603 號解釋設下了一個憲法的門檻，如果是採指紋或者是其他生物特徵作為換發身分證的要件，都應該受到嚴格的憲法審查。

最後一個問題，如果我們認為新換發的身分證將侵害人民憲法的權利，那內政部能不能有宣告舊證失效的權力？首先，依照釋字第 603 號解釋，新換發的身分證如果侵害人民的憲法權，人民應該是可以拒領的。舉例而言，若內政部這次又偷渡指紋必須要作為換領身分證的要求，難道人民只能全盤接受嗎？今天已明知這身分證可能會違憲，難道我一定要領取？釋字第 603 號解釋給我們一個空間，只要是有違憲疑慮的身分證，照理來講人民是有憲法的權利可拒絕領取的。

其次，如果我今天已經明知這個身分證的違憲疑慮相當高，而拒絕領取身分證，那內政部能不能依照戶籍法第 59 條宣告我的舊證失效？依照前面提到的身分識別權角度來看，內政部不該有權做這樣的宣告，否則會直接剝奪人民擁有身分識別機制的權利。若沒有領取新證，舊證又失效的情況下，會變成我在這個國家沒有一個合法、有效的方式，去證明我是誰。除此之外，我也沒有辦法再去行使應考試，服公職，領取各項補助公家的權利，甚至私法上的權利也會受到波及

，這對我們的影響是相當大的。因此，我認為內政部適用戶籍法第 59 條在宣告舊證失效時，應該採取一個合憲性解釋的方式處理。

合憲性解釋的方法，並不是我現在為了要對抗數位身分證所獨創、憑空想像的。其實在最高行政法院 107 年判字 240 號判決裡面，已經有處理過了。最高行政法院認為，主管機關在解釋原住民身分法第 2 條的解釋方法，有違反憲法平等原則，及憲法保障原住民政治參與地位的疑慮存在。所以，不能依照主管機關的解釋去適用法律，而是應該要做出一個合憲性的解釋。那套用在現在數位身分證的例子，我會認為內政部全面換發新的數位身分證的理由，基本上是違法違憲，內政部不能在這種情況之下，還要再依照換發期程逕自宣告舊證失效，以避免侵害人民的身分識別權和其他憲法上權利。

結論，從剛剛主講人跟與談人的討論，我們可以很明顯地得知一個訊息：數位身分證違反法律保留原則、侵害人民的資訊自主權、甚至這次的身分證換發也蒐集不必要的生物特徵 - 600 dpi 解析度的數位照片。基本上 600 dpi 解析度的照片能夠拿來作為人臉辨識使用，可以算是非常強的生物特徵了。我今天要辨識人民的身分，有需要用到這麼高強度的生物特徵嗎？這也是非常有疑慮的。

因此，我們在這裡，要跟內政部呼籲：內政部不應該在之後數位身分證換發期程中宣告舊證失效，藉以強迫人民換領數位身分證。人民應該要有選擇權，可以選擇保留舊式的紙本身分證，或者領取新式的數位身分證作為身分辨識的機制。

最後，我希望內政部可以回應以下兩個問題：第一個，中研院扣留了我的身分證後放在警衛室，依照戶籍法要怎麼處理？第二個，內政部有沒有在換發數位身份證後，宣告舊證失效的計畫？謝謝。

李柏鋒（開放文化基金會董事長）

大家好，我是開放文化基金會李柏鋒。很感謝各位能夠撐到現在，大家要給自己一個鼓勵。謝謝大家配合。

我不是技術人也不是法律人，然後又被排在最後一個講，我實在很害怕講錯，所以如果有錯誤的話請各位多包涵。

開放文化基金會是一群阿宅組合而成的，我們關心開放資料、開放原始碼、開放政府議題。我們當初只是一個很簡單的願望，想要在 Linux 上面能夠讀自然人憑證，然後下去挖，開始挖看看會發生什麼事，結果越挖越發現隕石大坑，到現在陷在裡面爬不出來，問題一大堆。

早上有先進覺得說，我們要往美好的技術方面，要變科技立國這樣子。所以，我雖然有一點點對這個 eID 跟 T-Road 有一點質疑，但是我要火力展示一下，我自己有用愛沙尼亞的 eID，然後我自然人憑證第一代、第二代都有用。那我是阿宅，我本業是醫師，我也有個醫師憑證卡這樣子，證明我是醫師。那自然人憑證第二代其實就已經有 RFID 功能了，它可以嗶卡，可能很多人都不知道，它其實可以嗶了。所以大家擔心的話，回去記得要用鋁箔紙把它包起來一下。然後我問憑證中心，他說有這個功能，但是沒有機構使用這個功能。所以很有趣啊，大家都說，剛剛唐鳳政委也說我們先做嘛，對不對？可是做了，大家都不知道，可以嗶卡也不知道，所以這個我贊同前面各位先進講的，也許道要先行，路要晚點開這樣子。

那前面大家都講很多了，我只挑三個小小的地方，也許會偏細節，但是跟各位討論一下。落實個人資料保護，釐清這三個東西──識別、認證、授權，X-Road 跟 Blockchain。第三點前面也有老師提過了，我們等一下會再檢視一下。

這個圖是 108 年智慧行動方案的圖，我們政府一直強調說，需要一個 New eID，開啟我們 T-Road 上面的資料交換，它是給我們一個迎向未來的鑰匙。我從這個圖開始講。其實我們個人資料就是散落在各個地方。個人資料保護法其實有授權我們每個個人，公務機關就要把我們這四個東西顯示出來，為什麼？這很簡單啊。因為個人資料保護法授權我們可以刪資料，那我們不知道什麼資料被蒐集了，所以當然政府要先告訴我們你們蒐集了哪些資料，這在個人資料保護法的第十七條就已經規定了。可是很不幸的，我們個人資料保護法的主管機關，就是各個事業目的主管機關、各縣市政府。所以公務機關它自己沒做到，像台北市政府，

它自己又是主管機關，所以沒有人能夠治得了它。所以它如果沒有列出這個蒐集清單的話，它又是主管機關，那誰能夠治得了它？所以前面先進也有寫到，要有一個獨立的個人資料主管機關，才能夠真的去監督個人資料保護。

那內政部其實做得還不錯，在網站上其實就有一個保有個人資料的清單，甚至連 108 年的清點時間點都寫出來。第一個就很有趣：「幸福小棧報名人資料表單」，這聽起來就可以刪掉。所以，是不是大家可以練習一下去刪掉一下？或者說，戶政司是不是可以自己主動刪掉？因為這感覺好像過期了就可以不需要用了對不對？大家有空可以上去玩一下。

那接下來是警政署，這個就比較敏感一點。警政署很乖喔，也有在列。第一個就更可怕的是：「國民身分證相片影像系統」。這個前面也有很多先進在討論，就是說為什麼它會有這個照片？這個照片其實就是從身分證來的。個人資料保護法賦予我們可以去更新這些資料的權利，所以如果政府覺得我們十年到了一定要換資料，那我們換這個照片就好，我們就用舊證，那是不是可以只換照片，不要換資料的格式？就是早上我們講的 eID 的問題。那我們可不可以刪（資料）？假設 T-Road 建好了，我們可不可以刪？因為以後有 T-Road 了嘛，那你要資料就可以從 T-Road 要，為什麼要保留一份完整資料在那邊？那甚至說，我們不可以中央直接蒐集指紋，對不對？那現在臉部辨識很發達，臉部辨識和指紋一樣都是生物特徵，那我們可不可以刪？大家不知道要不要挑戰一下。

經濟部可能資料太多了它就沒有做這個事情。那經濟部的主管機關也就是它自己，我不曉得要找誰申訴，找經濟部申訴我想它也不會管我就對了。（會後補充後來有朋友指出，經濟部也有個人資料蒐集清單，只是很難找。[1]）

所以就是說，我知道大家都說 GDPR，其實我們個人資料保護法就已經還蠻嚴的。我們可以查詢、要求複製本、要求更正、要求停止蒐集、要求刪除。問題是，我們不知道有哪些資料可以在 T-Road 上面交換來交換去，（如果）我們根本不知道有哪些資料被交換，那是不是政府可以從最基礎（的地方）告訴我們，我們有哪些資料在你手上？給我們個清單，能刪的就刪一刪，不能刪的告訴我們為什麼不能刪。

接下來就是講識別認證跟授權。eID 就是開啟服務的一把鑰匙，那鑰匙也許是認證、也許是授權、也許是識別，我是覺得在我們的規格書裡面是沒有講清楚的。這個是從 T-Road 規格書裡面抄出來的東西，它 RFP 上面有寫說要建置一個 Single Sign-On 的模組，這個我順序稍微調整一下，分別是這些，識別碼、密碼。

[1] https://www.moea.gov.tw/Mns/populace/information/PersonalData.aspx?menu_id=4475

多因子，就是健保卡卡號加戶號，這有點像我們報稅，我們報稅就是用戶號加上一個認證碼。健保卡。GPKI，就是政府可以核發的憑證，這聽起來像憑證，但是不是自然人憑證還不曉得。還有未來內政部發行的 New eID。政府說 eID 一定要發，因為它是我們開啟數位政府的鑰匙，結果我們自己的 RFP 裡面就寫說，其實不用，你有很多把鑰匙可以開。那既然這樣子，政府強迫我們每個人接受 eID 的理由是什麼？明明有這麼多方法可以開啟，為什麼要強迫我們接受？所以我覺得它就喪失了公正性的問題。所以我還是堅持，假設我們人民要求普通的卡片，我覺得我們還是要能夠拿到。

接下來就講識別、認證跟授權。在這個卡片裡面，我們 RFP 裡面有講到識別跟認證，識別跟認證也不好區分，不過現在混在一起講。我們卡片假設輸完密碼後，我們就認證了我（的身分），我跟國家講我是李柏鋒。可是，這不代表說我有授權，我只證明我是我、我可以拿資料，可是我要怎麼樣去授權，要授權多久？什麼時候會消滅？在 RFP 裡面沒有講。我相當認同也許我們不需要等到全部的法律備齊再講，但至少我們 RFP 裡面要寫，至少我們要有個行政命令，假設我們沒辦法弄法律的話，是不是政府至少要有個行政命令或者辦法之類的和大家講清楚這個授權期間是多久，才不會有剛剛前面各位先進講的說，到底這個資料它是不是可以永久保存？那可不可以刪掉？技術上來講我們當然是可以做一個一次性的密碼讓它解開來以後，就沒辦法再用了，可是問題是，它總是要讀取，因為電腦的（運作原理）就是這樣，它讀了以後總是有可能再偷偷複製一份，那這就可能不是技術的問題。假設只是技術的原因，那當然是最好。另外一個想法是說，如果技術上不能解決的話，是不是我可以一律禁止部會間交換資料？一律就是我先下載變成 MyData 之後，我先看看我有哪些 data 之後，我再上傳給那個部會去用我的資料，上傳完之後馬上要求它刪掉這樣。這就是按照目前法律框架去做的，而且 MyData 也可以做。那是不是可能有這個機制？T-Road 當然沒有這個機制。我們（的提案）default 是禁止部會間交換資料，是由我們先下載看過之後再上傳，並且要求它用完馬上要刪掉這樣子。

最後一個就是 T-Road 跟 Blockchain，這個也是很有趣。這是 RFP 裡面抄出來的。廠商必須以區塊鏈的方式規劃建置紀錄調查平台，而且區塊鏈建置節點至少三處。這個很有趣，這個大概懂 Blockchain 的人就會知道這根本是沒有意義的事情。第一個，X-Road 沒有 Blockchain，這個前面愛沙尼亞的 NIIS 的 CTO 就寫了篇文章，這剛剛前面有先進有講過，這篇文章大家可以上網查一下。X-Road 沒有用 Blockchain。台灣要不要用 Blockchain 當然可以討論，可是這個規則非常的有趣，如果這三處是同一個廠商掌控，那根本就不用用 Blockchain，因為（廠商）

它自己就可以改（紀錄），它就沒有意義了。如果你是真的擔心說它會竄改紀錄，那很簡單，你紀錄馬上給三份不同的廠商。如果你相信我們的話，那我們開放文化基金會也幫你們保留一份沒有關係，我們不會亂改。那這樣子你有三份以後，直接用資料庫複製的技術，根本也不需要用 Blockchain。所以我真的很想問一下，這個 RFP 是誰寫的？這條是哪個廠商建議的，還是哪位先進建議的，我是很想學習一下。

所以我埋了一個梗，The Road Ahead？(T-Raod 真的是未來的 Road 嗎？) 比爾蓋茲在 1995 就寫了一本書 The Road Ahead，可是那一年他其實低估了 Internet 的發展，大家如果還聽過 Netscape 的話，他那時候被 Netscape 打得很慘。那本書寫完不到一年，他就補充了二十萬個單字，馬上就寫了第二版。我當然覺得我們要建 T-Road，這個技術當然是要，我們也要有 eID 的基礎建設，可是問題是，我們這些基礎建設背後是 RSA 的加密技術，那 RSA 的加密技術隨時都有可能會被量子電腦破解。這也不是我危言聳聽，已經有很多老師之前有提。

2023 年左右美國就會開始有量子力學加密的標準。那假設這個 eID 十年不換（台灣身分證每十年換一次），民眾又以為這個很安全，我們是不是其實給他一個很危險的路讓他走向一個懸崖？所以我還是覺得，我們還是要讓人民保持有紙本的自由，保持塑膠卡片的自由。如果你很厲害，像我覺得我很厲害，我願意拿 eID、我願意拿晶片卡，那我也可以（拿這些晶片卡）。那如果不願意拿 eID 的人，那就是想辦法，其實現在內政部已經讓步了，你可以把晶片裡面的資料印出來，他會給你蓋關防，那就是你的資料然後你就是把你的晶片拿去微波、把它燒掉這樣。這是最最最最最後的最下策，你可以這樣子去對抗政府。我可能會幫我阿公阿嬤這樣做，我是講真的不是我開玩笑的。這樣子其實他還是可以去投票。

我當然是不希望大家做到這個程度，我是希望大家好好談，究竟我們什麼樣的晶片卡，應該如何設計，比方說跟德國一樣可以關閉晶片功能，把它變成一個單純塑膠卡。謝謝各位。

廖宜恩（國立中興大學資訊科學與工程學系教授）

大家好我是廖宜恩，今天我要先特別感謝中央研究院法律所李建良所長，以及許多的協辦單位，舉辦這麼一個與臺灣未來至關重要的研討會。我也非常感謝吳介民教授剛剛提供的有關中華電信資拓宏宇跟它的子公司的相關資料，我還記得 2003 年陳水扁政府時，對於中國採取所謂積極開放有效管理的政策，那時候我們就覺得整個臺灣的產業，可能會因著這個政策帶來很大的危機，所以我在中興大學舉辦一個認識中國的研討會，特別邀請吳介民教授發表論文介紹「中國的關係政治學」。在那個年代，許多台灣人對於中國有很大的夢想。但是到 2020 年的這個時候，大家都已體悟到中國帶給臺灣或全世界的，是非常重大的威脅！剛剛吳介民教授提到的案例，我相信大家聽了之後真的會頭皮發麻，今天我們在討論的 eID 問題，可能未來真的會惡夢成真！

今天我就簡單地跟大家分享一下幾個主題，第一個就是我認為現在民進黨政府在推動的國民身分證換發政策，其實是先射箭再畫靶。第二個我要討論的是國家安全視野下的政府資訊系統委外建置與維運的問題，最後是我要給民進黨政府的一些提醒。

為什麼這個政策的推動是先射箭再畫靶，我們看一下這個整個換發的政策的推動，在今年的三月十九號，內政部才公布國民身分證全面換發辦法，這個靶是最後才畫出來的，但是它的生效日期卻追溯到去年的一月一號，原因就是因為去年開始內政部已經射了三支箭，所以今年三月十九號才把靶畫好，這樣剛好都是命中紅心。第一支箭是在去年的四月十九日，內政部公告國巨顧問管理公司得標「新一代國民身分證換發規劃案」，總經費是五百萬元，整個規劃案的執行期間是到去年的十一月三十日，但是這個規劃的成果報告是在今年的二月二十七號才開會討論，三月二十三號才對外公開。關於這個 eID 規劃案成果，內政部其實是沒有與社會對話。

內政部的第二支箭就是在整個規劃案尚未完成之際，最貴的硬體製卡案，已經在去年的六月十四日以限制性招標的方式，委由中央印製廠來承作。昨天我們聽到內政部戶政司的副司長提了很多次中央印製廠，好像是要我們相信中央印製廠應該是可信賴的公司，沒有資安的問題。但是事實上並不是這樣子，這就是我們非常擔心的供應鏈資安問題。中央印製廠在去年九月二十日，公告了「PC 晶片卡及印製設備」採購案，結果是在今年的二月二十一日由東元集團，結合剛剛

王仁甫所提到的 idemia 公司以三十二億八千萬元得標，但是問題是整個 eID 換發規劃都還沒有完成，怎麼知道要買什麼？而且還花了這麼多錢已經先買了！

第三支箭就是在整個規劃報告尚未完成確認前，牽涉資安風險最高的新一代國民身分證換發系統建置與維護案，已經在今年的一月三十日公開招標了，當時預算金額是八億九千萬，整個招標案經過三次的流標，在五月四日第四次招標，經費提高到約十億元，最後在今年的六月二十日決標，由中華電信以十億六百三十八萬元得標。問題是二月二十七日討論規劃案成果報告時，有多位委員針對相關的資安與隱私的問題提出意見，認為應該要修改規劃成果報告，但是事後我們才知道當時因為招標規格已經公告了，所以招標規格書不會依據二月二十七日委員的意見而修改，所以這整個 eID 政策的推動，不是先射箭再畫靶嗎？建議政風處應介入查察是否有涉及違法之行為。

第二個要討論是政府資訊系統的委外建置，我們知道政府許多的資訊系統，絕大部分都是委外建置與維運，也都有委外廠商的工程師常駐在中央與地方政府機關裡面，負責整個資訊系統的維運。剛剛吳介民教授所講的問題，其實是很大的問題，就是維運廠商的管理員，他們擁有這個系統的 super user 的管理權限，所以當這些管理者接觸到機敏資料的時候，是不是有安全的查核機制？各個單位是不是有落實避免內部威脅的風險管理機制？所以我們要建議政府，應該針對所有的委外建置與維運的系統，以及其資安管理機制進行盤點與體檢，以避免機敏資料被竊取。

最後我要給民進黨政府一些提醒，我們知道中國處心積慮要併吞臺灣，對臺滲透也已經相當嚴重，剛剛幾位主講者所提到的都是很真實的案例，所以臺灣的個資與機敏性的資料都是中國積極要獲取的獵物。我們今天看到許多的朋友站出來反對 New eID 倉促上路的這些學者，其實都是過去幾十年和民進黨一起在街頭為台灣民主化共同打拼的戰友，譬如我們的呂忠津教授，他擔任過台灣教授協會會長，在太陽花學運的時候都在立法院裡面陪伴學生。而我擔任台灣教授協會的創會秘書長，當時跟賴中強律師，在廢除懲治叛亂條例的獨台會案與一百行動聯盟的抗爭，都是一起打拼的戰友。所以我們要提醒民進黨政府：民主政治的可貴在於政黨會失去政權，請不要以 eID 開啟通向北京的 T-Road，建議民進黨政府應該以公開、透明、對話、集智的方式來處理 New eID 這個政策的爭議，才有辦法建立數位治理最重要的基石。今天我們以這一個研討會，試圖來和民進黨政府溝通，希望這樣的溝通是有效果的，不要讓許多過去的戰友變成會在街頭上和民進黨政府對抗的情形，我們希望不要有這樣的情況發生，謝謝各位。

呂忠津（國立清華大學電機工程學系教授）

我先講一個這幾年比較困擾的事情，我去擔任外部的審查工作，主辦單位要我簽出席費領據的時候，因為報稅的關係，一定要填身分證字號。填完了隨即跟我要身分證的正、反面影本。我就覺得很奇怪，為什麼你要我的身分證正面反面的影本？若是為申辦較重大的事項，例如貸款，也許尚仍稱此要求與目的相稱，但簽領據為什麼要求？其理由是要查對我填寫的號碼是否正確。這讓我非常震驚，就只是為了身分證號碼的偵錯。各位想一想，身分證的正面有什麼？除了有身分證字號、姓名，也有出生年月日。反面更不得了了，有父母的姓名、配偶的姓名，還有出生地，當然戶籍地址也在反面。可是社會普遍習以為常了。我就拒絕，說根本就沒有道理跟我要這個東西。我更震驚的是，不給就用 e-mail 來要，最後不然說你給正面就好了，很難想像說他們為什麼這麼堅持要身分證的正反面影本。從這個例子來看，今天我們身分證的使用所衍生出來個資被蒐集的問題是多麼地嚴重。

我們今天面對的樣態跟過去不一樣。過去(在尚未數位化的時代)有發生個資被盜取，冒用身分去貸款或做土地買賣等案件。過去要實施這樣的犯罪行為沒有如此容易，成本是蠻高的，因此案件量不是很大。但這幾年為什麼此類案例越來越多？當然跟科技發展有關係。我們今天面對的樣態是什麼？第一是新科技大大提升了資料處理運算能力，提升到你無以想像的地步。第二是網路的連線速度也快了不知道多少倍了。第三是資料儲存的容量也大大提升，也就是說現在用非常少的金錢就可以買到非常大量的儲存空間，我講的是電子式的儲存。在這三者配合之下，資料的蒐集與運用變得相當容易與方便。

因為這樣的改變，大量的個資竊取案件容易發生。可以在非常短的時間內，透過一個高速的資料處理平台，高速的網路連線，將竊取的大量個資儲存在非常便宜的硬碟裡。再以所蒐集的資料，利用強大的資訊處理能力，加上人工智慧機器學習演算法，可以做到剛才沈伯洋教授講的，精準地投放假訊息來影響這個社會。將來精準犯罪、精準威脅，都會出現。而精準犯罪與威脅的尺度，跟過去是不一樣的。因為犯罪成本大量地降低，整個社會為了犯罪或威脅所付出的代價，將遠超過往而且急速地上升。

對執政當局來說，這樣的改變是時尚、是潮流，認為應往這個快速便利的方向去走。再加上這次對武漢肺炎做適當處置的過程中，發現運用先進的科技與網路，做了很多效果好的控制措施，反而認為更是需要加快 eID 的實施，而不去管

程序問題，或者法制是不是完備了。但問題是，貿然實施 eID 將衍生系統性的風險。剛才前面幾位先進所講的都是系統性的風險，從系統建置的硬體的風險，到整個維運系統的風險，都是非常巨大的。

吳介民教授談到中華電信得到了新身分證的建置跟維運系統平台的標案。那我必須揭露我目前擔任中華電信的獨立董事。我今天並沒有代表中華電信，而是代表我個人前來。由於特殊的淵源，中華電信負責很多政府的標案，所產生的風險讓我知道責任重大。我非常感謝吳介民教授的分享以及主辦單位籌辦此研討會，以上是我必須要先聲明的事情。

除了軟硬體系統的風險之外，剛才幾位先進也提到它所造成的社會風險。社會風險是從個人的，比較經濟財物的，一直到透過假訊息精準投放，像剛才沈教授所說的，慢慢地進入了對公共政策的影響。所以它會對我們的民主制度造成一個系統風險。所有這種不管是個人風險或是在民主制度裡面造成風險，當然就會造成國安的風險。所以在科技的浪潮下，反而要往另外一個方向思考，就是不要來增加身分證的利用，而是反過來要來限縮、要來窄化、要單純化身分證的使用。要以立法明文規範，什麼樣的場合才能使用身分證，而不能再出現類似我剛開始講的時候，那種濫用身分證而衍生個資蒐集的風險。

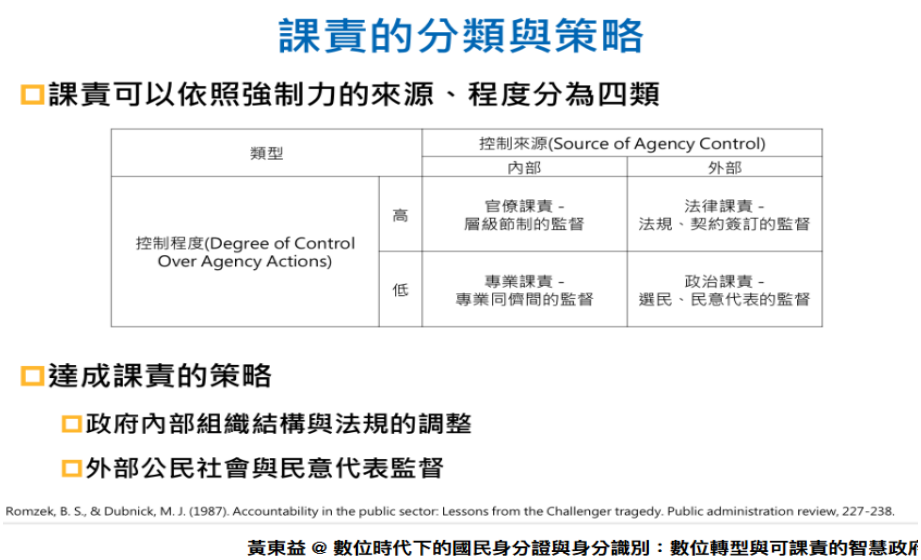
以目前所設計的 eID，它前面一、二區裡面的資料都是沒有加密的，可以很容易拿取，類似於我們現在的紙本身分證，且有過之，比如說它放了一個高解析度的照片，這使得資安風險更高。所以我們要反向思考，將來如果真的要實施這個 eID 的時候，那是不是裡面的資料反而要再削減，讓身分證字號類似美國的社會安全碼(social security number)作為報稅、作為國家公權力機關基本運作所需即可，而不要再涉入商業或是其他的行為。尤其在今天的數位時代，有很多的方式可做身分認證，就是說利用分散的方法來確認個人的身分。分散式的身分認證才是最安全的，也是降低系統風險的最好方法。我們從所舉的例子以及在這個場合的討論中可以了解，身分證施行的制度跟國家安全是息息相關的，我們今天貿然踏出去了，要挽救回來不是說不可能，但是要承擔多大的風險？付出的社會成本有多高？所以我在此呼籲，未來如果我們有這個修法的機會時候，應該嚴格的把目前身分證的使用，單純化、限制化、窄化，謝謝。

高嘉良（g0v.tw 台灣零時政府社群共同發起人）

今天這個場次的題目「數位轉型與可課責的智慧政府」真的是很大的題目，我的與談大概主要著重在「課責」這個議題上面。這兩天的議程中，課責這個議題其實有蠻多不同層次意涵，我先把它稍微分類，一個是「特定議題的課責」，例如 eID 或是 T-Road，如果真的實施的話，這個系統本身的課責是其中之一；再來是數位政府相關的議題，包括 eID 跟 T-Road 這個「政策形成、流程的課責」。為什麼這方面的課責重要呢？因為數位化的一個特點，就是把所有風險，包括安全、隱私的風險都放大了。例如，社會中本來就有假消息，大家會耳語相傳假消息，會有謠言（rumor）的傳遞，可是在數位化的社會中，這可能會變成所謂的「運算宣傳」(computational propaganda)，也就是說，可以用機器人來做大規模假消息攻擊，這個風險跟耳語傳遞假消息是不一樣的，數位社會中機器人傳遞把假消息的風險整個放大了。所以，任何智慧政府或是數位化流程裡面，我們可能要重新去檢視並評估風險，以及探究政策形成的過程中，是否存在可課責性。

再者，一般化整體政府決策流程之課責，也就是跨議題、法制化的課責流程。目前大概只有行政程序法中有「得召開公聽會」之規定，但也沒有說一定要召開，僅在於特定議題，像是環保或都市更新程序有某程度審議流程之規範。那麼，數位化的這些基礎建設，是不是也應該有類似的流程來做通盤的程序規制？這個議題非常重要是因為，大家搜尋一下就會發現，在座有幾位 20 年前就已經在討論晶片身分證的議題（國民卡），何老師從頭髮黑關心這個議題直到頭髮白，我們必須要為未來 20 年的數位化發展做好必需的基礎建設。

借用黃老師關於課責的分類，分為這四種，這四個象限（詳見下圖）：



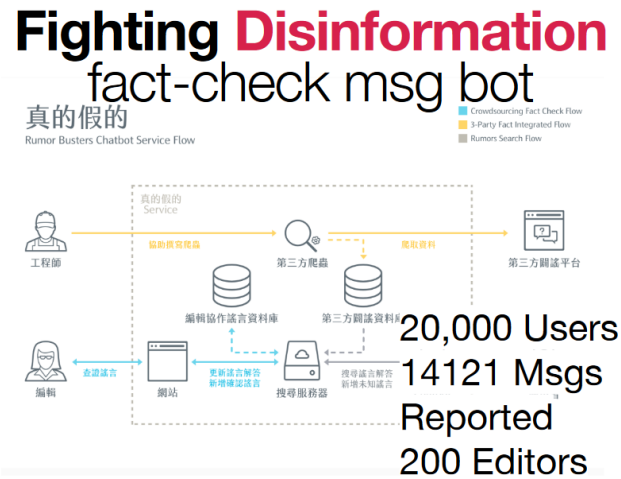
假設現在回到 eID 這個議題，它有沒有左上角的內部「官僚課責監督」？可能有，也可能沒有。我們已經經過了三次的政黨輪替，這項爭議性極高的政策，依然持續被推進中，所以顯然沒有辦法透過內部官僚監督來達到課責的目的。那，外部「法律課責」？昨天有蠻多關於法規的議題的討論，也就是在問：「為什麼不先制定完備的法規之後再上路？」國發會也提到，目前各個資料的主管機關在管理上是破碎化的，法規破碎化然而依舊硬是推行上路，因此顯然也沒辦法透過法規制定達到課責要求；再看表格左下角，「專業課責」，這基本上就是我們今天在做的事情。但是，以 eID 這個議題來講，不覺得有點晚嗎？在 2017 年的時候，黃老師有幫忙主持過 eID 的公民審議會議，這個事情在整體的流程裡面我覺得非常重要。剛才林次長也提到說，除了這個核心價值之外，整體的這個流程是什麼？

如果是這樣子的話，我們其實只能回到右下角的「政治課責」，也就是說如何做到「外部公民社會與民意代表監督」？假設是 eID 這個政策，要如何做？但最後我們還是希望可以透過外部政治課責來達到法治、法規層面的課責流程。

談到課責，各位可以參考《Accountability 101》。又，今天的議程上面有看到若干政府單位受邀但不克出席，不確定是不克出席還是不想出席。但，「課責」在香港似是翻譯成「問責」，就是說人家問你要出席、要來回答，這第一件事。第二個，剛才提到 2017 年的 eID 公民審議會議（目前只能從 web archive 上面找到 Wayback Machine 裡面關於 eID 公民審議會議的存檔資料，在內政部網站，卻沒有辦法找到過去的審議結果），在該會議中，有許多民間專家提出很多議題及討論。我覺得這才是政策推動的正常程序。踐行程序之後，eID 政策真的要上路實施的時候，要告訴大家過去審議程序中的爭議點，以及目前的評估程序及結果為何，是風險很小、一定程度地可以容忍？然而，目前在這兩天討論中，幾位先進或是政府內部報告內容，看起來比較是報喜不報憂的情況，在在表示：「我們這個都很好、很方便、我們會注意資安」。但是實際有風險的時候、風險被放大的時候，我們要怎麼應對？我覺得政府單位沒有回答這些問題。這就讓我想到，g0v 零時政府在 2012 年發起的時候，當時有一個非常有名的國發會廣告叫做「經濟動能推升方案」，就是一個「政府說：你們不用懂太多，就是交給我們就對了」的政策廣告，而我覺得現在政府 eID 政策的推動也有這種傾向。

所以，到底如何做到「外部政治課責」——也就是從公民發動、實際有效的課責？g0v 零時政府有一個蠻久的專案叫做「政治獻金數位化」。最早政治獻金會計報告只能向監察院申請查詢，必須且只能憑身份證去影印，不能攜出數位檔案。所以，g0v 的黑客松就揪集了許多人，每天去印，之後再把它數位化。我們

刻意不用一些 OCR 自動辨識系統，而是把它變成一個「文字遊戲」，分格之後以打字輸入的方式數位化，大概 30 萬筆資料，在一天內有將近一萬人參與。三年後呢，你可以看到像這張圖（見投影片）是鏡傳媒做的，以相同的模式做出來的資料分析。另外，今年監察院政治獻金數位化的查詢系統也真的上線。這就是剛才講的 cycle，從外部性問責、課責去促進法規的改變，以及整個行政體系的改變。另舉一例，面對假消息這件事情，其實在民間就有「真的假的 Service」(Rumor Busters Chatbot Service Flow)這類的機器人試圖去解決這樣的問題。



因此，將視角拉回今天的議題來看，我們到底能夠做什麼事情，才能夠讓這個 cycle、外部的力量來影響這個歷經三次政黨輪替都沒有辦法動搖的「我們一定要有 eID」的爭議性政策？我把它稱做 Grass-root Accountability。就有點像剛才政治獻金那種作法。唐鳳政委在講說，政府對待假消息的方法是 Humour over Rumour，那如果把現在政府跟民間尚未有足夠充分溝通的 eID 的跟 T-Road 政策，當作一種 Propaganda 或是 Rumour，我們要怎麼樣用 Humour 與之抗衡呢？首先我想知道，在場會跟唐鳳一樣，在 eID 推行之後真的都去辦兩張卡的，可以舉個手嗎？Anyway，我覺得這個就是議題，大家可以在 social media 等地方開始問朋友：「欸，唐鳳都這樣子了耶，你覺得這個是不是有疑慮阿？」那另外，我不知道有沒有錯誤引用？昨天潘處長說可能不會把想把 eID 帶在身上，因為覺得可能會有一些風險。我認為這都是讓民眾可以從自己身邊開始開啟對此議題的對話及討論。當我們講到外部性公民力量的政治課責，就一定要有足夠強大的公民社會，而台灣不管是口罩地圖，或是當有類似 318 學運這種大家覺得是一個災害事件發生的時候，台灣社會的動員能量是非常非常強的，我們必須讓這整個社會

的認知(awareness)提升，讓公民社會認知到，政府所推動的政策，確實有風險、也真的正在推行中。

最後，剛剛講到這 20 年來，法治的 consultation process 好像並沒有發揮其功能，也就是說，政府可以吃一個審議自助餐，我喜歡的時候就開審議會，似乎有落實審議民主，而不喜歡的時候就直接推行政策。基本上，這個事情我們必須要從長遠的角度來講，如同黃老師剛剛所講，假設是從公民社會長遠健全發展的角度來講，我們必須要讓這件事情發生。那我自己的話我會做什麼呢？前陣子跟一個朋友聊天，他說討論這個議題的這個學者其實就是 20 年前討論（國民卡）的同一批人，大家真的很辛苦，年輕人一定要做點什麼。我就想說，我們如何讓更多人知道這個議題，才能夠促進討論。我非常相信昨天潘處長講的，以政府的角度出發，推動數位政府、智慧政府相關政策，絕對是以善意、便民為目標，但這中間有很多風險，必須經過審慎討論，若沒有經過公民社會足夠討論，其實很難去推動「真正有效的 consultation」。因此，我今年底會做一個藝術展覽，預計呈現 2030 年的 dystopian，也就是「反烏托邦」情境：所有人都已經持有數位身份證了，然後你可能突然就被連署了一個你不支持的公投，或者是你的個資被拿去做什麼事情你卻不知道，用遊戲的方式呈現這些可能性。這個展覽主要目的還是推動大家來討論這個議題。這個議題其實已經箭在弦上，現在討論都已經太晚了，但是我們就是要開始做一點什麼。你想要做什麼來改善這個狀況嗎？可以到 g0v 的 slack: join.g0v.tw，有 eID channel，謝謝大家。

郭耀煌 （國立成功大學資訊工程學系暨研究所　特聘教授
數位生活科技研發中心　主任）

要談 eID 政策及國家數位轉型，我想先從目前幾個社會現象談起；最近政府推出三倍券，民眾購買紙本券數量完勝數位券，據統計比數是九比一，也就是大家還是比較傾向購買紙本券，但還是拿健保卡去預購，因此可以看到一個現象是原本的專用卡有變成通用卡的傾向；再者，我想到高速公路的 ETC 收費系統，其實 eTag 也可算是身分辨識工具的一種。因為要自費安裝，因此剛開始推動時，很多人不願意安裝。後來變通的方法是利用影像辨識技術，辨識車牌號碼後就可以向民眾收取通行費。當時包括遠傳電通、警政單位都希望利用 eTag 做許多加值運用，但因社會有所疑慮，最後只能用於收取高速公路通行規費。另外，我家前幾年引進智慧門禁系統，可以指紋辨識方式解鎖，但指紋辨識常常不靈光，而且容易受到環境光影的影響，很快地就被我多數家人放棄，而只用輸入密碼的方式解鎖開門。但是，最近討論的問題變成：輸入密碼時是否應該用手遮住以免被他人看到？由此可知，最先進的科技利用有時還是需要用最原始的方法來保護隱私。這些現象讓我們知道，其實科技的導入，不單純是增進便利性的問題，也不單純是已盡力做加密保護就足夠。事實上，有很多更複雜的社會、使用者行為(user behavior)因素，我認為在導入新的科技工具時，都必須納入政策施行的考量中。

因此，對目前正在推行的 eID 政策就有幾個提問。不過，第一個提問並不是單純針對 eID 而有的問題，因為包含 eTag、民生公共物聯網等不同的科技應用範疇皆可能有身分辨識的問題。我想問的就是：智慧政府建置、萬物聯網之後，應有什麼樣的身分辨識、身分管理政策？個人認為身分證具有 root identity 性質，除此之外，每個人還可以有其他的身分辨識方式，並且避免所有應用或服務都以 root identity 作為接取利用該服務的鑰匙，因為這樣終究是有風險的。在萬物聯網的時代，個人應有各式各樣 identity 呈現的方式，這是第一個要思考的問題。

第二是「eID 結合自然人憑證讓民眾可以藉以接取政府服務」的課題，目前，內政部談到可用自然人憑證申請的服務有三，一是公務，一是金融，另一個是醫療。金融跟醫療服務多數是涉及民間經營的，eID 將來可以用來申請哪些服務？適用範圍如何？是除了政府服務之外，委由民間提供或民間經營的金融或醫療服務也都可以適用嗎？如何規範？這點似乎在目前公開的規劃文件中，並不清楚。

再者，依據網路上的公開資料，內政部將 eID 定性為「推動智慧政府關鍵的鑰匙」，但其理由何在？關鍵性何在？是否有配套措施？這些也應該告訴國民。

所有科技工具都無法保證百分之百的安全性，必定有風險。那麼，目前的風險管控及課責機制如何？國民都了解嗎？內政部的回應是，依個資法、資通安全管理法、電子簽章法，即可因應 eID 所帶來的法制挑戰。但據我所知，電子簽章法有很多排除適用的地方，目前法律規範是否周延，仍有疑問。雖然內政部及國發會皆提到，為因應 GDPR 規定下適足性認定之要求，將進行個資法修正，並且討論個資保護專責機關之設立，其具體進程以及與 eID 政策推行之搭配關係如何，一樣是不清楚的。另外，今年四月份內政部發布新聞稿，提到會進行國民身分證及戶口名簿製發相片影像檔建置管理辦法的修正工作，但其進度如何？顯而易見的，此辦法跟 eID 的推動有很關鍵的關聯，因為要製發 eID，檔案格式跟傳統身分證的格式可能都不同，此辦法若尚未修正，推行 eID，會不會有問題？這都要注意。

如果 eID 是政府推動數位轉型重要的關鍵政策，與智慧政府的建置息息相關。那麼，討論 eID 的同時，就應該要問：政府數位轉型的目的為何？參考美國數位政策辦公室(Office of Digital Strategy, ODS)的任務內容，台灣政府數位轉型可以下述幾點為目標：第一點，用數位工具拉近政府跟人民的關係，第二點是用數位工具以優化人民的生活方式，第三點是增進公民權、落實民主的意涵。eID 如果是打開智慧政府的關鍵鑰匙，政府應該更具體的告訴人民，以 eID 來驅動的智慧政府藍圖跟進程，且告訴我們 eID 對於上述三個目標有什麼關鍵性的影響，不應該是用一個新的載具來做身分呈現而已，它應該要有更積極的意義。

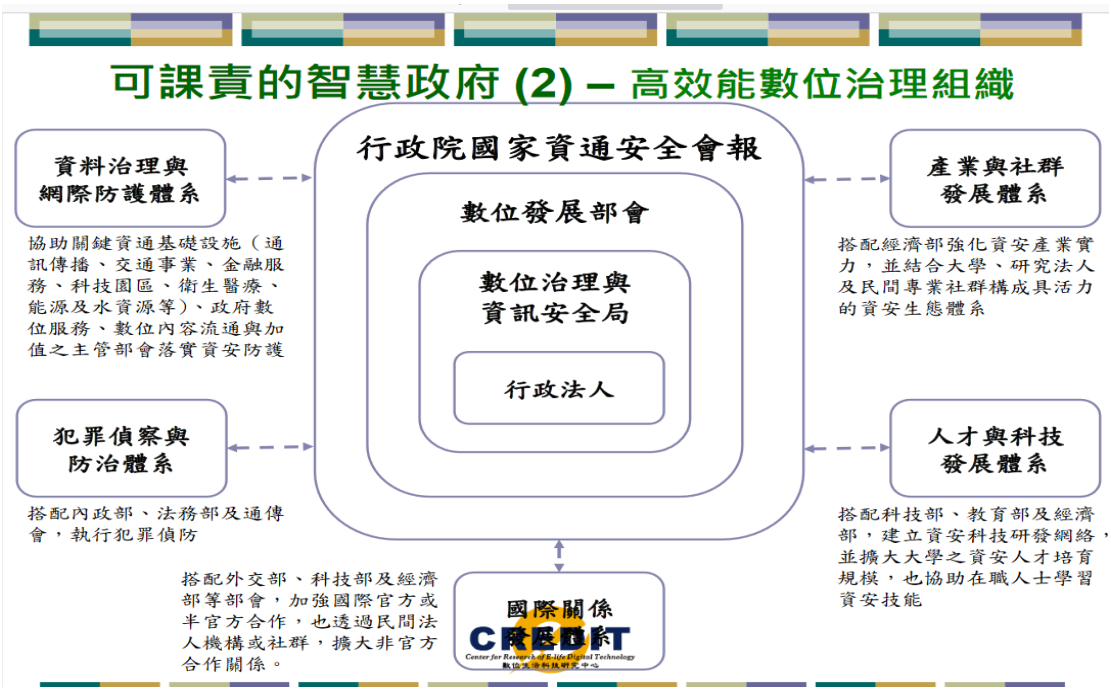
我認為，政府數位轉型應該有幾個核心價值。第一個當然是「民眾為本」；eID 的推動有沒有兼顧不同價值觀、不同使用習慣的國民之需求？第二，政府數位轉型必須提昇人民的信賴感。數位轉型目的之一是提升政府的效能，政府推行 eID、告訴國民說：「將來你用 eID 很可以很便捷地獲得政府提供給你的服務」，但問題是如何讓國民信賴？信賴是非常重要的；第三點，民主深化；透過數位轉型、eID 可以對深化民主有什麼貢獻？我們要不要跟國民講清楚？我過去在行政院時參與很多智慧政府服務的討論，希望推動跨部會把相關服務串起來成為一條龍的服務，那 eID 在這種跨界串連的服務，可以產生什麼積極性的作用？這也必須要談，人民才知道 eID 的正面價值；另也要告訴國民，會採行什麼樣的措施或政策設計，同時發揮 eID 的正面價值，又得以保障每一個人的個資主體之權利、尊重每一個人的使用習慣，這點非常重要。

因此，重點不在是否要推動 eID，eID 是有其正面價值，重點是如何做風險及損害的管控？這就涉及政府的「可信賴性」。

我們很難告訴國民說：「你們就相信我就好，一切安全」，因為過去社會對政府的信賴還沒有到那個程度，所以政府可信賴性的建立很重要。而且，我建議

不要只針對 eID 做風險評估，必須從智慧政府推動的整體規劃來看，因為我們今天所討論的議題，將來在非 eID 的範疇可能也都會碰到。而整體來看，「可信賴的智慧政府」有幾個重點基礎：第一，智慧政府服務的品質、service level 到什麼程度？第二，目前 national cybersecurity 的防護能力現在是否被國民信任？第三，資料治理的落實情形如何？資料治理不單純是資料開放的議題而已，它有更多需要討論的層面；那當然還有第四點，隱私保護。這些都必須對國民有充分的說明及溝通。

智慧政府的推動，另外也要問的是，台灣有沒有一個高效能數位治理組織？當前政府的政見之一，就是要成立數位發展部會，組織設計上應有一個專責機構負起數位治理跟資訊安全的責任，並且做跨部會的整合協調工作。以下這張數位發展部會之架構圖為我個人的意見，不是政府的立場，提供諸位參考。



智慧政府所不可或缺的，還有「完備可行的法制跟配套措施」、「可信賴且獲落實的作業準則」，以及「透明而積極的社會溝通」。韓國今年 (2020) 修訂了數據三法：個人資訊保護法、信用資訊法、資訊通信網法，台灣呢？配合 eID、智慧政府的推動，準備了什麼？它整個修法的進程是什麼？談到「可信賴」，隱私、透明、公平、穩健跟可課責性很重要。歐盟晚近公布了《人工智慧作業倫理準則》，也強調了透明性、隱私性、公平性。為什麼？因為，談智慧政府不止是身分辨識的問題，將來還會用很多國民的資料來做分析、來做智慧政府服務。是以，將來相關的個資蒐集處理、利用等行為，勢必要符合相關倫理準則，而且，

這個倫理準則之內容，必須是國民可以接受的。

既然談智慧政府，一定也需要持續的服務創新，包含：「流程改善」、「體驗創新」、「資料加值」、「品質保證：可利用性(availability)、可靠性(reliability)、安全性(security)」、「普遍可近用性(universal access)」等。我要特別強調的是，最後一點「普遍可近用性」，也就是智慧政府提供服務，不能有歧視，應有各種接取政府服務的方式，而不宜只以 eID 作為近用的唯一途徑，這是智慧政府應該有的原則。

最後，快捷便利跟安全可靠之間，其實涉及不同價值的衡量跟選擇，我個人一直在想是不是可以有更多元的選擇？有比較長的適應期？這是很重要的。另外，我們談可信賴度、談可課責性，這兩點是推動 eID 及智慧政府相當關鍵的要素。重點是，政府跟社會之間的互信度，在台灣，其實一直都不是那麼強，所以我們的社會溝通是不是要更具有說服力才對？這是我的想法。最後要強調的就是，我們現在不能只談資安或各自獨立去談這些議題，網路安全(cybersecurity)、資料安全(data safety)跟隱私保護(privacy protection)，這三者是應該視為整體來檢視，如此，要推動智慧政府才會有比較踏實的基礎。

附件四

研討會貴賓、主持人致詞

致詞

黃進興

中央研究院　特聘研究員兼副院長

李所長，各位女士，各位先生，各位貴賓，各位同仁，大家好。今天很高興受到主辦單位的邀約，來為「數位時代下的國民身分證與身分識別研討會」簡單講幾句話。自 70 多年前我國發行第一張身分證，到了今天從辦理各種行政手續，到銀行開戶、公司求職、飯店住宿等民間事務，身分證已經與大家的日常生活息息相關，可說是無所不在。原本預計今年 10 月要進入第 6 次身分證的全面換發，對在場的所有人而言，包含我本人在內，都可以說是一件大事。

事實上，若我們回顧歷史，可以發現身分證的使用，由來已久。其實，在唐代就有所謂魚符（鮮魚的魚，符咒的符），為官員所用，魚符上刻有官員的姓名，及所屬與品級，作為公務身分識別之用。明代時則擴展到各階層民眾所用，稱為牙牌，其上刻有姓名、履歷，職務等，以作為身分識別之用。由此看來，在古代即有隨身攜帶的身分證，除了方便國家確認持有者的身分，區別我群及外人，以及決定法律地位，與權利義務外，基本上沒有其他的作用。這種以國家掌握人口為中心而使用身分證的傳統，一直延續到二戰時代都沒有變化。直到民國 31 年，戴笠呈給先總統蔣中正的報告就表明，隨身攜帶貼有照片的身分證，對戰時維持治安及配給物質的作業而言，非常方便。此外，英國雖然是民主先進國家當中至今仍無國民身分證的例子，但也曾於 1939 年為戰時統治的目的，發行了身分證。

然而，隨著時代的變遷，身分證的使用到現在竟普及到像是申辦會員卡；以及私人間日常生活的廣泛使用，其實跟過去有不小的差距。原本預計於今年 10 月換發第 7 代身分證更是準備朝向數位化，進而邁入一個新的歷史進程。未來身分證數位化之後，凡相關使用記錄變更及各式資料，更容易留在電腦的作業環境上，這對政府與私人企業來說，在發展所謂的大數據時代的人工智慧上，在資料的掌握上，可說是更為便利。但是，這也帶來有別於以往的風險，這種發展是好是壞，端賴大家認真的思考及借重大家的智慧。

為此，我們需要更多關於數位身分證的規劃資訊。因為我想，在場大多數人

都跟我一樣，對這次數位身分證的實際內容與其利弊，都只有相當粗淺的印象。一般人大概只記得，之前新聞簡報上面所說的，卡面的美術設計而已。至於，哪些資訊要留在卡面上，哪些資訊要放到晶片裡面，及更細項的議題仍不太清楚。

有鑒於此，本院法律學研究所與其他院內外協辦單位及專家學者，共同舉辦了今天這場研討會。邀請負責相關事務的行政官員來到這裡，與學界人士、公民團體等，一同對身分證的議題來進行深入而廣泛的討論，希望能讓社會大眾，對於數位身分證這件事情，有更清楚的瞭解。最後，在此預祝研討會圓滿成功，謝謝大家，祝大家平安健康，萬事如意。謝謝！

致詞

陳建仁

中央研究院 院士

中央研究院基因體研究中心 特聘研究員

謝謝建良的介紹，李德財院士、在座的各位貴賓、與會者，大家早安、大家好。很高興能夠接受主辦單位及李德財院士的邀請，我謹代表關注國家自由民主政治未來發展的公民，來參加這場「數位時代下的國民身分證及身份識別研討會」。我在報章雜誌上看到昨天研討會中，各位都是知無不言、言無不盡，看了我也對我們國家當前數位身分證的發展有比較清晰的了解。我們一方面可以體認到政府為了要把這個數位化帶來的好處分享給所有的國民，而且能夠透過更有效的資料交換，達到便民的目的，所以我們能夠透過數據的分析，也能夠優化我們政府決策的品質。但是我們大家對於最近很多的資料外洩事件，及個人隱私保護的議題，都非常的關心。這帶給我反思，在得到便利的過程當中，我們個資及隱私是不是也能夠得到很好的保護？還有個資是不是也要經當事人的同意，才能夠釋出？在民眾有任何憂慮、擔心時，政府是責無旁貸的，一定要好好地溝通。在民主政治的理念當中，最重要的當然就是法治精神，所以我覺得能夠在公開透明的環境下，透過充分了解相關的知識背景，且公民審慎的討論以後再做出決定，我想是最好的方式。

我記得以前在衛生署工作時，那時候我開了兩次審議式公民會議，有一次就是關於代理孕母的議題。雖然現在代理孕母尚未合法化，可是當時我們也是透過公開透明的方式，讓大家有充分的資料來了解後，我們才能夠做出最好的決策，所以當時審議式公民的會議是在有條件下開放代理孕母，但是今天我們還沒有通過這條法律，可見在法律的訂定上我們需要有相當審慎的討論。根據過去的經驗，我們都知道，政府任何的政策一定要得到人民的信賴、人民的支持以後才能夠達到最好的效果，我就以最近 covid-19 的例子來看，在我們一個自由民主開放的國家當中，要實施 covid-19 的防疫而限制了民眾的自由，大家要居家隔離、居家檢疫，或者是自主健康管理，我們一定要全民能夠團結一致才能夠達到這個目標。

而要團結一致達到這個目標，最重要的一個精神就是 transparency，就是透明公開，所有的資訊都一定要知道，所以 CECC 有每一天的疫情說明會，那是在那段期間全民所關注的最強說明會，每一次上網都有兩三萬人，在那樣的情況下政府公開透明地跟大家交換意見，媒體的記者也可以提出各式各樣的問題，在這樣很好的溝通情況下，慢慢地我們的 CECC 就得到人民完全的信賴，它具有專業的權威，更重要的它在決定任何決策的時候，是聆聽人民的需要來設計然後得到最好的結果，所以 CECC 在有充分的公信力，還有充分的專業知識帶領我們大家來做，而人民也就因為這樣能夠來配合政府的各項措施，包括居家檢疫、邊境管制等，還有養成良好的衛生習慣，保持社交距離、避免群聚活動，大家都做得很好，原因是因為有一個良性的循環，政府公開透明，並且願意和民眾一起努力，民眾做得很好以後，疫情就控制得越來越好。

所以我也很盼望這一次的討論會，透過學界還有政府之間充分的交流，大家把心裡的話都講出來，怎麼樣來避免資料的外洩、個資的洩漏，如何來保護隱私權，然後更重要的，自由民主法治國家的目的就是為了保障人權，為了要關懷弱勢。所以在追求數位化的過程當中，要求便民利民的同時，我們也要了解人民所擔心、關懷的是哪些問題。昨天的研討會很精彩，很可惜我沒有辦法參加，可是我希望這個研討會能夠做出一個蠻好的結論讓政府來參考，我相信只有彼此互相能夠有很好的課責機制，然後人民得以進行有很好的、有效的監督的情況下，我們才能夠把所有的施政都做得很好。昨天唐鳳政委也提到，希望能夠成立一個專責的個資保護機關或機構，我覺得這是一個很好的構想，只有在這樣的情況下，政策才能順利推行。

這四年來我從事了很多在大家看來、在改革創新上蠻吃力不討好的工作，如年金改革、婚姻平權、國家人權委員會的設立，甚至最近的 covid-19 防疫政策，即使如此，政府推行政策最重要的就是溝通、溝通、再溝通，當各界提出不同意見時，大家坐下來談、得到共識，那才是政府施政最好的基準。那今天實在是很謝謝我們所有的學者專家大家所提供的意見，中央研究院的任務之一，本來就是要對政府政策提出所謂的政策建議書。過去我參與過新興傳染病防治政策建議書的提出，裡面所建議的許多項目到目前大概只有百分之六十能夠做到，百分之四十還沒有辦法做到，原因就是施政需要時間、需要有更多方面的考量，所以今天學者專家討論之後，我相信相關的法規或辦法未來一定會在立法院、或者在相關單位經過進一步的考量進而實施，無論如何，對話是政策最佳化的開始。

今天看到這麼多人來參加，在 covid-19 這麼盛行的時候，還有這麼多人來關心這件事情，我實在是非常感謝大家。作為一個公民，我很感動也很高興有這麼

多人關心我的權益，在這裡預祝我們今天的研討會都能夠順利圓滿成功，也祝福大家討論的結果能夠綜合起來，寫出一個具體的政策建議讓政府相關單位能夠來參考，這樣作為一個公民的我就會感到是生活在幸福美滿當中，謝謝大家，謝謝。

開場

致詞

李建良

中央研究院法律學研究所　特聘研究員兼所長

黃副院長、李律師、李院士、各位學界先進，還有關心國民身分證及數位時代相關身分識別問題的朋友們，大家早安。首先，歡迎大家參加本場學術研討會。就本所來說，這場研討會可以說是疫情之後第一場大型學術研討會，看到這麼多朋友來參加這個會議，對此由衷地表示感謝。

我們的院長 - 廖院長在中研院 90 週年的時候，曾提出中研院雄心善智、航向未來的願景。其中，在關鍵議題上善盡社會責任，即是非常重要的指標之一，這也是我們作為研究學人念茲在茲的主要任務。本所一直以來在各領域持續地關注社會關鍵議題，提供我們作為研究人員應有的社會責任。我們法律所也為因應數位時代新興科技的發展，成立了資訊法中心，首任中心主任，為邱文聰研究員。資訊法中心這一次特別因應公眾所關心的國民身分證相關議題，舉辦了本場研討會。在此，我首先感謝邱文聰研究員以及他的團隊，讓會議能夠順利舉行。

這場會議依議題共分為 5 個場次，而這 5 個議題之間，其實都是相互關聯的。首先，會議第 1 個場次就是大家所關心的身分證議題。就大家所瞭解，身分證基本上是戶籍制度的延伸，而未來我們的身分證可能會從紙本身分證變成數位（晶片）身分證，第 1 場主要討論的就是可能涉及身分證晶片化及數位化後的議題。那麼隨著身分證的數位化，未來數位身分證的使用上可能會留下許多數位足跡。透過個人的數位足跡，我們個人的形象也將逐建構築出來，我們一般把這個稱為叫剖繪。在數位身分證使用之下，可能會慢慢形成發展為這樣的一個趨勢，這是第 2 場所要討論的。延續前兩場，在第 3 場將聚焦於身分證使用的發展，將來會不會成為所謂的「一卡通」(一卡萬事通)。另一方面，在使用身分證進入所謂政府骨幹的資訊平臺，一卡通的同時我們的資訊將可跨機關分享及大量串聯。

因此，到第 4 場，我們關心的議題就延伸到這樣發展結果，有沒有資訊安全、個人安全、乃至於更廣而及之的國家安全問題，這是我們第 4 場要討論的。那麼最後，我們更提昇到所謂國家圖像的問題。現在，我們自稱為智慧政府。那麼智慧政府到底可不可課責，是我們最後一場，要跟大家分享跟討論的議題。

以上為簡單地跟大家做一個開場，我們今天很高興請到我們的副院長-黃進興副院長，來跟我們致辭。黃副院長是我們人文的大家長，他同時也是知名的歷史學家。他從歷史的觀點其實可以看到，我們今天討論比較具有縱深性的觀點。那麼我們現在就歡迎，黃副院長來跟我們致辭。

最後，我是簡單的做一個結論。剛剛大家都提到釋字第 603 號解釋，第 603 解釋是 2005 年的 9 月 28 號做成的，可以推想進行言詞辯論的時間，大概是現在這個時候。對此，我們大概可以有一種臨場感，就是 15 年前，大家對這個指紋案問題的關心。那如果，李律師還記得的話，我還記得最後結辯時，李律師講了一句話：「現在最大的問題呢，就是，我們其實不太知道問題的嚴重性。」那我想 15 年過了，我發現大家應該都知道這個問題的嚴重性，這是我們最大的進步。

附件五

研討會討論問答紀錄

戶籍管理與身分證的晶片化及數位化

Q&A 紀錄

陳榮祥（資訊業）

我姓陳，陳榮祥，是資訊界出身。請教有關談社會信任那位教授，因觀察到臺灣政治氣氛比較特殊，有時會牽涉到政治問題。那跟政治無關的議題，有可能取樣、調查，都會失真。我們看到高鐵當初要通車的時候，我記得馬英九總統還說他不敢坐，那你看現在，有多少人還沒有搭過高鐵？這是臺灣人民的一個行為現象。另外戴口罩的服從度，也是臺灣人民的一個特色，我們有全世界表現最好的口罩國家隊。還有搭乘臺北市的捷運，民眾排隊禁止飲食的服從行為等。所以，我覺得臺灣人民真的非常的複雜，用國外的調查比較來看臺灣的話，可能會有失真。我的意思是說，有很多好的政策推動初期，可能臺灣人民充滿了不信任，這個我同意，因為臺灣太複雜了，大家對很多的政府政策，都不是非常的信賴。但是，真正做下去了以後，大家又非常的服從，做得非常的好，這是第一個我要表達的。

第二個，要請教剛剛有談到臺灣科技的老師，應該是第二位。臺灣的科技，不管在讀卡機、晶片，或系統設計、管理機制，應該都沒有問題。

這個就牽涉到最後一位律師，在談的，中央研究院能不能扣留你的身分證？這絕對不是戶籍法，或者戶政司的問題，是中央研究院的問題，是執行的問題，這個跟法哪有關嘛？他可以不扣你的身分證，可以用你的名片來換，對不對？

雖然還有很多的疑問，但還是有發言時間的限制。我覺得在科技的發展，美國是因為科技立國鼓勵創意，所以她變得非常的偉大。那臺灣這麼小的國家，沒有特別的資源，如果我們要走在科技的前頭，要怎麼做？各位法律人，也要從科技法律來看國家的發展，謝謝。

謝穎青（亞洲矽谷中心法制長）

謝謝，我是亞洲矽谷中心的法制長謝穎青。想請教內政部的長官，關於 eID 的換發，現在在規劃上面，知道第一階段是要取代紙本的身分證；那第二階段，

是不是將擴及到應其他機關，也可要求民眾使用 eID 在公共服務上？除了公務用途外，未來還有沒有規劃將來會提供民間機構或者是商業發展使用。目前，有人認為 eID 是一個很好的載具，可以供民眾日常生活應用甚至商業應用，那這個是不是也在 eID 的規劃中？三個階段，是不是都包含在我們所關注的 eID 的使用？請內政部回復。

與會民眾

李所長，各位先進大家好。謝謝今天各位主講人和與談人的說明，讓我們知道目前身分證的功能，除了身分證明外，已經到身分辨識的功能。也就說，它應該是已經建立一個身分識別制度，形成人民去經營個人和團體間用來辨識身分的重要文件。那身分證之所以可以辨識個人的個身分，很重要的原因是身分證揭露的個人的身分資料。那，如果說，後續內政部可以強制換發這個 eID 的身分證，那晶片上所能載入的，還有所能夠植入的個人資料，也就是辨識身分、識別個人最重要的文件。

所以，從這邊我們可以知道，這個 eID 身分證的製作，從空白身分證製作就是一個高度公權力的一個行使，因為必須是有公權力的行為，就是一個國家的行為，去製作身分證才有辦法讓人民信賴，也才能夠維護資訊安全，保障人民的個人資料。那我們從戶籍法第 53 條規定可以看出，空白國民身分證的製發是由直轄市或是限制的主管機關印製，如有必要的話，才是由中央主管機關統一印製。也就是說，這是統一印製國民身分證這個行政行為是保留給行政機關行使。但是從目前內政部的招標還有相關的作法等，看起來內政部是把空白身分證的印製，委外給中央印製廠去製作，中央印製廠再去外包給其他的這個廠商製作，甚至，相關的晶片是進口而來的。那，似乎就違反了所謂委託行使公權力。如果行政機關不自己做要去委託私人辦理的話，應該要有法律所授權，或者有法律明文或是法律授權的辦法去做授權。那內政部在沒有這樣的授權之下，直接讓中央印製廠或是再由其他的這個民間機構去承製這樣子的作業、去製作晶片，那會不會從一開始製作晶片的源頭，就被例如植入相關木馬程式，那從硬體安全、系統安全等，從頭就已經遭到破壞，這樣子是不是有違反戶籍法第 53 條相關規定？以上，就教於主講人和內政部副司長。謝謝。

李德財（中央研究院資訊所客座講座）

我是中央研究院資訊所李德財。

剛剛聽鄭副司長提到說，現在的細部規劃還在繼續進行當中，還在調整當中。那這點間接解釋了，我們一直跟那個戶政司要求，希望能夠看到細部規劃書的結案報告，一直拿不到的原因，是因為內政部現在目前還在調整修正中。當然我也聽到，也感受到說，這件事情是一個好事，因為內政部願意聆聽民眾的聲音。把原本在製卡過程即把國民身分證跟自然人憑證兩卡合一的規劃，接受了民眾的建議，將提供民眾選擇權，可以選擇不開啟自然人憑證功能。

我就回到一個問題說，當初你們在進行細部規劃時，硬體招標案已經公告且決標，那個時候的招標規格，都是依照原先的規劃，採兩卡合一的方式建置晶片身分證。那我想要了解的是，對於不希望使用自然人憑證的民眾，戶政司這邊有沒有去了解，若國民身分證功能為供識別之用，那國民身分證加上晶片卡的必要性在哪裡？民眾可不可以要求，我不要一個有晶片的國民身分證，例如維持現在紙本身分證或者是什麼樣不同方式的身分證？那我想再了解，對於晶片自然人憑證沒有需求的民眾，是不是可以不要晶片身分證？這一點，我希望戶政司能不能夠給我們一個回答。當然，我知道戶政司曾說，維持紙本卡跟晶片卡兩卡並行的方式，對於維護體系來講，會增加成本。但是我想，針對這個問題又講到成本，如果提供可以不需要晶片卡這個選擇時，會有多少比重的民眾不需要晶片卡，如果比重很多，是不是就不需要印製晶片卡，那不是會減少更多的印製成本？謝謝。

鄭信偉（內政部戶政司副司長）

所長，各位老師，兩位大律師，剛才有四位關心 New eID 的朋友提出問題。其中有三位，都是提到內政部的事情，所以我想先從李諮委的提問開始，跟大家說明。

當時的規劃是在 eID 裡，有一個自然人憑證區，那個時候的想法是想直接把自然人憑證放在裡面；然後，因為民眾反應的聲音，為了回應民眾的想法，所以，內政部改變原本的規劃，讓民眾自行決定是否要把自然人憑證功能寫入 eID。如果不要自然人憑證區，卡片本身其實還有其他區。當初會把自然人憑證寫入 eID 的目的，是供我們在數位時代做身分識別之用。另外，把晶片放入卡片另一個目的，就是要把身分證版面的一些資訊，放到晶片裡面（例如，放在加密區裡面），這樣做可以把版面個資極小化。如果說不要晶片，這些資料勢必又必須放回版面

上，那版面就會跟現在的紙本身分證一樣。當時是因為考慮到偽造仿冒、甚至個資保護的問題，才採用晶片卡。

所以，我認為要不要自然人憑證，與要不要晶片的議題應該切開來看，eID是否保有自然人憑證功能，我們尊重民眾的選擇，看看他們有沒有需要在網路上做身分識別使用的需求。但是，就個資保護來講，例如加密區裡有父母、配偶的姓名，這些資料還是要放晶片裡來做加密保護。所以說，我們基本上還是會發行有晶片的New eID；至於，自然人憑證功能要不要寫入，由民眾選擇。以上跟李諮委先做簡單的報告。

剛才提到戶籍法53條有關印製的問題，我們現在的身分證的卡，例如紙本身分證的卡與上面的膠膜，我們都是委託給中央印製廠負責處理。因為這張卡，除晶片裡頭的資訊以外，外部的防偽還是很重要，而我們相信中央印製廠的防偽功能。我們要減少偽造仿冒的可能，保護每個民眾的權益，因此我們要做好避免及減少偽仿冒的情形。至於中央印製廠將這部分委外的事情，是我們要引進國外的技術進來，畢竟這邊以往沒有發行過一個晶片身分證，而國外有經驗。在晶片的部分，剛才有跟各位報告是台積電的晶圓，還會在中央印製廠那邊經過一些細部的流程，好像是洗卡，然後會在外面都不能進入的密閉空間裡產製晶片身分證。我們就是因為考慮到安全，因此，才委由中央印製廠來處理這個部分。

然後，有一位先生提問，當紙本身分證變成晶片身分證，會有哪些機關需要去讀取晶片裡面的資料？這部分我們會去看有哪些機關需要讀取晶片的資料，如果有機關提出申請，我們會請他們去申請所謂的secure API來讀取晶片的資訊。但是，晶片裡頭的資料，我們不僅是分區加密保護，而且就算是加密區裡資料，也可以指定要看那些資料。例如，有機關只需要看父母的資料，他就不能看到配偶的資料。因為有些地方因為業務上需要知道父母或是配偶的資料，因此，我們就有設計，依業務需求需要甚麼，我只給你什麼。我們不會把所有的個資，全部開給那個機關或者民間機構，以上簡要的說明。

邱文聰（中央研究院法律學研究所研究員）

我簡單回應剛剛幾位的提問。我必須先澄清剛剛李念祖律師提到的一個區分，就是證明及辨識。抱歉，其實是我沒有說清楚，因為其實在35年時，就已經使用辨識這個字眼，那時就已經存在了。當時戶籍法就已經說身分證的功能就是供身分辨識之用，然後效用及於全國各地，然後不用隨地換發。後續文字稍有改變，但整個制度的精神並沒有改變。

但是，最大的問題其實是出在這部戶籍法，當初並沒有想像到本來身分辨識功能，應該僅限於規範國家跟人民間的關係，所以法律的規範範疇只有這樣，但是身分證實際的運用，實已超越了這個範疇，但相關的法律卻沒有跟上來，進一步去規範其他的私人用途。比如說，剛剛林律師提到，他在中研院門口被要求要留置身分證實體，今天如果我們換一個情境，他不是被要求留置這個身分證實體，而是要求抄錄他的身分證資料，才准讓他進來，或者像各位可能最近因為疫情關係，到餐廳會要求說出示身分證，我要登錄你的相關資料才可以進來，在這些情況下那到底是可以做還是不行？按照現在內政部說法是說，這些個資法都有規定。可是，我要強調的是，有關這種一般私人間的身分證使用，在德國、日本的法律其實都有非常清楚詳盡的規範。德國連影印身分證都有規範，身分證可以影印，但只限本人使用影本，如果是第三人使用影本，不管是行使的人或者接受的人，都是違法的。德國法針對公務機關以外使用晶片身分證的情形，通通必須要先取得事前的授權許可。所以，不是說在中研院在門口要求拿出身分證，就可以隨便抄錄；或是餐廳要求插卡，餐廳就可以看你的身分證。每一個身分證的使用需經過事前的許可，同時，什麼情況是可以把資料留存下來？所以，驗卡是一回事，辨識是一回事，但是把資料留下來，甚至進行串聯是另外一回事。

德國法律很清楚地規定，不能使用卡片上面的證號進行資料串聯，這在日本的 My Number 也是一樣，日本只限於三種用途：稅的用途、社福用途跟防災對策的用途，才可以使用 My Number。相較於臺灣，我們現在都沒有規範，卻非常廣泛的使用，只說這些都推給個資法規範，或者說這是執行面的問題。就是因為沒有清楚規範，且欠缺後端的管制，所以才會出現非常多的這種私人使用。所以，我要強調的是，國外有專法並不是疊床架屋，因為德國也有訴願法、行政程序相關法律等，那為什麼還需要專法，原因就在於說有針對這種非常廣泛的使用，做比較細緻的一個規範需求。那再來就是剛剛提到，因為內政部當初設定國民身分證的用途為可攜性及可識別之用，內政部說從紙本到晶片並沒有改變格式。那我要反問，國外難道從紙本到晶片片不是也符合這兩個要件嗎，那為什麼還需要專法呢？所以重點還是在於，專法必須針對數位資料後續的蒐集處理利用有更為詳盡的規範。

至於，有關身分證的相片問題，剛剛副司長提到，相片是臨櫃驗證身分使用。那如果是臨櫃要驗證身分，還要看相片的話，那為什麼還需要記載，甚至可以提供在虛擬世界使用呢？愛沙尼亞就非常強調這一點，她說他們的相片，不會存在晶片上面供虛擬環境使用。為什麼呢？因為虛擬世界，不需要使用相片做身分認證，確實只有臨櫃才有這個需要。

既然如此，愛沙尼亞為什麼不會變成是我們的例子呢？我們反而說，我們學愛沙尼亞，但是在相片這件事情上面，卻又跟愛沙尼亞有所不同？那我想拉拉雜雜，先講到這邊好了，可能會後還有機會，我們再做其他的討論。謝謝。

李育杰（中央研究院資訊科技創新研究中心研究員）

好，其實副司長相當辛苦的，剛提到 2000 萬筆個資外洩的事情，內政部的反應，讓大家可以感受到，每個人都說不是我，因為格式不一樣。那請各位想一下，如果我今天偷到一些資料，然後我把繁體變簡體，那就不是從內政部出去的？我並不是說，這個一定是內政部外洩的，我只是要告訴各位，當資料外洩的時候，到底誰該負責，很多單位都會自動去撇清責任。

另外一個我比較擔心的就是全民都有 eID，我們有 2300 多萬，甚至 2400 萬，這麼大的一個 base，基本上幾乎可以斷定就是會有些資安事件發生。

那我剛剛提到的，未來量子電腦對現行所有的密碼都會有問題，但是其實不只是副司長這樣回應我，也很多人有相同的看法。但我要問的是，為什麼我們明明可以選擇直接用後量子密碼學的系統，而我們現在卻要 create 這麼大的風險用現行的密碼？為什麼我們要說，反正別人也可能有問題，我擔心什麼？我想面對 risk 應該不是這種態度，我簡單報告到這裡。

吳齊殷（中央研究院社會學研究所研究員兼副所長）

剛剛有人提到怎麼拿愛沙尼亞和臺灣不同的調查資料去比較社會信任的問題，我這樣呈現並不是真的要做這兩個國家的比較，而是把它當成是一個例子提出來，供大家一起來思考社會信任的問題。我覺得您剛剛提出有關臺灣是一個典型的、非常複雜、異質性相當高的社會，反而比較重要。這一個複雜性，可能來自於民眾間的政治信仰，使得其基本價值頗有差異，這個我們都可以互相尊重，來想這個問題。但重要的是說，您剛才也有提到臺灣口罩國家隊政策推行的成功，反應出來的是，臺灣人民對政府似乎也不是那樣的缺乏信任感。可是我要提的是說，在一個越複雜的社會底下，信任機制的建立是非常辛苦的，可是，要損壞也是非常的快。也就是說，當人民對口罩國家隊的表現給予很高度肯定，可是接下來行政院推的三倍券，爭議可能會很大。我的意思是，我們對某一項政策的信任感很難擴及到其他政策信任感，所以，政府不應該認為在某項政策的成功，就保證同樣的態度去推後續其他的政策，應該就會得到同樣的效果，人民對政府的政策推動已經開始有能力分化，且會對每一項政策都會一一檢驗。我在這要特別強

調提醒的是，在一個複雜社會好不容易建立起來的社會信任，可能會因為後續其他政策推行的疏忽，把好不容易的社會信任又毀壞掉了，那是個非常可惜的。好，以上是一點淺見。

李念祖（私立東吳大學法學院暨法律學系兼任教授／總統府第一至五屆人權諮詢委員會諮詢委員）

就剛剛文聰講的證明與辨識，其實我最主要是要說，身分證的目的究竟是證明或辨識，是非常重要的關鍵，因為這涉及誰是主體。當身分證持證人是主體時，他可以在他需要證明自己的時候，把身分證拿出來證明；而需要使用身分證用來辨識時，主體就不是持證人，而是辨識持證人的對方。那現在是政府要辨識持證人時，他就一定會提出要求出示證件，所以關鍵是你到底有沒有被要求一定要出示身分證？這個才是真正我想要講的問題，至於，戶籍法法條用語最早是證明還是辨識，我覺得那個其實是其次的問題。謝謝。

林煜騰（圓矩法律事務所律師／民間司法改革基金會執行委員／台權會籌措民間反 eID 律師團召集人）

我今天在這裡提到中研院押身分證換停車證的例子，其實是要強調現在個人資料的運用，基本上很多都是私人機關要求人民主動交換或提供資料。像 Facebook 或其他社群媒體，都是非常類似。但是，數位身分證跟前面案子不一樣的地方是：今天內政部想要嘗試幫這些廣泛的私人機構架設好一個舞臺，讓這一些私人機構可以更輕易的去取得和應用我們的個人資料，但是卻沒有任何的法律規範跟規則，去限制說他們的使用。甚至說現在唯一的規定，也變成只是訓示規定而已，這樣對我們的個資運用的風險是相當大的。所以，我才會希望政府應該要好好審慎地考慮這個問題，並且要讓自己的法律規範更完備，去因應接下來的資訊應用問題。

數位足跡、剖繪與監控

Q&A 紀錄

何建明（中央研究院資訊科學研究所研究員）

我有幾個問題想請問唐鳳政委，還有請李世德參事補充。我們期待政委在這樣的一個 position，能夠把你現在相信是對的事情實踐出來。我們聽到您今天談到的一些事情，到底我們能夠有什麼樣實際的作為往下再做下去。

第一個問題，是剛才明誼問的很多已經發生的問題，那這裡面有多少是政府可能做得到，或完全不想去做，只用口頭 guarantee 不會怎麼樣。

那第二個是有關 eID 的問題，只要有一個一般的讀卡機就可讀取 eID 那幾區的資料，那很明顯地 eID 的設計，是要鼓勵各方努力蒐集個人資料，包含政府機關、及民間企業等等。民間企業的話，其實有時候讓人家覺得很無奈，我錢給你就好，你要我的資料幹嘛？尤其是今天在民間企業交易如果必須用我 ID，即便 ID 不一定是實名的，但如果 ID 的資料與現在政府的 eID 資料連在一起之後，我就不只是給你孫中山這或幾位小朋友而已，而是我的 ID 相關資料被拿走且被連結在一起了。那如果整個 eID 變成公、私部門用來蒐集個資的工具時，政委您這個 position 可以做什麼事情，能不能擋得下來？

再來一個就是，發生公務人員的個資外洩、2000 萬戶政個資在暗網販售的事情，政府只撇清說不關他的事，推說格式明顯不同，都不是從政府洩漏的，一定都是民間蒐集整理後拋出去販售的。好，對這些事情我有幾個問題請問，第一個是說，那政府要不要積極地去找出來到底是誰幹的？第二，我們有沒有法律可以加以追訴及課以責任。第三，政府能不能更有擔當說，既然民眾的個資都已經流落在外，比方說，將來我們是不是有可能改名字、改生日、改身分證字號等等，甚至於將來是不是一個人可以有很多個身分證字號？

你剛剛提到，我們不要等到大的事情發生，再來解決問題，可是我們現在是真正大條的事情已經發生了，可是民眾不在乎，政府也不在乎。我不曉得政委您怎樣對於這些事情有沒有一些更好的因應或看法。以上幾個問題請教。

邱伊翎（國際特赦組織臺灣分會）

國際特赦組織臺灣分會邱伊翎第一次發言。其實國際特赦組織臺灣分會也有加入台灣人權促進會，及開放文化基金會所發起的連署。我們認為說，在還沒有專法，也沒有獨立的個人資料專責機構之前，甚至我們其實還沒有看到整個數位身分證計畫的必要性，以及隱私權相關的風險評估之前，我們認同所有 eID 相關的計畫，都應該要暫停推動。

那其實國際特赦組織之前也針對人臉辨識的部分也有發表聲明，認為說政府公部門或私人機構，如果在沒有辦法確保人臉辨識的技術，不會有隱私疑慮，或者說不會用來監控，其實也應該要全面暫停使用。

其實剛聽到唐鳳政委有連署 WhyID 的連署，當然也是非常高興。剛剛台權會提到的 WhyID 文件所指出的各種問題之外，其實也提出很具體的建議，認為政府在推動數位身分證計畫時，其實應該要做評估，而且如有必要應暫緩推動。

所以，我也想跟唐鳳政委，以及國發會確認，在臺灣還沒有關於晶片身分證或數位身分證相關的專法前、還沒有獨立個人資料專責機關前，也沒有看到任何一份對於這個計畫的隱私風險，人權評估之前，政委和參事兩位認為政府應該要繼續推動下去嗎？還是應該要暫緩？ 謝謝。

洪賜齡律師（守越法律事務所）

你好，我是守越法律事務所洪賜齡律師，我想請教兩個問題，也是請教唐鳳政委，跟李世德參事。

首先，我們看起來 New eID 好像已經勢在必行，但是我們想問的是，就是早上很多學者專家都說要立專法，但戶政司副司長說，另訂專法是疊床架屋。身為個資法主管機關的國發會，不曉得李世德參事對於內政部的說法有什麼評論。然後或者是說，國發會針對 New eID 專法是不是在法制化的部分已經在進行了，如果已在進行的話，要不要跟國人報告一下。

然後，第二個是說，法制上人民是否可以基於資訊自主，保留領取紙本身分證的選擇，就算紙本身分證可能有像唐鳳政委剛剛講的說，有一種有比 New eID 有可能有一些缺陷，但是基於資訊自主，人民是不是可以保留領取紙本身分證的選擇。兩個問題，以上。謝謝。

何建明（中央研究院資訊科學研究所研究員）

我想再確認一下，就是 New eID 是不是便利各方都可以很順利擷取資料這個問題，看起來似乎沒有打算處理。

還有另外一個公務人員銓敘個資的遺失，跟這個所謂的兩千萬人的戶政個資的外洩，這兩個問題。政府有甚麼回應我，謝謝。

與會民眾（科技業的 PM）

各位講者好，我目前是科技業的 PM，我之前有研究過 GDPR 在科技業的法規，早上一直講到說，個資法或是其他法律可以涵蓋 eID 的一些規範，我覺得這是很值得存疑。

就是比如說，最小的資料揭露這件事情好了，我就不懂為什麼臺灣的身分證要揭露你的配偶跟你的父母是誰，這件事情根本沒有必要阿。我就看過歐盟或是日本的身分證根本沒有揭露這個東西，就算 eID 他把他數位化在晶片裡面，但是這件事情到底沒有在身分證上記載的必要性，我覺得這是很奇怪的事。

然後，第二個是 GDPR 他會有一些指導原則，像是 check list，或者是說目前哪些科技是合規，或者是哪裡不合規。這個他會有一些指導方針，但是臺灣的目前相關的法律是，至少我沒有看到。就是我覺得這樣太過法律純法律，科技純科技，這樣子對於科技業就是說，我們想要發展一些，比如說 DID 相關的技術，是無法可循。對，大概是這樣。謝謝。

與會民眾（科技業的 PM）

如果是提問的話，沒有特別哪一位，但是等下可以跟唐鳳拍照嗎？謝謝。

李德財（中央研究院資訊科學研究所客座講座）

我有個問題想要請教，想要確認一下，剛剛說國發會是個資主要的統籌機構，不是個資的專責機構。那我想要請教唐鳳政委是說，目前這個國家有沒有一個在成立個資專責機構的進度，這 DPA 的 agency 的進度到哪裡，是不是有這個規劃。

因為今天上午內政部講說他們在處理 eID 方面，都不存任何的資料，所以就不會有什麼監控數位足跡，等於說沒有 log。但這都是嘴巴說的，口說無憑。現

在民眾也沒有機制能 verify 到底政府做了哪些事，有做或沒有做使用個人資料的情形，驗證的機制到底在哪裡。那我想說，sousveillance 反監控，我們要怎麼樣來確保政府沒有在處理或濫用我們的個資，這是第一個問題。

第二個問題是你剛剛提到說 MyData，MyData 現在目前有在試行，試行的計畫在規劃當中。就我了解，因為目前沒有 eID 晶片卡，所以 MyData 事實上跟 eID、晶片卡一點關係都沒有。

我在想說，整個 eID 是內政部在推動，說 eID 要試行，要什麼小規模舉辦等等的。那我想說在試行過程，沒有專法，也沒有個資法專責機關的情況下，是不是可以把國民身分證、自然人憑證兩卡合一的作法脫勾，把兩個卡分開來。讓身分證歸身分證，應用應用，先讓民眾了解 eID 這個身分識別制度。了解之後，再來進行這個。是不是有這個可能性讓兩卡脫勾，剛好有一位同仁問到說，是不是有紙卡，維持現在紙卡的這個 option 是 available。

那第三個問題就是你剛剛提到說 opt-in，這個概念是不是現在是有，好像目前就我了解就是 opt-out。沒有 opt-in 的概念。

就是我想了解說目前的狀況是怎麼樣，唐政委的 position 是什麼。謝謝。

何明諠（台灣人權促進會副秘書長）

其實我覺得今天來好像一直在試圖揣摩兩位長官的意思，所以我剛剛有聽到那個李世德參事這邊有說，那個我們會先建立一個個資保護的專責機關，然後也許這個機關可以再討論討論，專法到底應不應該做等等，這樣的立場。

我聽了是覺得很開心，因為看起來似乎參事是覺得我們應該在這個程序上該是先建立 DPA，DPA 再考慮要不要專法。考慮完之後，才能決定要不要辦，應該是這樣的程序對不對，我想要問參事。

唐鳳（行政院政務委員）

我先回答何建明研究員的問題。第一個問題是剛剛前面講到的，很多事情在行政部門能夠做多少改變，以及哪些是可為，哪些不可為。這是第一個。那第二個是說，因為一般的讀卡機都讀卡，就可以蒐集資料，那我們是不是故意要把身分證做成消費足跡蒐集工具的一部分。那第三個就是說，之前已經有過很多個資

洩漏的事件了，我們是不是有做 attribution，就是去找出到底是怎麼發生的，以及有沒有可能做一個類似的 DID 的東西，就是一個人有很多不同、分散式的身分證。

我先講一個小故事，就是我在報名這場研討會的時候，發現說只要你有博士學位就不用揭露性別，然後你沒有博士學位你就得揭露性別。這個是必選，這個點是選在博士上面的。然後呢，如果你是男性的話，就不用揭露婚姻別，那女性的話你就必須揭露婚姻別。所以，事實上是 WhyID 裡面講到 marginalized community，非常不幸的狀況，我必須要按右鍵，然後開那個 inspector 去改網頁的前端程式碼，把博士那一端拿掉，然後我才能夠送出，因為我不需要什麼敬稱。

那大概這個就是說，我並沒有覺得他是惡意的，我是覺得說是不是從什麼英文的系統翻過來的時候，不小心留了一些這個不是很恰當的事情。所以我就說你如果這個選項真的不能拿掉，你要不要加一些選項，好比像小哥、先生 （未婚）、人夫等等的選項，這樣子是不是就是比較公平一點。那這個就是 sousveillance，這個就是 sousveillance。因為我是按照這個一般參與者的這個身分，然後去看到而且去回報這個不公平的情況。那當然我馬上就接到一封信說，報名網頁已經調整，所以各位如果比我後報名的話，都不用填這個敬稱。

那我要舉這個例子的原因就是，剛剛我講那個你行你來並不是開玩笑的。也就是說如果沒有一個會眾，像我這樣子自己按了右鍵編輯了前端程式碼，然後說你要不要考慮平衡一下你的這個選項，我想這個報名系統大概也就會一直這樣下去。然後他本來改過來的那個英文的那個可能其實早就沒有這個問題，甚至女性 Ms.，根本不用揭露自己已婚或者未婚，說不定我們中文的版本因為我們沒有這個傳統的，就會繼續這樣的下去，這叫做習焉而不察。

所以第一個就是回答何建明研究員這個 how and how much，完全取決於 how much you care。如果有足夠多的人 care 這件事情，好比像說經過這樣子的公共研討會，然後讓內政部，也好讓我們的就是朋友的知道，有更好的處理這件事的方法。

好比說像 CRL，CRL 不像 OCSP 碼，如每天下載一次或者兩次的憑證撤銷清單，自然就不會需要到哪個網域去驗證的問題。那這個到底是寫在要點層次呢，寫在程式碼裡面呢，還是要像各位有些朋友提到，要提到法律裡面呢，這個就是可以討論的。

因為我們在作用法是一回事，就是我們剛剛講到的是組織法，要有一個個資專責機關，作用法要講說這件事情他的蒐集跟利用要受到什麼限制。那以及演算

法，因為並不是說你有作用法跟組織法，演算法就會自動冒出來，還是要有人像我這樣子按右鍵，然後說你演算法上面可以採取這些 PET。

所以我這邊的主張就是說，第一個，大家都知道我 hacktivist 就是說演算法應該先行，民間如果看到一些更好的，能夠個資保護的一些作法，那就應該先做。那就像 g0v 的活動一樣，拋棄著作財產權。那讓政府可以說有這樣的作法，那太好了，我們來參採。

那這個一部分也是回答讀卡機的問題，因為各位剛剛提到很多其實在現在的紙本的光學身分證，也是有一樣的問題。

事實上有更大的問題，像明諠剛剛提到便利商店的例子非常好，就是便利商店電視機有一個 cam，現在 cam 的解析度都非常的高，拿你的紙本身分證甚至於可能用那個手機拍身分證正反面影本，就可能偽造了。

那事實上辨識上面的字比起讀卡機讀取所花費的時間說不定更短，因為身分證上就是文字及數字，除非是非常罕見的姓名，機器可能會辨識錯誤外，其他欄位應該都能馬上辨識。

所以，當時我非常感謝明諠，我也有公開說，就是我們在印製三倍券時，確實我們當時內部討論有一個版本，就是把所有的券號都是透明揭示出來。但是後來我看了台權會的主張之後，我就說不行，真的必須要去用信封，把券號的序號必須遮蔽住。為什麼呢，我說店員抄錄並不是店員拿手去抄，可能要澄清一下。而是說店員只要用後面的那臺攝影機，在給顧客三倍券時候稍微舉起給 cam 看到，他馬上就可以把券號紀錄下來，確實是如此。當民間提出了這樣的想法，我們馬上就參採。雖然我以前當行政院的專案顧問的時候，可以捐台權會，而且也有捐給台權會，但是現在據說不行了。所以，如果大家有數位綁定三倍券的話，記得可以用 1984 這個捐贈碼，唐鳳不能捐，台權你來捐。

那在第三個部分，就是回復 HoHo 有關個人可不可以有不同的身分證或不同身分證號，這個是非常好的問題，事實上我們有做 DID 這邊的一些評估，資策會有做這樣子的報告，我覺得這是兩件可以並行的事情。就是在試行的時候，可以採 opt-in 的方式，好比讓民眾自己決定換發 eID。那這也應該讓剛剛講的個資專責機關有點事情做，可以去看這個新的 flow 長什麼樣子。那如果後來發現說確實採用複卡的方式，或者是採取像內政部有提出就是他可以把 secret API 的那個部分，用類似身分證影本的方式，這樣子變成一個紙本文件，發現這樣子類似 DID 的這個做法，反而比較好，那我覺得也沒有什麼不可以。好比像說我也改過名字，雖然改名字不會長高，但是事實上就是說，如果大家都有隨時改名的一種

權利，那你在改名的時候可以順便改一個證號，我說真的不覺得這是一件壞事，我覺得這是 open to discussion，我覺得這真的是可以討論的。

那剛才這個 Amnesty International 這邊有兩個問題。一個是我們是不是要停止那個 facial recognition，雖然我不是很確定這是像國外是停止 funding，還是說全面禁用。因為如果都不能用的話，那我這臺 iPad 的 face ID 可能也不能用。

所以，可能不是完全剎車踩到底，而是說除非他可以證明說他不會傳輸到別的地方，不然的話我們就不應該採用這種 general purpose facial recognition，這個我個人是很支持。

而且之前在看很多案子的時候，當他們用類似 facial recognition，或是根本不是 facial recognition，他只是說有人去看有人會不會踩到那個危險的線呢，什麼之類。我都說那你這個用一個 infrared sensor，你用一些就是不會到後來變成人臉辨識的東西。事實上都比這些 RGB cam 來的好用，所以我個人是支持的。

那在講這個 WhyID 的時候要做 list of impact，那這個就是我想我的這個想法就是剛才講了，就是我們是不是應該要有一個 sandbox，那這個是不管服務系統也好，或者是願意換證的也好，都是 opt-in，而且至少六個月，不然我不是很確定我們在演算法層級的 impact assessment 到底要怎麼做。我們當然可以在作用跟組織法的層級去做一些評估，去做一些預想。但是我想有很多 case，就像剛剛那個三倍券的信封的封套一樣。

我們可能事先很難把那個三倍券要點裡面想到這些細節，但我覺得很需要大家用一種參與式的驗證方法，不是說一定要換發，而是換發後揭露從頭到尾的用法，那把這用法揭露之後，如果有看到什麼不太對勁的地方，那這個就是新的個資專責機關的事情，以及我們希望接下來就是在 regulation level，或是在立法院大家可以討論的一個素材。大概如此。

舉兩個例子來說明，一個是我來幫忙這邊改他們的報名系統，那另外一個是台權會質疑三倍券可能在便利商店被蒐集序號。事實上像現在大家如果是有用信用卡的話，應該了解到信用卡你不會把他的背面影印給別人，因為大家都知道你在店商付款的時候，靠的是後面那個不會被留下來的那個 CVV，就是那三碼。

所以說如果把信用卡背面拍給別人的話，差不多這張信用卡也就可以報廢了。那現在我想要剛剛強調的就是說，所謂的 norm shaping，就是關於這件事情的常規，我們要怎麼樣讓整個社會了解到說，如果假設有 New eID，你把你的 New

eID 的背面影印的話，就是把你的這個序號，就是讀取碼去給予所有人，那這是絕對不可以做的事情。

那當然這裡面有兩個部分，一個是應然的部分，就是我們是不是要在我們的作用法上面，或者是在我們的法規命令裡面去說，不可以這樣子做。但是縱使我們說不可以這樣子做，如果大家還是很習慣的去把身分證的影本，也是就他的讀取碼拍個照，然後去傳輸給別人的話，那我們這邊再怎麼的立法，可能要花比較長的時間才能夠收效。 所以，我剛剛強調的並不是說，前面這一端不應該做，而是後面這段，就是 norm shaping 的部分，需要大家一起來做。這個是我覺得已經蠻具體的回應，並不是閃躲這個問題，這是第一件事。

那第二個事情是，銓敘人員有沒有做 attribution，我很誠實地講，就是因為這部分屬於資安處的業務，那資安處的業務我一直到大概兩個月前都還沒接觸到，這部分我會回去跟簡宏偉老師再確認。

我想，Readr 有整理一個蠻好的一個對照表，就是我們本來的舊版的那個身分證則正面的性別日期，發證日期跟背面的父母姓名、配偶姓名，役別、出生地、住址等等，都是在新版的卡片是拿掉的。

有兩件事情要先講一下，一個就是說，以我的理解，凡是組改相關的都是人事行政總處在負責，所以如果內政部或是國發會說還沒有處理到這個個資專責機關的組織法的話，確實是如此。以我目前看到的都是在人總的這個版本。但是這是他們的 priority，所以我想應該下一個會期應該是會有版本提出來。那當然行政院要是有版本提出來，是要院會同意，所以我也不可能代替院會去說，我們什麼時候這件事情，但是以我的了解，有這件事情，而且是我們的 priority。

那另外一個就是 MyData，如果大家去 MyData 看，目前一共有五種登入方法，就是自然人憑證、工商憑證、健保卡、TW FidO，跟動態的密碼，一共有五種。當然有些方法的強度比較強，所以如果你用比較弱的登入方式，是不給你讀取的。但是無論如何，自然人憑證都是可以讀取的，所以至少自然人憑證這個剛才講說，是不是我們用自然人憑證先行，我覺得這個是非常棒，好比說像說在看直播的這個葉平老師，就是我們萌典專案的發起人、共同作者。也是說，他希望未來好比像說我要 opt-out，就是禁止紀錄足跡、刪除足跡等等這些東西，是不是也有可能在 my data 那個介面做。我覺得這是非常好的一個主意。那葉平老師也是說，是不是可以在同一個介面上面去揭到那個獨立驗證，那這裡就回到剛才 DPA 的問題。

就是說如果那個需用機關按照目前個資法是主管機關，他自己說他自己做了一個 independent audit，然後都沒有問題啊，其實你也不相信他，你相信他的程度不會比現在多。那所以就說所謂的 independent，只要他的錢跟人都還是那個需用機關自己在出，那事實上我們都知道社會部門是覺得這個是沒有公信力。所以我覺得還是要有一個處理 independent 的 DPA，有那個 DPA 來做 independent audit，讓使用機關就是這樣子繞過去。那剛剛講的試行期 opt-in 還是 opt-out，因為我的理解是 opt-in。

就是說在試行的區域，就是戶政事務所，在試行期好比說六個月去換發那這個換發的過程裡面，不是說到六個月結束之後，住那些地方的人都要強制換發，因為那個就不叫 opt-in 了。而是說在那兩個地方設籍，然後以及一些資源要加入先期測試 program，好比像說我啦，就可以去那邊的戶籍地說我要 opt-in，直到試行期結束，我們那個測試的報告出來以前都是如此，不會說在試行期結束之前，那兩個戶籍地都必須要強制換發，沒有這種事情。

那最後就是說，我自己去換發的時候，我也是會兩卡分開拿，就是會付工本費，然後有一個就是 New eID，那它當然是有剛講到的序號的那個 Open API 的部分、secure API 的部分，六碼的密碼。那然後我會另外用一個自然人憑證，就是新辦的自然人憑證，它就加強了因為新的自然人憑證它是八碼以上的密碼，至少不會說你有自然人憑證跟你的 security API 用同一個密碼的情況，因為密碼長度根本就不一樣。那這是我會選擇的，因為我未來如果還想要用什麼魔鬼氈把這兩個黏在一起，我隨時都可以把它黏在一起便於攜帶。

那事實上就是我會覺得說我拿來簽章，就是 authorization，跟去做身分的驗證 authentication，我自己看起來是兩個不同的應用情境，所以我自己也會選擇兩卡分開拿，這個部分也是 opt-in。

唐鳳（行政院政務委員）

回應何副祕書長，確實啦，就我理解到這兩個也沒有邏輯上的先後次序。我們當然純粹只是想說如果有 DPA 的話，DPA 對於這整件事情的意見，看起來尤其如果 DPA 的組成裡面有足夠多的社會部門的朋友的話，感覺上他們社會認受性、正當性會比較高。

那至於劉靜怡老師剛才講到說，運安會只是做事實認定，以後 DPA 要做更多這當然是如此沒有錯。我剛才講的只是在組織法上的獨立性，並不是說在組織

法裡面的處務規程等等，要做的事情作用法上面是被限縮到像運安會那樣，並不是我的意思，合先敘明。

那這邊要回答一下就是兩個具體的問題。一個是說，就是剛才所講的是不是挑簡單的先做，看來歐盟也要先討論 GDPR，DPA 也是大家都覺得需要的事情，所以我們就挑簡單的先做。但是比較困難的，好比像說一人一個身分證字號就稍微拖一下，就是比較不去檢討，而是而去換發這件事情。那我聽起來莊老師似乎是覺得這是思覺失調的這樣子一個現象。

不過，以我的理解，這兩個都是法律層面的事情，立法院先處理社會比較有共識，或者是社會上面已經討論到一個程度，或國際上看起來是一個趨勢的事情。其次，去檢討比較尚未成熟的情況，這似乎不能夠說是一種思覺失調，而是民主社會正常的一個運作的情況。所以，我可能不覺得說，我自己在行政院能夠去好像那個腦波遙控立法院，去改變他們的 priority，我如果真的有這種想法，才是思覺失調。

那另外是一個很具體的問題，就是說主責的政委。在行政院裡面，政委是處理還沒有分派到特定部會，或者部會跟部會之間，對同一件事情有不同立場的情況下，會由政委來進行協調。那這個是在政策的前期，好比像說，以前電競，文化部說電競沒有一百年的傳統，所以是教育部。教育部說電競沒有動到大肌肉，所以應該是經濟部。經濟部主張他們管的是球場，球員怎麼會給我們管，這應該是文化部。像這種情狀的時候，政委就有工作的一個空間。但是以我的理解，就是 eID 這件事情，因為他是院核定，那院核定他是已經不是在先期的這個情況，那各部會之間，好像也沒有什麼太灰色地帶的這個情況，所以他目前已經回到各部會分管，這是我的理解。

李世德（國家發展委員會參事）

好，我回答剛剛律師提的這個專法的問題，那我們現行國家的體制裡面，普通法跟特別法一直都是在做這樣的一個模式的推演。

那個資法是屬於普通法，在早上報告人在報告的題目內也有去做的一個對照表，那我看到對照表有去提到，日本還有德國，或者愛沙尼亞等等。那他們的處理模式裡面，他們有他們自己的個資法。但是在處理數位身分證這一塊，我們看到國際的趨勢，是另外會再訂一個專法，那不是訂在個資法裡面，這個也是對的一個處理的模式。

那若針對數位身分證這邊是不是要專法，當然還是要給內政部來回答。而在國發會的角度是說，若沒有其他專法之前，都是要在這個現有的法律制度下運作，例如：資安管理法或個資法等。其實之前立法委員也有在關切，若在沒有訂專法的情況下，個別法律的一個運作模式是如何。那從我們國發會的立場說明，取用數位身分證的公務機關或非公務機關，即使只有去讀取公開區，當然都是個人資料的蒐集。那一區塊是居於辦理怎樣的業務，需要使用這份資料的內容，那就會完全回到個資法的一個規範，包含讀取完資訊之後，能不能再做目的外利用，或提供給第三人，也是一樣回到個資法。以前在跟內政部的同仁討論這塊的時候，我們也跟他們很清楚的說，個資法在處理這個議題，是假設沒有另外再去立一個專法情況下，我們只是在個資法目前現有的原理原則，去規範每個想要去蒐集到數位身分證內資料的人。

但要不要去用一個晶片身分證來去取代紙本，那這個問題沒有辦法說仍有個資法適用而可解決，的確是另外一個議題，只是在現在提到是不是用專法去規範?當然這已經超過國發會職權範圍，但假如說大家都在討論這個議題，或許個資法所展現出來的角度，的確是屬於比較後端，而不是站在前端去針對數位身分證，做一些特別的要求跟規範。但是至少在進入後端的這塊行為裡面，個資法它當然會扮演它的角色。剛剛唐鳳政委已經提到一些所謂專責機關將會處理的問題，未來我們國家可能會有一個這樣的制度即將要產生。

那若有個人資料保護的專責機關的時候，當然可能對現在討論整個數位身分證事情的過程，可協助其他機關在推展業務之際，面對所碰到的個資保護議題。未來專責機關，相信應該可以扮演輔助的角色，去協助其他機關推展業務時，包含其他機關決定是要訂專法、不要訂專法的過程，都有一個更積極受諮詢的角色。那我就先報告到這邊。

回應一下剛剛何副秘書長解讀我的說明，我應該不是那個意思，因專法最後的主政方還是在內政部，國發會的角色僅為協助。現有在討論要不要立專法的議題，我知道內政部他們自己討論後，也會有一個思考決定。只是說在專法還沒出來之前，這個制度要繼續推的時候，國發會因為是個資法的解釋主管機關，那我們當然還是會提醒說，數位身分證制度施行過程，當然是會有個資法的適用，這是沒辦法迴避的。

至於說身分證專法跟個資專責機關是不是有一個連動關係，就是說「一定要個資專責機關先出來，然後再繼續去規劃專法」，我覺得我們在跟歐盟討論設計個資專責機關的大的架構面過程，是沒有談到各個部門立法前，一定要有個資專責機關才足夠。

所以，目前現在剛好也在討論 New eID 的議題，那也同時在討論個資法專責機關議題，這兩個議題我覺得當然可以互相去做參考，但是至少目前現階段，我沒有那個意思是說誰為誰的條件，然後才能繼續去推動另外一件事情。那我就簡單說明到這邊。

邱文聰（中央研究院法律學研究所研究員）

因為剛剛那個唐政委有提問那個劉老師的一些問題，我剛剛透過腦波跟她聯繫了一下，我就幫忙回復那個就是對於 sousveillance 的用語，確實原來的字面用意是說，個人拿起自己的 camera 去反監控。

可是在 eID 的情境底下，當那個 camera 不在個人手上的時候，所有的資訊是被政府所壟斷，政府到底有那些足跡，這件事情根本無從，個人拿起 camera 來進行反監控，確實就需要像日本跟愛沙尼亞這樣，政府自己來建立自己的足跡，然後並且提供人民來進行監督，這是第一點。

第二點是有提到就是這個，運安會的例子做為是個資獨立監管機關的案例說明。但是運安會這個三級機關本身只是做事實的認定，也就是說，運輸的這個事件當中，發生的原因為何，那跟這個個資的監管單位，它需要肩負的這種管制的責任可能不太一樣。所以，如果只是一個三級的機關，要來承擔一個個資獨立監管的目的跟功能的話，可能沒有辦法期待它能夠達成的。這是第二點。

我有兩個自己的小問題，就是說這個在就剛剛大家不斷提到的說，這個紙本有沒有可能留存。那我舉德國為例，德國它雖然是塑膠卡，它裡頭也是預設晶片，但是它在憑證的部分是個人 opt-in。除此之外，對於那個晶片本身，可以 opt-out，所以，等於是當你 opt-out 這晶片功能，讓它純粹變成是一張塑膠卡，所以，在這個意義底下等於是剛剛幾位提到說，有沒有可能紙本跟晶片同時並行的可行性。就是說在德國確實是發生的。

那我也想請教唐政委，就是說目前到底行政院主責 eID 的事情的政委是哪一位，因為我聽起來好像目前在陳美伶主委離任之後，這件事情就沒人管。至少在政委的層次，所以不曉得唐政委知不知道這件事情，因為您剛才提到 norm shaping 是很重要的，我也非常贊同。但就是這個 norm shaping 除了說去改變大家日常生活習慣之外，恐怕還是得從法制上面，剛剛這個參事也提到，就是個資法可能是不足夠的。

那我們從比較法上面的觀察也可以看到說，真的需要一部法律去來好好的針對這種數位身分證的使用，到底什麼時候可以用，什麼時候可以蒐集，什麼時候下載資料，誰不能下載，可不可以留存這些，做比較詳細的規範。以上。謝謝。

莊庭瑞（中央研究院資訊科學研究所副研究員）

我的感受是臺灣的政法上有一點思覺失調，就是說重要的事情應該做的，但是因為它太困難了，所以我們不能做，來不及做，所以我們就挑容易做的事情就先做。

我舉一個例子，個人資料保護專責機構這個議題大概講了 20 年，那 20 年以來都很困難，所以一直以來都沒辦法有進展。那戶籍法這裡面規定每 10 年要換發身分證，所以每 10 年就有身分證要用晶片、要按指紋這個議題會產生。就好像每 10 年要出一次疹子，但是具體上是發紙本身分證。從上次身分證換發到現在也 10 年，那 10 年之間到我們這個中華民國政府在這個戶籍制度身分證的體制上面，卻不能進一步去演化。到現在這種很難處理的狀況。

所以說這似乎是思覺失調，就是應該做的事情都知道，但是沒辦法去做或做不了。那我是覺得臺灣的戶籍制度跟這個身分證，一人一證強制換發攜帶，發給的身分證字號終生不變，這種作法在數位時代好像變成一個恐龍，這恐龍的體制如果不能順利演化的話，前景會蠻黯淡的。

蔡文軒（中央研究院政治研究所副研究員）

我只有一句話而已，就是民主跟威權國家在資訊的一個監控上，在思維跟做法確實有許多的不同。謝謝。

T-Road 的資料庫串連與數位身分證的近用控制 Q&A 紀錄

余至浩（iThome 電腦報採訪主任）

你好，我是 iThome 電腦報的採訪主任余至浩。我有兩個問題想要請教潘處長。第一個是說，現在政府一些便民的服務上面，其實就已經可以允許跨機關的資料傳送，那我還是好奇想問一下，就是，有 T-Road 和沒 T-Road 它的關鍵差別是什麼？就是，它到底解決了哪些關鍵的問題。第二個問題是，今天剛好 MyData 也試營運上線，也好奇這套平台背後是否也用到一些 T-Road 的這種資料傳輸通道的技術。那怎麼樣將這種不同的資料來整合在同一個平台上面。謝謝。

與會民眾

我是資訊背景的。那我也是想問一下處長，就是其實前一場就有討論到關於立法的問題，那我們知道像行政院機構是可以向立法院提案的。那像 T-Road 這樣子可能會有不知道我們的資料給了政府機構或是私人企業它們要怎麼使用的問題，想問有沒有關於要提案立法規範的規劃，謝謝。

與會民眾

想請問一下，我們現在看起來，共識是說資料隱私保護和資料價值，有些是要做取捨的，trade-off。那有沒有一個好的方法，在國際上有沒有看過，可以去討論這個取捨要怎麼去做有效的討論跟收斂成共識。

王仁甫（資訊工業策進會資安科技研究所策略總監）

我要請教一下潘處長，因為剛才有提到說，未來 eID 是會串接很多政府的電腦資訊服務。那因為只有一把鑰匙，其實我們搞資安的就知道，如果你憑證都是同樣的，大家都用同一個憑證，像之前某大的資訊公司，就是發生一樣的事情。一個憑證大家用，結果就被偷走了。所以如果只是這把鑰匙，然後你又沒有多重

驗證，又可以開那麼多東西，然後帶走那麼多 MyData 的東西，那我們是不是幫中共開了一條路，以後的 MyData 就是 China-MyData 對不對？這個事情到底要怎麼樣防護？在軍事上重重防護，可是我們在資安卻開了一條 T-Road，那這到底要怎麼做？謝謝。

潘國才（國家發展委員會資訊管理處處長）

謝謝大家的提問，先針對現在就已經有的相關的便民服務，而有些也是透過一些資料傳輸的方式。我先從技術上面回答這個問題，因為現在各種資料傳輸的方式非常多元、使用的資訊技術也不一致，以各種網路連結方式為例，各機關間會用不同方式連結，而且規範也不見得是一致的，所以我們剛剛說，希望做一個 T-Road 出來之後，有一個一致性的傳輸方式。

具體說明一下，現在的傳輸方式，有的是機關間講好了之後，可能就去申請點對點互連的 VPN 就去傳遞了，有的是透過中心（centralized）的方式（來傳遞）。我們從技術上面規劃了 T- Road 之後，希望用一致規範透過點對點的方式在安全內網架構下去傳資料。所以 T-Road 最重要的，就是希望在內部架一個資料傳輸的機制。

剛剛有提到 MyData 是不是也用 T-Road 的這個（傳輸機制）？目前 MyData 沒有，因為 T-Road 還正在建置當中。那 MyData 如果各位有注意，剛剛唐政委也說，我們有試營運已經開始在做。未來 T-Road 建好了之後，會逐步的把相關的資料庫接上 T-Road，屆時 MyData 的資料都會透過 T-Road 做政府內部的傳遞。

另外還有提到說，是不是有給企業去使用。目前，T-Road 並沒有規劃要去給企業去使用。那 T-Road 上面，我剛剛跟各位報告，T-Road 上面所傳遞的「資料內容」是用現行的法規所允許的傳遞的方式。所以現在已經有一些法規同意資料可以在機關之間互相傳遞的話，當 T-Road 建好了之後，就可以透過 T-Road 去做傳輸。

另外仁甫最後有問到說，eID 是一把鑰匙。這一點，可能在這邊稍微在技術面上做一個說明。eID 在形容上面是一把鑰匙，可是並不是有了 eID 後我就可以到所有政府資料庫裏面，翻箱倒櫃的可以把自己的資料通通都找出來。還是會有一個介面程式把關，還是會有程式去身分識別。早上有老師提到證明或者識別，因為我自己除了知道所謂的證明跟識別的差異性，一個是主動拿出來，另外一個是別人來做認知之外，並不是太了解他們之間太大的差異性。但是強調的就是 eID 它在網路上面的時候，你透過程式驗證後，可以做程式所允許你做的事情。

也就是那個入口網上面，或者 MyData 上面程式所控管的、提供出來的服務。

那是不是只靠一把 eID、New eID 就去做所有的事情？其實並不是。如果各位有機會上 MyData 平台的話，MyData 有多種的認證方式，甚至於包括有些專家在上一場可能前面幾場有提到說，健保卡是不是也是一個不好的認證方式，但是我們在現行的情況之下，還是把它納到識別的方式之一。所以不是每個服務都是要靠 eID，不是每件事情都要拿著 eID 去到入口網上面、到 MyData 上面去執行。它有根據各種不同的認證的服務機敏度。有些服務裡面涉及到的資料跟個人機敏度非常高的時候，當然我們認證的機制、識別的機制要比較強化一點。如果有些的服務並沒有那麼強烈的話，我們並不是每件事情都是要用 eID，都是要用自然人憑證。我想大概先簡單回復。

顏厥安（國立臺灣大學法律學院特聘教授）

剛才好像有位提到中國因素，我們能不能回應一下？

潘國才（國家發展委員會資訊管理處處長）

就是這一個，我們並不是說全部拿 New eID 當作識別。

吳全峰（中研院法律學研究所副研究員）

我想說，資料的可用性和資料隱私保護，可能顏老師把三十分鐘給我都還不一定講得完，那是個大哉問，基本上每個國家都一直在尋求一個可以平衡兩者的答案。其實王大為老師都已經講過了，類似 privacy by design、differential privacy 或是 synthetic data 都是可能的解決方案，基本上就是我們都不斷地在嘗試找各種方式去解決資料可用性和資料隱私保護的平衡問題。但必須要講，這個問題沒有標準答案。

但一個重點是，資料可用性和資料隱私保護的平衡方式一定要有一個法制基礎，平衡方式才能具有正當性。所以剛剛處長有講過，T-Road 現在基本上是希望找一個一致性的傳輸方式去解決這個問題。但這只是技術層面的問題，也就是希望提供一個達到某種效果的工具；我認為這是一個可以接受的方向，多數講者其實也沒有反對 T-Road 這項技術，或是 T-Road 希望達成的效用，但技術層面是否能完全解決法制上正當性的疑慮，卻是有問題的。換言之，當我們在追求達成一致性傳輸方式的時候，為什麼不能同時建立一致性的法律規範？這是我們在追求

資料可用性和資料隱私保護平衡時所不斷問的問題，也就是若一致性法律規範可以建立，並不表示一致性傳輸方式就會被排除或禁止，所以重點一直是在如何建立規範，並且在規範的基礎上達成一致性傳輸方式的目標。

另外一個問題是，是不是一定要先建立規範才能夠去做技術上促進資料使用效用的事情。我知道不同的技術可能要求並不一樣，但是把所有的隱私概念都當成一致性的隱私概念、所有的資訊都當成一致性的資訊，不管資訊之特性或是在不同資訊下隱私保障強度之差異，一概要求以資料可用性之效用追求作為優先追求的目標，那可能就要畫上一個很大的問號。不可否認會有很多的新興技術的發展，但社會上還是會認為有些技術在沒有規範下就是不能讓它做的；舉個例子來講，科學家已經有技術可以做出複製人或是操弄基因編輯製造超人，那是不是就可以允許科學家在沒有任何規範下就先利用這個技術進行創造先做？相信多數人的答案是否定的，認為還是要有規範，才能決定這個技術到底要不要被允許實際上操作。

既然承認某種程度規範的存在是有其必要性，那問題就在於，剛剛處長也承認的規範碎裂化的問題，如何在規範碎裂化的過程當中，能夠確保 MyData 或 T-Road 所使用或傳輸的所有資料，不管是敏感性還是非敏感性的個人資料，不會有規範不足的地方？還是必須要有思考在既有規範外，是否有必要確立一個比較好的規範去管制 MyData 或 T-Road 的運作？我認為透過這樣的討論才能夠達到一個資料可用性和資料隱私保護的平衡狀態。而不是說，今天既然已經有了技術，那就不管是否有規範；如果有了規範，卻也不去檢視規範是不是合適管制這技術，就先上路，那這樣資料可用性和資料隱私保護的平衡才會被打破。最後，只有當規範建立起來了之後，才能進一步去討論在這個規範之下，資料可用性和資料隱私保護的平衡是不是有問題，也才不至於偏重任何一方而造成失衡的狀態。

邱文聰（中央研究院法律學研究所研究員）

中研院法律所邱文聰提問。我想，一把鑰匙可以開啟很多個門，跟很多把鑰匙可以開啟門是兩個不同層次的問題。剛剛潘處長的回答似乎是說，現在有好多把鑰匙都可以來開門，但這個回答似乎沒有辦法解決剛剛的提問說，用一把鑰匙可以開啟非常多門，甚至政府的每一個門都可以去開啟的問題，所以我覺得這兩者還是不同的。所以可能等一下再請潘處長是不是可以再做回應。就是用一把鑰匙開啟這麼多門所衍生的風險到底要怎麼解決。那第二個想要請教的就是，如果我們不要讓它變成 China-Road，那對於剛剛王大為老師說的，TW-Way，對潘處長來講，是不是有可能實現？就是比較起現在 T-Road 的設置的話，TW-Way 或

是 T-Way 這樣子的想法，在我看起來是比較 appealing 的。那是不是有可能政府在發展的時候是用那樣子的模式來取代現在以技術為優先，但是技術卻沒有辦法解決整個政策或者是法治文化上面的問題的狀況。

李德財（中央研究院資訊科學研究所客座講座）

我是中研院資訊所李德財。就剛剛邱文聰老師的發問、提問，我也有同樣的問題想要請教潘處長。

剛剛提到 MyData，我想要了解，MyData 是一個試行的方案，那 MyData 在建構整個基礎架構的憑證，MyData 的重點是什麼，是有 multiple 的這種多重、各種各樣的認證，個人的憑證卡都可以使用的嗎？我想要知道 MyData 在上面運行的整個機制跟現在 T-Road 的關係是什麼？因為剛剛 MyData 在講的時候好像有提到，將來 eID 有了的話，eID 也可以納入到 MyData 的試行方案裏面，那如果是這樣的時候，MyData 和 T-Road 有什麼不一樣？那 T-Road 將來建立起來了，是不是只有 eID 可以（使用）？剛剛就講說 eID 事實上照戶政司張司長講的，eID 是一把開啟智慧政府的鑰匙，也就是一把鑰匙可以串通這麼多個資料庫，那跟 MyData 這個 multiple 多重的資料庫，多重的這種憑證，開啟的多重資料庫，到底差別在哪裡？如果是一樣的話，那為什麼要重複建置？如果不一樣，不一樣在哪裡？能不能夠請潘處長說明一下，謝謝。

何建明（中央研究院資訊科學研究所研究員）

那我想問的問題當然，第一個從 MyData 問起。因為 MyData 我反而覺得還蠻恐怖的。如果我想要退出的話，我怎麼退出？因為我可不希望說，因為所有資料我都有，政府也有，那我是不是有需要讓我的資料在網路上可能會曝光，這可能是一個我要選擇的問題。那當然另外一個想到像這個 MyData，當然可以想到它後面有一些應用。我想今天像全峰、大為你們在提到的一些政府的應用裡面，比方說剛剛在講跟金融機構之間的連結，這時候可能我的 data 會過去，那其實那個 data 我也可以自己填給這些銀行，沒有理由說非得要政府給它的銀行它才相信。所以我自己心裡也覺得是說，當然很佩服整個資訊處這邊，在國發會這邊那麼努力地有任務必達，所以做了很多很好的工作。可是這裡面有很多是規範面的問題。所以我想請教，當然這個問題我們也知道，當然潘處長可能有答案，就是這個規範應該是在哪裡來制定，可是我在猜，這裡面除了主持人之外，可能只有全峰能夠回答這個問題，就是說，最後我們還是要問的就是，規範到底要從哪裡

開始啟動？ 必須要有一個規範出來，這樣大家今天講的很多擔心的問題才有辦法處理，資訊處長也才有辦法在那樣的架構之下去發揮它們最高的作用。這個要怎麼辦？

潘國才（國家發展委員會資訊管理處處長）

謝謝。我一些問題可能沒辦法逐一的回覆，我大概就總整一下。不管是MyData、不管是 New eID、不管是任何的識別，我們都是從服務的角度，從線上服務的角度來看這件事情。也就是說，政府有各項線上的服務，我們希望未來越來越多線上的服務是比較方便。不過我在這邊也補充一下，我們不是用線上的服務來取代臨櫃的服務，我們推動的是多元性的服務方式，所以將來有線上服務的時候，臨櫃的服務依然會存在。這一點先跟大家報告一下。

然後我們回到所謂線上的服務。線上的服務有各種不同識別的方式，這點我想大家都非常的認同，那 New eID 發了之後是不是就只能夠靠 New eID？當然不是。那很多的服務它有沒有其他的識別？或者是它要不要用其他的識別？是 ok 的，是看那個服務（本身要用哪種識別）。我舉例來講，假設未來有所謂的老人的服務、敬老的服務、要推出一個線上的服務，那要不要推出一個敬老卡，然後透過敬老卡去取用一個線上的服務？這是完全沒有問題的。不是說我們所有各項的東西就是靠一把鑰匙去到政府的各個機關。這是從服務的面向來看，它是有各種不同服務的需求，那它要去發展出它的各種識別方式。那識別的方式之一，有可能是用 eID。

當然很多人非常的擔心，包括我自己說實在的也不見得是說所有的東西都是要用 eID，隨身將來要帶著 eID。如果將來能夠去發出，因為可能年紀也到了，去領到所謂的敬老卡，然後某個我所在的、居住地的市政府，它也可以去發出一張敬老卡，然後給我在網路上面去用的話，當然我也很高興。我去搭公車或者我在網路上去取用服務，就用這張敬老卡就好了，不需要帶著 eID 到處都拿著用。

所以我剛剛說，eID 是一把鑰匙，這句話可能造成大家就是靠著這把鑰匙就把所有政府機關的服務就一網打盡，全部都是用這把去完成，其實這不是我們所規劃的一個內容。

那王大為老師所規劃的 T-Way 是不是將來我們很好的一個方向，我覺得那個將來是可以做我們進階版的一種考量。現在非常的流行所謂的 1.0、2.0、3.0，所以 T-Road 建完之後，搞不好明年度就會有所謂的 T-Road 2.0，那 T-Road 2.0 我們再跟王老師再做進一步的請教。T-way 的部分呢，就 T-Road 2.0，我們可以改

名 T-Way 沒有問題。那這部份我們可以向王老師來做請教。

李柏鋒（開放文化基金會董事長）

對不起，我要直話直說，這實在不太公平。政府要發 eID 的時候就說 eID 可以開啟所有的服務，現在講到安全就說，不用不用，我們 eID 不用開啟所有的服務。讓我有點腦子混亂，不曉得誰講的才是真的。所以，是不是大家靜下來坐一下，寫一些不管是法律啊、行政命令啊寫一下好不好，要不然我都不相信要聽誰的這樣。

我想回答一下剛才那個疑問，我覺得很好。我們會不會變成 China-Road？其實技術上是真的可以解決的，其實我以前也跟處長提過說，哪些憑證可以開啟哪些服務，列個表，然後我們是不是可以去決定把其中哪些關掉。像我阿公阿嬤的我一定會去把它全部都關掉，絕對不能在網路上傳輸任何資料，他要去做什麼我就幫他拿書面的就去做就好。那我自己，我擔那個風險嘛，我就全部把它打開來在網路上，我覺得這樣很好，大家很方便。

事實上這次三倍券就是這個例子，大家其實很多還是用書面的。所以我覺得有數位的很方便，我自己就是用數位的，數位預定、數位預購。可是真的有些人，像何老師權高位重，他資料很寶貴所以就把它關起來。所以我說，T-Road 將來還是要拜託處長納入考量，就是說列一個表看能不能關掉這樣子，謝謝。

王柏堯（中央研究院資訊科學研究所研究員）

就是，我還是覺得這個隱私的問題其實遠比大家想像的複雜，尤其是政府機關之間，這麼大量的資料串連，就是已經在國際上出現過太多太多這些不是很好看的例子。那我還是覺得說，大家不要把隱私跟安全混在一起看。因為這樣子…講說遲早會出亂子好像有點太狠了，不過我相信現在這個世界的研究不會是這個樣子，謝謝。

王大為（中央研究院資訊科學研究所研究員）

一定出亂子。

我第一個要謝謝處長，我覺得你們今天看，他是真的今天來這邊，真槍實彈的跟各位、跟我們在溝通，我是非常非常希望越來越多的政府做決策的人 be transparent，把你心裡面的話講出來讓我們知道，我們可以跟你一起想。

對不對，我想一想，至少我的 TW-Way 就是比 T-Road 厲害，因為是 TW。你當初問我，這個就不一樣啦。所以我是覺得這個態度上是要公開，transparent，因為 keyword 是 trustworthy society。你要 be smart，你沒有 trustworthy，那個 smart 會小聰明、很危險。

結論就是，道不行久矣。再這樣搞下去，保證危險。

查士朝（國立臺灣科技大學資訊管理系教授）

好，那這個我想很多時候看到很多服務是政府有在做了，包括說你現在說要禁止，其實資料也是在傳輸。所以在這種情況下，其實我們比較需要是說有一個規範，把現在新的做法把它定義清楚之後，大家再來看說我們怎麼樣去做這樣子的一些事情。那這樣子會比較好一點，因為基本上我們現在看到就是，到最後 T-Road 可能就是到幾家配合的政府機關，那就部分的這些重點應用上面來去做一些這樣子的示範性的應用。反而是我們如果說，真正大家對於政府機關一些個人資料保護的期望來說，會希望說是有一些方法是大家能夠有一個很好的規劃再去做這樣的事情。

那當然如果 T-Road 它其實目標不用喊這麼大，我們其實最基本來講，如果我們就是要幹掉過去的 SFTP 這樣子的過去一些不安全的陋習，這個目標如果沒那麼大，我們做好一些基本的事情，那這個是蠻值得期望的，謝謝。

吳全峰（中研院法律學研究所副研究員）

好，謝謝。我最後再多說一點，就是剛剛老師也提到說，到底誰要主導立法的事情。我覺得最主要的問題在於，資訊處本身雖然是負責技術性開發，可是問題在於技術與規範是無法完全切割的，在 T-Road 的發展上是不可能不遇到法律的挑戰，而這些挑戰也不是將管制責任「直接回到各個主管機關」便可以解決的，仍是要從 T-Road 主管機關本身來思考如何解決這些法律問題。

舉個例子來講，假設今天民眾認為銀行蒐集我的資料不符合最小蒐集化原則，那理論上民眾是可以到金管會申訴，質疑銀行為什麼可以蒐集那麼多資料？但是假設民眾同時在跟金管會的申訴過程當中，他能不能同時跟 T-Road 的主管機關講說，請你暫時把這一塊先關掉，不要讓銀行去要這個資料？那 T-Road 主管機關是誰？民眾是要跟資訊處說請暫時關掉這一塊諮詢傳輸作業嗎？還是應該跟國發會說？

我個人認為，T-Road 既然已經發展出來了，那就應該有一個主管機關，那個主管機關本身應該要負責 T-Road 對外管理審核的業務，並且有明確的規範。這就是王老師剛剛講的，當那個「道」能夠出來、那個規則能夠出來的時候，T-Road 本身的順暢性，或是民眾的信任感才能建立，才能夠運作得比較久遠。

顏厥安（國立臺灣大學法律學院特聘教授）

好，謝謝。今天這場活動是法律所辦的，不過這場的法學性質是比較弱一點的。我們法學界談隱私啦，最重要就是釋字 603 嘛，我們其實前後兩任所長都跟這個 603 有密切的關聯性，在座也有些朋友跟 603 都有些關聯性。不過前兩天有個朋友跟我講說，可是將來這個 eID 實施後，希望不要等到文聰當了大法官，用釋字 1450 號才能把它解決。

那我想我們今天這個活動，很感謝幾位的參加，我們最後再用熱烈的掌聲謝謝幾位引言人。活動就到這邊結束，謝謝。

戶籍、身分個資與國家安全

Q&A 紀錄

李德財（中央研究院資訊科學研究所客座講座）

好謝謝賴中強律師，我們上午事實上還有差不多將近半個鐘頭的時間，我們聽了三位報告人從各個面向談到國家安全的問題相當沈重，我們與談人也提出各種各樣的問題，剩下的時間就開放給在座的各位，看各位有什麼樣的問題要提給我們的報告人或者是與談人。提問時請先說明你的單位姓名好嗎？

陳榮祥（資訊業）

我是剛從那個電腦界退休的人員，我民國 67 年參加台北市的電腦公會，我到今年六十九歲現在七十歲退休。那我覺得我今天來參加這個會，剛好是被那個臺灣隱私權協會的理事長邱月香邀請我參加，因為她我也最近要加入臺灣隱私權協會。那我在台北市的電腦公會擔當理監事大概三十年的時間，我看到整個臺灣的資訊產業的發展。我覺得今天比較遺憾的這麼重要的一個會，好像沒有看到我們業界的重量級的人來參加，這個有點一面倒，那個臺灣現在比較重要的兩個資訊的會，一個是台北市電腦公會，他幾乎等於是臺灣的電腦公會，另外一個是中華民國軟體協會，那剛好那個邱月香理事長，她是剛從中華民國軟體協會的理事長退下來，那我相信大家在座的應該都知道她的背景，所以我想不要懷疑她的背景。那我從昨天聽到今天，我是交大畢業的，應該我也算半個內行，昨天聽到今天大概可以把討論的議題，我的感覺分幾個議題切割來談。一個是 eID 的問題，那 eID 是一個 device 是一個辨識身份的 device，那我想那個呂教授應該很清楚，現在臺灣用的很多身份辨識的 device 不管你的信用卡，或者你其他的它的安全度跟 eID 的安全度，這個我覺得應該從技術的角度要有人深度的去探討這是一塊，這是你 input 你要代表你的身份進到一個系統，那這個安全度要有人來檢討。

另外一個就是 T-Road 的問題，T-Road 是一個傳輸的一個共通的高速通路，它有很多的那個出口跟入口，那以前我們政府的系統是在各個單位自己建，然後外包給不同的廠商，那很難去溝通，所以你要非常沒有效率的進到那個電腦的系

統去做很多事。那這已經是全世界潮流，既然在座也認為那個資訊科技是一個國家最重要的競爭力，那怎麼解決資料大量傳輸的安全問題，這又是另外一塊問題。

那另外還有一塊問題就是資料庫，分散式的資料庫還是集中式的資料庫這個問題，那我覺得因為我從技術背景出來跟法律比較不相關，到底那個隱私權人權這個糾葛，不是我們技術人可以做的，所以我今天等於以一個退休的人，半退休因為我後來做了創投投資很多新興的產業，包括生物科技我都投資了，所以我提出這三塊我希望包括昨天討論的，今天的討論的主講者也好或與談者能夠把這三塊，講的更清楚一點。然後整個系統的整合，要怎麼去管理什麼分法令可以結合在一起，這個可能是一個大的 issue 那大概是這樣。

徐子涵（開放知識基金會）

你好那個開放知識基金會徐子涵，我想大概有幾個聽剛剛幾位講者講幾個東西後，還有這個來自業界，那我覺得在我的觀察裡面大概有幾個前提或許我們需要了解，譬如說 eID、T-Road 這件事情並不是倉促上路，它其實大概可能研擬了六年到七年吧，只是當年不是用這種方法來實現。所以在那些過程當中可能包含我們的安全的領域的圈子，安全領域包含資訊安全、國家安全的圈子並沒有涉入，那為什麼在這六年之間沒有涉入或是不了解這個事情的重要或者是嚴重性，那我覺得可以推導出一個大概比較可能的觀察就是，基本上政府在處理這種新興議題跨境是沒有能力，能力是不足這個要成立，但是有權力所以這個前提應該先抓住，這個事情不是倉促上路，相關的討論可能在 internal 六到七年，至少他們跑日內瓦跑各個國家都有。那第二個其實我覺得就是在討論這些議題的時候因為，可能今天場合出席代表的關係，所以都比較談 high politics 層面也就是一般人是沒有辦法處理到的，但是在很多涉及資安及國安這個層面有實務面的問題，比如說我們也遇到受管制人員去上廁所，手機就放在桌上沒有鎖，基本上如果我是壞人就把他手機拿了，基本上我整個網子給他破了，那像這一種在 operational 層面對事涉機敏人員，也不牽涉到 high politics 的東西，是不是也需要做一些精進的作為，因為這些威脅的樣態跟資料的蒐集其實都還蠻難想像。那最後一個我覺得再二十秒，因為檯面上的大家其實都長期參與相關的政策的討論，甚至有還有中華電信獨董身份的呂兄，那我覺得是不是可以不要呼籲了，因為我們在場的可能很多都沒有相關的職位或是 background 或 position，如果在這樣的位置可以多做一些事情的話，我們就不要再每一次退下來再期待，在 decision making process 有一些作為，那我覺得這件事情可能是在國安體系都被 bypass 了，那這個代表什麼問題？是不是 espionage 可能要考量一下，謝謝。

王仁甫（資訊工業策進會資安科技研究所策略總監）

剛才那個先進就是有提到說業界的看法，我想我們臺灣的資訊界應該要檢討，我自己資安業者如果不認識我，應該不做資安，不是做資安的。我最近發生一件好笑的事情，某資安業者遞給我名片，上面名片就是 wechat，上面有印 wechat 我說那你還做資安嗎？所以第一個我覺得我們自己做資訊軟體跟資安的業者，自己心要定下來。如果你要做資安、要做軟體，麻煩你讓自己安全，不要想著要去中國做生意，人家拿你的 source code 以後可以做很多事情。這是第一件事情，所以我們當然期待業界更來參與，可是業界只想著賺錢很少人願意參與。

然後第二件事情，剛才有講到安全度的問題，我剛剛第一次演講我就說 Black Haty 在 2008 年，注意是 08 年，十二年前就破了 eID 了，那時候都有 cc 驗證人家就破了，不要跟我說它很安全，事實就破了，就像我之前講的一銀案為什麼發生？很多年前 Black Hat 就是把錢噴出來。

然後第三件事情，我想要講的是說，剛才賴律師有講到非常好的部分，data set 要分散還是集中這件事情。其實這不是技術問題，是一個安全的問題，那賴律師就講的很清楚 Verification and Validation Facility (IV&V) 的機制應該要導入，如果沒有導入這些大型的資料庫，基本上以前我在做 AI 的時候，我們程式自己寫，現在還有誰認真在自己在寫程式？全部都用 open source，open source 後面埋了多少東西誰知道？這個 data set 有多少問題誰知道，所以 IV&V 的機制其實非常重要，現在很多東西已經不是技術問題是安全問題。

然後最後一件事情我在想的是，剛才有一個先進談到說，會什麼 T-Road 這些東西六、七年很多時候大家已經討論了，為什麼到現在我們還在討論一樣的事情？我自己一直在思考這件事情，我覺得是因為大家沒有把安全當一回事，包含我們政府的官員，大家都不會像金融之前 Black Hat 的錢噴出來，你如果跟金管會，跟銀行講，每一個都回你說我們實體隔離不可能發生，可是事實上他就是發生了，我覺得這是一個安全意識問題，以上。

呂忠津（國立清華大學電機工程學系教授）

首先感謝同仁的鼓勵，我目前在中華電信有影響力，所以會去做這件事情。謝謝吳介民教授那麼清楚的分析，中華電信也是最近才成為資拓宏宇的最大股東，過去都是資策會在主導。確實每個人都要盡力，不管是有位置或沒有位置。

剛剛談到政府能力不足的問題，這是一個系統面的問題，我剛剛談到的風險就是系統的風險，系統風險常常是最困難去處理的問題。我們講說政府部門的風險在哪裡？大家都了解，政府對一個新的領域會怎麼做？因為行政體系可能沒有能力，所以它要依靠顧問公司，由顧問公司 study，剛剛廖教授有提到，顧問公司規劃完以後，行政體系才有能力提出一個 RFP(就是招標案)，RFP 訂完了以後它才能夠找外部的廠商來做建置。問題是再下來那營運怎麼辦？系統建置完以後怎麼辦？結果它還是沒有能力，所以還是委外，可以看得出來問題的嚴重性。這裡並不是說要政府是萬能的，而是說要有系統風險的概念，然後要有一個制度面，就是法制。為什麼要法制進去？剛剛賴律師講得非常清楚，我們政府過去常知道問題，但是沒有用法制來解決。相對來看不管是美國或者是歐盟，它們碰到問題都用法制去解決。我們都非常了解（法制解決這件事），但是為什麼我們做不到？這也是為什麼這兩天大家在這裡齊聚一堂，要政府重視背後系統的風險。之前講的政府做事情所謂能力不足問題，其實並不是它真的能力不足，而是不能體認系統的風險，要用體制、法制來解決。

另一件要講的事情是公私協力。一個現代化的先進國家，最多的 talent 是在民間。以私部門來取代公部門做公益的事情，是應該走的方向。以私部門的力量，會比公部門所做的服務更精緻更有效率，做得更好，也能夠跟上時代的進步。

但是公私協力如果沒有透過一個體制、法制的規範的時候，它就會歪掉了。尤其臺灣跟中國之間特殊的關係所造成的風險更大，更需要專屬法制面的處理。而法制面要有一個主責機關去執行。如剛剛賴律師所提，我們現在的法規，都是很一般性的，立意良好也跟著世界潮流在走。可是執行的時候，就發現這些系統性風險都散佈在各個部會，然後每個部會都認為好像都不是它最後要做管制，做管理，所以這個風險的管控沒有人做了，這才是最大的危機所在。這次數位身份證的施行影響太大了。臺灣正走到一個階段，是一個 branching point 的時候，需要一些人出來好好把這個事情做對了，讓我們整個國家可以做一個正確的選擇，現在就在 branching point。意思是在這個地方，問題並不是說很困難，而是在於我們的意志力夠不夠，我們的執政當局是不是能聽到這個聲音？要怎麼樣做一個正確的選擇。我覺得從昨天到今天談的非常清楚：法制化權責機關，是最基本的。賴律師剛剛講的很多都沒有做，那這麼重大的事情，我們今天這個主題又是跟整個社會安全、國家安全非常有關係，再加上吳介民教授有講，我們整個氛圍對國家的安全主權其實是高漲的，這是很好的一個時間點，也了解到說今天我們在這個世界局勢之下應該做的事情。

所以我還是回復大家說，技術一定會往前走，像在賽跑，在不斷追趕的過程中必須要有一個單位能持續不斷地 tracking 這件事情，而且不能只是被動的，像昨天唐鳳政委講的，成立一個像飛安會一樣的機構，只是做事件調查，而是要主動地去制訂一些東西，像是最近我們常常講的超前部署，什麼叫超前部署？就是要知道未來可能的風險要怎麼控管，所以必須要先想好、制定好一個制度，當風險來臨的時候，它自然就會降低了。那當我們不斷地精進到一個時間點，如果再看到未來有新科技的發展，譬如說量子電腦慢慢成熟了，雖然昨天我們副司長說一產生是全面打倒的問題，雖然是沒有錯，但是我們今天談的是一個重要國家政策的問題，當然它就受害更大對不對？因為科技的發展有個大突破的時候就進展迅速，我們來得及反應嗎？我們能不能超前部署？我們的法制、體制因應這些進展，是必須要一起來配合的。

沈伯洋（國立臺北大學犯罪學研究所助理教授）

我很簡短的三十秒，就是說剛剛業界的朋友有提到，因為這個牽涉的很廣，畢竟很多議題在兩天研討會也沒有辦法全面的談到。我不是要回應喔，我是反而是很高興子涵在這裡，那我想把他一個話把他講完就是說，之前我記得子涵有盤點過，就是其實跟 eID 有關的議題可能有十一個、十二個，但是資安就算做到完美，就是做到 perfect 也就是一百分也只能十分，人權做好可能有二十分，法制做好可能三十分。這個議題牽扯到太多的領域，那不是說我們今天只要有一個做好然後這個東西就可以推動，所以就是順便用剛剛子涵寫過的東西順便回應一下這樣。

李德財（中央研究院資訊科學研究所客座講座）

謝謝。我想預留一些時間給我們與談人，我們最後一個問題，不知道在座還有沒有什麼問題，要提出來給台上？（**陳榮祥：**我剛剛建議就是說，業界為什麼沒有被邀請來參加這一次的會？這個我是希望主持人能就中央研究院的立場來稍微答覆一下。主辦單位是中央研究院吧？）對的。主辦單位是中央研究院，這個會議是對外公開的。我們也發出了邀請函，但是業界是否參加，不是主辦單位可以代他們答覆。（**陳榮祥：**我覺得今天這麼重要的一個會，不要把臺灣的業界污名化。現在讓臺灣人得意的台積電，也是業界辛辛苦苦打上來的。資訊產業從軟硬體打的很辛苦，然後資訊產業的軟體，剛剛資策會的那位同仁，我覺得你非常的失職。你在資策會，資策會就是被我們業界攻擊最厲害的地方。為什麼？因

為國家的...）我們把時間留給我們在場其他人好不好，謝謝。（**陳榮祥：**抱歉喔，因為這個是業界，我從昨天聽到現在，對業界太不公平了，所以我特別在這裡發聲，我不是做這個的。）

王仁甫（資訊工業策進會資安科技研究所策略總監）

我才剛到資策會我也罵很兇，我們都有邀請啊，我們 iThome 也有邀請啊，我們資安產業也有邀請啊，我們軟體產業也有邀請啊，如果你今天要來嗆聲，先講清楚你在 TCA 什麼角色，然後你之前在哪一間公司講清楚，還是你是中共派來的？請你講清楚。

陳榮祥（資訊業）

抱歉喔我覺得今天台上的太政治了，我是陳水扁當市議員的時候我就是福爾摩沙的會員，我出道的比你早，你不要用這樣扣帽子的方法來扣我。你去查我的名字叫陳榮祥，你去查我的背景我第一個上市的公司，你在上面不要太政治，大家為臺灣的發展我只是覺得，我是覺得這麼重要大家在講資訊的技術，為什麼沒有真正代表臺灣資訊產業的進來，我只是請教中央研究院。

李德財（中央研究院資訊科學研究所客座講座）

這是公開的場合好不好，我想我們回歸到今天的主題，在座不知道還有沒有要提問這個我們報告人，最後面我們請那位。

與會民眾

主持人，各位與會的大家好。其實今天我在聽這些主題，然後對照昨天那個唐鳳政委的一個對這個政策要上路的表態，我覺得有點擔憂。因為在臺灣，我們談國防、談國安，那個是總統的職權，然後現在這個政策本身是在行政院，它是一個要上路，然後也是開始有一些招標，所以這裡有一些在我們憲政體制上的混亂，那也有那些在監督面、在執行面的問題。那如果我們今天要對話的是在整個政院的體系，還是總統的這個位置的體系，我想已經很清楚了。所以剛才才有業界人士，他是針對說臺灣的產業上的憂慮，那業者沒有被充分的諮詢，可是某一部份我們看到也是在國防國安上的議題，所以我想如果有機會今天的報告做成一

個比較綜合性的結論，那也扣合早上陳前副總統的一個呼籲的話，我覺得這個可能要回到一個比較政治層面的處理，然後可能是擴大比較整體的一個諮詢，否則我覺得是憂心可是我們也看到職權上不符，然後沒有一個比較有政治影響力的 leader 他願意把他的 leadership 展現，我想這是一個國家的憂慮，謝謝。

李德財（中央研究院資訊科學研究所客座講座）

謝謝我們這位同仁的關心，的確我們這一場次我們事實上邀請兩位，一個是總統府負責資安部分的副秘書長，李俊俋副秘書長，還有國安會的代表，他們兩位官員都不克出席。那剛剛業界的部份，這是一個 open forum，事實上是我們邀請函出去的時候的確是有法人，因為這是一個學術研討會，我們是以學術研討會的方式來針對國家這個在推動資安議題來做個討論。但是來參加的人員是什麼人員，我們事實上是一個公開的（研討會），我想這一點是我並沒有說排除業界，因為時間的關係我們是不是讓與會的報告人跟與談人，是不是做一個簡單的一分鐘或三十秒的一個結論好不好？那個從王仁甫這邊開始。

王仁甫（資訊工業策進會資安科技研究所策略總監）

我必須先跟剛才這位先進道歉，我剛才有比較激動。但是我必須澄清我剛到資策會，我們資策會有在改變。然後再來第二件事情，我自己都有廣泛邀請產業界的人，所以我剛才只是要澄清，如果在全球化美國整個對中國的態度改變時，我們自己資訊業者跟資安業者要有自己的態度，現在美國在講的都要是安全的 5G，如果我們想著說我們要臺灣的資訊業還要在中國做生意，然後這邊也賺那邊也賺，然後兩面討好我覺得那個才是沒有資安意識，那如果你要做資安中國的生意就不要來承包臺灣的案子。

吳介民（中央研究院社會所研究員）

時間關係我講的非常簡短，我覺得對臺灣我們在討論這個 eID 的問題，就是說除了一般民主國家所注重的隱私跟人權議題之外，臺灣的國家安全確實是一個不能忽略的問題。那我覺得我們的政府到我們公民社會，特別是我們政府要非常非常嚴肅以對，非常非常嚴肅以對，而且這兩天的研討會集合了資安資工的專家，集合了法律的專家還有政治社會學的專家，其實就顯示這個問題其實在臺灣的學術界是有很大的共識，我們必須非常謹慎處理這件事情。我覺得中研院包括李院

士在這裡，我覺得中研院有很大的責任要讓我們最高層的政治政黨的領導，要知道說這件事情攸關我們臺灣未來的發展，這個發展包括經濟發展喔，我們資安沒做好怎麼發展經濟是不是？所以呢我們不是不要經濟發展喔，我剛才說過我們不是不要數位轉型，我們不是要落後於世界最新科技的發展，而是我們怎麼樣去駕馭這個科技，然後我怎麼樣獲得更好的發展模式更安全，這是第一個訊息。

第二個訊息是因為這裡面因為國家安全牽涉到中國因素，那中國就是擺明中華人民共和國就是要吞掉、吸納掉、吃掉中華民國臺灣或是臺灣中華民國，那這個事實你要不要當作一個真實的威脅來看待，如果不要的話我們今天什麼事情都不用談，今天這個 panel 可以取消掉，所以這是一個基本的事實我們要不要面對？那這裡面就存在一個剛剛王仁甫先生也提到的，其實臺灣就是整個資訊產業有大量的利益跟中國糾結在一起，那我覺得這是一個歷史共業，我覺得我們不要站在污名或譴責或獵巫的角度看這個問題。但是另外一方面也不能不顧這件事情，過去幾十年跟中國的經濟的連帶關係，造成今天臺灣未來發展的問題，我覺得這兩面性都要顧到，我們不能鴕鳥也不能獵巫，然後要勇敢去面對這個問題這是一個歷史共業。

那中華電信，然後中華電信底下的子公司、孫公司，還有資策會，它們裡面的大量的人員其實裡面還有過去 IBM 商業單位的，這整個網絡是一個歷史共業，那臺灣如果要一個安全乾淨的處理到隱私權人權資料的運用，承包工程跟營運，到底怎麼獲得一個安全乾淨的作業的環境，其實真的需要大家集思廣益，真的是要好好思考，那這個是一個非常嚴肅的問題，在這個事情都還沒解決之前政府真的不應該匆促上路。

沈伯洋（國立臺北大學犯罪學研究所助理教授）

我簡短總結一下就是說，因為我還是回歸就是我自己原來的領域就是犯罪學，那不管這種個資的蒐集，它其實最主要在我們犯罪學界，還是歸類在人權的侵害，那只是說現在的討論不得不讓我們先把國家安全擺到最前面來談，因為就是這是立即的一個威脅。但是因為弱勢者他可以受到這個的保護，我們不是說我們完全否定這樣一個制度，因為像日本的法制在這些的例外裡面就有一個譬如說社會福利稅務等等之類的，就是弱勢者的確有可能會得利，但是弱勢者更可能會受害，因為他不知道要怎麼拒絕，或者是他沒有能力去拒絕這樣一個系統，所以在這樣一個人權侵害之下，更不能忘記的是不管是華爾街還是保險公司，還是像美國很多大學，都是利用這些數據過來做詐欺，然後進而再讓這些人掉到社會的深淵裡

面不得翻身，所以這些事情其實就是就像我剛剛提到的，它牽涉的層面真的太廣了，我們光是做好其中一個層面都沒有辦法說我們很有信心的把這件事情推出去，我想這是我最想要強調的一點事情，謝謝。

廖宜恩（國立中興大學資訊科學與工程學系教授）

我有兩點結論，第一個就是有關政府資訊系統委外廠商的安全稽核，以及供應鏈管理與風險管理，都是非常的重要，尤其是 eID 政策的推行。第二點就是我剛剛講了，也是回應昨天吳齊殷教授與剛剛陳建仁前副總統所講的，整個 eID 政策的推動，政府應該採取公開、透明、對話與集智的方式，才能建立數位治理最紮實的基礎。

呂忠津（國立清華大學電機工程學系教授）

我想做一點結論，就是希望經過這次的討論後了解到，目前推動 eID，在沒有法制化的情形下是不應該進行的。但是我希望更進一步，如果未來有法制化的機會，能夠將身分證的使用單純化，把它限制下來明文規定，讓在高科技的時代裡面，所增加的風險能夠持續的降低下來，謝謝。

賴中強（經濟民主連合智庫召集人/恒達法律事務所律師）

港版國安法被中國人大制定生效以後，任何臺灣人如果到香港即使只是轉機，香港特區政府有權力要求這個臺灣人交出涉及中國國家安全的資料，請問我們這個晶片身分證計畫，到時候的總工程師、高階工程師或擁有密碼的人，他如果到了香港被迫要求資料的時候，我們政府是怎麼應對？我們該不該管制這些人出國？如果我們要管制他出國的話法律依據是什麼？前一陣子為了要肺炎期間要管制醫護人員出國那個法律依據就引起很大的爭議，而我們將來能夠不管制這些人到香港到中國嗎？如果我們要管制這些人到香港到中國的時候，立法完成了沒？沒有法律依據這個晶片身分證可以上路嗎？

我絕對不懷疑許文龍先生是愛臺灣的，我也不懷疑今天來參加這個研討會的人，大家都是愛臺灣的，但是就如同當年許文龍先生為了他的鎮江廠被封廠，被銀行抽銀根，他的幹部他的愛將要被關到中國的監獄裡面，許文龍先生妥協了。他必須妥協，因為他為了救他所愛的，不要讓臺灣人面臨跟許文龍一樣的兩難，讓他被迫要講出他支持反分裂國家法，許文龍先生在後來的許多場合，他都拜託

他所認識的朋友幫他澄清，我今天也幫許文龍先生再澄清一次，他是被迫的，希望我們不要有下一個被迫。

李德財（中央研究院資訊科學研究所客座講座）

謝謝，今天這個場次的確是中央研究院召開這麼一個研討會，主要也是希望有這麼一個公開的場合，讓我們專家表示對政府在推動這個 eID 計畫需要考慮的問題。我想這兩天大家看到問題、聽到問題，我希望這些問題就像今天陳建仁陳前副總統講的，希望透過這個公開的機制，讓我們能夠提出我們的建議。今天上午這個議題的確牽涉到國家安全，的確是相當嚴肅的問題，各位也聽到了問題，我們希望利用這個場合，讓更多人了解，其實事實是我們坊間去問，隨便問人說到底政府在推動晶片身分證的計畫知不知道？多數我接觸的人都不知道、不清楚政府在推動這個計畫，當然更遑論說這個計畫對我們國家安全的影響。

事實是之前我在國安會擔任諮詢委員的時候，我對這件事情，一直呼籲就是剛剛那位同仁提到說，這個是行政院的還是府方的？因為職權是在行政院。的確我們站在國安會立場提出政策建議，提出需要國家安全的考慮，幾位報告都已經呈現出，希望利用這個機會，讓更多人了解這個 eID 計畫沒有準備好最好不要上路，或是在這個方向下，我們怎麼樣調整行政院在推動的這個 eID 計畫，我們做政治上的調整，是不是先立法完成之後，先設好專責機關，然後是不是在這個計畫當中，如果內政部礙於這個國民身分證每十年需要換發的法規，是不是可以把國民身分證的部分、自然人憑證部分、T-Road 的部分脫鉤？讓行政院負責把國民身分證換發就先上路，然後在 T-Road 那部分再慢慢按照 my data 的方式，小規模來測試是不是來進行，這是不是一個解決方法？我想我們利用這個機會，事實上今天我們中央研究院應該會有一個報告，正式呈給行政院或是總統府這邊參酌，是中央研究院政策報告對 eID 政策的疑慮是什麼，結論是什麼。

今天這個會議我真的是感謝大家，有這個機會大家有公開交換意見，我想時間的關係就結束上午第四場的討論會，謝謝與談人。

數位轉型與可課責的智慧政府

Q&A 紀錄

潘國才（國家發展委員會資訊管理處處長）

各位先進午安，謝謝嘉良引述我昨天講的話，我到現在也都是抱持同樣的態度。其實我是要謝謝郭老師，我昨天講那句話，其實是偷看到了郭老師今天簡報裡的內容。那張有 root identity 的圖讓我印象非常深刻，老師建議可透過 root identity 衍生出很多不同的 identity 出來，對於這個建議，我非常的認同。所以我在這邊想要請教的是郭老師的看法，如果將 New eID 套用郭老師 root identity 的概念的話，國民有 root identity 之後，在各種其他的應用場景上面會衍生出各式不同的 identity one、identity two、identity three 等，甚至於還有其他的方式在網路上面去做身分識別，這是不是可行的方式？也就是說，每個國民還是有一個基本的一個 root identity，root identity 就用 eID，New eID 做為憑證，不曉得是不是一個適當的方法？

郭耀煌（國立成功大學資訊工程學系暨研究所特聘教授／數位生活科技研發中心主任）

我會放那張投影片是因為每年上物聯網設計的課時都會拿出來跟學生講，我個人覺得確實是一個方向，至於細節的部分需要再研究。我是從工程系統、工程應用做討論，從目前現狀來看，身分證對我來說本來就是 root identity，我跟潘處長一樣，不帶身分證，我只帶駕照在身上，身分證、健保卡都是放在家裡，因為 root identity（身分證）萬一掉了很麻煩。我們現在身上一堆卡，本來就有不同的 identity 的資訊、不同的呈現。只是將來萬物聯網之後，identity management 會很重要，尤其跟政府事務有關的 identity management，我是覺得要有更完善的設計。回到潘處長的問題，個人認為應該是一個可行的方向。

與會民眾 1

你好，我想請教高副主委，剛剛聽起來介紹了很多智慧政府想要達成的願景跟功能，不過，要達成政策優化的目標，好像並不一定要跟數位身分證有直接關聯。在不推動數位身分證的狀態之下，政府的資料交換，還有一些數據統計，本來就可以做到，或取得這些政策所需要的一些資料。另外也想要問，剛剛有提到說人民要申請政府服務的時候，都會經過人民自己的同意，但是關於同意這件事情，大家都看過很多同意書，它就是很長很長的條款，那會不會在我想要使用政府的服務、下載我自己的資料同時，和我在打勾選取「我同意」的時候，不小心授權了我的資料被加值應用這件事情？因為剛剛也有提到說有「加值應用」這件事情，可是彼此之間並沒有明確的區分，因此這部份會有一些疑慮，謝謝。

與會民眾 2

各位演講者大家好，我想請問高副主委，也是當事人同意的問題。高副主委有提到政府跟人民拿資料的時候一定要經過當事人的同意，但是我們知道，人民跟政府的地位不對等，當事人同意往往其實會缺乏個人自由意志。政府有沒有打算要解決這件事情？我知道的是歐洲 GDPR 是有做一定的規範，政府需要有一定的審核機制，但是台灣的個人資料保護法好像沒有這一點。另外就是，政府如果要做目的外的使用的話，根據現行個人資料保護法第 16 條，至少有三項的例外規定，像第六項是有利於當事人權益，第二項是為維護國家安全或增進公共利益所必要，也就是公共利益條款。這其實規範得相當空泛，我們怎麼樣確保政府不會做目的外的使用，也就是不會僅依據這些公共利益的空泛條款來做目的外利用？

高仙桂（國家發展委員會副主任委員）

第一個問題，政府政策的優化跟 New eID 的關係為何？今天為什麼會把智慧政府方案具體地跟大家說明，就是因為大家討論的重點似乎是認為沒有 New eID、沒有 T-Road 的話，智慧政府的若干政策就沒有辦法推動。事實上，New eID 只是作為數位身分辨識之用，通過辨識後，民眾透過 T-Road 的入口網取得線上服務。這僅是智慧政府推動方案其中的一部份而已，並不是全部。所以數位治理的優化，的確不一定需要 New eID。今天跟大家報告智慧政府行動方案，主要係數位治理對政策的優化很重要。我舉一個例子，在疫情期間我們怎麼樣判定整個經濟活動有沒有明顯的復甦？過去都要靠統計的數據，但統計數據都要花一些時

間，可是我們現在某程度可以用到非涉個資的數位足跡，看到封城禁令解除、開放以後大家的活動形態，就可以做為景氣好壞的判斷，也就是說，智慧政府的相關措施，在政策優化、政府決策這方面，透過所謂的大數據可以發揮作用，這個其實是不需要 New eID 的。

第二，先前其實有講到，智慧服務取得，設計的機制是需人民同意，亦即無論是 MyData 或者是將來 T-Road，所謂的人民同意，都一定要符合個資法所規定的明確告知，條款中會載明取用資料的內容、時間、地點、運用的範疇，都必須要符合個資法的規定。我們在規劃 MyData 平台，同仁在研擬同意條款的時候，會請法制單位的同仁參與，一定要符合個資法的相關規定，不會是氾濫的授權。

第三，其實我們的 MyData 跟 T-Road 都是人民向政府索取個人的資料，無涉政府去取用個人的資料。跨政府（機關）之間目的外的利用，一定要有公共目的，或者是研究條款。政府取用人民的資料做目的外利用的時候，如果違反個資法的相關規定，都要負起民事、行政與刑事法律責任。剛剛其實大家有提到，我們怎麼樣去增進人民或公部門的個資素養及認知，這很重要，行政部門也儘量朝這個方向來邁進，公務員在處理涉及民眾個資事務時，絕對是會遵守既定的法令。

與會民眾 3

我想請教黃東益老師，剛剛提到民眾調查的結果蠻悲觀的，對隱私這個概念，民眾無感，似乎並沒有很清楚的認知，那麼我們現在做這件事情（指討論 eID 政策）實際上很重要，卻可能沒有民意基礎（因為人民對於隱私風險似乎無感），國會就不會重視，進而行政體系也沒有一個監督壓力，關於這方面的議題我想就不會受到行政機關的重視。請問您有什麼看法？

黃東益（國立政治大學公共行政學系教授）

我可能沒有很清楚了解你提問的內容。統計資料結果要強調的是說，民眾在決定要不要把他的隱私資料授權給政府的時候，隱私的風險不是一個考量因素。民眾比較重視的利益，或者是他對政府信不信任這件事情。我覺得你剛剛好像把這個結果做了一個比較不一樣的詮釋？

與會民眾 3

所以我剛剛就是提到，人民對於便利性會勝於對隱私風險的考量，因此想請教的就是，如何讓民眾對於隱私的潛在風險更有所意識，進而願意去討論？不知道黃老師對這方面有沒有什麼想法？

黃東益（國立政治大學公共行政學系教授）

這是大哉問。我們政府部門通常會投注很多資源在看得到、感覺得到的具體風險，比如說針對核電廠安全性，會有核安的演練；然而至於一般的民眾，甚至在學校中，我們有做過什麼樣的資安演練嗎？好像沒有。我自己的經驗是有一天早上打開電腦發現，信箱中大概有好幾百封的信突然不見了，為此我其實難過了好幾天。我想大家應該有類似的經驗。所以，關於你的問題，如何讓民眾的隱私風險意識能夠提升？也藉這個機會回應高嘉良兄所提到的，政府有些時候面對審議民主的態度是，如果想要辦審議會就辦，辦完了之後，可能也不是非常嚴謹地去看待這件事情。如果要讓民眾一起關心這個議題，那我們可以做一些事情設法引起公共的討論。例如，丹麥的 The Danish Board of Technology，針對很多社會上可能還沒有辦法形成共識的議題，由民眾提案，委員會就根據民眾的提案去開審查會及公眾的審議及討論會，該委員會也發展出各種不同的討論方式，透過公共資源制度性、長期性的投入，可以讓民眾來關心這些議題。另外，如法國公共政策辯論委員會(La Commission nationale du débat public, CNDP)，也有類似的機制。而民間團體的力量當然也重要，比如說 g0v，或是開放文化基金會等。但民間的資源還是不夠，如果政府能夠長期性地建立機制的話，我覺得對於民眾隱私風險意識的提升應該會有幫助。不過，公共審議機制的建立，我大概也是在頭髮還蠻黑的時候就開始倡議了，現在頭髮變半白了，都還沒有看到成立，我想是人微言輕。這個大概是我的想法，謝謝。

邱文聰（中央研究院法律學研究所研究員）

首先我要謝謝高副主委跟林次長來參與這個會議，這兩天的會議當中，在各個政府部會當中，最高層級的應該就是兩個國發會跟科技部，參與度最高。尤其是國發會，除了今天副主委到場之外，昨天潘處長與李參事也都參與。其中潘處長在這個會議之前就已經約了我們大家先進行一些意見的交換跟溝通。所以我想國發會確實非常認真看待這件事情。不過我接下來要請教的問題是，剛剛高副主委提到的兩個關鍵詞，我覺得非常好，一個是「以人為本」，另外一個就是您也

覺得「可課責性」這件事情是重要的。但現在問題是在於，如果我們強調整個智慧政府是要以人為本的話，但是現在偏偏我們看到 eID 的發行當中，除了允許個人可以選擇關閉自然人憑證，卻不允許個人可以選擇是否開通或者是關閉晶片的功能。在這樣的一個情況下，還能夠稱做是一個「以人為本的智慧政府」的方案嗎？我知道您剛剛有提到，eID 確實並非推動智慧政府的一個必要的元素，而且 eID 的發行也不是國發會執掌的範圍，但做為整個推動智慧政府的一環來講，目前的 eID 政策可能真的會讓這種以人為本的智慧政府的推動沾染上非常大的一個陰影，這是第一點。第二點是您講到可課責性的部份，尤其是 T-Road 這個部份，從剛剛您的說明當中，一再強調說未來一定是可以課責的，包括說政府彼此之間的資料交換會遵循個資法的規定，T-Road 本身也會記錄政府資料的足跡，不過之前我們跟潘處長的一個交流過程當中，大概得知的狀況是，T-Road 本身對於其他政府機關之間的資料交換，並不會做管控，意思就是說，國發會所創的這條 T-Road 只是一個 Road 而已，只是類似高速公路的建設工程，做完之後，路上要怎麼跑、跑什麼車、要不要有交通警察、要不要設置紅綠燈，這些都不是國發會要處理的事情，這樣的話，這條 T-Road 可以確保它的 Accountability 嗎？這是第二點。除此之外，方才提到所謂的數位政府足跡，我們了解到的是，為了要知道這個 T-Road 的 KPI，所以我們要記錄各政府機關之間資料交換的次數，至於哪一個政府部會以什麼樣的理由蒐集或者要交換另外一個部會的資料，以及提供被查詢者反查詢的機制，其實並不在 T-Road 規劃裡面。那這個部份對於要達成可課責性的數位政府來講，是一個蠻大的缺憾。副主委在這幾個議題上是不是可以提供我們一些說明？整體來講，如果要推動數位政府的話，對於公務機關與非公務機關對於數位資料的蒐集、處理、利用，單純僅仰賴個資法的規範，恐怕是不足的。從國外的經驗來看，包括德國、愛沙尼亞、日本等國家都有專法去規範數位資料的蒐集、處理、利用，尤其是與身分相關以及數位身分的資料。如果由內政部來推動，顯然比較困難的話，可否請國發會這一端，在個資法的修法的過程當中，納入一個專章來處理數位身分足跡的蒐集、處理、利用的問題？這是附帶補充的問題，謝謝。

方修忠（台灣科技產業法務經理人協會）

我回應一下邱老師的意見，我認為專法是非常重要的。以個資法來說，最近一次修法是 104 年。個資法修法有一定要配合 GDPR 嗎？應該是不需要的。20 年前我們在談個資法的時候，法規主管機關為法務部，修法背景是因為中華民國台灣—台澎金馬要加入 WTO。現在如果要做 eID 的話，以個資法第 55 條來看，法務部也有一定的權責，可是，國發會又在個資法上面把這個責任承擔起來了。

各目的事業主管機關之認定，會因不同事業而有異，因此難以統籌。第二，電子簽章法的主管機關又是經濟部，資通安全法的主管機關就更特別了，是行政院。所以這兩天一直在講的這三部法：個資法、電子簽章法、資通安全法，其實是很難去操作的，所以我同意剛剛中研院邱老師的意見，我認為應該要有一個專法，或至少在上開法律中設置專章，同時也要有一個專責的政府機關加以統籌。另外，這兩天也談到所謂 T-Way，T-Way 跟 T-Road，我覺得大家似乎是抱持某些開玩笑的意味在談，但是 T-Way 是屬於一個韓國航空公司的商標，經濟部網站上應該可以查到，所以不建議開這樣的玩笑，以上。

高仙桂（國家發展委員會副主任委員）

謝謝邱老師還有另外一位與會者的提問。關於邱老師的第一個問題，我們數位政府推動絕對是以人為本，因為政府所有的施政都以創造人民最高的福祉為依歸，我想這是沒有疑義的。我方才有提到，其實我們在國家數位化的進程裡面，我們會享受到數位化的利益，可是我們也會遭受到數位化帶給我們的風險，比如資安的風險、個資的侵害風險等。在 New eID 內政部現行版本中，可供民眾決定你可以選擇自然人憑證開啟與否。但是在我們開跨部會會議的時候，也有部會提議一定要把自然人憑證放進去。基本上，台灣是一個多元的社會，有不同的聲音，嘉良有講到一個很好的事情就是，不管是內部政府的課責或是外部公民的力量，其實都可以反映給我們政府，提出政策建議。這兩天的會議其實就是一個公民力量非常好的展現，得以對政府政策提出意見及建議。其實，我們之所以在這裡、內政部也有來參加，也就是因為政府部門都很願意聽取大家的意見，做為後續政策研擬及修改的參據。不過礙於層級有限，我就說到這裡。

第二個問題，談到 T-Road 的可課責性時，提到在 T-Road 入口網，如果是個人要申請所需要的資料或服務時，若經申請人同意，是沒有問題的，個人可以分別到 A 機關、B 機關要資料，或授權 A 機關將資料傳送到 B 機關；然而若涉及跨機關的個人資料交換，的確，現在沒有一個法令可以規範跨機關的資料交換。為什麼？因為政府的服務太多元化了，我不知道是否有辦法透過專法來規範跨機關的資料交換，還是要回歸到所謂的個資法母法的相關規定？也就是說，所有的機關取得資料一定要在其法定職權內蒐集、或具備公共利益，在不然就是取得當事人同意，不然是違反個資法的規定。至於目的外的使用，有一大堆條款，我只能跟大家說，我們透過 T-Road 提供政府服務時，如果涉及未經個人同意的跨機關資料交換時，一定會充分檢視該資料交換行為是否違反個資法之規定。我們只能做這樣的承諾。

再者，關於專責機關與專法相關問題，個資專責機關的部份，唐鳳唐政委昨天業已以行政院的層級宣示，現在正在籌劃跟規劃中。至於專責機關設立的程序跟 New eID 的發行不一定有必然的關係。另是否在個資法增訂專章來規範數位足跡之問題，個資法的修正刻正檢討中，可能無法在此給予承諾，但我覺得今天參加會議很有收獲，我會把大家給我們的意見及建議，做為我們後續推動智慧政府相關措施的重要參據。謝謝大家。

謝國雄（中央研究院社會學研究所特聘研究員兼所長）

今天高副主委來傾聽民意，我們預祝她高升，民意才能上達天聽。接下來請何老師發言。

何建明（中央研究院資訊科學研究所研究員）

我其實想問一個不成熟的問題，這個問題是來自於剛才林次長提出來的——核心價值很重要，而尋求核心價值何在、或從何而來，必須要有比較系統性的思考。從系統性思考的觀點出發，我想提出的就是：MyData 政策其預計的核心價值為何？以及，其到底在整個系統裡面扮演什麼角色？我在思考的是，我的人生到底什麼時候會用到 MyData？最後我猜想，人生中我自己應該不會用，而是我兒子在我離開以後他可能會用，因為他可能會希望把我的 Data 總歸戶。我很懷疑我是否真的會需要它。因此我的第一個問題是，如果我要退出的話，能不能讓我退出？另外一個問題是，我的資料原來都分散在各個部會，那現在把資料集中起來，是我的風險，同時也是政府的風險。因此我希望的是，一開始沒有我的同意，資料不應該被集中，這部分也牽涉到剛剛講的核心價值的問題，也就是說，在設計機制的時候，核心價值有沒有被思考。就我所知，目前政府機關政策制定者可能都覺得說，技術上將資料集中在一起，好好發揮利用價值就是好事，卻忽略了核心價值思考，也就是所謂的系統性的思考。剛剛討論到數位足跡與個資可能要增訂專章來因應，那麼智慧政府的整體規劃，從系統性思考、核心價值的思考面向而言，是否也應該有專法來處理？

高仙桂（國家發展委員會副主任委員）

剛才提到 MyData 核心價值在哪裡的問題，其實我覺得只有一個核心價值，就是便民。比如說，今天我要去申辦某項政府服務，需要攜帶三張證件，但我只帶了兩張（證件），這個時候，如果剛好是屬於 MyData 平台 31 項資料其中之一，

也許就可以用電腦，透過身分識別憑證，就可以從 MyData 取得該資料了。我們的核心價值就是，在已邁入數位世代的現況下，透過 MyData 使儲存在政府的資料，民眾得以直接透過線上取得，也就是便利性，當初的想法是這樣。至於所謂系統思維，我們絕對沒有因為設置 MyData 平台而把所有的資料集中在一個地方，其實 MyData 只是一個入口，還是必須進入政府 GSN 網路，進而連到各個部會，也就是說，我們現在只開放 31 項資料，各該資料必須個別取得同意才能取用，比如說戶政資料必須連到戶政機關，經過個人同意，而且通過身分辨識、個人同意，再連到 GSN 網路，戶政機關這端還是有一個緩衝(buffer)，確認以後，再從系統進去拿資料出來。所以 MyData 的後台，不是把你一個人所有資料都放在那個地方。最重要的，沒有你個人同意，其實是完全拿不到的。另外開個玩笑，我們現在還沒有代理人制度，所以何老師你的兒子要拿你的資料大概也有難度。

謝國雄（中央研究院社會學研究所特聘研究員兼所長）

謝謝，關於核心價值如何貫穿到整個政府施政裡面，還是要請林次長來回應。

林敏聰（科技部政務次長）

核心價值是會因為你站在不同的立場與位置，以及不同的個性而有所不同。比如說，一個很依賴 MyData 的人，他可能覺得很方便，像是最近要報稅／申報財產，藉由自然人憑證就非常簡單，只要按照指示填寫就好，也不用刻意去找存摺。可是另一方面也要很小心，在這個便利性過程當中，你可能就不知不覺掉到沒有意識到的價值陷阱當中，比如個資保護或後來可能會有的風險。所以，核心價值不是一等於一、二等於二這麼簡單的事情，它必須要有一個共同討論的過程與民主的參與過程，不是有誰來定義之後就沒有爭議了，也不是極端保守或極端自由，這兩個極端的光譜中間的平衡、共識怎麼建立是我們所要討論的。關於這點，我想分享關於共同協作的概念，以北歐為例，北歐社會民主國家就很重視工會、政府跟資方對於重大的公共政策跟勞資的共同協作，彼此共同去找出解方。一般來說，這三個單位其實是代表不同的核心價值，資方的核心價值跟勞方的核心價值，在資本主義社會，有很大的不同。當然政府就不一定了。所以在這裡面其實有一個共同協作的過程，也就是說，類似像這樣的一個爭議性比較大、在價值上可能是有比較具體衝撞的爭議，應該有個共同協作的一個程序；另外一個是共同監督，像是剛剛討論到 MyData 會不會被濫用這件事情，沒有透過一個民主參與程序去共同監督這 Data 本身的運作跟營運，其課責性就也不可能具體產生，因為人民根本不知道這政策形成及施行過程中有發生什麼事情、決策究竟如何作

成。我想有這樣的民主參與過程才有辦法把類似課責的機制引入想像中的制度裡面，才有辦法達到一個比較具備可信賴性的政策決定，可信賴性本身必須透過一些具體機制去建立。謝謝。

潘國才（國家發展委員會資訊管理處處長）

再利用大家一點時間。第一，我再強調一次，MyData 沒有將大家的資料集中放在一起；第二，回應邱老師剛剛的提問，T-Road 上面為什麼不去做一個記錄？其實是有記錄，但我們以資料最小化的蒐集方式來處理。也就是說，是我們不是把各項的資料全部都集中記錄下來。因為這麼做的話，那麼 T-Road 反而變成了資料蒐集的機制，這樣子反而蒐集了更多人的資料保存在 T-Road。因此，T-Road 上面會留下來的資料是是機關之間傳遞的紀錄，至於傳遞的內容是什麼，則是由調閱資料機關會提供。調閱機關會記錄傳出了什麼資料，而不是記錄在 T-Road 系統上。

莊庭瑞（中央研究院資訊科學研究所副研究員）

對 MyData 系統仍然感覺有些議題可能還需要澄清，問題在於究竟是採用 opt in 還是 opt out 模式？也就是說，是使用 MyData 把自己資料調出來？因為現在有商業機構接受個人從政府機關調閱資料加以申請貸款，就會產生疑問：是否所有人的資料都可以經由 MyData 調出來？如果不希望使用 MyData 服務的人，他要特別跟國發會聲明退出這個系統？還是以申請書表明我需要使用 MyData、請把我的個資加入此服務系統當中？我希望能夠澄清此議題。

謝國雄（中央研究院社會學研究所特聘研究員兼所長）

高副主委表示可否會後再一同交流？我們今天這場到這裡結束，謝謝引言人、與談人，以及各位熱烈的提問，謝謝大家。

附件六

研討會議程

2020

National ID Card & Personal Identification in the Digital Era

數位時代下的國民身分證與身分識別研討會

National ID Card & Personal Identification in the Digital Era

活動時間

109.7.29 WED — 30 THU

活動地點

中央研究院人文社會科學館3樓 國際會議廳

7.29 WED

09:30-09:45 報到

09:45-09:55 開場致詞
黃進興 中央研究院 副院長

主題一：戶籍管理與身分證的晶片化及數位化

10:00-12:00 主持
李建良 中央研究院法律學研究所 特聘研究員兼所長

報告
邱文聰 中央研究院法律學研究所 研究員
李育杰 中央研究院資訊科技創新研究中心 研究員
吳齊殷 中央研究院社會學研究所 研究員兼副所長

與談
羅秉成 行政院 政務委員（不克出席）
鄭信偉 內政部戶政司 副司長
李念祖 私立東吳大學法學院暨法律學系 兼任教授／總統府人權諮詢委員會第一至第五屆委員
林煜騰 民間司法改革基金會 執行委員／圓矩法律事務所 律師
Q&A

12:00-13:00 午餐

主題二：數位足跡、剖繪與監控

13:00-15:00 主持
林子儀 中央研究院法律學研究所 兼任研究員／前司法院大法官

報告
劉靜怡 國立臺灣大學國家發展研究所 教授／中央研究院法律學研究所 合聘研究員
莊庭瑞 中央研究院資訊科學研究所 副研究員
蔡文軒 中央研究院政治學研究所 副研究員

與談
唐　鳳 行政院 政務委員
李世德 國家發展委員會 參事
何明諠 台灣人權促進會 副秘書長
Q&A

15:00-15:10 茶歇

主題三：T-Road的資料庫串連與數位身分證的近用控制

15:10-17:30 主持
顏厥安 國立臺灣大學法律學院 特聘教授

報告
吳全峰 中央研究院法律學研究所 副研究員
查士朝 國立臺灣科技大學資訊管理系 教授
王大為 中央研究院資訊科學研究所 研究員
王柏堯 中央研究院資訊科學研究所 研究員

與談
潘國才 國家發展委員會資訊管理處 處長
簡宏偉 行政院資通安全處 處長
李柏鋒 開放文化基金會 董事長
Q&A

7.30 THU

09:30-09:45 報到

09:45-09:55 開場致詞
陳建仁 中央研究院基因體研究中心 特聘研究員

主題四：戶籍、身分個資與國家安全

10:00-12:00 主持
李德財 中央研究院資訊科學研究所 客座講座

報告
王仁甫 資訊工業策進會資安科技研究所 策略總監
吳介民 中央研究院社會學研究所 研究員
沈伯洋 國立臺北大學犯罪學研究所 助理教授

與談
總統府 李副秘書長俊俋（不克出席）
國家安全會議（不克出席）
廖宜恩 國立中興大學資訊科學與工程學系 教授
呂忠津 國立清華大學電機工程學系 教授
賴中強 經濟民主連合 智庫召集人／恒達法律事務所 律師
Q&A

12:00-13:00 午餐

主題五：數位轉型與可課責的智慧政府

13:00-15:25 主持
謝國雄 中央研究院社會學研究所 研究員兼所長

報告
郭耀煌 國立成功大學資訊工程學系暨研究所 特聘教授
何建明 中央研究院資訊科學研究所 研究員
陳舜伶 中央研究院法律學研究所 副研究員
黃東益 國立政治大學公共行政學系 教授

與談
林敏聰 科技部 政務次長
高仙桂 國家發展委員會 副主任委員
蕭景煜 行政院科技會報辦公室數位國家組 主任
高嘉良 g0v.tw 台灣零時政府社群 共同發起人
Q&A

15:25-15:35 茶歇

綜合討論及會議結論

15:35-16:30 主持
李建良 中央研究院法律學研究所 特聘研究員兼所長

與談
李育杰 中央研究院資訊科技創新研究中心 研究員
劉靜怡 國立臺灣大學國家發展研究所 教授／中央研究院法律學研究所 合聘研究員
吳全峰 中央研究院法律學研究所 副研究員
王仁甫 資訊工業策進會資安科技研究所 策略總監
何建明 中央研究院資訊科學研究所 研究員

主辦單位

中研院法律所 資訊法中心 Information Law Center, IIAS

協辦單位

中央研究院 社會學研究所 Institute of Sociology, Academia Sinica
開放文化基金會 Open Culture Foundation
WITSA
TAUP
TWNIC
Watchout沃草
ISA