

國立政治大學公共行政學系

碩士學位論文

社群網站運用數位足跡的政府監理策略探討－

以 Facebook 在台灣的運作實況為例

Regulatory Strategy on Social Media's Digital Footprint -

A Case Study of Facebook in Taiwan

指導教授：蕭乃沂 博士

研究生：陳柏安 撰

中華民國 110 年 4 月



摘要

劍橋分析事件的爆發，監理社群網站利用數位足跡投放針對式廣告的行為日益重要。筆者嘗試透過檢閱文獻釐清探討監理策略應達成的目標，並透過利害關係人訪談瞭解執行的現狀以及可能遭遇的困難。茲簡述發現如下：

首先，監理策略應該達成保護使用者隱私、保護寡占市場下的使用者權益，與杜絕業者欺罔行為的目標。第二，雖然對於通訊監察的疑慮，應不致構成外界反對政府監理的明顯理由，但是懷疑政府是否有足夠能力執行監理事務。目前監理策略也多停留在立法階段，執行不是幾乎沒有開始，就是還在起步，也導致後續執行與評估的探討幾乎無以為繼。第三，經濟部工業局雖然受命為社群網站的個資法主管機關，基於產業推動優先，與監理任務難以與既有業務相容的現實，監理社群網站的態度趨於被動。第四，仿照歐盟設立資料保護專責機關的芻議，看似解決事權不集中的良方，但也將面臨法制與組織面水土不服、設立初期權限與既有監理機關競合，以及任務如何順暢交接等，組織設計過程也宜審慎思量。

綜上所述，筆者提出以下建議：首先，政府從事資料治理時，應摒棄效率至上的心態，在日常作業中便應將資料保護完整落實。第二，政府不應拘泥於設立形式或組織上的個資保護專責機關，而是從服務設計與傳遞著手，確保使用者與業者的需求能被立即滿足。第三，雖然本研究尚未證實管制悖論文獻所警示的，監理可能扭曲市場機制，並加劇數位廣告產業壟斷的因果關係是否存在；然而數位廣告的產業的壟斷卻已廣受矚目，筆者認為後續的重點不是繼續論證該關係的存在，而是立即就既成事實盡速研擬對策。

關鍵詞：社群網站、個人資料保護、數位足跡、監理、管制

Abstract

The outbreak of Cambridge Analytica scandal has aggravated the importance of regulating social media exploiting of digital footprint on serving targeted-advertisements. I clarified goals of regulatory strategy by reviewing literature and difficulties of implementation by interviewing stakeholders. Findings are briefly discussed below:

First, a successful regulatory strategy should protect users' privacy and other rights under oligopoly, and prevent from firms' deceiving behaviors. Second, even though concerns of government surveillance are not yet to be main reason for opposing regulatory policy, interviewees are skeptical of government's capability to run them well, and most legislated policies are either not implemented or implemented in initial stage, not ready for further evaluation. Third, though Industrial Development Bureau, Ministry of Economic Affairs, is in charge of social media's violation of Personal Data Protection Act, their attitudes toward regulation remain passive since promoting industrial development is their priority. Fourth, even though setting specialized data protection agency as European Union did is regarded as panacea solving problems of fragmented responsibility on data protection, it may not be accustomed to our local legal and organizational practice, including how to cooperate with previous regulatory agency, and how to hand over their mission. These issues may be also crucial to forthcoming organizational design.

I suggest, first, our government adapt data protection to their daily work, rather than setting efficiency as supremacy. Second, our government should not be rigid in establishing organizational specialized data protection agency; instead they should focus on service design and delivery to accommodate most users and firms' needs. Third, even though the monopolization of digital advertising industry aggravated by regulation has not yet proved in this work, the phenomenon of monopolization has received wide attention. It's time for government to solve it instantly rather than sticking on demonstrating their causality.

Keyword: Social Media, Personal Data Protection, Digital Footprint, Regulation

目錄

第一章 緒論.....	1
第一節 研究背景與動機.....	1
第二節 問題意識與研究目的.....	3
第三節 研究範圍與重要名詞解釋.....	6
第四節 研究流程.....	8
第二章 文獻檢閱.....	11
第一節 業者運用數位足跡的可能機制.....	11
第二節 贊成政府監理社群網站利用數位足跡的理由.....	16
第三節 反對政府監理社群網站利用數位足跡的理由.....	21
第四節 以自律為主的數位足跡監理機制.....	25
第五節 以他律為主的數位足跡監理機制.....	37
第六節 問題盤點與可能改進策略.....	53
第三章 研究設計.....	57
第一節 研究架構.....	57
第二節 研究方法.....	60
第四章 研究分析.....	75
第一節 外界對於業者運用數位足跡的行為評價.....	77
第二節 外界對於業者自律措施的評價.....	82
第三節 外界對於業者法遵措施的評價.....	87
第四節 政府監理策略的實施與相關議題.....	93
第五節 綜合討論.....	104
第五章 結論與建議.....	115
第一節 研究發現.....	115
第二節 實務建議.....	116
第三節 研究限制與後續可能精進方向.....	121
參考文獻.....	123
附錄 個別受訪者訪談大綱.....	139

表目錄

表 2-1：Facebook 資料政策分析結果簡表.....	12
表 2-2：Digital Advertising Alliance 發佈之自律原則及補充規定.....	33
表 2-3：各監理模式之間的比較（摘要）.....	49
表 3-1：評價現行監理策略的關鍵問題清單.....	62
表 3-2：訪談大綱題庫列表.....	63
表 3-3：受訪者名單列表與順序.....	65
表 3-4：對於公民團體（代碼 A1、A2）的訪綱題目列表.....	66
表 3-5：對於公民團體（代碼 A3）的訪綱題目列表.....	67
表 3-6：對於業者委任律師（代碼 B1、B2）的訪綱題目列表.....	68
表 3-7：對於國內相似同業（代碼 B3）的訪綱題目列表.....	69
表 3-8：對於主管機關（代碼 C1）的訪綱題目列表.....	70
表 3-9：對於科技法學者（代碼 D1）的訪綱題目列表.....	71
表 3-10：對於傳播學者（代碼 D2）的訪綱題目列表.....	72
表 3-11：對於個資洩密事件受害者（代碼 E1）的訪綱題目列表.....	73
表 4-1：外界主要關心業者運用數位足跡的手法.....	78
表 4-2：外界關注業者運用數位足跡的主要的影響.....	79
表 4-3：外界對於業者運用使用者數位足跡行為的主要期許與訴求...81	

圖目錄

圖 1-1：數位足跡與個人資料關係圖.....	8
圖 1-2：研究流程圖.....	9
圖 3-1：監理策略的整體樣貌.....	57
圖 3-2：監理策略法令規範的理想組成要素.....	58
圖 3-3：理想的執行面各行為者組成與策略.....	59
圖 4-1：資料分析流程簡圖.....	76
圖 4-2：現行監理策略的實際樣貌.....	111
圖 4-3：監理策略法令規範的實際組成要素.....	112
圖 4-4：實際的執行面各行為者組成與策略.....	113





第一章 緒論

社群網站提供了嶄新的人際交流管道，使世界更開放，聯絡也更緊密。使用者享受社群媒體帶來的便利的同時，卻也承受資料被蒐集與濫用的風險。由於資料被譽為驅動經濟的新原油，商業網站積極蒐集使用者的數位足跡以輔助決策，也可能轉賣第三方獲利甚至操弄使用者行為。由於利用數位足跡過程可能造成隱私權的侵犯，若被用於不法，造成的傷害也難以彌補。隨著追蹤科技的急速發展，以及隱私侵害事件的接連爆發，要求限制業者利用數位足跡的呼聲也水漲船高，提出適當監理方案，約束業者蒐集與使用資料的行為成為當務之急。

長期以來，政府監理業者利用個人資料的工具以立法為主，現存文獻也多專注於立法技術的研討，對於後端的執行與評估，以及其他可能的政策工具則甚少著墨。且立法費時長、政治阻力大，缺乏彈性等缺點，導致無法單獨成為完善的方案，外界對於現行個人資料保護法令的施行成效也不無質疑，通盤檢討現有監理政策顯得益加迫切。

第一節 研究背景與動機

資通科技（information and communication technology, ICT）的發展，為民眾帶來空前的便利，卻也可能為業者的濫用大開方便之門。早在網際網路問世前，業者便廣泛收集消費者個人資料，作為改善服務的參考。資通科技的蓬勃發展，則使質與量皆有急遽提升的趨勢，業者不再只是被動地推論與預測使用者的偏好，而能配合行為科學技術，意圖將使用者塑造成其想要的樣子，頗類似知名電影《駭客任務》中人類被科技寡頭支配認知與行為的情節。Shoshana Zuboff（肖莎娜·祖博夫，2020）稱之為監控資本主義（Surveillance Capitalism），作為一種資本主義病態的變異，資本家將掠奪自然資源的野心擴及對社會秩序的支配，業者賺得暴利滿載而歸，使用者則失去人性與自由。

其中最廣為人知的技術，便是針對性廣告（targeted-advertisement），根據對當事人的了解，投放客製化的廣告以提高媒合率與利潤。美國零售商塔吉特百貨（Target）曾成功以消費紀錄研判少女未婚懷孕，以嬰兒用品折價券疲勞轟炸，使懷孕事跡提早敗露（杜希格，2012：216-218; Duhigg, 2013: 436-438）。2018年3月，劍橋分析公司（Cambridge Analytica）涉嫌竊取數千萬名 Facebook 使用者的資料，用於操弄多次選舉。由於過去開發者只要付費，便能在 Facebook 網站上

開發應用程式，以從中獲取使用者的資料，這也被視為 Facebook 利用使用者個資賺錢的方式之一（布特妮·凱瑟，2020：173）。儘管未有足夠證據斷定，這事件純屬資安漏洞還是出於默許，Facebook 對於劍橋分析事件的爆發，恐怕必須負起相當責任。這也讓民眾驚覺，針對性廣告的應用已從商業擴及政治作戰，也一度引發對 Facebook 的抵制潮。同年 7 月，知名通訊軟體 LINE 一度更新隱私權政策，要求使用者同意 LINE 新版隱私權政策，授權業者較大的資料蒐集與使用權限方可繼續使用軟體（彭慧明，2018；林河名，2018）；儘管使用者點選同意後，能進入軟體設定頁再次勾選關閉（林庭安，2018），仍形同給予 LINE 在撤回同意前的空窗期搜刮數位足跡（新版的 LINE 則已經取消該規定）。由於資訊營運商緊握通訊需求的咽喉，縱使使用者不滿業者的予取予求，卻通常只能概括承受。

例如主流社群網站 Facebook 坐擁近 20 億使用者，個別使用者又能再細分為至少五萬個資料點，並透過資料聚合（data aggregation）技術串接其他資料庫，以及追蹤瀏覽（tracking）近乎全面與即時地剖繪（profiling）使用者，潛在利潤與影響力非常可觀（Christl, 2017a）。數位足跡也可能在使用者上網或使用手機 APP 時，被各業者和廣告商植入的追蹤器傳送至相關網域（Brandtzaeg, Pultier, & Moen, 2019; Falahrastegar, Haddadi, Uhlig, & Mortier, 2016; Seneviratne, Kolamunna, & Seneviratne, 2015）。又如許多網站使用 Google Analytics 進行流量分析，使用者的瀏覽行為便可能被置於 Google 的監控範圍內。除非採取反監測手段，例如安裝臭鼬（Privacy Badger）、Facebook Container 等程式，只要連上網路便可能被置於全面監控的陰影下。

由於股東權益優先的公司治理現實，使用者對於被蒐集資料的內容、流向與用途通常無從瞭解，也幾乎無權置喙。即使能記憶業者蒐集了哪些自主填寫的註冊資訊、發文動態及上傳的影像，對於自動化監測以及第三方追蹤瀏覽則幾乎防不勝防。即使透過複雜的申訴程序，要求廠商刪除或修正蒐集而得的資訊，業者事後若想暗地重建，恐怕技術上也不困難。業者使用數位足跡的用途不夠透明，也就難以保證多數使用者不會蒙受隱私外洩或濫用，使用者經常也是事後才驚覺受害。且現實上由於獨占與賣方市場的優勢，業者缺乏誘因提出對於使用者較為友善的隱私權政策，隱含使用者與服務提供者的關係，兼具資訊與權力不對稱的性質。除非一開始就拒絕使用有安全疑慮的服務，通常也只能屈服。

由於網際網路的不可或缺，傳統的資訊禁慾手段顯然不切實際。即使完全棄用網際網路，仍可能被物聯網等機制側錄與傳播。若上網時還要擔心言行被側錄且不知將流竄何處，且可能多年後被放大檢視，也將造成寒蟬效應與自我審查（麥爾荀伯格，2015：13-15）。保障隱私權的意義，不僅事關人性尊嚴與社會衡平，還有自由權甚至民主價值的維繫。近來網路服務的市場佔有率、利潤分配均急遽集中化，對於網路安全、公共利益等層面也影響甚鉅。資料保護政策及施行成效的良窳，不再只是企業社會責任，而應以更加嚴格的基準檢視。皮尤研究中心（Pew Research Center）的調查也顯示，美國民眾對於各業者利用個人資料的方式不甚信賴（Auxier, Rainie, Anderson, Perrin, & Kumar, 2019）。即使 Facebook 執行長已宣示不再讓第三方應用程式存取使用者個人資料，然而劍橋分析事件的爆發，之後又被發現繼續授予多家公司存取的權限（周峻佑，2018）、以及傳出付費換取使用者同意安裝追蹤器的醜聞（Constine, 2019），也令人懷疑其對於改善隱私權的保護的承諾，只是宣示大於實質。對於社群網站蒐集數位足跡，以及其衍生的外洩等相關弊害，提出合宜的監理策略成為當務之急。

第二節 問題意識與研究目的

監理社群網站利用數位足跡與落實資料保護，已成為公共政策的重要問題。然而現有研究與實務，對於政策工具的規劃與佈署，多侷限於問題認定，對於後端的執行與成效評估則較少著墨。現有文獻多為法學或工程領域學者所撰寫，法學文獻重點多聚焦於立法正當性來源，從「為什麼管」及「該管什麼」的角度切入，由於監理政策的制定涉及民意對於隱私權的主觀期待、及接受政府介入的程度，探討規範層面的正當性來源固然必要，但是對於「該怎麼管」的細節幫助有限，多讓行政機關自己想辦法處理。工程領域的文獻則幫助我們釐清問題的現狀，特別是追蹤瀏覽的氾濫程度，追蹤網路的業者組成，可能的傳輸機制等。但是對於監理策略如何在技術面落實，及如何從政策角度評價現有監理政策的良窳，以及從台灣的國際現況妥善運用政策工具，監理 Facebook、Google 等大型科技業者，則存在許多未知地帶。工程師若未對公務機關實況有足夠了解，對於資訊技術該如何順利落實於監理程序，也未必摸得著頭緒。這些也讓後端執行的重要性被嚴重忽略。從現象而言，立法雖然成為資料保護最廣為利用的手段，如何在實務徹底落實也存在諸多疑點。例如民眾對於業者的侵權行為，通常是透過訴訟處理，雖然現行我國個人資料保護法（下稱我國個資法）第 29 條，有難以舉證

實際損失時，業者對於每人每事件賠償新台幣 500 元至 2 萬元之規定，但是對於彌補民眾損失與訴訟成本，及嚇阻業者踰矩行為的效果，顯然都非常有限。又如該法第 22 條雖賦予政府行政檢查權，但是合格標準不明確及跨境執法、取得稽核所需資料的困難，造成該權限經常有名無實（林冠佑，2012：30）。從公共行政的視角，重新審視規劃與執行之間的落差並加以矯治，顯得益加迫切。

再者，師法境外經驗，固然可能是建置與改善監理策略的途徑。歐盟一般資料保護規範（General Data Protection Regulation，下稱 GDPR），因為制度相對完善，加上歐盟龐大的政經影響力，成為目前主要被仿效的對象。筆者檢閱文獻也大致認為，我國個資法與 GDPR 相比存在甚多瑕疵，而建議與之看齊，然而複製歐盟的經驗也必須慎防水土不服的弊端；加上經歷威權統治的陰影，台灣民眾是否願意賦予政府與 GDPR 相若的職權，顯然不無疑問，若有比政府更適合擔綱監理的角色，也應納入考慮。且一如歐盟在制定 GDPR 過程中，必須考慮全球主要的網路服務供應商均為美國公司的現實，以免嚴重影響經濟秩序，台灣在制定監理政策時也必須更為細緻。

最後，管制政策文獻已明確警告，意圖干預市場機制的運作，將可能阻礙競爭甚至造成俘虜現象，進而適得其反。許多報導已指出 GDPR 提高法遵門檻與成本，造成大量中小企業消失，由大型科技公司填補真空，進而提高其議價能力（Stapp, 2019; Layton, 2019）。GDPR 固然能迫使業者提升對資訊系統的安全性投資，以降低資料外洩的可能風險（Yuan & Li, 2019），卻也可能同時提高業者使用數位足跡的能力，令使用者反而更缺乏保障。且社群網站已逐漸轉型成為高牆花園式（walled garden）的經營手法，以避免資訊落入他人之手。科技巨擘提高安全性的同時，也降低了資料被其他人運用的機會，進而壟斷資料來源與提高議價能力，業者與使用者之間的權力不對等關係也更形擴大。審慎面對並檢討管制政策的未預期後果，也勢將成為探討監理策略的另一道重要環節。

本研究共分為三個階段。第一階段透過文獻檢閱，盤點國內外現有主要監理政策的實施概況，以及各領域對於監理政策的目標與期許。第二階段則就現有可得資料衡量，衡量現行監理政策的施行成效，以及可能的差距或未預期後果，最後據此提出改進之道。並自此建構研究問題如下，並鋪陳往後的研究目的：

1. 社群網站針對數位足跡有哪些自律行為？成功的政府監理策略，應該達到哪些目標？現行政府監理社群網站使用數位足跡的策略有哪些？
2. 政府對於社群網站數位足跡監理策略已經獲致哪些成效？目前的成效與上述目標存在哪些差距？造成哪些未預期的後果？
3. 造成上述差距的原因有哪些？現行對於社群網站的監理策略，應該做出哪些改進或調整？

一、 探討與評價立法與執行之間的可能落差

政策制定者遇到的最大困難，不只是訂出法律所認為的理想狀態，還有完成執行的龐大工程。現有文獻對於多聚焦於前端的立法技術，卻可能忽略與執行之間可能失落的環節。盤點與檢討兩者之間的可能落差也同等重要。

理想與現狀的落差可謂隨處可見。如商業網站冗長且複雜的隱私權條款長期為人詬病，不僅造成閱讀的龐大時間成本，也徒增舞弊的可能空間。對此 GDPR 於第 12 至第 14 條，要求業者以簡單易懂的格式，對使用者說明各重要事項（張陳弘、莊植寧，2019：177-178）。然而條款冗長的問題迄今依然存在，筆者以社群網站業界中最具代表性的 Facebook 為例，閱讀後除了感覺冗長之外，閱讀數次後仍難系統地了解條款的內容。一部條款是否複雜，固然存在許多主觀的詮釋空間，但是懷疑這是否為我們所滿意的現狀。雖然迄今 Facebook 並未傳出被勒令中止在歐洲業務的消息，歐盟當局短期內也應不至於要厲行 GDPR 的所有內容，但是 GDPR 實施已滿兩年，立法與執行的落差也正逐漸被放大檢視，而有必要探討與評價。

二、 探討除立法外可能的政策工具

立法是常用且符合直覺的政策工具，也是政策合法化的必要環節。但是其費時長、政治不確定性高，應用上缺乏彈性等缺點，難以成為單獨的解決方案。且法律雖然能對於業者使用科技工具的方式設下相當限制，然而仍需留意科技本身只是工具和障眼法，「會依照主導的社會與經濟邏輯而有所改變」，單靠傳統的反托拉斯手段，也可能只會讓更多類似 Google、Facebook 等採行監控資本主義的企業出頭，使我們在與科技的賽跑中疲於奔命（肖莎娜·祖博夫，2020：47、58-

59)。探討除立法外可能的政策工具。重新釐清問題的本質，及探索非傳統解決方案的可能性也亦形迫切。

再者，在現行體制下，訴訟事實上已成為法律執行的主要途徑。但在我國受到以和為貴的文化影響下，訴訟通常被視為最後通牒而不被鼓勵。且訴訟程序的高成本與複雜程序，加上台灣缺乏代理訴訟團體，及金額近乎無限的懲罰性賠償實務，也降低被害人尋求救濟的誘因，徒法不足以自行的問題勢將更加明顯。直接從源頭減少數位足跡的濫用，可能是較為理想的作法。

第三節 研究範圍與重要名詞解釋

一、 研究範圍：

目前對於社群網站問題的討論，大致可分成兩大類。第一類是個別使用者的行為所衍生，如閱覽權限設定不周造成的隱私曝光或被轉載（極端案例如狗仔隊）、假消息或仇恨言論的傳佈等。本研究則聚焦在第二類，服務提供者利用數位足跡的行為及可能造成的弊害，如大量佈署偵測工具蒐集數位足跡，及將使用者資料與廣告商共享，用以投放針對式廣告，或藉由演算法操弄使用者優先看到的貼文內容等。

二、 社群網站：

社群網站常又被稱為社群媒體（social media）、社群網站服務（social network（ing） service, SNS）等；學理上泛指技術基於 Web 2.0，介面允許使用者自主產製內容（user-generated content, UGC）（如貼文與影像）、建立個人識別系統（自我介紹頁面），及自發連結人際關係與彙流資訊的平台式網站（Boyd & Ellison, 2007; Obar & Wildman, 2015）。國人常用的通訊軟體 LINE 雖不以網頁形式運作，但是允許建立聊天室與個人產製內容，也可能是廣義的社群網站。由於 Facebook 在台灣與全球均擁有較高的市佔率與使用者人數，營運模式、相關事件也較具有代表性，而作為本研究的主要對象，並聚焦於其在台灣營運的情形。由於社群網站在資料蒐集的手法、強度均有一定代表性，研究結果也可能類推於監理一般網站的資料利用行為。

三、數位足跡

俗話說「凡走過必留下痕跡」。數位足跡顧名思義，為使用者從事網路活動時產生，可供追蹤的檔案或歷程紀錄，包括但不限於 IP 位置、登入與登出紀錄、發佈言論、購買紀錄與存取的檔案等，以及相關詮釋資料（郭戎晉，2012：26-27；Christensson, 2014）。筆者參考文獻後發現，數位足跡與法律上個人資料之間的關係，迄今仍不甚明確。例如我國個資法第 2 條對於間接識別的實務判準為何似乎未臻明確，只能含糊地以能否結合其他資料，進而識別特定個人作為指標（郭戎晉，2012：27-31）。截稿前歐盟最新的電子隱私條例（e-Privacy Regulation）草案（Council of the EU, Presidency, 2021; European Parliament, 2021）¹，其前言（Recitals）第 14 點也主張對電子通訊資料採取較為寬鬆的解釋，包含通訊內容及其（技術上的）詮釋資料，且該文第 2 點對於詮釋資料也採取近乎無法窮盡之列舉方式。考慮 GDPR 對於個資的認定方式採取相對我國個資法嚴格的「任何人標準說」（張陳弘、莊植寧，2019：31），我國為與 GDPR 接軌並取得跨境傳輸之適足性認證，個資法的認定基準料將只會更嚴格。且受到新興科技的影響，法律界對於個資的認定方式，也從傳統「是否為」的二分法，逐漸轉變為個別衡量其被識別的可能性與程度（張陳弘、莊植寧，2019：40）。由於資料聚合技術的應用已成為社群網站運作的常態，且透過人臉辨識等功能與內嵌詮釋資料，即使是傳統的類比影像，仍可能被用於識別特定個人，進而符合個人資料的定義。

故本文採取較為寬鬆的基準，將所有數位足跡，即使用者在瀏覽社群網站時，及在站外被其追蹤瀏覽機制利用的所有檔案與歷程紀錄均視同法律上的個資處理。數位足跡與個資的關係如圖 1-1 所示。舉例而言，使用者在 Facebook 留下的照片、文字、瀏覽紀錄等，被視為個資應無疑義。但是也有非數位形式存在的個資，例如紙本病歷、基因等。由此認定個資涵蓋範圍大於數位足跡看似違反直覺，卻可能更符合現況。

1 本文使用的版本為 2021 年 2 月 10 日發佈，指定用於與歐洲議會談判的稿件（mandate for negotiations with the European Parliament）。預計將用以取代既有的隱私及電子通訊指令（Directive 2009/136/EC）。

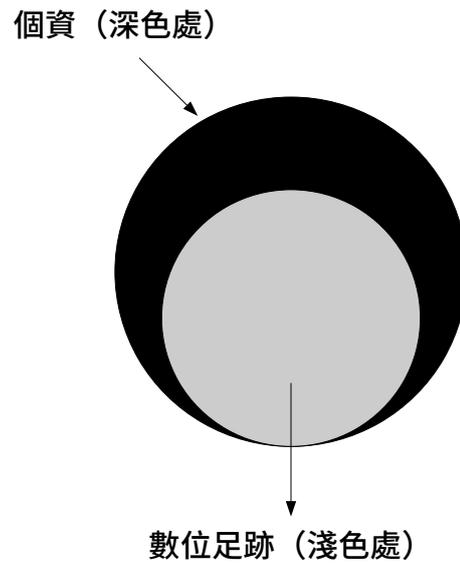


圖 1-1：數位足跡與個人資料關係圖

資料來源：本研究繪製。

第四節 研究流程

本研究旨在探討政府監理社群網站運用數位足跡的策略，以及釐清可能遭遇的困難或待改進之處，具體操作流程如下（及圖 1-2）：首先於本章緒論說明研究動機與目的，並建立問題意識，並為文獻檢閱指引方向。第二章分別從多個角度爬梳文獻，首先從事實層面了解業者利用數位足跡的可能機制，再分別從規範層面探討，外界贊成及反對政府監理社群網站利用數位足跡的相關理據。接著又繞回事實層面，分別從業者自律、法遵行為切入，探討既有監理機制的施行概況與可能發現的問題，並進行問題盤點。隨後於第三章依據前揭結果進行研究設計，特別是訪談對象的遴選以及題綱的製備。並於第四章撰寫研究分析並闡述結果。最後於第五章提出結論與建議。

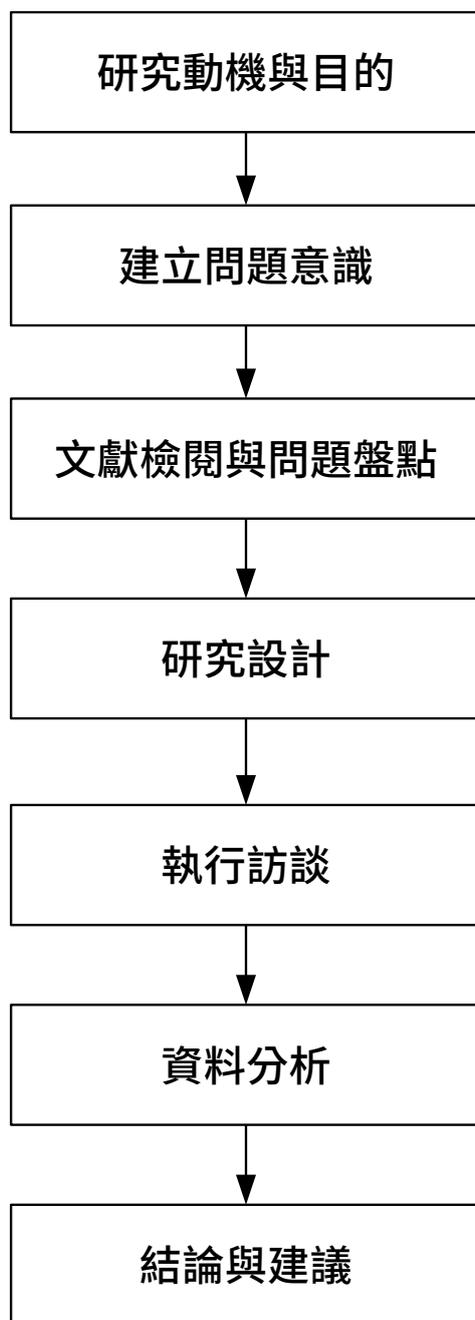


圖 1-2：研究流程圖

資料來源：本研究繪製。



第二章 文獻檢閱

探討政府監理社群網站使用數位足跡的可能角色或策略，顯然需先對於問題的整體背景做系統性的釐清，目的除釐清事實本身，也須留心於外界的評價，以及釐清現有監理策略未能解決的問題。本章依序就業者的運作機制、各界贊成或反對監理的理由，與現有的監理方案及其比較進行文獻檢閱，最後進行綜合討論，並研擬下一步可能改進的方向。

第一節 業者運用數位足跡的可能機制

探討可能策略的第一步，顯然需要對於社群網站運用數位足跡的可能機制有基本認識。最直接的方式，便是查閱業者頒布的資料政策（data policy）或隱私權政策（privacy policy）。這方法看似簡單，實作後卻發現困難重重。第一個困難便是條款的冗長與複雜。以社群網站龍頭 Facebook 為例，其資料政策（官方的中文版本）²，經文書處理軟體 LibreOffice Writer 計算，文長約 7900 個中文字，且常見非技術使用者難以理解的專有名詞，恐怕非其所能輕易負擔。另一個國人常用的社群網站 Twitter，則甚至沒有提供中文版本。使得這類文件缺乏實質的通知意義，而經常流於取得使用者形式上同意的工具。

第二，資料政策看似清楚敘明資料的蒐集與利用範圍，但因為收集資料類別與用途的繁雜，且散落於條款各處，筆者閱讀數次後，仍難清楚確認條款的授權範圍，及使用者所能介入或控制的程度等，而需要外界詮釋型文件的輔助³、民間或政府的研究報告，與學術單位的調查成果等。儘管筆者已盡所能之仔細與注意，卻難免有錯漏之處。對此我們也不妨思考，當使用者對於社群網站的作為有疑慮時，由哪一方負起舉證責任（burden of proof），所造成的整體社會成本最低？是社群網站自證清白比較容易，還是使用者證明社群網站的缺失比較困難？更有甚者，若定型化契約成為幫助廠商能以鄰為壑，轉移舉證責任與損害至弱勢使用者的工具（伯納賽克、蒙根，2015：168；布特妮·凱瑟，2020：166）。在制度設計上便應該讓社群網站負起自證清白的義務，才不至於造成社會更多的無謂損失。

2 筆者行文當下引用的資料政策為 2018 年 4 月 19 日的版本，截稿前的最新版則為 2021 年 1 月 11 日。然而筆者使用 LibreOffice Writer 的比對文件功能之後發現，除部份文字修訂之外，內容大致不變。本文仍沿用較舊的版本。

3 如隱私權倡議團體所創設的 Terms of Service; Didn't Read 網站（<https://tosdr.org/>）。

為精簡用詞起見，以下對資料政策的探討將業者所蒐集的數位足跡大致區分為（1）使用者自願提供的資料（volunteered/provided Data），例如使用者填具的註冊資料、主動上傳的文字、影像等；（2）企業主動蒐集（observed data），例如利用第三方 cookie 追蹤使用者的瀏覽行為；（3）經程式產生的推論資料（inferred data）等三大類（Christl & Spiekermann, 2016: 84; European Data Protection Board, 2020: 12-13）（以下通稱為類型一、類型二...等）。不過實作上前兩種資料的性質並非完全互斥，而常需酌情處理。例如使用者主動上傳的照片本身，視為其自願提供的資料（類型一）應無疑義。然而 Facebook（2018）在其資料政策言明，將收集相片的詮釋資料（metadata）「例如相片的拍攝地點或檔案的建立日期...」，雖然同樣為使用者自主上傳，但由於非技術使用者可能未預期 Facebook 也收集這些詮釋資料，因此筆者視之為類型二資料。

由於類型一資料的性質相對簡單⁴，使用者填表、或上傳圖片的過程也應相當程度意識可能的風險，本文將著重在 Facebook 對類型二資料的蒐集（表 2-1）。

表 2-1：Facebook 資料政策分析結果簡表

第一部份	收集特定裝置資料，特別是唯一識別碼	是
	收集個人位置資訊	是
	追蹤瀏覽第三方網站	是
	自第三方網站收集個人資料	是
第二部份	使用者發佈的內容可能被傳送至第三方	是
	使用者的個資可能被傳送至第三方	是
第三部份	資料有保存期限/自動刪除機制	否
	使用者可要求修改/刪除資料	否

資料來源：本研究整理。

該表格分為三個部份，第一部分是資料蒐集的範圍與強度，特別是若干較敏感的資料如地理資訊、裝置唯一識別碼（類似電腦的網路卡號碼）；以及除站內的追蹤行為外，業者是否追蹤使用者在其他網站的瀏覽行為，也就是常見的追蹤瀏覽，及從第三方如資料仲介（data broker）取得其他使用者資訊的可能性。這些指標主要測量業者進行資料聚合及使用者輪廓剖繪的能力與強度。

4 例如使用者在 Facebook 註冊帳號時，Facebook 只要求填具姓名、電子郵件地址、出生年月日等資訊。

第二部份則是 Facebook 是否可能將取得的數位足跡，不論是類型一或類型二，移交給該組織外的第三方使用；該指標主要測量服務提供者同時扮演資料仲介的能力或強度。而第三部份，則涉及蒐集所得資料是否可能被永久保存，以及使用者對於這些被蒐集的資料，擁有多大的控制權。這也可能同時牽涉 GDPR 的「被遺忘權」（right to be forgotten）。

一、資料蒐集的範圍與強度

第一部分的判讀結果顯示，Facebook 收集了使用者數個較為敏感的識別詮釋資料，特別是裝置的唯一識別碼、瀏覽器類型、作業系統等資訊；儘管為文隱晦，但是使用者不論是否登入 Facebook，均可能會被收集這些資訊。只要交叉比對裝置識別碼與登入紀錄，業者就能判斷個別裝置可能屬於哪一位使用者，並進一步剖析可能的行為模式：

廣告主、應用程式開發商和發佈商可以透過他們所使用的 Facebook 商業工具向我們傳送資訊，這些工具包括我們的社交外掛程式（例如「讚」按鈕）、Facebook 登入...這些合作夥伴會提供您在 Facebook 以外網路空間的活動相關資訊，包括您的裝置資訊、您瀏覽過的網站...，無論您是否擁有或登入 Facebook 帳號皆然。（Facebook，2018）

只要網站植入了 Facebook 相關的應用程式，在未登入 Facebook 的情況下，Facebook 仍可能透過第三方機制追蹤使用者的網路活動。筆者以臭鼬監測後發現，Facebook 在一些沒有明顯設置其社交外掛程式的網站上也設有追蹤器，只是程度較 Google 輕微，也懷疑實情遠不只如此。然而官方沒有言明的，還有與第三方業者的具體互動為何，迄今仍存在許多謎團，外界的詮釋也可能存在多種版本。Christl（2017a）顯示 Facebook 有從安客誠（Acxiom）與甲骨文公司（Oracle）的大型資料庫輸入資料，且從字面看來偏向單方面的輸入行為；美國參議院的報告則指出，資料仲介也可能反過來從社群網站獲取資訊（US Senate Committee on Commerce, Science, and Transportation, 2013: 21）。雖然究竟實情為何短期內顯然難以全盤了解，但是幾乎可以確定有與資料仲介往來的事實。Facebook 這樣做的動機，應該是希望讓網站成為資訊的高牆花園（walled garden），廣告主必須透過網站內部的中介機制才能在其擁有的服務推播廣告與媒合交易：

我們提供廣告主觀看其廣告的用戶類型及廣告執行成果報告，...例如，我們為廣告主提供一般人口統計和興趣等資訊（例如一位年約 25 至

34 歲、住在馬德里、喜歡軟體工程的女性看過廣告），以協助他們更瞭解廣告受眾。（Facebook，2018）

而與資料仲介的交易，無非是為了提升預測的精確度，以爭取更多的議價籌碼（伯納賽克、蒙根，2015：216）。鑑於這些資料豐厚的經濟價值，業者當然也有充足的誘因，設立關卡避免資訊落入他人之手。對於現今資料保護的相關立法技術可能造成的衝擊，也有待進一步釐清。

二、使用者資料可能的流向

社群網站既然可能會從第三方網站蒐集數位足跡，當然也可能會讓資料外流他處。Facebook 在其資料政策指稱的第三方為（1）使用我們分析服務的合作夥伴、（2）廣告主、（3）成效衡量合作夥伴、（4）合作夥伴在我們的產品中提供商品和服務、（5）供應商和服務提供者、（6）研究人員及學者、（7）執法機關或法律要求。具體為哪些團體則似乎沒有明確說明，隱含 Facebook 對此擁有非常大的自我裁量權，推定在非法律必須的情況下，資料仍可能被傳送至使用者不確定的第三方。從部份歷史資料，也可看到更複雜的內幕。2010 年至 2015 年 5 月之間，開發者只要付費，便能在 Facebook 網站上開發自己的應用程式，以從中獲取使用者的個人資料，甚至其好友資料，也就是後來惡名昭彰的「好友 API」，大致上劍橋分析也是透過該機制，以心理測驗程式取得大量數位足跡，以用於操弄輿情（布特妮·凱瑟，2020：173）。這也可能是 Facebook 具體（但間接）從使用者個資賺錢的方式。雖然 Facebook 聲稱 2015 年 5 月起已經關閉了前述接口，最新的資料政策也強調「不會也絕不可能向任何人出售您的任何資訊。我們也會嚴格限制合作夥伴使用和揭露我們所提供的資料。」。然而實務上若細看 Facebook 的資料政策，則可合理懷疑該機制仍以某種隱晦的形式繼續存在（粗體為筆者所加）：

若您使用的第三方應用程式、網站或其他服務使用了我們的產品，或與我們的產品整合，則他們也能收到您的貼文或分享內容等資訊。例如，當您與 Facebook 朋友一起玩遊戲，或在其他網站上使用 Facebook 的「留言」或「分享」按鈕時，遊戲開發商或網站可以取得您在遊戲中的活動資料，或是收到您從網站分享到 Facebook 的留言或連結資訊。此外，當您下載或使用此類第三方服務時，他們可以存取您在 Facebook 上的公開個人檔案，以及您與他們分享的所有資訊。**如果您選擇與所使用的應用程式和網站分享 Facebook 朋友名單，他們就會收到此等資訊，但無法從您這裡收到有關您 Facebook 朋友的其他任何資訊，或有關您 Instagram 粉絲的任何資訊**（當然，您的朋友

和粉絲有可能自行選擇分享這些資訊)。這些第三方服務所蒐集的資訊，均受其**各自的**條款及政策規範，而非本使用條款與政策。(Facebook, 2018)

表面上 Facebook 封鎖了第三方服務者間接取得使用者好友的相關資訊，但是如果使用者未採用較為寬鬆的隱私權政策，或者第三方服務者取得了較為寬鬆的權限，第三方服務者仍有可能取得前述的隱私訊息。開發者也可能算準了「絕大多數使用者都不願意去讀服務條款，然後就勾選了同意...他們(原文指使用者)這麼做的同時還洩漏朋友的個人資料，而這些朋友本人並沒有同意」(布特妮·凱瑟, 2020: 166)。因此，筆者認為這未能從根本消弭資料外洩的風險，而只是讓 Facebook 和開發者踢皮球，將維護隱私權責任被移轉到使用者而已；不但增加管控的難度，以現行使用者的習慣與模式，資料外洩的風險恐將持續存在。劍橋分析事件的爆發，及事後被揭露仍有第三方開發者繼續存取資料的狀態下(周峻佑, 2018; Lindsey, 2019)，Facebook 恐怕也難取信民眾能履行諾言。儘管第三方網站如何取得社群網站的資料，已經超出本研究所探討的範圍，然而廠商獲得資料後，若未能將外洩的風險控制在合理範圍，我們便需要思考從源頭監理資料蒐集的可能性。

三、使用者對於資料的可控制性

最後，這些資料被收集之後，將如何被儲存也是觀察的重點。呈現於第三部分的判讀結果顯示，使用者對於被蒐集的資料，控制權可謂非常低落。在 Facebook 的資料政策中，雖然有「我們提供您存取、修正、傳輸和清除您資料的功能。請前往 Facebook 設定和 Instagram 設定瞭解更多資訊。」的指示，然而筆者進入設定頁面後發現，能申請更正、刪除的幾乎都是類型一資料，雖然筆者能從活動紀錄(activity log)刪除自己的貼文，但是只能手動逐項刪除，後來則可批次刪除，但是想刪除歷年數以百計的動作紀錄仍然難度頗高；類型二資料幾乎看不到相關頁面，也就無法知道 Facebook 在幕後蒐集了筆者哪些資訊，更別提要找到修正或刪除的功能。

四、小結

以上分析能大致發現社群網站利用數位足跡時的若干重要特徵，以及可能衍生的問題。首先是範圍的廣度與深度，儘管外界對於社群網站如何取得數位足跡的細節或具體手法，尚存在許多未知之處。然而綜合分析使用者條文與相關文

獻，以及觀察近來重大事件，即使在毫無證據的情況下，推定社群網站同時廣泛地與深入地搜刮使用者近乎所有的生活細節，應無太大疑義。第二，是雙方嚴重的資訊不對稱；筆者是使用反追蹤程式，才稍微能描繪追蹤瀏覽模糊的輪廓；一般非技術使用者對於社群網站實際搜尋了哪些資料，可說是毫不知情，社群網站對此也想必多予隱瞞，懷疑實情應遠比能發現的事實嚴重得多。資訊豐富者為追求利潤極大化，以價格歧視或類似勾結行為剝削使用者的情形也可能愈加嚴重（伯納賽克、蒙根，2015；麥爾荀伯格，2015：147）。資訊不對稱的本質也是權力不對稱，若人際的應有平等關係，隨著財務與資訊的落差逐漸流失，也無異為對民主的戕害。在缺乏隱私與遺忘的環境下，人傾向謹言慎行甚至自我審查以自保，也失去了言論自由與行動的自由（麥爾荀伯格，2015：146）。如果我們認為線上行為受到監控與言論審查不應姑息；線下的行為資料被日趨廣布的監測系統與資料仲介紀錄與轉賣，也就絲毫不應容忍。尋求合宜監理策略以矯正亂象，成為當務之急。

第二節 贊成政府監理社群網站利用數位足跡的理由

系統性地了解贊成政府監理社群網站的相關論述，既可確立權責界線，也能釐清成功的政府監理措施，應達成何種目標。本研究認為成功的監理措施，應至少達到捍衛使用者隱私、維護公共利益、保護寡占市場下的使用者權益及杜絕欺罔行為等四大目的，茲分述如下：

一、 捍衛使用者隱私

雖然我們身處民主社會，監控通訊的除政府外，另有企業建立的近乎無所不在的追蹤網路。隨著通訊科技的急速發展，方式也從傳統的監聽，進化成為大規模的第三方追蹤瀏覽、與資料仲介的買賣與資料聚合，及個人的輪廓剖繪等（Christl, 2017a）。保護使用者免於上述威脅，以免重蹈威權時代的覆轍，顯然刻不容緩。由於資料蒐集是所有侵害使用者權益行為的開端，若能從源頭限制業者收集使用者的行為，除了能較大程度避免對使用者隱私的侵害，也能直接降低資料外洩的風險。

隱私權的內涵主要內涵是人際相處「不被干擾」（the right to be alone）及私人交談免於被宣揚的權利（Warren & Brandeis, 1890: 195）。人在被監視的情況下，出於擔心言行被永久側錄，甚至日後為不知名第三方所評價的恐懼，造成寒

蟬效應甚至行為改變，景況恐怕也與極權體制下的生活趨近（劉靜怡，2006：42；麥爾荀伯格，2015：146；Christl, 2017b: 25）。業者對於數位足跡近乎無限制的收集、處理甚至轉賣，不僅貶損個人尊嚴，也可能戕害民主體制。儘管許多主要國家並未明文將隱私權寫入憲法，且憲法的隱私權主要是規範政府與人民關係，而非企業與人民之間的互動，使得隱私權在後者的法益地位履受質疑，甚至被批評信念大於實質（Determann, 2012）。但是承認其地位並逐步擴張解釋為人民積極權力的法律學說與實務仍不在少數（劉靜怡，2006；洪家殷，2019）。隱私權的存在與否顯然不應該拘泥於是否有成文法的基礎，而是該以怎樣的形式來表達或實現。

然而這問題也轉變為，誰能夠擔綱捍衛隱私的角色？由於政府在歷史上不論是濫權的惡名，或其管制的業務特質，均與人民的隱私多有抵觸。儘管在追究這類問題的時候，仍必須將一般性的管制業務，與履受罵名的犯罪偵防業務甚至特務體系適度區分（Loo, 2019: 1606-1614），政府角色的適格性仍不無疑問。但是如果我們同意業者能以自律顯然太過天真，也勢必需要有比政府更適合的人來擔綱制衡的角色。以下探討也會繼續圍繞這個問題。

二、保護寡占市場下的使用者權益

社群網站呈現使用者高度集中化的現象。財團法人資訊工業策進會（2017）的調查顯示，國人常用的社群網站或類似服務，穩居龍頭的 Facebook 與 LINE 覆蓋率大約九成；第三名起則急遽下滑，批踢踢實業坊與 Twitter 則分別未滿四成與兩成，推得台灣社群網站服務顯然已處於寡占市場的狀態，且考慮 Facebook 已併購 Instagram、WhatsApp 等潛在競爭者的情況下，國人若要滿足日常的社交或通訊需求，幾乎可說別無選擇。保護使用者權益免受業者濫用市場權力的傷害，也成為當務之急：

（一）提供使用者實質選擇與消弭權力不對等

寡占意味著業者與使用者處於高度權力不對等關係，當業者片面給予使用者較差待遇時，使用者也幾乎無法招架，可能衍生業者濫用權力，甚至實施掠奪性定價（predatory pricing）的風險（Bostoen, 2019; Graef, Clifford, & Valcke, 2018; Robertson, 2019）。這不僅挑戰前述對於公平的規範性價值，權力優勢者作惡時也可能更加有恃無恐，如透過權力轉嫁風險與傷害予弱勢的使用者。

儘管在民主體制下，政府不可能以公權力干預個人意志，要求其轉移至其他服務。卻可能促使政府延伸思考資訊應用公共化的議題。從效率的觀點，政府長期倚重特定網路服務作為傳播的窗口看似合理，然而若民眾必須仰賴特定服務的媒介才能接觸重要訊息，業者同時採取資訊高牆的營運策略，也顯然違背公共服務的開放透明精神，也與服務外包應基於公平競爭的原則存在抵觸。當上述網路服務明顯有隱私或資安疑慮時，也可能讓民眾捲入資料濫用甚至剝削的風險。雖然政府無法直接要求業者改變應用數位足跡的行為，仍可能仿照異地備援的精神，在多種不同傳播載體之間靈活操作，例如除了在 LINE 之外，同時在新型通訊軟體如 Telegram 發佈訊息，以增加民眾媒介的選擇減少該風險，或可作為一種嘗試。雖然在新型通訊載體的衝擊下，傳統網頁的訊息傳布途徑，料將面臨業績慘澹的困境，但就風險分散的考量而言仍不可偏廢。

（二）捍衛合理取價信念

業者知道使用者的資訊越多，也愈有可能從中得知或推敲其所能或願意支付的最高價格，透過個別定價策略追求最高利潤，結果可能犧牲消費者的福祉；業者也可能操縱消費者可得資訊及排序，如搜尋引擎的顯示內容與排名，以誘導點選利潤較高的廣告或產品（伯納賽克、蒙根，2015：139; Loo, 2019: 1591）。若我們對於極權國家控制媒體，只允許報導有利執政者的訊息的作法感到毛骨悚然，我們日常依賴用以通訊的社群網站，與資訊主要來源的搜尋引擎，做法恐怕也很相近，只是以往都是在檯面下進行。魏則西事件使搜尋引擎的競價排名機制及伴隨的風險開始被華人社會廣為討論。劍橋分析事件則讓民眾對於針對式廣告的疑慮延燒至政治場域。

使用者人數與資料集中於特定網路服務的趨勢，則可能衍生業者坐擁權力實施掠奪性定價的弊端。若業者挾市場優勢，片面訂立對使用者漸趨苛刻的條約，以便更大限度地利用數位足跡，甚至以增加對使用者推播廣告密度等方式攫取更多利潤，進而降低服務品質，也可能是變相哄抬價格的行為（Bostoen, 2019; Graef et al., 2018; Robertson, 2019），而與公共利益中合理取價信念嚴重抵觸，成為監理政策急欲解決的問題。

(三) 確保對使用者的透明

確保資訊透明有助於避免隱匿有害生產過程與成份，暨舞弊行為造成的危害，現行消費者保護相關法令通說也保護消費者「知的權利」。然而社群網站利用使用者數位足跡的機制，現今仍存在許多外界不清楚之處，不是包裝成各種模糊之術語散置於資料政策之字句，便是被視為營業祕密而拒絕公開。使用者若非對後台演算法之運作機制有相當概念，便無從得知與判斷，社群網站基於使用者資料客製化所為之決策機制，如對動態消息（news feed）之排序、顯示的針對性廣告等，是否構成歧視或其他弊害。此處強調的不限於常見或可直接觀察之歧視，使用者或商家尚可在搜尋引擎輸入關鍵字，得知是否被排在較後面的順位；但是當可操弄之變數一多，且演算法設定者居心不明時，便潛藏舞弊的空間，使用者經常已不自覺地受害，或得知時往往已經事態嚴重（Loo, 2019: 1596-1598）。有鑑於使用者與社群網站專業嚴重落差的現實，本文一再強調在制度設計，應儘可能偏向對使用者有利之舉證責任分配的重要性，當使用者對於社群網站的作法有疑慮時，宜由舉證較容易（或成本較低）之社群網站來自證清白，業者也始有足夠誘因自律。

三、 杜絕業者欺罔行為

商業活動需要專責監理機構，保障交易秩序及弱勢者免於受到欺罔行為的傷害。由於社群網站主要獲利來源為廣告業務，不實廣告也成為重要的問題。第一類不實廣告主要來自外部，社群網站透過中介機制所媒合的廣告。社群網站雖不主動生產數位內容，僅提供廣告服務者與使用者之間的媒合機制賺取收益，實則可能透過演算法，競價排名、甚至特定政治偏好等因素，操弄顯示特定內容的順序，進而剪裁與控制使用者的消息來源，而應以與傳統媒體相似的標準加以檢視。劍橋分析公司涉嫌搜刮 Facebook 使用者資料，投放針對式廣告操弄多次選舉便為顯例。雖然基於法定言論自由權的保護，政府對於廣告的實質內容與投放方式，所能監理的範圍相當有限，但是確保廣告業務關鍵資訊的透明，如資金來源、投放者資訊、錨定對象與議題的揭露等，則為可能的方向（Wood & Ravel, 2018: 1255-1263）。

第二類不實廣告則是社群網站本身欺騙使用者之廣告用詞，例如對免費服務的誤導。網路服務常主打免費服務以吸引使用者，然而「免費」一詞應僅限無條件或對價地提供財貨及服務，業者聲稱提供免費服務，卻於後台蒐集使用者數位

足跡並衍生營利行為，便有誤導之嫌疑（Hoofnagle & Whittington, 2014）。許多使用者可能直到劍橋分析事件爆發後，才驚覺自己的數位足跡被用於投放針對式廣告，並衍生嚴重後果。網站對於針對式廣告的說明，也僅限於強調提供個人化服務的優點，但對於後續可能的哄抬價格等剝削行為等風險，則顯然避重就輕（羅鈺珊，2018；麥爾荀伯格，2015）。2019年12月匈牙利政府也以宣稱免費服務誤導使用者裁罰 Facebook（陳曉莉，2019；Szakacs & Fincher, 2019）。如今 Facebook 的登入頁面，吸引註冊帳號的標示只有「建立新帳號。快速又簡單。（Create a new account. It's quick and easy.）」的字樣。儘管對於多數非技術使用者而言，這類廣告用詞的修正還遠不足以達到警惕的效果，且只將「點擊『註冊』即表示你同意我們的使用條款、資料政策和 Cookie 政策」的警語以較為低調的方式呈現，卻也不失為改變的重要起步。

四、捍衛公共價值

社群網站對於使用者隱私的侵害、利用市場優勢攫取暴利的行為，不僅傷害使用者福祉與尊嚴，也強烈挑戰我們認為日常待人接物應遵守的道德規範，如公平取價（fair price）、童叟無欺（honest dealing）、與顧及旁人安全（safety）等普世信念（Eisner, Worsham, & Ringquist, 2000: 6）；我們早已預期這些想法與商業的江湖規矩勢必存在落差，但是如果明知業者的行為不斷違反上述信念，卻無法提出具體方案矯正時，也形同教導大眾這些信念只是空號，可以棄若蔽屣，猶如某知名企業家曾說「民主不能當飯吃」一般。物質文明的蓬勃發展造成許多價值觀的崩解與衍生之問題，部份原因也可能根源與此。鑑於諸多認知限制可能無形地影響使用者的隱私揭露行為或設定，若完全任其自我管理，將可能引致嚴重傷害（Acquisti, Brandimarte, & Loewenstein, 2015; Cho, Roh, & Park, 2019）；且年紀較輕、教育程度較低的使用者，也較容易揭露自己的隱私（Punj, 2019: 146）。除教育使用者基本的資訊安全概念之外，我們也有義務避免弱勢族群受到上述監測技術的侵害。倘若社群網站無法嚴守道德與法律的底線，令使用者的尊嚴（dignity）與自主（autonomy）獲得最低限度的保障，以及合法與公正的裁量甚至蒙受傷害時，也是政府必須介入監理的時機。

五、 小結

經由一系列文獻探討，可將支持政府監理社群網站利用數位足跡的論點，歸納為保障屈居弱勢的使用者，能享有公平的交易條件，以及免於業者濫用市場權力所造成的侵害。而兼具追求公共利益，並維繫社會價值的穩定的使命。然而仍遺留數個待解決的問題。其中最明顯的是，應該維護個人權利到什麼程度，甚至與經濟發展之間該如何取得平衡？畢竟若對個人權利的主張無限上綱，現存主要的網路產業的商業模式恐將無以為繼，其後果恐也非我們樂見。其他產業在客戶關係管理（customer relationship management, CRM）的經驗或可作為借鏡，仍未能在實務上給予具體的尺度。即使不否認上述目標的社會意涵，也難免令人懷疑論述上是否站得住腳？捍衛公共利益的理由，也容易陷於論述大於實質的窘境。

第三節 反對政府監理社群網站利用數位足跡的理由

政府基於保護使用者權益與捍衛公共利益的立場，監理社群網站利用數位足跡，無疑有其重要性。但是問題與反對意見，恐怕也遠比預期效益與支持意見還多。其中最直接的爭議，仍然在於政府角色的定位。既然清楚社群網站不是慈善事業，政府也缺乏立場要求其收斂甚至改變其營利模式，使用者應該反求諸己，自行決定是否停用信譽有問題的服務。況且政府行為對於民眾隱私的侵害也殷鑑不遠，監理合法性也令人存疑。管制悖論也嚴厲警告，政府的監理能力不足，也可能導致與企業助紂為虐的悲慘下場，因此制定監理政策時也更應三思而後行。

一、 使用者應善盡的責任

使用者應清楚明白社群網站不是慈善事業，為享受服務勢必需要付出代價，只是該代價是否合理。民眾也不能只是被動地要求政府監理業者，卻對於自身應善盡的責任漠不關心與不願採取行動。隱私悖論（privacy paradox）尖刻批評使用者對隱私的珍視宣示大於實質，⁵若使用者未能以行動捍衛自身權益，政府也難有置喙餘地（Fuller, 2019）。鑑於政策資源有限的事實及管制悖論的相關風險，監理也不是萬靈丹。使用者與其只出一張嘴，或被動地坐以待斃，不如自動善盡公民責任，並主動學習媒體識讀的相關知識（布特妮·凱瑟，2020：368-373）。使用者應對於社群網站的運作機制有基本認識，並清楚意識到社群網站是經由續

5 隱私悖論大致的意義，是指使用者聲稱珍視隱私，實際行為卻犧牲隱私換取特定利益，諸如方便或享受的矛盾現象。對此較詳細的文獻探討，請參見江淑琳（2014：87-90），與陳憶寧、溫嘉禾（2020：35-36）。

密設計，使其願意花更多時間駐足，以便從中攫取注意力以及行為資訊並轉化為收益，使用者也應學習以聰明的方式使用社群網站、培養有意義的社交與休閒活動方式，而不至任由科技產品擺佈（卡爾·紐波特，2019）。使用者也應避免貪圖一時的方便，而依賴特定業者的服務，果決與信譽有瑕疵的業者斷絕往來，並預擬替代方案以便隨時轉移至其他業者。電子郵件雖然古老，但是格式互通且能將信件分散儲存於不同業者的伺服器，甚至可以自行架設伺服器，避免被單一廠商掌握的風險，可能是個好選項（洪朝貴，2018）。

儘管這些論述難免被批評轉移焦點、忽略業者應盡的社會責任，令人難以啟齒的根本原因其實也是知易行難。除了使用者普遍短視近利、經常是一盤散沙的難堪現實，也可能是政策倡議者缺乏毅力鑽營單一議題，經常轉移焦點或者任憑船過水無痕，最後錯失改革良機（史蒂格勒，1991：223-224）。但是唯有如此才算開始有意義地改善問題。

二、可能對於使用者隱私權的侵害

鑑於政府在歷史上的濫權經驗，使用者也難免擔心業者迫於壓力將其資訊轉交給政府單位（Fuller, 2019: 370）。雖然業者通常有權基於法律的要求與政府分享使用者資訊，態度通常也較為謹慎，畢竟要是失去使用者的信任，業者也將失去一切。然而我們也應當體認不同業務性質的政府機關，採取的手段必有細微差異：將惡名昭彰的特務機構與犯罪偵防機關⁶，與日常的產業管制混為一談，難免以偏概全；將蒐集組織營業數據，與個別使用者的數位足跡畫上等號，顯然也不甚明智（Loo, 2019: 1606-1614）。儘管這不能完全解決監理過程對隱私權侵害的疑慮，處理相關論述時宜應更加細緻。這也衍生另一個待解的問題，如果政府的確不合適，有哪些更適合的人足資擔綱監理的角色？這也可能是現有文獻尚未能有效回答的空白。

三、對於風險認知的差異

由於政府對於舊的（已知的）風險管制一般較為寬鬆，對於新的（未知的）風險則較為嚴厲（Huber, 1983）。對於社群網站問題解讀方式的差異，也可能造成截然不同的監理策略。業者在認為現有的監理機制對其有利的情況下，勢必需要透過傳播工具引導民眾相信對其有利的認知。例如不斷對外強調，雖然社群網

6 在原文可泛指如美國國家安全局、中央情報局與聯邦調查局等。

站看似深奧莫測，其本質仍與既有的商業模式相似。Facebook 雖被公認為網路平台，但是平台經濟早已存在數百年，相關管理經驗亦有跡可循（Marsden, 2018）。換言之，我們面臨的依然是舊的（已知的）風險，是否非要以全新的治理模式，甚至另立新法限制社群網站業者的行為也就有待商榷。監理者若輕視遊說者對於議題設定的能力及可能造成的影響，只顧著政策規劃而疏於建立主張社群網站是新風險的論述或尋求證據，以鞏固監理的合法性，勢將無法克服政治阻力而招致失敗。

四、對政府能力的質疑

管制政策若要成功，管制者須先具備足夠道德水準與能力，儘可能降低管制失敗的風險與後果，也必須有足夠知識「偵測與證實」違規行為，並熟稔業界的相關（潛）規則與舞弊的方式，查緝案件也必須切中要害，而不只是巨細靡遺但是敗絮其內的統計報表（史蒂格勒，1991：203-204）。然而政府的現況可說是差強人意，美國參議員在劍橋分析事件後，對 Facebook 聽證會上荒腔走板的表現，「似乎連社群網站如何營運的基本概念都沒有」（簡恒宇，2018）便是明證。Facebook 在劍橋分析事件則幾乎是全身而退，聯邦貿易委員會（Federal Trade Commission, FTC）「重罰」50 億美元也幾乎無法與該公司動輒數百億的營收相比，並被揶揄「只是做生意的必要成本，因此違法很划得來」（徐榆涵、黃秀媛，2019）。歐洲的 GDPR 執行近來也屆滿兩年，也不乏研究報告巨細靡遺地闡述統計資料，如 GDPR 推行後政府處理了多少違規案件，罰了多少錢等資訊（李億誠，2019；Barrett, 2020），卻對於 GDPR 實施兩年來，Google 是唯一遭到重罰的科技巨擘的難堪事實難以啟齒，遑論單次違規只被處以十分之一的日營業額的難堪事實，也無怪乎 GDPR 被譏為紙老虎（Satariano, 2020）。這也勢必難以杜悠悠之口，為何中小企業要承受如此沉重的監理壓力，但是許多惡名昭彰的科技巨擘卻似乎能全身而退？政策的失敗恐怕將是自我實現的預言。以下就管制悖論常見的論述，判斷政府可能會在哪些地方遭遇失敗。

五、俘虜現象與扭曲市場規則

即使經過縝密規劃，管制政策仍可能失敗並造成嚴重後果。管制失敗典型的症狀包含俘虜現象（capture）與扭曲市場機制。俘虜現象泛指管制機關的議程設定（agenda setting）與利益結構被特定團體掌控，而淪為追求私利的工

具。Bernstein (1955; 轉引自羅清俊, 2015: 301-302) 的管制委員會生命週期理論指出, 管制機關被擄獲可歸咎於系統性因素: 對內隨時間發生惰性, 逐漸忘記為誰而戰, 民眾對議題的關注衰減也使機關逐漸失去政治支持, 徒增有心人士見縫插針的機會; 隨著管制者與業者的互動加深, 雙方的專業認知與利益結構也趨於一致, 合流成為新的利益集團, 最後被業者吸收而淪為階下囚。

管制政策也可能扭曲正常的市場機制。常見的形式為貿易壁壘或價格補貼, 為弱勢的國內產業阻絕競爭, 消費者也可能因此無法享受較便宜的價格或較佳的技術。另一種形式為政策上獨厚特定產業, 如 Stigler (史蒂格勒, 1991) 在名著〈經濟管制理論〉直指: 「管制通常是行業主動要求的結果, 而且基本上是為了該行業的利益而設計和運作的」(第 145 頁)。或者執意採取社會總成本較高的方案: 「(就石油進口配額政策而言) ...即使國防確實是配額的目標, 那麼加徵關稅也可能是更經濟的效率工具」(第 146 頁), 政府為何還要使用成本較高的配額政策呢? 可能的原因是管制者無需承受失敗的後果, 既然痛的是別人也就能無所顧忌(第 204 頁)。筆者懷疑在極端的情況下, 這類政策將未能達成整體社會的最大福祉, 而讓業者的私利極大化, 管制政策也就淪為魚肉鄉民的工具。

近來 Facebook 執行長 Zuckerberg 呼籲網路需要被加強管制的論調 (Press Association, 2019; Zuckerberg, 2020) 引起熱議, 表面上是承認現行自我管制架構的瑕疵, 而願意讓渡長期緊抓的網路主導權⁷; 或者在企業營利與社會價值之間難以取捨, 「...祖克柏認為每天做這些決定太麻煩了, 所以不如讓政府來當裁判吧!」(劉仕傑, 2020)。索羅斯 (George Soros) (2020) 則質疑, Facebook 大可直接拒絕刊登政治競選廣告, 又何必等到政府出手? 筆者推測 Zuckerberg 是相當篤定政府介入管制對其有利才會出此言。一種可能是管制能阻礙競爭, 其相關原理與後果將詳下所述。

六、阻礙競爭

管制政策的直接後果便是阻礙競爭。優勢者藉由設立進入障礙, 或遊說制定只有少數人能達到的標準, 美其名是透過淘汰機制提升產業水準, 實則打壓競爭者的生存空間 (羅清俊, 2015: 304-305)。受網路效應之影響, 大者恆大、勝者全拿向來為網路產業的常態。通常大型企業才有充足的資源與技術, 以應對近乎

7 儘管原文主要是針對網路言論自由, 例如政治廣告或爭議內容等 (但也有部分觸及隱私), 對於本研究的案例應該也尚稱適用。

苛刻的法遵細節，中小企業也幾乎只能將儲存業務外包給大型雲端業者，也形同創造只適合特定業者生存的空間（Sirur, Nurse, & Webb, 2018: 92-93），自然也助長許多中小企業的消失，以及大廠獨占利益的局面（Layton, 2019; Stapp, 2019）。我們一方面可能將其單純視為社會變遷的代價，並藉此淘汰法遵意識薄弱的業者，以防堵網路生態中其餘的資安隱患。然而這也勢將加劇社群網站的獨占局面，業者的行為可能也就更難被駕馭。

這也迫使我們思考數個麻煩的問題。首先，到底是業者只要有努力便能達到GDPR的標準，還是確實只有大型機構能夠企及？此時政府單位及時提供的輔導文件，可能幫助中小企業能加速接軌（Sirur et al., 2018: 93）。此外，是否所有的資料都必須以如此嚴苛的標準處理？在資源有限的事實下，較合理的方式似乎還是依照不同資料的機敏程度，施以程度不一的保護方式。這標準又該如何設定，也可能是本研究必須思量的重點。

七、小結

本節就反對政府監理社群網站利用數位足跡的觀點，做出稍具系統性的整理與分析。理由大致可歸納成為對政府角色定位的爭議，與對政府能力的質疑兩大類型。政府在制定監理政策時，避免過於樂觀的評估也顯得益加迫切。日後在探討監理角色時，也宜著重思考在，首先從規範面的角度來看，政府的角色是否合適？又有哪些更適合的人足資擔綱上述角色？監理的力度該多大，與著重在哪些面向與方式，以期避免造成弱勢業者的衝擊，也能以兼顧效率與經濟的要求來達成最大效益？這同時牽涉到實證層面的問題，究竟現行監理成效又為何？而有待進一步釐清。

第四節 以自律為主的數位足跡監理機制

雖然社群網站利用數位足跡的方式，通常不會因為當事人國籍、族群身份的不同，而有明顯的差異，差異也主要體現於後端的決策裁量，如即時動態訊息與廣告的排序與顯示方式。然而對於政府角色定位的分歧，衍生截然不同的監理模式，而可粗略分類為以美國以自律為主，與歐盟、我國以他律為主的兩大模式，本節先探討美國的自我管制模式。

顧名思義，自我管制泛指政府不強勢干預，儘量授權被管制者主導與自主執行的模式。不過自我管制並不同政府完全放棄管制的權力，且完全放任模式在

實務上也極少存在，經常也需要有人在背後施壓業者，與政府保留部份干預的空間，業者才會以較為認真與務實的態度，研擬與執行相關措施。因此在討論自我管制措施時，也應將外部驅策的角色一併考慮在內，並視為動態平衡的關係。業者基於自身利益考量，通常也只會擬定最低程度的自律方案，迫於壓力才會悻悻然地稍微提高標準。邇來有人提出「共同管制」(co-regulation)的第三條路，主張業者與政府共同協調以遂行管制目標，以期互補傳統措施與自我管制各自的優缺點，其本質仍可能是自我管制模式的變體(羅清俊，2015：316；Hirsch, 2011；Wood & Ravel, 2018: 1244-1246)。形式依照干預的強弱，可能從幾乎完全放任或只設定原則性規範，到雙方共同研商可能的具體方案，但是業者保有最終執行的彈性皆有。

一、主張自我管制措施的理由

雖然政府干預經常被視為處理重大問題直覺且立即的手段。然而基於民主政治與市場經濟的運作原則，通常期待政府只扮演被動的角色；且迫於政府行政資源日益短絀、社會分工日趨複雜的現實，授權產業自我管理，也成為節約行政資源與保持市場機制正常運作的可能手段。也經常因為政治環境的限制，管制政策的立法與推動有明顯困難，自我管制成為唯一可行的方式。長期以來美國不乏有志之士欲推動全面性的個人資料保護立法，但經常無疾而終。且認為社群網站使用者不應享有隱私權的論述阻力也頗高(Determann, 2012)。這固然可歸因於缺乏政治可行性，特別是利益團體的阻撓，政府濫權的陰影造成民意的敵對卻也是不爭的事實。特別是九一一事件之後，各國政府為了反恐近乎無限制地利用個人資料時，也就更難有立場要求民間反其道而行(麥爾荀伯格，2015：206-207)。此時授權業者自律與其說是必然，不如說是不得不然。

但是主張自律也並非全無理據；管制措施對自由權可能的傷害自不待言，主流民意對於政府施政危害自由權的憂慮，可能遠高於業者的踰矩行為，監理措施勢也將承受更大阻力。管制悖論的探討也已提到，管制政策勢將提高成本；美其名是透過淘汰機制提升總體產業水準，卻也可能造成俘虜現象，大型企業得以雄厚政治資本與以捍衛公共利益之名，遊說政府制定只有少數人能達到的標準，以打壓潛在競爭者，阻礙競爭與加劇社會資源分配的極化(羅清俊，2015：304-305；Layton, 2019; Stapp, 2019)。即使法律真能令使用者獲得基本的保障，市場機制終究才是驅策業者採取行動改善的最大動力(麥爾荀伯格、庫基耶，2013：

226-227；Bowie & Jamal, 2006; Davis & Marotta-Wurgler, 2019; Marotta-Wurgler, 2016)。且若使用者不願以行動捍衛自身權益，監理措施也難有置喙餘地。另一方面，政府也顯然缺乏能力制定與執行合宜的監理措施；美國國會議員在劍橋分析事件的聽證會上荒腔走板的表現被戲稱為「科技文盲」，便是難堪的事實（高敬原，2018）。立法議程冗長與時間滯延的特性，監理措施能否跟上科技業快速發展的步調，也著實令人懷疑。更何況是否有足夠執行資源，諸如及時與明確的指引（guidance/guidelines）（Jackson, 2018a, 2018b）、執法人力（Jackson, 2018a; Stupp, 2020）、或被監理對象是否有足夠法遵人力與所需知識（Jackson, 2018a; Tidd, 2018）等，恐怕也不無疑問。

二、現行自我管制措施的實施概況

美國是採取自我管制措施較具代表性的國家。美國少有類似歐陸法系國家全面性的資料保護法令，主要為依特定產業或領域量身訂作的「部門式立法」，如兒童線上隱私保護法（The Children's Online Privacy Protection Act, COPPA）（翁清坤，2010, 2016, 2018）⁸或依英美法傳統鑲嵌於行政細則或歷屆裁判中。糾紛主要以發起（主要為民事）訴訟（邱祥榮，2001），或送交主管機關處理。雖然有看似較全面的隱私法案，例如隱私法（Privacy Act of 1974），然而該法效力實際僅及於聯邦政府（U.S. Department of Justice, 2015）。另一部看似與隱私權切身相關的電子通訊隱私法（Electronic Communications Privacy Act, ECPA），則因為法律管轄權的問題在 *In re DoubleClick Inc. Privacy Litigation* 案中⁹，被判決不適用於 DoubleClick 利用 cookies 投放針對式廣告的行為（Solove & Schwartz, 2018: 900-902）。

美國自我管制的主要思維是，影響業者行為的主要力量在於市場，例如成人網站業者必須比同業嚴格限制數位足跡的蒐集，以維持使用者的信賴（Davis & Marotta-Wurgler, 2019: 307; Marotta-Wurgler, 2016）。自我管制的目標，只是確保使用者事前能至少在形式上知情與同意（notice and consent）的情況下與業者締約，其餘則儘量由市場機制處理，但是業者一旦締約便必須遵守，否則聯邦貿易委員會便可以欺罔行為追訴之，該會也因此成為事實上的主管機關（翁清

8 儘管近期號稱輕量級 GDPR 的加州消費者隱私保護法案（California Consumer Privacy Act, CCPA），已於 2020 年元旦起實施，但是迄今實行時間仍短，且尚有半年的寬限期（陳曉莉，2020），執行成效仍不甚明確。故暫不在本文討論範圍之內。

9 該案全名為 *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2D 497 (S.D.N.Y. 2001)。

坤，2010：23-24, 2016：165、212, 2018：959-961）。由於對業者的不公平行為與資料搜刮行為對使用者的傷害，實務上舉證困難，也缺乏具公信力的估價機制，實務上該會的業務仍著重於取締業者在契約與實務之間的落差，造成的欺罔行為（Hoofnagle, 2018: 176）。雖然聯邦貿易委員會頒布文件多半不具強制力，業者仍會適時遵守聯邦貿易委員會的相關指引，至少以表面工夫減緩外界力主干預的壓力。兩者的互動已長期達成以下的動態平衡：

（一） 完全由業者設立標準

雖然政府通常不干預經濟活動，仍鼓勵業者自行設立標準與認證機制。不僅能兼顧效率與經濟的治理圭臬，評鑑的標準化也能幫助使用者貨比三家，並預留聯邦貿易委員會以欺罔行為干預的法理依據。TrustArc 是行之有年的網站隱私認證機制，其前身為電子開拓基金會（Electronic Frontier Foundation, EFF）支持的 TRUSTe（始於 1997 年），早期主要業務為評定網站隱私的保護程度並核發標籤（劉靜怡，2002：152），如今為順應法律與市場趨勢，TrustArc 也有為企業訂做法遵工具或解決方案的業務（TrustArc, n.d.）。業者或類似 TrustArc 的認證機制，也必須對外宣稱符合主要法規要求，才可能有拓產業務的機會。然而此聲稱意味著業者的認證機制，也必須確保能符合相應法令，否則主管機關便可以欺罔行為追訴之。這也意味在法律逐漸主導網路行為，連帶影響市場機制的趨勢下，完全由業者主導與設立標準的自律模式，可能事實上已經不存在。

（二） 行政指導

儘管聯邦貿易委員會頒布之文件或相關指引多半不具強制力。然而業者仍須適時參考上述資訊，以減緩外界力主干預的壓力。這類通常被稱為行政指導的措施看似只有輕微干預，效果仍不容小覷。典型的例子為聯邦貿易委員會於 1999 年頒布的公平資訊慣例（Fair Information Practices, FIPs），可追溯至 1973 年自動化資料系統委員會（The Committee on Automated Data Systems）出版的《個人資料系統：紀錄，電腦和公民權》（Records, Computers and the Rights of Citizens）報告及其五大原則，一般認為是西方國家個資保護法制化的先河，並影響日後多個資料保護相關規定的架構（潘兆娟，2007：32；Dixon, 2007）。公平資訊慣例之主要原則簡述如下（轉引自 Bowie & Jamal, 2006: 326）：

1. 告知/察覺原則 (Notice/Awareness Principle)：業者應清楚對使用者說明其資訊使用政策，特別是蒐集的對象與方式。
2. 選擇/同意原則 (Choice/Consent Principle)：業者必須讓使用者能選擇或控制使用資料的方式，特別是除了完成交易所需的用途之外，是否還願意挪做他用，甚至分享（或拒絕分享）給第三方或協力廠商。典型的作法為選擇退出 (opt-out) 及選擇加入 (opt-in) 的介面設計。
3. 存取/參與原則 (Access/Participation Principle)：業者必須提供使用者方便的途徑，以便隨時察核資料的正確性或完整性。
4. 安全原則 (Integrity/Security Principle)：業者必須採取措施保護使用者資料免於外來的侵犯，例如網路攻擊或未經授權的第三者（包含組織內員工）窺視甚至盜賣。
5. 強化原則 (Enforcement/Redress Principle)：對於上述原則建立一套可落實的機制 (mechanism)。

嗣後官方仍以公平資訊慣例為基礎，繼續更新與補充多個隱私指引文件，如聯邦貿易委員會分別於 2000 與 2012 年出版的隱私指引 (FTC 2000/2012 Privacy Guidelines) (Marotta-Wurgler, 2016: 11-15)。然而這些大致只能說是告知並鼓勵業者政府認為的理想狀態，業者無需唯其馬首是瞻，實際作法也可能經常背道而馳。聯邦貿易委員會實務上也只能基於消弭資訊不對稱的立場，鼓勵網路服務業者自行訂定線上隱私權政策，在滿足基本告知義務的前提下，業者能自由決定使用數位足跡的方式，並以前述追訴欺罔行為的職權作為後盾。儘管業者可隨時片面頒布較為利己的新約，業者主動制定資料政策，仍然可能對使用資料的權限造成限制。業者之所以願意配合，一方面能夠安撫使用者，並以提高透明性創造商業利基，也可能是基於更現實的考量，避免日後主管機關採取強硬措施，破壞對業者有利的現狀，而在小事上盡可能妥協。這也可能衍生業者對於主管機關屈居於被動回應姿態的關係，將詳述如後。

(三) 業者的被動回應

由於政府的監理措施常與業者的利益對立，業者出於趨吉避兇的本能行為，可預期通常不會積極配合，而以消極配合或在突發事件與主管機關商討可行的方案，換取繼續自治的空間或避免被施以更嚴厲的措施。

第一種模式是從組織層面著手，宣示成立同業的自治團體。有別於我國常見的法定強制參加的同業公會，美國傾向於志願組成與參加的組織。為了減緩聯邦貿易委員會的干預壓力，業者先後成立多個同業組織與行為準則（code of conduct），既可統一標準以降低成本，也能集體宣示改善決心，但這些努力通常以失敗收場（Hirsch, 2011: 457-464）。為回應聯邦貿易委員會於2009年初發佈的《網路行為廣告自律原則》（Self-Regulatory Principles for Online Behavioral Advertising）（下稱自律原則）及附帶的課責要求，多名業者於2010年10月成立數位廣告聯盟（Digital Advertising Alliance）及啟動AdChoices專案，允許使用者瀏覽網頁時，透過其功能閱覽網站資料政策，並選擇退出網站的針對式廣告功能，但是實務上仍飽受批評。

第二種模式則是個別業者與主管機關達成協議。近期較著名的事件為劍橋分析事件後，Facebook遭聯邦貿易委員會裁罰50億美元。值得注意的是，官方懲罰的主要原因，並非因為對使用者的傷害，而是違背2012年與官方達成的和解協議與連帶的欺騙行為（Federal Trade Commission, 2012, 2019）。事件可溯及美國與歐盟於2010年簽訂的安全港協議（Safe Harbor Privacy Principles），Facebook宣稱採取多項隱私保護措施，第三方應用程式卻能任意蒐集資料，且未清楚說明與採取有效防堵措施，而違反其遵守安全港措施的聲稱，被聯邦貿易委員會起訴，雙方於2012年達成協議，Facebook承諾不再允許第三方程式違規取得個人資訊，卻不但違約且將使用者的手機號碼私自用於廣告用途，因而於2019年再次被聯邦貿易委員會起訴，最終達成裁罰50億美元的和解協議（周宥廷，2020）。雖然一般認為聯邦貿易委員會2019年的裁罰決定，與當時熱門的劍橋分析事件有直接關係，然而仔細檢閱前述的新聞稿即可發現，劍橋分析只出現在正文中兩次，且被定調為「一個相關卻分離的事件」（In a related, but separate development）。由此推斷其實劍橋分析事件不是Facebook被處罰的主要原因，而是與該事件相關的欺罔行為，且實際上也不只這樁事故。在此階段雖然是業者與政府達成協議，主管機關其實已經掌握相當的主動權，能否歸類為自我管制恐有爭議。只是比起傳統模式下政府多採取先發制人的姿態，業者顯然也有相當的議價能力，否則聯邦貿易委員會也無需等到2019年才做出較為嚴苛的裁罰，何況50億美元與Facebook的企業規模與社會影響相比幾乎可說是不成比例。

(四) Facebook 的自律努力

Facebook 作為全球最大的社群網站，也需要自主採取行動以取信使用者。以下簡單歸納其公關頁面¹⁰所羅列對於隱私權或資料保護的自律措施，然而配合篇幅與時間侷限，本文以一年內發佈的新聞稿為主，且著重於已採取，且較具代表性的案例，純屬規範性論述的稿件則予以忽略；也只著重 Facebook 的最核心功能（如貼文、訊息、普通相片分享等），附加功能或服務如 Instagram、Facebook 商店、約會功能等也予以捨棄。

對資料蒐集的限制而言，除提醒使用者做隱私設定健檢外，近期主要的努力為限制超過 90 天未使用的應用程式，存取使用者的非公開資料，然而官方仍坦承有漏網之魚待處理 (Papamiltiadis, 2020)。在既存資料的管理介面，則新增了活動紀錄管理功能，允許使用者以批次勾選的方式，刪除不必要的活動 (Facebook, 2020b)，儘管實作測試時仍只能透過手機應用程式運作，且筆者使用時效能仍不甚穩定，仍為重要的改進。雖然該新聞稿承諾日後將會推出桌面版 (available on desktop)，然而截稿前實作測試發現，仍無法透過網頁進行批次刪除，此時距離該新聞稿發布也已超過半年。對於慣用網頁版的筆者而言，刪除數位足跡的技術障礙仍然存在。Facebook 也新增了站外動態工具 (Off-Facebook Activity Tool)，讓使用者檢視與刪除各網站或應用程式與 Facebook 分享的數位足跡 (Protti, 2020)，也在既有的資料下載介面新增了類似功能 (Facebook, 2020a)。儘管這無疑頗大的進步，不過 Facebook 又如何與其他網站分享數位足跡的問題，似乎仍不得而知；且使用者似乎看到事後的紀錄，而無法事前決定哪些網站能與 Facebook 分享相關資訊，筆者實作站外動態工具的刪除功能時系統警語也言明，下次瀏覽外部網站時，Facebook 仍會接收到相關數位足跡，顯然該功能只是刪除紀錄，並未完全阻斷未來與外部網站的聯繫與資料聚合功能。截稿前筆者也再次檢視了廣告的喜好設定，發現雖然可以設定禁止 Facebook 使用協力廠商提供的資訊來向使用者使用廣告，然而對於設定廣告商能用於顯示廣告的特定類別資料，選項則相對有限，且該功能的文字解釋也讓筆者感到費解，筆者似乎只能如此解讀：除（該列表上）的（任職）公司名稱、職稱、學歷與感情狀態可以由使用者選擇關閉之外，其他登記在該網站的資訊例如年齡、性別等特徵，仍能作為投放針對式廣告的依據。這些也令該功能對於減少數位足跡蒐集的成效打了不少折扣，卻仍有助於使用者察覺業者對於數位足跡的貪得無厭。

¹⁰ <https://about.fb.com/news/>

（五） 整體廣告業者的自律努力

由於新興網路產業普遍以廣告作為主要收入來源，廣告業者的自律努力，取得追求獲利極大化與社會責任之間的平衡也非常重要。為回應聯邦貿易委員會於2009年初發佈的自律原則，業者也於同年7月發佈自己的自律原則，現由數位廣告聯盟（Digital Advertising Alliance）維護，並衍生多個補充文件（見表2-2），有趣的是標題居然與政府的版本一模一樣。

其所頒布的7大自律層面分別為：（1）教育（Education）：向使用者闡明線上行為廣告的性質，以及其所能做的選擇（2）透明性（Transparency）：揭露資料蒐集行為及用途（3）消費者控制（Consumer Control）：提供使用者更多控制數位足跡利用的選項（4）資料安全（Data Security）：數位足跡的儲存安全、目的與時間的限制，以及去識別化（5）數位足跡的利用方式有重大改變時，須再次獲得同意（6）對於機敏資料的利用限制，如禁止蒐集幼兒與特定財務與健康資料（7）課責（accountability）：與（不）定期監測締約業者是否符合規範，並揭露違約的業者。2013年對於行動裝置運作環境（mobile environment）的自律原則，則著重透明性、目的限制、機敏資料蒐集的限製、安全性與課責，內涵與2009年的總則也大同小異；但是另有禁止將資料用於就業、信用、醫療與保險適格性（employment/credit/healthcare treatment/insurance eligibility）評量的限制（pp. 31-32）。2011年、2015年與2018年又分別頒布對於多網站（multi-site data）、跨裝置、與政治廣告的數位足跡利用的補充規定，除對於政治廣告的部份，還強調贊助廠商的資訊揭露之外，也與2009年的總則相符。這些文件都非常簡短，只有2009年與2013年發佈的兩個自律原則篇幅稍長，對於著重事項也多只是原則性的陳述。補充規定對於特定事項的一再強調，透明性與課責甚至出現2次，隱含這些可能是目前最為外界詬病的問題。

表 2-2：Digital Advertising Alliance 發佈之自律原則及補充規定

作者與年代	名稱	著重事項
American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, & Interactive Advertising Bureau (2009)	Self-Regulatory Principles for Online Behavioral Advertising	A. 使用者教育 B. 透明性 C. 使用者控制 D. 資料安全 E. 條款修訂時須取得「再同意」 F. 機敏資料限制 G. 課責
Digital Advertising Alliance (2011)	Self-Regulatory Principles for Multi-Site Data	H. 資料蒐集的制限 F. 機敏資料限制 G. 課責
Digital Advertising Alliance (2013)	Application of Self-Regulatory Principles to the Mobile Environment	B. 透明性 C. 使用者控制 G. 課責 F. 機敏資料限制 I. 目的制限 J. 安全
Digital Advertising Alliance (2015)	Application of the DAA Principles of Transparency and Control to Data Used Across Devices	B. 透明性 C. 使用者控制
Digital Advertising Alliance (2018)	Application of the DAA Principles of Transparency & Accountability to Political Advertising	B. 透明性 G. 課責

資料來源：本研究整理。

儘管可預期業者在頒布自律準則時，對於細節會提出利己之解釋，且有不少但書或除外規定。部份陳述也可能與政府的監理模式抵觸，關鍵不只是自律準則涵蓋了什麼，還有些事能被列入管制範圍內的認知差異。如 2011 年對於跨網站資料的蒐集限制 (pp. 2-3)，及 2013 年對於行動裝置運作環境的自律準則中的目的制限 (pp. 30-31)¹¹ 規定，基於系統管理需要、市場研究與產品開發的目的收集的資料，及資料在去識別化過程中 (前) 之合理所需時間內，可豁免上述的制限便不甚合理。由於市場研究可涵蓋的範圍甚廣，此舉可能讓所有保護機制形同虛設。且就 GDPR 而言，任何只要未經嚴格去識別化的資料 (即使是處在作業流程內)，都應當適用與個人資料同等的制限。筆者也感覺該準則比較重視取得使用

11 甚至該條款也未具體陳述業者具體該做哪些目的制限，顯然與主流資料保護立法的精神相悖。

者至少形式上的知情同意，對於如何讓使用者掌握自身資料流向，則顯得避重就輕。對於坐擁市場優勢的廠商而言，要取得使用者形式上的同意並不困難，也難免引來只要形式同意在手，業者便能無所不為之譏諷。

另外一個明顯的差異，則如某個在 2013 年的自律準則中提及的除外規定，除非第三方是經明確授權（affirmatively authorized）而蒐集精確定位資訊（precise location data），否則該服務的第一人（first party）¹²無義務為此替該第三方徵得使用者的同意（pp. 25-26）。這作法可能是基於正當程序的立場，服務擁有者既然無需為第三方未經授權的行為背書，自然無需還為其爭取使用者的同意。然而聯邦貿易委員會為劍橋分析事件究責 Facebook 時，恐怕很難接受這類形同互踢皮球的說詞，比起劍橋分析可能利用安全漏洞竊取個資的事實，聯邦貿易委員會顯然更在意的是 Facebook 未依協議防堵安全漏洞而被趁虛而入。這些自律準則所著重的事項，看似與歐陸法系的資料保護法規高度重合，但是在定義或執行細節上顯然都不如成文法嚴謹。後期文件對透明性的不斷強調，隱含業者對於資料蒐集的細節，不是一直交代不清楚，就是無法以外界能理解的方式表達，業者自律的成效也無需等到劍橋分析事件的爆發，便可以預見失敗。

除多次補充上述原則外，數位廣告聯盟也啟動 AdChoices 專案，允許使用者瀏覽網頁時，透過 AdChoices 的功能閱覽網站資料政策，並選擇退出該網站的針對式廣告功能。AdChoices 雖為多個業者所響應，但也招致不少批評：首先，即使網站不顯示針對性廣告，仍可能繼續追蹤使用者的瀏覽行為。第二，標章無法引起多數使用者的注意。第三，這類退出機制的原理是利用瀏覽器的 cookie 標記，使用者清除瀏覽紀錄時，退出請求可能也會被重設，也徒增使用者未同意下被蒐集資料的風險（Johnson, Shriver, & Du, 2020: 36）。第四，AdChoice 也可能是不良的溝通媒介，有不少人誤以為點擊該圖示可能彈出更多廣告（Leon et al., 2012: 26），甚至誤認為是惡意程式（Johnson, Shriver, & Du, 2020: 41）。若使用者因而不願或不敢點擊，此類退出機制也就形同虛設。對於上述問題筆者認為可能的解釋是，要求業者採取理想上使用者同意才收集個資的模式無異擋人財路，業者當然就千方百計以迂迴的方式，增加使用者的退出成本，面臨外界壓力時也只願意做表面功夫，貓捉老鼠的戲碼也料將輪番上演。

12 按照該自律原則的名詞解釋（p. 7），大致為該服務的擁有者或控制者。

三、對於自我管制措施的批評

儘管自我管制看似有許多優點，外界的批判卻也不在少數，其中最嚴重的是不被認為具備經驗上的可行性。許多網站的隱私權政策，未完全符合官方對於自律原則的期待（Culnan, 2000; Marotta-Wurgler, 2016）；加入自律措施的業者的實際隱私表現，也未必真的比較好，隱含採取自律措施可能是廣告大於實質（Listokin, 2015）。令我們對於業者能否成功自主管理抱持許多疑問。

（一）從規範性角度違背隱私的本質

第一個顯而易見的批評，是從規範性（normative）的角度認為隱私權是可讓渡，或即使被讓渡也無傷大雅的物件。儘管在美國法律實務，個人資料被肯認為業者的財產與營業祕密，然而將個人資料的法律地位財產化本身，便可能是對人格尊嚴的侵害（翁清坤，2018）；主張隱私應該視為集體價值而不得有妥協或自願放棄的空間的論述恐怕也不在少數（Baruh & Popescu, 2017: 590）。況且在資本主義弱肉強食的運作現實下，完全放任業者自律也恐怕會淪為下一坡個人隱私的圈地運動，其後果恐怕也不為多數人所樂見。

（二）缺乏有效的誘因機制

自我管制措施也在實務上屢次被批評缺乏可行性。自我管制成功的前提是業者必須認同政策目標，且政府也要適時掌握業者自律實施的情形（Wood & Ravel, 2018: 1246）。然而現實上業者面對管制時，通常也不可能心甘情願，也難免因為無法駕馭惰性與貪婪而破功。政府是否有充份行政資源與能力防堵舞弊行為，恐怕也不無疑問。且若強勢業者一開始便拒絕自律，自我管制也勢將形同具文。由於投放針對式廣告的營收可達傳統途徑的兩倍（Johnson et al., 2020），使用者若能輕易退出廣告追蹤機制，勢將嚴重衝擊利潤。業者基於自利考量，顯然傾向拖延或虛應故事。

（三）冗餘的退出步驟阻礙使用者選擇

從使用者的角度，成功的軟體介面應避免不必要的操作步驟，以增進使用效益並節省適應的時間，許多網站的隱私權設定卻反其道而行，意圖以無謂的決策步驟提高使用者的退出成本，以盡力將其留在監控範圍內。現行美國主流的資料保護機制，必須由使用者自行選擇退出，方可通知業者將其排除於追蹤網路之外。業者可能利用冗長的法律條文或認知干擾，避免使用者知悉與觸發該功能，

儘可能使其繼續留在追蹤網路內；或是廣設障礙使其知難而退，或置於難以察覺之處。早期使用者還需親筆寫信，或付費並登記信用卡號碼，方能透過直銷協會（Direct Marketing Association）退出電話行銷網路（Hoofnagle, 2005: 2）。使用者點選 AdChoice 的使用者介面退出廣告追蹤網路，或啟動 Firefox 瀏覽器的請勿追蹤（Do Not Track, DNT）功能時，也等於向業者揭露隱私偏好，與再次揭露隱私幾無差別。在前述 2012 年聯邦貿易委員會起訴 Facebook 的事件中，Facebook 也曾在使用者的隱私設定頁面提供連結，讓使用者由其連接至第三方應用程式的設定頁面，以更改設定及防堵該程式竊取個資，然而 Facebook 並未有效向使用者揭露該機制，應用程式也繼續利用該漏洞竊取個資（周宥廷，2020）。其實最直覺也符合常理的做法，就是 Facebook 無需問任何人意見，便逕行關閉該接口，然而業者基於私利考量，顯然不願如此辦理。

退出追蹤網路的使用者比例極低的現象（Johnson et al., 2020: 40），雖無法直接證明與前述現象存在因果關係，也可能是隱私悖論所認為，使用者對隱私權的主觀估值與實際採取行動不一致的現象所導致；卻也令人懷疑自我管制政策與選擇擇出機制的應用，是否真能起到保護多數使用者的效果。且若擇出追蹤網路的人多半屬於資訊能力較強與收入較高的群體（Johnson et al., 2020: 34, 48-49），也可能表示必須從社會政策的角度的角度，針對弱勢者設計一套保護機制，以避免為強勢業者所剝削的可能風險。

（四） 只能管看得到的地方

任何監理策略的成敗，取決於業者揭露資訊的透明程度。隨著網路科技的急速發展，更大的挑戰是第三方 cookie、資料仲介等難以被察覺的型態（Christl, 2017a; Christl & Spiekermann, 2016; Crain, 2018; Hoofnagle, 2005; US Senate Committee on Commerce, Science, and Transportation, 2013）。使用者既然無法知道自己被誰、及如何收集資料或追蹤，也就更難有退出的可能，也成為保護的新難題。如在第一節已提及，Facebook 使用者在隱私權設定中對自主提供的資料做非常有限的控制，對於被動產生與蒐集的資料，則幾乎看不到相關功能可資查閱、修正或刪除的功能。且由於現行 Facebook 資料政策規定，只要網站被植入了 Facebook 相關的應用程式，即使是在未登入的情況下，Facebook 仍可能透過第三方機制追蹤網路活動；使用者等於在未知情與同意的情況下，暴露於 Facebook 的追蹤網路。但是如果使用者連自己有沒有被追蹤都不甚清楚，又該怎麼知道自己

的資訊如何被蒐集與利用？也導致使用者往往事後才驚覺受害。若業者不願主動提高對使用者數位足跡蒐集與利用方式的揭露，自我管制措施也將毫無意義。

第五節 以他律為主的數位足跡監理機制

綜合以上討論不難想見，單憑業者的自我管制措施，似乎難以達到合宜的保護成效。許多國家則採取以他律為主，甚至全面立法的監理機制，然而其手段是否合宜與是否達成預期成效仍有待釐清。綜合國際趨勢與在地需求，以下將分別探討號稱國際標竿的歐盟一般資料保護規範（GDPR），以及我國個資法，以及兩者的可能優缺點，進而引導可能的研究方向。

一、 歐盟一般資料保護規範（GDPR）

歐盟的一般資料保護規範（GDPR）於2018年5月25日正式施行，取代1995年通過的資料保護指令（Data Protection Directive 或 Directive 95/46/EC）。由於對業者課與繁重的義務，加上其嚴苛的罰則（最高可處2000萬歐元或全球4%年營業額擇高者），而被譽為史上最嚴格的個人資料保護法。GDPR援用了許多前衛的概念，如跨境適法、預設資料保護設定（data protection by default），事前需徵求使用者的明示同意及衍生的選擇加入原則、與設計階段納入資料保護（data protection by design，即在資料蒐集的初期階段，便考慮隱私與安全風險等，如該法前言之Recital 78）（林思惟，2016；蔡昀知，2019：33-38）。2020年9月7日，歐洲資料保護委員會（European Data Protection Board）發佈《對於瞄定社群媒體使用者之指引 8/2020》（Guidelines 8/2020 on the Targeting of Social Media Users）初稿¹³，並徵求公開意見至該年10月19日為止，該指引將針對式廣告投放者進一步分為社群網站服務提供者（social media provider）與瞄定者（targeter，即透過社群網站服務為中介，尋找最終行銷對象的業者，例如廣告主），並對其在投放過程的決策角色與責任歸屬、法遵義務進一步釐清與界定。

（一） 與社群網站使用個資較為相關的規範

由於GDPR與相關法制的龐雜，基於本文定位與筆者專業上的限制，難以巨細靡遺地列舉與分析其所有內容。以下僅摘述社群網站使用個資較為相關的條文

¹³ 請見 https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf

或規範並加以簡介。相關細節或其他未竟之處，請參見其他（含以下引用）之專業書刊或研究報告。

1. 資料處理的原則性規定

GDPR 的第 5 條作為總綱，規定處理資料應遵守下列原則：（1）合法、公正與透明性（2）目的限制（3）資料最少化（4）正確性（5）儲存時間限制（6）完整與保密（7）負完全法遵責任。上述總綱內容也分別體現於賦予使用者的權力與課與業者的義務中。

2. 賦予使用者的權力

賦予使用者的權力，強調數位足跡的流向應擁有相當的主動權，具體而言包含知情權（the right to be informed）、近用權（right of access）、更正權（right of rectification）、刪除權或被遺忘權（the right to erasure/to be forgotten）、限制使用權（the right to restriction of processing）、資料可攜權（right of portability）與拒絕權（right to object）等（張陳弘、莊植寧，2019：165-166）。在此基礎下業者利用數位足跡時，需能舉證使用者的同意完全出於知情與個人意願（第 7 條）。徵求使用者同意時，也必須給予其一定的控制權限，例如在（1）預設勾選使用者同意（或稱默示同意）、只能一鍵同意所有資料利用（楊皓勻，2020; Nouwens, Liccardi, Veale, Karger, & Kagal, 2020: 2, 5）、（2）勾選同意方能進入所有網頁或服務（Nouwens et al., 2020: 5; Zuiderveen Borgesius, Kruikemeier, Boerman, & Helberger, 2017: 8-9）¹⁴、（3）同意聲明無法被輕易地撤回（Nouwens et al., 2020: 5）、（4）業者未清楚揭露資料用途、或以話術包裝甚至誘導（楊皓勻，2020）等情況下，皆可能不算取得有效的同意。

3. 課與業者的義務

除第 5 條規定事項外，業者還必須履行維護安全性、設置資料保護長（data protection officers, DPOs）、妥善儲存資料處理紀錄、執行資料保護影響評估（data protection impact assessment, DPIA）等義務（張陳弘、莊植寧，2019：239）。也必須在「意識」（aware）到外洩事件發生的 72 小時內通報主管機關，包含外洩內容、對當事人可能影響、採取之緊急應變措施、資料保護長聯絡方式等事項，及通報當事人等（張陳弘、莊植寧，2019：244-255；張腕純，2018）。

¹⁴ 然而這類被稱為“cookie wall”（Nouwens et al., 2020：2）或“tracking wall”（Zuiderveen Borgesius et al., 2017：9）的手法是否自動無效，前引文獻則指出實務尚未有定論。

4. Facebook 宣稱的法遵措施

Facebook 為符合境外傳輸的適足性規定，以維繫在歐洲的業務與平衡公關壓力，仍有遵守 GDPR 的需求。其公關文件也強調透明性（transparency，向使用者闡明資料的處理方式）、控制（control，提供使用者控制資料處理方式的選項）與課責（accountability，取信使用者能妥善處理資料），而在節錄 GDPR 對於資料處理的核心原則時，則著重在出於契約之必須（contractual necessity，資料的處理必須以實現服務或契約之必須為前提），使用者同意（同前述 GDPR 的相關事項），處理資料須有合法基礎，且不能與基本權益抵觸（legitimate interests）（Facebook, n.d.）。儘管在實務上 Facebook 是否真能達到上述承諾可能有待驗證，仍或可作為監理政策目標設定上的輔助。

（二） 批評

儘管 GDPR 以巨細靡遺的成文法為著稱，對於資料主體的法律保護也相對與明確完善，美國法學界鼓吹仿效歐盟模式，由聯邦政府主導全面性立法的芻議也不絕於耳。然而也難免被批評充斥理想主義，失敗的結果也看似在所難免：

1. 徒法不足以自行

缺乏執行能力向來是法律面臨的指謫之一。GDPR 的內容與歷屆資料保護法規的高相似度，也可能招惹只是浪費時間處理相似問題的批評（Determann, 2012: ¶10）。條文的疊床架屋，也難免引發執行永遠跟不上立法的訕笑。業界缺乏法遵意識、缺乏執行必要能力與業者仍掌握最大主動權，恐是歐盟模式屢次失敗的最關鍵因素：

（1） 業者缺乏法遵意識

自我管制措施在執行過程，因不敵人性的怠惰與貪婪而屢戰屢敗，以成文法為主的資料保護政策也相去不遠。許多業者並沒有認真看待 GDPR 的嚴格要求與罰則，直到施行前夕才在臨時抱佛腳。不是根本沒有開始準備，就是停留在非常初步的階段（Jackson, 2018a; Lopes & Oliveira, 2018）；也有業者事前高估了自動化技術的處理能力，直到猛然發現許多事務仍需人工處理時才兵荒馬亂（Jackson, 2018a）。另一方面 GDPR 也留有許多詮釋與執行的模糊地帶，令業者無所適從，例如要求設立合理的資料保存期限看似簡單，但是該設多久卻是大問題，這也形成另一個現象，業者因畏懼重罰，寧可大小事都彙報主管機關，也加重政府

端的負荷 (Jackson, 2018a)。這種混亂固然可視為新法令執行前夕的必然，然而若業者主動並早日因應，應不至於到了緊要關頭才在臨時抱佛腳。

(2) 業者仍掌握最大主動權

GDPR 規範雖然看似縝密，但是許多關鍵的法遵程序，如資料保護影響評估等，實則仍由資料控制者（如業者）主導執行，倘若資料控制者行事不夠周延，GDPR 的保護效果恐怕也將大打折扣 (Gonçalves, 2020)。再者，資料保護政策成功的先決條件之一，是使用者必須能履行近用權，查詢與修正被蒐集的個人資料，也方可起到防弊的效果。然而使用者能否查到上述資料，也還是業者說了算。如於本章第一節所述，使用者在 Facebook 只能對類型一資料實現非常有限的控制權。在香港通訊業的研究案例中，研究者即使聯繫主動客服人員，往往也只會得到官腔式的回應，屢次婉拒使用者調閱被儲存的通聯紀錄，有時甚至必須援引法律文件，才可能得到稍微積極的回應，且業者仍可能推諉 (Tsui & Hargreaves, 2019)。雖然缺乏證據，但筆者推測社群網站的狀況恐怕也相去不遠，也難保 GDPR 的執行環境下不會發生類似的情形。

(3) 政府缺乏執行必要能力

政府也缺乏必要的執行能力，其中以執法系統的失靈最為嚴重。除了高訴訟成本外，個資外洩事故在訴訟上低落的成案率與勝訴率，也可能是民眾不願訴諸審判，導致法律無法完善運作的重要因素 (Park, 2019)。此外，雖然 GDPR 號稱是全歐盟通用，且不若資料保護指令還需要國內法化的過程，但是執行則由公司註冊之會員國各自為政，料將會繼續有執行不同調的問題，且主要的跨國科技公司除亞馬遜以外，均設籍於愛爾蘭 (Stupp, 2020)，但是截稿前查詢 GDPR Enforcement Tracker 網站¹⁵得知，該國也遲至 2020 年 12 月，才對 Twitter 開出（第一張）45 萬歐元的罰單；反而是德國在 2019 年便以欠缺資料保護專員為由，對 Facebook 裁罰 51,000 歐元。也透過查詢前述網站得知，Google 於 2019 年 1 月遭法國裁罰 5000 萬歐元¹⁶，一直是裁罰金額最重的案例。隱含 Google 幾乎是 GDPR 上路近 3 年以來唯一被重罰的大戶，且只被罰日營業額的十分之一 (Satariano, 2020)。與日後 Facebook 遭聯邦貿易委員會裁罰 50 億美元相比，幾乎不成比

15 <https://www.enforcementtracker.com/>

16 主因是使用者「未被充份通知」資料被用於個人化廣告的方式 ("not sufficiently informed" about how Google collected data to personalise advertising) (Fox, 2019)。

例。這恐怕也令外界對於政府是否有足夠執行能力，遏止業者的踰矩行為的信心打了相當大的折扣。

2. 抵觸社會衡平價值

由於 GDPR 對於業者的資安設下非常高的要求，在消費者看來看似好事。但是誠如第三節對於管制悖論的研討，此舉卻也可能讓科技業淪為寡占甚至獨佔市場，而將多數中小企業或初期創業者拒之門外。因而對於社會衡平的衝突也值得深思。筆者無意重述管制悖論的探討，而著重於強調資安的可能後果。GDPR 的立法目的固然是希望雙管齊下，同時從前後兩端限制業者蒐集與使用者數位足跡的範圍，並提高資安層級以降低非法入侵的機會。但是既然社群網站已經轉型為資訊高牆花園的運營型態，即使不否認資安的重要性，但是應該檢討需要分配多少資源在資安事務，以及分配的方式是否合理？防止資料被以類似劍橋分析事件的方式非法使用甚至盜賣固然重要，但是於立法（及隨後的設立組織編制等）再次強調與要求業者加強資安，是否顯得冗餘？有鑑於近來資安事件的頻傳，這或許還值得商榷。然而過度保護的資安立法，也可能給予優勢業者絕佳理由建立資訊高牆，以法遵之名獨佔營業關鍵資訊進而阻礙同業競爭？因此資料保護政策不能只是鐵板一塊，在使用者知情同意與不造成傷害的前提下，適度放寬甚至強制共享部分被視為機密的資料，以就各種利益角度，如財產權、資訊安全與商業競爭之間取得平衡，也是應審酌的問題（Graef et al., 2018: 220-222）。

（三） 現有文獻對於監理實施成效的評價

有鑑於 GDPR 的實施帶來的龐大成本，監理成效的評估也亦加迫切。在零星的現有文獻中，評估方式主要為檢測 GDPR 實施後，追蹤瀏覽行為的改變情形（主要為 cookie 的使用方式），部份則探討手機應用程式利用存取權限狀況的改變，以及徵求使用者同意的方式是否符合 GDPR 的要求等。儘管業者對數位足跡的利用看似有收斂的趨勢，仍與 GDPR 的標準有相當距離：

首先，對追蹤瀏覽行為依然普遍，有些甚至事前未徵得至少形式上的知情同意，使用者想主動避開通常也非常困難（Sanchez-Rola et al., 2019: 344）。有些網站甚至在使用者明確拒絕下仍然植入追蹤用 cookie，且 Alexa 排名在前的熱門網站部署第三方 cookie 的行為，雖然在 GDPR 實施之初顯著下降，但是不到一年後便幾乎被打回原形的似乎不在少數（Hu & Sastry, 2019: 137, 140）。另一份研究

也顯示，GDPR 實施當月，Alexa 排名在前的熱門網站佈署非合意性持久型（non-consensual persistent）cookie 的行為雖然有下降趨勢，降幅仍可能不如排名落後者（Dabrowski, Merzdovnik, Ullrich, Sendera, & Weippl, 2019: 266）。雖然上述研究是綜合各類型的網站，考慮社群網站通常也屬熱門網站之列，推定情況應該相去不遠。且考慮 Alexa 排名在前的網站，流量與使用時間通常也較大與較長，筆者懷疑 GDPR 減少網站追蹤瀏覽的效果相當有限。針對手機應用程式的研究則明顯看出，Facebook 在 GDPR 實施後，對於存取權限宣告（permission manifest）的變化不大，雖然徵求使用相機、聯絡人與通話功能的情形減少，但是徵求使用定位功能、感應器、與儲存空間的情形則增加（Momen, Hatamian, & Fritsch, 2019: 12）。隱含社群網站在 GDPR 實施後，業者對於數位足跡的應用仍然有增無減。雖然無法確知是社群網站的業務性質使然，造成敏感數位足跡的應用未見減少，還是因為業者能利用市場權力延緩遵守法規的要求，總體而言卻可能讓能被檢視的範圍與業者的實際情形稍微趨於一致。然而 Sanchez-Rola et al.（2019: 349-350）也指出，現有技術仍無法讓網站在啟用第三方內容的時候避免追蹤特定使用者，若要完全達到法遵要求，網頁可能必須對使用者只顯示靜態文字。這顯然也會對界面的美觀造成糟糕影響，這類可能屬於技術問題的限制，也需要以更細緻的方式處理。

在徵求使用者同意的程序中，實務也多差強人意。儘管隱私權政策文件在易讀性與法遵的程度稍有進展，仍然難以掩飾許多地方仍然不合格的事實（Linden, Khandelwal, Harkous, & Fawaz, 2020）。而經常在網頁下緣，用來徵求使用者同意使用 cookie 的同意管理平台（consent management platform, CMP），則幾乎只有一成的英國主要網站能達到 GDPR 的標準（Nouwens et al., 2020），隱含業者仍缺乏遵守的誘因，或者現行技術或實務仍無法滿足優求。另外值得注意的是，在有些網站使用者若接受預設選項，接收到的 cookie 還比其他只通知但沒選項，甚至連通知都沒有的網站還多（Hu & Sastry, 2019）。最後也發現一個值得注意的趨勢，儘管 GDPR 實施後，業者確實將使用者隱私視為重要課題，卻也對來自歐盟與非歐盟的使用者，存在明顯差別待遇（Dabrowski et al., 2019; Linden et al., 2020）。儘管業者試圖從非歐盟地區使用者多搜刮點資料的策略性作法，在商戰實務上不難理解；然而若被發現採取差別待遇，被指控歧視與連帶後果也不容小

觀。儘管業者可能的動機與相關算計的機制仍有待研究，也隱含 GDPR 的跨域影響能力可能被嚴重高估，業者也能有恃無恐。

（四） 小結

以上簡短探討了對於 GDPR 的批評，以及實施後造成負面影響的相關報導，發現論述主要集中在對於政府管制能力的懷疑，以及更嚴格的產業基準實施後，可能造成對市場機制的扭曲，甚至剝奪新進者與中小企業發展空間；實證研究也顯示業者對於隱私保護的改善程度非常有限，皆與管制悖論的預言大致呼應，以嚴肅的態度檢視並商討對策也益加迫切。業者在執行的關鍵環節仍掌握最大主動權力，也是目前已知監理政策未能攻克的關卡。

二、 我國個人資料保護法

GDPR 的實施固然會衝擊社群網站的運作實務，然而 GDPR 的保護範圍仍有地理界限，社群網站仍可對於非歐盟使用者進行大規模的資料處理，各國仍需自定專屬的相關保護法令。我國在 1995 年施行《電腦處理個人資料保護法》及後來的《個人資料保護法》（以下簡稱個資法），因其立法過程大量參考資料保護指令（Data Protection Directive 或 Directive 95/46/EC）相關內容，而接近歐盟早期的法制架構（李世德，2018：70）。該法迄今最大的修正於 2012 年 10 月 1 日起施行，並更名為《個人資料保護法》，重點在擴大保護範圍（不再限於電腦處理資料）、確保當事人自主性與權力行使、更嚴格規定業者利用個人資料的要件與落實安全維護、及賦予主管機關行政檢查權等（邱映曦、劉敏慧、何寶中，2013：46；財團法人資訊策進會科技法律研究所，2019：4-6）。2015 年的第二次修正除將病歷列入特種資料外，主要是局部鬆綁部份條文，容許業者在告知義務與使用者同意以更有彈性的方式處理（如當事人同意形式不限於書面為之，也貼近國際慣例），以及刪除該法非意圖營利而違反個資法之刑事責任，以避免與刑法競合與重複處罰的問題（財團法人資訊策進會科技法律研究所，2019：6-9）。為與 GDPR 接軌並取得跨境傳輸之適足性認證，國發會原訂於 2020 年再次進行個資法的修訂（林子蘅，2019）。¹⁷但是實際修法日程仍可能有相當變數。配合現行個資法架構，我國也已有參考 ISO 29100/191 標準制定的 CNS29100/191，對於隱私權、個人可識別資料（personally identifiable information, PII）等關鍵術語加以規

17 國家發展委員會法制協調中心（2019）的新聞稿則顯示修法作業已於 2019 年 9 月開始，然而此差異不致影響本文對該事件的詮釋。

範（行政院資通安全處，2014），及建立個人資料去識別化實務基準（孫鈺婷，2019），並建置臺灣個人資料保護與管理制度規範（Taiwan Personal Information Protection and Administration System, TPIPAS），提供業者法遵與認證的技術指引（臺灣個人資料保護與管理制度，2016）。經濟部工業局作為資訊服務業的主管機關（法務部，2015），也先後制定《製造業及技術服務業個人資料檔案安全維護管理辦法》，及出版《「製造業及技術服務業個人資料檔案安全維護管理辦法」導入說明手冊》與《資訊服務業提供服務之個資保護及案例說明手冊》，進一步規範業者的義務，如個資管理人員的位階與能力下限、個人資料風險評估與相關管理機制等（經濟部工業局，2017：9-10、16-30, 2018：17-19、27-33）。

（一） 資料處理的原則性規定

我國個資法對於個資蒐用行為的原則性規定，也與 GDPR 第 5 條總綱相似，分別為誠實信用（公平性）原則、比例原則（目的限制與最少蒐集）（第 5 條）、透明性原則（第 8 至第 9 條）、正確性、最短化儲存時間（第 11 條）、安全性（第 18 條、第 27 條、施行細則第 12 條）、法遵責任（第 7 條）等，雖然與 GDPR 相比散落於各處而缺乏系統性，規範事項仍大致相當（張陳弘、莊植寧，2019：68-74）。我國個資法與 GDPR 相比，雖有不少細節的簡略與闕漏，在部份條文的應用上卻較為嚴格，如（1）法務部函釋對於知情權的履行採取較嚴格的標準，需「個別通知」使用者（2）欠缺基於公共利益或研究目的，彈性延長儲存時間的規定（張陳弘、莊植寧，2019：71-73）。

（二） 賦予使用者的權力

我國個資法雖賦予使用者知情權（第 8 至第 9 條）、近用權（查詢、要求副本）（第 3 條、第 10 條至 14 條）、更正權（第 3 條及施行細則第 19 條、第 11 條）、拒絕權與刪除權（第 3 條、第 11 條），然而與 GDPR 相比，除有甚多細節的簡略或闕漏外，最為顯著的問題是欠缺目的外使用的再告知要求、以及將刪除權與拒絕權合併規定造成的混淆（張陳弘、莊植寧，2019：217-225），以及幾乎沒有資料可攜權、拒絕自動化數位剖析權、與被遺忘權的規定（張陳弘、莊植寧，2019：228-229；李世德，2018：89），使得效果大打折扣。

（三） 課與業者的義務

我國個資法課與業者的義務相較 GDPR 則更為精簡，除前述的總則事項及第 19 條、第 20 條的合法要件與目的外利用限制外，另有安全性維護（主要為第 6、18、19、27 條；施行細則第 12 條）與外洩時通知使用者的義務（主要為第 12 條、施行細則第 22 條），比較明顯的問題除敘述缺乏系統而散見於各條文外，另有（1）未強制業者執行資料保護影響評估（2）非公務機關未強制設立資料保護長（3）發生資安事故時僅須通知當事人而無須通報主管機關，且無 72 小時的通報期限（張陳弘、莊植寧，2019：279-280）。唯經濟部工業局（2018：35）於《資訊服務業提供服務之個資保護及案例說明手冊》規定，業者遇到足堪影響正常營運或涉及多人權益之重大事故時，仍必須通報該局及地方政府。

（四） 小結

我國個資法兼具條文精簡且遺漏許多重要原則，卻又在某些事項比 GDPR 嚴格的矛盾特性。顯見我國個資法的問題不是單純的過於簡略，還有一些可能不太合宜的細節必須深入釐清。此外，我國個資法也仍有存在多年的問題尚未被有效處理，如（1）罰則過輕（2）主管機關不明確（3）對於合法利用資料要件的認定過於偏袒資料控制者等（莊庭瑞，2003）。現行個資法的行政裁罰最高以 50 萬為限，且僅及於非公務機關；對於民事賠償的規定（第 28 條），雖然被害人在不易舉證實際損害時，可以每人每事件二萬元以下計算求償金額，顯然仍不足以彌補相對高昂的訴訟成本。再者，即使各行業有專責主管機關，如今隨著個資保護日趨專業化，而有比照 GDPR 統一設立專責機關的呼籲。最後，我國個資法對於公務機關與非公務機關處理資料單憑「對當事人權益無侵害」（第 15 條與第 19 條）及「有利於當事人權益」（第 16 條與第 20 條）便可分別進行目的內與目的外使用，正當性顯然過於薄弱（張陳弘、莊植寧，2019：106-107）。一種可能的解方是比照 GDPR 第 6 條第 4 項，設立須與原初蒐集目的相容的限制（張陳弘、莊植寧，2019：134-135）。陳泉錫（2016：137-139）則認為，我國個資法的關鍵問題不是罰則，而是欠缺執法的必要資源，如足夠的關鍵人力資源與經費、清楚的主管機關與權責分配、法律關鍵名詞定義明確¹⁸、及落實績效考核等，又我國個資法雖已於第 18 條明定公務機關需指定專責安全人員，卻沒有罰則而僅具宣示性質，也缺乏專責機關與管考機制，以及足額的專業資訊人員，這些皆可能使法

18 如該文第 138 頁提到，因為我國個資法對於個人資料處理目的限制的解釋不一，造成有些機關為避免觸法而保守處理，造成如榜單以「陳 OO」方式公告等令人啼笑皆非的結果。

令淪為具文。這也顯示立法只是探討監理政策的其中一個重要環節，執行面與績效管考可能更加關鍵，而這類文獻又更形缺乏。

且不難想見的是，我國除要面對前述徒法不足以自行的問題以外，由於國人常用社群網站幾乎皆由境外業者提供，政府是否擁有足夠跨境執行能力，顯然也是挑戰。歐盟畢竟有強勢的政治經濟影響力，而能將制度強加在許多境外實體，然而迫於許多關鍵網路節點仍為美國企業強勢主導的現實，在與美國進行適足性談判時仍須做出相當妥協，境外執法能力也有限，2000年通過的安全港協議，因為無法保護歐盟公民被儲存在美國的資料免於該國國家安全局（National Security Agency, NSA）的監控而最終宣告失敗（孫鈺婷，2016；Bowcott, 2015），於2016年取而代之的隱私盾協議（Privacy Shield）也因為類似理由，於2020年7月宣告瓦解（李芯，2020）。若歐盟的處境已經如此，我國迫於外交處境與政經影響力居弱勢的現狀，恐怕也只會徒增法律出不了國門的嘲諷，如何搜尋其他途徑突圍，也成為下一步研究的重點。

三、數位足跡管制模式之間的比較

本段就前文提及主要國家的資料保護政策模式，進行重點的比較分析。對象除了歐盟 GDPR 與我國個資法之外，美國則以數位廣告聯盟作為代表，綜觀其參與業者的規模，以及在現存文獻出現的頻率，該聯盟應該足以代表美國自我管制的現況。分項比較結果茲說明如下，並將主要異同羅列於表 2-3：

（一）法律適用範圍

在適用的資料處理事項中，GDPR 第 2 條規定（除第 2 項所規定事項以外），只要以系統性方式處理，意圖「構成檔案系統」的個人資料，不問是否自動化，均適用於其管轄範圍。我國個資法第 2 條與此大致相符，唯在用詞上 GDPR 第 2 條、第 4 條將所有處理方式均以「處理」（processing）表達¹⁹，我國個資法第 2 條又細分為「蒐集、處理、利用」三種方式。唯該差異並不足以影響整體解讀方向。綜觀 GDPR 與我國個資法對於個人資料的定義，字面上雖然無太大差異，都是指得以直接或間接方式識別該自然人的資料。張陳弘、莊植寧（2019：32-33）則批評國內學說與實務見解仍嫌紊亂，不若歐盟資料保護工作小組（Article 29 Data Protection Working Party, WP29）乾脆採用較為寬廣的定義方

¹⁹ 此處採用李世德（2018）的譯法。

式，將所有可能連結特定個人的資料納入保護；且我國以「是否」為個資的二分法架構，也難以用於處理新興科技情境中特有的間接識別個資，而宜從可能被識別的程​​度重新思考（張陳弘、莊植寧：40-44）。

屬於自我管制模式的數位廣告聯盟則採取分部式規範，規約範圍也侷限於數位廣告相關業務的數位足跡利用，分別於 2009 年與 2013 年出版了較完整的自律準則並加以擴充。與現行法律較重要的不同，除了對於個人可識別資料儘可能採取簡單與一刀切的定義外，2009 年的行為準則也將其定義為「關於特定個人的資料，包括名稱、地址、電話號碼與電子郵件地址，當用來識別特定個人時」（p.11），但也於該文評註（commentary）處有獨特的詮釋「當資料不是用做識別時，就不被視為個人可識別資料」，並舉例「當 IP 位置未與其他個人可識別資料連結時，就不會被列為個人可識別資料」，反之亦然（p. 25）；這顯然迥異於現行法律，例如 GDPR 的認定標準是，只要任何人能以合理方式透過該資料辨識特定個人，即使是獨立的 IP 位置，也會被視為個資（張陳弘、莊植寧，2019：31）。雙方對於個資保護定義的認知落差也在此一覽無遺。

業者自律規範的施行效力，顯然是侷限在該組織的範圍內，而無須贅言。兩法在適用的地理範圍也有明顯差異。GDPR（第 3 條）的思維是以網路無國界作為考慮，只要是涉及歐盟境內人民的資料處理行為，便可能會被列管（張陳弘、莊植寧，2019：8-9）；反觀我國個資法（第 51 條）雖規定對境外蒐集我國公民資料者亦適用，法務部又函釋需為設籍我國且處理我國公民之資料控管者，始適用於該法，未於我國設立據點，但是實際處理我國公民資料的境外實體，目前不屬於該法的監理範圍（李世德，2018：74），法律與函釋見解似乎不太一致。許多人可能認為 Facebook 無在台分公司，所以台灣無法可管，但查詢我國經濟部商業司「商工登記公示資料查詢服務」後得知，Facebook 已於 2014 年底以「台灣臉書有限公司」名義在台登記，另一個國人常用服務 Google 也已於 2006 年初以「美商科高國際有限公司」名義在台登記，也意味現階段我國對於主要社群網站，至少有名義上的境內監理標的（相關運作另見本文第 101 頁之分析），只是實際成效如何則有待評估，歐盟的執法經驗也或可作為借鏡。

（二） 賦予使用者的權力

如前文所述，我國個資法賦予使用者的權力與 GDPR 相比，有甚多細節的簡略或闕漏，使得效果大打折扣。數位廣告聯盟的自律準則，則幾乎未提及前述賦予使用者的任何具體權力，顯見由於業者與使用者的締約基礎，實際存在相當的權力不對等關係。

（三） 課與業者處理資料的義務

我國個資法與 GDPR 課與業者處理資料的義務，雖然精神與範圍大致相似；然而我國個資法仍存在許多過於簡化或不合理之處，仍需進一步釐清與矯治。數位廣告聯盟的自律規範，著重的事項看似與前述兩法相似，不外乎教育使用者、透明性、使用者控制、資料安全、特種資料的應用限制與課責等 7 大類，然而其思維與實務操作均迥異於現行法律，除前述對於個人可識別資料的認定外，法律著重的是在如何在結果上獲致較好的資料保護效果，自律管制著重的則是在程序上有效通知（教育）使用者，以得到至少形式上的同意；更精確地說，若業者能對使用者提出明顯不利的條件，但是使用者仍願意接受，也是使用者的選擇，法律也就不該輕言干預。政策制定者與立法者可能不苟同這類思維，但是也勢將需要建立穩固的論述結構，以減少可預期的阻力。

（四） 安全性與跨境傳輸限制

如前文所提及，我國個資法對於安全性的要求，內容不若 GDPR 繁雜與嚴謹，且缺乏類似 GDPR 第五章對於跨境傳輸的限制，如適足性規定（第 45 條）、未經適足性認定或無適切安全措施下的規定（第 45 至 49 條）等。但若接受國有相關法規但不符合我國標準，依我國個資法第 21 條規定仍能限制其傳輸。雖然數位廣告聯盟於 2009 年與 2013 年出版之自律原則，均將資料安全列為著重事項之一，如 2009 年版的著重於資料防護，資料保存須符合法遵要求，與服務提供者的必經程序；2013 年版則幾乎只是一筆帶過。與現行立法相比，自律原則對於資料安全的規範顯然簡潔得多，也沒有任何資料跨境傳輸的相關規定。但是既然資料是業者的關鍵資產，可預期自律原則也無需多費脣舌，還對業者本來就非常在意的安全問題說三道四。對政府監理者而言，這也或可成為另一種借鏡，檢討是否還應當花這麼高比例的政策資源，在業者自己本來就會做好的事情上，而著重在其他更需關注的事情上。

表 2-3：各監理模式之間的比較（摘要）

	GDPR	我國個資法 ²⁰	數位廣告聯盟	主要異同
適用事項範圍	涉及所有個人可識別資料之處理	同左	只針對特定業務的個人可識別資料處理	<ol style="list-style-type: none"> 1. GDPR 就可能被識別個資認定較為統一廣泛，我國個資法見解則較為寬鬆與分歧 2. 視用途差異，數位廣告聯盟對於資料可識別性的認定也可能會有所不同
適用地理範圍	具域外效力	以設籍我國機關與公民為主，幾乎沒有域外效力	限組織內部	<ul style="list-style-type: none"> • GDPR 具域外效力，我國個資法則幾乎沒有
資料處理原則	<ol style="list-style-type: none"> 1. 合法、公正與透明性 2. 目的限制 3. 資料最少化 4. 正確性 5. 儲存時間限制 6. 完整與保密 7. 負完全法遵責任 	<ol style="list-style-type: none"> 1. 誠實信用原則 2. 比例原則 3. 透明性原則 4. 正確性 5. 最短化儲存時間 6. 安全性 7. 法遵責任 	<ol style="list-style-type: none"> 1. 使用者教育 2. 透明性 3. 使用者控制 4. 資料安全 5. 條款修訂時須取得「再同意」 6. 機敏資料限制 7. 課責 8. 資料蒐集的限制 9. 目的限制 10. 安全 	<ol style="list-style-type: none"> 1. 我國個資法對於知情權（透明性原則）的履行較 GDPR 嚴格 2. 我國個資法缺乏基於公益、研究目的的儲存時間延長彈性設計 3. 我國個資法欠缺目的相容要件

20 我國個資法對公務機關與非公務機關有不同規定，但本文只聚焦於非公務機關之討論。

表 2-2 (續)

	GDPR	我國個資法	數位廣告聯盟	主要異同
資料主體權利	<ol style="list-style-type: none"> 1. 知情權 2. 近用權 3. 更正權 4. 刪除權 5. 限制使用權 6. 資料可攜權 7. 拒絕權 	<ol style="list-style-type: none"> 1. 知情權 2. 近用權 3. 更正權 4. 拒絕權與刪除權 	幾乎無規範	<ol style="list-style-type: none"> 1. 我國個資法欠缺目的外使用的再告知要求 2. 我國個資法將刪除權與拒絕權合併規定造成混淆 3. 我國個資法幾乎沒有資料可攜權、拒絕自動化數位剖析權、與被遺忘權的規定
資料控管者義務	<ol style="list-style-type: none"> 1. 維護安全性 2. 設置資料保護長 3. 妥善儲存資料處理紀錄 4. 執行資料保護影響評估 	<ol style="list-style-type: none"> 1. 安全性維護 2. 事故通知使用者 	<ol style="list-style-type: none"> 1. 教育 2. 透明性 3. 消費者控制 4. 資料安全 5. 資料利用方式改變時須再次取得同意 6. 對於機敏資料的利用限制 7. 課責 	<ol style="list-style-type: none"> 1. 我國個資法未強制業者執行資料保護影響評估 2. 我國個資法於非公務機關並未強制設立資料保護長 3. 數位廣告聯盟較著重於通知、教育使用者資料流向，及包含可能的拒絕方式 4. 發生資安事故時，我國個資法規定僅須通知當事人，而無須通報主管機關，且無 72 小時的通報期限

表 2-2 (續)

	GDPR	我國個資法	數位廣告聯盟	主要異同
跨境傳輸限制	原則禁止	原則允許	無相關規定	<ul style="list-style-type: none"> GDPR 採原則禁止，例外允許；我國則相反

資料來源：本研究整理自張陳弘、莊植寧（2019）、李世德（2018）、數位廣告聯盟各前揭文件。



(五) 小結

本段落比較了數位廣告聯盟自律原則、GDPR 與我國個資法等三種治理模式之間的差異。業者的自律原則一如預期，通常只能達到頂多寥勝於無的保護效果，在隱私事件接連發生的情況下，導入他律為主的監理機制仍為必要。雖然我國個資法整體內涵與 GDPR 仍然接近，然而在條款編排、細節的重視程度、學說及函釋的齊一性、罰則與對業者行為的控制等均與 GDPR 望塵莫及；卻偶有某些事項更嚴格的矛盾現象。我國的監理制度的修訂，顯然不能只照抄外國制度，而需就立術層面重新通盤考慮。仍需面臨以下問題：

1. 在複雜與簡單之間取捨

誠然我國個資法因為細節的不夠完整、法規被大量函釋與學說架空，可能造成法規保護效果不足甚至徒具形式。但是從相對的角度，若要像 GDPR 以近乎面面俱到的形式規範數位足跡的處理過程，可預期法規內容將急遽膨脹，並提高管制方與業者的法遵成本。另一方面，雖然我國個資法僅有 56 條，但是加上施行細則 33 條後，其實也與 GDPR 本文的 11 章 99 條相差無幾，且尚未計入因規範事項散落各處所衍生的時間成本，通盤修正成本也並非想像地高。從絕對的角度，我國個資法的問題也可能只是不夠精準，若能只酌與文字修正，並透過分析新聞事件或裁罰案例，精準決定監理事項與方式，也使法遵資源分配能漸趨合理，也不失為有效的方案。即便如此，在複雜與簡單之間取捨仍為重要議題。

2. 在立法面與執行面兼籌並顧

法律只是政府所認為的理想狀態，還必須將實際執行的情況，以及可能遇到的困難通盤考慮。盤點與檢討立法與執行面之間的可能落差，使政府說一套，業者做一套的譏諷不致成為現實，也同等重要。

3. 缺乏評判的有效基準

光只是比較三種常見的監理模式還不夠，終究必須依照我國的系絡背景，研製評判各監理模式優劣的工具或基準，以便作為政策規劃或評估的參考，然而相關基準仍相對缺乏，而只能大致獲得「一樣米養百樣人」的空泛結論。缺乏這類基準，面臨外界可能的質疑，例如 GDPR 與數位廣告聯盟自律事項都強調對資訊安全的保護，又何以指稱數位廣告聯盟做得還不夠好？或又為何 GDPR 的作法必

須被奉為主臬？或其他類似問題時，政策規劃者便有可能在此常站不住腳，最後只能順著利益團體的要求浮沉，監理政策自然也缺乏意義。

第六節 問題盤點與可能改進策略

儘管現有文獻對於成功監理政策應達成的目標，以及應避免的後果提供了相對明確的指引，對於解答部份問題的幫助仍然有限。透過業者釋出的公開資料，以及整理相關法令規章，固然能對現有的監理策略與自律措施有相當認識。但是對於如何在實務面落地、相關產出為何，以及我們是否滿意相關成果，所知非常有限。也難說明所謂滿意的定義與標準到底為何。儘管監理社群網站利用數位足跡措施的緊急程度，無法直接與災病防救類比，但是不難發現民眾基於風險認知的差異，對於政府可能侵害私領域的行為，可能抱持不同的態度。再者，單憑比較前述三種主要監理模式，也不足以構成對於我國監理政策的完整建議。縱使我國法學研究者，可能對於現行個資法規內容嚴謹程度頗有微詞，然而即使是為了滿足歐盟跨境傳輸適足性的現實需求，應否就將 GDPR 的法例照單全收仍不無疑問。即使囊括 GDPR 的法例，是否就符合我國輿情的期待，也是另一個問題。問題也可能不是法令本身，而是我們也缺乏一套管考制度，評估現有監理機制究竟獲致什麼成效，使得後續探討監理政策的良窳也更難有頭緒。

即使成功立法，我國現有行政資源與執行方式，能否達成法律所預期的保護效果？法令只能大致界定容許業者利用數位足跡的範圍，而難以約束其細部行為。探討監理策略的問題意識，除了管制的內容外，也必須逐漸將探討管制的方式一併考慮在列。再者，即使在本文寫作當下，Facebook 已陸續推出透明措施，陸續揭露數位足跡的來源與利用方式，然而使用者能控制的程度仍然相對有限，且通常也是事後才得知（詳如本文第 31 頁之分析），且業者願意揭露的事項，通常也只是實情的微小部份。但是即使從現象觀察而言，我們認為業者似乎還做得不夠好，以及只會達到最低標準的自律，這些懷疑只能算是假設。管制者似乎也很難拿出一套說詞，證明業者哪裡做得還不夠，最後淪為各說各話。這也使得成效評估機制的研製與施行益加迫切。因此建議後續應聚焦於下列事項的研究：

一、欠缺有效的成效評估機制

鑑於資料管制政策造成的龐大社會成本，實行成效評估並落實課責機制，並為日後政策的修正或存廢提供依據實屬必要。好的評估機制必須回答以下問題：

1. 現行的相關監理法規本身，是否堪稱完善？從絕對的尺度而言，法令本身能否起到應有的保護效果？從相對的尺度而言，儘管與 GDPR 相比，我國個資法管制範圍與罰則皆偏弱，卻也難以據此定奪兩者之間的優劣。畢竟過於嚴格的法令，也可能扼殺創新或減少民眾選擇，也非社會所樂見。如何取捨也是一大重點。
2. 法規是否與如何落實：如何監理社群網站利用數位足跡的行為？相關人力、設備、與組織編制是否到位？例如社群網站的主管機關為何，是否有相應的管理能力？民眾除訴訟之外，還有哪些尋求救濟的途徑？即使業者屬行現有規範的各項環節，是否等同帶來更好的保護？也可能值得注意
3. 除了官方的執法紀錄之外，如何衡量的監理執行成效？除了民眾的滿意度之外，業者對於監理政策又如何回應。

目前對於監理政策良窳的推斷，仍建基在零碎且不甚穩固的研究基礎上。即使我們透過文獻，確知 GDPR 實施後業者追蹤瀏覽的傾向看來有增無減，但是就此斷定監理政策的成敗，似乎有欠公允。就像我們不能單以刑案數的增加便認為警察執法不力，單以現行政策的保護成效不甚滿意，斷定監理政策的失敗顯然過於草率，成效評估機制與流程卻也亟待建立。再者，問題可能也不是出在法律本身，也可能是執行者未能善用工具造成的事倍功半。且光憑對於現象的描述，顯然也不足以回答問題的可能原因。況且在台灣連可用來評估的相關實證資料也似乎付之闕如。

二、從「做什麼」提升至「怎麼做」

現存主要的他律型監理策略，多聚焦於要求業者應該做什麼事以達到法遵標準，並提高對使用者的保護。然而光是告訴業者應該做什麼，或只知道業者做了哪些努力顯然還不夠，還應該將問題意識提升至該「怎麼做」的層次，使監理政策方能確實落地。例如業者利用投放針對式廣告的議題，重點不是該作法應否禁止，而可能是使用哪些數位足跡或方法，社會較能接受？甚至我們對於業者做到了多少，似乎也不是很清楚。

三、檢討稽核資源的分配權重

資料保護政策固然要兼顧資訊安全、資料保護與隱私權等多重目標，稽核資源分配的權重顯然有檢討的空間。如今業者已逐漸轉型成為以獨占資訊的獲利模

式，顯然已有相當誘因建立資訊高牆防堵外洩的風險，此時便值得討論，是否還需要將那麼多稽核資源配置在察核如防火牆是否設置妥當這類事務上。此外也應以務實的角度，檢討制度設計與評估機制，及其的論理假設是否合理。陳敦源（2012：359-360）指出，課責機制的設計必須考慮到，資訊不是愈多愈好，而應兼具關鍵性、完整性與可理解性，且不能有死角，否則將成為舞弊的溫床，並引述 Cowen & Glazer（1996: 114）的比喻，考試只考一題比考十題還難準備，因為任何微小的失誤都可能招致零分，考生也必須兢兢業業。改為隨機抽查或可減少業者的僥倖心理，但是實際效果為何仍有待檢證。GDPR 的問題可能不只是條款的冗長，而是監理者被賦予的察核內容與程序缺乏隨機性，而未能以兼顧效率與經濟的方式完成稽核。

四、對使用者較有利的舉證責任分配

社群網站的現況，顯然未能起到足夠充份告知及公開透明，令廣大使用者充分知悉其運用數位足跡的機制，並接連導致嚴重弊害。使用者常可能懷疑自身數位足跡被用於不法途徑，卻難有跡證可供揭發，或令吹哨者陷於業者揚言提起訴訟之陰影下。因此筆者一再強調舉證責任分配（burden of proof）在制度設計的重要性，當使用者對於社群網站的作法有疑慮時，宜由舉證較容易（或成本較低）之社群網站來自證清白，所有監理（含自律）措施方能達致較佳之效果。

五、由政府以外行為者負責監理的可能性

文獻對於政府是否適合主導資料保護政策，意見仍然相當分歧。且綜觀我國國力與外交處境，不論是對內政府能力與社會對政府的信任程度，或對外的跨域執行皆備受質疑。若有更適合的行為者來擔綱資料保護的權責，甚至更好的治理方式，也應該列入考慮；但是可能借助的對象及搜尋方式為何，文獻似乎也未有明確指引，或可作為本研究努力的方向。



第三章 研究設計

經由一系列文獻檢閱，筆者認為欠缺有效的成效評估機制，以了解政策規劃與執行之間可能落差之成因，是目前探討監理策略較為嚴重的問題，缺乏足夠連實證資料，欲進一步提出評價也更形困難。為進一步釐清現有監理策略各環節的實施情形、過程可能遭遇的困難，以及衍生的後果，筆者擬進一步訪談相關重要人士，並綜合各方意見進行三角檢核，嘗試釐清事件的全貌並據此提出相對公允的評價。為上述訪談任務的預備與實施過程，為本章的主要內容。第一節將介紹研究架構的建立過程，盤點出欲評價監理政策，需優先回答的重點問題，以指引後續資料蒐集程序的規劃。第二節則決定研究方法、擬約訪對象及訪談大綱的建置，以及訪談流程的設定。

第一節 研究架構

本節聚焦於研究架構與藍圖之介紹，以指引後續的訪網設計與資料蒐集。本研究旨在找出政策規劃與執行之間可能的失落環節，主要聚焦於法令規範確立後，如何被主管機關執行與業者遵守、執行成果為何，以及如何反饋至現有的監理機制。若以監理政策過程先立法、後執行與評估的階段論邏輯來理解，現行監理策略的整體樣貌，可理解為各環節相互反饋所組成的迴路系統，以及內部各行動者之間的競合關係（圖 3-1）。

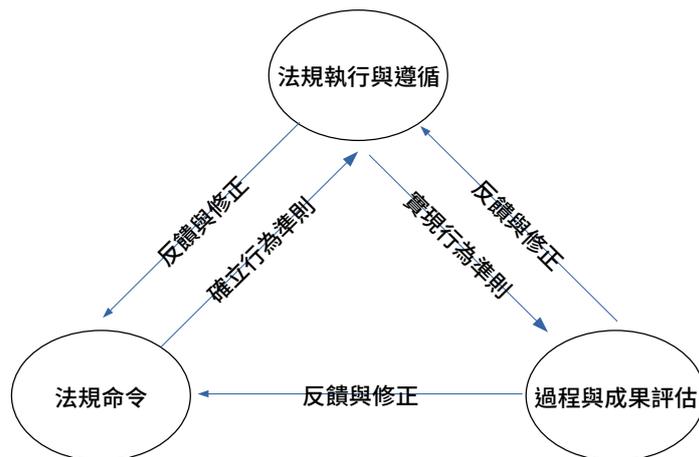


圖 3-1：監理策略的整體樣貌

資料來源：本研究繪製。

法令規範顧名思義，旨在建立一套遊戲規則與理想狀態，約束主管機關與業者的行為，也勢必衝擊業者利用資料拓展業務的計劃。法規制定完成後，仍需透過執行相關程序，才可能轉化成為可被察覺的成果。執行除主管機關的主動稽查，或被動接獲民眾檢舉與訴訟外，業者如何將法令規範轉譯於商務流程中，也是關鍵環節。執行與評估過程對於發現問題的回饋與修正，也會反映於執行端甚至衝擊立法實務。探討監理策略時必須特別留意的是，法規無法直接影響監理策略的結果，必須通過至少一個決策點，後續步驟才可能實現，這也是徒法不足以自行的重要原因。多組專業與立場各異的人員正確地分工也至關重要。法律無法直接影響監理策略的成果，後者卻可能直接影響立法過程，進而改變遊戲規則。

一、 法令規範

法令規範作為監理的基礎與描繪理想狀態，受民眾對政府的角色定位期待、國際法例所影響（圖 3-2）。法令規範除個資法以外，另有如民法對於非完全行為能力者的規定、主管機關函釋等。經由文獻檢閱，監理政策應達成的目標與應避免的問題應已大致釐清。鑑於民眾對於政府主導監理角色仍頗有疑慮，若有比政府更適合的人選，或除現有監理與自律之外更好的處理方式，授能或改變作法也可能是更好的方式。另一方面，政府若想發揮監理能力，也需要有健全的制度。文獻所點出的現狀，距離該理想顯然非常遙遠，但具體該怎麼修改方為適當？本研究對於法令規範的探討聚焦於：哪些人或治理手段可能比政府更適合擔綱監理的角色？以及如何修正現有監理策略的法制架構，以更有效地發揮功能？

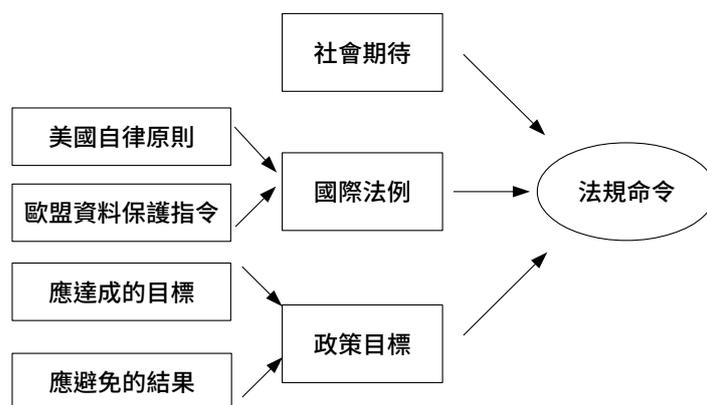


圖 3-2：監理策略法令規範的理想組成要素

資料來源：本研究繪製。

二、法規執行與遵循

對於執行的觀察重點，在於以動態的角度，審視監理的指令可能如何在主管機關與業者內部傳遞，以及可能發生的困難。本過程雖名為執行過程的審視，實則蘊含相當的評估成份。由於目前探討執行狀況的文獻，除國外零星對於 GDPR 的研究或報導，可說非常稀少。此處採取逆推法，並將主要角色分為政府與業者，並大致呈現拉拒的狀態（圖 3-3）²¹。業者行為分成推諉（shirking）、法遵與自律行為三種。常見的推諉行為有怠惰、遊說立法機構降低標準。法遵成本愈高、與相關安全技術的可行性愈低，也愈可能助長業者的推諉行為。社會期待以及公民團體的壓力，則可能促使業者自律，並抵消政府出手的壓力。政府的監理壓力，則可能促使業者採取較高層級的法遵措施。

目的事業主管機關如何落實執行細節，目前也存在許多未知地帶，是首要必須解答的問題。本研究假設，影響政府監理能力有兩大主要因素，分別是關鍵資源的供給，例如人力、物力（如經費）與組織支持，其中制度支持除了法律在消極面，不致有扯執行者後腿之規定外，也包含組織是否積極支持這件事，例如將資料保護業務排在任務中優先的順序。法律規定則主要指稱，執行業務程序中皆有清楚的指引，例如對專有名詞與主管機關的繫屬都有清楚的規定，執勤者也不至於迷惘。另一方面，受規範業者又如何將監理法規轉譯於企業實務，及遇到哪些困難尚似乎無跡可循，也同等重要。承接法令規範的討論，執法機關應在組織與資源配置如何改進，以有助於達成理想的監理效果？也是重要的問題。雖然此處探討的是主要監理策略的執行狀況，實則已蘊含過程評估的概念。

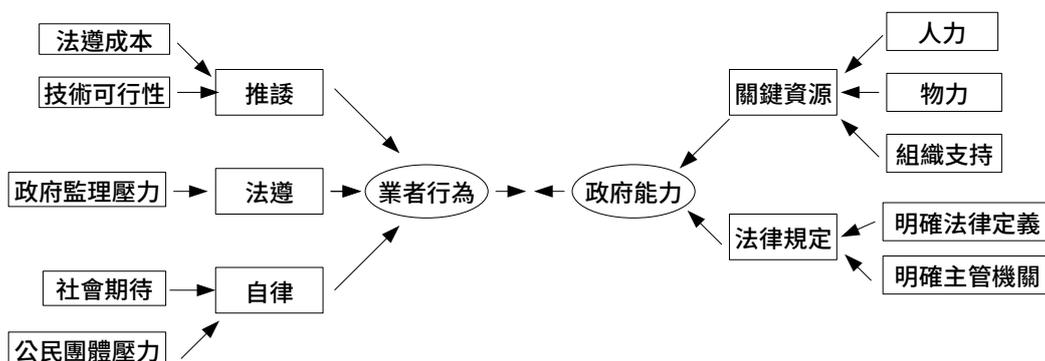


圖 3-3：理想的執行面各行為者組成與策略

資料來源：本研究繪製。

21 為讓表達更清晰，本圖文字後來做了一些修訂，故與訪談實際使用之題綱存在差異。

三、過程與成果評估

過程與成果評估，分別從靜態的視角，審視監理策略實施後的結果是否達成預期目標；及從動態的角度，探討上述結果及發現的問題，將如何反饋至監理策略的修正，進而影響執行的方式與法令。由於過程評估已經在執行與法遵的環節便開始進行，此處聚焦在成果評估的部份。

循著前述政策目標的脈絡加以審視，導引出第一組問題：現有監理政策究竟達成了多少前面提及的目標，如寡占市場下的使用者利益、杜絕欺罔行為等（及其他可能未竟事項），未達成的原因又可能為何？第二組問題則是，鑑於文獻已提及管制政策可能造成的弊害，現有監理政策能多大程度地避免這些後果？是否也有其他非預期後果出現？最後，這些問題也將協助進一步評價監理策略的良窳與可能的改進方式。

配合核心研究問題，本研究對於成果評估的探討，聚焦在「評估什麼」的討論：（1）目前政府的監理策略與業者的法遵行為，造成的結果是否與政策目標吻合，進而促進使用者的福祉？（2）這些監理策略造成哪些後果，不論是可預期或不可預期的？（3）可能改進的策略，以及這些發現的問題，應該如何回饋至今日的監理系統中。

第二節 研究方法

本節主要內容，係根據前節完成之藍圖與架構，進一步將訪綱設計、資料蒐集對象與程序等附諸實施。本節分為五大部份，第一部份為本研究將採用的半結構式訪談法之簡介，以及利用該方法的原因與目的。第二部份為根據上節之研究藍圖，進一步完善訪談大綱之題庫建構。第三部份是介紹訪談對象之遴選與訪談流程，將簡單介紹受訪者的基本背景，以及遴選之考量。第四部份則為根據上述受訪者的背景，客製與執行之訪談大綱之簡介。並以第五部份之檢討做為結尾。

一、半結構式訪談法

為進一步了解各行為者對於政府監理社群網站利用數位足跡策略之看法，以文獻分析的成果為基礎，透過半結構的深度訪談，可能獲得更為詳細的看法及相關建議。由於細部資料取得困難，對於業者或使用者採取參與觀察法基本上毫無可行性與時效性，且有抽樣的困難與觀察造成的干擾。透過立意抽樣訪談具代表性的專家，取得可能的替代來源，也可使資料能有相當的可信度。對於報章雜誌

執行文本分析，或可獲得零碎的專家意見或事實陳述，對於釐清支持或反對政府監理社群網站的理由，也可能有所助益；對於其他研究問題，特別是政府的監理策略獲致哪些成效，幫助則甚為有限。符合台灣系絡的資料少而零碎，且主流論述也多聚焦在假消息與仇恨言論的處理，難以進行有系統性地分析，是次級資料分析法在此最主要的限制。透過立意取樣與半結構訪談法，融合三角檢核精神追問專家意見等方式，可能是較能兼顧時效與資料信效度的解決方案。也可能事實上有公開存在的次級資料，但是需要熟知該領域的專家帶路，或協助轉譯成研究者較能理解的語言或模式，及指明某些專業的潛規則。例如我國個資法與 GDPR 的法條本身，與相關裁判均為公開資料，但是要從中找到關鍵的裁判案例，或訴訟實務中的「眉角」，仍需要相關從業人員的指引與協助方能知悉。

第二，在探討監理策略的良窳，研究者不只需要單純得到是或否、好或壞的答案，還需要綜合受訪者的背景、專業養成與受訪當下的情境等，以及透過適時的補充提問，了解受訪者可能的考量與理據，方能進一步做出結論。此時結構性的訪談或自填性問卷，可能便不甚合適。第三，在受限於時間與受訪者規模的情況下，研究者可能需要透過訪談一個較大與靈活的題目，透過事後推論等方式，嘗試處理問題清單中若干較為結構化的問題，也有必要保留較為寬鬆的提問與詮釋空間。綜此，半結構式訪談應為較有助於回答研究問題的研究方法。

二、訪談大綱之題庫建構

綜合第一節對於各監理環節的討論，表 3-1 整理出為評價現行監理策略，個別情境應優先回答的關鍵問題清單。依情境排序題組大致呈現金字塔型的結構，偏重實施成效既評估與改進策略的討論（對應研究問題二、三）。雖然法遵執行與遵循本質較接近政策執行的過程，題項設計實則已納入相當的成效評估。訪談大綱也將以本表之問題盤點結果為基礎進行設計。

考慮題項過多造成受訪者的負荷與影響回答意願，且在問題盤點過程中，難免已融入筆者的主觀意識，例如第 6 題「...造成的結果是否與政策目標吻合？」，該「政策目標」字眼係基於文獻檢閱所發現的各項贊成與反對監理的理由推論而得（詳見第二章第二節、第三節），若直接設為訪談問項，頗有預設立場與誘導之嫌疑，較好的提問方式可能改為較模糊的文字敘述，研究者事後再依據訪談結果自行判斷，監理結果可能與目標不符之處。因此訪綱之設計重點，為合併相似性質的題項，及改以較為模糊的文字敘述，並保留訪談過程之彈性。

表 3-1：評價現行監理策略的關鍵問題清單

研究問題	對應情境	問題概念	關鍵問題
問題一	法令規範	政府正當性	1. 哪些人或治理手段可能比政府更適合擔綱監理的角色？
問題一	執行與遵循	政府正當性	2. 如何修正現有監理策略的法制架構，以更有效地發揮功能？
問題二	執行與遵循	實施成效	3. 目前目的事業主管機關如何落實執行細節，及遇到哪些困難？
問題二	執行與遵循	實施成效	4. 受規範業者如何將監理法規轉譯於企業實務，及遇到哪些困難？
問題三	執行與遵循	改進策略	5. 執法機關應如何在組織與資源配置上改進？
問題二	執行與遵循	成效評估	6. 目前政府的監理策略與業者的法遵行為，造成的結果是否與政策目標吻合？
問題二	成果評估	成效評估	7. 這些監理策略造成哪些後果，不論是可預期或不可預期的？
問題二	成果評估	成效評估	8. 現有的監理策略好不好（或夠不夠好）？
問題二	成果評估	改進策略	9. 可能改進的策略？
問題二	成果評估	改進策略	10. 這些問題應該如何回饋至今日的監理系統中？

資料來源：本研究整理。

最後產生之訪談題綱題庫詳如表 3-2。依照研究問題所設定的順序排列，第一題是針對第一組研究問題，旨在解答在現有自律與監理架構之外，可能有哪些更好的治理模式，甚至比政府更適合的人選，使網際網路能維持較好的運作；此舉既在梳理現有的監理策略與目標設定，並反應在法令規範的環節探討。第二題與第三題則作為回答第二組研究問題預備題目，分別探討主管機關的執法及業者的法遵行為的整體過程，特別是企業如何將上述要求實現於內部作業流程與使用者介面設計中，以符合設計階段納入資料保護（data protection by design）的法制趨勢，並對於研析政府的監理策略已獲致哪些成效的後續問題奠定基礎。進而推行出（第四題）現有監理策略之得失，及（第五題）造成了哪些（未）預期的後果？而概念上屬於法令規範的，對於現有監理策略的法制架構的可能修正方向，由於問題性質與執行面組織與資源分配的檢討大致類似，被併入第六題處理。

按照原定計劃，是將表 3-2 作為類似題庫的方式，依照受訪者的性質擷取適合的訪談題目使用。然而實務操作配合時間限制及受訪者性質差異，以及研究後

期因為某些問題的累計回應推定已達理論飽和，或需深入探究特定問題的細節時，需要針對上述題目進行增刪，故實際呈現之題目，尤其是後期的受訪者，將可能與表 3-2 內容略有不同。為讀者查閱方便，也將訪談過程新增的題目增列至該表下緣。例如（序號）新增 1 係訪談開始前依照受訪者 C1 建議，先從事實層面詢問受訪者各自關心的業者利用數位足跡的行為，與對使用者可能造成的影響，再進一步詢問各受訪者對業者自律措施、法遵、政府監理措施等的看法，作者也對該建議表示謝忱。為求版面精簡，列表之新增題項僅以常用之為限。

表 3-2：訪談大綱題庫列表

訪談題項（序號）	對應環節
Q1. 您認為管理社群網站利用數位足跡的策略，除現有的自律與監理兩大模式之外，有哪些其他的角色或方式？	法令規範
Q2. 請問主管機關對於社群網站執行個人資料保護相關法令的狀況為何？遇到哪些困難？	執行
Q3. 請問社群網站業者如何將個人資料保護法的要求，融合於日常作業的實務中？遇到哪些困難？	執行
Q4. 您認為政府監理社群網站利用數位足跡的現有策略，做到了哪些事，還有哪些事還沒做到？	成果評估
Q5. 您認為個資保護的執行造成了哪些（未）預期的後果？	成果評估
Q6. 對於現有的個資使用監理架構，請問您認為還可以做哪些改進？	成果評估
新增 1. 您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？	無

資料來源：本研究整理。

三、訪談對象遴選與流程

訪談對象之遴選基準，主要依據各題項之性質，研判可能有能力回答的專家或從業人員，以及重要利害關係人，大致分為（A）公民團體（B）社群網站從業人員（C）政府主管機關（D）專家學者（E）使用者等五大類。對於現行監理法令有相當了解，也是成為受訪者的基本條件。原定訪問對象與順序如下：

由於欲探討監理策略良窳，必須先從事實層面了解業者實現法遵的情形，以及主管機關的監理執行，原擬邀訪社群網站業者（代碼 B）與政府主管機關人員（代碼 C）至少各二位，邀訪至少各兩位的用意是基於三角檢核的精神，避免可能的觀點局限與偏差（以下亦同）。然而考量 Facebook 的營運重心不在台灣，缺

乏具代表性的人員，被授權受訪的可能性也甚低，且能做出公關內容以外回應的機會也不高。最後以筆者所能及之人際網路內，熟悉相關實務的其他從業人員替補。實際訪談接受業者委任的律師2名（受訪者B1、B2），以及曾在國內性質相似同業人員1名（受訪者B3），計3名。其中受訪者B1、B2受訪時任職於某大型律師事務所；受訪者B3則曾於經營類似業務的某跨國企業任職多年，應能相當程度反應業者的觀點與立場，以半個局外人的身份也有助於維持中立，以及回應部份較為敏感的問題。

主管機關人員的約訪，以現行個資法主管機關為主，其中主管機關又可分為該法之解釋機關（現為國發會）及執行之目的事業主管機關（本例為經濟部工業局）。原計畫各邀訪至少一名，然而筆者經所能及及管道探尋，在經濟部工業局內無法找到合適現職對象，最終只約訪到國發會內某高階文官（受訪者C1）。然而代表使用者的受訪者E1表示曾於經濟部工業局任職，並允許將發言列入分析，故政府實際受訪人數雖然只有一名，研究者仍能大致了解兩個機關的執行概況。雖然按照原定計劃，政府機關擬排在較前面的約訪順序，然而筆者後來決定，先將各受訪者意見彙整後，再統一請教國發會人員的相關意見較為妥當，也兼具回饋政府單位的目的，故後來排定於較後面的順位。

為達到交互參照以降低來自官方說法的偏見，對於上述問題，原擬約訪熟悉社群網站運作現況及監理政策執行情形（下稱兩大領域）的公民團體（代碼A）至少各2位，即總共4位。然而實作後發現，筆者所能及範圍內符合上述條件的受訪者人數不足，且回應內容也無太大差異，推測接近理論飽和。故最終訪談公民團體人數共3位，分別為曾於某人權團體長期任職人員、某資訊公民團體委任律師與某資訊公民團體特約撰稿人。

由於使用者（代碼E）也是重要的利害關係人，本研究原定訪問至少兩位使用者代表。最後實際訪談一名個資外洩事件與電話詐騙得逞的受害者，並有向加害業者提出訴訟的經驗。由於筆者詢問該受訪者後得知，目前國內幾乎沒有與劍橋分析事件類似之受害者。考慮時間限制，且該受訪者意見與經歷應該已堪具代表性，故雖有無法做交互檢證之限制，但短期內只能先如此取捨，並列為研究限制之一。

最後委請專家學者（代碼D），依據前述各受訪者的回應內容，提出兼顧專業與立場平衡的洞察並做總結。由於考慮時間限制，且預期專家學者的身份應已

融合多個立場，及三角檢核精神，最後按原定計劃邀訪科技法律與傳播兩大專長，且具實務經驗的專家學者各一位。

綜上所述，原先擬定之訪談順序，為從業人員、主管機關（順序為1或2，下同）→公民團體、使用者（3或4）→專家學者（5），待受訪者約訪成功及名單確定後，也將綜合各別受訪者方便的時段，機動調整訪談的順序，以及視受訪者經驗與背景客製訪談題綱及使用的術語。實際執行情形因上述原因，與筆者想法的變動，而與原定計劃略有不同，茲簡述如下（及如表3-3所示）：

第一組受訪者雖然仍為從業人員（即兩位業者委任律師B1、B2），然而第二組開始順序便有所變動，主因為有些受訪者可透過筆者之人際網路約訪，為追求時效而優先進行，或配合其行程而造成延後。另一種情況則是，如原本筆者希望將主管機關（受訪者C1）排在較前面的順序，實際上也是優先聯繫並被同意約訪。但是該次聯繫後，筆者發現宜先完成其他訪談後，綜合所有受訪者意見再請受訪者C1做總結性的回應，並給予政府相關政策回饋較為妥適，政府單位又被安排在較後面的順位。這些原因造成實際受訪順序的變動與混亂，而特此敘明。

表 3-3：受訪者名單列表與順序

代號	所屬群體	身份性質	受訪順序	受訪日期
A1	公民團體	曾於資訊人權相關團體任職	3	2020/12/24
A2		資訊公民團體之委任律師	4	2021/01/15
A3		資訊公民團體之特約記者	9	2021/03/10
B1	從業人員	與業者合作的律師	1	2020/12/08
B2				
B3		相似同業之已離職人員	8	2021/03/08
C1	主管機關	熟悉監理政策執行情形	7	2021/02/08
D1	專家學者	出身於科技法律專業	5	2021/01/17
D2		熟悉我國通訊產業運作狀況	6	2021/02/03
E1	使用者	資料外洩事件受害者	2	2020/12/19

資料來源：本研究整理。

四、各受訪者實際訪談題綱

以下表格（表 3-4 至表 3-11），由左而右分別為對各受訪者使用的訪談題綱之實際序號、受訪者代碼-採用表 3-2 之題項與題幹。雖然以大型比較表（改採橫向頁面）的方式直接呈現可能較為簡潔。由於即使是在同一群組之受訪者，採用之題項順序、題幹內容與語氣皆可能有所不同，而造成呈現之困難與視覺上的紊亂，故筆者最終決定仍以多張表格（並維持縱向頁面）的方式呈現，也減少讀者翻閱時必須將文件轉向的困擾。

表 3-4 為對於公民團體（受訪者代碼 A1、A2）的訪綱題目列表，雖然兩者在不同時間受訪，由於筆者是在幾乎同一時間發出邀約，而採用同一訪綱。第一題是先從事實層面，先了解從公民團體相關人員的角度，對於業者可能利用數位足跡的方式，以及對使用者可能影響的認知為何。第二題是探尋業者執行自律措施與法遵的情況，以及可能遇到的困難。第三題是探討政府執行相關監理措施時，對於業者可能造成的影響與未預期後果。最後則是總結性的題目，建議現行監理策略能做何改進。

表 3-4：對於公民團體（代碼 A1、A2）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	A1、A2-新增 1	您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
2	A1、A2-Q3	您認為業者對此採取了哪些措施？這些措施足夠嗎？業者還應該做哪些事情，以減少民眾的恐懼或疑慮？
3	A1、A2-Q4、Q5	您觀察到政府機關採取了哪些措施？您對政府的作法滿意嗎？政府採取的措施是否造成了哪些（未預期）的後果？
4	A1、A2-Q6	您認為現行的監理策略，哪些地方還可能做得更好？

資料來源：本研究整理。

對於後續公民團體特約記者訪綱的設定（表 3-5）與表 3-4 內容類似。但是除題幹內容與語氣外，第三題問法也略有不同，如詢問對於政府監理策略的看法的同時，將原表 3-4 的第四題（監理策略如何做得更好）直接併入以避免冗餘。原本對政策的未預期後果在表 3-4 的問法（第 3 題），基於避免誘導的原則，給予受訪者較大的空間；然而筆者在多次訪談發現，受訪者無法清楚了解該題目的意思，而必須額外說明，第 5 次訪談完成後決定，後續受訪者直接以本研究最關心的問題之一，即管制政策是否加劇數位廣告相關產業的壟斷為題幹詢問之。²²

雖然受訪者 A3 時序上是較晚的受訪者，但是因為筆者的疏失，未將第一題題幹改為「您最關心社群網站…」，然而應不致嚴重影響原意的表達。在實際訪談過程中，筆者則對此補充說明，兩種途徑皆可以是受訪者論述的方向（詳見該篇逐字稿，受訪者 A3，行 59-60）。

表 3-5：對於公民團體（代碼 A3）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	A3-新增 1	您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
2	A3-Q3	您如何看待使用者對業者採取之資料保護措施的質疑？業者還應該做些什麼，方可能降低使用者疑慮？政府對此能提供業者哪些協助？
3	A3-Q4、Q6	政府在監理社群網站運用使用者數位足跡的過程中遭遇哪些困難？根本的原因可能有哪些？哪些地方還可能做得更好？
4	A3-Q5	有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？

資料來源：本研究整理。

22 唯訪綱成文與訪談當下，是以「網路廣告產業的集中化」來表達，而與（後續修正過的）正文用詞不同。故介紹訪綱時仍保留修正前的用詞，以下亦同。

表 3-6 為對於業者委任律師（代碼 B1、B2）的訪綱題目列表，兩位為同時受訪，並採用同樣的訪綱。與表 3-4 的情況類似，第一題是先從事實層面，先了解業者委任律師對於業者可能利用數位足跡的方式，以及對使用者可能影響的認知為何。第二題是探尋業者執行自律措施與法遵的情況，以及可能遇到的困難。第三題是探討政府執行相關監理措施時，對於業者可能造成的影響與未預期後果。最後則是總結性的題目，認為現行的監理策略能做何改進。

表 3-6：對於業者委任律師（代碼 B1、B2）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	B1、B2-新增 1	您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
2	B1、B2-Q3	據您所知，業者對於上述問題採取了哪些自律措施？又如何將個人資料保護相關法令的要求，融合於日常作業的實務中？遇到哪些困難？
3	B1、B2-Q5	您認為現行的監理策略造成了哪些未預期的後果，不論是對業者或民眾？
4	B1、B2-Q6	您認為現行的監理策略，哪些地方還可能做得更好？

資料來源：本研究整理。

表 3-7 為對於國內相似同業的訪綱題目列表，雖然同屬業者群組，然而隨訪問對象與時序較為後面，加上之前的受訪者的對於部份問題的回應也大致同質，因此改採不同的問法。後續產生的訪綱內容與語氣也與表 3-6 略有不同。第一題的內容從剛開始訪談較為廣泛的問法（「您認為…做什麼」），限縮成受訪者「最關心」哪些問題。第二題由於是直接問經營類似業務的平台業者，不再是委任律師，所以語氣也更直接與精準。第三題則詢問業者對於政府監理策略的看法，並將原表 3-6 的第四題（監理策略如何做得更好）直接併入以避免冗餘。原本第四題（政策的未預期後果）在表 3-6 的問法，基於避免誘導的原則，而給予受訪者較大的空間；然而筆者在多次訪談發現，受訪者無法清楚了解該題目的意思，且筆者必須額外說明。由於許多受訪者也表示沒辦法回答，第 5 次訪談完成後也決定只對業者與專家學者詢問該題目，並直接以本研究最關心的問題之一，即管制政策是否加劇數位廣告相關產業的壟斷為題幹詢問之。

表 3-7：對於國內相似同業（代碼 B3）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	B3-新增 1	您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？
2	B3-Q3	從同業的角度，您如何看待這些大型平台業者採取的自律與法遵措施？對於外界對於業者的質疑，您會如何看待與回應？政府對此能提供業者哪些協助？
3	B3-Q4、Q6	您如何看待政府監理社群網站運用使用者數位足跡的過程的措施？哪些地方還可能做得更好？
4	B3-Q5	有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？

資料來源：本研究整理。

表 3-8 為對於主管機關的訪綱題目列表。除第一題問法與其他受訪者大致相同外，其餘題目則以主管機關的性質加以重新設計。第二題除業者採取之措施之外，主要聚焦於以主管機關人員的角度，對於現行個資保護相關法令是否滿意。第三題則聚焦在對於許多受訪者所期待的個資保護專責機關的設立，主管機關的看法，以及可能對現行政府組織架構的衝擊等。最後則是政府在政策執行相關過程可能遭遇的困難。至於在其他訪綱常見之，管制政策是否加劇數位廣告相關產業的壟斷的相關問題，則因先前多次訪問受訪者後發現，連專家學者（D 組）也不一定有能力回答該題項，推論以受訪者 C1 之背景恐怕也難以回答，加上考慮時間限制故最終予以捨棄。

表 3-8：對於主管機關（代碼 C1）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	C1-新增 1	您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？這些問題如何影響個資保護的相關立法？
2	C1-Q3、Q4	您希望個資保護相關法令能達到哪些目標？您認為現行法令符合您的期望嗎？您對於目前社群網站所採取之資料保護措施看法為何？
3	C1-Q2、附加	許多人主張應設立個資法的專責主管機關。請問您對於這件事的想法為何？這可能會對政府的組織架構造成哪些影響？
4	C1-Q4、Q6	政府在監理社群網站運用使用者數位足跡的過程中還遭遇哪些困難？根本的原因可能有哪些？哪些地方還可能做得更好？

資料來源：本研究整理。

表 3-9 為對於科技法學者的訪綱題目列表。除第一題問法與其他受訪者大致相同。第二題主要聚焦法律學者於業者相關資料保護措施的看法，第三題除聚焦在以科技法學者的觀點，認為現有個資保護法令所應達成的目標外，另有對個資保護政策執行現況的看法。最後第四題則是聚焦在管制政策是否加劇數位廣告相關產業的壟斷的相關問題。

表 3-9：對於科技法學者（代碼 D1）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	D1-新增 1	您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？
2	D1-Q3	您對於目前社群網站所採取之資料保護措施看法為何？業者還應該做些什麼，方能降低使用者疑慮？
3	D1-Q2、Q4、Q6	您希望個資保護的相關法令能達到哪些目標，現狀符合您的期望嗎？您認為政府在監理社群網站運用使用者數位足跡的過程中遭遇哪些困難？哪些地方還可能做得更好？
4	D1-Q5	有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？

資料來源：本研究整理。

對於傳播學者的訪綱題目（表 3-10）雖與法律學者相似，但是法律學者主要偏向法律層面，然而傳播學者則是偏向業者與實務的觀點。第一題與第四題問法與其他受訪者大致相同。第二題主要聚焦於身為了解業界實務的傳播學者，如何看待使用者（包含其他受訪者）對於業者採取資料保護措施的質疑，以及政府所能扮演之角色。第三題則聚焦在從實務的觀點，政府執行個資保護相關政策遇到的困難。

表 3-10：對於傳播學者（代碼 D2）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	D2-新增 1	您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？
2	D2-Q3	您如何看待使用者對業者採取之資料保護措施的質疑？業者還應該做些什麼，方可能降低使用者疑慮？政府對此能提供業者哪些協助？
3	D2-Q2、Q4、Q6	政府在監理社群網站運用使用者數位足跡的過程中遭遇哪些困難？根本的原因可能有哪些？哪些地方還可能做得更好？
4	D2-Q5	有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？

資料來源：本研究整理。

表 3-11 為對於使用者兼個資洩密事件受害者的訪綱題目列表。第一題問法與其他受訪者大致相同。第二題主要聚焦在業者相關資料保護措施的看法，第三題除聚焦對個資保護政策執行現況的看法，也將政策未預期後果的問項併入政策執行的問項。由於受訪者 E1 在時序上較早受訪，最後第四題是採用較早期版本的訪綱，以認為現行監理策略能做何改進的總結性問項作結尾。

表 3-11：對於個資洩密事件受害者（代碼 E1）的訪綱題目列表

序號	受訪者代碼-衍生自表 3-2 題項	題幹
1	E1-新增 1	您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
2	E1-Q3	據您所知，業者對於上述問題採取了哪些自律措施？在法遵過程中做了哪些努力？您對於業者採取的行動感到滿意嗎？
3	E1-Q2、Q4、Q5	您觀察到政府機關採取了哪些措施？對此您感到滿意嗎？政府採取的措施是否造成了哪些（未預期）的後果？
4	E1-Q6	您認為現行的監理策略，哪些地方還可能做得更好？

資料來源：本研究整理。

五、小結

作為研究方法的介紹，本節簡述了訪談方法之選取、受訪者遴選過程與訪談大綱之建立。然而迫於時間與訪綱篇幅限制，原先出現在表 3-1 與表 3-2 題庫的，探尋政府以外的可能監理行為者的相關題項，最後未呈現在實際訪綱內，也未能對每位受訪者詢問，是為研究的一大限制。然而由於探討該問題的先決條件，是先詢問受訪者對於政府角色的相關態度，仍有機會透過受訪者的言談，揣摩其可能看法，但是可能面臨證據能力不足的問題。但是上述瑕疵，應不致嚴重影響對於監理策略的相關討論。



第四章 研究分析

為探討現行政府監理社群網站使用數位足跡之策略，及其可能的盲點與可資改進之處，本章將對訪談所得資料進行分析與整理。分析的流程如圖 4-1 所示，基本上是以外界是否滿意的二分法，來決定是否進行下一步的探討。例如若外界對於業者的自律行為大致滿意，也就沒有探討其他他律措施的必要，便逕至綜合討論結案；反之則探討不滿意原因，並逐步往業者法遵、政府監理措施的方向著手直至綜合討論。本章探討共分為五個階段：第一階段先從事實面進行問題界定，了解外界如何評價社群網站業者運用使用者數位足跡的手法與影響，以及對業者的訴求，這過程也將強調雙方對於某些問題的歧見（詳如第一節）。第二階段則檢視外界對於業者自律措施實行情況的評價，並指出外界不滿意的原因（詳如第二節，下同），並導引至第三階段對於業者法遵行為（詳如第三節），以及第四階段對於政府監理策略及成效的評價，特別是外界認為不足之處（詳如第四節）。最後則以綜合討論作為結尾（詳如第五節）。

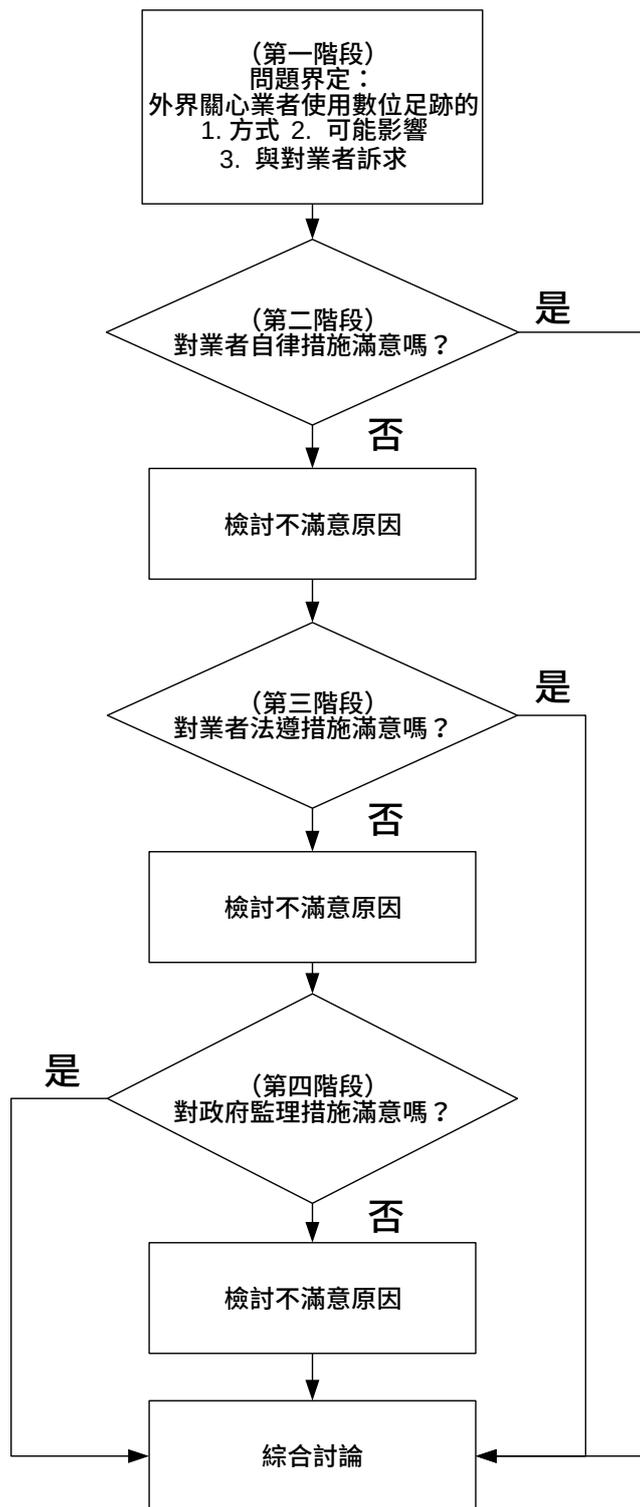


圖 4-1：資料分析流程簡圖

資料來源：本研究繪製。

第一節 外界對於業者運用數位足跡的行為評價

本節先從事實面進行問題界定，為了解外界對於社群網站業者運用數位足跡行為的相關評價，以及與業者之間可能的認知落差。本研究整理各受訪者關心的利用手法、較為擔心的對於使用者可能造成的影響，以及期待業者所能改善的事項如（如表 4-1、表 4-2、表 4-3），作為後續的討論基礎。

一、 外界主要關心的數位足跡利用手法

就事實層面的詮釋而言，儘管內涵與敘述深度略有差異，幾乎所有受訪者皆關注業者將使用者數位足跡用於精準行銷的傾向，部份受訪者雖未言明與針對式廣告的關係，但是從前引文獻與相關資訊常識推知，應不致嚴重偏離其範疇（受訪者 B1，行 115-118；受訪者 B2，行 122-129；受訪者 B3，行 190-199；受訪者 C1，449-450；受訪者 D1，158-188；受訪者 E1，行 230-233）。由於近來業者運用數位足跡所衍生的爭議，不論是 Facebook 的劍橋分析事件，或 LINE 一度要求使用者擴大運用其資料於行銷用途的授權，也與精準行銷或針對式廣告高度相關，受訪者一致對此表示關注也不難預期。雖然筆者在每次訪談開始前，為說明方便有提供論文計畫書給受訪者翻閱的習慣，然而考慮前述客觀因素，且受訪者翻閱時間有限，筆者認為該程序造成的誘導可能性甚低。而其他未言明關注何種用途的受訪者（受訪者 A2 與受訪者 D2），從其後續其他論述推知，與主流論述應不致有嚴重落差，而推定與精準行銷或針對式廣告衍生的問題大致類似。

就動機而言，業者委任律師傾向認為只是業者試圖讓效益極大化的慣常做法，廣告主想將每一分錢花在刀口上，平台業者則希望廣告版位能獲致最大收益，也是人之常情（受訪者 B1，行 115-118、受訪者 B2，行 122-129）；且呼應本文第二章第一節對於業者使用數位足跡可能機制的討論，雖然不排除將去識別化後資料轉賣的可能，但是業者不需要直接轉賣資料，媒合機制的加值服務就可能是收益來源（受訪者 B2，行 122-129），也很難就此證明會對使用者造成直接的危害。綜此也可推知業者傾向將論述限縮在事實層面，將精準行銷及其手段視為單純的商業運用，或者提升使用者體驗的工具。也不難想像 Facebook（2020c）對於影片《智能社會：進退兩難》（The Social Dilemma）的指摘，反應如此強烈。

然而外界似乎沒有如此輕描淡寫，有些受訪者關注的問題不只是業者的行為本身，還有背後的意涵及使用者感受。身為個資外洩事件受害者的受訪者 E1 表示，雖可預期業者會做網站內的行銷，但是「你怎麼可以不經過我同意，就單方面把這個資料拿到另外一個平台去使用呢？而且有的平台還是有跨境傳輸的問題耶。」（受訪者 E1，行 230-233）。雖然現行法規並未明文禁止這類跨網站的行銷（受訪者 D2，行 180-182），也預期業者對此也有一套說詞，強調這一切均在合法的基礎下進行，且使用者也同意了相關條款才使用該服務。但是綜觀使用者的意見與業者的可能回應，也難免感覺雙方仍處於各說各話。不過在現行法律架構下，完全契約自由的締約模式也不應再是常態，而應該重新以法律的角度審視條款內容是否合理（受訪者 D1，行 217-248）。受訪者 D1 與 A2 則強調決策黑箱的問題，其中較具爭議的為使用者在當下未清楚意識到正受自動化決策的影響，從抽象的業者與使用者之間的資訊與權力不對稱（受訪者 D1，行 185-193），到具體的可能造成歧視性的後果，也認為業者應該事先就揭露其可能性或事實（受訪者 A2，行 188-191、458-483）。即使如今自動化決策似乎已經成為常識，但那也是層出不窮的案例發生後，才終於逐漸為人周知。

表 4-1：外界主要關心業者運用數位足跡的手法

受訪者	主要關心手法
A1、A2、A3、B1、B3、C1、D1	投放針對式廣告與精準行銷
B2	提高廣告版位獲利率
B2	去識別化後資料的轉賣行為
D1	使用者與業者之間的資訊與權力落差
E1	跨網站行銷與跨境傳輸

資料來源：本研究整理。

二、對於使用者可能造成的影響

同樣是評論精準行銷及針對式廣告對於使用者的可能影響，不同受訪者提及關心的面向雖然分歧，但是大致不偏離主流論述。值得注意的是，受訪者的身份與關心的問題，並沒有發現明顯相關性，而難以斷定某類受訪者必定關心何種議題。未被提及也不必然表示該受訪者漠不關心，可能只是受訪當下想到的答案。

從微觀到巨觀排序，論述大致可分為四大類。第一類屬於對使用者體驗造成的不良影響，包含追蹤瀏覽可能造成使用者的不適感（受訪者 A1，行 220-223；

受訪者 B1，行 119-121；受訪者 C1，行 445-450）；以及對使用者隱私的侵害（受訪者 B3，行 190-199），還有使用者在不知情的情況下，被演算法推播的內容操弄情緒與認知（受訪者 A3，行 68-71）。廣告本身對於使用者體驗難免有負面影響，然而因為難以證明對使用者造成的直接危害，與其他問題相比也不嚴重，且受訪者對此也多只是一筆帶過，故為本研究所忽略；追蹤瀏覽可能造成的隱私侵害及情緒與行為操弄則是觀察的重點。第二類則是對使用者的個別自動化決策，可能造成的歧視或差別待遇，例如前述文獻所提及的差別取價等（受訪者 A2，行 454-456、行 459-481；受訪者 D1，行 344-361）。第三類則偏向資訊自主權，例如使用者能否清楚或控制數位足跡被蒐集內容的流向，及被用於跨網站甚至跨境行銷用途（受訪者 A3，行 66-68；受訪者 B2，行 130-132；受訪者 D1，行 364-370；受訪者 E1，行 240-245、行 712-717）。其中除了數位足跡的被利用本身，還有網站設下多少技術或使用者操作的障礙，令使用者無法便利地刪除被蒐集的資訊或選擇退出（受訪者 A3，行 75-81）。第四類屬於較為宏觀與政治性的，對於演算法控制使用者閱聽內容，造成的輿情極化或影響爭議訊息傳布路徑的疑慮（受訪者 A1，行 200-217；受訪者 C1，行 450-460；受訪者 D1，行 103-126）。這也是筆者寫作當下最為社會關注的議題，也使得爭議訊息傳布的控制成為各界優先處理的問題。

表 4-2：外界關注業者運用數位足跡的主要的影響

受訪者	類別	主要關心影響
A1、B1	一	對於追蹤瀏覽行為可能感到的不適
B3	一	對於使用者隱私的侵害
A3	一	不知情下被操弄情緒與認知
A2、D1	二	自動化決策可能造成的差別待遇
B2	三	資訊流向與用途不明確
A3、D1、E1	三	對使用者資訊自主權的侵害
A1、C1	四	可能造成的輿論極化
D1	四	影響爭議訊息的傳布

資料來源：本研究整理。

三、 外界對於業者的期許或訴求

外界對於業者的期許或訴求，固然為政府的監理策略重要的目標設定參考。雖然由於本論文的研究重點，主要在政府監理策略的實施狀況與初步成效，因此在訪談題綱設計之初，並未直接納入使用者對於業者的期待或訴求，然而透過分析或推論受訪者的回應，仍能歸納出數類形式。

第一類訴求偏向自動化決策機制的透明性，要求 Facebook 比照監察委員會（Oversight Board）的現有機制，²³將演算法或利用數位足跡的方式，供外界審視其公正性，或至少沒有用來做壞事（受訪者 A1，行 282-290；受訪者 D2，行 112-120）。受訪者 A2 則認為應該對個別使用者客製化資料使用報告，敘明使用了哪些類型的資料和基本用途（受訪者 A2，行 489-492）；但是也有相對溫和的選項是，業者不一定要揭露演算法，但需清楚對使用者陳明有差別定價的事實（受訪者 A2，行 459-481）。然而筆者認為受訪者 A2 的訴求可能稍嫌理想主義，首先演算法是重要的營利工具，業者當然不願意公開；即使強行要求公開，也與營業祕密法第 2 條所謂「合理保密措施」抵觸。受訪者 D2 雖未明言，但是態度傾向只讓第三方公正的專家來檢視（受訪者 D2，行 112-120），這實際上也大致是監察委員會目前的運作基調。受訪者 B3 認為，公開業者演算法不但可能造成服務品質的下降，也可能讓有心人士用於更惡劣之途，例如操縱搜尋結果排序（受訪者 B3，行 244-248）。然而也坦承因為業者不能把話說清楚，所以尤其在出事的時候，外界的質疑也就更大，造成惡性循環（受訪者 B3，行 250-252）。筆者認為消極地演算法鎖在暗處，也未必能禁絕其被用來為惡的可能性。雖然受訪者 B3 未明言，但是筆者推論其意見與受訪者 D2 相似，即頂多只將演算法對特定的專家揭露與讓其審視。

這些也顯示外界對於業者應該揭露使用數位足跡的實況到什麼程度，以及用什麼方式，意見不甚一致。若只採納受訪者 A2 所建議，陳明差別定價的事實的做法，在投放針對式廣告幾乎成為常識的現況下，筆者認為這恐怕形同什麼話都沒講，多數民眾恐怕也不會以此為滿足。對個別使用者提供客製化使用報告，看似對其最有利，但是在技術與法律上顯然皆不甚可行，且也可能給予有心人士透過類似逆向工程的方式操弄的機會。受訪者 A1 與受訪者 D2 建議仿照監察委員會

23 監察委員會是由 Facebook 以信託基金方式設立的獨立組織，負責審理爭議言論的存廢，並擁有推翻 Facebook 既有裁決的權力，相關新聞資料請見戴敏琪（2019）、陳文蔚（2020）。

的模式，或可兼顧保護營業秘密與專業課責的目的，這種務實的態度雖然違背民主社會的公開、透明等規範性價值，且可能招惹專家獨裁與替業主背書的指控，但也可能是短期內所能達到的最大公約數。不過筆者認為，業者還是有相當的餘裕能對使用者開誠佈公，也不應該將使用者對於演算法的無知做為掩藏的理由。

第二類訴求則是改變推播機制，避免集中於特定性向的廣告或貼文，減緩演算法的導引效果（受訪者 D2，行 127-133）。如塔吉特百貨發現預測懷孕的機制，可能會嚇跑敏感的顧客，因此在廣告內混入一些與懷孕無關，甚至可能互斥的商品以避免穿幫，既能讓顧客安心，也有助於提升營收，可謂兩全其美（杜希格，2012：230-231; Duhigg, 2013: 441-442）。此做法或許將大幅犧牲業者的短期營收，但是筆者認為有助於培育使用者較長期與穩定的信任，仍可能划得來。

第三類訴求則偏向讓使用者能更大程度控制資料的蒐集範圍與流向，如選擇只授權業者利用維持該服務所必須之資料，例如受訪者 D1 提到的，使用者可以只選擇「瘦肉」（必須或基本的服務）而不要「肥肉」（其他不必要的加值服務），或者類似受訪者 E1 所提到的，使用者可以只選擇「基本的套餐」（受訪者 D1，行 269-275、643-660；受訪者 E1，行 712-722），或協助使用者在法定權利的相關行使（受訪者 B2，行 383-386）。雖然這事實上也是 GDPR 等法制的其中一項要求，然而這勢必嚴重衝擊業者的營利機制，實務上也勢將面臨許多阻力，業者實際的達成程度也不甚一致，恐也難單靠業者的自律達成。

表 4-3：外界對於業者運用使用者數位足跡行為的主要期許與訴求

受訪者	類別	對業者的訴求或期待
A1、D2	一	讓商業模式也供外界審視
A2	二	主動揭露自動化決策可能的差別待遇
D2	二	平衡演算法的導引效果
B2	三	協助當事人權利的相關行使
D1、E1	三	能更大程度控制資料的蒐集範圍

資料來源：本研究整理。

四、 小結

本節從事實面進行問題界定，了解外界對於社群網站業者運用數位足跡行為的相關評價，以便進一步討論外界與業者之間可能的認知落差，以及後續的解決方案。雖然以上表格是整理自受訪者的發言逐字稿各處，受訪者也未言明所關心業者利用資料手法、對使用者可能造成影響，以及對業者的期許或訴求之間的關聯。但就常理推斷，筆者認為三者之間仍依稀存在一些關聯性。而業者的自律及法遵措施與政府的監理策略是否成功，某種程度上也能取決於業者是否能最大限度消弭上述對使用者的可能影響，或者符合外界之上述期許。

第二節 外界對於業者自律措施的評價

基於民主政治與市場經濟的運作原則，政府通常不直接干預企業事務，而儘可能讓業者在不違背法律的前提下自行處理問題。此時業者的自律措施是否能堅守空間底線，而能繼續享有自律的空間，也是探討監理策略時的第一個重要前提。本文共分成四個部份分述之：第一部份是業者採行自律的理論與實務基礎。第二部份則是業者自律措施的實際狀況。第三部份則為外界對於業者自律措施的批評。最後以小結做收尾。

一、 社群媒體的問題技術上只能透過自律處理

出於多種困難，受訪者 D2 認為社群媒體的問題，技術上只能透過自律處理。首先，我國政府現實上不可能前往境外執行稽核，頂多接下來提供足夠條件吸引對方將資料落地，然而社群網站業者對於台灣的經營環境並非十分信賴（受訪者 D2，行 83-91）。再者，我國也沒有法源授權進行相關演算法的監理，業者更沒有義務與政府分享相關資訊（受訪者 D2，行 100-107）。第三，由於演算法的多變與複雜性，政府也幾乎沒能力審視，唯一可行的辦法是仿照監察委員會的現有機制，委由公正的外部專家來稽核，然而該構想迄今尚未付諸實施（受訪者 D2，行 112-120、行 281-288）。

二、 業者的自律措施，多以遵循國際標準為主。

在缺乏外界稽查的情況下，業者委任律師表示，目前採取的自律措施，多以與國際標準接軌為主。業者通常會請管理顧問公司協助，去採用一些國際個資保護制度的標準來建立自律規範，例如常見的 BS 10012 標準，政府機關提供的指引

則非常有限（受訪者 B2，行 251-254）。然而業者具體如何遵循這些標準，因為業者未必會請教律師技術層面的問題，基本上等於無法知悉（受訪者 B1、B2，行 282-291），且這些事務的決策核心也多在境外，台灣方面也就更難有機會得知相關細節（受訪者 B2，行 255-268）。總體而言，究竟社群網站營運者採取的資料保護措施細節為何，業者委任律師僅能提供規範性的陳述，而缺乏更深入的細節。筆者即使有機會詢問業者內部人士，可能也只會得到類似其網站公關文件的罐頭式回應。

三、 外界對於業者自律行為的批評

由於瀏覽現有公關資料，與訪談業者委任律師後，對於業者自律措施的實施現況了解仍然有限，而多限於描述性的陳述。綜觀文獻與許多受訪者的回應，對於業者的自律措施也多有批評，其中最嚴厲的便是業者未能提出比法遵更高標準的自律而缺乏意義，茲具體分述如下：

（一） 業者未能提出比法遵更高標準的自律

首先也是最嚴重的問題是，業者未能提出比法遵更高標準的自律。受訪者 D1 認為，業者行為應該清楚凸顯自律與法遵的差異，且有意義的自律行為帶來的保護標準應該高過法律的要求，「要不然我們就依照法律，不就是有強制性的規範了嗎？」（受訪者 D1，行 668-675）。雖然筆者認為該說法略嫌理想主義，且忽略實際執法過程的成本與困難，但是也同意尤其是位居龍頭的業者，不應只以追求合法為滿足，而應以更高的基準來自我審視利用數位足跡的行為。從法遵的標準多半高於自律的實際現狀而言，以近來最為嚴重的劍橋分析事件為例，若業者連法律的要求都無法達成（未取得使用者知情同意，及違反安全港協議造成的欺罔行為），實在很難相信業者到底在自律措施做了哪些努力（受訪者 D1，行 714-720）。再者，若業者是在被政府邀請「喝咖啡」的情況下提出自律措施，由於其行動還算是出於其自由意志，尚且能稱作自律。然而當實情仍為「法律要求做一步，業者才開始做一步」（受訪者 D1，行 679-680）時，對外界而言也不過是另外一種形式的法遵而已；且 GDPR 剛好在與劍橋分析事件相近的時間點生效，也就更難認定 Facebook 提出的措施排除任何法遵的目的。第三，有意義的自律應該是基於未雨綢繆的超前佈署，且很多意外其實可能事前預防或至少有跡可循，例如查閱相關資料庫並對已知的風險投入預防（受訪者 E1，行 662-

665、669-673)。然而業者往往是在出事之後才急忙補破網（受訪者 E1，行 529-531、610-612），也當然稱不上是自律。

儘管 Facebook 聲稱已採取多項自我管制措施，實務上仍著重於控制來自使用者的爭議訊息的傳播，而未對業者端利用數位足跡的方式有根本的改善，而僅止於皮毛。儘管態度與立場有所不同，受訪者 A1 與 D2 不約而同地指出，既然 Facebook 成立了監察委員會，應可比照成立由外部專家組成的個資保護監查委員會，來稽核業者個資保護與內容推播演算法的實行狀況（受訪者 A1，行 282-290、受訪者 D2，行 112-120），如此也有助於消弭外界的質疑，以及對於業者與使用者的行為採取兩套標準的不良觀感。

（二）業者自律措施的可行性難以被外界信任

站在業者的角度，無非是希望政府不要有太多監理，但是業者應該清楚告訴外界，他的自律措施是如何施行的，政府也應該盡到把關的責任，確保業者提出的方案是具體的且能被落實（受訪者 E1，行 522-528）。且即使業者所出具的個人資料保護計畫確實合乎法規要求，也不保證業者就會落實，否則如劍橋分析這類違規事件也不應該接連發生。筆者認為，實務上業者除趨於制式的公關文章之外，幾乎沒有再透露具體的作業細節。迄今外界對於使用者的資料流向，以及可能的利用方式，也僅止於很籠統的「官方說法」，亦或只是透過外界如公民團體，透過旁敲側擊所得非常有限且不甚可靠的資訊。即使業者委任律師主張該坦承的事項，均已在使用者條款敘明，只是使用者往往認為太麻煩，而索性略過不看（受訪者 B2，行 355-357）。然而業者常用的使用者條款，受訪者與許多文獻皆已長期批評此為無效的溝通方式，但仍為業界主要採用的取得使用者同意的方式，也難免給人矇混過關的觀感（受訪者 A2，行 274-280）。

儘管業者委任律師對此表示感到為難。首先是現有技術，仍難有比制式的使用者條款更有效的溝通工具；再者，許多消費者也急於享受這些服務，經常不管三七二十一就點選同意了，而未能對後續可能的風險審慎評估（受訪者 B1，行 310-354）。受訪者 C1 對此也提出類似觀點，指出使用者在貪圖方便或一時找不到替代服務的情況下，也只能摸摸鼻子接受了（受訪者 C1，行 472-478），貪圖方便或許還能歸咎於使用者的享樂主義，但是如果使用者真的幾乎別無選擇，就可能要留意是否為業者壟斷，令使用者必須接受對業者較有利的合約。第三，在

合作廣告商頻繁更替的業界常態下，再告知義務的履行技術上有明顯困難，使用者是否也必須知道這麼多廣告商的細節，也不無疑問（受訪者 B2，行 373-377）。筆者雖然對於業者委任律師所提出的前兩點未有強烈辯駁，因為前者事實上似乎還沒有更好的溝通工具，後者姑且不論資料自主權與締約雙方權力不對等的問題，使用者是否詳閱條款，也與風險意識的培養高度相關，單方面怪罪業者也未必合乎情理。然而對於第三點則抱持較保留的態度，畢竟不能以廣告商頻繁更替，或一般使用者無需或無能力理解為由，片面剝奪使用者知的權力。不論是何種原因，倘若業者或使用者任一方，無法充份告知或知悉業者自律的技術細節，並相信該方案是具體且能落實，恐怕也難以說服外界自律行為的可行性。

（三） 單方面強調透明難以取信使用者

儘管社群網站已逐漸將透明視為重要的價值，然而單方面地強調透明，無法完全解決使用者的疑慮。透明不過是一種底線，單方面告訴使用者知道接下來該如何與業者相處，距離理想的溝通，或是使用者資訊自主權的實現顯然有相當大的差距（受訪者 A1，行 354-359）。業者要做的事不應該只是消極的透明，把該講的事情講完即拍拍屁股走人，也不應該將責任轉嫁給使用者，使用者也沒有義務為了使用一個服務，還必須事先了解專家可能也感到複雜的網站運作模式，遑論預防日後可能的糾紛；使用者知悉實情後也可能更害怕，特別是業者可能與政府分享特定機敏資料時（受訪者 A1，行 316-328、347-352、375-380；受訪者 E1，行 495-499、771-772）。若透明反而帶來使用者的不信任，業者應該從根本檢討有問題的商業模式，而非繼續將數位足跡無限上綱地用於他途。且若使用者數位足跡的利用方式，可能影響不實資訊的傳布方式與路徑（受訪者 A1，行 282-290；受訪者 D1，行 103-115），也就更應該執行相關的審查或監理機制。

（四） 對於自動化決策的後果難以被課責

由於業者無義務，通常也不願意揭露對使用者施行自動化決策的相關技術細節，特別是演算法。即使業者願意揭露，由於資料分析與相關實驗是動態且快速變遷的過程，且有多個研究正在進行，恐怕也很難精準回答，接下來可能會發生什麼事情（受訪者 A2，行 182-188）。但是若連業者都難以保證，使用的演算法等技術細節，是否可能對使用者造成不利的影響，特別是可能造成歧視性的後果等（受訪者 A2，行 188-191），也無法透過民間或第三方公正機關來協助審視

時，自動化決策的後果也將難以被課責，業者的自律措施也難以發揮應有的功效。

（五） 定型化契約的溝通的思維難以與主流法制相容

與業者合作的委任律師認為，業者其實已盡其所能，告知使用者利用個資之方式。然而個別使用者現實上缺乏時間與能力閱讀相關資料，日後有問題時才怪罪業者不應該這樣使用資料。站在業者委任律師的觀點，使用者似乎較理想的作法，也只能拒用不信任業者的服務，但是對使用者而言又知易行難，也導致後續不必要的紛擾（受訪者 B2，行 359-366）。雖然這不是直接出自業者的發言，但可預期與業者的立場大致相似。業者與使用者的溝通的思維，顯然仍以定型化契約的思維為主，使用者仍然是被框限在業者指定之選項內，而非完全出於其意願，被蒐集與利用其數位足跡。然而從事實面來看，即使是一般認為資料保護規定較為寬鬆的美國，其科技業主要群聚地加州，皆已經推出消費者隱私保護法案（CCPA），這類較為嚴格的個資保護基準（受訪者 D1，行 224-236）。儘管這事實不致直接影響現行使用者條約的有效性，然而締約方式也可能逐漸難與現行主流法制相容，況且現有契約趨近「瘦肉綁肥肉」的締約模式（締約時要求使用者同時授權使用非必要範圍的資料），也與現行法令的資料自主權等精神逐漸相悖（受訪者 D1，行 258-291）。這類以定型化契約與使用者溝通的實務，甚至實質上最終成為「你丟我撿」的主從地位關係，不僅難以滿足落實資訊自主權的法遵要求，也與自我管制中，讓業者基於道德意識，自主約束利用個資的原初精神存在諸多扞格，甚至反倒成為一面免死金牌，而有重新審視與調整之必要。儘管 GDPR 的實施之後，部份業者已逐漸調整徵求使用者同意的策略，例如在首次進入業者網站時，能在其 cookie 政策的說明頁，選擇允許使用 cookie 的範圍。或如 LINE 已經讓使用者勾選，不同意將其資料用於行銷用途。然而那通常是在政府單位表態之後帶來的改變，而非業者主動採取的策略。在多數情況下，業者似乎只是亦步亦趨相關法遵措施，而非提出比更高層次的自律。

四、 小結

綜合前述受訪者意見可知，雖然業者在其公關文件，屢次強調保護使用者隱私的重要性，宣傳其採取之自律措施也不遺餘力，然而也外界對此也多有批評。其批評的重點大致可歸納為，首先也是最明顯的，未能提出比法遵更高標準的措施，使自律缺乏意義；第二，業者缺乏具體與透明的實作過程，且在至少在應盡

之注意下，無法保證自動化決策，不會帶來嚴重後果的情況下，也就難以得到外界的普遍信任。第三則是自律措施仍無法脫離定型化契約溝通的思維，使用者仍然是被框限在業者指定之選項內，而非完全出於其意願，被蒐集與利用其數位足跡，而與現行主流法制的趨勢，以法律限制締約的範圍與內容有相當違背。在此情況下，也就難以令人相信單靠業者的自律，可能還是需要政府適時出面提醒，甚至執行相關監理措施，才有較大的機會維持對使用者友善的數位環境。

第三節 外界對於業者法遵措施的評價

綜合上述討論顯示，單憑業者的自我管制措施，似乎難以達到合宜的資料保護成效。即使業者自律措施實行成功，仍需要至少符合所在國的法律規範才能算數。觀察業者法遵措施的執行情況，也成為本研究另一焦點。以下將分成三個階段，第一步從規範面闡釋業者對於法遵的態度，第二步則從事實面描述業者對於法遵的實際作為，最後則是外界對於業者法遵措施的批評，並以小結做收尾。

一、業者對於法遵的態度

由於對業者而言，多一套法遵工序意味著更高的成本，業者也經常設法將法遵的工續與細節簡化以降低前述衝擊。儘管這可能是冒著投機取巧甚至舞弊的風險為之，但也不能就此斷定業者註定與監理者作對。歸納受訪者的意見，筆者初步得到兩個結論：首先，比起法規的嚴厲，業者更在意明確的遊戲規則，也儘可能不要反覆。第二，業者雖然儘可能與當地政府事先溝通相關法遵細節，儘可能消弭雙方歧見，並在能力範圍內遵守，然而當上述要求可能與企業的經營理念嚴重抵觸時，業者可能選擇寧可冒著放棄這個市場的風險，而拒絕落實相關法遵細節，以下將評述之。

（一） 比起法規的嚴厲，業者更在意明確的遊戲規則

一反常人認為業者總是遊說鬆綁法令的形象，業者委任律師（受訪者 B1）表示，儘管 8 年前對於個資法的修正有所批評，也一度認為荒謬，但是由於民間的資料保護意識逐漸提高，法務部及其後的國發會對於法遵意識的宣導、相關法令解釋也不遺餘力，如今也較能接受繁瑣的法遵要求（受訪者 B1，行 202-219）。比起法律的嚴格程度，業者其實更在乎的是可穩定遵循的遊戲規則：

（業者）他希望的是不管你怎麼改，你要告訴他他可以怎麼做，不可以怎麼做。他需要的是一個比較清楚的答案，而不是一個很概括的判

斷標準…反正你遊戲規則出來，我們就照著做。然後不要留下太多解釋空間。（受訪者 B1，行 178-181）

（二）業者的態度經常是基於懲罰規避的心理

長期在政府任職的受訪者 C1 觀察，業者的態度大致為只要政府不要裁罰，業者都願意對話，並儘可能做出相關調整。其派駐在台灣的公關人員，也願意不定期與政府人員聯繫，雖然經常只是願意將政府的相關請求，傳回在境外的母公司，而恕難給予立即與實質的承諾（受訪者 C1，行 407-417）。我們或可從上述觀察，大致發現業者的懲罰規避心理。畢竟對於業者而言，受罰兼有財務與商譽上的損失。且政府採取行動後雖然某種程度上鞏固了遊戲規則，例如 LINE 片面修改隱私權條款事件引起國發會的關切後，也間接確立了社群網站由經濟部工業局主管的大方向（受訪者 C1，行 355-359），這對業者來說也可能是好事，但是遊戲規則被寫死後，也可能讓後續業務推動缺乏彈性與緩衝，也未必是樂見的結局。然而政府倘若撕破臉，也可能傷害未來業者與政府合作的意願，可謂贏了面子卻輸了裡子，所以政府也不輕言使用該最後通牒。這推論也可能為接下來討論政府與社群網站業者之間的互動，提供一些指引或借鏡。

（三）業者對於擔負超過法律以外的責任仍有猶豫

雖然業者看似願意完全順服法遵的要求，對於擔負法律以外的責任則顯有猶豫。儘管業者委任律師觀察認為，業者處理使用者的資料也非常小心與尊重，對於法遵也願意完全做到現行的要求，甚至對於達標「有潔癖，就是一定要 100 分…好像沒有 60 分或 100 分的差別」，也少有投機取巧的心態（受訪者 B1，行 151-168）。但是對於本來不存在法律的要求，監理者自然也沒有立場要求多做什麼，否則就應該先修法（受訪者 B1，行 168-171）。從字面看來，受訪者偏向從法律的觀點與規避懲罰的心理去思考，主管機關不應在法律以外的部份再施以重擔，不然就應該修法並事先告訴業者新的遊戲規則。且以境外新創公司的思維，也較偏向法律沒明文禁止的事項，除非能從現有法令找到理據，主管機關也沒有權力阻止甚至裁罰（受訪者 D2，行 179-183、245-261；受訪者 E1，行 801-808）。然而筆者認為，誠然若希望業者做到法律以外的要求，應該回歸到自律的層面處理或詮釋，然而此說法也可能會對外界傳達，類似業者已經仁至義盡的觀感，但是筆者懷疑外界許多人可能不以此為滿足。又如先前討論，業者是否做

到了超出法律以外的要求，至少就筆者現有資料而言，顯然難以博取外界的普遍信賴，甚至可能實際上違法違都不一定能達到，也就更難進一步討論自律。

此外，如同對於自律的討論，對於業者如何在日常作業中落實法遵細節，因為業者未必會請教律師技術面的問題，業者委任律師也幾乎無法知悉（受訪者 B1、B2，行 282-291）。這也對於促進外界對於業者的信任幫助非常有限。

（四）業者落實法遵的其他條件

跨國業者進入新市場時，通常不會毫不遲疑地遵守當地的法遵要求，而需權衡與業者的經營理念可能的衝突、以及對使用者的衝擊等。受訪者 D2 觀察認為，美國的主要業者發展國外市場時，固然盡力以符合當地法律要求為優先，也儘量與當地政府溝通，以消弭雙方可能的歧見，不管是與使用者人權，或業者經營理念的衝突；然而若覺得遵守該國法律，有可能必須以傷害使用者的基本人權（如言論自由）為代價時，業者便可能寧可放棄這個市場。但是對於我國的經營環境具體存在哪些問題，受訪者表示不方便透露細節，只能含糊提到我國政府防治爭議訊息的方式令許多業者不滿（受訪者 D2，行 139-172）。

對此筆者固然能理解業者在執行法遵細節的諸多考慮，然而作為公共行政研究者的立場，由於法遵事務事涉國家主權的行使，難以因為業者單方面的要求或不滿，便輕易退讓或妥協。如果業者對於法遵造成的衝擊確實有所顧慮，宜公開指出具體問題出在哪裡，以供外界審視與思辯。然而現階段許多議題似乎仍流於封閉式的討論與各說各話，也與訴求公開透明的民主價值不甚相合。

另外一個爭議的可能來源，則是業者在跨國經營時，面對不同國家的法遵要求所發生的衝突。例如受訪者 B3 提到，某網路相簿業者來到亞洲某國拓展業務時，當地法務人員就曾就應該遵循色情認定標準較為寬鬆的美國模式，還是較為嚴格的德國模式發生激烈爭執。儘管出於對法務人員的方便，該網站一度採取德國模式審查相片，但也引起當地使用者捍衛言論自由的反彈，還一度成為公關危機，最後業者考慮該服務當地使用者甚少，採取美國模式尚稱無傷大雅而妥協，並對外宣稱這是技術錯誤（受訪者 B3，行 497-507）。儘管上述兩個案例較偏向內容治理，與本論文提到的數位足跡利用並無太大關係，但或可作為理解業者在法遵過程面臨兩難的線索。然而筆者認為由於業者對於數位足跡的利用，性質上偏向屬於業者的內部行為，或較大層面牽涉與廣告商的互動，要與使用者的基本

權益相提並論恐怕有點牽強。根本問題恐怕不是業者要採取哪一個駐在國的資料保護標準，而是業者在即使完全自律的情況下，又願意以多高的道德標準，來運用使用者的數位足跡。

二、 外界對於業者採取法遵措施的批評

對於社群網站法遵的相關的努力及事例，除了來自官方的公關報導外，目前尚難取得其他資料。儘管業者委任律師觀察認為，業者已盡其所能達到法遵的相關要求，然而外界對於業者採取法遵措施的批評顯然不絕於耳。其中最直接的原因，是業者早已違法在先，對於採取法遵事務的姿態也經常是消極與被動。外界也難以看到業者採取行動的相關細節，也就更難以證實其努力的可驗證性。以下將分段詳述之：

（一） 業者已有明顯違法案例

外界對於業者法遵努力首先也是最尖銳的批評，在於業者就已有明顯違法案例，例如劍橋分析事件最具爭議的地方，就是業者在未經使用者知情同意的情況下，將資料與第三方共享，以及隨之的欺罔行為，不論是受訪者 D1 引用英國衛報報導的「『欺騙』使用者能保有個人資料私密性的控制能力（“deceiving” users about their ability to keep personal information private）（Davies & Rushe, 2019）」（受訪者 D1，行 509-512、682-684、696-699、733-738、743-747），或曾在本文第 30 頁提及的符合安全港協議要求的不實聲稱。受訪者 D1 認為 Facebook 的問題可以分成兩部份來討論，其一是業者違法，主要在未經使用者知情同意的情況下，將資料與第三方共享；其二則是業者未必違法，但是資安防護不夠到位，導致外人可以輕易竊取其個資（受訪者 D1，行 714-756）。業者既然已違法在先，也就難以令人信服其在後續法遵事務上的努力與成效。

（二） 業者對於法遵事務的姿態經常是趨於消極與被動

業者對於法遵事務的姿態經常是趨於消極與被動，基本上都是政府介入甚至被處罰之後，才聲明要提出改善措施，而令人懷疑業者的誠意；也讓人認為業者只是出於一種規避懲罰的心態來推動法遵事務，而非從根本面去重新審視資料政策與安全防護是否到位，導致事件一再發生（受訪者 D1，行 722-728）。雖然身為資料外洩事故受害者的受訪者 E1，坦承劍橋分析事件之後，業者確實有做了補救措施，但也僅止於事後補洞，且對於既有的受害人補償可說是微乎其微（受訪

者 E1，行 603-608）。也認為業者不是沒有能力確實執行法遵要求，只是願意與否和做到什麼程度而已，畢竟將使用者數位足跡的用於商業途徑的潛在利益非常可觀，想必任何業者皆不願意輕言放棄這座金礦，「像 Facebook 好了，他們每一次出事，每一次那種因應措施，你覺得他事前都沒有能力做嗎？」（受訪者 E1，行 649-657）。

請讀者留意，接下來的論述攻防只是筆者擷取各受訪者的發言及立場，而非這些受訪者實際參與對話。受訪者 B3 以曾為同業人員的身份以及利用社會學的相關知識，提出另類的觀點。認為當矽谷的精英們在引入新的科技與制度的當下，發生這類副作用也在所難免，甚至也難以預期，例如設計社群網站相關系統的時候，也無法料想到爭議訊息會藉此快速流竄。又如受訪者 B3 談到劍橋分析事件時，認為 Facebook 的 API 設計從技術的角度來看，並沒有太大問題，也「從來沒有預設一個隨便你們濫用的立場，但它（API）就是被濫用了」，發現時往往傷害也已經造成（受訪者 B3，行 214-220）。受訪者 E1 則認為，即使業者不可能完全防堵所有資安威脅，很多意外仍可能事前預防或至少有跡可循，例如查閱相關風險資料庫並對已知的風險投入預防，而不能單以科技風險難以預判而加以推諉（受訪者 E1，行 661-668）。

但是這段攻防也不禁讓筆者思索，到底社群網站所面對的問題是未知還是已知的風險（詳如本文第 22 頁討論）。筆者詮釋認為，儘管受訪者 B3 否認 Facebook 存在技術上的資安漏洞，但是從管理的角度認為，矽谷的科技巨頭無法事前料想到爭議訊息的流竄，以及日後 API 被有心人士濫用，導致劍橋分析事件的爆發。隱含時下再完善的資安措施，也無法完全防堵人性的險惡與貪婪。劍橋分析事件的主要吹哨者布特妮·凱瑟（Brittany Kaiser）（2020：166）也坦承，當時公司也算準了多數使用者不會詳閱心理測驗應用程式的服務條款，在衝動趨使下便勾選了同意，該自白也或可作為佐證。換言之受訪者 B3 主張的應該是未知的風險，從這樣來看監理策略似乎應該採取較為嚴格的基準，以防堵日後可能的新破口，而這顯然非新興科技業者所樂見，但是倘若業者也無法清楚交代該如何防堵這些新風險，外界恐怕也難接受放任業者自律。然而受訪者 E1 則從資訊安全的角度，認為 Facebook 未善盡把關資安漏洞，導致有心人士趁虛而入。雖然受訪者 D1 未詳述細節，但也認為 Facebook 的資安並沒有做得很好，導致資料外洩事件頻傳。若採取受訪者 E1 的主張，則隱含認為這些風險其實是已知的風

險，政府應該用既有的監理方式處理即可，然而這與實情顯然也存在相當差距，問題也演變成業者的自律與法遵機制，甚至政府的監理機制究竟出了什麼問題，導致原本可能預防的資安事件一再發生。

雖然筆者並未完全同意上述兩位受訪者的觀點，不過偏向認為這些仍然是未知的風險。不管是將劍橋分析事件定性為黑天鵝²⁴，還是資訊管理機制的人謀不臧，都顯示我們難以從根本面預測與杜絕上述風險的存在，而建議後續的嚴加關注，下一個問題則是政府如何，以及是否已經準備好應對這個新趨勢。

三、小結

綜合前述受訪者意見，筆者認為與前文對於自律的相關批評類似，業者及相關人士不願或不便揭露更具體的法遵執行細節，而多只能概括或含糊的語言帶過。外界對於業者法遵執行的實際情形的了解，可能比自律措施還更少，也就更難以信任其可行性。

筆者從上述攻防的過程，似乎也觀察到社群網站的做法與態度和各受訪者訴求之間，存在的一些落差。首先，較偏向業者的論點，似乎習慣將管理爭議訊息或色情圖像的思維，套用在利用數位足跡的相關管控機制，面對不同國家的法遵要求，及基於對人權的保護等因素，能採取不同的標準。然而從人權團體與使用者的立場，即使未言明，但也可推知其認為業者對於數位足跡的利用，應該也要有同樣嚴格的基準，而不應將內容治理的作法照抄，畢竟內容治理與數位足跡利用，各自有迥異的性質與利害關係人。況且業者即使在規範較為寬鬆的國家（如美國），也已發生違法事例。第二，業者雖然主張以面對無法預知的新風險，認為資安漏洞所造成個資外洩的後果與傷害在所難免，卻不利在管制政策的論述攻防，因為主張面臨新的科技風險的同時，也就等於鼓勵政府對此採取比較強硬的管制行動。相對地，當使用者以資安事件為已知的風險而責難業者時，也構成論述上的矛盾，因為如果是面對已知的風險，要求政府強力施壓也不甚合理。雖然上述討論或許難產生立即的政策協助，但是或可使我們重新思索對此類問題的論述結構，何者較為合理，對於日後的監理策略實務的擘畫或許也有重要意涵。

最後，還有一個使用者可能在意的問題，則是業者在類似劍橋分析的事件發生之後，是否給予受害者合理的補償。由於國內尚難找到相關事例的受害者，故

24 該詞彙一般認為由作家 Nassim Nicholas Taleb 首創，泛指難以預測，但造成毀滅性後果的事件，詳見納西姆·尼可拉斯·塔雷伯（2011）。

該問題恐怕尚難獲得妥善處理，但是預期在境外也多以司法程序處理，來自業者主動的賠償機制恐怕也不多見。與一般消費糾紛相比，這類賠償機制的發展恐怕也相對不成熟，然而相關實務的發展，或可成為日後的一個研究重點。

第四節 政府監理策略的實施與相關議題

由於社群網站業者運用使用者數位足跡的行為，不論在自律或法遵措施的實施過程，表現皆難以獲致外界大致的滿意與信任，政府相關監理策略的介入，也將成為一道重要的防線。這也衍生兩個問題：第一，監理的執行狀況究竟為何？第二，外界對於政府監理策略的實施情況又為何？透過一系列訪談分析，筆者認為結果不甚樂觀。本節依序先指出可利用資料不足的現實，並指出各類法制面與實作面的缺陷，作為後繼者的研究參考。值得注意的是，儘管外界對於政府擔任監理的角色，並未表示明確的反對態度，但是對於政府執法能力與決心的質疑可謂不絕於耳，這也值得政策主事者留心。

一、關於評價監理實施現況的資料不足

筆者綜合受訪者意見後認為，探討監理策略的首要障礙為資料的缺乏，以及傳播效率的低落，外界也難以適時搜尋到必要的資訊。目前缺乏可清楚了解政府監理社群網站利用數位足跡的概況的資料，筆者甚至認為，相關資料的缺乏程度可能更甚於業者。業者做了什麼事即使稍嫌含糊，至少還有若干公關文件可供參詳。但是當問及受訪者政府的施政狀況時，回應的基調也常是未看到，或不知道政府做了什麼事等，甚至表示幾乎未感覺到政府有出手監理（受訪者 A1，行 487-498；受訪者 A3，行 714-721；受訪者 B1，行 475-477），連業者委任律師也表示似乎找不到公開的資料庫，以知悉歷屆的裁罰案例（受訪者 B1，行 492-494）。但是實情可能不是政府刻意隱瞞，而是對於大型業者迄今就是沒有裁罰案例，外界也就感受不到政府做了什麼事情。況且政府對於個資保護政策的後續規劃，也幾乎不是沒有就是還在起步。例如業者委任律師也表示，雖然知道主管機關正要蘊釀下一波個資法的修訂，但是一切幾乎還在紙上談兵，業者也還沒有機會加入討論（受訪者 B1，行 173-177、218-219），若連修法的狀況都不太明確，要談接下來的監理如何執行，也有明顯困難。

除了資料不足以外，也可能是資訊傳遞的效率不彰。除裁罰之外的行政措施及相關勸導，例如國發會介入 LINE 片面更改隱私權政策的過程，若非訪談相關

官員，外界恐怕也只能知悉很零碎的片段，遑論對其施政過程與績效做出評價。這些也導致欲探究政府監理社群網站運用數位足跡的實際狀況，處於資料不足的狀態，甚至可能認為政府敷衍。

如何提升政府在監理事務上的資訊傳播效率，可能是一個重要的議題，主要需借重在兩種角色與層面。首先是資訊傳播的協助者，例如以筆者與受訪者 C1 的訪談經驗而言，對方熱心提供了筆者許多監理過程的相關公文與新聞稿，並表示都是可公開查閱之資料。問題的關鍵，可能不是政府不願意提供這些事務的相關細節，而是缺乏有效的資訊彙集與傳播機制，或者類似受訪者 C1 的「領路人」，能協助相關研究人員將資訊以更有效率的形式傳遞。

然而第二個層面不但較為尷尬，且可能與前者論點存在相當抵觸，由於探討監理策略的時候，難免要談到行政（指）勸導甚至裁罰的相關議題，揭露這類紀錄對於業者往往甚不光彩，且可能造成業者與政府關係的緊張。儘管受訪者 C1 未言明，然而筆者揣摩其在 LINE 片面更改隱私權政策事件的態度（詳見受訪者 C1，行 317-385），推測政府在業者願意對話與改善的前提下，通常儘可能大事化小，小事化無，更不輕言威脅裁罰。儘管純屬筆者臆測，然而政府顯然有相當誘因，不管是基於產業推動的任務需求，或者純屬風險規避的考量，在合法的前提下也儘量不要張揚太多監理業者的執行細節，遑論出手裁罰與公開相關紀錄。這也可能是可得政府資料甚少的原因之一。

二、 外界對於政府角色的期待

儘管各受訪者對於政府對於監理社群網站使用數位足跡的議題，難免抱持迥異的態度或立場。甚至筆者一度懷疑，會否有受訪者以通訊監察侵害使用者隱私、或對言論自由的侵害等疑慮反對監理。然而筆者執行訪談迄今，似乎未見受訪者明確提出上述疑慮。即使筆者將通訊監察的疑慮詢問曾於人權團體任職的受訪者 A1，對方卻也回應對此詢問感到意外，甚至表示受訪當下未想到資料保護政策會和通訊監察扯上關係（受訪者 A1，533-534）。儘管還缺乏足夠證據，且證據能力也非常薄弱，但是筆者猜測在台灣，即使民間不完全對政府信任，但是對於言論自由與使用者隱私的保護，應不至於成為反對政府監理社群網站使用數位足跡的明顯理由。反倒是在政府任職的受訪者 C1 表示，仍然感受到相關指控與阻力的存在而不敢大意（受訪者 C1，行 564-567）。

即便如此，外界對於政府在此議題的角色，總體而言沒有抱持正面的期待。儘管角度與立場各異，主要的原因倒也不是原本筆者擔心的通訊監察及伴隨的傷害，而偏向對政府能力的質疑。受訪者 B3 作為曾經的同業人員，認為政府管得愈少愈好，首要的原因是政府通常必須以單一標準來對待所有業者，但是這會帶來許多不必要的 unfair，相關問題在本文第 23 頁，對於管制可能扭曲市場機制的討論也甚豐，也與後續對於廣告產業的壟斷現象的討論高度相關；受訪者 B3 也認為業者通常能獨立解決與使用者之間的爭端，實務上也少有案件嚴重到須對簿公堂，且基於行政資源的合理分配，政府只需扮演被動的角色（受訪者 B3，行 519-523）。受訪者 A2 也提出類似看法，認為現在的局勢，也還沒發展到亟須政府出手的地步，並認為社會規範（social norm）也將逐漸發揮較大的影響力（受訪者 A2，行 220-230）。對此，筆者承認其指出第一個關於公平的爭議，是監理過程中常見且嚴重的問題；但是以使用者的立場，並不完全同意其第二個論點，畢竟許多時候表面上使用者與業者沒有糾紛，實則可能只是由於對使用者而言，向業者申訴或發起訴訟的成本過高，造成使用者對於小事也多予隱忍。監理者顯然不應視若無睹，也不應樂見業者抱持這種苟且偷安的心態。筆者雖不明確反對受訪者 A2 的論點，但是認為坐等社會規範的形成，可能太過樂觀與天真，如同經濟學家凱因斯的名言：「長期而言，我們都死了（In the long run we are all dead.）」，社會規範的形成可能需要長達數年的時間，然而濫用使用者個資所造成的危害，則可能立即發生。也認為若非 GDPR 及類似法令的強勢施行，或其他裁罰的壓力（儘管這也可能有違市場期望），業者恐怕也不會立即改變其可能長期有害的利用使用者資料的方式。筆者認為至少在重大資料外洩事件發生時，政府的介入管制，可能還是有立即的需要，但也坦承長期而言可能需要更多討論與調整，才能逐漸達致社會接受的最大公約數。

另一方面，受訪者 A2、受訪者 B3、受訪者 D2 與受訪者 E1，則偏向認為政府缺乏能力做這些事情。受訪者 B3 表示，雖然政府因應數位轉型的能力，特別是在唐鳳上任之後，已經比以前好上很多，法令與組織結構整體仍然落後於今日趨勢，況且數位轉型也不可能單靠唐鳳即可成功（受訪者 B3，行 452-456）。又如從事實層面而言，以本例的目的事業主管機關經濟部工業局為例，該局處理既有產業推動業務已經自顧不暇，遑論新增的監理業務（受訪者 E1，行 954-962）。且政府在缺乏跨境執法能力的情況下，強行管制恐怕也只會傷到國內的

新創產業，對於解決問題幾乎沒有幫助（受訪者 A2，行 337-340、568-574）。何況政府也沒有足夠專業能力，處理目前飽受爭議的演算法的問題（受訪者 D2，行 112-115、行 285-289）。

雖然綜觀各受訪者的意見，應該不致完全否定政府在監理相關角色的正當性，但是不認為採取主動與強勢的「硬監理」會得到很好的收穫。隱含鼓勵將資源投注在被動或緩慢，但可能有長期效果的「軟監理」事務。例如資訊素養的教育（受訪者 A2，行 328-331；受訪者 A3，行 551-560；受訪者 B2，644-647）、建立有利本土資訊產業的發展環境，也有利資料落地（受訪者 A1，行 620-631）、或者鼓勵民間組織到國際舞台去發聲（受訪者 A2，行 332-338）等。然而筆者認為兩者仍不可偏廢，政府仍然須在必要的時刻，適時發揮維護市場秩序與使用者權益的職責。為確保該職責的遂行，政府也應先釐清自己的監理角色和限制，以下也將述及政府在監理社群網站運用數位足跡時所遭遇的問題。

三、 個資法的缺陷

由於完善的法令規範，是監理策略能妥善執行的主要前提。在正式談到行政組織本身的問題之前，應該先談談我國法令規範（主要為個資法）可能的缺陷。整理各受訪者的意見，發現個資法有下述缺陷：

首先，我國個資法第 2 條區分了公務機關與非公務機關，規定的疊床架屋徒增訓練與執行成本，比照 GDPR 的模式廢止此硬性區分的模式，或許是可以考慮的修法方向。第二，個資法第 20 條將「有利於當事人權益」，作為資料目的外利用合法條件之一，在字面上也啟人疑竇，擔心業者的濫用。第三，個資法只能說施加業者行為準則，在遵守一定遊戲規則的前提下取得使用者的同意，然而使用者面臨寡占或獨占的廠商，除了單方面同意業者利用資料的模式，似乎別無選擇，在此情形下結合反壟斷相關法令以制衡業者的想法也逐漸應運而生。

（一） 硬性區分公務機關與非公務機關的疊床架屋

呼應本文第 44 頁對於我國個資法的討論，我國個資法兼具條文精簡且遺漏許多重要原則，卻又在某些事項比 GDPR 嚴格的矛盾特性。其中在行政機關較棘手的，為個資法第 2 條分為公務機關和非公務機關，各自又有不同規定與原則，例如公務機關另有適用行政程序法與資通安全法的規定（受訪者 C1，行 769-774；受訪者 E1，行 1258-1263）。除徒增公務人員學習壓力與提高進入門檻以外，有

能力的應試者也可能選擇乾脆進入民間業界，以獲得得到較高的報酬或升遷機會（受訪者 E1，行 1258-1263）。第二個問題也與缺乏專責主管機關的議題類似，由於各個主管機關會因地制宜制定相關施行細則或辦法，不只影響法規執行的齊一性，對於業者的法遵業務也可能是一大困擾，甚至引來兩套標準的疑慮，儘管這問題可能尚未被普遍察覺，但也是長期必須解決的問題（受訪者 E1，行 1313-1318）。

（二） 「對當事人有利」目的外利用合法條件有濫用之虞

受訪者 E1 對於個資法第 20 條第 1 項規定「非公務機關對個人資料之利用…但有下列情形之一者，得為特定目的外之利用：」之第 7 款「有利於當事人權益」頗有疑慮，擔心業者會據此無限上綱地將使用者的資料用於行銷（受訪者 E1，行 348-351）。張陳弘、莊植寧（2019：106-107）對此亦有正當性過於薄弱之批評。對此受訪者 C1 表示，這一條本身並非當時法務部做的決定，而是立法委員誤以為個資法太嚴格，主張鬆綁所要求加的條文。不過也重申業者在實務上不能單以抽象的對當事人有利，就對使用者無限上綱地進行資料利用，而須就具體情況以及當事人的角度來認定，或至少當事人雖未明確同意，但預期願意接收相關行銷資訊。例如補習班在當事人主動詢問的情況下，將必要資訊提供給其合作的出版社。也表示雖然尚未在審判實務遇到有人挑戰該條款，但是也尚未見到有業者敢輕率地利用該條款，對使用者或消費者進行目的外利用，因為業者也擔心引起不必要的訴訟與賠償問題，基於保險起見，通常還是會乖乖地取得當事人同意，不過也坦承該條款可能會引起不必要的誤解，會列入後續修法時檢討的方向（受訪者 C1，行 737-789）。

（三） 單憑個資法的規定難以落實實質的保護

不論是我國個資法還是境外的 GDPR 等，所能做的最多只是確保業者在經過當事人明確同意的情況下，以及在業務範圍內對個人資料合理的使用。然而隨著數位廣告產業寡占的態勢日益明顯，使用者即使知道可能不好，能避免使用這些服務的機會卻也愈來愈少（受訪者 C1，行 472-478）。享樂主義心態的作祟，往往也會趨使使用者在未經思索的情況下，不管三七二十一就同意業者條款的予取予求（受訪者 B1，行 312-318）。即使業者確實依照個資保護法令的相關要求，取得使用者的同意，也未必是對使用者有利的結果。

對此數位受訪者意見、既有文獻與近期新聞，均指出主要國家除採用傳統的個資保護法令之外，反壟斷（或維持市場競爭）的相關立法與相關行政調查也正進行中，近期開始研究以反壟斷為由立法制衡業者的是法國與德國（另見 Graef et al., 2018; Robertson, 2019）。歐盟執委會（European Commission）也正在研究以兩個新的法制架構，分別為數位服務法與數位市場法，來因應此趨勢（受訪者 C1，行 526-561）。然而該會委員 Margrethe Vestager（2021）重申，數位市場法雖然與既有的競爭法互補，但其本質並非競爭法，也不與該法抵觸。更精確地說，有別於傳統的事後裁罰，數位市場法是以預先向優勢業者課與更嚴格的義務，來確保市場的公平競爭（國際瞭望，2021; G'sell, 2021）。然而仍不改變以政府力量介入市場運作的本質。近期美國聯邦貿易委員會也以 Facebook 大量併購競爭對手，以壯大其市場影響力為由，正在提出反托拉斯法的相關訴訟（鍾巧庭，2020）。我國步調雖然遠遠落後歐盟與美國，但是公平會已正在初步進行相關的研究，雖然僅止於資料蒐集的階段（受訪者 B1，行 496-501；受訪者 B2，行 627-630）。不論立論及方式如何，以個人資料保護與競爭法案雙管其下，限制業者利用數位足跡行為的監理趨勢，似乎已經逐漸成型。

四、政府監理社群網站的態度較為被動

法令的不甚完備，固然可能是監理策略效果不彰的原因之一，然而法律執行者的態度也非常關鍵。從歷次訪談結果似乎可歸納出以下結論：即使是在政府內部，對於要監理社群網站等大型網路業者，態度其實也不甚堅定。首先是核心業務受制於人的難言之隱，由於台灣政府大量仰賴國際業者協助推展事務（受訪者 D2，行 23-24），且產業推動與經濟發展，已經事實上成為主要績效指標，為鼓勵海外業者來台投資、設廠，政府也就不願意多方得罪（受訪者 A2，行 348-350；受訪者 E1，行 924-931）。受訪者 A1 更直指，由於政府大量運用這些平台蒐集輿情與推展公關業務，也等於默許這些業者這樣使用個資，也可說是共犯結構的一部份（受訪者 A1，行 508-513）。

第二，迫於政策資源必須花在刀口上的現實，政府必須優先處理可能有立即危害的問題，或優先應付外部壓力，如 GDPR 對我國業者的適足性認證要求（受訪者 E1，行 244-249）。又如近來爭議訊息的氾濫已廣為人知，且被認為會影響選舉，這也多少解釋為何我國政府在處理假新聞，會採取相對主動的姿態（受訪者 B1，行 104-105；受訪者 E1，行 862-864），而由於利用個資衍生的針對式廣

告，會影響爭議訊息的傳布路徑（受訪者 D1，行 103-109）又如近期傳聞美國資料仲介商 Equifax 資料外洩事故受到官方的注意，也是因為懷疑有中國人涉案，也擔心中國官方的滲透（受訪者 E1，行 873-883），這才使得個資保護的議題逐漸浮上檯面。但是對於資料保護議題本身，若非其引致的後果成功被納入公共政策議程，往往會在零星事件發生過後不久再度復歸沉寂。也難免招惹兩套標準，甚至認為政府推動資料保護政策主要是政治考量的指控。

第三，由於各主管機關的既有業務以推動產業發展為優先，附帶的監理任務的性質與手法，與既有業務難以相容，也演變成主管機關推動監理業務，真正的目的是帶動資安產業發展的奇特現象，也與監理的制衡精神違背，且組織在既有任務已經忙不過來的狀況下，也就更難期待會用心經營監理事務（受訪者 E1，行 924-1002）。且主管機關對於監理業務，基本上也抱著多一事不如少一事的態度，當各主管機關只願意（或其實也只能）各管各的時候，也就造成事權不集中，例如內政部只管公布多少來自 Facebook 的犯罪數據，至於主管機關要怎麼裁罰，那就不關我的事，監理自然就成效不彰（受訪者 E1，行 1217-1224）。這也能解釋何以許多受訪者主張必須設立獨立專責的個資保護主管機關。

五、政府缺乏人力與專業足以實行

政府通常也不是不願意落實個人資料保護的政策，但是現實上就是無力，也無暇處理這麼大量的個資。其中第一個明顯的問題，是連經濟部商業司，這個平常最頻繁執行電商監理的機關，本身都缺乏足夠的專業能力實施行政檢查，而是外包給資策會科法所（受訪者 E1，行 288-297）。經濟部工業局的狀況恐怕也相去不遠。趕鴨子上架，以及看誰比較倒楣來接任的分派模式，也使經驗與知識難以累積（受訪者 E1，行 1236-1238）。第二個問題便是欠缺科技執法能力，受訪者 E1 以偵辦詐騙集團為例指出，因為詐騙集團的斷點能力很好，現有司法系統通常只能抓到第一線的人頭帳戶（受訪者 E1，行 138-144）。倘若政府在偵辦犯罪行為都已經如此，面對新興的個資濫用事件顯然難有招架之力。

第二，即使是公部門，也難以落實個人資料保護法的相關程序與細節，對於資料保護的稽核也常流於形式，甚至索性將難以管理的個資銷毀或隱藏。受訪者 E1 表示，曾聽聞某機關因為缺乏人力落實個資盤點的必要細節，於是大家索性將保存的資料藏起來，或是乾脆銷毀；但是也緩頰道不是當事人想要敷衍了事，而

是個資的量實在太大了，現實上難以消化（受訪者 E1，行 940-953）。然而若政府無法以身作則落實轄內機關個資的保護，恐怕也難要求業者比照辦理。

六、 民眾缺乏有效的尋求救濟機制

除了政府主動查緝違規的業者之外，民眾的自力救濟，也是協助監理廣義商業網站運用使用者數位足跡的重要環節。然而現階段，台灣民眾似乎缺乏有效的尋求救濟機制。個資外洩的舉證困難，是其中一個顯而易見的問題，現行個資法罰則與求償上限過輕的問題，也早已為許多人所詬病。受訪者 E1 指出一個真實案例是，對於不肖廠商設置假網站，並在 Facebook 上買廣告的問題，因為受害者在政府單位到處求助無門，一度到國發會的公共政策網路參與平臺提案聯署「建請主管機關重視 FACEBOOK（臉書）購物詐騙一案，研議如何防制與作為，望請各界連署支持」，²⁵並成立同名 Facebook 粉絲團（受訪者 E1，行 21-31）。第二，民眾也難從主管機關要到業者導致個資外洩的違規證據，甚至需循政風途徑才有機會拿到，由於電子商務主要由經濟部商業司管轄，但是民眾若直接去問，大概只能得到官腔的回應，受訪者 E1 表示還是透過政風人員的協助，才能拿到比較詳盡的資料，並作為協助受害者打官司的依據（受訪者 E1，行 378-389）。若政府單位也無法協助民眾對於個資外洩事件進行自力救濟，也令人難以相信政府在監理社群網站運用使用者數位足跡時，能發揮足夠的效益。

七、 設立專責機關的相關課題

幾乎所有受訪者皆主張，我國應當比照歐盟，設立專責的個人資料保護機關。首先，成立專責主管機關，對於政策才有後續討論的基礎，否則依照政府運作的常規，每件事都可能由不同的機關負責，「你現在問任何一個問題，都可能立刻被打散成，不知道多少個問題再散出去」（受訪者 B1，行 423-432、568-569）。又如若要查詢各目的事業主管機關實施行政檢查權的情況，可能必須同時詢問多個主管機關（受訪者 A2，行 524-527），甚至有時可能還不知從哪裡問起。例如筆者雖然知道經濟部工業局是社群網站的個資法主管機關，但是透過管道詢問局內相關人員時，卻又不知道該詢問局內的哪一個組別。若連如筆者這種較常人熟知行政組織架構的研究者，都要查個老半天才知道主管機關以本例而言，可能是經濟部工業局，但至今仍然不太清楚是該局的哪一個部門。遑論較少與政府打交道的中小企業與民眾，甚至個資外洩事故的受害者？

25 相關網頁請見：<https://join.gov.tw/idea/detail/352b4277-dc75-498b-90ac-01e0e648aeff>

受訪者 B1 也舉出另一種極端，由於政府分工的高度分殊化，也造成若業者的服務內容涉及多個類別時，有問題時許多機關一擁而上，最後卻也沒有任何機關負全責的窘境（受訪者 B1，行 423-432）。這也可能引申為，業者有事時可能也不清楚該專注於哪一個對口，而延誤應變的黃金時間。第二，有了專責主管機關，事權才能集中，相關規範的實施也才不致各自為政與多重標準（受訪者 B1，行 420-423；受訪者 B2，行 571-573），也有利調查權的行使（受訪者 A1，行 696-707），對於違規事件的裁處也不至於各主管機關互踢皮球（受訪者 E1，行 1079-1099）。然而從行政組織的角度，難道設立專責機關就是最好的解法嗎？除了考慮如果所有事情都設立專責機關，可能導致行政組織員額無限膨脹之外，難道設立了專責機關，事權就能夠比較集中，監理的執行也就能比較不偏頗嗎？比較嚴謹的方式應該還是先了解在現行體制下，監理策略的實施的程序與原則，方能知悉兩種制度之間的優劣。下文也將討論這些議題：

（一） 在現行體制下監理策略的發動機制

儘管設立獨立專責的個資保護主管機關，已被許多受訪者認為是我國推動資料保護的當務之急。然而在進一步討論之前，仍需要先了解在現行體制下，監理策略的實施的程序與原則，方能知道專責機關是否就是最適合的做法。受訪者 C1 以國發會處理 LINE 片面更改隱私權政策事件為例，對現行監理策略的發動方式提供相關資料與說明：

監理政策發動的第一步，須先確定政府對此機關擁有管轄權（受訪者 C1，行 173-175）。雖然按我國個資法第 51 條規定：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」，然而法務部法律字第 10703502240 號函規定，在我國領域外利用我國人民個人資料的機關，必須同時符合（一）須為我國之公務機關及非公務機關為之、（二）所利用者為我國人民之個人資料，方適用該法之管轄（另見李世德，2018：74）。雖然受訪者 C1 表示，這部份肇因於該條文修正時的時空背景，由於當時幾乎不存在今日 GDPR 域外效力之概念，加上為避免個資法第 2 條所謂之管轄範圍，被無限上綱地適用出去，故有此被嚴重限縮的情形（受訪者 C1，行 140-143、行 159-166）。儘管筆者認為上述立法思維在目前時空背景下，確實可能有修正之必要。所幸在多數情況下，境外業者仍會在台灣派駐人員與設立機構（不論該形式為分公司或辦事處等），不論其工作內容為何，至少在國內有名目上的管轄標

的，由於 LINE、Facebook 和 Google 等皆在台灣設有上述機構，故仍適用於本法管轄（受訪者 C1，行 275-293）。

確定該案件與機關適用我國個資法管轄後，第二步則是確認繫屬的機關。而依行政院 103 年 5 月 28 日院台法字第 1030135223 號所附之會議決議，對於未有明確中央目的事業主管機關的資訊服務業者，由經濟部擔任個資法之中央目的事業主管機關。由於 LINE 不是第二類電信業者，故不屬於 NCC 管轄，在無明確主管機關的情況下，便劃歸經濟部管轄（受訪者 C1，行 190-201），其餘則是經濟部內如何分工的問題。經濟部工業局於 2016 年制定的「製造業及技術服務業個人資料檔案安全維護管理辦法」之附表，將資訊服務業（編號 631）涉及網路產業發展的部份劃歸工業局管轄，於是工業局成為 LINE 的個資法主管機關（另見受訪者 C1，250-271）。後來 LINE 的事件發生時，國發會也發佈新聞稿要求改善（另見國家發展委員會，2018），工業局也允諾會和 LINE 溝通這件事（受訪者 C1，356-359）。後來因為 LINE 也做出相關讓步與調整，風暴遂逐漸止息（受訪者 C1，384-385）。

由此可知，雖然台灣還沒有個資法的專責主管機關，但是行政院事實上仍有一套管轄權的認許機制，來支持個資法執行的相關運作。然而筆者認為該機制頗為複雜且缺乏效率，面臨科技產業快速變遷恐怕難以招架。且恐怕也難以應對單一議題可能有多個主管機關在主導的情形。

另外，儘管受訪者對於我國跨境監理這些大型平台業者，即使是像 Google 這類已在台灣設置資料中心者的能力多有質疑（受訪者 A1，行 561-578；受訪者 A2，行 214-218；受訪者 D2，行 82-86），然而綜合受訪者 C1 的意見，筆者卻認為有無跨境執法能力，反而可能不是那麼重要，主要是因為在業者願意與政府溝通的前提下，貿然使用強勢的手段來干預，反而可能造成反效果。受訪者 B3 也抱持類似看法，認為業者通常能獨立解決與使用者之間的爭端，實務上也少有案件嚴重到須對簿公堂，基於行政資源的合理分配，政府只需扮演被動的角色，而無須事必躬親（受訪者 B3，行 519-523）。不過必須留意的是，這可能是出於一廂情願的推論，倘若業者有一天強勢到缺乏溝通意願時，政府終將要面臨抉擇，是不惜冒著業者撤出台灣市場的風險，仍堅守法律底線？還是只能向業者低頭？另一方面，不論採取何種方法干預大型平台業者都有困難，長久之計應該是營造

有利發展本土資訊產業的市場環境，一方面是讓資料落地，也能杜絕廠商套牢（vendor lock-in）的風險（受訪者 A1，行 626-639）。

（二） 設立專責機關的課題

儘管設立個資法的專責機關，看似已成為日後台灣的趨勢。然而設立專責機關，仍可能面臨其他議題，其中有些可能也與政策的現狀相似：

首先，是我國法制類似歐盟的歷史基礎，可能導致引入其法制時發生水土不服的問題。受訪者 C1 引述相關研究指出，歐盟在 GDPR 設立專責個資主管機關，是因為歐盟為防止類似納粹德國，以蒐集個資的為工具進行種族清洗的悲劇重演，²⁶而在歷屆法制已有以專文保護個人資料的歷史背景，然而台灣尚缺乏類似的歷史脈絡（受訪者 C1，行 697-733）。這也多少可以解釋，即使在爭議訊息與選舉廣告的加溫下，為何個資保護在台灣社會，通常不會單獨成為矚目的議題。又如歐盟在設立專責機關時，慣用獨任制的委員（commissioner）或監察人（ombudsman）；然而在我國法制慣例與語境，仍慣用合議制的委員會（commission）（受訪者 C1，行 615-639）。若原封不動地引入歐盟制度，也勢將造成我國政府組織的無限膨脹。

第二，專責主管機關設立後，如何與既有監理機關合作？特別是在設立初期，有些已有明確且高度監理機關的業者。受訪者 C1 舉例例如銀行的監理業務向來是由金管會負責，日後銀行發生個資外洩事件時，專責主管機關與金管會的權限可能互相競合，兩機關的合作也將備受挑戰（受訪者 C1，行 667-673）。不難想見業者還是習慣聽從金管會，因為金管會還有銀行執照發放與廢止的權限。此時專責機關是否形同虛設，也不無疑問。這些事例也顯示，專責主管機關的成立，管轄權競合與跨組織合作的議題仍可能以其他形式存在，而需要在組織設計過程嚴加考慮。

第三，如何訓練與協助新的監理機關承接分管機關的既有業務，以及相關個資保護法規的執行等？例如學校的個資利用，大學以上是由教育部來監理，高中職以下則由當地教育局來負責，倘若全部都移交該專責機關執行，該專責機關恐

26 麥爾荀伯格（2015：183-184）也有類似案例：荷蘭是二戰前人口普查最為完整的國家之一，卻也為納粹入侵該國後的迫害惡行大開方便之門，結果當地猶太人受害的情況幾乎也是歐洲之最。

怕一時也難以招架（受訪者 C1，行 683-685）。同時該專責機關又需要多大的預算與員額，才足堪承擔前揭任務？

（三） 設立專責機關相關事務的近期發展

在本文接近截稿之時，行政院公布了增設數位發展部等一系列組織調整規劃。在此之前許多人可能認為，數位發展部是最接近個資保護專責事務的受命機關。然而筆者檢視行政院（2021）的新聞稿發現，該部組織設計對於資訊安全事務頗為重視，為此還新設了資通安全署與國家資通安全研究院，但是對於個人資料保護的事務則幾乎隻字未提。從國發會移轉的業務，也僅限智慧政府與開放資料，而不包含現由法制協調中心擔綱的個資法解釋的事務；反倒從經濟部移轉了許多資訊技術與產業發展的相關業務。這似乎也與受訪者 E1 認為，政府運作實況是推動產業發展優先於監理的觀點不謀而合。也隱含短期而言，個人資料保護應該也不是數位發展部的核心業務，既有的管轄權認許與監理執行機制也料將繼續存在並主導相當時間。雖然未有充份證據表明，現有的機制運作必然缺乏效率，上述趨勢與事實仍可能讓許多資料權利倡議者失望。

第五節 綜合討論

前文經由分析深度訪談資料，已依序將外界對於業者與政府相關事務的評價，大致做出系統性的整理，後續的討論則將聚焦於監理策略的相關得失。首先將總結業者的資料與政府在執行保護措施所遭遇的問題，在發現各界對於政府表現不甚滿意與缺乏期待的情況下，也將探討可能比政府更適合擔綱監理的角色。接下來也將探討監理策略，是否也助長目前頗為敏感的數位廣告產業壟斷的現象，並提醒未來公共政策須審慎應對。最後將探討現有監理措施可能還少了什麼，供日後政策改進的參考。

一、 業者的資料保護措施所遭遇的問題

業者不論是要採取自律或法遵措施，實施在利用使用者數位足跡過程的相關保護，基本要求便是符合當地的法律標準。然而外界對於業者能否達到此標準，特別是在劍橋分析事件的爆發後，顯然多有懷疑。儘管業者的委任律師評論指出，業者在檯面下有厲行相關保護措施，筆者則認為業者發佈的公關文件或新聞稿，對於相關事務的記載，仍多屬於價值性的論述，或對於前端使用者介面的相關改進，但是對於外界真正在意的後端資料管理相關細節敘述甚少，也自然難以

獲致外界的普遍信任。以公關運作的常識而言，在發生重大事件時，外界若無法從官方途徑得到滿意的回應，便可能轉而尋求各種替代的資訊來源，其中可能也不乏小道消息或競爭對手的中傷，也可能讓爭議訊息的傳布更難被控制。業者如何在前者與營業祕密的保守之間取得平衡，也一直是公關人員面對的難題。

近期業者已陸續出版相關透明度報告，如 Facebook 近期出版的透明報告，已簡單列舉 2020 年上半年被各國政府要求存取使用者資料的統計資訊 (Sonderby, 2020)，迫於市場與輿論壓力，特別是對於提供使用者資料予政府的相關疑慮，應該是業者出版相關文件的主要驅力。筆者認為比起政府的幾乎默然不語，業者的努力堪稱嘉許，但是也引發業者是否應該進一步，對個別使用者出版客製化的資料利用透明報告的討論 (另見受訪者 A2，行 490-492)，此舉也勢必觸及業者營業祕密的禁臠，後續發展仍有待關注。另一方面，隨著第三方追蹤瀏覽技術近期逐漸遭遇法律面與技術面的攔阻，業者利用使用者數位足跡的方式，料將出現頗大的變化，相關衝擊也將於本節第三點詳述。

另一方面，隨著歐盟隱私及電子通訊指令 (2002 Privacy and Electronic Communications Directive，簡稱 ePrivacy Directive) 將擴張適用於更多通訊服務的監理，Facebook 對於歐洲的服務也相應做出隱私調整與服務內容的限縮 (胡雅筑, 2021; Salla, 2020)。²⁷這可能解釋為，因為更高的隱私權基準要求，歐盟使用者必須犧牲部份享受創新服務的機會；然而對於非歐盟居民而言，也可能造成隱私權保護上的差別待遇，也呼應本文第 41 頁起對於 GDPR 實施成效的討論，及留意相關趨勢的形成。使用者與業界的後續反應，也可能是日後的觀察重點。

二、政府在監理過程所遭遇的問題

對於政府而言，探討監理社群網站運用數位足跡的策略，首先也最為嚴重的問題，是關於政府監理現況的可利用資料不足，不是幾乎沒有資料就是散落各處，研究者也難以繼續對監理執行情況，乃至於後期的成效評估做出評價。從公共行政學理的角度，這也可能造成施政缺乏可課責性，進而造成信譽的嚴重損害。且若重要的監理細節只有熟知內情的人士可取得，可能對新創業者是一大進入障礙，也與政府的透明價值不相稱。再者，倘若大型網路業者已陸續出版透明度報告，主管機關也應該以身作則，主動將相關事例及內容，公開予外界審視。

27 Salla (2020) 指涉的 ePrivacy Directive 事實上已有修正版，目前官方發布的最新版為 2009 年的 Directive 2009/136/EC。

況且外界若對於政府監理業者的行為，可能與通訊監察、侵害言論自由等問題掛鉤等真有疑慮，加速施政內容的公開透明將更為迫切。

第二，外界對於政府監理策略的質疑，有別於筆者的預想，主要並非對於使用者相關權益侵害的疑慮，而為主管機關缺乏足夠知能與資源與大型科技業者交手，甚至被玩弄於鼓掌心而不自知。儘管我國政府的數位能力從國際尺度看來，還算表現不俗，然而許多科技研究計畫必須委外的實情也表示，政府的獨立研發能量明顯不足（許淑梅，2020），外界的質疑也就不難理解。筆者擔心從公共政策的學理角度擔心，政府若不嚴肅以對，後果輕則為低估特別是跨境監理的技術難題，對業者也抱持不切實際的期待，雖然筆者與受訪者 C1 訪談後，認為國發會主責的事務官對此態度尚稱務實，然而這難以類推其他機關的立場或態度，特別是擔心政務人員在民意壓力趨使下，強行通過窒礙難行的法案或施政計劃而貽笑大方。重則為在不熟悉產業現況下強行推動政策，最後不但未能達到監理的目的，還反倒傷害國內其他新創產業。不過從短期來看，倘若受訪者 E1 在工業局之服務經驗為真，目前執行機關所面臨的最大問題，反而是推動自身既有業務都已分身乏術，論及監理可能造成的上述非預期後果，恐怕還言之過早。但這也更令人懷疑，政府現在連基本的監理業務的規劃與推動，都可能具有明顯困難。

第三，儘管許多受訪者認為，比照歐盟制度設立個資保護專責主管機關是解決現有監理策略發生的各項問題，如事權不集中、使用者求助無門、業者找不到政府對口等的良方。從使用者與業者的角度，此舉或許能省去許多繞歪路的困擾。但又如受訪者 C1 所言從組織設計的角度，即使順利成立，相關人力配置、任務的重分配及與既有目的事業主管機關的磨合，也勢將成為一大挑戰。筆者認為，使用者與業者真正在乎的，其實是能在龐雜的政府機構群中，找到適當的對口並獲取協助，成立專責主管機關是否最好，恐怕還需更多研究方能定奪。

此外筆者也認為，個資保護也應從政府的組織文化改革著手，特別是對效率的討論凌駕相關資安、倫理議題的積習。如受訪者 C1 引述相關研究，歐盟成立專責機關是立基於獨特的歷史背景，特別是對於納粹大屠殺悲劇的反省。雖然台灣也有類似的政治事件，但其性質與政府運用個資為惡的細緻程度，與前者仍有相當差距。筆者懷疑不論是政府或民間與歐盟相比，對於個資保護的重要性恐怕仍缺乏深切認識。在日常生活中筆者不難發現，業者常採取鼓勵民眾以填寫個資換取小禮物或優惠的行銷手法，但是當事人對於個資日後流向與可能後果恐怕也

缺乏認識（另見受訪者 B1，行 223-226；受訪者 B2，行 644-647）。政府或公營事業的做法，也經常如出一轍。例如 2019 年 7 月起，大台北地區的公車實行乘客上下車刷卡，否則將無法享有轉乘優惠的新政策，相關論述主要聚焦在該政策實施後的潛在效益，特別是精準利用運能以獲致效率與經濟（許鈺屏，2020）。雖然筆者不否認相關工具性效益的重要性，但是認為對此舉可能衍生的，對乘客動向精準追蹤、設置轉乘優惠的享受門檻衍生的資料貨幣化，甚至用於資料聚合等倫理議題顯然未充份討論。

又如公務人員長期習慣用 LINE 辦公，長官也常以此指派工作，還一度引起變相加班的疑慮（邱瓊玉，2016；陳素玲，2016）。姑且不論 LINE 是否實際存在資安的漏洞，或近期傳出工程師涉嫌濫用權限，多次瀏覽使用者個資的醜聞（2021 年 3 月 18 日，經濟日報 A8 版），或因貪圖方便而使用私人帳號辦公的疑慮。大量公務資料透過境外業者管理的網路節點流通，從國防的角度而言顯然不甚妥適。但是筆者質疑公部門對此仍少有檢討，也多聚焦在勞動權益的相關問題。加上筆者觀察過去政府處理數位身份證爭議的態度，雖然最後是在民意反彈與新竹市暫緩試辦下，由時任行政院長蘇貞昌宣佈暫緩（賴于榛、鄭煒，2021；陳熙文、劉宛琳、鄭煒，2021；黃瑞典、徐偉真，2020），但是由此推斷政府若必須在行政效率與資料保護之中抉擇，恐怕還是會選擇前者。這樣看來即使有專責機關，筆者猜測其在行政組織也終將淪為橡皮圖章，更別提有足夠的員額或預算，其權責也無法正確運作於日常的行政實務中，任何努力也終將淪為徒然。正本清源，筆者認為政府應該先檢討旗下組織使用民眾資料的態度與思維，若連政府自己對於資料使用的內部控制機制都不甚完善，實在很難要求業者比照辦理，也更難啟齒要對資料保護與相關監理機制做進一步變革。

三、可能比政府更適合的監理行為者

儘管受訪者對於政府作為目前事實上的主要監理者，未普遍表達明確的反對立場，但是對於政府是否有足夠能力進行違規偵察，以及面對複雜的跨境監理議題，幾乎都持以非常悲觀的態度。下一個問題則是，是否可能有比政府更適合的監理行為者，能擔綱這艱鉅的任務？

雖然因為這問題並未出現在訪綱中，除非筆者訪談當下有追問，否則便只能藉由分析受訪者的言談來推測其可能的想法。然而歸納出幾種可能的模式或角

度。受訪者 A2 雖未明言要讓民間組織取代政府的角色，但是認為台灣政府的能力有限，也幾乎不可能是規則制定者，反而民間組織有機會與國際串聯，間接影響科技巨擘的決策（受訪者 A2，行 331-337）。不過筆者以自身學術背景與實務觀察而言，對此抱持相對悲觀的立場，主要的原因是非營利組織普遍缺乏可靠與獨立的財源，即使能抗拒利誘堅守政策立場，仍可能不敵接下來可能與科技巨擘攻防的資源消耗戰而終究失敗。且筆者寫作當下正逢新冠肺炎疫情的高峰，在民眾普遍擱節非必要支出的情況下，非營利組織的財務處境恐怕只會更加艱難。受訪者 D2 則基於政府缺乏專業能力的現實，建議 Facebook 應該比照現有監察委員會的模式，委由公正的外部專家來稽核，然而該構想迄今尚未付諸實施（受訪者 D2，行 112-120、行 285-288），筆者也懷疑其在短期內的技術可行性，且除了何謂公正專家的潛在爭議以外，也可能衍生專家獨裁的弊端。

正當本文寫作邁入尾聲時，科技業也發生戲劇性的轉變，Apple 與 Google 相繼推出更嚴厲的資料保護政策。²⁸Apple 於 2020 年 9 月宣佈「隱私標籤」計劃，要求應用程式開發者以更簡明的方式，敘明對使用者個資的利用方式，以及遵守更嚴格的隱私權準則（林奕榮，2020）。Facebook 也大動作回擊，在美國主要報紙刊登巨幅廣告，指控 Apple 影響廣告投放、扼殺中小企業生存空間，並宣示與全球的中小企業站在同一陣線（莊蕙嘉，2020）。Google 也於 2021 年 3 月宣佈將停用第三方 cookie 及相關追蹤機制（莊蕙嘉，2021）。筆者認為這些科技巨擘的變革，並非單純出於尊重與保護使用者資料之類的道德情操，而是出於競爭目的打擊 Facebook，以及鞏固其市場壟斷地位的目的。只要使用者繼續黏著在這些平台上，這些巨擘利用使用者數位足跡的方式也幾乎沒有改變，只是名目上從第三方來源變成第一手資料（詳見以下第四點討論）。然而科技巨擘間的鷸蚌相爭，也看似為在乎隱私的使用者多了一個選擇。

這或許也導引出一個可笑又可悲的結論，使用者的資料保護，不是靠業者的自律與法遵完成，也不是靠政府的監理落實。而是在業者與政府之間，或業者與業者之間的廝殺中逐漸成型。以前文提到的透明度報告為例，業者擔心被發現將大量使用者資料交給政府後，將失去使用者的普遍信任，如此業者也將失去一切，而被迫出版相關透明報告供外界周知，有時甚至不惜提起訴訟抗拒政府的要求。這也讓筆者想到，Google 拒絕美國司法部某次要求調閱搜尋紀錄之後，於

28 以下段落的内容大量改寫自與受訪者 A3 的訪談紀錄（受訪者 A3，行 251-311），但為行文方便，筆者採取自己的筆法與引述文獻，但也特此致謝受訪者。

2007年宣佈網站後台將只保留2年內搜尋者的識別資訊，以防日後政府再次提出調閱搜尋紀錄的要求，結果引發同業競相縮短識別資訊的儲存時間，此事最後也成為經典案例（麥爾荀伯格，2015：224-227）。如今 Apple 與 Facebook 出於競爭目的，分別在保護使用者隱私和中小企業的生存爭奪道德制高點，筆者以局外人觀點除了感到荒謬之餘，也只能喟嘆歷史不會重演，但是驚人地相似。使用者終究只能在這些夾縫之中求生存。

四、 監理策略是否加劇數位廣告產業的壟斷？

呼應第二章對於管制悖論的討論，即使經過縝密規劃，管制政策仍可能造成有利於被管制產業，結果傷害使用者權益的非預期後果。下一個問題便是，現行監理社群網站運用數位足跡的策略，是否反而加劇了數位廣告產業的壟斷，進而造成使用者的權益更難被保障？

儘管在第二章的文獻探討（見本文第24頁），筆者也援引了一些指稱 GDPR 實施後，因為法遵成本的遽增，造成中小型廣告產業消失的報導（Layton, 2019; Stapp, 2019），但是這些也僅止於實務現象報導或推論，而尚未得到系統性的檢證。然而當筆者詢問幾乎每一位受訪者²⁹對於上述說法的評論時（雖然口吻與內容隨訪談時序有所調整），受訪者均表示無力回答這個問題。即使是訪問專家學者，也只能說從推論而言確實可能會發生，但是無法確證在經驗上是否成立，受訪者 D2 甚至表示傳播學者多半不會注意這類事情（受訪者 D1，行 912-985；受訪者 D2，行 191-220）。除了在台灣缺乏研究之外，政府對於社群網站運用數位足跡的行為的監理不是幾乎沒有，就是仍在起步階段，也可能是這問題至今缺乏定論的原因之一（受訪者 B1，行 471-483）。

受訪者 A1 基本上認為，GDPR 或其他個資保護法令本身造成的影響並不明顯，根本原因是這些業者握有大量的使用者資訊，而中小企業也幾乎沒有較量的本錢（受訪者 A1，行 645-649）。受訪者 B3 雖然不否認 GDPR 與個資保護法令日趨嚴格可能造成的衝擊，但是認為部分衝擊也來自市場風氣的改變，隨著民眾個資保護意識的提升，加上隱私提升工具（privacy-enhancing technology）、及以主打隱私保護的瀏覽器如 Firefox、Safari 的崛起，第三方追蹤機制也將逐漸無用武之地，接下來將只有握有大量第一手使用者資料的業者，才有機會取得較大的

29 由於經過多次訪談後，發現連傳播學者都表示無法完整回應該問題，故從受訪者 C1 的訪綱開始移除該題目。

勝算，然而多數中小業者難以具備這種能力，所以受益的當然還是大型業者（受訪者 B3，行 334-374）。Google 於 2021 年 3 月宣佈將停用第三方 cookie 及相關追蹤機制時，便有業者批評此舉將加深廣告主對 Google 的依賴，進而鞏固其壟斷地位（莊蕙嘉，2021）。這傾向也令人想起麥爾荀伯格（2018：195-197）所提出，應有強制大型業者對競爭業者開放資料的機制的倡議，然而此時基於私利使用者加強資料保護，與基於公益開放近用之間的拉扯也逐漸浮現。

乍看之下資料保護策略弊大於利，因為其在理論上製造了只有利於大型業者生存的空間。受訪者 A2 偏向消極認為，台灣政府在缺乏跨境執法能力的情況下，即使管了也只會扼殺國內的新創產業，對於解決本研究關心的問題沒有太大助益（受訪者 A2，568-574）。然而受訪者 D1 則認為，即使管制確實可能造成副作用，主管機關也不應作繭自縛。雖然有些產業確實可能會因此消失，但在這個洗牌過程也可能讓新興產業崛起，例如專精法遵業務的業者（受訪者 D1，行 892-896）。再者，如同食安的標準不能因為造成生產成本的墊高而妥協，也不能因此任憑網路產業的資料保護標準持續低落，讓業者恣意利用使用者的個資（受訪者 D1，行 900-908）。受訪者 E1 也抱持類似看法，認為 GDPR 並不是奧客找碴，而訂出如此嚴苛的裁罰基準，而是立法者認為一家公司應該投入在資安的成本，強迫業者寧可花這筆錢在資安上，也不要到時出事還上新聞（受訪者 E1，行 1115-1117），且對於中小企業與科技巨擘，對於其投入資安成本多寡的規範也會有不同標準與相應比例原則，不會強人所難（受訪者 E1，行 1158-1177），隱含單憑生產成本的墊高，並不能減損相關立法的正當性與必要性。

話雖如此，筆者也擔心在法令公布的初期，因為相關判決與案例皆不甚明朗，這類不確定性與疑懼，就足以讓部分新創產業的業主卻步。且由於不是所有中小企業都具有得天獨厚的法遵能力與條件，在面臨上述衝擊時也會相對辛苦（Sirur et al., 2018）。從公共政策的角度的角度，政府是否能協助這些業者挺過衝擊，至少不至於被市場淘汰，也不無疑問。綜觀歷史，中小企業通常還是產業轉型的受害者。問題的另外一個關鍵，可能是現在也缺乏便宜且方便操作的軟體或法遵方案的套裝（package），供財力與技術皆有限的中小企業大量佈署（受訪者 A1，行 678-685；受訪者 A3，行 650-662）。然而這些問題不論在境內外能得資料相對稀少，故筆者也難做進一步的評論，但是可能成為日後的一個觀察重點。

但是若如受訪者 B3 所述，隱私提升工具日益普及的趨勢為真，GDPR 等資料保護法規的恐怕也就不是主要考量，而可能是整體市場趨勢不可逆的轉變。加上 Apple 與 Facebook 出於對隱私權政策的歧見針鋒相對的新聞，問題焦點也不再是要不要立法，而是在這既存現實下，如何降低產業轉型過程對中小型業者帶來的衝擊。然而筆者懷疑，迄今公共政策似乎尚未發展出很好的實務方式來應對，這也可能是成為日後的觀察重點。

五、現行監理策略的得失

最後，讓我們來檢討現行監理策略的相關得失。首先將以系統性的視角，鳥瞰現行監理策略的實際樣貌（如圖 4-2 所示）。監理策略的實際樣貌，大致呈現殘缺與空白而幾乎無法描繪。雖然訪問多位受訪者，但是發現不論從業者或政府，均難以取得足夠資料以進行立法後的法規執行與遵循相關細節的探討，後續的過程與成果評估也就無以為繼。業者相關受訪者缺乏意願或權限提供進一步的法遵資訊，是相關資料不足的主要原因。政府部分除了國發會以外，雖然未訪談現職的經濟部工業局官員，但是訪談離職人員與比對外圍受訪者言談，仍能推得政府現在就是自顧不暇，或是缺乏相關工具的結論。也隱含政策規劃與執行系統皆出現嚴重問題，以下也將簡述與評價之。

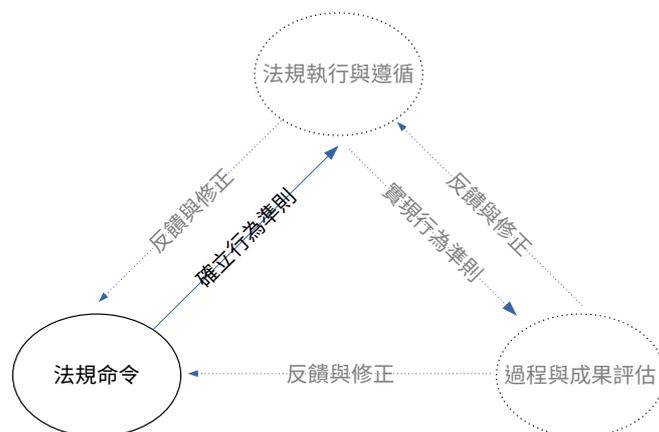


圖 4-2：現行監理策略的實際樣貌

資料來源：本研究繪製。

第一部份先探討法令規範面臨的問題（如圖 4-3 所示）。基於特別法優於普通法的原則，下文主要以我國個資法作為主要探討對象。綜觀法令規範的形成過程，筆者認為影響我國個資法相關內容的元素，仍以國際法例為主，特別是制定

過程大量參考的歐盟資料保護指令（Data Protection Directive 或 Directive 95/46/EC）的相關內容。日後為滿足 GDPR 更加嚴苛的適足性認證需求，我國個資法日後的面貌料將與 GDPR 更加接近。相較之下，美國業者的自律原則在我國個資法中的影響力則明顯被淡化。我國個資法的修訂以繼受外國法制為主的事實，也可能意味著立法者對於該法應該達到什麼目標，並不是非常清楚，而只能幾乎照單全收。受訪者 A1 也建議，如果 GDPR 有自己要解決的問題，且台灣也沒有能力比照 GDPR 執行跨境監理的任務，也應該在繼受相關法制時做適當調整（受訪者 A1，行 551-560）。又如前述受訪者 C1 所言，台灣欠缺類似歐盟法制的歷史基礎，若原封不動地引入恐有水土不服之虞。筆者也偶爾在相關研討會聽聞專家發言，意思大致是台灣學者已經做了很多先進國家的法制研究，接下來應該是將這些成果融會貫通，而不是已經消化不良，又要去學新的東西。

對此筆者認為，台灣應該先做到的，是建立普遍尊重個資的社會風氣。雖然經過一系列資料外洩事件後，可預期台灣民眾對於資料保護與隱私的意識將有所提升，但若如受訪者 B1 所言，填個資換取小禮物或優惠的風氣仍然興盛，也表示台灣民眾處理個資的態度不甚嚴謹。實務上政府也是基於效率至上的思維，以非常輕率的態度在運用民眾的個資。這些因素疊加下來，也就不難解釋，我國即使有修訂個資法，似乎長期處在徒法不足以自行的狀態。

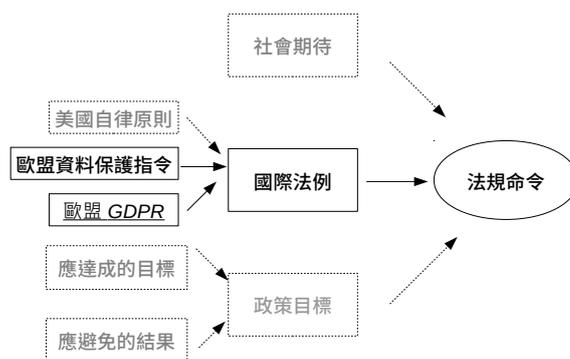


圖 4-3：監理策略法令規範的實際組成要素

資料來源：本研究繪製。

若法令規範作為施政理想狀態的體現，已經堪稱千瘡百孔。也就令人難以想像下一步的執行會是怎樣的景況（如圖 4-4）。業者行為一如預期，由於棄用針對式廣告等精準行銷技術的機會成本甚高，加上追求獲利極大化的人性趨使，通常不會主動約束上述行為，往往還是法律要求做一步，業者才開始做一步，這也

間接導致劍橋分析事件等重大資安事件的爆發。儘管受訪者 B3 與 E1 對於劍橋分析有截然不同的看法，不管認為是 API 使用者的惡意濫用或資安漏洞，業者未善盡管理之責造成軒然大波，仍然是不爭的事實。且除了歐盟以外，其他先進國家幾乎沒有如納粹德國專精於以蒐集個人資料用於種族清洗的難堪歷史，多數人應該也是因為近來資安事件的頻傳，才對相關議題開始了解與重視，但是尚不足以成為全民運動。質言之，除了本來活躍的相關資訊公民團體之外，社會期待並不足以造成有力的約束。反而是敵對同業的競爭行為，比較有機會促成變革，也算是本研究意外但諷刺的發現。

另一方面，雖然受訪者 E1 認為業者許多資料保護措施不是做不到，只是要不要做的問題而已。不過從如同本文第 42 頁關於 GDPR 的討論所述，資料保護與使用者體驗的美觀與便利之間，技術上似乎存在不小張力，儘管這不應成為我們妥協或搪塞的理由，然而也不應無視相關困難，也宜進一步追蹤相關的發展。

政府方面至少在台灣，由於其執法能力不足，但部分也根源於國際處境的現實，業者缺乏誘因提出對使用者友善的資料政策，應該是無需贅言的事實。誠如陳泉錫（2016：137-139）指出，政府在實質面上缺乏關鍵資源，特別是人力、經費與組織制度上的支持，不論是既有人力應接不暇或缺乏專業能力，或是程序上缺乏專責主管機關的老問題，也已被受訪者屢次述及。另外，在此處的制度支持，除了可能指涉專責主管機關的問題外，還有在組織任務分配與指揮鏈傳遞過程，是否將個資保護列為優先？否則主管機關遭遇產業推動與監理業者之間的衝突時，恐怕仍以前者為優先。這些也料將成為監理策略執行的最大隱憂。

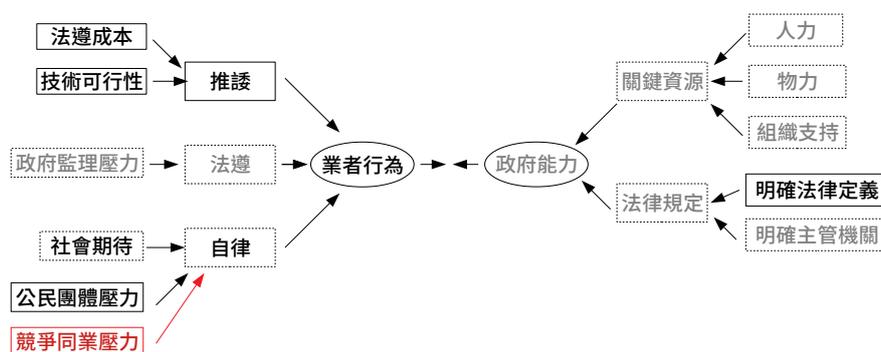


圖 4-4：實際的執行面各行為者組成與策略

資料來源：本研究繪製。

最後筆者認為，儘管為配合歐盟 GDPR 的適足性認證，相關法制的修訂可能仍然重要，不過台灣的現狀是更缺乏一套可執行的政策工具與監理流程。至於明確法律定義，以及許多受訪者所提到專責機關的問題，由於法務部與經濟部工業局，已經針對個人資料及相關受轄產業做出相當完善的定義，即使缺乏個人資料保護的專責主管機關，在實務運作上雖可能仍有混亂，但應不至於癱瘓，反而不是筆者認為最迫切的問題。只是長期而言，仍應加緊在服務設計及事權分配的改善，否則民眾與業者終將無所措手足。筆者認為最麻煩的問題，反而是政府的行政文化，若不從此根本面處理效率至上的思維，不論是哪種資料保護制度被引入政府，可能都終將只是枉然。



第五章 結論與建議

經由一系列文獻探討深度訪談，前文已對於境內外主要國家，現有對於社群網站運用數位足跡的監理策略，及其相關利弊得失，大致進行系統性的梳理與探究。本章之要旨則為摘要上述成果，並據此提供相關實務建議，並於文末坦承餘下未臻完善之處，以為後續研究改善之參考。本章之行文架構簡述如下：第一節以摘要形式闡述研究發現，內容將聚焦於現有業者採取資料保護行動，以及政府監理政策執行的相關得失，並點評其實務意涵；第二節將依據上述發現提出相關政策建議；最後則探討研究限制及其可能成因，並期待日後精進與解決之機會。

第一節 研究發現

本研究嘗試從政策執行的角度切入，探討社群網站運用數位足跡及衍生之問題之監理策略及執行成效，並釐清其所遭遇之困難，特別是與理想之落差及可能衍生的弊害，以作為後續改進之借鑑。為達致上述目的，筆者原定兼以檢閱大量文獻與對多位利害關係人進行深度訪談，依序回應三組研究問題（詳見第一章第二節）。研究問題一是分別從應然面與時然面切入，了解成功的監理策略，應該達到哪些目標，以及現有監理策略（包含自律與他律）手段的施行概況。研究問題二則檢視上述策略獲致的成效，成效與目標之間的差距及可能衍生的弊害。研究問題三則解釋上述問題的成因及可能改進的方向。最後獲致如下發現：

首先（回應研究問題一），筆者歸納大量文獻後指出，成功的監理策略應該達成捍衛使用者隱私、保護寡占市場下的使用者權益、以及杜絕業者的欺罔行為（詳如第二章第二節）；受訪者則認為業者在消極面應主動揭露其商業模式，特別是自動化決策可能造成的差別待遇，使用者也應能更大程度選擇數位足跡被利用的範圍，積極面則應該設立機制，平衡演算法的行為導引效果，以及協助使用者行使法定權力（詳如表 4-3）等，作者也大致贊同上述立場。

第二（仍回應研究問題一），雖然 Facebook 宣稱採取了若干自律措施，如遵循數位廣告聯盟與 AdChoices 的自律規範（業者委任律師則提及遵循 BS 10012 等國際標準），以及賦予使用者若干資料控制能力，特別是在手機應用程式設置批次刪除活動紀錄的功能，然而筆者無從了解業者如何落實上述自律細節，受訪者亦不乏類似批評。且業者只緩慢釋予使用者非常有限的數位足跡控制權，且仍保留大量用以投放針對式廣告的權限，利用資料的方式也未有根本的改變。加上業

者又在劍橋分析事件觸法且被 FTC 裁罰的事實，也就更難博得外界的信任。這些也構成本研究的第一個發現，即單憑業者的自律與法遵措施，恐怕不足以獲致上述成功監理策略所應達成的目標，如今在各類負面新聞流竄下，多數使用者即使不去參閱各類技術文獻或報告，大概也會下意識認為，在 Facebook 所看到的動態訊息和廣告都是「被洗過的」，筆者認為即使再次要求業者主動揭露其自動化決策與差別待遇，恐怕意義也不大。

第三（同時回應三組研究問題），雖然業者不論在自律或法遵措施皆飽受外界批評，姑且還有公關文件可供參詳。而筆者能從政府得到的監理執行相關細節，還比業者更少，也幾乎找不到裁罰案例，推論監理機制仍大致停留在立法，後續執行不是完全沒有，就是還在起步階段。這也導致欲探討後續的成果評估，幾乎無以為繼。即使國發會在 LINE 片面更改隱私權事件，有發佈相關新聞稿要求業者改善，也看似有微薄的約束效果，終究為事後才介入瞭解，且前提也要業者願意與政府合作與溝通。筆者坦承本文除了解析各利害關係人對於業者與政府行為的評價之外，對於監理機制的實證探討則缺乏突破性的進展；然而也半開玩笑地認為，證實我國相關監理策略貧乏的殘忍現實，可能就是一大貢獻，建議往後研究可直接聚焦在政策設計的層面。

最後（呼應研究問題二），雖然尚未有足夠證據，證明因為個人資料保護相關法令提高產業標準與進入門檻，直接造成數位廣告產業的壟斷。然而該產業的利潤與營運規模集中化，與業者與使用者之間權力不對等日益擴大已成為事實。另一方面，不論上述法令是否存在，近期科技巨擘之間為隱私權政策隔空叫罵，以及使用者逐漸善用隱私提升工具、及注重保護隱私的瀏覽器的趨勢，造成包括中小型業者在內的第三方追蹤瀏覽機制逐漸失去效用，終將可能造成只有利於握有大量第一手數位足跡的大型業者的生存環境。此時政策的焦點，可能不再是繼續爭論監理是否可能造成不良影響，而是立即就廣告產業壟斷的現象，研擬相關對策。

第二節 實務建議

經過前一節的研討，可簡單將監理策略所遭遇的問題歸納為（1）業者與政府皆缺乏資訊的主動揭露，話說不清楚也就造成許多未知與混亂；（2）政府監理能力與心態建設不足，監理策略不是完全沒有，就是處在躊躇不前或剛起步的狀態，業者也表示缺乏參與的機會；（3）雖然未能確定數位足跡利用監理策略

與數位廣告產業壟斷的因果關係，然而產業生態的改變與使用者逐漸善用隱私工具，仍可能造成只有利大型數位廣告業者生存的環境，而應立即研擬對策。本節則基於上述發現，分別對於業者、公部門與使用者提供相關實務建議：

一、對於業者之建議

筆者已多次論及，業者對於數位足跡利用方式的缺乏揭露，加上已有違規案例與造成使用者的傷害，是外界對於業者採取資料保護措施缺乏信任的主因。也提及以公關運作的常識而言，在發生重大事件時，外界若無法從官方得到滿意的回應，便可能轉而尋求各種替代的資訊來源，其中可能也不乏小道消息或競爭對手的中傷，也可能讓爭議訊息的傳布更難被控制。在各類公民團體、研究機構陸續出版相關報告，甚至刊載於學術期刊的情況下，外界接下來顯然也只會想知道更多事情。筆者無意在增加對資料處理程序的透明度、揭露演算法等老問題上繼續打轉，也深知上述訴求勢必觸及營業祕密的禁巒，要業者自主實施的可能性也甚低。以下只基於受訪者回應與研究發現，提供幾個實務上可行的建議：

首先，鑑於基於演算法的自動化決策、行為與情緒導引是目前社群網站運用數位足跡過程頗具爭議的問題。對此筆者援引受訪者 D2 的發言，建議在演算法中設立平衡機制，也可能刻意加入完全不一樣甚至相反的內容，以減緩行為導引的衝擊。也或可仿效塔吉特百貨的做法，穿插隨機的推播內容讓使用者安心，該公司也因此贏得更多營收（杜希格，2012：230-231; Duhigg, 2013: 441-442）。

第二，不論基於前引文獻或受訪者評價，皆顯示外界對於業者利用資料的方式仍不甚信賴。減少業者持有的資料數量，進而降低風險及可能的傷害，或許是短期內較可行的途徑。對此，筆者建議業者引入自動遺忘機制（或稱「到期日機制」），即將特定時間內未使用，或利用目的消失的資料自動刪除的機制，其好處除了保護使用者隱私之外，主要還有技術上相對可行，且避免過時的資料影響推播的品質，也有助於精準行銷（麥爾荀伯格，2015：220-231）。Google 現在已經有類似功能，使用者設定啟用後，將只保留該帳號 3 至 18 個月前的搜尋紀錄、即時定位紀錄等資訊。隨著 Facebook 迄今已營運超過 15 年，很早就註冊的使用者也可能擔心，多年前在網站留下的紀錄，會開始對其未來造成不利影響。以筆者從 2009 年使用 Facebook 迄今為例，累積了許多貼文、朋友圈與即時訊息等事務，但是難免也有不光彩的紀錄或回憶。雖然被某些朋友討厭或甚至封鎖的問題，不可能靠刪掉這些數位足跡就能解決。但是筆者私下也希望，對於過時的

貼文或內容能有自動刪除的機制，也減少日後被找碴的風險。然而 Facebook 近期仍只能利用手機應用程式做貼文等內容的批次刪除，且必須人工逐項選擇，這也嚴重影響筆者繼續使用 Facebook 的意願。儘管本論文所提及的各種問題，也不是筆者採取該行動的唯一動機，但是坦承是重要的原因。況且這還只是對於使用者主動提供的類型一資料的討論，還尚未論及更敏感的系統自動蒐集的類型二，與推論而得的類型三資料。

第三，筆者於第二章第一節的討論與數位受訪者的發言，皆有提到使用者條款與資料政策缺乏易讀性的弊病。除了降低使用者的閱讀意願，過於複雜的法規也徒增居中舞弊的空間，也與 GDPR 第 12 至第 14 條，要求業者以簡易格式告知使用者重要事項的原則不甚吻合。改善易讀性除了能提高透明度，進而增加業者改進隱私權政策的誘因外；也意味使用者將承擔更大的自主管理隱私權，以及獨立判斷是否繼續使用該服務的權限與責任。

英國資訊專員辦公室 (Information Commissioner's Office, ICO) (ICO, n.d.) 對此已提供若干範例，例如最初只顯示主要標題，使用者可自行點選展開細節的分層式途徑 (layered approach)，以及以儀表板 (dashboards) 形式呈現選項，供使用者自行控制資訊分享的對象或權限等。實務上 Facebook 已在隱私設定頁面，提供使用者類似儀表板的功能自行設定上述權限，其資料政策的呈現方式雖然貼近分層式途徑，仍幾乎完全以文字呈現，且將近 8000 個中文字，顯然與簡明原則相去甚遠。筆者建議可以參考部份業者的做法，以扼要的表格陳明使用者，內容包含該公司究竟收集了哪些資料、收集的目的、是否向第三方分享、以及最重要的：使用者能否限制分享這些資料。筆者甚至認為這可能遠是比 ICO 的範例更有效的途徑，也相信社群網站業者做得到。

二、對於政府機關之建議

對於政府的批評的細節，筆者已大致闡述於第四章與本章扉頁處，故不再於本處贅述。筆者認為建立一套可行的監理施政流程，是比起修法更為迫切的議題，而公務人員的心態是否完備，與重新設計組織指揮鏈以提高流暢性，也將是成功的先決條件。筆者也將先從施政的思維層面，到組織與實作層面對政府提出相關實務建議，最後則論及應對廣告產業壟斷的新興現象研擬對策。然而本階段恕無法指出具體的政策設計與方案，而待後續進一步鑽研。

首先，承接第四章第五節對於現行策略得失的討論，政府在制定相關監理策略之時，應優先調整資料治理的心態與思維。如果政府的心態，仍然是以產業推動與施政效率作為優先，即使立再多相關監理法案，抑或成立個資保護的獨立專責主管機關，筆者預期也只會構成徒法不足以自行的結果，進而斷傷政府的威信。對此筆者也已多次於第四章闡述類似論點，於本處也不再贅言。另一方面，筆者認為政府人員使用通訊載體時，普遍未落實資安與風險控管，例如公務人員倚重 LINE 處理公務的現象，大量公務資料透過境外業者管理的網路節點流通，不論從國防、業務性質或單純分散風險的角度，顯然皆不甚妥適，也宜加以檢討。若現實上必須採用這類通訊軟體，基於避免公務人員以私人帳戶處理公務的考量，厲行相關管理配套實為必要。也可能仿照異地備援的精神，在多種載體、帳號之間靈活操作與分流，例如除了在 LINE 之外，同時在新型通訊軟體如 Telegram、Signal 等操作，或可作為一種嘗試。

第二，呼應筆者第四章第五節對於獨立專責主管機關的討論。民眾與業者真正在意的，應該不是真的要組織編制上的專責主管機關，而是像緊急救護服務一樣，遇到事情時能馬上被轉介到適合的機關去處理。若將前者比喻成硬體，利用制度將政府機關拆分成無數個隔間，後者則偏向軟體的層面，即服務設計與指揮鏈的傳遞。鑑於使用者資料保護對於政府而言，仍然是非常新且陌生的概念，加上組織改造在金錢或時間上的成本皆非常高，即使據傳下一波組改要成立數位發展部，要為了資料保護這個本來不存在台灣法制的概念，大幅更改組織架構成立專責機關，甚至成立獨立預算與員額，政治可行性恐怕也不高；且還尚未論及是要仿照歐盟的獨任制，還是依照我國慣例採取合議制的問題。揣此筆者認為以現階段而言，改善軟體的層面，可能才是合乎效率兼經濟的長久之計。

第三，呼應管制悖論文獻的警示，本文也嚴密注意監理策略是否使法遵成本提升，造成技術與財力較為弱勢的中小企業消失，與數位廣告產業的壟斷，最後更嚴重傷害使用者的福祉。經過前面的密集探討，筆者認為重點已經不是爭論該因果關係是否存在，而是政府應盡速數位廣告產業壟斷的既成事實，審慎研擬對策。即使不論壟斷或寡占是否可能影響使用者福祉，產業與活動高度集中於特定業者，若不幸出事造成的危害也就不容小覷。然而筆者自承非該問題專家，只能點評至此，但是希望有後續研究能聚焦在這類事件的發展與相關對策。

三、對於使用者之建議

綜合前文所述，筆者認為政府短期內應無法提出相對完善的監理方案，而業者基於市場優勢，恐怕缺乏誘因大幅改變利用數位足跡的方式。該現象恐怕為典型的囚徒困境賽局（Prisoner's Dilemma Game），即雙方無限制追求私利，但是無法獲致對全體最有利的結果。該結論固然悲觀，不過應相當貼近現實。不過筆者坦承本論文的基調，確實有將使用者的權益無限上綱的疑慮，且筆者在第二章第三節也論及，使用者應該清楚明白社群網站不是慈善事業，為享受服務勢必需要付出代價，只是該代價是否合理。也不能只是被動地要求政府監理業者，卻對於自身應善盡的責任漠不關心與不願採取行動。如此看來，民眾資訊素養的建立看來空泛，仍可能還是重中之重。

儘管市場競爭，例如前述科技巨擘（Apple、Facebook 與 Google）之間近期在隱私權條款的鷸蚌相爭，或許短期仍是推動業者變革的最大力量，不過使用者恐怕也不能因此高枕無憂，況且此時使用者的處境，也可能更像戰火下的難民。即使近期 WhatsApp 更改政策，強迫使用者同意與 Facebook 分享部份個資的事件，引發逃難至 Signal 與 Telegram 的風潮（顏嘉南，2021）。然而以筆者經驗為例，轉移的人數恐怕仍不足以在異地重建相似的人際網路，多數人料將摸摸鼻子，繼續留在原有通訊軟體上。也部份解釋 WhatsApp 何以有恃無恐。如同經濟學家凱因斯的名言：「長期而言，我們都死了（In the long run we are all dead.）」，筆者不認為透過市場機制的調節，能帶來明顯的幫助。

綜上所述，使用者應該清楚作為弱勢的買方，隨時便處於被價格控制者剝削的風險。綜然現實上不可能完全棄用這些網路平台，基於風險控管目的，將資料與通訊備援與分流至其他服務，雖然可能造成不便，仍為必要之舉。筆者在社群網站除原有的 Facebook 帳號外，也在相對冷門的 Plurk、Mastodon 等開設帳號；即時通訊方面，除既有的 LINE 帳號之外，也有 Telegram 的備援。但是 WhatsApp 的案例也清楚指出，在網路效應的限制下，不是所有使用者皆能或願意轉移。此時問題的關鍵應該是，使用者是否有採用技術上通用的格式，而能在不同服務之間互通與轉移。而在目前生活中應用可行性較高的，可能就是較早問世，但可能在監理機制上也較成熟的電子郵件。電子郵件雖然古老，但是格式互通且能將信件分散儲存於不同業者的伺服器，甚至可以自行架設伺服器，避免被單一廠商掌握風險，可能是個好選項（洪朝貴，2018）。雖然以新世代資訊使用者的角

度，筆者的做法與倡議還可能會招致資訊原始人的罵名與譏諷，但在方便與資訊自主權無法兼得的現實下，短期似乎也沒有更好的方法。

第三節 研究限制與後續可能精進方向

雖然筆者以盡其所能之注意，務求本研究各項細節的嚴謹執行，仍難免有其限制與不足之處，也將於下文詳述，並建議後續可能精進的方向。然而除非必要，下文將不再贅述受訪者人數，或原訂訪談題項沒問到等芝麻小事，而偏向從較宏觀或方法學的角度為之。

一、 缺乏量化方法以推論利害關係人的行動態樣

本文採取質性訪談法訪談多個利害關係人，試圖以初探角度，了解其認為的監理策略的執行狀態，也藉此試圖拼湊事實的樣貌。然而除了受訪人數少與同質性高的先天限制外，缺乏量化的測量方法與標準化的基尺，也難以再依據受訪者的性質與背景，從中建立假設推導其可能的態度與行動態樣，更別說建立理論。建議後續研究可從本研究或相關成果中，擷取重要概念進行量化工具的繪製。

二、 缺乏具體的個案研究

筆者認為本文最嚴重的限制，便是缺乏具體與多重個案的比較。雖然以劍橋分析事件作為本文楔子與假想對象，但是未能緊扣具代表性的個案，例如曾在法院爭訟的案例，導致難以聚焦與衍生研究資源浪費，最後也只對於我國資料保護政策的施行概況，提出相對空泛的結論。我國缺乏劍橋分析事件的直接受害者，是難以進行個案研究的主要因素，雖然筆者嘗試以訪談普通商業網站資料外洩事件受害者補足，但該事件性質與劍橋分析事件仍有相當差距。但是樂觀而言，政府處理普通商業網站資料外洩的經驗，或許相當程度能類推至社群網站。

三、 增加多重與異質個案的比較

本研究所援引之劍橋分析事件，固然有社會影響的代表性，然而也非歷史上唯一的重大資安事件。且縱使社群網站在常人看來是新科技，筆者相信普通商業網站的治理經驗有機會類推適用，是此本文也大量引用普通的資料保護相關法令的文獻。更為理想的探討方式，應該是將普通商業網站與社群網站具代表性的案件並列，並比較多重案例之間，業者自律、法遵與政府監理方式與結果的異同，如此也才有機會建立較為穩定的因果推論與理論架構。後續研究也宜延伸至異質

性更高的個案比較，例如資訊服務業與傳統產業、金融業等，檢測其在監理策略執行的關鍵步驟與結果，是否存在相似的問題、處置程序與因果關係。反過來說，社群網站的主管機關，也或可汲取若干特種行業，例如金融、食品與藥品等的監理經驗，作為進一步擬定與改進的參考。



參考文獻

- 卡爾·紐波特 (2019)。深度數位大掃除：3分飽連線方案，在喧囂世界過專注人生，洪慧芳譯，台北：時報。譯自 Digital Minimalism: Choosing a Focused Life in a Noisy World. Newport, C. 2019.
- 史蒂格勒 (1991)。人民與國家：管制經濟學論文集，吳惠林、鍾琴、黃美齡 (譯)，台北：遠流。譯自 The Citizen and the State: Essays on Regulation. Stigler, G. J. 1975.
- 布特妮·凱瑟 (2020)。操弄：劍橋分析事件大揭秘，楊理然、盧靜 (譯)，新北：野人。譯自 Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again. Kaiser, B. 2019.
- 江淑琳 (2014)。流動的空間，液態的隱私：再思考社交媒體的隱私意涵。傳播研究與實踐，4 (1)，85-104。doi：10.6123/JCRP.2014.005
- 行政院 (2021年3月25日)。行政院會通過國防部、科技部、數位發展部暨所屬三級機關 (行政法人) 組織法、行政院組織法及中央行政機關組織基準法 (修正) 草案等 16 項法案。上網日期：2021年4月22日，取自：<https://www.ey.gov.tw/Page/9277F759E41CCD91/a0c440d6-f9f1-4225-84b8-7124bd9430a4>
- 行政院資通安全處 (2014年6月4日)。CNS 29100 資訊安全個資管理國家標準。上網日期：2020年11月13日，取自：<https://nicst.ey.gov.tw/Page/7CBD7E79D558D47C/282835f2-5d6c-466c-bd7e-de029ac7aa04>
- 伯納賽克、蒙根 (2015)。失控的大數據，吳慕書 (譯)，台北：商周出版。譯自 All You Can Pay: How Companies Use Our Data to Empty Our Wallets. Bernasek, A. & D. T. Mongan. 2015.
- 杜希格 (2012)。為什麼我們這樣生活，那樣工作？全球瘋行的習慣改造指南，(鍾玉珏、許恬寧譯)，台北：大塊出版。譯自 The Power of Habit: Why We Do What We Do in Life and Business. Duhigg, C. 2012.
- 肖莎娜·祖博夫 (2020)。監控資本主義時代，溫澤元、林怡婷、陳思穎 (譯)，台北：時報出版。譯自 The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Zuboff, S. 2019.
- 邱映曦、劉敏慧、何寶中 (2013)。我國個人資料保護法與個人資料管理制度。資訊安全通訊，19 (1)，45-62。
- 邱祥榮 (2001)。論美國網路個人資訊隱私保護型態轉變之初探。全國律師，5 (12)，80-91。
- 邱瓊玉 (2016年3月5日)。加班超時要寫報告 公務員怨-人事處長：沒要求寫，應是局處執行偏差。聯合報，第 B2 版。

- 李世德（2018）。GDPR 與我國個人資料保護法之比較分析。**台灣經濟論衡**，**16**（3），69-93。
- 李芯（2020年8月12日）。《隱私盾協定》遭廢！歐美個資傳輸恐違法，逾5,000家企業面臨「罰7億」風險。上網日期：2020年8月27日，取自：<https://crossing.cw.com.tw/article/13787>
- 李億誠（2019）。歐盟一般資料保護規則（GDPR）裁罰案例解析。**科技法律透析**，**31**（12），26-38。
- 周宥廷（2020）。簡述兩則近期美國聯邦貿易委員會與 Facebook、Google 及 Youtube 和解案。**聖島智慧財產權實務報導**，**22**（2），1-18。
- 周峻佑（2018年7月6日）。劍橋分析事件爆發後，臉書仍舊提供61間公司使用者個資的存取權。上網日期：2019年10月24日，取自：<https://www.ithome.com.tw/news/124339>
- 法務部（2015年4月21日）。個人資料保護法非公務機關之中央目的事業主管機關列表。上網日期：2020年10月14日，取自：<https://www.moj.gov.tw/cp-793-47377-1acb3-001.html>
- 林子蘅（2019年12月24日）。國發會明年推數位三法 個資法、組織法、開放資料專法。**經濟日報**。上網日期：2020年7月29日，取自：<https://udn.com/news/story/7238/4246581>
- 林河名（2018年7月15日）。LINE 新隱私權政策 國發會：要求改善。**聯合報**，第 A8 版。
- 林冠佑（2012）。社群網站與個人資料保護初探。**司法新聲**，**101**，19-32。
- 林奕榮（2020年12月16日）。蘋果 App Store 新增隱私標籤。**經濟日報**，第 A8 版。
- 林庭安（2018年7月13日）。被 LINE「綁架」、強迫授權個資？官方證實能取消，一張圖教你怎麼做。上網日期：2020年10月19日，取自：<https://www.managertoday.com.tw/articles/view/56390>
- 林思惟（2016）。歐盟新規：個人資料保護規則—數位防護的新縱深。**金融聯合徵信**，**29**，14-22。
- 洪家殷（2019）。公務機關資料之蒐集與個人資料之保護。**東吳法律學報**，**30**（4），29-68。
- 洪朝貴（2018年7月17日）。資訊人權貴出疑：Line 不僅是高牆花園，也是國安要害。上網日期：2020年6月23日，取自：<https://ckhung0.blogspot.com/2018/07/line.html>
- 胡雅筑（2021年2月26日）。Facebook 將停用歐洲使用者 Ig 及 Messenger 部分功能。上網日期：2021年3月22日，取自：<https://hsu.legal/en/article/31>
- 孫鈺婷（2016）。歐美跨境資料傳輸新框架—從歐美安全港協議無效談起。**科技法律透析**，**28**（7），22-30。

- 孫鈺婷 (2019 年 6 月 4 日)。我國去識別化實務發展－「個人資料去識別化過程驗證要求及控制措施」。上網日期：2020 年 11 月 12 日，取自：<https://stli.iii.org.tw/article-detail.aspx?no=66&tp=3&i=158&d=8261&lv2=158>
- 徐榆涵、黃秀媛 (2019 年 7 月 14 日)。濫用個資 臉書被罰 1500 億-美科技業最高罰金…「僅是做生意的必要成本，划得來」。聯合報，第 A8 版。
- 納西姆·尼可拉斯·塔雷伯 (2011)。黑天鵝效應，林茂昌 (譯)，台北：大塊文化。譯自 *The Black Swan: The Impact of the Highly Improbable*. Taleb, N. N. 2010.
- 翁清坤 (2010)。論個人資料保護標準之全球化。東吳法律學報，22 (1)，1-60。doi：10.6416/SLR.201007.0001
- 翁清坤 (2016)。網路上隱私權政策之效力：以美國法為中心。臺大法學論叢，45 (1)，151-248。doi：10.6199/NTULJ.2016.45.01.03
- 翁清坤 (2018)。賦予當事人個人資料財產權地位之優勢與局限：以美國法為中心。臺大法學論叢，47 (3)，941-1051。doi：10.6199/NTULJ.201809_47(3).0001
- 莊庭瑞 (2003)。個人資料保護在台灣：誰的事務？。國家政策季刊，2 (1)，53-70。doi：10.6407/NPQ.200303.0053
- 莊蕙嘉 (2020 年 12 月 18 日)。翻臉！為隱私權限制 臉書槓蘋果-新版 iOS 將限制蒐集用戶數據 臉書怒買美國 3 大報廣告反批。聯合報，第 A10 版。
- 莊蕙嘉 (2021 年 3 月 5 日)。Google 明年停止追蹤個人網路瀏覽-還客戶隱私？改用「隱私沙盒」 廣告商：權力更集中。聯合報，第 A8 版。
- 財團法人資訊工業策進會 (2017 年 5 月 1 日)。八成以上台灣人愛用 Facebook、Line 坐穩社群網站龍頭 1 人平均擁 4 個社群帳號 年輕人更愛 YouTube 和 IG。上網日期：2020 年 5 月 5 日，取自：https://www.iii.org.tw/Press/NewsDtl.aspx?nsp_sqno=1934&fm_sqno=14
- 財團法人資訊策進會科技法律研究所 (2019)。個資保護 2.0 (二版)。台北：書泉。
- 郭戎晉 (2012)。論數位環境下個人資料保護法制之發展與難題—以「數位足跡」之評價為核心。科技法律透析，24 (4)，18-39。doi：10.7062/STLR.201204.0018
- 陳文蔚 (2020 年 5 月 8 日)。台灣學者陳憶寧列名 FB、IG 全球獨立監督委員會有權准駁爭議性內容。上網日期：2021 年 5 月 7 日，取自：<https://www.rti.org.tw/news/view/id/2063268>
- 陳泉錫 (2016)。我國現行隱私保護政策施行成效之省思與建議。電腦稽核，33，136-143。

- 陳素玲（2016年3月24日）。仿德國「拒絕聯繫權」下班可拒回LINE？勞動部：列考慮-洪慈庸虧柯P是「賴魔人」 陳雄文：同仁LINE公務都已讀不回。聯合晚報，第A8版。
- 陳敦源（2012）。民主治理：公共行政與民主政治的制度性調和（二版）。台北：五南。
- 陳熙文、劉宛琳、鄭煒（2021年1月12日）。數位身分證疑慮多 蘇同意暫緩-指示沈榮津召集盤整法制層面 待資安防護完備再重啟。聯合報，第A4版。
- 陳憶寧、溫嘉禾（2020）。台灣臉書使用者的隱私行為研究：劍橋分析事件之後。傳播與社會學刊，54，27-57。
- 陳曉莉（2019年12月9日）。臉書宣稱服務免費，被匈牙利以誤導用戶為名判罰400萬美元。上網日期：2020年1月17日，取自：<https://ithome.com.tw/news/134705>
- 陳曉莉（2020年1月3日）。美國最嚴厲的加州消費者隱私法案正式上路了。上網日期：2020年4月23日，取自：<https://www.ithome.com.tw/news/135154>
- 高敬原（2018年4月12日）。遇上一群「科技文盲」，兩天十小時國會聽證，看佐克伯如何全身而退。上網日期：2019年9月20日，取自：<https://www.bnext.com.tw/article/48768/mark-zuckerberg-day-2-congressional-testimony-data-bias>
- 國家發展委員會（2018年7月14日）。回應LINE隱私政策變更新聞稿。上網日期：2021年4月2日，取自：https://www.ndc.gov.tw/nc_27_29932
- 國家發展委員會法制協調中心（2019年12月29日）。國發會推動個資法修法，力拼GDPR適足性認定。上網日期：2020年11月13日，取自：https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA26F1A3&s=632E56DC2B36CB76
- 國際瞭望（2021年1月29日）。歐盟的平臺管制野心：數位服務法與數位市場法（上篇）。上網日期：2021年4月29日，取自：<https://blog.twNIC.tw/2021/01/29/16751/>
- 張陳弘、莊植寧（2019）。新時代之個人資料保護法制：歐盟GDPR與臺灣個人資料保護法的比較說明。台北：新學林。
- 張腕純（2018）。個人資料外洩如何通知？參考歐盟GDPR之規範與指引。科技法律透析，30（2），33-42。
- 許淑梅（2020年2月27日）。台灣政府數位程度全球第九！開放資料表現佳，跨部會溝通不順暢。上網日期：2021年3月20日，取自：<https://futurecity.cw.com.tw/article/1281>

- 許鈺屏 (2020 年 11 月 12 日)。為何雙北要推「公車上下車刷卡」？實施後發生了什麼改變？。天下雜誌。上網日期：2021 年 3 月 20 日，取自：<https://www.cw.com.tw/article/5102710>
- 麥爾荀伯格、庫基耶 (2013)。大數據：「數位革命」之後，「資料革命」登場：巨量資料掀起生活、工作和思考方式的全面革新 (第一版)，林俊宏 (譯)，台北：天下文化。譯自 Big Data: A Revolution That Will Transform How We Live, Work, and Think. Mayer-Schönberger, V & K. Cukier. 2013.
- 麥爾荀伯格、蘭姆格 (2018)。大數據資本主義：金融資本主義退位，重新定義市場、企業、金錢、銀行、工作與社會正義 (林俊宏譯)，台北：天下文化。譯自 Reinventing Capitalism In The Age Of Big Data. Mayer-Schönberger, V & T. Ramge. 2018.
- 麥爾荀伯格 (2015)。大數據：隱私篇-數位時代，「刪去」是必要的美德 (第一版) (林俊宏譯)。台北：天下文化。譯自 Delete: The Virtue of Forgetting in the Digital Age. Mayer-Schönberger, V. 2009.
- 彭慧明 (2018 年 7 月 13 日)。LINE 調整隱私權政策。經濟日報，第 A14 版。
- 黃瑞典、徐偉真 (2020 年 12 月 26 日)。數位身分證惹民怨 民代促暫緩試辦 不要「為國捐軀」-新竹人不想當資安白老鼠…。聯合報，第 A4 版。
- 楊皓勻 (2020 年 1 月)。歐盟法院裁決：網站「預先選取同意」不構成 ePrivacy Directive 及 GDPR 合法有效的同意。上網日期：2020 年 7 月 23 日，取自：<https://stli.iii.org.tw/article-detail.aspx?no=55&tp=1&i=0&d=8378>
- 經濟部工業局 (2017 年 2 月 16 日)。105 年「製造業及技術服務業個人資料檔案安全維護管理辦法」導入說明手冊。經濟部工業局。上網日期：2020 年 11 月 30 日，取自：<https://www.moeaidb.gov.tw/ctrl?PRO=filepath.DownloadFile&f=news&t=f&id=6512>
- 經濟部工業局 (2018 年 1 月 24 日)。資訊服務業提供服務之個資保護及案例說明手冊。上網日期：2020 年 11 月 30 日，取自：<https://www.moeaidb.gov.tw/ctrl?PRO=information.rwdInformationNewsView&id=23762>
- 臺灣個人資料保護與管理制度 (2016 年 5 月 31 日)。臺灣個人資料保護與管理制度規範。臺灣個人資料保護與管理制度。上網日期：2020 年 11 月 13 日，取自：<https://www.tpipas.org.tw/model.aspx?no=159>
- 蔡昫知 (2019 年 1 月 1 日)。歐盟個人資料保護治理之變遷：從《資料保護指令》到《一般資料保護規則》。國立臺灣大學政治學研究所碩士論文，未出版，台北。
- 潘兆娟 (2007)。網路企業自律機制對消費者信任影響之研究：隱私保護及交易安全認知觀點。國立政治大學科技管理研究所博士論文，未出版，台北。

- 劉仕傑 (2020 年 2 月 19 日)。名家論壇》劉仕傑／祖克伯要求立法管制網路，真心話？上網日期：2020 年 5 月 20 日，取自：<https://www.nownews.com/news/forum-2/celebritycomment-forum-2/3944889>
- 劉靜怡 (2002)。網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河。《資訊管理研究》，4 (3)，137-161。
- 劉靜怡 (2006)。隱私權：第一講隱私權的哲學基礎、憲法保障及其相關辯論——過去、現在與未來。《月旦法學教室》，46，40-50。
- 賴于榛、鄭煒 (2021 年 1 月 22 日)。數位身分證喊卡 先立專法再換-計畫暫緩 蘇揆：政府會謙卑反省 內政部：專法草案沒時間表。《聯合報》，第 A5 版。
- 戴敏琪 (2019 年 9 月 19 日)。嚴格監管！Facebook 成立獨立監督委員會審查平台內容。上網日期：2021 年 5 月 7 日，取自：<https://newtalk.tw/news/view/2019-09-19/300680>
- 鍾巧庭 (2020 年 12 月 10 日)。美國政府向 Facebook 提告！面臨反托拉斯訴訟戰 臉書恐忍痛出售 IG、WhatsApp。上網日期：2021 年 3 月 3 日，取自：<https://www.storm.mg/article/3284179>
- 簡恒宇 (2018 年 4 月 11 日)。各問各的、不熟臉書》44 位議員 5 小時「拷問」沒問出重點 參議院聽證會祖克柏安全下桌。上網日期：2019 年 10 月 24 日，取自：<https://www.storm.mg/article/423275>
- 顏嘉南 (2021 年 1 月 16 日)。Signal 下載次數 暴增 4,200%-WhatsApp 更改個資政策。《工商時報》。上網日期：2021 年 5 月 8 日，取自：<https://readers.ctee.com.tw/cm/20210116/a06aa6/1105960/96d759c41f61d613d0328abfb1355f97/share>
- 羅清俊 (2015)。《公共政策：現象觀察與實務操作》(初版)。新北：揚智文化。
- 羅鈺珊 (2018)。數據經濟下共融成長的挑戰：大數據的兩面刃。《經濟前瞻》，178，87-93。
- Facebook (2018 年 4 月 19 日)。資料政策。上網日期：2020 年 1 月 14 日，取自：<https://zh-tw.facebook.com/about/privacy/update>
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514. doi:10.1126/science.aaa1465
- American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, & Interactive Advertising Bureau. (2009, July). Self-Regulatory Principles for Online Behavioral Advertising. Retrieved June 19, 2020, from https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf

- Auxier, B., Rainie, L., Anderson, M., Perrin, A., & Kumar, M. (2019, November 15). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Retrieved April 1, 2021, from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf
- Barrett, C. (2020). Emerging Trends From The First Year Of EU GDPR Enforcement. *Scitech Lawyer*, *16*(3), 22-25,35.
- Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579-596.
doi:10.1177/1461444815614001
- Bernstein, M. H. (1955). *Regulating Business by Independent Commission*. Princeton, New Jersey: Princeton University Press.
- Bostoen, F. (2019). Online platforms and pricing: Adapting abuse of dominance assessments to the economic reality of free products. *Computer Law & Security Review*, *35*(3), 263-280. doi:10.1016/j.clsr.2019.02.004
- Bowcott, I. T. O. (2015, October 6). Facebook row: US data storage leaves users open to surveillance, court rules. Retrieved June 10, 2020, from <https://www.theguardian.com/world/2015/oct/06/us-digital-data-storage-systems-enable-state-interference-eu-court-rules>
- Bowie, N. E., & Jamal, K. (2006). Privacy Rights on the Internet: Self-Regulation or Government Regulation? *Business Ethics Quarterly*, *16*(3), 323-342.
doi:10.5840/beq200616340
- Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230.
doi:10.1111/j.1083-6101.2007.00393.x
- Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2019). Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy. *Social Science Computer Review*, *37*(4), 466-488. doi:10.1177/0894439318777706
- Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Computers in Human Behavior*, *101*, 1-13.
doi:10.1016/j.chb.2019.07.001
- Christensson, P. (2014, May 26). Digital Footprint Definition. Retrieved May 5, 2021, from https://techterms.com/definition/digital_footprint
- Christl, W. (2017a, June 8). Corporate Surveillance In Everyday Life (Web Version). Retrieved December 16, 2019, from <http://crackedlabs.org/en/corporate-surveillance>

- Christl, W. (2017b, October). How Companies Use Personal Data Against People. Retrieved January 1, 2020, from https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf
- Christl, W., & Spiekermann, S. (2016). *Networks of control: a report on corporate surveillance, digital tracking, big data & privacy*. Vienna: Facultas.
- Constine, J. (2019, January 29). Facebook pays teens to install VPN that spies on them. Retrieved October 24, 2019, from <https://techcrunch.com/2019/01/29/facebook-project-atlas/>
- Council of the EU, Presidency. (2021, February 10). Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)-Mandate for negotiations with EP. Retrieved April 29, 2021, from
- Cowen, T., & Glazer, A. (1996). More monitoring can induce less effort. *Journal of Economic Behavior & Organization*, *30*(1), 113-123. doi:10.1016/S0167-2681(96)00845-1
- Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, *20*(1), 88-104. doi:10.1177/1461444816657096
- Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing*, *19*(1), 20-26. doi:10.1509/jppm.19.1.20.16944
- Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). Measuring Cookies and Web Privacy in a Post-GDPR World. In D. Choffnes & M. Barcellos (Eds.), *Passive and Active Measurement* (Vol. 11419, pp. 258-270). Cham, Switzerland: Springer International Publishing. doi:10.1007/978-3-030-15986-3_17
- Davies, R., & Rushe, D. (2019, July 24). Facebook to pay \$5bn fine as regulator settles Cambridge Analytica complaint. Retrieved January 17, 2021, from <http://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint>
- Davis, K. E., & Marotta-Wurgler, F. (2019). Contracting for Personal Data Symposium. *New York University Law Review*, *94*(4), 662-705.
- Determann, L. (2012). Social Media Privacy: A Dozen Myths and Facts. *Stanford Technology Law Review*, (July), 1-14.
- Digital Advertising Alliance. (2011, November). Self-Regulatory Principles for Multi-Site Data. Retrieved June 19, 2020, from https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Multi-Site-Data-Principles.pdf

- Digital Advertising Alliance. (2013, July). Application of Self-Regulatory Principles to the Mobile Environment. Retrieved June 19, 2020, from https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_Mobile_Guidance.pdf
- Digital Advertising Alliance. (2015, November). Application of the DAA Principles of Transparency and Control to Data Used Across Devices. Retrieved June 19, 2020, from https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_Cross-Device_Guidance-Final.pdf
- Digital Advertising Alliance. (2018, May). Application of the DAA Principles of Transparency & Accountability to Political Advertising. Retrieved June 19, 2020, from https://aboutpoliticalads.org/sites/politic/files/DAA_files/DAA_Self-Regulatory_Principles_for_Political_Advertising_May2018.pdf
- Dixon, P. (2007, December 19). A Brief Introduction to Fair Information Practices. Retrieved May 22, 2020, from <https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>
- Duhigg, C. (2013). How Companies Learn Your Secrets. In D. Starkman (Ed.), *The Best Business Writing 2013* (pp. 421-444). New York: Columbia University Press. doi:10.7312/star16075-025
- Eisner, M. A., Worsham, J., & Ringquist, E. J. (2000). *Contemporary regulatory policy*. Boulder, Colorado: Lynne Rienner Publishers.
- European Data Protection Board. (2020, September 20). Guidelines 08/2020 on the Targeting of Social Media Users. Retrieved November 30, 2020, from https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_on_thetargetingofsocialmediausers_en.pdf
- European Parliament. (2021, March 20). Legislative train schedule. Retrieved April 29, 2021, from <https://www.europarl.europa.eu/legislative-train>
- Facebook. (2020a, March 30). Updating Our Data Access Tools. *About Facebook*. Retrieved July 14, 2020, from <https://about.fb.com/news/2020/03/data-access-tools/>
- Facebook. (2020b, June 2). Introducing Manage Activity. Retrieved April 2, 2021, from <https://about.fb.com/news/2020/06/introducing-manage-activity/>
- Facebook. (2020c, October 3). What 'The Social Dilemma' Gets Wrong. Retrieved November 13, 2020, from <https://about.fb.com/wp-content/uploads/2020/09/What-The-Social-Dilemma-Gets-Wrong.pdf>

- Facebook. (n.d.). General Data Protection Regulation. Retrieved July 14, 2020, from <https://en-gb.facebook.com/business/gdpr>
- Falahrastegar, M., Haddadi, H., Uhlig, S., & Mortier, R. (2016). Tracking Personal Identifiers Across the Web. In T. Karagiannis & X. Dimitropoulos (Eds.), *Passive and Active Measurement* (pp. 30-41). Cham, Switzerland: Springer International Publishing. doi:10.1007/978-3-319-30505-9_3
- Federal Trade Commission. (2012, August 10). FTC Approves Final Settlement With Facebook. Retrieved April 24, 2020, from <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>
- Federal Trade Commission. (2019, July 24). FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. Retrieved April 24, 2020, from <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>
- Fox, C. (2019, January 21). Google hit with £44m GDPR fine. Retrieved May 25, 2020, from <https://www.bbc.com/news/technology-46944696>
- Fuller, C. S. (2019). Is the market for digital privacy a failure? *Public Choice*, *180*(3), 353-381. doi:10.1007/s11127-019-00642-2
- G'sell, F. (2021, January 25). The Digital Markets Act Is Changing EU's Approach to Digital Gatekeepers. Retrieved April 29, 2021, from <https://promarket.org/2021/01/25/europe-digital-markets-act-new-approach-gatekeepers/>
- Gonçalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research*, *23*(2), 139-152. doi:10.1080/13669877.2018.1517381
- Graef, I., Clifford, D., & Valcke, P. (2018). Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law*, *8*(3), 200-223. doi:10.1093/idpl/ipy013
- Hirsch, D. D. (2011). The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? *Seattle University Law Review*, *34*(2), 439-480.
- Hoofnagle, C. J. (2005, March 4). Privacy Self Regulation: A Decade of Disappointment. Retrieved October 12, 2019, from <https://www.epic.org/reports/decadedisappoint.pdf>
- Hoofnagle, C. J. (2018). The Federal Trade Commission's Inner Privacy Struggle. In *The Federal Trade Commission's Inner Privacy Struggle* (pp. 168-183). Cambridge, United Kingdom: Cambridge University Press.

- Hoofnagle, C. J., & Whittington, J. (2014). Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, *61*, 606-670.
- Hu, X., & Sastry, N. (2019). *Characterising Third Party Cookie Usage in the EU after GDPR*. In Proceedings of the 10th ACM Conference on Web Science - WebSci '19 (pp. 137-141). Boston, MA. doi:10.1145/3292522.3326039
- Huber, P. (1983). Exorcists vs. Gatekeepers in Risk Regulation. *Regulation*, *7*(6), 23-32.
- ICO. (n.d.). What methods can we use to provide privacy information? ICO. Retrieved April 30, 2021, from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>
- Jackson, O. (2018a). GDPR implementation is harder than expected. *International Financial Law Review*. Retrieved March 24, 2020, from <https://search.proquest.com/docview/2137332713?accountid=10067>
- Jackson, O. (2018b). GDPR: on the right path? *International Financial Law Review*. Retrieved April 24, 2020, from <https://www-proquest-com.utorpa.lib.nccu.edu.tw/scholarly-journals/gdpr-on-right-path/docview/2045017398/se-2?accountid=10067>
- Johnson, G. A., Shriver, S. K., & Du, S. (2020). Consumer Privacy Choice in Online Advertising: Who Opt's Out and at What Cost to Industry? *Marketing Science*, *39*(1), 33-51. doi:10.1287/mksc.2019.1198
- Layton R. (2019, May 6). When evaluating California data regulation, don't forget the thousands of US firms no longer operating in the EU. *AEIdeas [Blog]*. Retrieved March 29, 2020, from <https://search-proquest-com.utorpa.lib.nccu.edu.tw/abicomplete/docview/2220520568/93191CA49D0B469EPQ/3?accountid=10067>
- Leon, P. G., Cranshaw, J., Cranor, L. F., Graves, J., Hastak, M., Ur, B., et al. (2012). *What do online behavioral advertising privacy disclosures communicate to users?* In Proceedings of the 2012 ACM workshop on Privacy in the electronic society (pp. 19-30). Raleigh, NC. doi:10.1145/2381966.2381970
- Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 47-64. doi:<https://doi.org/10.2478/popets-2020-0004>
- Lindsey, N. (2019, November 14). Another Facebook Privacy Breach, This One Involving Developers. Retrieved January 5, 2020, from <https://www.cpomagazine.com/data-privacy/another-facebook-privacy-breach-this-one-involving-developers/>

- Listokin, S. (2015). Industry Self-Regulation of Consumer Data Privacy and Security. *John Marshall Journal of Information Technology and Privacy Law*, 32(1), 15-32.
- Loo, R. V. (2019). The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance. *Vanderbilt Law Review*, 72(5), 1563-1632.
- Lopes, I. M., & Oliveira, P. (2018). Evaluation of the Implementation of the General Data Protection Regulation in Health Clinics. *Journal of Information Systems Engineering & Management*, 3(4), 28. doi:10.20897/jisem/3939
- Marotta-Wurgler, F. (2016). Understanding Privacy Policies: Content, Self-Regulation, and Markets. *SSRN Electronic Journal*. doi:10.2139/ssrn.2736513
- Marsden, C. (2018). Prosumer Law And Network Platform Regulation: The Long View Towards Creating OffData. *Georgetown Law Technology Review*, 2(2), 376-398.
- Momen, N., Hatamian, M., & Fritsch, L. (2019). Did App Privacy Improve After the GDPR? *IEEE Security & Privacy*, 17(6), 10-20. doi:10.1109/MSEC.2019.2938445
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*. In 2020 CHI Conference on Human Factors in Computing Systems. Honolulu. doi:10.1145/3313831.3376321
- Obar, J. A., & Wildman, S. (2015). Social media definition and the governance challenge: An introduction to the special issue. *Telecommunications Policy*, 39(9), 745-750. doi:10.1016/j.telpol.2015.07.014
- Papamiltiadis, K. (2020, July 1). Improving Data Limits for Infrequently Used Apps, Simplifying Platform Terms and Developer Policies. Retrieved July 13, 2020, from <https://about.fb.com/news/2020/07/improving-data-limits-simplifying-terms/>
- Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, 58, 132-145. doi:10.1016/j.irl.2019.03.007
- Press Association. (2019, March 30). Mark Zuckerberg calls for stronger regulation of internet. Retrieved May 20, 2020, from <https://www.theguardian.com/technology/2019/mar/30/mark-zuckerberg-calls-for-stronger-regulation-of-internet>

- Protti, M. (2020, April 24). Final FTC Agreement Represents a New Level of Accountability for Privacy. Retrieved July 13, 2020, from <https://about.fb.com/news/2020/04/final-ftc-agreement/>
- Punj, G. N. (2019). Understanding individuals' intentions to limit online personal information disclosures to protect their privacy: implications for organizations and public policy. *Information Technology and Management*, 20(3), 139-151. doi:10.1007/s10799-018-0295-2
- Robertson, V. H. S. E. (2019). *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data* (SSRN Scholarly Paper No. ID 3408971). Rochester, NY: Social Science Research Network. doi:10.2139/ssrn.3408971
- Salla, A. (2020, December 21). Changes to Facebook Messaging Services in Europe. Retrieved March 14, 2021, from <https://about.fb.com/news/2020/12/changes-to-facebook-messaging-services-in-europe/>
- Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. A., et al. (2019). *Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control*. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (pp. 340-351). Auckland, New Zealand. doi:10.1145/3321705.3329806
- Satariano, A. (2020, April 27). Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates. Retrieved May 11, 2020, from <https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html>
- Seneviratne, S., Kolamunna, H., & Seneviratne, A. (2015). *A measurement study of tracking in paid mobile applications*. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '15 (pp. 1-6). New York. doi:10.1145/2766498.2766523
- Sirur, S., Nurse, J. R., & Webb, H. (2018). *Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)*. In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (pp. 88-95). Toronto. doi:<https://doi.org/10.1145/3267357.3267368>
- Solove, D. J., & Schwartz, P. M. (2018). *Information privacy law* (Sixth edition.). New York: Wolters Kluwer.
- Sonderby, C. (2020, November 19). Our Continuing Commitment to Transparency. Retrieved March 14, 2021, from <https://about.fb.com/news/2020/11/biannual-transparency-report/>

- Soros, G. (2020, February 18). George Soros: Remove Zuckerberg and Sandberg from their posts. *Financial Times*. Retrieved May 20, 2020, from <https://search-proquest-com.utorpa.lib.nccu.edu.tw/abicomplete/docview/2357116426/F50BD8968FB24694PQ/1?accountid=10067>
- Stapp, A. (2019, May 24). GDPR After One Year: Costs and Unintended Consequences. *Truth on the Market[Blog]*. Retrieved March 29, 2020, from <https://search-proquest-com.utorpa.lib.nccu.edu.tw/abicomplete/docview/2248463460/2979A70777994DEAPQ/2?accountid=10067>
- Stupp, C. (2020, March 16). Brussels Report: Frustrated European Regulators Seek Tweaks to GDPR. *Dow Jones Institutional News*. Retrieved March 26, 2020, from <https://search.proquest.com/docview/2377571497?accountid=10067>
- Szakacs, G., & Fincher, C. (2019, December 6). Hungary watchdog fines Facebook for misleading users. Retrieved January 17, 2020, from <https://www.reuters.com/article/us-facebook-hungary-fine-idUSKBN1YA24X>
- Tidd, M. (2018). Who will protect us from the data protection workload?(headteachers' responsibility in implementing the General Data Protection Regulations) (Column). *Times Educational Supplement*, (5295), 29.
- TrustArc. (n.d.). TRUSTe Privacy Certification and Assurance Services. Retrieved June 4, 2020, from <https://trustarc.com/truste-certifications/>
- Tsui, L., & Hargreaves, S. (2019). Who Decides What Is Personal Data? Testing the Access Principle with Telecommunication Companies and Internet Providers in Hong Kong. *International Journal of Communication*, 13, 1684-1698.
- U.S. Department of Justice. (2015, June 27). Overview of the Privacy Act of 1974 (2015 Edition). Retrieved July 10, 2020, from <https://www.justice.gov/opcl/introduction>
- US Senate Committee on Commerce, Science, and Transportation. (2013, December 18). A Review of The Data Broker Industry: Collection, Use, And Sale of Consumer Data for Marketing Purposes. Retrieved January 1, 2020, from http://educationnewyork.com/files/rockefeller_databroker.pdf
- Vestager, M. (2021, March 17). Competition in a digital age. *European Commission*. Text. Retrieved April 29, 2021, from https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/competition-digital-age_en
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220.
- Wood, A. K., & Ravel, A. M. (2018). Fool Me Once: Regulating “Fake News” and Other Online Advertising. *Southern California Law Review*, 91(6), 1223-1278.

- Yuan, B., & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Environmental Research and Public Health*, *16*(6), 1070. doi:10.3390/ijerph16061070
- Zuckerberg, M. (2020, February 16). Mark Zuckerberg: Big tech needs more regulation. *FT.Com*. Retrieved May 20, 2020, from <https://search-proquest-com.utorpa.lib.nccu.edu.tw/docview/2355765716?accountid=10067>
- Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., & Helberger, N. (2017). Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review*, *3*(3), 353-368. doi:10.21552/edpl/2017/3/9





附錄 個別受訪者訪談大綱

個別訪談知情同意書（受訪者 A1）³⁰ （敬致某機關 000）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

揣此，本研究擬透過一對一深度訪談方式，希望了解公民團體對於業者利用數位足跡所衍生的議題、採取之保護措施，以及政府所扮演監理角色的評價，希望借用您約一個小時的時間。

詳細研究摘要與說明請參考附件一，附件二則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxx

信箱：xxxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____ 日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____ 日期：_____年_____月_____日

30 基於去識別化考量，本（含接下來）訪綱之姓名呈現與實際訪綱略有不同。

個別訪談知情同意書（受訪者 A2）
（敬致：某資訊公民團體 000 律師）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，探討以法務人員的觀點，如何協助業者應對個人資料保護相關法令的要求，以及與主管機關互動可能遇到的困難，倘若情況允許，也麻煩您兼從公民參與的觀點來討論，所需時間約為一個小時。

詳細研究摘要與說明請參考附件一，附件二則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxxx

信箱：xxxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____ 日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____ 日期：_____年_____月_____日

個別訪談知情同意書（受訪者 A3）

（敬致：某資訊公民團體 000）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，訪談內容主要聚焦在以資訊公民團體的立場，如何看待業者的作為，以及政府的監理政策等，當然還有可能遇到的困難，所需時間約為一個半小時。

詳細研究摘要與說明請參考附件，附件一，附件二為歷次訪談成果的摘要、附件三則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxx

信箱：xxxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____日期：_____年_____月_____日

個別訪談知情同意書（受訪者 B1、B2）
（敬致：某法律事務所 OOO 律師、OOO 律師）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，探討法務人員如何協助業者應對個人資料保護相關法令的要求，以及與主管機關互動可能遇到的困難，所需時間約為一個小時。

詳細研究摘要與說明請參考附件一，附件二則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxxx

信箱：xxxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____ 日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____ 日期：_____年_____月_____日

個別訪談知情同意書（受訪者 B3）
（敬致：已離職某平台業者 000）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，探討業者應對個人資料保護相關法令的要求，以及與主管機關互動可能遇到的困難，所需時間約為一個半小時。

詳細研究摘要與說明請參考附件一，附件二則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxx

信箱：xxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____日期：_____年_____月_____日

個別訪談知情同意書（受訪者 C1）
（敬致：國發會某單位 000）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，探討貴機關制定現行法令授權監理社群網站業者利用使用者瀏覽行為資料的情形，以及可能遇到的困難，所需時間約為一個半小時。

詳細研究摘要與說明請參考附件一，附件二為歷次訪談成果的摘要、附件三則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxx

信箱：xxxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫

研究者簽名：_____日期：_____年_____月_____日

個別訪談知情同意書（受訪者 D1）
（敬致：某大學系所 000 教授）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，探討專家學者對於現行業者自律行為，與主管機關執行個人資料保護相關措施的評價，及可能遇到的困難，所需時間約為一個半小時。

詳細研究摘要與說明請參考附件一，附件二則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxx

信箱：xxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____ 日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____ 日期：_____年_____月_____日

個別訪談知情同意書（受訪者 D2）
（敬致：某大學系所 000 教授）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，探討專家學者對於現行業者自律行為，與主管機關執行個人資料保護相關措施的評價，及可能遇到的困難，所需時間約為一個半小時。

詳細研究架構摘要與說明請參考附件一，附件二為歷次訪談成果的摘要、附件三則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxx

信箱：xxxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____日期：_____年_____月_____日

個別訪談知情同意書（受訪者 E1）
（敬致：OOO）

敬愛的受訪者您好：

我是國立政治大學公共行政系碩士班研究生陳柏安。目前正在本系蕭乃沂副教授指導下，撰寫學位論文《社群網站運用數位足跡的監理策略探討》。

近來社群網站業者運用使用者瀏覽行為資料，投放針對式廣告的經營手法，及可能伴隨的弊害（如使用者行為與偏好的操弄）引起廣泛注意。我國也正在師法國際經驗，試圖發展出能保護使用者的監理策略，但是顯見許多困難之處。本論文旨在以政策工具與執行為焦點，探討可能改進之道。

崙此，本研究擬透過一對一深度訪談方式，煩請您以個人資料洩漏事件受害者的觀點，探討業者利用數位足跡所衍生的議題、採取之保護措施，以及政府所扮演監理角色的相關議題，所需時間約為一個小時。

詳細研究摘要與說明請參考附件一，附件二則為本研究之訪談大綱。為記錄正確的資料，訪談過程擬全程錄音。如果您不願意錄音、不願某段發言列入紀錄，甚至中途想停止，請隨時提出，本研究將恪遵學術倫理以匿名處理受訪者的基本資料與相關錄音內容。錄音資料將會彙整成為逐字稿以供分析，筆者事後也會寄送研究成果之電子檔供您參閱與確認，再次感謝您的協助！

國立政治大學公共行政學系

研究生 陳柏安 敬上

聯絡資訊

手機：09xx-xxxxxxx

信箱：xxxxxxxxx@nccu.edu.tw

研究參與者簽署欄：

錄音：同意 不同意

成果回饋：無需 研究完成請提供報告，傳至電子信箱：

受訪者簽名：_____ 日期：_____年_____月_____日

研究人員簽署欄：

本同意書一式兩份，將由雙方各自留存，以利日後聯繫。

研究者簽名：_____ 日期：_____年_____月_____日

附件一 研究摘要與說明³¹

本研究旨在找出政策規劃與執行之間可能的失落環節，主要聚焦於法規命令³²確立後，如何被主管機關執行與業者遵守、執行成果為何，以及反饋至現有的監理機制。若以監理政策過程先立法、後執行與評估的階段論邏輯來理解，現行監理策略的整體樣貌，可理解為各環節相互反饋所組成的迴路系統，以及內部各行動者之間的競合關係（圖 1）。

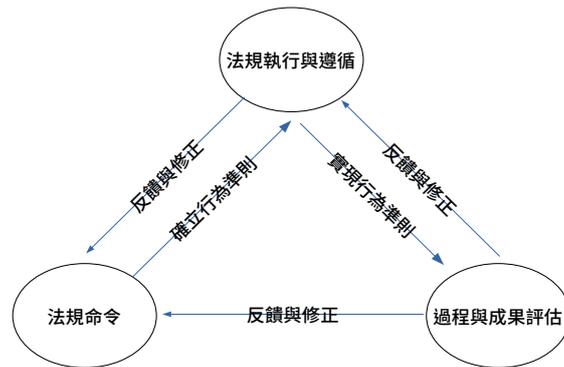


圖 1：監理策略的整體樣貌

法規執行與遵循的過程，則理解為政府與業者之間的較勁（如圖 2）。基於自利的人性假設，政府有足夠的執法與查緝能力，是業者遵守法令的主要前提，否則業者將推諉以待，政府執行能力則取決於關鍵資源充裕與行政程序明確的程度。儘管已有文獻從理論層次探討上述資源不足，導致政府的執法效率低落，但是事實層次的討論，如主管機關在現實生活中如何執法、擁有或利用了哪些科技工具，過程遭遇了什麼困境等，則欠缺著墨。附件二設計的一系列訪談大綱，便旨在解答這些問題，並尋求可能的改進之道。

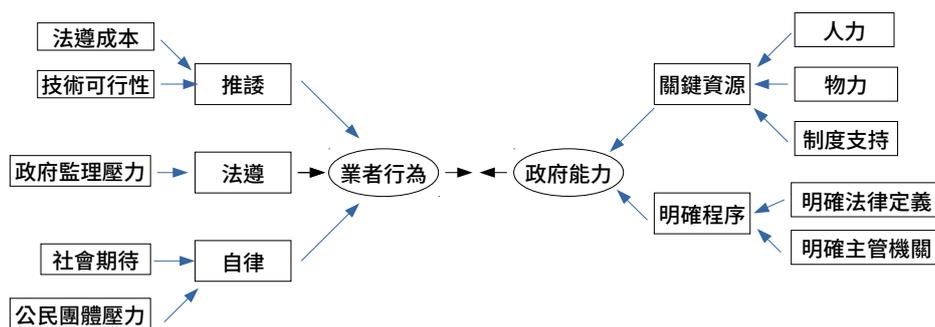


圖 2：執行面各行為者組成與策略

31 所有受訪者均有拿到這份附件。

32 於論文正文後來修訂為「法令規範」，唯本處為呈現已發出的訪綱，仍保留該用詞。

附件二 《社群網站運用數位足跡的監理策略探討》訪談進度摘要³³

自研究計畫書通過審查為止，已進行 5 次深度訪談（6 位受訪者），每次用時約 2 小時。受訪者屬性有業者委任律師、公民團體、個資外洩事故受害者與學術單位等。茲摘要各受訪者論述重點如下：

1. 對於業者利用數位足跡的疑慮：
 - (1) 對使用者體驗（user experience, UX）的損害。
 - (2) 跨網站追蹤時損害使用者資料自主權。
 - (3) 使用者對於自動化決策未能充份知情。
 - (4) 自動化決策助長社會意見的極化。
 - (5) 劍橋分析事件後雖有廣告用於政治作戰的疑慮，然而實際效果仍有待更多檢證。
2. 雖然業者代表聲稱已厲行個資保護，且完整做到現行法遵所需內容。該論點也無可避免地受到一面倒的批評，主要為：
 - (1) 現行使用者條款通例看似完整履行告知義務，但是第一是幾乎無效的溝通模式，第二是難以落實資料自主權的最終目標。
 - (2) 業者未能提出比法遵更高標準的自律措施，自律措施因而缺乏意義。
 - (3) 即使在現行法遵架構下，業者資料外洩事故仍然頻傳，進而失信於使用者。
 - (4) 業者之措施幾乎皆是事發或受罰過後才提出，而被質疑其誠意。
 - (5) 迫於保密原則，受訪業者代表無法透露業者執行保護措施的相關細節，只能論述性地聲稱已符合相關國際規範。也讓業者論述更難有說服力。
3. 對政府主導監理策略的質疑：
 - (1) 國內雖已有個人資料保護法令，無法確知該法第 22 條之行政檢查權如何被履行，及相關具體事例，更幾乎無開罰紀錄。
 - (2) 現有個資法 20 條之 6 存在嚴重缺陷，「對當事人有利」成為業者使用個資的免死金牌。限期改善條款亦有類似問題。
 - (3) 所有受訪者都指出缺乏專責主管機關造成事權不集中的問題。社群網站迄今也無明確主管機關。（我們也去做了功課，發現似乎不是工業局的知識服務組）
 - (4) 現行政策架構下，各主管機關重視產業推動甚於監理業務，且兩業務之間存在明顯角色與利益衝突。
 - (5) 政府缺乏足夠專業人力，即使是在政府內部，機關也未必能履行法定法遵義務，而常虛應故事。

33 只有受訪者 A3、受訪者 C1、受訪者 D2 有拿到這份摘要。

- (6) 政府平常已大量運用社群網站，進行輿情分析與政策宣導，政府也更難有誘因落實監理（也等於默許甚至支持該商業模式繼續存在）。
 - (7) 台灣迫於國際現實，難以成為遊戲規則制定者，即使訂立相關法令，業者也可能難有遵守的意願。有人主張台灣應該還是要做，不能因噎廢食；但也有人主張應該是讓公民團體位居主導角色，聯合國際相關組織施壓業者。
 - (8) 公民團體未對由政府主導的監理，表示明確的反對意見。對於政府的質疑也主要在管制能力是否足夠，而非可能伴隨的通訊監察等疑慮。
4. 筆者也關心管制政策可能造成的負面影響，特別是廣告產業的加劇化（境外文獻也有類似批評）。目前得到幾種不同的意見：
- (1) 大者恆大是網路產業行之有年的生態，非專業者也難以確證管制政策加劇產業集中化的因果關係。
 - (2) 業者面對法遵應有新的思維，不能停留在過去的日子裡。也不能因為營業成本墊高而與資安等價值妥協。
 - (3) 也有人質疑即使政策出台，也可能只管得到國內的業者，甚至衝擊新創產業。
 - (4) 由於目前尚未有具體的管制政策出台，至少對於台灣業者而言也可能言之過早。且本地多數廣告業務為境外業者所承攬。
 - (5) 也有人主張 GDPR 的裁罰基準，主要目的是確保業者有合理的資安投資，且對於中小企業也有設定相應的比例原則，而仍有其正當性。但是具體實施情況與造成衝擊仍需更多檢證。

附件二 訪談題目（受訪者 A1）

一、 基本資料

請簡單介紹您的職業，與推動資訊人權的相關經驗及見聞，亦可談談您對現行實務的看法。

二、 以下題目，請就您所知與參與之經驗進行回答。

- （一） 您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
- （二） 您認為業者對此採取了哪些措施？這些措施足夠嗎？業者還應該做哪些事情，以減少民眾的恐懼或疑慮？
- （三） 您觀察到政府機關採取了哪些措施？您對政府的作法滿意嗎？政府採取的措施是否造成了哪些（未預期）的後果？
- （四） 您認為現行的監理策略，哪些地方還可能做得更好？



附件二 訪談題目（受訪者 A2）

一、 基本資料

請簡單介紹您的職業，與輔助業者法遵的相關經驗及見聞，亦可談談您對現行實務的看法。

二、 以下題目，請就您所知與參與之經驗進行回答。

- (一) 您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
- (二) 據您所知，業者對於上述問題採取了哪些自律措施？在法遵過程中做了哪些努力？您對於業者採取的行動感到滿意嗎？
- (三) 您觀察到政府機關採取了哪些措施？對此您感到滿意嗎？政府採取的措施是否造成了哪些（未預期）的後果？
- (四) 您認為現行的監理策略，哪些地方還可能做得更好？



附件三 訪談題目（受訪者 A3）

一、 基本資料

請簡單介紹您的職業，與相關撰稿經驗及見聞，亦可談談您對現行實務的看法。

二、 以下題目，請就您所知與參與之經驗進行回答。

- (一) 您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
- (二) 您如何看待使用者對業者採取之資料保護措施的質疑？業者還應該做些什麼，方可能降低使用者疑慮？政府對此能提供業者哪些協助？
- (三) 政府在監理社群網站運用使用者數位足跡的過程中遭遇哪些困難？根本的原因可能有哪些？哪些地方還可能做得更好？
- (四) 有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？



附件二 訪談題目（受訪者 B1、受訪者 B2）

一、 基本資料

請簡單介紹您的職稱以及輔助業者法遵的業務內容。

二、 以下題目，請就您所知與參與之經驗進行回答。

- （一） 您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
- （二） 據您所知，業者對於上述問題採取了哪些自律措施？又如何將個人資料保護相關法令的要求，融合於日常作業的實務中？遇到哪些困難？
- （三） 您認為現行的監理策略造成了哪些未預期的後果，不論是對業者或民眾？
- （四） 您認為現行的監理策略，哪些地方還可能做得更好？



附件二 訪談題目（受訪者 B3）

一、 基本資料

請簡單介紹您的職稱以及主要業務內容。

二、 以下題目，請就您所知與參與之經驗進行回答。

- (一) 您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？
- (二) 從同業的角度，您如何看待這些大型平台業者採取的自律與法遵措施？對於外界對於業者的質疑，您會如何看待與回應？政府對此能提供業者哪些協助？
- (三) 您如何看待政府監理社群網站運用使用者數位足跡的過程的措施？哪些地方還可能做得更好？
- (四) 有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？



附件三 訪談題目（受訪者 C1）

一、 基本資料

請簡單介紹您的職稱以及主要工作內容。

二、 以下題目，請就您所知與參與之經驗進行回答。

- (一) 您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？這些問題如何影響個資保護的相關立法？
- (二) 您希望個資保護相關法令能達到哪些目標？您認為現行法令符合您的期望嗎？您對於目前社群網站所採取之資料保護措施看法為何？
- (三) 許多人主張應設立個資法的專責主管機關。請問您對於這件事的想法為何？這可能會對政府的組織架構造成哪些影響？
- (四) 政府在監理社群網站運用使用者數位足跡的過程中還遭遇哪些困難？根本的原因可能有哪些？哪些地方還可能做得更好？



附件二 訪談題目（受訪者 D1）

一、 基本資料

請簡單介紹您的職稱以及研究社群網站議題的相關經歷。

二、 以下題目，請就您所知與參與之經驗進行回答。

- （一） 您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？
- （二） 您對於目前社群網站所採取之資料保護措施看法為何？業者還應該做些什麼，方可能降低使用者疑慮？
- （三） 您希望個資保護的相關法令能達到哪些目標，現狀符合您的期望嗎？您認為政府在監理社群網站運用使用者數位足跡的過程中遭遇哪些困難？哪些地方還可能做得更好？
- （四） 有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？



附件三 訪談題目（受訪者 D2）

一、 基本資料

請簡單介紹您的職稱以及研究社群網站議題的相關經歷。

二、 以下題目，請就您所知與參與之經驗進行回答。

- （一） 您最關心社群網站（例如 Facebook、YouTube 等）哪些利用使用者瀏覽行為資料的可能方式？及其對使用者造成的影響？
- （二） 您如何看待使用者對業者採取之資料保護措施的質疑？業者還應該做些什麼，方可能降低使用者疑慮？政府對此能提供業者哪些協助？
- （三） 政府在監理社群網站運用使用者數位足跡的過程中遭遇哪些困難？根本的原因可能有哪些？哪些地方還可能做得更好？
- （四） 有論者認為嚴格的個資保護法令加劇了網路廣告產業的集中化，您如何看待此說法？對於網路廣告產業的集中化，我們能如何回應？



附件二 訪談題目（受訪者 E1）

一、 基本資料

請簡單介紹您的背景，與洩密事件的相關經驗及見聞，亦可談談您對現行實務的看法。

二、 以下題目，請就您所知與參與之經驗進行回答。

- （一） 您認為社群網站（例如 Facebook、YouTube 等）可能利用使用者的瀏覽行為資料做什麼事？對使用者可能造成哪些問題？
- （二） 據您所知，業者對於上述問題採取了哪些自律措施？在法遵過程中做了哪些努力？您對於業者採取的行動感到滿意嗎？
- （三） 您觀察到政府機關採取了哪些措施？對此您感到滿意嗎？政府採取的措施是否造成了哪些（未預期）的後果？
- （四） 您認為現行的監理策略，哪些地方還可能做得更好？

