國立政治大學公共行政學系

碩士學位論文

e 管家還是 e 管區？數位身分識別證下的隱私計算

Convenience or Surveillance?
Privacy Calculus Model for New eID Policy

指導教授：黃東益 博士

研究生：黃宗賢

中 華 民 國 109 年 4 月

DOI:10.6814/NCCU202000421

National Chengchi University

Department of Public Administration

Master's Thesis

Convenience or Surveillance?

Privacy Calculus Model for New eID Policy

Advisor: Dr. Tong-yi Huang

Graduate Student: Zong-Xian Huang

April 2020

DOI:10.6814/NCCU202000421

謝辭

謝辭是這篇論文寫作順序上的最後一章，卻放在了開頭，就好比資訊隱私與eID是我初入研究所很早期就接觸到的議題，但卻放在了最後。論文寫作過程就好似在思想的流沙當中，嘗試打撈出碎片般的珍珠，拼拼湊湊企求回應點什麼，當然其中不乏刺人的粗礪，在此也請本文的讀者加以見諒。

謝謝黃東益老師在過程中給予我全然的信任與殷切的關懷，除了在論文上的指導外，也點醒了我對研究所生活與人生規劃上的許多迷霧，能夠在政治大學遇見您，是我的幸運。蕭乃沂老師與黃婉玲老師在計畫書與學位論文口試上的評論與溢美，也同樣是本文作成不可或缺的部分，感謝兩位老師提出許多精闢的觀點與建議，讓本文得以更加完整。除了指導老師與口試委員之外，在政治大學公共行政所就學期間，謝謝顏良恭老師、朱斌妤老師、陳敦源老師、莊國榮老師與董祥開老師在課程上的養分，都著實令我獲益良多、不勝感激。

三年多來在政治大學遇見許多的人，若要一一寫出則難免顧此失彼，請容我用「分組」方式表達我的感謝。謝謝電子治理研究中心作為我研究的起點、謝謝選舉研究中心作為我蹲馬步的訓練場、謝謝中研院計量營作為我學術夢的前言、謝謝TY Lab 8F研究室作為我永遠都找得到鑰匙的避風港。當然，還有好多好多，像是一直保持理想的校本部夥伴、永遠能都再摸一將的麻將聯盟等等，謝謝你們。

我也要謝謝我的父親、母親、妹妹郁綺與弟弟柏豪，謝謝你們諒解我這幾年來的自私與未盡的義務，我對你們的感謝勝過一切。謝謝向怡多年來的支持，我既無法預測股價、也沒辦法預知未來，但唯一可以肯定的是，我們共同經歷的那些。最後，我將這段話留給自己，學術路是孤單、寂寞的良心事業，我現在也不知道這條路上是丟失的多、還是拾起的多。但願你看到這段話時，已經足夠智慧到，能夠泛起一絲富含深意的微笑。

DOI:10.6814/NCCU202000421

摘要

民眾授權個人資料的意願，是個人資料自主管理（MyData）政策成敗的關鍵。本研究以數位身分識別證政策為個案，應用隱私計算模型分析個人資料授權意願背後的隱私因素，採用偏最小平方法結構方程式（PLS-SEM）來探索數位身分識別證議題上，民眾在利益與風險間的權衡，並經由政治大學選舉研究中心建置的「線上調查實驗室」（PollcracyLab）進行資料蒐集。

本研究發現財務報償、個性化服務與服務兼容性都有助於提高民眾的隱私利益認知，而隱私利益認知則進一步會提高授權個人資料的意願；然而，隱私風險認知並不會影響民眾透過數位身分識別證授權個人資料的意願，代表民眾對隱私所帶來的風險有過多的忽視。本研究援引了行為經濟學、隱私悖論與遲滯性風險的觀點，探討了導致此認知缺口的可能邏輯。

本研究側面印證了臺灣是一個「遲滯型高科技風險社會」的推論，在具高度不確定性的科技議題上，民眾可能低估了潛在的隱私危害，並高估了預期效益。未來推動數位身分識別證的決策者，應跳脫僅以民意調查作為決策參考的思維，嘗試納入多元的決策機制於政策過程之中。最後，本研究討論了納入調節變項與高階構念等模型修正策略，以及建議未來研究者可以透過入選機率調整法（Propensity Score Adjustments）與實驗設計（experimental design）等方法修正調查方法上的偏誤。

關鍵詞：數位治理、數位身分識別證、隱私計算、科技風險、結構方程式、My Data

DOI:10.6814/NCCU202000421

Abstract

The success or failure of the MyData policy depends on citizens' willingness to authorize their personal data. This study applied privacy calculus model on the case of national electronic identification card (New eID) policy to analyze privacy factors which affect personal data disclosure intention. Partial Least Squares Structural Equation Modeling (PLS-SEM) was used to explore how citizens balance benefits and risks associated with the New eID issue. Research data were collected from PollcracyLab affiliated by Election Study Center of National Chengchi University (NCCU).

The study concludes that financial compensation, personalized services, and service compatibility can enhance cognition of privacy-related benefits of citizens, while this cognition will further promote their willingness to authorize their personal data. Citizens' cognition of privacy-related risks, however, has no statistical effect within the model, and shows that citizens excessively neglect privacy-related risks. The perspective of behavioral economics, privacy paradox and delayed risk are cited in this study, to demonstrate the abovementioned cognitive gap.

This study verifies the inference that Taiwan consists of a “Delayed High-tech Risk Society”. In technology issues with high uncertainties, citizens may underestimate the potential privacy-related risks, and overrate expected benefits. Therefore, policy makers in charge of implementing the New eID policy should incorporate diversified decision-making mechanisms into their policy process, and avoid taking opinion polls as the only reference.

Finally, this study discusses model revising strategies such as adopting moderator variables and higher-order components. Future researchers are also recommended to correct survey method bias by such approaches as Propensity Score adjustments and experimental design.

Keywords: Digital Governance, New eID, Privacy Calculus, High-tech Risk, Structural Equation Modeling, MyData

DOI:10.6814/NCCU202000421

目次

第一章　緒論 1

第一節　研究動機與背景 1

第二節　研究問題與目的 3

第三節　研究對象、途徑與流程 5

第二章　文獻檢閱 7

第一節　個人資料在數位治理的意涵 7

第二節　個人資料揭露意向 15

第三節　隱私計算模型的發展 22

第四節　隱私情境的影響 28

第三章　研究設計 39

第一節　研究架構與研究假設 39

第二節　變項操作化 41

第三節　資料蒐集流程 45

第四節　統計方法：PLS-SEM 46

第四章　資料分析 47

第一節　敘述統計 47

第二節　測量模型的統計結果與評估 53

第三節　結構模型的統計結果與評估 63

第四節　小結：模型之外的故事 74

第五章　結論 83

第一節　研究發現與理論意涵 83

第二節　政策建議 84

第三節　研究限制 88

第四節　研究建議 89

DOI:10.6814/NCCU202000421

第五節　研究貢獻 90

參考文獻 92

附錄一 問卷設計 108

附錄二 次數分配表 112

附錄三 控制變項重新編碼表 128

DOI:10.6814/NCCU202000421

表次

表 1 研究假設 40
表 2 問卷構面與操作性定義 42
表 3 樣本基本資料表 48
表 4 測量變項敘述統計表 51
表 5 反映性指標檢驗結果表 57
表 6 Fornell-Larcker 指標 60
表 7 形成性指標檢驗結果表 63
表 8 結構模型結果摘要表 72
表 9 研究假設檢證表 74
表 10 修正後結構模型結果摘要表 80

DOI:10.6814/NCCU202000421

圖次

圖 1 研究架構 40
圖 2 結構模型路徑分析圖 72
圖 3 風險計算中的調節效果 76
圖 4 隱私計算中的調節效果 77
圖 5 修正後結構模型路徑圖 79

DOI:10.6814/NCCU202000421

第一章　緒論

本研究將探討民眾對於數位身分識別證（New eID）的隱私認知，以及分析影響民眾授權個人資料意願的因素。緒論將先說明本研究的研究動機與背景，並在研究問題章節針對本研究重要的概念進行綜覽性地介紹，其次說明本研究目前規劃的研究流程與對象，最後說明本研究的預期貢獻。

第一節　研究動機與背景

隨著近年來私人企業或公共組織越加重視資料驅動（data-driven）的決策流程，資料治理（data governance）領域開始關注如何透過個人資料的加值應用（value-added reuse）來創造價值（余孝先、趙祖佑，2015; Bhansali, 2013）。我國晚近的數位治理研究亦開始探討如何透過政府資料來創造額外的價值（蕭乃沂、朱斌妤，2018）；其中，透過個人資料自主管理（MyData）機制來提供個人化服務，被認為是下一世代政府數位服務的創新里程碑（顧振豪，2016）。基於上述個人化數位服務發展的需求，國家發展委員會於2019年所核定的「智慧政府推動策略計畫」中，揭示未來我國政府需積極應用數位身分識別來串連各部會業務資料，以便更主動地為民眾提供個性化服務（國家發展委員會，2019）。行政院在2019年6月更進一步核定了數位身分識別證換發計畫，將數位身分識別證定調為未來智慧政府的使用金鑰，可結合社會福利、交通監理、動產交易與公投連署等16項個人化數位服務。然而，該政策最富爭議性與受到質疑的焦點之一，即在於民眾對於個人資料揭露（personal data disclosure）上的隱私疑慮。

民眾的隱私自主權是數位身分識別證的主要爭點之一，許多人權團體擔心數位身分識別證的換發，將導致民眾過度揭露個人資訊，使得政府從無微不至的裨

DOI:10.6814/NCCU202000421

姆，轉變為無孔不入的老大哥。但不可否認的是，環諸多個世界上資通訊建設齊全的先進國家，未來政府線上服務的發展策略，勢必將會更重視民眾對個人化資料庫的自主管理與授權（蕭乃沂、陳恭、郭昱瑩，2017）。因此對民眾而言，願意揭露多少程度的個人資料給予服務提供的機關？什麼因素會影響個人資料揭露的意願？民眾如何權衡隱私上的利益與風險？以上這些問題目前尚缺乏國內數位治理或電子化政府研究領域的關切與討論，也是我國政府未來持續推動數位身分識別證時亟需探討的重要議題。

在資訊社會快速發展之下，因現代科技所衍生的科技風險已然成為風險社會中的一個要角（周桂田，2015）。民眾需要透過風險感知（risk perception）、風險評估（risk assesment）與風險管理（risk management）等三個階段來處理不同的風險，因此瞭解民眾與知識社群的風險認知與風險感知，是發展風險管理策略的關鍵（蕭新煌、徐世榮、杜文苓，2019：4-21）。較為可惜的是，現有國內的數位治理研究領域，尚未充分探討未來換發數位身分識別證後所可能產生的隱私風險與民眾對該政策的風險認知。

我國現有關於數位治理下隱私權研究的主軸，仍過度著重於法律條文的規範性分析，而缺乏實證資料的檢證與討論。雖然有部分學者依據世界網路計畫（world internet project，簡稱WIP）的跨國指標發展出主觀調查問卷，來衡量民眾對隱私的主觀認知（可參見李仲彬等人，2017；黃東益等人，2018；廖興中等人，2019），但目前的實證研究多止步於描述性分析而缺乏完整的模型分析與推論。本研究認為，隨著未來個人化數位服務與個人資料庫的建置，隱私研究會逐漸成為數位治理中不可或缺的環節；透過理解民眾對個人資料隱私的認知機制，將有助於未來數位身分識別政策推動時，行政流程的管理規劃與再造。基此，本研究以數位身分識別證作為研究標的，探討影響民眾個人資料授權意願的因素。

DOI:10.6814/NCCU202000421

第二節 研究問題與目的

許多電子商務領域的研究指出，個人資訊揭露意願與資訊隱私關切程度間的關聯密不可分（Li, 2012; Smith, Dinev, & Xu, 2011）。例如隱私計算理論（privacy calculus theory）認為個人資訊揭露與隱私關切兩者間係為一種交換關係（trade-off），強調個人會評估服務所可能帶來的效益與隱私風險後，經由成本效益分析後決定個人資訊揭露的意願（Dinev & Hart, 2006; Stone & Stone, 1990）。更進一步說明，隱私計算理論當中包含隱私風險（privacy risk）與隱私效益（privacy benefit）兩項構念，其中隱私風險代表個人資訊被企業洩露所可能帶來的損失與風險，隱私利益則代表個人揭露資訊後所能得到的個人化與經濟效益，而個人評估該服務可能的隱私風險越高或隱私效益越低，則資訊揭露意願則會越低(Smith et al., 2011）。

在隱私計算理論的基礎下，Li（2012）應用了Rogers（1975）所提出的保護動機理論（protection motivation theory），將隱私計算模型進一步擴張為二元計算模型（dual-calculus model）。Li認為隱私計算模型中的隱私風險可以進一步區分為風險評價（risk appraisal）與應對評價（coping appraisal），也就是說，隱私計算模型中的隱私風險除了該資訊洩露可能帶來的淨風險之外，同時也需考量個人應對風險的機制與能力（coping mechanism），意即個人對於隱私控制的自我效能感有助於使其平衡隱私威脅，自覺隱私保障能力較高的使用者較可能從事更高風險的數位交易行為。較為可惜的是，Li（2012）的研究僅提出相應的概念框架而尚缺乏足夠的實證資料驗證。

如前所述，上列有關隱私計算模型的討論與研究幾乎都是集中於強調高度個人化服務（personalized services）的電子商務（e-commerce）領域，使用者擔心個人資料在許可範圍之外被不當的蒐集與運用，而選擇揭露錯誤或是不完整的資

DOI:10.6814/NCCU202000421

料給予提供服務的企業（Sheng, Nah, & Siau, 2008）。然而，該模型在電子化政府或數位治理內的應用則相當稀少（Carter & McBride, 2010）。本研究認為隨著政府持續推展個人化數位服務與數位身分識別等政策，數位治理領域內隱私研究的重要性將與時俱增，也會更加凸顯學術界與實務界對隱私計算分析架構與實證應用的需求。

值得注意的是，資訊隱私研究無法忽略情境（context）帶來的影響，不同情境會對於隱私模型產生調節或是直接影響的效果（Smith et al., 2011: 1002-1003）。有別於數位商務領域，本研究認為當隱私計算模型應用於數位治理領域時，政府信任感（government trust）、政府監控疑慮（government surveillance concern）與政府配套措施等概念應被納入原有隱私計算模型之中。以政府監控疑慮這項概念為例，Dinev、Hart與Mullen（2008）發現民眾對政府侵害（government intrusion）的擔憂會直接提高其對於隱私的關切。自由之家（Freedom House）在2018年的國際網路自由評估報告中亦指出，許多政府將維護公民隱私作為理由，要求跨國科技公司需將資料庫設置於國內伺服器之內，企圖增加國家安全機構對於個人隱私資料的掌握能力；尤有甚者，中國甚至透過積極發展網路監控技術（internet surveillance），藉此更全方面地監控網路言論與公民行為（Shahbaz, 2018）。也就是說，不論是民主或是獨裁國家，政府在蒐集、管理、儲存與使用公民資料時的角色已逐漸與過去不同。

基於上述討論，目前數位治理研究領域尚缺乏對於民眾隱私認知與行為的實證性研究，而資訊管理領域所發展出來的隱私計算模型亦缺乏政府要素的涵融。因此，本研究主要的研究動機即在於嘗試應用二元計算模型在當前我國重要的數位政策議題New eID之上，探討個人資料授權意願與隱私認知間的關聯，以補充

DOI:10.6814/NCCU202000421

現有數位治理分析架構之不足。此外，本研究也將探討與政府相關的情境因素在隱私計算模型當中扮演何種角色。歸納而言，本研究主要研究問題可以羅列如下：

（1）在數位身分識別證上，影響民眾授權個人資料意願的隱私因素與情境因素有哪些？

（2）不同的隱私與情境因素對個人資料授權意願所造成的影響為何？

第三節 研究對象、途徑與流程

根據《戶籍法》第57條的規定：「有戶籍國民年滿十四歲者，應申請初領國民身分證，未滿十四歲者，得申請發給」。有鑒於數位身分識別的其中一項功能在於取代預定要換發的紙本國民身分證，再加上本研究的探討主題為民眾對於個人資訊的揭露態度，因此在研究對象上以14歲以上國民為宜。此外，數位身分識別證推行的目的即在於增進更高品質的數位服務提供，絕大多數的數位服務所涉及的個人隱私是屬於虛擬層次的數位個人資訊，且預計未來可使用網路辦理的服務有部分為成年後才可行使之權利，例如動產交易、公投連署甚至於未來可能推動的電子投票等。因此，本研究將研究對象範圍進一步限縮為20歲以上有使用網路的一般民眾。

本研究將採用實證研究途徑，透過統計分析的方式來驗證隱私計算模型內不同概念間的關係。需要進一步說明的是，例如個人資訊揭露意圖等概念屬於難以直接測量到的態度，因此大多數現有研究均是透過結構方程式(structural equation modeling，簡稱SEM）的方式，運用多個測量變項（measurement variable）來建構出潛在變項（latent variable）的內涵，結構方程式同時也可以用來檢驗不同潛在變項間的關係。因此，本研究也將應用結構方程式作為主要的統計方法，更進

DOI:10.6814/NCCU202000421

一步的指標建構與模型辨識（model specification）等內容將於研究設計章節詳細說明。

本研究的研究流程可分為五個部分，首先將回顧電子商務領域與數位治理領域有關資料治理、個人資料揭露與隱私計算等的相關研究，藉以建立概念定義與發展研究假設。第二，釐清研究架構內概念與概念間的關係，並以此設立統計模型。第三，說明本研究之研究設計流程，例如資料蒐集方式、資料蒐集對象與統計方法的內涵等。第四，針對蒐集的資料進行統計分析與詮釋。最後，說明本研究的研究發現與貢獻，並提出針對數位身分識別政策提出政策建議。

DOI:10.6814/NCCU202000421

第二章　文獻檢閱

本章將由上而下，從幾個層次分別檢閱相關文獻。首先將探討個人資料在數位治理中的角色、意涵與相關應用，接下來則說明個人資料揭露的種類與影響個人資料揭露意願的因素，第三節將介紹隱私計算模型的發展與模型內的變數定義，最後於第四節時說明外在情境對隱私計算模型造成的影響。

第一節 個人資料在數位治理的意涵

在數位服務盛行的現代，民眾會揭露個人資料以交換相對應的數位服務或產品；而隨著數位服務與產品更加多元，服務多樣性使得使用者幾乎難以挑選適用的服務或產品，因此服務供應商便更積極於蒐集更多的使用者資料來提供個人化的服務。最常見的例子即是個人瀏覽紀錄（cookie）的揭露可讓服務供應商（例如Amazon、eBay等）通過自動推薦系統（automated recommender systems），將符合需求的商品推薦給使用者，此時個人資訊的揭露即可促成有效率的線上交易（Jeckmans et al., 2013）。較為可惜的是，相對於跨國社群媒體或數位商務企業已發展出成熟的生態系統（ecosystems），並熟稔於結合使用者個人資料於服務或商品的提供之上，公部門卻因為服務的共有性質與缺乏身分認證架構，限制了身分驅動（identity-driven）的公共服務提供（Rissanen, 2016）。

然而，隨著資料逐漸從服膺於組織業務的客體，轉變為可以加值應用的主體，晚近的數位治理研究開始重視資料治理（data governance）的角色，期望政府可以透過資料來創造額外的公共價值（蕭乃沂、朱斌妤，2018）。因此，本節的第一部份將說明資料治理的重要內涵與個人資料在資料治理中的角色。其次，由於個人資料管理的重要性，包含美國、英國、芬蘭與我國政府等，在近年來均也嘗

DOI:10.6814/NCCU202000421

試推動個人資料管理平台與相關機制，來使政府得以取得民眾的個資授權。因此，本節的第二部分將概覽介紹國際間的重要機制與國內政策的發展，並說明數位身分識別證在其中的角色與定位。

一、資料治理與個人資料

資料治理是一組企業[1]用來管理重要數據的流程，用以確保重要資料是可信的，而當品質不良的資料產生不利的後果時，也會有相對應的課責機制（Isson & Harriott, 2012: 71）。Khatri與Brown（2010: 149-150）將資料治理分為下列五個決策領域，分別為：（1）資料準則（data principle）：釐清資料是組織中的重要資產；（2）資料品質（data quality）：確保資料的準確性、即時性、完整性與可靠性；（3）後設資料（Metadata）[2]：整合與一致化不同類型的資料，並透過模型建立等方式提供資料的可詮釋性；（4）資料取用（data access）：建立資料取用的標準與流程，包含資訊安全意識的培養等；（5）資料生命週期（data lifecycle）：盤點與汰舊組織內的資料，並依循法規制度進行檔案歸類的調整。

然而在實際的政府運作上，政府儘管蒐集了相當廣泛的行政或公民資料，但卻較難以通過資料來發揮公共價值，使得資料治理（data governance）在實務上僅剩下大量的政府資料（government data）。對於公部門採納資料治理的效果，Thompson、Ravindran與Nicosia（2015）運用澳洲的審計（audit）資料，評估了當地衛生與警察部門的資訊管理系統，發現研究對象在資料輸入時的核對、資料取用的標準等地方均有明顯的瑕疵，從而導致政府資料無法作為決策時的支援。Thompson等人認為，公部門在處理資料治理議題時，不能僅強調投入技術，而是

[1] 由於資料治理最早淵源於資訊管理領域，因此 Isson 與 Harriott（2012: 71）此處的用詞為企業（enterprise），然而本研究認為將其運用於公共組織（public organization）仍為適當。
[2] 後設資料亦被稱為詮釋性資料，是用來描述其他資料的一種資料類型（data about data）。

DOI:10.6814/NCCU202000421

要考量政策與行政的治理框架；除此之外，Thompson等人認為公部門具備更高的透明度與課責性，因此應扮演資料治理的領先指標，作為私人企業良好的標竿。

值得注意的是，在資料治理的框架當中，個人資料的管理與授權是資料如何創造「價值」的關鍵。Bhansali（2013: 5-6）認為資料治理可以使組織藉由顧客與資料間的價值鏈（value chain）來提高組織的收入，並降低錯誤的資料所帶來的風險。由此可知，當政府部門欲透過資料來生產額外的價值，如何使政府的外部顧客（也就是民眾）願意授權個人資料？如何管理與運用民眾的個人資料，才能發揮效益？係公部門與數位治理領域在應用資料治理時的重要課題。

隨著資料治理的重要性逐漸凸顯，國家發展委員會（2018）所提出的「服務型智慧政府推動計畫－第五階段電子化政府計畫」中，即點出我國政府下一世代的資料治理範疇包含巨量資料（Big Data）、開放資料（Open Data）與個人化資料（My Data）等三個部分整合。其中個人化資料的整合可作為政府決策時的參考，以及提供民眾客製化服務等效益，係資料治理無可或缺的一大部分。然而，相對於汗牛充棟的開放政府資料與巨量資料的研究，個人化資料在國內數位治理研究領域所受到的關注顯然較為稀缺。因此，本節下一個段落將聚焦於資料治理範疇內的個人化資料部分，探討近年來國際間的重要案例與發展。

二、個人資料自主管理（MyData）的發展

隨著個人化資料在不同領域的重要性逐漸提高，許多推動數位轉型的國家開始思索如何建置一個讓民眾得以自主控管個人資料的使用平台，同時也提供一個授權渠道，讓欲使用民眾個人資料來創造價值的第三方（例如政府機關、私人企業或非營利組織等）使用。本段落將說明美國、英國、芬蘭與臺灣的相關創新方案，並探討數位身分證在MyData中扮演什麼角色。

DOI:10.6814/NCCU202000421

1. 美國：The Blue and Green Button

美國自2010起，由退伍軍人事務部（Department of Veterans Affairs）開始推動「Blue Button」計畫，並隨後與國防部、衛生及公共服務部（Health and Human Services）合作，擴大了其受益者群體。Blue Button的核心宗旨為讓使用者得以快速在線上入口網站取用到部分個人電子病歷（electronic health records，簡稱EHRs）的內容，例如掛號預約紀錄、疫苗接種紀錄、過敏藥物清單與疾病史等，使用者亦可以列印或分享這些個人資訊，來提高所獲得的醫療品質（Turvey et al., 2014）。此外，衛生及公共服務部在2013年，亦於原有的架構之下推出「Blue Button plus」，擴增了個人資料的機器可讀性、傳輸安全性與自動化更新等功能。[3]

除了用以授權個人化醫療資料的Blue Button之外，美國能源部（United States Department of Energy）也推出管理個人與家戶能源使用的「Green Button」[4]。消費者透過電力公司所提供的Green Button連結，即可以快速下載自己的能源使用情況，與Blue Button的使用方式相似，消費者可以將這些資料用於管理自身的能源使用狀況，亦能將其提供給第三方作為創新用途，例如用以評估企業新推出的節能商品有效性、調整設置的太陽能板角度等。

由上述的Blue Button與Green Button的案例可知，美國的個人化資料管理與應用的核心精神之一，在於將個人資料利用具有商業價值的醫療與能源領域，並透過公私協力的方式，讓資料擁有者在自主授權的情況下，將個人資料提供給自己信賴的服務供應商，進而創造資料的額外價值（顧振豪，2016）。另外值得注意的是，由於強調商業性的應用，因此不論是Blue Button或Green Button，在推動

[3] 參考資料：https://web.archive.org/web/20140517003307/http://bluebuttonplus.org/。
[4] United States Department of Energy (2011). Green Button: Open Energy Data. Retrieved Feb 27, 2020, from https://www.energy.gov/data/green-button。

DOI:10.6814/NCCU202000421

的初期都積極強調資料格式的一致性與機器可讀性，先行確認合作機構的資料品質後，再利用資料交換協議（data exchange protocol）的方式，逐步增加應用的機構與適用的對象。

2. 英國：Midata

英國的Midata計畫發源自英國政府於2011年推動的消費者賦權策略「Better Choices: Better Deals」，該策略結合了政府、消費者與企業，讓消費者可以存取與管理自己在不同企業的消費記錄。Midata計畫由志願夥伴所組成的工作小組推動，逐步建立以使用者的個人資料為核心，圍繞著財務金融（finance and banking）、能源（energy）、電信服務（telcos）與零售業（retail）等四大領域的生態體系（Shadbolt, 2013）。Midata計畫發展出了一套管理個人化資料的一般性原則－「TACT」，意即透明（Transparency）、取用（Access）、控制（Control）與傳輸（Transfer）。持有使用者資料的組織需要確保個人資料被使用的透明性，並讓使用者擁有個人資料的取用權與控制權；在建立雙方的互信後，藉由資料共享的方式，將資料傳輸給欲加值運用的企業或組織來創造額外價值。

更具體而言，Midata計畫提出了9項的操作原則：（1）開放給消費者的資料需要符合標準的開放資料格式，如可再利用性、機器可讀性；（2）消費者可以安全地訪問、檢索與儲存其個人資料；（3）消費者可以分析、變更（manipulate）、整合與分享其個人資料；（4）跨部門間的用語（terminology）、資料格式與資料共享程序需要先行標準化；（5）快速回應消費者對資料的要求；（6）將有用的資料運用於決策過程；（7）任何組織均不得以任何形式阻礙資料的保留與再利用；（8）使用資料的組織，應盡力提高消費者對授權個人資料所可能帶來的機

DOI:10.6814/NCCU202000421

會與責任的認識；（9）使用資料的組織，應清楚告知消費者其資料蒐集流程、所蒐集的資料內容與發生問題時的課責對象（Shadbolt, 2013: 206-207）。

3. 芬蘭：MyData

芬蘭於2014年提出MyData的運作架構，認為MyData是一種對於個人資料管理的典範轉移（paradigm shift），關注的焦點從組織中心轉變為個人中心（human centric）。除此之外，公民對於哪些公司或機關取用個人資料具有決定權，政府跟企業需要規劃相對應的授權與退出制度來保障個人資料的自主控制權。

芬蘭的MyData運作原則包含：（1）以個人為中心的自主權與隱私保障：個人是管理資料的主體，應當擁有自主管理個人資料與隱私的權利與方式；（2）資料可利用性：MyData可以將封閉的資料轉化為可運用的格式，並用於創造新的商業模式與促進經濟成長，因此透過安全、標準化的應用程式介面（Application Programming Interfaces，簡稱APIs）來存取機器可讀的個人資料至關重要；（3）開放的商業環境：共享MyData架構可以實現個人資料的分權化管理，並讓企業更可以遵守個資規範，消費者也得以自由選擇服務供應商（Poikola, Kuikkaniemi, & Honko, 2015）。

除了MyData的架構之外，芬蘭政府亦建置了「芬蘭信任網絡」（The Finnish Trust Network，簡稱FTN），提供身分供應者（identification provider，簡稱IDP）與服務供應商之間一個標準化的技術和法律框架。Rissanen（2016）認為，MyData所提供的個人資料授權，可以與FTN的法律框架相結合，提供芬蘭公民一個完善的身分驗證服務，讓公民享受公部門與私部門不同的創新服務。

DOI:10.6814/NCCU202000421

4. 臺灣：從「我的e管家」到「健康存摺」

如同前述所提及的美國、英國與芬蘭等國政府均開始推出管理民眾個人化資料的實作策略與個案，我國政府在2019年亦推出「智慧政府推動策略計畫」作為推動MyData的重要指導綱領。國發會目前正協同衛生福利部、交通部、內政部等、教育部等機關積極試辦MyData架構，讓民眾可以在不同部會自主下載重要的個人資料（國家發展委員會，2019）。透過MyData架構，政府可以主動提供民眾需要的個人化服務、減少民眾洽公成本。舉例而言，未來民眾在辦理政府業務時，承辦機關可以在民眾的授權下，串接政府業務資料庫，民眾即不需要準備紙本文件辦理。

然而，我國政府事實上從2007年開始，即為了回應「一站式數位服務」的發展，建置了「我的e管家」網站與應用程式，強調以民眾需求導向核心，整合政府服務來提供客製化的公共服務（陳怡君，2008）。本研究認為，我的e管家在創建初期，就核心目標與精神上，與現有所欲推動的MyData大相徑庭，均是為了讓政府主動提供民眾諸如牌照換發、水電費繳納等個人化數位服務；兩者最大的差異之一，在於引入個人身分認證的機制，與取用民眾個人資料的程度。

在「我的e管家」建置之後，我國衛福部中央健康保險署於2014年推出的「健康存摺」，可謂是國內成功結合身分認證機制與個人化服務的首要個案。健康存摺可以讓民眾快速存取三年之內的醫療資訊，包含就醫紀錄、用藥情形與醫師診斷結果等，力求將個人健保資料的自主權還諸於民。健保署更於2018年新增了「行動電話認證」的方式，來取代過去僅能利用讀卡機讀取健保卡的身分認證機制，提供行動裝置使用者更高的便利性；截至2018年底，已有超過100萬人登錄並使用健康存摺（李伯璋、林寶鳳、張齡芝，2019）。

DOI:10.6814/NCCU202000421

健康存摺的成功，顯見運用個人資料所能帶來的額外價值。然而，目前國內在推動MyData的相關加值應用所遇到的困難之一，即在於不同部會各自儲存著民眾資料，且自行建置線上平台供民眾使用；在缺乏整合性的身分驗證機制與管道的情況下，反倒容易產生民眾使用上的困擾與數位服務輸送時的斷點（曾憲立、蕭乃沂、宋同正，2020：93-99）。基此，行政院於2019年6月核定了數位身分識別證換發計畫（New eID），將數位身分識別證定調為未來智慧政府的使用金鑰（內政部，2019），並希望透過全面換發數位身分識別證，為民眾與政府提供一個整合性的身分認證機制，藉以帶動政府業務資料庫中個人資料的創新運用。

曾憲立等人（2020）在盤點多國MyData使用案例與身分認證機制後指出，雖然各國的身分認證機制各有不同，但其操作原則仍是結合現有的虛實流程，來提供使用者便利的認證機制。因此，從數位身分識別證的政策立意而言，由於現行國民身分證具有「一人一號」的實名性質，且目前使用的國民身分證為民國94年所換發，亦有全面換領之需求，因此藉此政策契機全面換領數位身分識別證應為可行的政策方案。然而，雖然內政部與行政院曾多次說明未來換發的數位身分識別證，將會比現行的國民身分證更能保障民眾個人隱私與資料自主權，仍無法完全迴避國內人權團體對數位身分證全面換領後，所可能帶來的隱私外洩風險與政府監控疑慮的指控。

環諸各國推動MyData的案例，隱私疑慮與民眾意願往往是難解的課題。例如美國在推動Blue Button時，有研究即針對政府在推動個人醫療資料的授權與管理時，如何進行修正與調整現行隱私法規提出討論（Longhurst, Harrington, & Shah, 2014），也有研究探討影響民眾接受該服務的因素（Turvey et al., 2014）。正如芬蘭政府所宣示的MyData核心價值：「個人無法自主控制的資料不能被稱

DOI:10.6814/NCCU202000421

之為MyData」[5]。因此，民眾如何去理解個人資料授權後所可能帶來的利益與風險，以及影響其授權意願的背後邏輯為何，係未來持續推動MyData發展時，不可避免探究的關鍵課題。

綜整而言，本節探討了資料治理的概念與數個國家的MyData政策，嘗試為本研究提供一個研究定向。更具體來說，本研究從宏觀的資料治理概念為起點，並以數位身分識別證此一國內重要數位政策為研究個案，探討在MyData架構之下，影響民眾授權個人資料意願的隱私因素。因此，下一節將進一步說明個人資料授權與揭露意向的相關研究。

第二節 個人資料揭露意向

資訊隱私具有多面向的意涵，在討論隱私議題時，必須先嘗試將隱私的概念清楚界定，作為進一步討論的基礎。因此本節將先探討資訊隱私與個人資料的分野與內涵為何，再說明不同的個人資料種類，最後探討過去研究中所提出可能影響個人資訊揭露的因素。

一、資訊隱私權與個人資料的分野

有關資訊隱私（information privacy）的定義，Westin（1967: 6）認為資訊隱私為「個人、團體或機構可以自主決定自己的資訊在何時、透過哪些方式與多大程度上地傳送給他人知悉」[6]。Stone、Gueutal、Gardner與McClure（1983）則進一步將資訊隱私限縮於個人層次之上，認為資訊隱私是「個人對於自身資料的控

[5] 原文為：Personal data that is not under the respective individual's own control cannot be called MyData（Poikola et al., 2015: 2）。

[6] 原文為：the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1967: 6).

DOI:10.6814/NCCU202000421

制能力」[7]。上述的定義與法律或哲學的觀點亦相當接近，例如哈佛憲法學教授Charles Fried即主張隱私代表可以自我控制個人資料的使用與流向，在法律概念上也包含「不受干擾的權利」的意涵（轉自劉靜怡，2002：143-144）。由上述不論是數位商務或是法律領域的定義可以得知，資訊隱私權反映出對個人資料的控制權，也強調個人可以自主決定個人資訊的傳送、儲存與消除，申言之，侵害一個人的資訊隱私，即代表對於該人的資訊自主控制權的剝奪。

關於個人資料（personal data/personal information）[8]的意涵，則可從法律上的規範來探究，例如美國將個人識別資訊（personally identifiable information，簡稱PII）的內涵規範為「任何可以用來追蹤或是區分個人的資訊，例如姓名、社會保險證號、出生日期與地點或生物特徵等紀錄，此外可以連結到個人的任何其他資訊，例如醫療、教育或財務資訊也均屬之」（McCallister, 2010：2-1）。歐盟於2018年生效的《一般資料保護規範》（General Data Protection Regulation，簡稱GDPR）將個人資料定義為「可直接或間接用於識別自然人的數據資料，包含姓名、身分證號、位置資訊或其他生理、心理、經濟、文化與社會身份等所特有的一個與多個因素」。我國的《個人資料保護法》也將個人資料定義為「指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」。因此，從美國、歐盟與我國現行的法律規範來看，凡是可以作為追溯與識別個人之用的資

[7] 原文為：the ability (i.e., capacity) of the individual to control personally (vis-a-vis other individuals, groups, organizations, etc) information about one's self (Stone et al., 1983: 460).

[8] 在現有的討論當中，多將個人資料（personal data）與個人資訊（personal information）作為同義詞使用，本文在後續的討論中會將兩者視為同義詞交錯使用。

DOI:10.6814/NCCU202000421

料，不論是生理特徵、身分證號、聯絡方式甚至於社會角色均可以被視為個人資料的一部分。

歸納而言，從上述資訊隱私與個人資料的概念意涵界定，可以發現資訊隱私強調的是個人對於自身資料的控制權，而個人資料則屬於資訊隱私權當中的客體，意即隱私考量反映的是個人控制這項客體（個人資訊）上的能力與程度。舉例而言，在數位身分識別政策當中，我國的人權團體臺灣人權促進會曾公開發文表示現行數位身分識別的規劃無法落實保護隱私與資料自主的功能，其中的質疑即包含其他單位是否可以在欠缺個人同意的前提下取用數位身分識別內的資料、個人是否可以檢視個人資料被使用與讀取的紀錄等。[9]顯示國內對於數位身分識別隱私的關切與討論，與國外隱私權研究有相同的討論脈絡，均著重於資料主體（data subject）控制力的有無與程度高低。

需要說明的是，關於網路世代的資訊隱私權該如何界定與其範疇等規範層次的探討，在科技法律領域已有相當繁重的辯論與法律分析。例如我國過去曾規劃推行「國民身份健保合一智慧卡（國民卡）」時，就即有研究將國民卡當作個案分析電子化政府推動下的資訊隱私權議題（何明諠，2016；紀佳伶，2000），以及網際網路時代時代下，電子商務領域蒐集民眾資訊所可能衍生的倫理與法律問題（劉靜怡，2002）。然而，本研究認為上述國內研究仍僅止步於規範面上的討論，缺乏對於個人資料的擁有者在隱私認知與實質行為上的理解；換言之，現有關於電子化政府的隱私研究多半從政府應然層次出發，以法規條文與政府方案作為研究標的並詮釋其可能的效果，忽略民眾在隱私問題下的認知與行為。

[9] 何明諠（2019）。為何我們反對內政部的 eID 政策，2019 年 11 月 5 日，取自：https://www.tahr.org.tw/news/2435。

DOI:10.6814/NCCU202000421

先驗性的規範性研究固然作為隱私權研究無可排除的一部分，但若缺乏實際現象的觀察與資料驗證，則容易淪為主觀性的價值辯證，使得具爭議性的政策停滯不前。即使是在科技法律領域，近年來的實證法學研究也開始強調透過實際狀況的驗證來累積法律經驗（劉尚志、林三元、宋皇志，2006）。因此，有別於過去隱私權研究多以法律面的應然分析為主軸，本研究將嘗試從實然面的個人態度出發，探討民眾對於個人資料的揭露意願，以及影響資料揭露意願的因素。

二、個人資料的種類

由於個人資料具有多元的種類與範圍，而不同種類的資訊也相當程度影響該資料的揭露意願，在探討影響個人資料揭露意願之前，有必要先針對不同種類的個人資訊進行說明。Phelps、Nowak與Ferrell（2000: 28）將個人資訊分類為人口特徵（demographic characteristics）、生活方式（lifestyle）、消費習慣（purchasing habits）、財務資料（financial data）與個人識別資料（personal identifiers），並發現消費者最不願意提供金融等財務資料與姓名或電話等個人識別資料。Phelps等人認為個人識別資料具有相當程度的隱私侵害性，因此政府或企業在規劃隱私政策時，應對較具危害性的類型採取較嚴格的規範，而較不具威脅性的人口特徵或消費習慣等則可適度放寬規範。

不同研究者也曾針對自身的研究旨趣提出不同分類，例如Meinert、Peterson、Criswell與Crossland（2006）將個人資訊分為（1）聯絡資訊（contact information）：如姓名、電子信箱或是手機號碼等；（2）基本資料（biographical information）：例如性別、年齡與收入等人口統計資訊；（3）財務資訊（financial information）：例如銀行帳號、信用卡卡號等。Kim與Kim（2018）將個人資訊歸類為（1）使用模式（usage pattern）：查詢內容、瀏覽網頁的時間與使用流量等；（2）個人識別資料（personal identifiers）：銀行帳號、個人身分字號、聯絡方式等敏感性資

DOI:10.6814/NCCU202000421

訊；（3）基本資料（biographical information）：姓名、性別、年齡與家庭狀況等基本資訊；（4）使用行為（usage context）：意指消費者使用時的情境，例如使用服務時的IP位址、裝置與設備等；（5）回饋資訊（feedback information）：如消費者意見與評分等。

除了上述在數位商務領域的分類之外，醫學研究也指出健康狀況、用藥行為與過去病歷等醫療資訊（health information）應屬於另外一項特殊的資訊種類（Bansal, Zahedi, & Gefen, 2010）。例如電子病歷的整合即是近代醫學改革的一項重要成就，不同醫療保健領域的紀錄可供大規模的健康趨勢分析與管理之用，但病患對於自身的資訊缺乏控制權也使得隱私權的關注成為該項改革的主要阻力（Milutinovic & De Decker, 2015）。我國健保署所推動的「健康存摺」個案亦是涉及醫療資訊的保存與使用授權；有趣的是，蕭乃沂等人（2017）的調查結果顯示，我國民眾對於提供醫療資訊以換取醫療服務所願意承擔的風險為最高，而提供金融資料供線上交易之用的風險承擔意願則為最低。本研究認為其背後的邏輯與先前所提及的隱私計算理論息息相關，反映出臺灣民眾對於醫療資訊授權的成本效益分析，也就是高品質醫療服務的主觀效益是高於醫療資訊洩露的預期風險，從而使得民眾願意提供個人資料來換取更高品質的醫療服務。

歸納而言，個人資料從機敏性由低到高至少可以分為三個層面，首先是機敏性最低的人口特徵資料，例如性別、年齡、教育程度等，經由去識別化的程序後即難以追蹤回個人的資料，調查研究也時常蒐集這類型的資料做為研究之用。第二個是個人使用行為，此類資訊經過整理後可以拼湊出個人的基本樣貌與行為模式，例如電子商務品牌會透過個人搜尋紀錄進行運算，來將不同使用者進行歸類後以推薦適合的產品或服務，此類資料仍具備相當程度的匿名性，除非透過特定的程序，否則難以透過資料直接追溯回特定個人。最後即是機敏性最高的個人識

DOI:10.6814/NCCU202000421

別資料，舉凡身分證字號、銀行金融帳號、臉部特徵、聲紋或指紋等可以直接用於識別單一個人的資料則屬此類。

三、影響個人資料揭露的因素

民眾為什麼願意揭露自己的個人資料？過去有許多研究在探討影響個人資料揭露的因素，其中絕大多數的研究都將使用者的資訊隱私考量（privacy concern）視作最重要的決定因素。使用者對於隱私的擔憂源自於委託代理人理論當中的資訊不對稱現象，在資訊不對稱的情形下，使用者擔心個人資料會被取得資料的團體或機構，不正當地蒐集、取用或未經同意的轉售（Li, 2012）。例如，Smith等人（2011）提出APCO模型（Antecedents-Privacy Concerns-Outcomes model），將民眾的資訊揭露意願視為結果（outcomes），認為民眾過去的隱私受侵害的經驗（experience）、隱私警覺性（awareness）、個性（personality）、人口特徵（demographic）與文化（culture/climate）會形塑出不同的隱私考量，而隱私考量則會作為中介變數再去影響個人資料的揭露意願。此外，Bansal等人（2010）的研究也發現隱私考量與個人健康資訊時的揭露意圖之間，呈現顯著的負向關聯。因此，隱私考量對於民眾來說，反映的是提供個人資料背後的風險評估，當對隱私的關注度越高，對提供個人資料的可能風險也會有較高的評估，從而降低提供個人資料的意願。

然而，除了風險的考量之外，揭露資訊所可能帶來的利益考量也是甚為重要。從Homans（1958）的社會交換理論觀點來看，個人會評估揭露資訊的效益與成本來決定是否提供個人資訊（Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010）。此種觀點通常伴隨著將隱私視為一種商品（commodity）的意涵，例如Hagel與Rayport（1997）就認為，並非是使用者非常重視個人隱私，而是企業未能提供足夠的誘因與利益來換取個人的數據。此一論述受到許多電子商務研究的關注，並

DOI:10.6814/NCCU202000421

逐漸發展完備成為隱私計算理論，也就是同時考慮民眾對於利益與風險的權衡，認為民眾會願意去承擔個人資料可能外洩的隱私風險，而去換取有用的利益（Stone & Stone, 1990）。Hui、Tan與Goh（2006）將消費者在數位商務領域揭露資訊的動機歸納為內在效益（intrinsic benefits）與外在效益（extrinsic benefits），並可再細分7種不同的利益動機。[10]顯示資料主體在揭露個人資料時除了考量隱私風險之外，也同時會將揭露資料後所可能得到的服務效益納入計算。

現有針對個人資訊揭露意圖的研究多以企業服務作為研究標的，電子化政府或數位治理相關研究則鮮少以個人資訊揭露意向為討論主軸。究其原因，主要在於政府服務多半具有寡佔或獨佔性質，再加上政府就實務層面上並不需要跟民眾「索取」這些個人資訊，許多必要的個人資料（例如性別、教育程度與就業保險資料等）大多也早已儲存於相關單位的業務資料庫當中。在現有的研究中，數位治理相關研究多以「取用授權」（access authorization）為探討主體（Papadopoulou, Nikolaidou, & Martakos, 2010）。本研究認為，數位商務上的「資料揭露意圖」與數位治理上的「取用授權」，兩者在概念具有相當高度的重疊性，均是用以表達使用者提供個人資料（或提供取用個人資料的權限）以換取數位服務的提供。然而，數位治理領域仍相當缺少對於取用授權的範圍或是有關民眾授權個資意願的實證分析，或僅將其納於無所不包的信任內涵之中，鮮少獨立探討之。[11]因此本研究將應用個人資料揭露的相關概念與理論，來影響數位治理中關於個人資料取用授權意圖的因素。

[10] 內部效益包含愉悅感、新奇感與利他主義的幫助行為，而外部效益則包括節省金錢、節省時間、自我增強與社會調節效果（Hui et al., 2006: 420-423）。

[11] 例如 Papadopoulou 等人（2010）即把電子化政府上關於個人資料的驗證（authentication）、確認真實性（authenticity）與授權（authorization），歸類對電子化政府的資訊儲存信任（trust in stored data）。

DOI:10.6814/NCCU202000421

總結而言，本節嘗試釐清隱私與個人資料的內涵與種類，並歸納現有的數位商務領域的相關研究，發現民眾的隱私考量會是影響其個人資料揭露意願的先決因素。同時，隱私的考量則可再進一步分為因為隱私所帶來的風險與利益，也就是隱私計算理論的概念基礎。本研究接下來將詳細說明隱私計算理論的發展與相應的研究發現，作為本研究最主要的研究架構。

第三節 隱私計算模型的發展

本節將說明隱私計算理論概念的源起，以及討論現有的隱私計算模型內具備的構念，最後探討隱私計算模型最新的發展趨勢與擴張後的二元隱私計算模型。

一、隱私計算理論的源起

隱私計算理論的概念最早由Laufer與Wolfe（1977）所提出，Laufer與Wolfe認為個人在考量是否願意個人資料時，會考量這個行為背後在可能發生的後果。舉例而言，由於醫療人員可能基於精神病患自我揭露的一些個人資訊，選擇將其送往精神病院或是繼續觀察；因此，病患會基於成本與效益考量，而去管理個人資料的披露程度。Laufer與Wolfe進一步提出，選擇揭露或是不揭露個人資訊並非只單純對於未來行為可能造成的後果擔憂，當個人認為後果有益時，對於提供個人資料也會有高度的意願。Stone與Stone（1990）延伸了上述隱私計算的概念，當資訊主體（也就是使用者）認為自己對未來的資訊使用有控制能力，以及自身提供的資訊與服務具相關性時，使用者將認為提供資料換取服務是可靠且有效的，不會將資料提供視為一種隱私的侵犯。

基於上述的概念分析，我們可以發現，當使用者認為揭露個人資料具有正面淨效果（net outcome）時，人們會願意接受任何可能的隱私損失。然而此概念在提出之初，雖然相當具備的清晰性與理論直覺性，但尚缺乏實證模型的驗證

DOI:10.6814/NCCU202000421

（Culnan & Bies, 2003），直至Dinev與Hart（2006）才提出較為成熟的隱私計算模型研究，並實際蒐集資料以驗證之。Dinev與Hart嘗試將兩種不同的信念同時置放於模型之中，用以觀察隱私風險與隱私利益這兩種相互消長的信念對於資料揭露意圖的影響。因此，本節的下一個部分將從Dinev與Hart建立的隱私計算模型為基礎，探討隱私所帶來的風險與利益，這兩者在隱私計算模型中的內涵與影響。

二、隱私計算模型的內涵：隱私風險與隱私利益

Dinev與Hart（2006）最初是以誘惑信念（enticement beliefs）一詞，來指涉個人在網路上的隱私利益。Dinev與Hart認為個人對於網路的興趣反映出一種信念，這種信念不見得會「消除」（eliminate）個人對於網路隱私侵害的風險感知，但是有可能「超越」（override）個人對隱私的擔憂，進而促成資料揭露行為的發生。更重要的是，Dinev與Hart建構了隱私風險、網路信任與網路興趣等變項的操作化指標，並應用結構方程式此進階的統計方法來驗證概念間的關聯。Dinev與Hart發現，雖然隱私風險確實對於揭露個人資料的意圖呈現負向影響，然而個人的網路興趣所產生的正向影響則可能大過於對於風險的擔憂，進而促使個人在揭露個人資料以便在網路上進行交易（transaction），反映出個人對於自主資料管理的態度，仍是基於自身理性下的成本效益計算分析。

在Dinev與Hart的基礎之上，Xu、Teo、Tan與Agarwal（2009）以裝置上的定位服務（location-based services，簡稱LBS）作為研究標的，並率先將隱私計算模型分野並命名為隱私利益與隱私風險這兩項構念。由於LBS服務可以透過使用者當時的位置來提供適合的推薦商店等個人化服務，但對使用者而言，也需要同時承擔個人位置外洩的風險，因此相當適合作為驗證隱私計算模型的數位服務個案。值得注意的是，由於Dinev與Hart的研究當中只利用了內在動機（個人網路興趣）作為隱私利益的指標，因此Xu等人的研究則嘗試驗證經濟補償

DOI:10.6814/NCCU202000421

（compensation）這項外在動機對於感知隱私利益的功能。Xu等人發展出「推力與拉力」這兩種使用情境來驗證研究模型，推力情境是指系統主動會向使用者推送個人化服務，換言之，也就是系統無時無刻都在取得使用者的位置資訊；而拉力情境則代表當使用者需要個人化服務時，才需要向系統授權個人位置。其研究結果發現，在推力情境當中，經濟補償對於隱私利益的認知有顯著的正向影響，但經濟補償在拉力情境則缺乏效果，顯示當使用者是基於數位服務的需求時提供資料，經濟補償所帶來的外部動機將會被內在的需求動機所消除。

Li、Sarathy與Xu（2010）進一步將模型內的概念操作化得更為精細，他們將隱私利益區分成屬於內在動機的實用性（usefulness）與外在動機的金錢報償（monetary rewards），將隱私風險區分為隱私保護信念（privacy protection belief）與隱私風險信念（privacy risk belief），發現實用性、金錢報償與隱私保護信念對與個人資料揭露意圖有正向關聯，而隱私風險則反之。該文同樣也考量了揭露資料情境的調節效果，發現當揭露的資訊與服務間存在低度關聯程度時，金錢報償反而會降低資料揭露意圖。綜整而言，Li等人（2010）的研究結果與Xu等人（2009）的發現一致，也就是當使用者認知到企業或組織僅僅是在花錢購買他們的個人資料，而非提供相對應的服務時，會造成使用者的反感進而不願意提供個人資料。

隱私計算模型在經過驗證早期理論模型的發展期，逐步確認與建構完成隱私利益與隱私風險這兩項主要構念與操作化指標後，開始被資訊管理領域大量用於不同的使用情境之上。許多研究紛紛將自己有興趣的次構面視為驗證性因素分析中的一階因素（first order factor），而將隱私利益或隱私風險視為模型中的二階因素（second order factor），用以驗證使用者在不同服務內的個人資料揭露意圖。例如有研究針對醫療穿戴設備的使用進行分析，發現穿戴式設備所帶來的隱私利益，如資訊有效性（informativeness）與適用性（functional congruence）等，會提

DOI:10.6814/NCCU202000421

高對於醫療穿戴設備的採用；此外，個人的創新精神（innovativeness）與使用醫療穿戴設備所帶來的聲望（prestige）將有助於減少所認知的隱私風險（Li, Wu, Gao, & Shi, 2016）。也有研究以需要大量個人資訊的物聯網（Internet of Things，簡稱IoT）服務作為研究標的，發現在醫療保健、智慧家庭（smart home）與智慧交通（smart transportation）這三種不同種類的物聯網服務上，只有當涉及醫療保健項目時，隱私風險才具有負向的影響力，顯示使用者在使用智慧家庭與智慧交通時，往往只考慮個性化服務帶來的利益，而忽略潛在的隱私風險（Kim, Park, Park, & Ahn, 2019）。

從上述的討論可以發現，雖然不同研究者會發展出不同的一階因素於模型之中，在隱私計算模型當中的二階因素－隱私風險與隱私利益－已受到多數研究的驗證與使用。綜合現有的研究當中來看，目前對於隱私利益的定義較為清晰且一致，隱私利益反映出使用者在揭露資料後預期可以得到的回報或利益，在次構面中可包含：（1）有形的財務回報，如補償金、折扣等（Li et al., 2010; Li, 2012; Xu et al., 2009）；（2）有效的個人化服務（Kim & Kim, 2018; Li et al., 2010; Li, 2012; Wang, Duong, & Chen, 2016; Xu et al., 2009）；（3）服務兼容性，如個人化服務與其他服務的融合與價值外溢（Kim et al., 2019; Li et al., 2016）等三個不同次構面。

與隱私利益相比之下，形成隱私風險的內涵與相對應的一階因素則相對較為模糊與不一致。例如國家監控的疑慮（Dinev et al., 2008）、資訊的敏感性（Kim et al., 2019; Li et al., 2016）、對於資訊的控制能力（Wang et al., 2016）與法規保障（Li et al., 2016）等因素都曾在研究中被提出作為隱私風險的前因（antecedent）。基於隱私風險定義上的模糊，Li（2012）經由文獻檢閱與釐清概念後，認為隱私風險對使用者而言包含了另一個層次的損益權衡，其中可包含風險評價（risk

DOI:10.6814/NCCU202000421

appraisal）與應對評價（coping appraisal）。風險評價反映出個人資料可能帶來的危害，而應對評價則代表個人應對風險的機制與能力，使用者會權衡預期的風險與自身應對風險的能力後，形成對於揭露資訊的隱私風險認知。Li（2012）將關於隱私風險的計算稱之為風險計算模型（risk calculus），並且將隱私計算模型進一步擴張成包含隱私計算與風險計算的二元隱私計算模型；前者代表隱私利益與隱私風險間的權衡，後者則代表風險評價與應對評價間的權衡。

本研究認為Li所提出的風險計算釐清了個人對於隱私可控制的能力與對未來預期風險間的權衡，重新定義了過去研究當中相對模糊的隱私風險，從而拓展了隱私計算模型在理論架構上的完整性，相當具有理論驗證的潛在價值。然而，僅有少數的實證研究應用二元隱私計算模型進行研究分析（Kim & Kim, 2016; Kim & Kim, 2018）。因此，本研究下一個階段將會介紹二元隱私計算模型的概念與相關研究，作為本研究後續模型建立之重要參照。

三、擴展隱私計算模型：二元隱私計算模型

最初的隱私計算模型僅包含了隱私利益與隱私風險的權衡，而Li（2012）的研究則進一步將隱私風險擴展（extend）為風險評價與應對評價這兩種認知間的計算，並將其命名為風險計算，因此完整的二元隱私計算模型可包含隱私計算與風險計算這兩個層次。

風險計算的理論源起於保護動機理論（protection motivation theory），使用者的保護動機來自於對於威脅事件的可能性與危害性的評估，以及所採取的應對措施能否可以有效地防止該危害的發生（Rogers, 1975）。舉例而言，Lee與Larsen（2009）應用保護動機理論於探討中小企業採用反惡意軟體（anti-malware software）的意願，發現當廠商認為惡意軟體具有嚴重性與本身資料具有脆弱性

DOI:10.6814/NCCU202000421

時，會提高使用反惡意軟體的意願。此外，當認為反惡意軟體的安裝是簡單易用的，且其功能有效性高時，也會提高使用反惡意軟體的意願。

Li（2012: 476）將保護動機理論應用於自己所提出的風險計算模型當中，綜合了過去的研究提出了四個會影響隱私風險的因素，分別是（1）感知威脅的嚴重性；（2）感知威脅的可能性；（3）預防行為的有效性；（4）採取預防行為的自我效能。前兩者共同組成了對於個人資料揭露的風險評價，代表揭露資料可能發生的預期風險，而後兩者則組成了應對評價，反映出個人對於風險控制的能力。舉例而言，當提供個人資料所可能的危害很小或是發生機率很低，個人採取保護措施（例如不提供個人資料）的機率也會很低；另一方面，若個人認為自己處理風險的能力較佳，採取保護措施的機率也會下降。

風險計算模型整合了過去散落於不同文獻當中曾發現會影響隱私風險的各種因素，並拓展了隱私計算模型的應用性與理論架構。在有限的研究當中，Kim與Kim（2016）以慶南地區的大學生為研究對象來嘗試驗證雙元計算模型，其中並沒有發現個人風險處理能力對於隱私風險計算兩者間存在關聯。基於2016年的研究成果，Kim與Kim在後續的研究中進一步擴張了樣本的規模與範圍，並驗證了雙元計算模型在不同種類資訊揭露下的不同效果。Kim與Kim（2018）的研究發現，對隱私外洩嚴重性的認知，與個人資訊的揭露意願之間呈現負向關聯，而自我的應對效能則對個人資料的揭露意願產生正向影響。

綜合上述，隱私計算模型自Dinev與Hart（2006）奠定模型測量基礎與驗證後，其累積了相當豐碩的研究成果於資訊管理領域的應用之上。相對於資訊管理領域對於個人隱私計算與認知的研究，數位治理領域現有的研究則顯得相當不足且有限。儘管部分數位治理的研究時常呼籲隱私的重要性與政府對於個人資料可能的

DOI:10.6814/NCCU202000421

侵害（Carter & McBride, 2010），而政府的政策制定也日漸強調資料驅動（data-driven）扮演的角色，以及個人化服務的加值應用（余孝先、趙祖佑，2015）；現有的國內外數位治理研究仍缺乏隱私計算模型的應用與分析，對隱私權的討論也多只停留在應然面上的論述或法律條文上的解讀，尚缺乏對公共服務的使用者在隱私認知與行為意圖上的關切。

值得注意的是，許多隱私計算的研究都曾提及，特定的使用情境將會影響資料提供者對於隱私風險與隱私利益的權衡（Li et al., 2010; Smith et al., 2011; Xu et al., 2009），意即資料提供者無法基於真空條件下進行選擇，而是會考量資料提供的對象、程序與配套措施等。因此，為完善本研究之研究架構，下一節的文獻回顧將說明不同使用情境下，對於民眾的隱私計算所可能產生的效果。

第四節 隱私情境的影響

在真實的使用情境當中，民眾多半不只考量利益與風險這兩個元素，而是有更為複雜的思維機制。以本研究的研究個案－數位身份識別證為例，民眾對於使用新科技預期所需投入的成本、政府相對應的風險管理機制、以及民眾對政府這位資料蒐集的「代理人」在資料儲存與交易行為上的信任，都可能會影響民眾的隱私認知。舉例來說，基於組織形態與運作模式的差異，民眾對於政府政策與企業商務可能會產生截然不同的認知；與企業不同，國家係為一具強制力的政治實體，因此當數位治理領域應用隱私計算模型時，民眾對政府監控的疑慮亦須納入考量。本節將會說明，預期投入、風險管理機制、政府信任與政府監控疑慮對於隱私計算模型所可能產生的影響，並探討現有的研究發現。

DOI:10.6814/NCCU202000421

一、預期投入的影響

就理性的考量上，除了上述隱私計算模型中的風險與利益之外，為了取得可能的利益，民眾也會先行評估所需要投入的成本，此種預期投入的概念隨著電腦、文書系統等新科技的日漸普及，開始受到研究者的重視（Venkatesh, Morris, Davis, & Davis, 2003）。舉例而言，Davis（1989）提出深具影響力的科技接受模型（Technology Acceptance Model，簡稱TAM），認為民眾在面對一項新科技時，系統的易用性與操作清晰性會影響民眾使用的意圖，也就是當民眾感受到系統越便於使用時（perceived ease of use），使用該項新科技的意願會越強。除了科技接受模型之外，創新擴散理論（Innovation Diffusion Theory，簡稱IDT）與電腦可用性模型（Model of PC Utilization，簡稱MPCU）也都指出使用便利性會影響到使用者的採納意願（Moore & Benbasat, 1996; Thompson, Higgins, & Howell, 1991）。

Venkatesh等人（2003）綜整理性行為理論、科技接受模型、創新擴散理論等多種探討科技使用意圖的研究模型，提出了整合科技接受模型（Unified Theory of Acceptance and Use of Technology，簡稱UTAUT）。Venkatesh等人在UTAUT中，將TAM、IDT與MPCU的易用性概念進行的統整，並提出新的概念構面「預期投入」（effort expectancy）。預期投入被定義為一種使用系統時的輕鬆程度，[12]而當所使用的科技或系統處於越早期的階段，也就是越少人接觸過該項科技時，預期投入所產生的影響也最為顯著。然而值得注意的是，洪新原、梁定澎與張嘉銘（2005）使用後設分析方法（meta-analysis），檢閱了58篇科技接受模型的實證分析結果，發現易用性與使用意圖之間的效果較為不穩定；在16篇提及易用性的研究當中，有8篇發現易用性與使用意圖間呈現顯著的正向關聯，另外8篇則未有

[12] 原文為：Effort expectancy is defined as degree of ease associated with the use of system. (Venkatesh et al., 2003: 450)

DOI:10.6814/NCCU202000421

統計上的顯著效果。因此，雖然科技接受模型與整合科技接受模型等均是被長期反覆驗證的模型，在易用性上的研究假設仍屬於未來研究可以進一步探索之處。

基於上述的討論，本研究將預期投入視為民眾使用數位身分識別證時所需要付出的努力與成本，當民眾預期未來系統是便於使用時，透過數位身分識別授權個人資料的意願也會越高。此外，民眾除了會考量要事先付出什麼，才會取得利益之外，同時也會考量當發生負面後果時，有可能的補償或管控機制為何。因此，本節的下一部分將討論，政府所提出的風險管理機制對於民眾隱私認知的影響。

二、風險管理機制的影響

政府在推動政策時，民眾往往會希望政府可以一併端出「配套措施」來降低政策實施後的不確定性。以隱私權議題為例，政府如何在系統或技術上減少隱私外洩的風險，而倘若重要的個人資料不幸外洩，又該如何控管並極小化隱私外洩後對民眾產生的危害，即是推動數位身分識證時的關鍵配套機制。有研究即指出，政府的風險管理機制與民眾的隱私擔憂習習相關，當民眾對政府在隱私管理機制的感知越弱，民眾對隱私外洩的疑慮就會越強；Lwin、Wirtz與Williams（2007: 574-575）認為這種現象源於民眾感受到權力與責任間的不對等，進而透過反動行為[13]來降低不平衡感。

由此可知，風險控管機制扮演著影響民眾隱私認知的關鍵角色，而最為常見的風險控管機制之一即是隱私權條款的提供；因此，許多研究開始應用實驗設計的方式來探討隱私權條款的框架效應（framing effect）。Tsai、Egelman、Cranor與Acquisti（2011）即發現，當隱私保護的敘述變得更明顯且易於接收時，消費者

[13] Lwin 等人（2007）將使用者的反動行為分做三類：（1）偽造（fabricate）：提供錯誤的個人資料；（2）保護（protect）：使用某些工具保護自身的線上隱私；（3）保留（withhold）：拒絕提供個人資料或拒絕使用服務。

DOI:10.6814/NCCU202000421

會傾向跟較能保障隱私的店家購買。除此之外，其他研究也指出網頁上完整且明確的信任標誌，例如商標、公司名稱、第三方認證機制等，都有助於提高使用者提供個人資料的意願（Jensen, Potts, & Jensen, 2005; Xie, Teo, & Wan, 2006）。

除了企業的自主管控之外，在Smith等人（2011）中所提出的APCO模型當中，亦有討論到不同政府提供隱私管制（regulation）的有效性；並認為相對於企業所自行提供的隱私保護，政府所提供的普遍性與強制性的管制，可能將更有助於減少民眾的隱私疑慮。Miltgen與Smith（2015）透過實證資料，驗證了隱私管制感知有助於減少隱私擔憂的效果，同時也發現，當民眾更瞭解管制的內容時，[14]即會感受到管制所帶來的保護性。其他研究也多呈現相似的研究結果，當民眾對保護性管制的感受程度越高，隱私擔憂的程度也會越低，進而間接提高提供個人資料的意願（Lwin et al., 2007; Wirtz, Lwin, & Williams, 2007）。

綜整而言，本研究認為政府針對隱私問題所提出的風險管制機制，將可能有助於降低民眾對於隱私風險的認知，進而間接提高授權個人資料的意願。值得注意的是，風險管制機制在具體的應用當中，尚可分為不同的層次，因此本研究參考Miltgen與Smith（2015）的操作化定義，將風險管理機制區分為技術使用、損害控管與事前法律授權等三部分。然而，除了具體可見的如法規、隱私保護條款等形而上的風險管理機制外，其他的形而上信念也同樣扮演著影響民眾認知的一環。本節下一部分將探討另外一項相對較為抽象，但對於民眾隱私認知可能會產生相同或是甚至更龐大影響的概念－信任（trust）。

[14] Miltgen 與 Smith（2015）將其稱之為「管制知識」（Regulatory knowledge）。

DOI:10.6814/NCCU202000421

三、政府信任的影響

「信任」是電子化政府研究中，不可或缺的重要元素，但由於不同研究往往給予信任不同的定義與角色，導致電子化政府中的信任概念是混淆且難以界定（李仲彬，2011）。當「信任」的內涵無所不包時，就失去了這個概念的意義，像是有許多研究研究雖都是以「信任」作為自變數，來探討信任對於隱私風險跟電子化服務使用意願的關聯，但不論是在內涵或是變數操作化上，都存在有相當程度的差異。舉例而言，Bélanger與Carter（2008）、Teo等人（2009）的研究當中的信任代表的是民眾對於政府機構的信任；而Abu-Shanab與Al-Azzam（2012）、Sang等人（2009）研究當中的信任則代表政府線上服務的可信賴性與可靠度。

為釐清電子化政府信任的多種面向，李仲彬（2011）藉由文獻檢閱的方式，綜整了信任在電子化政府當中的四個面向，分別是組織信任、制度信任、科技信任與電子化政府信任；並認為數位治理當中的信任議題，無法純然地僅探討資通訊領域下的電子化政府信任，而是與傳統的政府施政信任有高度關聯。再加上隱私問題的根源之一為委託代理人理論當中，提供資料的個人（委託人）跟蒐集資料的機構（代理人）間所產生的資訊不對稱現象（Li, 2012）；由於政府在隱私議題中會扮演蒐集民眾資料的代理人角色，故政府信任所產生的效果將會近似於其他研究所提及的「機構信任」效果（Dinev et al., 2006; Kehr, Kowatsch, Wentzel & Fleisch, 2015）。因此，本研究認為在隱私研究當中，電子化政府信任應被定義為民眾對於政府組織的信任感較為適當，故後續的研究討論與分析則將側重政府信任的概念。

在過去的研究當中，政府信任對於隱私考量與提供個人資訊的影響可再分為直接效果與間接效果；也就是說，有些研究認為政府信任會直接影響個人意願，而有些研究則認為政府信任會藉由消除隱私上的風險認知，轉而間接影響個人意

DOI:10.6814/NCCU202000421

願。在直接影響部分，Carter與Bélanger（2005）認為除了科技接受模型與創新擴散理論（Diffusion of Innovation，簡稱DOI）可以用來解釋公民採用電子化服務的意願外，民眾對於網路與政府的信任度（trustworthiness）也是影響其採用電子化服務意願的另外一項重要因素。Teo、Srivastava與Jiang（2009）的研究也指出，相對於技術層次的信任（trust in technology），電子化政府信任的基礎是民眾對於政府的信任，高度的電子化政府信任有助於提高民眾持續採用電子化政府服務的意願，其他研究大多也支持電子化政府信任與民眾使用電子化政府服務意圖間的正向關聯（Abu-Shanab & Al-Azzam, 2012; Sang, Lee, & Lee, 2009）。在間接影響部分，有研究指出民眾對機構的信任感，可以消除使用者對電子化政府服務的風險感知，並藉以提高公民採用電子化政府服務的意願（Warkentin, Gefen, Pavlou, & Rose, 2002）。Bélanger與Carter（2008）的研究則同時驗證了政府信任對電子化政府服務使用意圖的直接與間接效果，也就是政府信任會減少民眾的感知風險，同時也會增強民眾使用電子化政府服務的意願。

綜整上述討論，本研究認為民眾對電子化政府的信任主要源於對政府機關這位資料蒐集代理人的信任感，此信任感有助於降低隱私風險認知，並提高授權個人資料的意願。除此之外，現有關於電子化政府信任的研究大多以「採用電子化政府服務的意願」作為最終的依變項（outcome variable），但本研究所關注的依變項則是「提供個人資料的意願」。本研究認為，未來的數位服務將更加重視個人化服務的提供，因此提供個人資訊的意願將會是未來採用電子化政府服務的一項重要的先決條件；較為可惜的是，目前僅有少數的數位治理研究以個人資料揭露意願做為探討對象（Mutimukwe, Kolkowska, & Grönlund, 2019），因此本研究成果將可適時補足現有研究缺口。

DOI:10.6814/NCCU202000421

最後，過去探討隱私管理的實證研究，絕大多數來自於資訊管理或數位商務領域。然而本研究認為，當數位治理領域應用隱私計算模型時，應考量政府與企業間的不同，例如政府除擁有更高程度的強制力外，民眾對於政府決策亦有相當程度的順服義務。據此，本節最後將探討在電子化政府的發展下，政府有系統性地蒐集民眾個人資料，其背後所可能產生的政府監控疑慮。

四、政府監控疑慮的影響

政府監控是數位治理在未來更深入民眾生活時，無法避免討論的一項難題。在政府開始運用資通訊科技的初期，即有學者認為電子化政府在某些層面強化了國家對於虛擬世界民眾的資訊取得、儲存與運用的能力，這種對於人民無孔不入的資訊監控（information surveillance）將有助於鞏固國家的統治與穩定（管中祥，2001）。政府大規模蒐集個人資訊的行為，也經常形成民眾情緒上的擔憂，並將政府賦予反烏托邦（dystopian）的「老大哥」形象來表達對政府監控的恐懼（Thompson et al., 2015）。在自由之家於2018年針對全球網路自由程度進行的調查中，發現全球許多政府在過去幾年，都戲劇性地開始增加在社群平台上的資訊控管，並且對於個人隱私產生一定程度侵害（Shahbaz, 2018）。

監控具有模糊且多層次的內涵，Foucault（1995）認為監控最早的形式可溯源至哲學家Jeremy Bentham所提出的全景監獄（Panopticon）設計；環形監獄藉由分隔囚室與採光設計等方式，營造出統治與紀律的氛圍，使得囚犯陷於一種無時無刻都被監視的感知之中。由此可知，Foucault將認為監控為一種壓抑與控制社會的手段與形式（Foucault, 1995: 195-220）。有別於Foucault所提出的社會控制功能，其他學者嘗試給予監控一個較具中立性的定義。例如Giddens（1985: 180-181）將監控視為一種國家的檔案蒐集行為，意指政府基於官僚或行政目的，蒐

DOI:10.6814/NCCU202000421

集、校對與重新編碼公民資訊的過程，舉凡出生紀錄、婚姻紀錄、職業統計或死亡紀錄等個人資訊的建檔與蒐集都屬於國家監控的範疇。

Allmer（2011）綜整了上述兩種有關於監控定義的討論，認為監控可分類為全景式（panoptic）與非全景式（non- panoptic）這兩種定義。全景式定義認為監控是負面的，會被用於侵害、壓迫公民以促成國家權力的集中化；非全景式定義則認為監控是中立的，僅僅反映出資料蒐集的技術過程，除了可能帶動國家權力集中外，也會有公民賦權的功能，例如提供公民與國家交流的機會跟能力（Albrechtslund, 2008）。然而，在資通訊科技快速發展的趨勢之下，Allmer（2011）認為非全景式的監控定義忽略了國家與大型私人企業具備不對稱的權力與資訊蒐集能力，未來的資訊社會監控形式將具備（1）數據更龐大、精確；（2）更分散且全方面的監控；（3）更快的資訊傳輸速度等特性。

在資通訊與網路快速開展的現代，不少研究或人權團體開使重視上述這種新形式的監控對人權、甚至是對廣泛的政治權利所造成的影響。例如Bernal（2016: 260）認為，監控所產生的影響不止於個人隱私權上的侵害，同時也影響個人生活方面的自治與自由權利，並且會侵蝕社區的重要功能，例如集會結社與言論自由等。Stoycheff、Liu、Xu與Wibowo（2019）以政府介入社群網站隱私條約的新聞報導作為刺激，來檢驗國家監控情境對公民的影響，發現國家監控情境可以顯著地阻卻民眾的意圖非法行為，但同時也會降低民眾線上參與的意願，顯示國家監控會產生相當程度的寒蟬效應，進而限縮公民的政治權利。

值得注意的是，現代國家越來越強調在基於安全與便利等目的下，透過資訊科技蒐集公民的個人資訊，使得侵犯隱私的研究對象開始從企業轉變為政府（Dinev, Bellotto, Hart, Russo, & Serra, 2006）。Dinev等人（2006）比較美國與義

DOI:10.6814/NCCU202000421

大利的一項跨國研究發現，當民眾對於政府監控有較高度的需求時，其對於隱私的關切程度也會較低。此外，該研究也討論了不同文化價值所產生的差異，發現美國民眾對反恐與安全的高度重視，導致美國民眾對於政府監控的需求較義大利民眾來得高。[15]其他研究也探討了國家監控與隱私間的關聯，例如Dinev等人（2008）認為911事件後，政府機構為提高國家安全所採取的多個大規模政策，從而導致民眾與政府機構間資訊不對稱的問題逐漸增長，並從實證資料發現民眾對政府侵害的擔憂會直接提高其對於隱私的關切。

除此之外，Steinfeld（2017）探討個人對國家監控與企業監控間的認知差異，發現當政府宣稱基於反恐或是安全考量時，公民會高度支持國家監控；但當蒐集資料的對象是企業時，公民則會擔憂私人企業的監控造成個人隱私的侵害，因此私人企業必須透過物質或金錢的方式來給予公民補償。值得注意的是，Steinfeld（2017）的研究亦發現「政府信任」是對民眾對國家監控支持與否最具預測力的因素，換言之，高度的政府信任可以提高公民對國家監控的支持。

綜合上述，國家監控有時被視為控制公民行動與集中化國家權力的工具，但部分為國家監控行為辯護的論點，則認為國家監控應被視為是中立性的資訊蒐集活動，公民只要沒有非法行為，即不用擔心國家的監控。本研究認為民眾對政府監控的疑慮將可能產生寒蟬效應，從而提高民眾對於隱私風險的認知，並使得民眾對授權個人資料感到卻步。更具體而言，本研究認為民眾對政府的監控疑慮會提高其隱私風險上的認知，同時降低其授權個人資料的意願。另外，政府信任與政府監控疑慮間的交互關係亦值得重視，高度的政府信任有助於減少民眾對政府監控上的疑慮。

[15] 需要額外說明的是，Dinev 等人的研究取樣時間是在 2001 年的 911 事件發生後，因此恐怖事件造成的情境影響可能會產生推論上的限制。

DOI:10.6814/NCCU202000421

本節綜整了預期投入、風險管理機制、政府信任與政府監控疑慮等四種隱私情境在隱私計算模型中的角色，嘗試完善本研究之研究模型。整合本章的內容來看，本研究在研究架構上以隱私計算模型為基底，以及應用擴展的二元隱私計算概念（隱私計算與風險計算），並加入數個使用情境上的可能影響，以試圖釐清影響個人資料授權意願的隱私因素。下一章節將說明本研究的研究架構、研究假設、變項操作化、資料蒐集流程與統計方法。

DOI:10.6814/NCCU202000421

DOI:10.6814/NCCU202000421

第三章　研究設計

本章將說明研究架構與假設，並且根據過去文獻內的操作化定義設計問卷，最後說明資料蒐集流程與概要的統計方法介紹。

第一節 研究架構與研究假設

首先需要再次說明的是，與企業或其他組織不同，由於政府已透過不同方式蒐集民眾的個人資料並儲存於業務資料庫中，因此政府並不會實際與民眾索取資料，而是民眾可以透過數位身份識別證，授權給特定機關來取用個人資料。本研究認為個人資訊揭露意願與個人資料授權意願為兩個重疊的概念，只是適用的機構對象不同，前者多用於電子商務領域，而後者則用於數位治理與電子化政府領域。如同本研究先前對於兩者的討論，這兩個概念都是代表資料主體（也就是民眾）將個人資料提供給代理機構（也就是政府）使用，以利後續服務提供的接受程度。因此後續分析為避免用詞混淆，將以個人資料授權意願作為主要用詞。

基於文獻檢閱時的討論，本研究運用Li（2012）所提出的二元隱私計算模型來探討數位身分識別政策下，民眾對於個人資料的授權意願。圖1為本研究的研究架構，而表1則為本研究所欲檢驗的研究假設。歸納而言，隱私利益會提高民眾授權個人資料的意願，而隱私風險則會降低授權意願。此外，民眾對於隱私風險的考量也同時受到風險評價與應對評價的影響，風險評價會提高對於隱私風險的認知，而應對評價則可能降低民眾對於揭露資料的風險認知。最後，本研究也探討數個政府因素對個人資料揭露意願直接與間接效果，例如政府信任、風險管理機制與政府監控疑慮等對隱私風險認知跟個人資料授權意願的影響。

DOI:10.6814/NCCU202000421

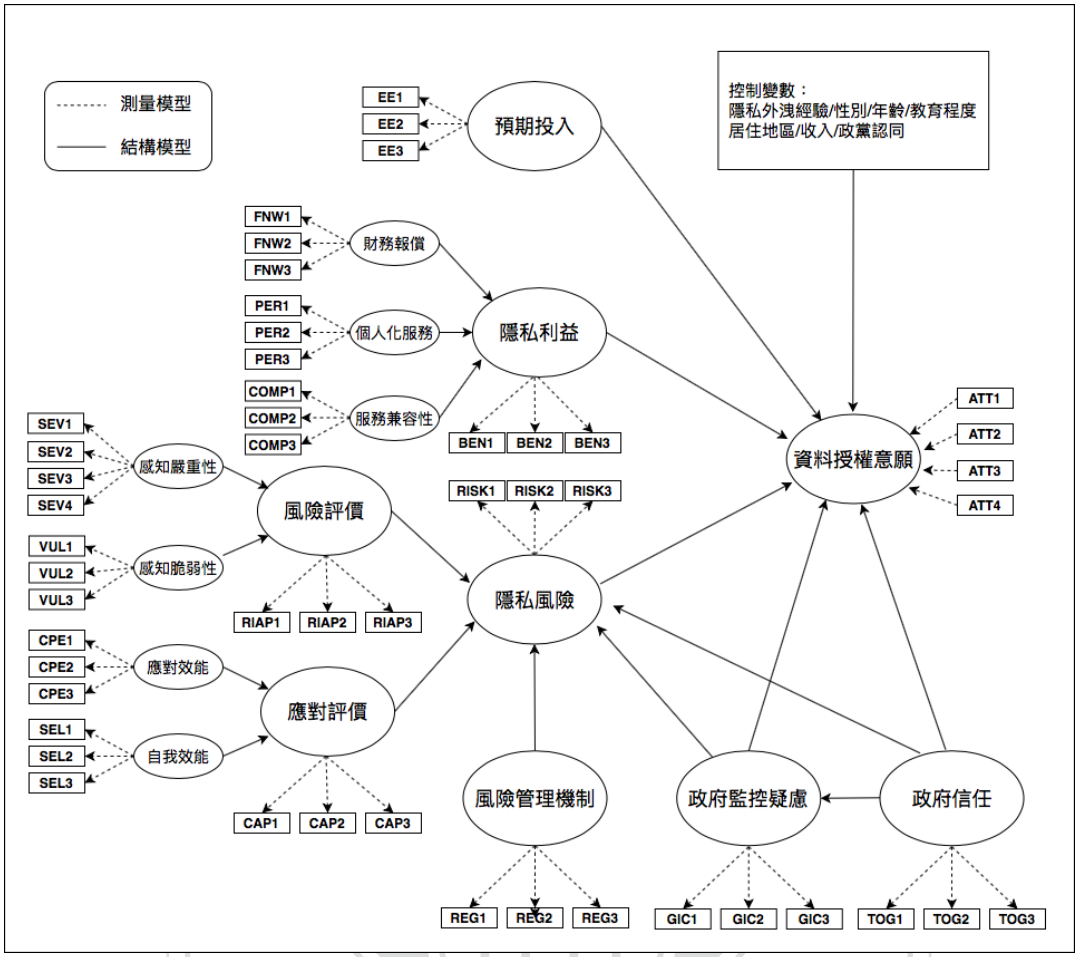

圖 1 研究架構

資料來源：本研究自行繪製。

表 1 研究假設

編號	研究假設	參考文獻
H1	隱私利益認知越高，則資料授權意願越高	Dinev & Hart, 2006; Xu et al., 2009
H2	隱私風險認知越高，則資料授權意願越低	Dinev & Hart, 2006; Xu et al., 2009
H3	自我風險評價越高，則隱私風險認知越高	Li, 2012; Kim & Kim, 2018
H4	自我應對評價越高，則隱私風險認知越低	Li, 2012; Kim & Kim, 2018
H5	政府信任感越高，則資料授權授權意願越高	Bélanger & Carter, 2008
H6	政府信任感越高，則隱私風險認知越低	Bélanger & Carter, 2008
H7	政府監控疑慮越高，則資料授權授權意願越低	Dinev et al., 2006
H8	政府監控疑慮越高，則隱私風險認知越高	Dinev et al., 2006
H9	預期投入成本越低，則資料授權授權意願越高	Venkatesh et al., 2003
H10	風險管理機制認知越高，則隱私風險認知越低	Miltgen & Smith, 2015
H11	政府信任感越高，則政府監控疑慮越低	Steinfeld, 2017

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

第二節　變項操作化

本研究依循過去文獻所執行的問卷內容，重新編譯並納入數位身分識別證的要素後，將各研究構面的操作化定義整理如表2。需要特別說明的是，由於現有針對二元隱私計算模型的實證研究均只發展了初階因素的操作性定義，也就是僅發展出感知脆弱性、感知嚴重性、應對效能與自我效能這四個構面的操作性定義（Kim & Kim, 2016; 2018），尚缺乏風險評價與應對評價等二階因素的操作性定義。因此，本研究溯源Li（2012）所提出的架構中，Li認為應對評價這項概念的源頭為計劃行為理論中的自我控制知覺（perceived behavioral control），因此本研究援引Azjen與Madden（1986）對於自我控制知覺的衡量作為替代指標。此外，由於風險評價代表資料洩漏的淨風險，因此本研究援引發展已久的全球隱私關切指標（Global Information Privacy Concern）來作為風險評價的替代指標（Malhotra, Kim, & Agarwal, 2004）。

在控制變項部分，本研究同時也蒐集受訪者的性別、年齡、教育程度、居住地區、收入、隱私外洩經驗與政黨認同等基本資料作為控制變項。受訪者基本資料分配表可參考表3，重新編碼過程則可參考附錄三。

DOI:10.6814/NCCU202000421

表 2 問卷構面與操作性定義

構面	操作性定義
資訊授權意願 Kim & Kim, 2018	ATT1 當我有個人化服務需求時，我願意透過數位身分識別，授權政府存取包含我的性別、年齡、婚姻狀況等個人資料
	ATT2 當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我過去的使用紀錄
	ATT3 當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的醫療與健康資訊
	ATT4 當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的銀行與財務資訊
隱私風險 Xu et al., 2009	RISK1 透過數位身分識別證授權政府機關使用我的個人資料，可能會產生預期之外的負面後果
	RISK2 透過數位身分識別證授權政府機關使用我的個人資料，有很高的機率會導致損失
	RISK3 整體來說，透過數位身分識別證授權政府機關使用我的個人資料是有風險的
隱私利益 Xu et al., 2011	BEN1 數位身分識別證有助於縮短我搜尋公共服務的時間
	BEN2 數位身分識別證有助於提高我所獲得的公共服務品質
	BEN3 整體而言，我認為使用數位身分識別證是有益的
財務報償 Xu et al., 2009	FNW1 透過數位身分識別證可以讓我申請到更多的社會福利補助
	FNW2 透過數位身分識別證可以節省我申請公共服務時的費用
	FNW3 對我而言，使用數位身分識別證具有經濟上的效益
個人化服務 Xu et al., 2011	PER1 數位身分識別證可以提供適合我的個人化公共服務
	PER2 數位身分識別證可以提供我想要的公共服務資訊
	PER3 數位身分識別證可以為我量身打造更多的個人化公共服務
服務兼容性	COMP1 數位身分識別證可以與我的工作緊密結合

DOI:10.6814/NCCU202000421

構面	操作性定義
Kim et al., 2019	COMP2 數位身分識別證適合運用在我的工作上
	COMP3 數位身分識別證可以提高我的工作效率
風險評價 Malhotra et al., 2004	RIAP1 授權個人資料給政府機關，對我來說是件很敏感的事
	RIAP2 授權個人資料給政府機關，可能會讓我的個人隱私在網路上被其他人搜尋到
	RIAP3 整體來說，將個人資料授權給政府機關會造成隱私問題
感知嚴重性 Kim & Kim, 2016	SEV1 當個人資料洩漏時，我的隱私可能會受到侵犯
	SEV2 當個人資料洩漏時，可能會造成我在金錢上的損失
	SEV3 整體而言，我認為個人資料洩漏是個嚴重的問題
感知脆弱性 Kim & Kim, 2016	VUL1 我的個人資料可能會不經我的同意被分享給第三方
	VUL2 我的個人資料可能會被用於服務提供的用途之外
	VUL3 我的個人資料可能會被非法的使用
應對評價 Ajzen & Madden, 1986	CAP1 我可以自行決定是否授權個人資料給政府機關
	CAP2 我可以掌握授權給政府機關的個人資料範圍
	CAP3 整體而言，我對於個人資料的授權有充分控制權
應對效能 Kim & Kim, 2016	CPE1 我有能力可以管理自己的個人資料
	CPE2 我可以遵循預防措施來保護個人資料
	CPE3 每當需要時，我都可以採取預防措施來保護自己的隱私
自我效能 Kim & Kim, 2016	SEL1 我可以防止他人非法存取我的個人資料
	SEL2 我可以防止個人資料洩漏造成的詐騙或身分盜用等損失

DOI:10.6814/NCCU202000421

構面	操作性定義
	SEL3 整體而言，我可以保護個人資料的安全
政府信任 Bélanger & Carter, 2008	TOG1 政府機關所提供的線上交易服務是值得信任的
	TOG2 我相信政府機關會維護我的最高利益
	TOG3 整體來說，政府機關是值得信任的
風險管理機制 Miltgen & Smith, 2015	REG1 我相信政府會運用安全的技術來管理我的個人資料
	REG2 當我的個人資料被濫用時，我可以取得政府相關單位的協助
	REG3 我相信政府會在適當的法律授權下來運用我的個人資料
政府監控疑慮 Dinev et al., 2006	GIC1 我擔心政府擁有監控網路活動的權力
	GIC2 我擔心政府擁有監控網路活動的能力
	GIC3 我擔心我在網路上的活動紀錄會受到政府的審查
預期投入 Venkatesh et al., 2012	EE1 對我而言，學習如何運用數位身分識別證很容易
	EE2 我認為數位身分識別證的操作是簡單且易懂的
	EE3 對我而言，熟練地使用數位身分識別證是很輕鬆的

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

第三節 資料蒐集流程

在資料蒐集部分，本研究使用政治大學選舉研究中心建置的「線上調查實驗室」（PollcracyLab），以網路調查的形式來蒐集資料。儘管網路調查勢必面臨樣本涵蓋偏差與無回應率高等問題（Dillman, Smyth, & Christian, 2014），但網路調查同時也具備成本較低、調查時程較短等優點（俞振華，2016：97）。除此之外，本研究所選擇的PollcracyLab，其中有92%的會員都是透過電話訪問調查方式蒐集而來的準機率樣本（pseudo-probability samples），與其他採完全開放填答的網路調查相比，PollcracyLab所蒐集的調查資料應具有較高效度。

需要注意的是，即使網路使用人數逐漸提高的現代，網路使用者與一般民眾的異質性界線看似逐漸消彌，但PollcracyLab的受訪樣本仍與電訪樣本有著相當程度的落差。俞振華（2016：108-112）即比較PollcracyLab網路調查與電訪調查所得到的樣本特質差異，即發現網路調查所得到的樣本，以30歲以下的年輕族群、大專以上學歷跟居住在都會區的族群為主。然而，雖然樣本的組成有所差異，俞振華（2016：108-112）在後續應用網路調查樣本與電訪樣本所進行平行比較之中，發現兩者在迴歸模型的統計結果差異不大，惟網路調查的統計穩定性較低。因此，在調查成本有限的情況下，應用PollcracyLab進行網路調查所得到的結果仍具有一定的效度，也就是「雖不中，亦不遠矣」。

基於上述成本與效益間的最適考量，本研究委託PollcracyLab協助執行本研究的資料蒐集過程。本研究於2019年12月13日執行問卷前測，共計取得31份樣本作為問卷修改之參考。在完成問卷修改後，本研究於2020年2月18日開始以正式問卷進行資料蒐集，並於2020年2月21日完成所需樣本數，經刪除未完整填答的樣本後，最終得到743份成功樣本作為後續分析之用。

DOI:10.6814/NCCU202000421

第四節 統計方法：PLS-SEM

本研究將運用結構方程式中的偏最小平方法（Partial Least Squares Structural Equation Modeling，簡稱PLS-SEM）作為本研究的主要統計方法。PLS-SEM與廣為應用的以共變異數為基礎的結構方程式(covariance-based SEM，簡稱CB-SEM）不同，PLS-SEM係以變異數為基礎（variance-based）的SEM方法，應用最小平方法的方式來進行路徑係數估算；PLS-SEM亦具備樣本需求較少、無資料分布假定、可同時處理反映性測量模式（reflective measurement）跟形成性測量模式（formative measurement），且較適用於結構模式複雜的分析上等特性（湯家偉，2016：11-14）。

由於本研究構念中的「資料授權意願」（可參圖1），其所測量的指標之間在邏輯上不具有可替代性，也就是個人醫療資料的授權意願並無法去替代其他個人資訊的授權意願，因此應將其視為形成性測量模式來避免模型錯誤辨識(model misspecification）而造成的估計偏誤（MacKenzie, Podsakoff, & Jarvis, 2005）。再加上在社會科學研究當中，CB-SEM所要求的變數多元常態性假定（multivariate normal distribution）往往較難達成，從而導致最大概似法估計上的偏誤。基於上述考量，本研究將選用PLS-SEM作為主要的統計方法，在統計軟體部分，本研究則採用R軟體中的semPLS套件進行分析（Monecke & Leisch, 2012）；而PLS-SEM的模型品質判讀方式與準則、路徑係數顯著性考驗等內涵，本研究將於資料分析章節說明。

DOI:10.6814/NCCU202000421

第四章　資料分析

本章將說明本研究的統計模型分析結果與主要研究發現，由於本研究採用PLS-SEM作為主要統計方法，因此模型可再區分為測量模型與結構模型。第一節將說明成功樣本的基本資料分布，與各個調查題目的敘述統計結果；第二節則說明測量模型的評估與信效度分析；第三節則說明結構模型的統計結果與主要研究發現；最後於第四節處針對原有研究架構不足之處提出討論。

第一節 敘述統計

表3呈現本次成功樣本的基本資料統計，本次調查共計完成743份成功樣本，在樣本數需求的部分，現有樣本數滿足結構方程式中的「十倍數原則」，意即樣本數至少需為路徑模型中，指向任一潛在變數的最大箭頭數的10倍（湯家偉，2016：15）。[16]其中，有超過四成的受訪者居住於北部地區，而男性受訪者略多於女性受訪者；由於採用網路調查的原因，因此在年齡分佈上以49歲以下的受訪者居多，且超過半數（66.5%）的受訪者具有大學以上學歷。此外，在隱私外洩經驗上，有32.7%的受訪者表示在過去一年來，自己的個人資料曾經有外洩的經驗。在政黨認同部份，將近一半的受訪者政黨認同為中立或其他政黨，而泛綠支持者略多於泛藍支持者，與政治大學選舉研究中心歷年的調查結果相比，本次樣本的政黨認同分佈情形與全國民眾政黨傾向態度差異不大。[17]

另外需要說明的是，雖然所回收的受訪樣本在年齡、教育程度、居住地區等基本人口變項上與我國全體人口有所差異，但由於本研究的資料來源（Pollcracy Lab）的受訪者名單並非源於單一母體清冊所得到的網路使用者資料，而是從不

[16] 「資料授權意願」為本研究中被指向最多箭頭的潛在變數，共有 19 條箭頭指向該潛在變數。
[17] 國立政治大學選舉研究中心（2019）。重要政治態度分佈趨勢圖，2020 年 3 月 11 日，取自：https://esc.nccu.edu.tw/course/news.php?Sn=165#。

DOI:10.6814/NCCU202000421

同調查管道（例如面訪、住宅電話調查、電話調查）所蒐集而來，國內目前尚未有適合的混合式網路人口調查研究可作為網路人口的母體清冊參考。在缺乏合適加權清冊的條件下，貿然透過戶籍人口或其他調查結果進行加權，不僅無法解決人口特徵上的偏差，反而可能增加額外的誤差（李政忠，2004）。基於上述考量，本研究後續的統計結果均採無加權方式的原始資料呈現。

表 3 樣本基本資料表

變數名稱		數量	比例
性別	男性	407	54.8%
	女性	336	45.2%
年齡	20 至 29 歲	135	18.2%
	30 至 39 歲	205	27.6%
	40 至 49 歲	200	26.9%
	50 至 59 歲	137	18.4%
	60 歲及以上	66	8.9%
教育程度	高中、職及以下	92	12.4%
	專科	157	21.1%
	大學及以上	494	66.5%
居住地區	北部地區	344	46.3%
	中部地區	190	25.6%
	南部地區	185	24.9%
	東部與離島地區	24	3.2%
隱私外洩經驗	有	243	32.7%
	無	500	67.3%
收入	28000 以下	118	15.9%
	28001 元~39000 元	143	19.2%
	39001 元~49000 元	103	13.9%
	49001 元~59000 元	113	15.2%
	59001 元~70000 元	80	10.8%
	70001 元~80000 元	55	7.4%
	80001 元~94000 元	44	5.9%
	94001 元~111000 元	31	4.2%

DOI:10.6814/NCCU202000421

變數名稱		數量	比例
	111001 元以上	56	7.5%
政黨認同	泛綠[18]	222	29.9%
	泛藍[19]	167	22.5%
	中立或其他政黨	354	47.6%
樣本總數		743	100.0%

資料來源：本研究自行整理。

表4呈現各測量變項的調查結果，本研究的調查題項採用1至7的連續尺度設計，並在網路問卷設計時採強制受訪者填答的機制，若沒有完整填答則無法送出完成問卷，因此本研究後續所分析的資料檔中並無包含任一遺漏值。一般而言，研究者可以藉由平均數、標準差與偏態等三項描述性統計量來評估測量變項，三者各自的衡量標準為：（1）各題項的平均數應介於該構面平均數的正負1.5個標準差之內；（2）各題項的標準差應大於0.75；（3）偏態絕對值應小於0.7（陳裕寬，2018：241）。

從表4中所呈現的三項統計量可以發現，所有測量變數的平均數均落於構面平均數正負1.5個標準差之間，代表題項間的衡量沒有過大的偏離；其次，所有測量變數的標準差均大於0.75，顯示同一構念下的題項具備一定鑑別度；最後，有5個測量變數的偏態絕對值大於0.7，包含感知嚴重性與感知脆弱性構念內的5個測量變數，顯示這兩個構念沒有符合常態性的要求。然而，由於PLS-SEM並不嚴格要求樣本分配的常態性，在資料違反常態分佈時，仍可以得出可靠的估計結果（湯家偉，2016：17），後續的參數顯著性考驗亦是利用無母數估計的拔靴法（bootstrapping）來進行（李承傑、董旭英，2017），因此違反常態性的測量變數仍可留於後續模型內進行分析，並不影響參數估計的可靠性。

[18] 民進黨、臺灣團結聯盟。
[19] 國民黨、親民黨、新黨。

DOI:10.6814/NCCU202000421

值得注意的是，在資料授權意願當中的醫療資訊授權意願題項ATT3，[20]所呈現的結果與原先預期有所差異。由於醫療紀錄屬於較為私密性的個人資料，本研究原本預期民眾的醫療資訊授權意願會低於個人基本資料與使用紀錄資料的授權意願，而略高於財務資訊授權意願。然而本次調查結果卻表明，民眾對醫療資訊的授權意願卻為該構面當中最高，此有趣的發現與蕭乃沂等人（2017）的結果一致，顯示我國民眾對醫療資訊的授權接受程度相當高，可能係民眾對國內醫療體系的高度信賴感所導致。若進一步比較各構面則可以發現，個人資料的感知嚴重性與感知脆弱性為明顯的左偏分配，顯示有不少民眾擔心個人資料所可能產生的外洩風險與危害。此外，政府監控疑慮的構面平均數為5.30，明顯高過於政府信任的構面平均數4.18，表示民眾對於政府對線上活動的可能監控行為，仍有抱持一定疑慮。

在信度分析部分，本研究的信度分析採用「內在一致性信度」（internal consistency reliability）來檢測，以Cronbach's α值呈現構面內各個問項的答題一致性。一般來說，Cronbach's α值大於0.7可以代表該構面信度良好，0.5至0.7之間則是信度中等，低於0.5則為信度不佳（羅清俊，2010：74）；從表4的結果可以發現，本研究所使用的16個構面均有良好的信度。其中需要特別說明的是，原先預期「資料授權意願」為一低信度的形成性指標，而雖然初步的結果顯示該構面具有高度的信度，然而本研究仍舊認為該構念所測量的指標之間在邏輯上不具有可替代性，因此在後續分析上仍將其視為形成性指標加以建構。黃紀（2013）曾直指計量方法（quantitative methods）的核心，即是緊扣理論的意涵，透過一系列的邏輯推論、建構假設、操作化、資料統計等流程來驗證抽象的理論概念，雖然資

[20] 題項題目為：「當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的醫療與健康資訊。」

DOI:10.6814/NCCU202000421

料分析的結果或可作為未來研究補充修正的空間，但在新的理論架構被清晰建構之前，研究者應先從現有理論為基礎進行邏輯推論為宜。

本節說明調查樣本的基本資料分布與測量變項的描述性統計量，並針對部分較值得探討的統計量進行說明與補充，以提供整體資料的概要輪廓，各題項詳細的次數分配表可參閱附錄二。然而，描述性統計所能提供的資訊仍相當有限，因此後續將於第二節與第三節說明整體模型的分析結果。

表 4 測量變項敘述統計表

潛在變項/構面	測量指標	平均數	標準差	偏態	構面平均數 [± 1.5 S.D.]	構面信度[21]
資料授權意願	ATT1	4.69	1.39	-0.57	4.43 [2.52 - 6.34]	0.876
	ATT2	4.47	1.48	-0.40		
	ATT3	4.91	1.44	-0.63		
	ATT4	3.65	1.65	0.02		
隱私風險	RISK1	4.99	1.30	-0.12	4.79 [2.96 - 6.63]	0.907
	RISK2	4.53	1.37	0.09		
	RISK3	4.86	1.32	-0.09		
隱私利益	BEN1	5.03	1.35	-0.56	4.94 [3.05 - 6.83]	0.927
	BEN2	4.83	1.35	-0.42		
	BEN3	4.96	1.35	-0.45		
財務報償	FNW1	4.34	1.51	-0.20	4.81 [2.95 - 6.68]	0.855
	FNW2	5.19	1.33	-0.67		
	FNW3	4.91	1.39	-0.49		
個性化服務	PER1	5.04	1.29	-0.48	4.94 [3.05 - 6.82]	0.937
	PER2	4.96	1.31	-0.41		
	PER3	4.81	1.39	-0.40		
服務兼容性	COMP1	4.20	1.48	-0.08	4.03 [1.97 - 6.09]	0.917
	COMP2	4.01	1.46	0.04		
	COMP3	3.88	1.52	0.01		
風險評價	RIAP1	5.05	1.41	-0.28	5.07	0.910

[21] 本研究採 Cronbach's alpha 係數作為信度指標。

DOI:10.6814/NCCU202000421

潛在變項/構面	測量指標	平均數	標準差	偏態	構面平均數 [± 1.5 S.D.]	構面信度[21]
	RIAP2	5.11	1.48	-0.38	[3.08 - 7.05]	
	RIAP3	5.04	1.43	-0.21		
感知嚴重性	SEV1	6.07	1.01	-1.03	5.95 [4.59 - 7.31]	0.774
	SEV2	5.56	1.21	-0.55		
	SEV3	6.23	1.04	-1.46		
感知脆弱性	VUL1	5.50	1.45	-1.16	5.45 [3.59 - 7.31]	0.867
	VUL2	5.55	1.32	-1.08		
	VUL3	5.32	1.42	-0.81		
應對評價	CAP1	4.92	1.47	-0.50	4.56 [2.53 - 6.59]	0.865
	CAP2	4.28	1.56	-0.06		
	CAP3	4.48	1.54	-0.16		
應對效能	CPE1	4.98	1.42	-0.54	5.02 [3.23 - 6.82]	0.871
	CPE2	5.14	1.26	-0.64		
	CPE3	4.94	1.35	-0.49		
自我效能	SEL1	3.92	1.51	0.15	4.17 [2.18 - 6.15]	0.884
	SEL2	4.14	1.52	-0.02		
	SEL3	4.46	1.37	-0.17		
政府信任	TOG1	4.33	1.43	-0.39	4.18 [2.06 - 6.30]	0.923
	TOG2	4.06	1.58	-0.21		
	TOG3	4.17	1.55	-0.35		
風險管理機制	REG1	4.49	1.59	-0.27	4.30 [2.30 - 6.29]	0.798
	REG2	4.17	1.57	-0.17		
	REG3	4.24	1.56	-0.29		
政府監控疑慮	GIC1	5.37	1.44	-0.60	5.30 [3.23 - 7.36]	0.925
	GIC2	5.31	1.46	-0.57		
	GIC3	5.21	1.53	-0.52		
預期投入	EE1	5.08	1.35	-0.51	4.98 [3.09 - 6.87]	0.949
	EE2	4.90	1.31	-0.33		
	EE3	4.97	1.31	-0.38		

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

第二節 測量模型的統計結果與評估

首先需要說明的是，結構方程式包含兩個主要模式，分別是呈現潛在變項（或可稱之為構念）與測量變項（或可稱之為指標）間關係的測量模型（measurement model）[22]，以及呈現潛在變項與潛在變項間關係的結構模型（structural model）[23]（湯家偉，2016：9）。由於PLS-SEM屬於整體估計的方法，也就是可以同時估計測量模型與結構模型，因此雖然本研究將結果分列於本章第二節與第三節呈現，但參數估計結果實際上係為同一模型所估計得來。除此之外，在參數權重計算方法（weighting scheme）部分，本研究依循湯家偉（2016：64）的建議，係採路徑權重計算法（path weighting scheme）來為內在潛在變數提供最高的R^2值，以最大化模型的解釋力。

另外，由於PLS-SEM對資料分布並無常態性假設，因此迴歸分析中的參數顯著性考驗並不適用於評估模型當中因素負荷量、權重與路徑係數的顯著與否，而需採用非參數估計的拔靴法來檢驗係數的顯著性（湯家偉：2016：107）。概要說明拔靴法的原理，即是從全體樣本中透過反覆抽取子樣本（即拔靴法抽樣數，bootstrap samples）來估計模型參數，透過多個子樣本所得到的結果來求出參數估計的平均值、標準差與信賴區間；一般來說，拔靴法的子樣本數應該大於成功樣本的總數，且建議以5,000個子樣本數為宜（湯家偉，2016：107-110）。後續測量模型與結構模型的因素負荷量與路徑係數的參數顯著性考驗，均是依循拔靴法的操作原則而得，後續分析則不再贅述。

在探討研究者所關心且較感興趣的潛在變項間的關聯前，具有信效度且真實反映研究構念的測量指標係結構方程式分析中不可或缺的要素。故本節首先將說

[22] 在 PLS-SEM 中亦可稱之為外在模型（outer model）。
[23] 在 PLS-SEM 中亦可稱之為內在模型（inner model）。

DOI:10.6814/NCCU202000421

明本研究測量模型的結果與評估其良莠。基於構念與測量變項間因果關係的不同，可再分為反映性測量模型與形成性測量模式來分別說明，兩者亦有不同的評估準則。

一、反映性測量模式的結果與評估

從表5的反映性指標分析結果可以發現，本研究中的所有測量變項與潛在變項間的因素負荷量係數均通過顯著考驗，表明潛在變項能充分反映測量變項衡量的概念。除了因素負荷量之外，研究者亦需要透過組合信度（composite reliability）、指標信度（indicator reliability）、平均變異萃取量（average variance extracted，簡稱AVE）與Fornell-Larcker指標（Fornell-Larcker criterion）來判別指標的信效度（湯家偉，2016：81-86）。

首先就組合信度的部分，組合信度介於0與1之間，當數值越高則代表該構念具備越高的內部一致性。組合信度的標準一般而言需大於0.7，但過高的組合信度亦可能產生問題，研究者需注意當組合信度大於0.95時，可能代表該構念的測量指標有冗餘、重複性的問題。本研究的潛在變項均符合0.7的組合信度標準，然而有5個構念可能有組合信度過高的冗餘性問題，包含隱私利益、個性化服務、政府信任、政府監控疑慮、預期投入。但由於每個潛在變項最少需要3個測量變項來估計出可靠的參數，因此本研究在後續分析上並未因組合信度過高的因素，刪除任一指標。

將標準化因素負荷量平方後可以得到指標信度，指標信度亦被稱之為指標共同性（communality），可以用來代表潛在變項解釋測量變項的程度。就常見的標準來說，潛在變項必須至少可以解釋測量變數50%的變異，也就是因素負荷量須大於0.708，而指標信度需大於0.5。從表5的結果來看，本研究的測量變項當中僅

DOI:10.6814/NCCU202000421

有REG1[24]的指標信度略低於0.5的標準，其餘測量變項均有0.65以上的高指標信度，顯示整體來說，潛在變項都能充分解釋測量變項的變異程度。

第三，平均變異萃取量(AVE)可以用來衡量潛在變項的輻合效度(convergent validity)，其計算方式為將同一構念中所有測量變項的指標信度加總，再求出平均值，用來代表該構念的平均共同性。與指標信度的標準相同，當AVE的值大於0.5時，即代表潛在變項解釋了測量指標超過一半的變異程度，也表示潛在變項所能解釋的比例大過於誤差項所能解釋的比例。從表5中可以發現，本研究所建構的潛在變項有良好的AVE值，絕大多數潛在變項的AVE值均在0.7以上。

最後，Fornell-Larcker指標是另一個較為嚴格的效度指標，用以衡量潛在變項之間的區別效度。Fornell-Larcker指標用來比較潛在變項AVE的平方根，與不同潛在變項間的相關係數之間的大小;潛在變項AVE的平方根應大於該潛在變項與模型內任意潛在變項的相關係數，也就是潛在變項對於其所屬的指標，相對於其他構念，應當擁有較大的共同變異。表6呈現本研究的Fornell-Larcker指標，除了形成性測量模式之外，所有的反映性測量模式在對角線上的數值(也就是該構念的AVE平方根)，應大於底下所有的數值(也就是該構念與其他構念的相關係數)才符合區別效度。需要額外說明的是，構念與構念間的相關係數，係經由模型估計後所得到各構念的因素分數 (factor score) 加以計算。

綜整來看，本研究的測量模型整體表現良好，潛在變項均能充分解釋測量變項的變異，Fornell-Larcker指標也支持各個潛在變項之間有區別效度的說法。然而，有部分潛在變項的組合信度過高，可能顯示問卷內的部分問題有冗餘之嫌，

[24] 題項題目為：「我相信政府會運用安全的技術來管理我的個人資料。」

DOI:10.6814/NCCU202000421

係未來研究者在採用相似問卷時需加以斟酌、修改之處。在說明完反映性模式後，本節的下個段落將說明形成性模式的結果與指標評估。

DOI:10.6814/NCCU202000421

表 5 反映性指標檢驗結果表

潛在變數	測量變數	因素負荷量	t 值	顯著水準	95%信賴區間		指標信度	組成信度	AVE
					下界	上界			
隱私風險	RISK1	0.896	84.16	***	0.874	0.916	0.804	0.942	0.843
	RISK2	0.923	108.62	***	0.905	0.938	0.851		
	RISK3	0.935	150.89	***	0.922	0.947	0.875		
隱私利益	BEN1	0.936	149.12	***	0.922	0.947	0.876	0.954	0.873
	BEN2	0.946	176.64	***	0.935	0.956	0.895		
	BEN3	0.921	110.01	***	0.903	0.936	0.848		
財務報償	FNW1	0.806	41.71	***	0.764	0.841	0.650	0.914	0.780
	FNW2	0.918	125.13	***	0.902	0.931	0.842		
	FNW3	0.921	144.30	***	0.908	0.933	0.849		
個性化服務	PER1	0.944	154.13	***	0.931	0.955	0.891	0.960	0.889
	PER2	0.948	137.47	***	0.933	0.960	0.899		
	PER3	0.936	150.69	***	0.922	0.947	0.876		
服務兼容性	COMP1	0.933	122.55	***	0.916	0.946	0.870	0.948	0.858
	COMP2	0.932	93.55	***	0.910	0.949	0.869		
	COMP3	0.913	90.63	***	0.892	0.932	0.834		
風險評價	RIAP1	0.899	78.73	***	0.876	0.920	0.809	0.943	0.848

DOI:10.6814/NCCU202000421

潛在變數	測量變數	因素負荷量	t 值	顯著水準	95%信賴區間		指標信度	組成信度	AVE
					下界	上界			
	RIAP2	0.926	124.85	***	0.911	0.940	0.857		
	RIAP3	0.936	140.21	***	0.922	0.948	0.876		
感知嚴重性	SEV1	0.837	47.93	***	0.800	0.867	0.700	0.871	0.693
	SEV2	0.836	57.76	***	0.805	0.861	0.699		
	SEV3	0.824	53.65	***	0.791	0.853	0.680		
感知脆弱性	VUL1	0.863	36.73	***	0.810	0.901	0.745	0.918	0.788
	VUL2	0.902	65.53	***	0.870	0.925	0.813		
	VUL3	0.898	67.59	***	0.871	0.923	0.807		
應對評價	CAP1	0.860	60.76	***	0.830	0.885	0.740	0.917	0.787
	CAP2	0.889	76.13	***	0.865	0.910	0.790		
	CAP3	0.911	108.57	***	0.894	0.927	0.830		
應對效能	CPE1	0.869	59.44	***	0.839	0.896	0.755	0.922	0.798
	CPE2	0.914	101.37	***	0.895	0.931	0.836		
	CPE3	0.897	73.43	***	0.870	0.918	0.804		
自我效能	SEL1	0.893	76.64	***	0.868	0.914	0.798	0.929	0.813
	SEL2	0.894	72.15	***	0.866	0.915	0.799		
	SEL3	0.917	124.36	***	0.902	0.930	0.841		
政府信任	TOG1	0.917	103.84	***	0.897	0.932	0.840	0.951	0.867

DOI:10.6814/NCCU202000421

潛在變數	測量變數	因素負荷量	t 值	顯著水準	95%信賴區間		指標信度	組成信度	AVE
					下界	上界			
	TOG2	0.937	120.53	***	0.920	0.950	0.878		
	TOG3	0.940	185.20	***	0.929	0.949	0.884		
風險管理機制	REG1	0.661	12.55	***	0.543	0.749	0.437	0.874	0.702
	REG2	0.897	63.66	***	0.864	0.921	0.805		
	REG3	0.929	106.01	***	0.911	0.946	0.862		
政府監控疑慮	GIC1	0.933	92.60	***	0.911	0.951	0.870	0.953	0.871
	GIC2	0.942	119.20	***	0.925	0.956	0.887		
	GIC3	0.924	117.33	***	0.908	0.939	0.854		
預期投入	EE1	0.947	172.61	***	0.935	0.957	0.897	0.967	0.907
	EE2	0.960	220.66	***	0.951	0.968	0.922		
	EE3	0.950	128.67	***	0.935	0.963	0.903		

資料來源：本研究自行整理。

說明：***：p＜0.001, **：p＜0.01, *：p＜0.05, NS：不顯著。

註：測量變數為 1-7 的連續尺度，採路徑權重計算法（path weighting scheme），信賴區間係藉由拔靴法所估計而得。

DOI:10.6814/NCCU202000421

表 6 Fornell-Larcker 指標

	資訊授權意願	隱私風險	隱私利益	財務報償	個性化服務	服務兼容性	風險評價	感知嚴重性	感知脆弱性	應對評價	應對效能	自我效能	政府信任	風險管理機制	政府監控疑慮	預期投入
資料授權意願	**形成性**															
隱私風險	-0.279	**0.918**														
隱私利益	0.613	-0.210	**0.934**													
財務報償	0.574	-0.176	0.744	**0.883**												
個性化服務	0.557	-0.173	0.788	0.842	**0.943**											
服務兼容性	0.450	-0.101	0.574	0.640	0.624	**0.926**										
風險評價	-0.324	0.674	-0.250	-0.189	-0.174	-0.130	**0.921**									
感知嚴重性	-0.050	0.374	0.022	0.086	0.111	-0.016	0.452	**0.832**								
感知脆弱性	-0.080	0.298	-0.051	-0.010	-0.046	-0.077	0.359	0.441	**0.888**							
應對評價	0.276	-0.040	0.274	0.292	0.273	0.249	-0.047	0.082	-0.171	**0.887**						
應對效能	0.217	0.031	0.220	0.203	0.207	0.168	-0.034	0.066	-0.135	0.595	**0.893**					
自我效能	0.187	0.020	0.232	0.204	0.224	0.232	-0.076	-0.014	-0.221	0.604	0.689	**0.902**				
政府信任	0.629	-0.401	0.597	0.527	0.522	0.456	-0.396	-0.109	-0.174	0.348	0.260	0.260	**0.931**			
風險管理機制	0.565	-0.393	0.543	0.503	0.490	0.435	-0.331	-0.073	-0.195	0.341	0.241	0.221	0.818	**0.838**		
政府監控疑慮	-0.341	0.535	-0.261	-0.194	-0.220	-0.156	0.571	0.326	0.275	-0.114	-0.080	-0.100	-0.474	-0.379	**0.933**	
預期投入	0.497	-0.099	0.733	0.539	0.557	0.422	-0.180	0.061	-0.013	0.260	0.279	0.256	0.472	0.385	-0.180	**0.952**

資料來源：本研究自行整理。

說明：對角線為構面的 AVE 平方根（僅反映性指標），其餘數字為潛在變數之間的相關係數，對角線數字應大於該欄其餘數字的絕對值才符合區別效度。

DOI:10.6814/NCCU202000421

二、形成性測量模式的結果與評估

形成性測量模式的特點在於測量變項被認為是同一構念當中的不同獨立成因，也就是測量指標間不一定會呈現高度的相關性，因此反映性指標所使用的組合信度、指標信度與平均變異萃取量已不適用於評估形成性測量模式。取而代之的是，研究者在一開始設計題項時應專注於內容效度（content validity），將該構念的主要面向納入問卷之中；在資料蒐集完成後，研究者也應先檢驗測量變項的共線性問題，再藉由拔靴法的方式對測量變項與潛在變項間的指標權重（outer weight）進行顯著性考驗，並利用因素負荷量來探討指標之間的相對與絕對重要性（湯家偉，2016：98-112）。

在內容效度部分，本研究所衡量的資料授權意願，從機敏性最高到最低可包含個人基本資料、使用紀錄、醫療資訊與財務金融資訊等四個不同內容的授權意願。此四個面向係參考過去研究的內涵加以綜整而出，並已盡可能考量到未來數位身分識別證政策實際執行之下，民眾授權個人資料的不同面向，故應具備有一定程度的內容效度。

除了內容效度的審視之外，研究者首先需評估形成性指標模式的共線性問題，由於形成性指標模式中的各個測量變數之間應相互不可替代，就統計資料的術語上來說的話，即是形成性測量指標之間不應該有高度的相關性，也就是不該有多元共線性（multicollinearity）的問題。研究者可以透過計算容忍值（tolerance）來檢視指標的共線性問題，容忍值代表某一指標無法被同一構念下的其他指標所解釋的變異量大小，當容忍值越小時，即代表該指標可以獨立解釋的變異量越小，其共線性問題越嚴重。形成性指標具體的容忍值計算步驟為：（1）以指標ATT1與其他同構念指標進行迴歸分析，也就是以ATT1作為依變數，ATT2、ATT3、

DOI:10.6814/NCCU202000421

ATT4作為解釋變數進行迴歸分析；（2）以該迴歸模型的R^2值計算ATT1的容忍值，計算公式為$1 - R^2_{ATT1}$；[25]（3）將依變項換為其他形成性測量指標（例如換為ATT2），並反覆執行上述兩個步驟，以得到4個指標的容忍值。

除此之外，研究者通常也會將容忍值取倒數後得到較為直觀的變異數膨脹係數（variance inflation factor，簡稱VIF），當VIF越大時，該指標的共線性則越嚴重。表7呈現本研究各個形成性測量指標的VIF值，根據湯家偉（2016：103）的標準，VIF小於5即代表低度的共線性問題，[26]而本研究的形成性測量指標共線性均小於3.5，代表測量指標間僅低度相關，亦反映此構念具備形成性指標的特質。

評估完共線性的問題後，研究者需要再透過拔靴法的方式，接續分析指標權重的顯著性，以及指標之間的相對與絕對貢獻。指標權重是形成性測量變項對形成性潛在變項的路徑係數，當指標權重通過顯著性考驗時，通常研究者即會保留該指標做後續分析。然而，當指標權重不顯著時，並非代表該測量指標品質不佳，而是需要考量到該測量指標對其所屬構念的絕對重要性（absolute importance）。當某一測量變項的指標權重未達顯著時，研究者需要再次分析其因素負荷量，若此指標的因素負荷量大於0.5，則代表指標仍舊對潛在變項具有絕對重要性；權重不顯著的結果僅是反映出該指標不具相對重要性，此時該指標依然建議予以保留。從表7的結果來看，ATT2在指標權重上未通過顯著性考驗，但其因素負荷量達0.861，代表對潛在變項具有絕對重要性，因此後續分析並未將該指標刪除。

本節完整探討與評估了本研究測量模型中的反映性測量模式與形成性測量模式的統計結果。整體來看，本研究模型中的測量模型表現良好，測量指標結果穩定、潛在變項與測量變項間的關係亦與原先預期相同，代表本研究的問卷設計

[25] 舉例而言，若該迴歸模型的 R^2 值為 0.9，ATT1 的容忍值即為 1 - 0.9 = 0.1。
[26] VIF 等於 5 時的容忍值為 0.2，代表該測量變數僅能獨立解釋 20%的變異量。

DOI:10.6814/NCCU202000421

具備相當的信效度，同時測量模型的良好結果，對於下一節的結構模型分析亦是一個可靠的分析基礎。

表 7 形成性指標檢驗結果表

潛在變數	測量變數	權重	t 值	因素負荷量	顯著水準	95% 信賴區間		VIF
						上界	下界	
資訊授權意願	ATT1	0.239	2.98	0.826	**	0.090	0.404	2.370
	ATT2	0.125	1.51	0.861	NS	-0.039	0.284	3.236
	ATT3	0.414	5.97	0.875	***	0.277	0.552	2.304
	ATT4	0.398	5.47	0.837	***	0.254	0.537	1.773

資料來源：本研究自行整理。

說明：***：$p<0.001$, **：$p<0.01$, *：$p<0.05$, NS：不顯著。

註：測量變數為 1-7 的連續尺度，採路徑權重計算法（path weighting scheme），信賴區間係藉由拔靴法所估計而得。

第三節 結構模型的統計結果與評估

在確認測量指標的信效度後，即可以開始分析結構模型當中，潛在變項間的關係與整體模型的預測程度。在結構模型當中，潛在變項可以再區分為兩者，分別是外生潛在變項（exogenous latent variable）與內生潛在變項（endogenous latent variable），前者即是研究中常提及的自變項與解釋變項，而後者則是依變項與結果變項。需要說明的是，PLS-SEM與CB-SEM不同，CB-SEM的統計邏輯係希望樣本共變數矩陣可以儘可能地與理論共變數矩陣相似，因此會透過如卡方值等整體適配度指標來評估理論模型是否被驗證。相比於使用整體適配度指標來評估模型的品質，PLS-SEM主要是以模型的預測能力作為判別模型的基準，因此評估的準則即是在**假定模型設定為正確時，內生潛在變項被外生潛在變項預測的程度**。

簡而言之，PLS-SEM的主要目的在於預測潛在變項之間的假定關係，並盡可能最大化內生潛在變項的解釋變異量，此統計特性特別適用於不同潛在變項在相對與絕對重要性間的比較。然而，由於缺乏前述的整體適配度指標，導致PLS-

DOI:10.6814/NCCU202000421

SEM難以直接不同模型間的品質，模型間的比較向來被視為PLS-SEM的最大限制（湯家偉，2016：63）。

PLS-SEM的結構模型評估標準主要步驟為共線性評估、路徑係數顯著性考驗、評估決定係數（R^2）與f^2效果值、評估預測相關性（Q^2）與q^2效應值（湯家偉，2016：138-139）。首先，共線性評估、R^2與Q^2可以用來衡量內生潛在變項被解釋的程度與模型的品質；其次，路徑係數顯著性考驗為主要的統計結果，用以呈現構念間的關聯；最後，f^2效果值與q^2效應值則可以用來評估潛在變項之間的相對重要性。因此本節將分為三個段落說明模型品質評估、模型路徑係數結果與潛在變項相對重要性比較。

一、結構模型品質評估

研究者可以透過共線性評估、評估決定係數（R^2）與評估預測相關性（Q^2）來衡量一個結構模型的良窳。首先在共線性評估部分，如同形成性指標模型中的共線性問題，研究者可以透過VIF值來判斷不同外生潛在變項的共線性程度。舉例而言，當我們要評估內生潛在變項「隱私風險」的共線性問題，即需要將與隱私風險有關的外生潛在變項篩選出來，在此例中即是風險評價、應對評價、政府信任、風險管理機制與政府監控疑慮等六個外生潛在變項。再以隱私風險的因素分數作為依變數，其餘變項的因素分數作為自變數的方式建立一迴歸模型，藉以評估同一內生潛在變項下的共線性問題，當共線性問題發生時，研究者即需要考慮刪除、合併構念，或是另外創建高階構念處理此問題（湯家偉，2016：139）。從表8的統計結果摘要中可以發現，外生潛在變項的VIF值均小於5，顯示結構模型並未有嚴重的共線性問題需要處理。

DOI:10.6814/NCCU202000421

決定係數（coefficient of determination，簡稱R^2值）係用來衡量結構模型測量的預測準確度，代表模型中所有外生潛在變項對內生潛在變項的整體效果，也是最常用來評估結構模型的標準，數值越高即代表模型預測力越好（湯家偉，2016：143）。一般而言，R^2值在行銷議題的學術研究中，0.75/0.5/0.25大致可被區分為顯著/中度/微弱的解釋力，但R^2值會因學門或模型複雜度而產生差異，因此顧客行為研究亦可接受0.2以上的R^2值（湯家偉，2016：143）。從圖2內的各個內生潛在變項R^2值可以發現，本研究的內生潛在變項幾乎都有微弱至中度的解釋力，而整體R^2值（average R^2）則為0.42，顯示結構模型具備相當的預測能力。

最後，除了透過R^2值來評估模型預測能力之外，研究者也需要透過盲解法（blindfolding）的方式，來檢核Stone-Geisser的Q^2值（Q^2 value），當Q^2值大於0時即代表結構模型中的路徑係數具有預測相關性（湯家偉，2016：145）。值得額外說明的是，盲解法與拔靴法類似，亦為一種重複使用樣本的統計方法，該方法會透過移除所有內生潛在變項第*d*個資料點，[27]再以剩下的資料進行估計；估計結果則被用以預測被移除的資料點，經過多次迭代後求取真實值（被移除的資料點）與預測值間的差異。圖2呈現本研究各內生潛在變項的Q^2值，除了形成性指標模型無法估算Q^2值之外（Henseler, Ringle, & Sinkovics, 2009: 305），其餘的內生潛在變項的Q^2值均大於0，代表結構模型在統計上具有良好的重建性（well reconstructed）。

從上述共線性、R^2值與Q^2值的討論中可以發現，本研究的結構模型約有中度的預測，且內生潛在變項均在統計上能為外生潛在變項所解釋，共線性問題亦不嚴重，代表本研究模型應具有一定程度的效度與穩健性。另外需要說明的是，在

[27] 參數 *d* 即為移除距離（omission distance），在操作上，移除距離不可使觀察值數量被整除。

DOI:10.6814/NCCU202000421

PLS-SEM中，雖然仍可計算適合度指標（Goodness of fit，簡稱GoF），但在使用上常為研究者所詬病，例如Henseler與Sarstedt（2013: 577）藉由模擬資料的測試，認為GoF並無法區分有效與無效的模型，這也是導致PLS-SEM較難運用於理論驗證，而多用於理論探索的主要原因。湯家偉（2016：150-151）亦直白表示，研究者應以路徑係數的比較作為主要評估標準，盡量不要使用GoF指標。基此，本研究將於下個段落討論PLS-SEM中最重要的元素：潛在變項間的路徑係數。

二、結構模型內的路徑係數

圖2與表8呈現本研究結構模型的主要統計結果。首先，本研究參考Jabbour等人（2015）的做法設定模型中的控制變項，也就是將控制變項以形成性指標的方式建立為潛在變項，並將其放入模型當中與其他潛在變項共同進行統計分析。本研究選用性別、年齡、教育程度、居住地區、過去隱私外洩經驗、收入與政黨認同等個人基本資料作為模型的控制變項，各變項的次數分配可參考表3。其中，本研究年齡、教育程度與收入視為順序尺度（ordinal scale）直接建立潛在變項進行分析，而性別、居住地區、過去隱私外洩經驗與政黨認同則視為類別尺度（nominal scale），先轉化為虛擬變數後再建立潛在變項進行分析，控制變項的重新編碼方式可參考附錄三。

需要說明的是，上述控制變項的處理方式並非是常規的結構方程式處理流程，大多數結構方程式分析均會強調模型的普遍性（generialization）原則，因此通常並不會特別納入控制變項於模型之中；若要探討不同群組間的比較，則需應用PLS-SEM多群組分析（PLS-MGA）的方法進行。然而，雖然不同群組間的異質性（heterogeneity）比較具有實務與理論的重要性（湯家偉，2016：202），但本研究主要關注的焦點並非在控制變項對於構念間關係的影響，且受限於樣本規模與研究量能並未執行群組分析方法。未來研究可以在樣本數擴大的基礎之下，

DOI:10.6814/NCCU202000421

以個人資料進行分組後，再行比較不同群組的資料分析結果。本段落將依照模型的主要區塊進行說明，並將其分為隱私利益區塊、隱私風險區塊與資料授權意願區塊等三個主要部分。

首先在隱私利益區塊部分，本研究發現財務報償、個性化服務與服務兼容性，都對於民眾的隱私利益認知有顯著的提高。從上述的結果可以得知，臺灣民眾在形塑對數位身分識別證的利益考量當中，對財務報償、個性化服務與服務兼容興等不同功能上會有相異的認知與影響，當未來的政府服務可以符合上述這三點時，民眾會更感受到使用數位身分識別證所帶來的預期效益。申言之，民眾關心的焦點在於如何透過數位身分識別的應用帶來更多數位服務，並減少辦理政府事務的金錢成本；除此之外，當未來數位身分識別證可以結合職場運用時，亦可提升民眾的預期效益。

其次，在隱私風險區塊部分，本研究的研究結果驗證了二元隱私計算模型中風險評價與應對評價這兩個構念，以及這兩個構念底下與之對應的四個潛在變項（Li, 2012）。然而，本研究原本預期應對評價對隱私風險認知應造成負向的影響，也就是當民眾認為自己擁有足以處理隱私問題的能力或技術時，則會對潛在的隱私風險給予較低的評價，但本研究在係數上卻呈現相反的結果。造成上述情況的原因可能有三：首先，由於本研究採用拔靴法的方式進行PLS-SEM參數的顯著性考驗，拔靴法本身存在著正負號不確定性（sign indeterminacy）的限制，亦即拔靴法無法直接確定潛在變項的路徑係數正負號，當信賴區間相當接近0時，其統計結果可能會與預期相反。[28]其次，不同族群的民眾可能對於應對評價跟隱私風險之間的關係產生調節效果，因而導致係數正負號與預期相左，本研究將於

[28] 但湯家偉（2016：109-110）建議研究者不要逕自改變正負號，以得到最保守的估計結果。

DOI:10.6814/NCCU202000421

本章第四節處深入說明此種可能。第三，應對評價高的民眾，可能源自於其對潛在風險認知較強，因而去學習相關的知識技能，也就是隱私風險與應對評價兩者可能會交互影響，從而產生民眾混淆的認知。

除了原有二元隱私計算模型的風險評價與應對評價構念之外，本研究在隱私風險區塊亦納入了風險管理機制、政府監控疑慮與政府信任等三項與政府相關的因素。研究結果發現，風險管理機制可以顯著地降低民眾對於隱私風險的認知，而政府監控疑慮則會顯著地提高民眾的隱私風險認知。從上述的結果可以發現，政府管制對民眾而言可以有正負面之分，當民眾感受到政府在法律層面等帶來的保護時，有助於減少民眾對隱私的擔憂（Miltgen & Smith, 2015）；於此同時，缺乏知情同意的網路監控活動則會提高民眾的隱私風險認知（Stoycheff et al., 2019），政府如何在兩種截然不同的管制之間取得平衡，係數位身分識別政策未來需要處理的課題。另外值得注意的是，與過去政府信任的相關研究（Bélanger & Carter, 2008）所得到的結果不同，本研究發現政府信任並無法直接降低民眾的隱私風險認知，但是可以透過降低民眾對政府監控的疑慮，「間接」地降低民眾的隱私風險認知。

最後，在資料授權意願區塊部分，本研究發現隱私利益認知與政府信任均對資料授權意願具有顯著的正向影響，而隱私風險、政府監控疑慮與預期投入則未有統計上的顯著效果；此外，本研究所納入的控制變項亦未有顯著的統計效果。將這個結果與上述隱私風險的討論相互對照後可以發現，我國民眾雖然有認知到個人資料外洩與政府監控行為所帶來的可能風險，但隱私風險認知並不會影響其透過數位身分識別證授權個人資料的意願，反而是個人資料所能帶來的利益認知能夠對民眾的授權意願產生更高的影響力。

DOI:10.6814/NCCU202000421

本研究認為行為經濟學（behavioral economics）、隱私悖論（privacy paradox）與遲滯性風險（delayed risk）這三種觀點，可以對上述結果提出合理解釋。首先在行為經濟學領域上，Acquisti與Grossklags（2007）針對民眾對隱私的認知提出了一項詰問：「隱私問題是風險問題還是不確定性問題？」。一般而言，風險被定義為一種「已知概率事件下的隨機結果」[29]，而不確定性則是「缺乏已知概率，且無法以數學機率表達的隨機效果」[30]。從不確定性的觀點來看的話，由於個人幾乎難以預先衡量隱私外洩下的客觀價值，因此無法形成可靠且有意義的價值評量，從而導致民眾忽略隱私可能產生的風險。基於不完整資訊（incomplete information）的約束下，個人的隱私決策可能會有部分的侷限性，例如產生高估利益與低估成本的情價效應（Valence effect），[31]以及對自己的隱私保護能力有過度自信（Over confidence）等的認知偏誤（Acquisti & Grossklags, 2007）。

除了行為經濟學的觀點之外，部分學者亦開始關注所謂的隱私悖論現象，也就是民眾的資料揭露意願可能會與實際的揭露行為相左（Norberg, Horne, & Horne, 2007; Kokolakis, 2017）。在現有且為數不少針對社群媒體資料揭露、數位商務使用行為的研究中可以發現一個令人稍嫌難堪的事實：儘管消費者會對隱私外洩的疑慮提出抱怨，並對隱私風險認知具有高度的自我評價，但在實際的揭露或授權行為上，卻往往有「口嫌體正直」的現象發生，仍然會幾近毫無限制地將個人資料提供予企業使用。基此，由於本研究僅有測量民眾的授權意願認知，未來相關研究或政策評估可以考慮額外測量民眾的真實行為，藉此更加完整對隱私認知模型的理解。

---

[29] 原文為：the possible random outcomes of a certain event have known associated probabilities。

[30] 原文為：randomness cannot be expressed in terms of mathematical probabilities, and the probabilities themselves are unknown。

[31] 亦有研究將其稱為「正面結果偏誤」（Positive outcome bias）。

DOI:10.6814/NCCU202000421

最後，遲滯性風險的觀點與行為經濟學的觀點雷同，都認為風險係為人類意識所主觀建構而成，並且更進一步提出，人類對風險的思想行為受到文化與社會的交互影響，即使在客觀上有預見可能的「危害」，但在主觀考量下卻會選擇忽略風險實質存在的事實（周桂田、張淳美，2006）。遲滯性風險論者認為臺灣社會係為一個「遲滯性高科技風險社會」，由於民眾缺乏正確的風險資訊、技術官僚線性的工具邏輯論述[32]與人權團體跟民眾間的知識鴻溝，使得臺灣社會在風險認知的建構上陷入惡性循環，從而嚴重低估風險帶來的危害（周桂田，2002；周桂田、張淳美，2006）。

綜整而言，本段落概括了結構模型中的主要研究結果與發現，並針對與預期不符的地方提出討論。從結構模型的結果中我們可以發現，本次受訪者對於隱私外洩的風險具有相當程度的認知，於此同時也能感受到個人資料所可能帶來的額外效益，但後者顯然對民眾最終資料授權意願產生較大的影響。除此之外，本研究也探討了風險管理機制、政府信任與政府監控疑慮等政府因素所可能產生的影響，並分析了政府管制的雙面性質。接下來，本節的最後將探討不同潛在變項的相對重要性，本研究認為透過比較不同構念的相對重要性，可作為研擬政策推動次序的參考依據之一。

三、潛在變項間的相對重要性

研究者可以藉由比較不同外生潛在變項的f^2效果值與q^2效應值，來判斷不同外生潛在變項對同一個內生潛在變項的相對重要性。f^2效果值與q^2效應值係為從前述模型品質評估中的決定係數（R^2）與預測相關性（Q^2）計算而來，研究者會

[32] 周桂田與張淳美（2005）以換發身分證按捺指紋案，探討兩種風險論述的對抗。其中，技術官僚針對新興科技所運用的風險論述，多係基於科學確定論的前提下的簡單線性邏輯，認為採用新科技即可達到預期政策目標，例如：身分證全面按捺指紋即可提高社會治安。

DOI:10.6814/NCCU202000421

藉由刪除模型內的特定外生潛在變項，透過兩次不同模型的結構模型估計，來計算刪除特定外生潛在變項前後的R^2值與Q^2值差異，藉以衡量特定外生潛在變項的f^2效果值與q^2效應值。一般而言，f^2效果值與q^2效應值的門檻均為0.02/0.15/0.35，分別代表特定潛在變項的小/中/大效果（湯家偉，2016：144-145）。更具體而言，若我們想要計算外生潛在變項「風險評價」對於內生潛在變項「隱私風險」的f^2效果值與q^2效應值，其數學公式可以表示為下列：

$$f^2 = \frac{R^2_{\text{含風險評價}} - R^2_{\text{無風險評價}}}{1 - R^2_{\text{含風險評價}}} \ldots\ldots \text{公式1}$$

$$q^2 = \frac{Q^2_{\text{含風險評價}} - Q^2_{\text{無風險評價}}}{1 - Q^2_{\text{含風險評價}}} \ldots\ldots \text{公式 2}$$

從上述的公式我們不難看出，f^2效果值與q^2效應值兩者的計算方式基本上是相同的，只是比較的模型品質指標有所差異。表8呈現本研究中各個外生潛在變項的f^2效果值與q^2效應值；需要說明的是，由於形成性指標模式無法Q^2值，故亦無法計算q^2效應值，而當外生潛在變項僅有一個時，亦毋須計算f^2效果值與q^2效應值。

首先在隱私利益區塊部分，我們從表8中可以發現個人化服務為最具有預測力的因素，此結果表明未來政府在推動數位身分識別證的認證機制時，設計貼近民眾需求的個性化服務是最重要的環節。其次，在隱私風險區塊部分，風險評價為最具預測力的外生潛在變項，而其餘變項的重要性則相對較小，代表民眾的隱私風險認知主要的主成分子仍舊是對於風險的評價。最後在資料授權意願區塊部分，政府信任與隱私利益分別為前二重要的外生潛在變項，其餘的變項則未有明顯的預測能力。本研究於此節完整探討了結構模型內的模型品質、路徑係數與變

DOI:10.6814/NCCU202000421

項相對重要性等三個議題，下一節將綜整本章的研究結果與本研究的研究假設，並針對研究結果與假設之間相同與相異處提出討論跟補充。

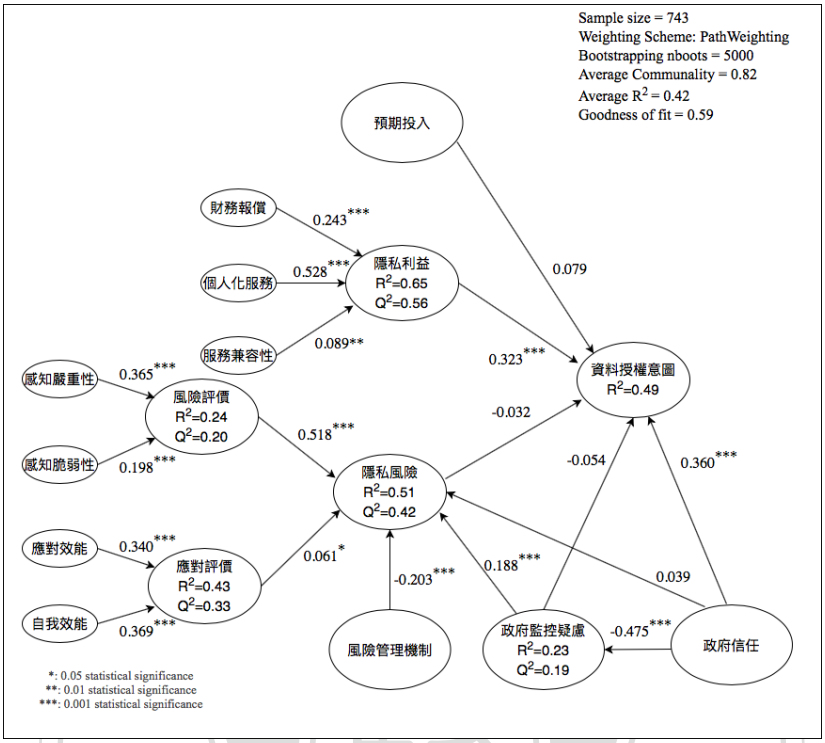

圖 2 結構模型路徑分析圖

資料來源：本研究自行繪製。

表 8 結構模型結果摘要表

外生變數	內生變數	路徑係數	t 值	顯著水準	95%信賴區間 上界	95%信賴區間 下界	f^2 效果值	q^2 效果值	VIF
隱私風險	資料授權意願	-0.032	-0.89	NS	-0.101	0.040	0.00	-	1.50
隱私利益		0.323	5.47	***	0.209	0.438	0.08	-	2.67
政府信任		0.360	7.33	***	0.266	0.459	0.12	-	1.99
政府監控疑慮		-0.054	-1.52	NS	-0.122	0.018	0.00	-	1.61
預期投入		0.079	1.43	NS	-0.033	0.185	0.00	-	2.25
性別（參照組：女性）		-0.024	-0.91	NS	-0.077	0.028	0.00	-	1.06
年齡		0.036	1.25	NS	-0.022	0.093	0.00	-	1.22
教育程度		0.012	0.44	NS	-0.041	0.067	0.00	-	1.08
隱私外洩經驗（參照組：無）		-0.009	-0.33	NS	-0.062	0.046	0.00	-	1.03

DOI:10.6814/NCCU202000421

外生變數	內生變數	路徑係數	t 值	顯著水準	95%信賴區間 上界	95%信賴區間 下界	f^2 效果值	q^2 效果值	VIF
泛綠認同（參照組：中立）		0.010	0.35	NS	-0.046	0.070	0.00	-	1.17
泛藍認同（參照組：中立）		-0.003	-0.09	NS	-0.063	0.057	0.00	-	1.25
收入		-0.001	-0.03	NS	-0.051	0.052	0.00	-	1.07
中部地區（參照組：北部）		-0.003	-0.13	NS	-0.057	0.049	0.00	-	1.09
南部地區（參照組：北部）		0.002	0.05	NS	-0.054	0.057	0.00	-	1.10
東部及離島地區（參照組：北部）		0.016	0.65	NS	-0.034	0.064	0.00	-	1.04
風險評價	隱私風險	0.518	14.29	***	0.445	0.588	0.35	0.25	1.54
應對評價	隱私風險	0.061	2.02	*	0.001	0.120	0.01	0.00	1.16
政府信任	隱私風險	0.039	0.61	NS	-0.084	0.167	0.00	0.00	3.45
風險管理機制	隱私風險	-0.203	-3.33	***	-0.324	-0.084	0.03	0.02	3.06
政府監控疑慮	隱私風險	0.188	5.11	***	0.118	0.262	0.04	0.03	1.67
財務報償	隱私利益	0.243	4.60	***	0.140	0.346	0.04	0.03	3.72
個性化服務	隱私利益	0.528	10.39	***	0.427	0.627	0.22	0.15	3.59
服務兼容性	隱私利益	0.089	2.53	**	0.020	0.157	0.01	0.00	1.77
感知嚴重性	風險評價	0.365	9.00	***	0.284	0.443	0.14	0.11	1.24
感知脆弱性	風險評價	0.198	4.35	***	0.111	0.288	0.04	0.03	1.24
應對效能	應對評價	0.340	7.05	***	0.246	0.436	0.10	0.07	1.91
自我效能	應對評價	0.369	7.46	***	0.272	0.465	0.12	0.08	1.91
政府信任	政府監控疑慮	-0.475	-15.05	***	-0.534	-0.412	-	-	-

樣本數 = 743, 迭代次數 = 7, 拔靴法樣本數 = 5,000

Average Communality = 0.82, Average R-squared = 0.42, Goodness of fit = 0.59

資料來源：本研究自行整理。

說明：***：$p<0.001$, **：$p<0.01$, *：$p<0.05$, NS：不顯著。

註：採路徑權重計算法（path weighting scheme），信賴區間係藉由拔靴法所估計而得。

DOI:10.6814/NCCU202000421

第四節 小結：模型之外的故事

本節將探討前三節的統計結果跟研究假設相異之處，並與原有研究架構進行補充與討論。表9呈現統計結果對研究假設的檢證結果，在本研究的11個假設當中，共有6項假設獲得統計上的支持。然而必須說明的是，雖然本研究看似有超過半數的研究假設獲得支持，但用以完整驗證隱私計算模型與二元隱私計算模型的假設（H2、H4）均無法獲得統計上的支持，因此本研究將在本節說明此背後的理論意涵。除此之外，本研究亦發現政府信任、風險管理機制與政府監控疑慮等三項與政府有關的變項對於隱私風險跟資料授權意願的直接與間接效果，在此節亦將探討其背後存有高階潛在構念之可能。

表 9 研究假設檢證表

編號	研究假設	檢證結果
H1	隱私利益認知越高、則資料授權意願越高	成立
H2	隱私風險認知越高、則資料授權意願越高	不成立
H3	自我風險評價越高、則隱私風險認知越高	成立
H4	自我應對評價越高、則隱私風險認知越低	不成立
H5	政府信任感越高、則資料授權授權意願越高	成立
H6	政府信任感越高、則隱私風險認知越低	不成立
H7	政府監控疑慮越高、則資料授權授權意願越低	不成立
H8	政府監控疑慮越高、則隱私風險認知越高	成立
H9	預期投入成本越低、則資料授權授權意願越高	不成立
H10	風險管理機制認知越高、則隱私風險認知越低	成立
H11	政府信任感越高、則政府監控疑慮越低	成立

資料來源：本研究自行整理。

一、缺塊的拼圖：不完整的隱私認知模型

本研究現階段的研究發現較為可惜之處，即僅能驗證「缺角」的二元隱私計算模型。申言之，在隱私計算部分，本研究發現民眾雖然會因為預期效益而提高個人資料授權意願，卻對於隱私所帶來的風險有過多的忽視；在風險計算部分，

DOI:10.6814/NCCU202000421

本研究證實了自我風險評價係會提高整體的隱私風險認知，但卻也發現個人處理風險的能力，也會提高整體的隱私認知，與Rogers（1975）提出保護動機理論有相違背之處。

基此，本研究認為上述預期與統計結果不符的情形，可能導因於潛在的調節效果。因此本研究進一步以自我應對評價、隱私風險認知作為自變項，以隱私風險認知與資料授權意願做為依變項，再以個人資料外洩經驗作為調節變項，進行後續的調節效果分析。圖3與圖4則分別呈現風險計算與隱私計算的調節效果比較，首先就風險計算部分（圖3），可以發現有個人資料外洩經驗的受訪者，其自我應對評價與隱私風險認知呈現正相關，也就是**即使自己處理隱私風險的能力較高、仍舊會覺得授權個人資料會帶來高度的隱私風險**。

此種結果反映出隱私經驗（privacy experience）在對隱私認知的影響，過去研究曾發現，當消費者意識到公司或組織有未經他們同意而蒐集個人的紀錄時，即可能產生對隱私外洩的擔憂（Cespedes & Smith, 1993; Smith et al., 2011）。也就是說，負面經驗可能導致二元隱私計算模型中的保護動機無法作用在過去曾經有隱私外洩經驗的民眾身上，過去曾經有隱私外洩經驗的民眾心中可能存在著近似於「一朝被蛇咬、十年怕草繩」的隱私認知，不論自身的隱私保護能力如何升級，仍然會認為是一種徒勞無功。

其次，在隱私計算部分（圖4），可以發現不論隱私外洩經驗的有無，隱私風險與資料授權意願均呈現穩定的負相關，顯示調節效果並不明顯。另外，隱私風險與資料授權意願在單變量間的顯著負相關結果，所告訴我們的資訊是，**隱私風險在整體模型中的路徑係數的不顯著，可能源自於同一內生潛在變項中的其他外生潛在變項具有更高的變異解釋量**。此結果可回應Dinev與Hart（2006）最初設

DOI:10.6814/NCCU202000421

立隱私計算模型的思維邏輯，意即隱私風險並非被「消除」（eliminate），而僅僅是被「超越」（override）；若進一步延伸此觀點，本研究認為隱私風險可能不是僅僅是被「超越」如此簡單，而是會被隱私利益所「壓抑」（suppress）。

行為經濟學與遲滯性風險的觀點也支持上述說法（周桂田、張淳美，2006；Acquisti & Grossklags, 2007），在預期風險具有高度不確定的隱私議題上，行為經濟學認為個人會高估利益，而遲滯性風險則認為個人會低估風險。本研究認為這兩種觀點共同導致了隱私計算模型的缺塊，尤其當隱私計算模型應用於新興且民眾尚未使用過的議題之上，此種缺角的現象則可能更加明顯。因此未來研究者除了考量到調節變項（moderator variable）的設計之外，壓抑變項（suppressor variable）亦是可以深究之處。[33]

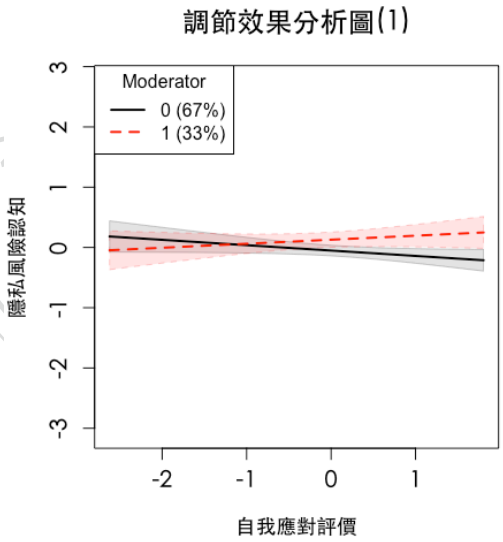

圖 3 風險計算中的調節效果

資料來源：本研究自行繪製。

說明：0＝ 無隱私外洩經驗; 1＝ 有隱私外洩經驗。

[33] 需要說明的是，時空環境的影響或許也可能壓抑民眾的隱私風險認知。本研究的調查時間係從 2020 年 2 月 18 日開始，此時期的臺灣社會受到源於中國武漢地區的新冠肺炎（SARS-CoV-2）疫情影響，部分公共服務（例如口罩實名制）多需要民眾個人資料才可使用，且在防疫的公衛需求下，隱私需求可能並非是政府或民眾的第一要務。然而，本研究當前的研究設計尚無法明確回答上述自然情境的效果為何，未來研究者可透過「反事實因果模型」（counterfactual model of causality，簡稱 CMC）等因果推論設計（黃紀，2008），更深入探討不同情境下的因果機制。

DOI:10.6814/NCCU202000421

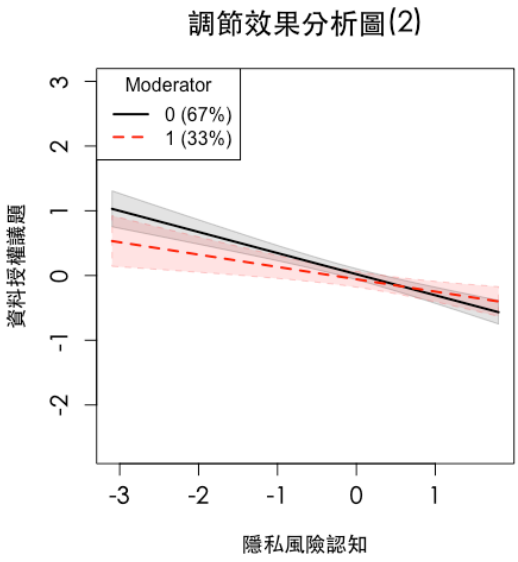

圖 4 隱私計算中的調節效果

資料來源：本研究自行繪製。

說明：0＝ 無隱私外洩經驗; 1＝ 有隱私外洩經驗。

必須要說明的是，由於本研究係將潛在變項的因素分數作為迴歸分析的依變項與自變項，因此本段落的探討僅為單變量之間的調節關係，並非完整的PLS-SEM多群組分析。在PLS-SEM中進行異質性的辨識與模型設定是另一種複雜的統計方法，同時亦牽涉到事前受訪者群體的特徵分佈與研究設計（湯家偉，2016：225-226），本研究在現有研究尺度的限制之下，尚無法處理此項議題，故僅先以單變量分析進行討論。

二、那裡還有東西？高階構念存在之可能

高階模式（higher-order models）的建立是PLS-SEM中的進階議題，當研究者在探究多個複雜構念，而複雜構念之間亦可再進一步地做不同層次的抽象化定義時，研究者可以進一步將潛在變項分為低階成分（lower-order components，簡稱LOC）與高階成分（higher-order components，簡稱HOC），來提高模型的簡潔度並緩和共線性與低區別效度等問題（湯家偉，2016：187-188）。

DOI:10.6814/NCCU202000421

本研究架構中的政府信任、政府監控疑慮與風險管理機制等三個變項，都相當大程度反映了民眾對政府如何蒐集與處理個人資料的態度，並指涉了政府用來管理民眾個人資料上攸關蒐集、儲存與使用等不同機制。例如政府監控疑慮代表民眾對政府**蒐集**個人資料的能力上的擔憂；政府信任係為最廣義的機構信任，反映民眾對個人資料**儲存**機構的觀點；風險管理機制代表民眾對政府在**使用**個人資料時的手段認同程度。而從表8的共線性評估亦可看到，上述這三個變項在共線性問題上雖不嚴重，但也相對其餘變項來得高，代表三者之上可能有存在高階構念之可能。

現有隱私計算模型等相關研究在公共行政領域中仍屬相當薄弱的一環，而大多數的資訊管理領域亦不會特別在意政府在隱私認知模型中的角色，至多將其劃分為法律規範（legal framework）或管制（regulation）的層次（Smith et al., 2011）。然而，在政府可以主動蒐集與儲存個人資料的現代社會，政府在隱私計算模型應不僅扮演管制者的角色，而是會同時扮演不同角色與機制，民眾對不同角色與機制的認知亦可能有所不同；相較於資訊管理領域，上述不同角色的定位與討論仍有待政府資訊管理或數位治理的研究者更深入挖掘。

由於在問卷設計之初，並未考量到高階構念存在之可能，且抽象化定義與指標的建立仍有待政府資訊管理領域的研究者，更深入地歸納與整合其內涵後才得以建立一致的測量量表，因此本研究在此段落將嘗試應用重複指標法（repeated indicator approach）來處理高階潛在變項這個議題。本研究首先將政府監控疑慮所測量的三個指標進行反向編碼，使政府信任、政府監控疑慮與風險管理機制包含的九個測量指標間呈現良好的信度，藉此將其作為一反映性指標「政府因素」來處理；再將政府信任、政府監控疑慮與風險管理機制等三個潛在變項作為此高

DOI:10.6814/NCCU202000421

階構念的外生潛在變項，建立**反映性－形成性模式**的階層成分模式（湯家偉，2016：189）。

圖5呈現將上述三項政府相關因素重新建立為一高階構念後的統計結果，而表10則是完整的路徑係數結果摘要表。可以發現政府因素有助於減少隱私上的風險認知，並提高資料授權意願，而三個低階構念與高階構念間的路徑係數亦為顯著。另外，加入高階構念後，整體模型較為簡潔，且隱私風險與資料授權意願的R^2值與原有模型相比，並未有下降的情形，顯示就資料分析結果來看，與政府相關的高階構念應是可能存在且需要納入於隱私計算模型當中。

需要額外說明的是，由於採用重複指標法的緣故，所以該高階構念的R^2值會趨近於1，因為高階構念並未有自己的測量指標，因此其變異會幾乎為低階構念所解釋（湯家偉，2016：190）；由於高階構念的R^2值趨近1的緣故，在計算底下三個低階構念時的f^2值時，其分母會趨近於0（可參考公式1），使得結果趨近於無窮大，因此運用重複指標法時計算f^2值並無意義。

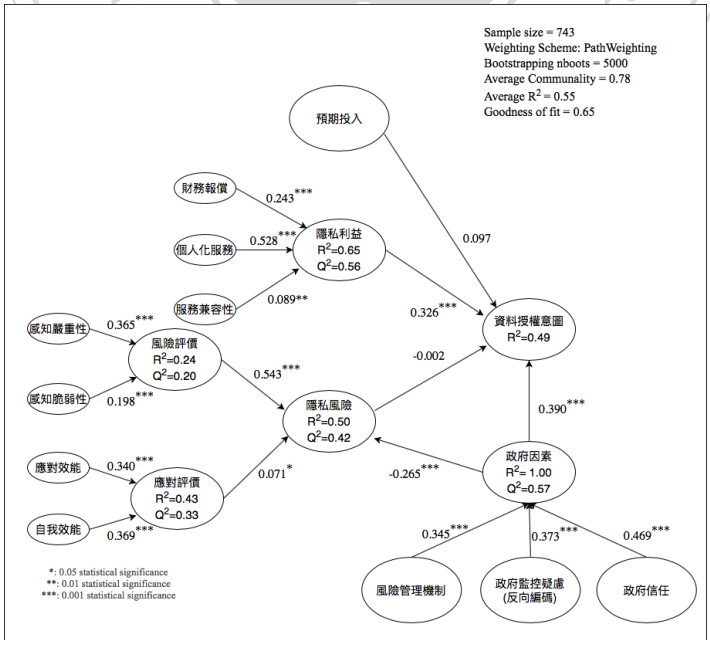

圖 5 修正後結構模型路徑圖

資料來源：本研究自行繪製。

DOI:10.6814/NCCU202000421

表 10 修正後結構模型結果摘要表

外生變數	內生變數	路徑係數	t 值	顯著水準	95%信賴區間 上界	95%信賴區間 下界	f^2 效果值	q^2 效果值	VIF
隱私風險	資料授權意願	-0.002	-0.06	NS	-0.072	0.069	0.00	-	1.43
隱私利益		0.326	5.41	***	0.209	0.445	0.08	-	2.66
政府因素		0.390	7.51	***	0.288	0.491	0.14	-	2.00
預期投入		0.097	1.75	NS	-0.012	0.203	0.01	-	2.23
性別（參照組：女性）		-0.017	-0.64	NS	-0.070	0.034	0.00	-	1.06
年齡		0.035	1.21	NS	-0.021	0.092	0.00	-	1.21
教育程度		0.012	0.43	NS	-0.045	0.065	0.00	-	1.08
隱私外洩經驗（參照組：無）		-0.010	-0.38	NS	-0.065	0.044	0.00	-	1.03
泛綠認同（參照組：中立）		0.013	0.44	NS	-0.044	0.070	0.00	-	1.17
泛藍認同（參照組：中立）		0.001	0.05	NS	-0.059	0.062	0.00	-	1.25
收入		-0.001	-0.04	NS	-0.052	0.051	0.00	-	1.07
中部地區（參照組：北部）		0.002	0.09	NS	-0.051	0.054	0.00	-	1.09
南部地區（參照組：北部）		-0.001	-0.03	NS	-0.057	0.052	0.00	-	1.10
東部及離島地區（參照組：北部）		0.011	0.43	NS	-0.039	0.061	0.00	-	1.04
風險評價	隱私風險	0.543	15.52	***	0.472	0.611	0.43	0.30	1.37
應對評價		0.071	2.27	*	0.011	0.133	0.01	0.00	1.14
政府因素		-0.265	-6.76	***	-0.340	-0.187	0.09	0.07	1.53
財務報償	隱私利益	0.243	4.68	***	0.139	0.347	0.04	0.03	3.72
個性化服務		0.528	10.55	***	0.427	0.626	0.22	0.15	3.59
服務兼容性		0.089	2.53	**	0.021	0.160	0.01	0.00	1.77
感知嚴重性	風險評價	0.365	8.94	***	0.284	0.446	0.14	0.11	1.24
感知脆弱性		0.198	4.32	***	0.110	0.289	0.04	0.03	1.24
應對效能	應對評價	0.340	6.92	***	0.242	0.435	0.10	0.07	1.91

DOI:10.6814/NCCU202000421

外生變數	內生變數	路徑係數	t 值	顯著水準	95%信賴區間		f^2 效果值	q^2 效果值	VIF
					上界	下界			
自我效能		0.369	7.21	***	0.268	0.471	0.12	0.08	1.91
政府信任	政府因素	0.469	45.36	***	0.450	0.491	-	0.09	3.22
政府監控疑慮（反向編碼）		0.373	29.19	***	0.348	0.398	-	0.12	1.29
風險管理機制		0.345	29.40	***	0.323	0.368	-	0.06	2.87
樣本數 = 743, 迭代次數 = 11, 拔靴法樣本數 = 5,000									
Average Communality = 0.78, Average R-squared = 0.55, Goodness of fit = 0.65									

資料來源：本研究自行整理。
說明：***：$p<0.001$, **：$p<0.01$, *：$p<0.05$, NS：不顯著。
註：採路徑權重計算法（path weighting scheme），信賴區間係藉由拔靴法所估計而得。

本節探討了原有研究架構所無法驗證的研究假設，並提出未來研究者可以進一步分析與討論的方向，在此節的最後，本文必須要再次重申一次本研究認同的計量研究精神。本節的討論係大多依循資料的統計結果而來，修正後的研究結構在模型品質亦有所改善；然而，本研究並不認為研究者可能僅依循統計結果而全盤推翻原有的研究架構，並依此創建符合資料分析結果的研究假設，而是要對理論的可能修正保持審慎評估的態度。

政治科學研究當中，連結與整合形式分析（formal anaysis）與實證分析（empirical analysis）的EITM途徑（empirical implications of theroetical models）被認為是用來修正現有思維脈絡的重要途徑。研究者需要先確保上層實質理論的邏輯一貫性（logically coherent），再據以下層計量資料分析結果為基礎，溯源而上去修正形式理論內涵（黃紀，2013；Granato & Scioli, 2004）。在依循資料溯源而上的過程當中，研究者須再次透過嚴謹的邏輯推論來修改研究假設，並重視那些無法被檢證的研究假設，才不至於淪為折磨資料（data torturing）的計量研究

DOI:10.6814/NCCU202000421

（Mills, 1993）。[34]綜合上述，本章評估了本研究的研究模型，並分析了本研究的主要研究發現、理論意涵、實務建議與可能的修改方向。本研究的最後部分將整合全文，針對研究發現、政策建議、研究限制與未來研究建議等部分做成結論。

[34] Data toturing 的意涵以一言敝之，即為「假如你花足夠多的時間折磨你的資料，它們會告訴你所有你想聽的一切」（if you torture your data long enough, they will tell you whatever you want to hear）（Mills, 1993: 1196）。

DOI:10.6814/NCCU202000421

第五章　結論

本章將整合本研究，回答最初提出的兩個研究問題：影響民眾透過數位身分識別證授權個人資料的因素有哪些？不同因素對個人資料授權意願所造成的影響為何？並依次說明研究發現、政策建議、研究限制與未來研究建議。

第一節 研究發現與理論意涵

本研究透過二元隱私計算模型，發現了數個影響民眾透過數位身分識別證授權個人資料的因素。統計模型在測量模型的表現良好，潛在變項間的衡量具有信效度；再從結構模型的決定性係數（R^2值）來看，整體模型約有中度的解釋能力，代表研究發現應有相當的可信度。

首先，財務報償、個人化服務與服務兼容性都有助於提高民眾的隱私利益認知，而隱私利益認知則進一步會提高授權個人資料的意願。此外，本研究也驗證了Li（2012）提出的二元隱私計算模型中的初階因素，包含感知嚴重性、感知脆弱性、應對效能與自我效能等四個構念；並發現風險評價則會提高民眾的隱私風險認知，但應對評價的路徑係數與預期相反，背後的調節效果值得進一步探究。

其中值得注意的是，與Dinev與Hart（2006）最初提出的隱私計算模型不同，民眾的隱私風險認知並沒有降低其授權個人資料的意願。本研究援引了行為經濟學、隱私悖論與遲滯性風險的觀點，探討民眾在對待隱私風險背後的思維邏輯。此外，本研究也探討了風險管理機制、政府監控疑慮與政府信任等三個常為資訊管理領域所忽視的因素，風險管理機制可以減少民眾的隱私風險認知，政府監控疑慮則有相反的效果，而政府信任除了直接提高個人資料授權意願外，也可能會間接降低民眾的隱私風險認知。

DOI:10.6814/NCCU202000421

在不同因素間的影響力比較當中，個人資料授權意願則主要受到利益認知與政府信任的影響為多，其中民眾的隱私利益認知可能超越甚至壓抑民眾的隱私風險認知。另外，個性化服務對於提高隱私利益認知具有最高的影響力，財務報償則次之。最後，組成民眾隱私利益認知的主要成分為對個人資料外洩的擔憂程度（也就是「風險評價」），代表民眾評價個人資料的風險高低，係源自於資料外洩的可能性多寡，而其他因素如政府監控的疑慮與自身處理隱私問題的能力等的影響力則相對較小。

本研究最後探討了模型修正的可能，包含將個人隱私外洩經驗作為調節變數，探討了負面經驗對於個人自我能力認知的影響。另外，本研究也發現政府信任、政府監控疑慮與風險管理機制，或許可以組成另一與政府相關的高階構念；此政府相關構念涵蓋了民眾對於資料蒐集、資料儲存與資料使用的信任程度，可以降低民眾的隱私風險認知，並提高授權個人資料的意願。然而，由於現有研究並未完整地建構政府在隱私研究中的角色，且本研究在取樣與目標母體的加權上上亦存有限制，因此現階段的推論應不宜過度。

第二節 政策建議

從研究發現可以得知，隱私上的風險對民眾未來是否使用數位身分證進行個人資料授權的影響不大。但本研究認為，上述研究結果並不意味著民眾不在乎數位身分識別證可能產生的隱私風險，而政府可循此儘速推動數位身分證；相反地，本研究認為民眾忽視風險的現象反倒是一種警訊，印證了過去研究認為臺灣是一個「遲滯型高科技風險社會」的推論（周桂田，2002）。在單一的技術官僚效率觀論述、公民風險認知的缺乏與社會團體難以有效動員的惡性循環之下，使得我

DOI:10.6814/NCCU202000421

國民眾在隱私計算模型中呈現「缺角」的隱私認知，民眾可能高估了預期的效益，並低估了可能的危害。

更進一步而言，由於風險認知的偏誤與風險資訊的缺乏，使得民眾可能此類科技政策的偏好有「輕率表意」的現象，此時民意（public opinion）甚難作為決策之依據（余致力，2002：65-66）。也就是說，在未來數位身分識別證的推動，乃至於更進一步我國MyData資料庫的建置，僅依靠民調方法所得到的政策支持程度必然有所偏誤；以有偏誤的結果作為決策參考，則可能導致後續政策執行時的一連串問題，因此決策者應納入多元的決策機制於此類重大公共政策之上。基此，本研究提出三點政策建議，包含建立風險溝通機制、完善服務流程設計與制定法令框架等三個部分。

一、建立知情、民主的科技風險溝通機制

沒有人會認為隱私或網路安全（cybersecurity）不值得重視，但由於網路上的個人資料具有無形性，且保障隱私的成效性難以評估，因此個人隱私就像是保健因子（hygiene factors）一樣，甚難成為民眾關注的核心（de Bruijn & Janssen, 2017）。本研究建議未來數位身分識別證或MyData資料庫的權責單位，可以參酌英國Midata的精神，盡力提高民眾對授權個人資料後，所可能產生的風險與責任的認知，並將資料蒐集流程、所蒐集的資料內容與發生問題時的課責對象，清楚且主動地告知授權民眾（Shadbolt, 2013）。

除了讓民眾充分知情（well-informed）個人資料授權背後的風險資訊之外，我國過去相關的環境風險、科技風險等研究中亦指出，現有技術官僚的菁英主義決策思維已然無法回應複雜的新興社會問題，因此發展具有實質溝通效果的審議民主途徑係可能的制度改革方式（杜文苓，2011；杜文苓、施麗雯、黃廷宜，2007；

DOI:10.6814/NCCU202000421

周桂田、張淳美，2006）。本研究建議未來推動數位身分識別證或其他數位政策的技術官僚，應跳脫以效率觀為主的科技確定論思維，透過民主程序來提升此類創新政策的民主正當性（democratic legitimacy），並提高民眾對創新政策的接受度與使用率（曾冠球、陳敦源、胡龍騰，2009）。

二、設計完善的服務輸送流程

我們從研究發現中可以得知，個性化服務係影響民眾利益感知的最重要因素，因此位居實務第一線的政府部門所面臨的挑戰可能是如何介接不同主管單位的業務資料，以提供符合民眾需求的個人化服務。曾憲立等人（2020）盤點了現階段國內MyData的測試方案是為相當重要的研究起點，未來權責機構可以進一步擴大盤點的規模與相關研究的執行。舉例而言，除了水平的跨部門數位服務整合之外，同一部門內決策單位、業務單位與資訊單位的一致化流程（alignment process）是創造標準化資料的關鍵，部門內的資訊整合也包含策略應用、專業知識、組織結構與文化等多層次的意義（Chan & Reich, 2007）。

為求整合並提出符合使用者需求的個性化服務，本研究建議未來數位身分識別證與MyData資料庫的權責單位，可採用敏捷開發過程（agile development）來研擬適合的服務流程。更具體而言，相關機關在設計服務流程同時，應摒棄過往強調由上而下的規劃、執行與評估的「瀑布」開發流程（waterfall software development），而是透過循環的設計（design）、建置（bulid）與測試（test）流程，藉由多次迭代（iteration）或短跑衝刺（sprint）來修正出適合使用者的服務流程（榮予恆，2019；Mergel, 2016）。

DOI:10.6814/NCCU202000421

三、制定限制行政權力的法令框架

政府應當扮演何種角色是政治哲學或公共行政的互久爭論，政府這頭「利維坦」（Leviathan）行使權力的界線與應受的限制，在不同立場的論者之間亦廣受爭論（周家瑜，2016）。在數位身分識別證這類的新興科技政策上，雖然政府極力追求將民眾個人資料廣泛用於創造更高的公共價值，但後續可能衍生的財務詐欺、隱私監控與身分歧視等不確定性問題不僅存在於科技使用層面，而是可能外溢成為整體社會的安全問題（周桂田、張淳美，2006）。

從研究發現可以看出，透過法律框架對可能的風險發生進行控管，可以有效地減輕民眾的隱私擔憂；而缺乏事前知情授權的政府監控，則會提升民眾對風險的認知。也就是說，在快速資訊化的現代社會，政府從霍布斯形容的巨獸利維坦化身為歐威爾筆下無時無刻盯著你的老大哥；但於此同時，政府也可以搖身一變，成為提供一站式服務、追求顧客導向的e管家。因此本研究認為，這種從科技不確定性風險轉變而成的社會不確定性風險，應當透過法律框架規範的方式，來減輕其可能的外部成本。換言之，縱然當代政府作為具實質強制力的利維坦本質尚難改變，但立法機關應藉由法律規範來「馴服」（taming）行政機關相關的舉措，以確保民眾個人資料的蒐集、使用與管理是用在數位服務的改善之上。

除了以法律限制行政機關的舉措之外，權責單位也應適時制定用以保障民眾權利的法令規範，例如被遺忘權（right to be forgotten）等機制的設立。被遺忘權為歐盟法院所認定的一種個人權利，認為資料主體（個人）可以向服務供應商或資料儲存機構要求移除負面或過時的個人資料。[35]本研究認為，未來相關政策應考量納入相似概念的刪除權或退出權，用以保障個人最底線的隱私自主權。

[35] 林妍溱（2014 年 05 月 14 日）。歐盟判決：人有「被遺忘的權利」，Google 必須依個人要求刪除搜尋結果。iThome，2020 年 04 月 10 日，取自：https://www.ithome.com.tw/news/87686。

DOI:10.6814/NCCU202000421

第三節 研究限制

本研究的研究限制主要有三個部分，分別為受訪樣本可能的偏差、隱私情境設計上的限制與行為指標衡量的困難。首先在受訪樣本的偏誤上，本研究所選擇的網路調查樣本最多僅能稱作為「準機率樣本」，且由於網路使用者的特性，受訪者具有高教育程度、低年齡層與居住於都會區等特徵。但數位身分識別證全面換領的對象不僅止於網路使用者，而是全國14歲以上國民均有換領義務；因此如何探詢到網路調查樣本之外的群體，是未來進一步推論此研究架構適用的基石。

第二個研究限制為隱私情境設計的困難，由於數位身分識別證該政策於本研究寫作當下尚未開始執行，因此現階段的調查問卷僅能探討民眾的「預期」想法。國內目前相關研究也尚在發展的初期，政府部門內部尚在規劃與研議未來MyData的應用機制（曾憲立等人，2020）。因此，民眾對於真實使用的情境可能僅有模糊的認知，也較難設計出真實的使用情境來「刺激」受訪者。

最後，隱私悖論中所闡明的「意圖-行為」間的矛盾現象亦值得我們關切。事實上，個體的調查資料往往難以完全消除僅衡量意圖的偏誤；以投票行為研究為例，選後民調的受訪者可能產生「西瓜效應」或「選擇性失憶」的情形，也就是受訪者不願回答自己真實的投票行為，從而導致特定候選人得票率的錯估（張順全、莊文忠，2017）。由於數位身分識別證政策尚未落實，本研究尚難以發展出相應的行為衡量指標；再加上，即使發展出相對應的指標，透過調查研究亦只能衡量到行為意圖。因此，蒐集實際行為的實地研究是未來研究者可以考量之處。

DOI:10.6814/NCCU202000421

第四節 研究建議

針對上述三個不同的研究限制，本研究提供兩項建議供未來研究參酌。在網路調查的樣本偏誤部分，未來研究可以考慮整合電訪調查所得到的結果，透過Webographic變數（例如就寢時間）來定義電訪調查與網路調查的差異後，藉由入選機率調整法（Propensity Score Adjustments，簡稱PSA）的方式來修正網路調查可能的偏誤（杜素豪，2015；俞振華、涂志揚，2017）。

透過混合調查方法（mixed-mode）來接觸不同群體的受訪者將會是未來調查研究的發展趨勢（Dillman, Smyth, & Christian, 2014:12-15；曾憲立、洪永泰、朱斌妤、黃東益、謝翠娟，2018），因此未來政府機構或研究單位在進行混合調查方法的同時，可考量納入PSA方法來校正網路調查可能的偏誤，以達到節省調查經費、提高調查效度等一石多鳥之效。

關於隱私情境設計與行為指標測量上的困難，本研究認為實驗設計（experimental design）的引入可能有助於未來研究者處理上述兩項限制。實驗法具備檢驗事實（searching for facts）、與理論對話（speaking to theorists）、影響決策者（whispering in the ears of princes）等三項主要功能（Roth, 1995），並且在近十年來開始受到政治科學研究的廣泛關注與重視，政治科學家大量應用隨機分派的實驗設計來探索實際的因果關係（Druckman, Green, Kuklinski, & Lupia, 2006）。相比於政治科學積極引入實驗法於研究場域當中，實驗法目前在公共行政領域的應用則相對較為稀缺。公共行政評論（Public Administration Review）的主編James L. Perry就直言實驗方法在過去的公共行政領域並未有太大的進展，並鼓勵公共行政學者嘗試混合實驗法與其他研究方法來進行相關的應用性研究（Perry, 2012: 480）。

DOI:10.6814/NCCU202000421

雖然有學者批判實驗設計難以應用於複雜的公共政策情境之上，以及忽略了社會中的價值多元主義；然而每一個公共政策的形成對社會來說都近似於一場自然實驗，政策評估理論發展的初期，即是以實驗設計為主軸的政策實驗評估時代（丘昌泰，2016：457-462）。許多數位商務的隱私研究已大規模的應用實驗法來檢證隱私宣言與商標信譽等因素對消費者的影響（Acquisti, & Grossklags, 2012），尤有甚者，不少研究會透過招募實驗參與者在社群媒體上進行實地的行為實驗（Wang & Chang, 2013; Wells & Thorson, 2017）。未來的研究者或政府機構可以考慮在嚴謹的實驗設計下，藉由招募知情志願者的方式，進行實地的行為研究，來更全面地瞭解民眾的隱私認知機制，藉以克服隱私情境與行為測量上的限制。

最後，本研究目前使用的二元隱私計算模型，在公共行政研究領域內的應用仍顯不足，研究者應持續思考，如何吸納此一來自於資管領域的研究模型，並將公共行政的重要概念涵融於其中。數位治理是公共行政學門當中，具有濃厚跨領域色彩的次領域，電子化政府、政府資訊管理或數位治理的相關研究者，可持續深掘隱私計算在不同案例、不同政府層級的應用，或是藉由紮根理論（grounded theory）等方式來建構具備公共行政脈絡的隱私認知量表。正如Janowski（2015）所指出的，未來數位治理的發展逐步要推往「脈絡化階段」（contextualization），研究者與政府實務工作者都需要在政策或研究上去回應、甚至針對新的數位科技進行適應和創新。

第五節 研究貢獻

公共行政的研究需要嘗試應用理論方法來處理行政實務上面臨的議題，而資訊隱私議題係政府在推動數位治理與資料治理時不可迴避的重要課題。本研究以國內重要的數位身分識別證政策為個案，從個人資料自主管理的角度切入，討論

DOI:10.6814/NCCU202000421

了影響民眾授權個人資料的隱私因素。本研究能提供資訊管理領域跟公共行政領域間在隱私認知模型上的相互對話，並促使數位治理研究在未來更加重視個人化資料背後的隱私問題。此外，本文的研究結果也可以提高服務提供者（公共組織、政府部門）對服務接受者（公民）的瞭解，藉以制定良善、貼切的公共政策，並回應公共行政對公共利益的永恆追求（Goodsell, 1990）。更進一步而言，本研究的研究貢獻可再分為實務與學術貢獻分述之。

在實務層面，數位身分識別作為我國未來推動智慧政府的關鍵政策，若未來政策順利推行後，隨著政府業務資料庫的串連，勢必會面臨民眾對個人資料提供的擔憂與抗拒，政府也需要發展出相應的處理機制應對。因此，本研究在實務上的貢獻即是藉由分析個人資訊揭露意向的影響因素，找出數個政府未來可以改進的面向以供政策規劃之用，同時也針對目前正在規劃的數位身分識別政策提出隱私政策參採。

在學術層面，過去國內數位治理領域甚少透過量化研究處理資訊隱私的議題，大多僅止於初步的描述性統計或規範層面的討論，並未應用完整的隱私計算模型於數位治理分析之上，本研究成果可適時補足此一學術缺口。與此同時，淵源自資訊管理領域的隱私計算模型，也甚少在模型當中探究政府角色的重要性，本研究亦溯源而上，與原有資訊管理領域的隱私計算模型進行對話、修正。

DOI:10.6814/NCCU202000421

參考文獻

內政部（2019）。**數位身分證之規劃、功能與經費**。2020 年 2 月 27 日，取自：https://lis.ly.gov.tw/lydb/uploadn/108/1080516/01.pdf。

丘昌泰（2008）。**公共政策：基礎篇**。臺北：巨流圖書。

何明諠（2016）。數位時代的隱私邊界：以健保資料庫與 ETC 交通資料庫為例。**台灣人權學刊，3**（4），139-153。

余孝先、趙祖佑（2015）。巨量資料應用，打造資料驅動決策的智慧政府。**國土及公共治理季刊，3**（4），27-37。

余致力（2002）。**民意與公共政策：理論探討與實證研究**。臺北：五南。

李仲彬（2011）。「信任」在電子治理中所扮演的角色：以文獻檢閱為基礎的初探性分析。**公共行政學報，39**，105-147。

李仲彬、洪永泰、朱斌妤、黃東益、黃婉玲、曾憲立（2017）。**數位國情總綱調查（4）：因應行動服務與共享經濟（資源）發展之策略**（編號：NDC-MIS-105-001）。臺北：國家發展委員會。

李伯璋、林寶鳳、張齡芝（2019）。健康存摺～你我的健康管家－整合民眾醫療資訊，一機在手健保跟著走。**消費者報導雜誌，457**，67-70。

李承傑、董旭英（2017）。偏最小平方法結構方程模型。**科學發展，539**，20-25。

李政忠（2004）。網路調查所面臨的問題與解決建議。**資訊社會研究，6**，1-24。

杜文苓（2011）。環境風險與科技決策：檢視中科四期環評爭議。**東吳政治學報，29**（2），57-110。

DOI:10.6814/NCCU202000421

杜文苓、施麗雯、黃廷宜（2007）。風險溝通與民主參與：以竹科宜蘭基地之設置為例。**科技醫療與社會，5**，71-110。

杜素豪（2015）。比較入選機率分組與其他加權方法對電話調查樣本的調整：上網率的推估，**臺灣社會學刊，56**，115-150。

周家瑜（2016）。馴服《利維坦》？霍布斯與絕對主義。**政治與社會哲學評論，59**，51-91。

周桂田（2002）。在地化風險之實踐與理論缺口－遲滯型高科技風險社會。**台灣社會研究季刊，45**，69-122。

周桂田（2015）。**臺灣風險社會十堂課：食安、科技與環境**。臺北：巨流圖書。

周桂田、張淳美（2006）。遲滯型高科技風險社會下之典範鬥爭：以換發身分證按捺指紋案為分析。**政治與社會哲學評論，17**，127-215.

俞振華（2016）。網路民意調查的理論與實務。載於陳陸輝（編），**民意調查新論**（4版）（95-116頁）。臺北：五南。

俞振華、涂志揚（2017）。探討以電訪資料及「入選機率調整法」修正網路調查偏誤的可行性。**政治科學論叢，73**，81-125。

洪新原、梁定澎、張嘉銘（2005）科技接受模式之彙總研究。**資訊管理學報，12**（4），211-234。

紀佳伶（2000）。**電子化/網路化政府資訊內容隱私權之研究**。國立政治大學公共行政學系碩士學位論文，未出版，臺北。

國家發展委員會（2018）。**服務型智慧政府推動計畫－第五階段電子化政府計畫**。2020年2月25日，取自：https://reurl.cc/1QnjMG。

國家發展委員會（2019）。**智慧政府推動策略計畫**。2020年2月25日，取自：https://reurl.cc/drdzQg。

DOI:10.6814/NCCU202000421

張順全、莊文忠（2017）。超越藍綠？政治版圖在 2014 年臺北市長選舉的新應用。**選舉研究，24**（1），97-132。

陳怡君（2008）。優質網路政府主動服務新思維－民衆 e 管家。**研考雙月刊，32**（1），57-65。

陳寬裕（2018）。**結構方程模型分析實務：SPSS 與 SmartPLS 的運用**。臺北：五南。

曾冠球、陳敦源、胡龍騰（2009）。推展公民導向的電子化政府：願景或幻想？。**公共行政學報，33**，1-43。

曾憲立、洪永泰、朱斌妤、黃東益、謝翠娟（2018）。多元民意調查方法的比較研究。**調查研究，41**，87-117。

曾憲立、蕭乃沂、宋同正（2020）。**智慧政府下 My Data 個案推動與模式建構：數位身分識別與服務流程優化**（編號：NDC-MIS-108-002）。臺北：國家發展委員會。

湯家偉（譯）（2016）。**結構方程模式：偏最小平方法 PLS-SEM**（原作者：Joseph F. Hair, Jr, G. Tomas M. Hult, Christian M. Ringle, Marko Sarstedt）。臺北：高等教育文化。

黃東益、胡龍騰、李仲彬、黃婉玲、曾憲立、朱斌妤（2018）。**數位國情總綱調查（5）：區域發展策略**（編號：NDC-MIS-106-001）。臺北：國家發展委員會。

黃紀（2008）。因果推論與觀察研究：「反事實模型」之思考。**社會科學論叢，2**（1），1-22。

黃紀（2013）。政治學計量方法的回顧與前瞻。載於吳玉山、林繼文、冷則剛（編），**政治學的回顧與前瞻**（39-64 頁）。臺北：中央研究院政治研究所。

DOI:10.6814/NCCU202000421

廖興中、朱斌妤、黃婉玲、洪永泰、黃東益（2019）。**數位國情總綱調查（6）：區域數位分級與數位國情世代進展研析**（編號：NDC-MIS-107-001）。臺北：國家發展委員會。

榮予恆（2019）。**邁向敏捷政府–敏捷專案管理在我國數位治理的應用與影響**。國立政治大學公共行政學系碩士學位論文，未出版，臺北。

管中祥（2001）。從「資訊控制」的觀點反思「電子化政府」的樂觀迷思。**資訊社會研究，1**，299-316。

劉尚志、林三元、宋皇志（2006）。走出繼受，邁向立論：法學實證研究之發展。**科技法學評論，3**（2），1-48。

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。

蕭乃沂、朱斌妤（2018）。資料驅動創新的跨域公共治理。**國土及公共治理季刊，6**（4），74-85。

蕭乃沂、陳恭、郭昱瑩（2017）。**第五階段電子化政府服務精進：國際趨勢與民眾需求探勘**（編號：NDC-MIS-105-003）。臺北：國家發展委員會。

蕭新煌、徐世榮、杜文苓（2019）。**面對台灣風險社會：分析與策略**。臺北：巨流圖書。

羅清俊（2010）。**社會科學研究方法：打開天窗說量化**。臺北：威仕曼文化。

顧振豪（2016）。完備資料開放與自主管理機制，建構數位國家發展基礎。**國土及公共治理季刊，4**（4），67-79。

Abu-Shanab, E., & Al-Azzam, A. (2012). Trust Dimensions and the adoption of E-government in Jordan. ***International Journal of Information Communication Technologies and Human Development (IJICTHD), 4***(1), 39-51.

DOI:10.6814/NCCU202000421

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy. ***Digital Privacy: Theory, Technologies and Practices, 18***, 363-377.

Acquisti, A., & Grossklags, J. (2012). An online survey experiment on ambiguity and privacy. ***Communications & Strategies, 88***, 19-39.

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. ***Journal of Experimental Social Psychology, 22***(5), 453-474.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. ***First Monday, 13***(3). Retrieved from source https://firstmonday.org/ojs/index.php/fm/article/view/2142/1949http%3A.

Allmer, T. (2011). Critical surveillance studies in the information society. tripleC: Communication, Capitalism & Critique. ***Open Access Journal for a Global Sustainable Information Society, 9***(2), 566-592.

Bansal, G., Zahedi, F. M. & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. ***Decision Support Systems, 49***(2), 138-150.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. ***The Journal of Strategic Information Systems, 17***(2), 165-176.

Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. ***Journal of Cyber Policy, 1***(2), 243-264.

Bhansali, N. (2013). The Role of Data Governance in an Organization. In Bhansali, N. (Ed.). ***Data governance: Creating value from information assets*** (pp. 1-18). CRC Press.

DOI:10.6814/NCCU202000421

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. ***Information Systems Journal, 15***(1), 5-25.

Carter, L., & McBride, A. (2010). Information privacy concerns and e-government: a research agenda. ***Transforming Government: People, Process and Policy, 4***(1), 10-13.

Cespedes, F. V., & Smith, H. J. (1993). Database marketing: New rules for policy and practice. ***MIT Sloan Management Review, 34***(4), 7-22.

Chan, Y. E., & Reich, B. H. (2007). IT alignment: what have we learned?. ***Journal of Information Technology, 22***(4), 297-315.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. ***Organization Science, 10***(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. ***Journal of Social Issues, 59***(2), 323-342.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. ***MIS Quarterly, 13***(3), 319-340.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. ***Government Information Quarterly, 34***(1), 1-7.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). ***Internet, phone, mail, and mixed-mode surveys: the tailored design method*** (4th Ed.). New Jersey, NJ: John Wiley & Sons.

DOI:10.6814/NCCU202000421

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. ***Information Systems Research, 17***(1), 61-80.

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. ***Journal of Global Information Management (JGIM), 14***(4), 57-93.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. ***The Journal of Strategic Information Systems, 17***(3), 214-233.

Druckman, J. N., Green, D. P., Kuklinski, J. H., & Lupia, A. (2006). The growth and development of experimental research in political science. ***American Political Science Review, 100***(4), 627-635.

Foucault, M. (1995). ***Discipline and punish: the birth of the prison***. New York, NY: Vintage Books.

Giddens, A. (1985). ***The Nation-State and Violence: Volume 2 of A Contemporary Critique of Historical Materialism*** (2nd Ed.). California, CA: University of California Press.

Goodsell, C. T. (1990). Public administration and the public interest. In Wamsley, G. L. (Ed.). Refounding public administration (pp. 96-113). Newbury Park, CA: Sage Publication.

Granato, J., & Scioli, F. (2004). Puzzles, proverbs, and omega matrices: The scientific and social significance of empirical implications of theoretical models (EITM). ***Perspectives on Politics, 2***(2), 313-323.

DOI:10.6814/NCCU202000421

Hagel III, J., & Rayport, J. F. (1997). The coming battle for customer information. ***The McKinsey Quarterly, 3***, 64-77.

Henseler, J., & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. ***Computational Statistics, 28***(2), 565-580.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. ***Advances in International Marketing, 20,*** 277-319.

Homans, G. C. (1958). Social behavior as exchange. ***American Journal of Sociology, 63***(6), 597-606.

Hui, K. L., Tan, B. C., & Goh, C. Y. (2006). Online information disclosure: Motivators and measurements. ***ACM Transactions on Internet Technology (TOIT), 6***(4), 415-441.

Isson, J. P., & Harriott, J. (2012). ***Win with advanced business analytics: Creating business value from your data*** (Vol. 62). John Wiley & Sons.

Jabbour, C. J. C., Jugend, D., de Sousa Jabbour, A. B. L., Gunasekaran, A., & Latan, H. (2015). Green product development and performance of Brazilian firms: measuring the role of human and technical aspects. ***Journal of Cleaner Production, 87***, 442-451.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. ***Government Information Quarterly, 32***, 221-236.

Janssen, M., Rana, N. P., Slade, E. L., & Dwivedi, Y. K. (2018). Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling. ***Public Management Review, 20***(5), 647-671.

DOI:10.6814/NCCU202000421

Jeckmans, A. J., Beye, M., Erkin, Z., Hartel, P., Lagendijk, R. L., & Tang, Q. (2012). Privacy in recommender systems. In Ramzan, N., van Zwol, R., Lee, J. S., Clüver, K., & Hua, X. S. (Eds.). ***Social media retrieval*** (pp. 263-281). London, LON: Springer Science & Business Media.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: self-reports versus observed behavior. ***International Journal of Human-Computer Studies, 63***(1-2), 203-227.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. ***Information Systems Journal, 25***(6), 607-635.

Khatri, V., & Brown, C. V. (2010). Designing data governance. ***Communications of the ACM, 53***(1), 148-152.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. ***Computers in Human Behavior, 92***, 273-281.

Kim, M. S., & Kim, S. (2018). Factors influencing willingness to provide personal information for personalized recommendations. ***Computers in Human Behavior, 88***, 143-152.

Kim, S., & Kim, J. (2016). A Study on Factors Influencing Privacy Decision Making on the Internet: Focus on Dual-Calculus Model. ***The Journal of Information Systems, 25***(3), 197-215.

DOI:10.6814/NCCU202000421

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. ***Computers & Security, 64***, 122-134.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. ***Journal of Information Technology, 25***(2), 109-125.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. ***Journal of Social Issues, 33***(3), 22-42.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. ***European Journal of Information Systems, 18***(2), 177-187.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. ***Journal of Computer Information Systems, 51***(1), 62-71.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. ***International Journal of Medical Informatics, 88***, 8-17.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. ***Decision Support Systems, 54***(1), 471-481.

Longhurst, C. A., Harrington, R. A., & Shah, N. H. (2014). A 'green button' for using aggregate patient data at the point of care. ***Health Affairs, 33***(7), 1229-1235.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. ***Journal of the Academy of Marketing Science, 35***(4), 572-585.

DOI:10.6814/NCCU202000421

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. ***Journal of Applied Psychology, 90***(4), 710-730.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. ***Information Systems Research, 15***(4), 336-355.

McCallister, E. (2010). ***Guide to protecting the confidentiality of personally identifiable information***. Pennsylvania, PA: Diane Publishing.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. ***Journal of Electronic Commerce in Organizations (JECO), 4***(1), 1-17.

Mergel, I. (2016). Agile innovation management in government: A research agenda. ***Government Information Quarterly, 33***(3), 516-523.

Mills, J. L. (1993). Data torturing. ***The New England Journal of Medicine, 329***(16), 1196-1199.

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. ***Information & Management, 52***(6), 741-759.

Milutinovic, M., & De Decker, B. (2015). Privacy-Friendly Management of Electronic Health Records in the eHealth Context. In C. Dolicanin, E. Kajan, D. Randjelovic, & B. Stojanovic (Eds.). ***Handbook of research on democratic strategies and citizen-centered e-government services*** (pp. 251-264). Pennsylvania, PA: IGI Global.

DOI:10.6814/NCCU202000421

Monecke, A., & Leisch, F. (2012). ***semPLS: Structural equation modeling using partial least squares***. Retrieved March 10, 2020, from https://cran.r-project.org/web/packages/semPLS/vignettes/semPLS-intro.pdf.

Moore, G. C., & Benbasat, I. (1996). Integrating diffusion of innovations and theory of reasoned action models to predict utilization of information technology by end-users. In Kautz, K., & Pries-Heje, J. (Eds.). ***Diffusion and adoption of information technology*** (pp. 132-146). Springer, Boston, MA.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2019). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. ***Government Information Quarterly***. Retrieved from https://www.sciencedirect.com/science/article/pii/S0740624X19300735.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. ***Journal of Consumer Affairs, 41***(1), 100-126.

Papadopoulou, P., M. Nikolaidou, & D. Martakos (2010, January). ***What is trust in e-government? A proposed typology***. The 43th Hawaii International Conference on System Sciences, Koloa, Kauai, HI, USA.

Perry, J. L. (2012). How can we improve our science to generate more usable knowledge for public professionals?. ***Public Administration Review, 72***(4), 479-482.

DOI:10.6814/NCCU202000421

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. ***Journal of Public Policy & Marketing, 19***(1), 27-41.

Poikola, A., Kuikkaniemi, K., & Honko, H. (2015). ***Mydata a nordic model for human-centered personal data management and processing***. Finnish Ministry of Transport and Communications.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. ***The Journal of Psychology, 91***(1), 93–114.

Roth, A. E. (1995). Introduction to experimental economics. In Kagel, J. H. & Roth, A. E. (Eds.) ***The Handbook of Experimental Economics*** (pp. 3-109). Princeton, NJ: Princeton University Press.

Sang, S., Lee, J. D., & Lee, J. (2009). E-government adoption in ASEAN: the case of Cambodia. ***Internet Research, 19***(5), 517-534.

Shadbolt, N. (2013). Midata: towards a personal information revolution. In O'Hara, K., Waidner, M., & Hildebrandt, M. (Eds.). ***Digital Enlightenment Yearbook 2013: The Value of Personal Data*** (pp. 202-224). IOS Press.

Sheng, H., Nah, F. F. H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. ***Journal of the Association for Information Systems, 9***(6), 15.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. ***MIS Quarterly, 35***(4), 989-1016.

Steinfeld, N. (2017). Track me, track me not: Support and consent to state and private sector surveillance. ***Telematics and Informatics, 34***(8), 1663-1672.

DOI:10.6814/NCCU202000421

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. ***Research in Personnel and Human Resources Management, 8***(3), 349-411.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. ***Journal of Applied Psychology, 68***(3), 459.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. ***Journalism & Mass Communication Quarterly, 93***(2), 296-311.

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2019). Privacy and the panopticon: Online mass surveillance's deterrence and chilling effects. ***New Media & Society, 21***(3), 602-619.

Teo, T. S., Srivastava, S. C., & Jiang, L. (2009). Trust and electronic government success: An empirical study. ***Journal of Management Information Systems, 25***(3), 99-132.

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. ***Government Information Quarterly, 32***(3), 316-322.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: toward a conceptual model of utilization. ***MIS Quarterly, 15***(1), 125-143.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. ***Information Systems Research, 22***(2), 254-268.

DOI:10.6814/NCCU202000421

Turvey, C., Klein, D., Fix, G., Hogan, T. P., Woods, S., Simon, S. R., ... & Wakefield, B. (2014). Blue Button use by patients to access and share health record information using the Department of Veterans Affairs' online patient portal. ***Journal of the American Medical Informatics Association, 21***(4), 657-663.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. ***MIS Quarterly, 27***(3), 425-478.

Wang, J. C., & Chang, C. H. (2013). How online social ties and product-related risks influence purchase intentions: A Facebook experiment. ***Electronic Commerce Research and Applications, 12***(5), 337-346.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. ***International Journal of Information Management, 36***(4), 531-542.

Warkentin, M., Gefen, D., Pavlou, P., & Rose, G. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. ***Electronic Markets, 12***(3), 157-162.

Wells, C., & Thorson, K. (2017). Combining big data and survey techniques to model effects of political content flows in Facebook. ***Social Science Computer Review, 35***(1), 33-52.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. ***International Journal of Service Industry Management, 18***(4), 326-348.

DOI:10.6814/NCCU202000421

Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. ***Marketing Letters, 17***(1), 61-74.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision-making process for location-aware marketing. ***Decision Support Systems, 51***(1), 42-52.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. ***Journal of Management Information Systems, 26***(3), 135-174.

DOI:10.6814/NCCU202000421

附錄一 問卷設計

行政院於 2019 年 6 月核定了「**數位身分識別證（New eID）**」換發計畫，規劃結合國民身分證及自然人憑證取代現有的紙本身分證，未來民眾可以透過這個數位身分識別證在臨櫃或網路上識別身份後，將個人資料授權給特定政府機關，以獲得包括社會福利、交通監理、動產交易與公投連署等 16 項個人化服務。

本研究將瞭解您對於數位身分識別政策的看法，麻煩您閱讀並同意我們的受訪者權益聲明後，再繼續填答問卷。本研究會確保您的意見與身分保密，這份問卷不會包含您的身分識別資訊，您的個人資訊將不會被公開。如果您拒絕參與這個研究，不會影響您任何權益，您也可以隨時終止填答問卷。

學術研究無法排除所有風險，但本研究已採取所有適當的預防措施，當您點選「下一步」開始進行調查，即表示您同意本聲明的條款。

《個人資料保護法》中的個資定義包含：「自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」

以下將請教您對個人資料管理的看法，1 代表非常不同意，7 代表非常同意，請您依真實的想法回答下列問題。

1. 請問您個人的每個月總收入大約是多少？（包括薪資以外的其他收入，如房租、股利等等）

   □01. 28000 以下　□02. 28001 元~39000 元　□03. 39001 元~49000 元
   □04. 49001 元~59000 元　□05. 59001 元~70000 元　□06. 70001 元~80000 元
   □07. 80001 元~94000 元　□08. 94001 元~111000 元
   □09. 111001 元~143000 元　□10. 143001 元以上

2. 請問在過去一年來，您的個人隱私資料有沒有受過侵害？如果有的話大約幾次？

   □有，大概__次　□(0)沒有

DOI:10.6814/NCCU202000421

題目	選項
3. 我有能力可以管理自己的個人資料	1 非常不同意 ・・・・・・ 7 非常同意
4. 我可以遵循預防措施來保護個人資料	1 非常不同意 ・・・・・・ 7 非常同意
5. 每當需要時，我都可以採取預防措施來保護自己的隱私	1 非常不同意 ・・・・・・ 7 非常同意
6. 我可以防止他人非法存取我的個人資料	1 非常不同意 ・・・・・・ 7 非常同意
7. 我可以防止個人資料洩漏造成的詐騙或身分盜用等損失	1 非常不同意 ・・・・・・ 7 非常同意
8. 整體而言，我可以保護個人資料的安全	1 非常不同意 ・・・・・・ 7 非常同意
9. 我可以自行決定是否授權個人資料給政府機關	1 非常不同意 ・・・・・・ 7 非常同意
10. 我可以掌握授權給政府機關的個人資料範圍	1 非常不同意 ・・・・・・ 7 非常同意
11. 整體而言，我對於個人資料的授權有充分控制權	1 非常不同意 ・・・・・・ 7 非常同意

《個人資料保護法》中的個資定義包含：「自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」

以下將請教您對個人資料外洩風險的看法，1 代表非常不同意，7 代表非常同意，請您依真實的想法回答下列問題。

題目	選項
12. 我的個人資料可能會不經我的同意被分享給第三方	1 非常不同意 ・・・・・・ 7 非常同意
13. 我的個人資料可能會被用於服務提供的用途之外	1 非常不同意 ・・・・・・ 7 非常同意
14. 我的個人資料可能會被非法的使用	1 非常不同意 ・・・・・・ 7 非常同意
15. 當個人資料洩漏時，我的隱私可能會受到侵犯	1 非常不同意 ・・・・・・ 7 非常同意
16. 當個人資料洩漏時，可能會造成我在金錢上的損失	1 非常不同意 ・・・・・・ 7 非常同意
17. 整體而言，我認為個人資料洩漏是個嚴重的問題	1 非常不同意 ・・・・・・ 7 非常同意
18. 授權個人資料給政府機關，對我來說是件很敏感的事	1 非常不同意 ・・・・・・ 7 非常同意
19. 授權個人資料給政府機關，可能會讓我的個人隱私在網路上被其他人搜尋到	1 非常不同意 ・・・・・・ 7 非常同意
20. 整體來說，將個人資料授權給政府機關會造成隱私問題	1 非常不同意 ・・・・・・ 7 非常同意

DOI:10.6814/NCCU202000421

民眾可以利用數位身分識別證(New eID)進行臨櫃或線上的數位身分識別，經數位身分識別後，即可以連結政府各機關的後端資料庫，以享受政府機關所提供的服務，例如健保、駕照監理、社會福利等。

以下將請教您對數位身分識別證（New eID）預期效益的看法，1 代表非常不同意，7 代表非常同意，請您依真實的想法回答下列問題。

題目	選項
21. 透過數位身分識別證可以讓我申請到更多的社會福利補助	1 非常不同意 ・・・・・・ 7 非常同意
22. 透過數位身分識別證可以節省我申請公共服務時的費用	1 非常不同意 ・・・・・・ 7 非常同意
23. 對我而言，使用數位身分識別證具有經濟上的效益	1 非常不同意 ・・・・・・ 7 非常同意
24. 數位身分識別證可以提供適合我的個人化公共服務	1 非常不同意 ・・・・・・ 7 非常同意
25. 數位身分識別證可以提供我想要的公共服務資訊	1 非常不同意 ・・・・・・ 7 非常同意
26. 數位身分識別證可以為我量身打造更多的個人化公共服務	1 非常不同意 ・・・・・・ 7 非常同意
27. 數位身分識別證可以與我的工作緊密結合	1 非常不同意 ・・・・・・ 7 非常同意
28. 數位身分識別證適合運用在我的工作上	1 非常不同意 ・・・・・・ 7 非常同意
29. 數位身分識別證可以提高我的工作效率	1 非常不同意 ・・・・・・ 7 非常同意

內政部現行規劃的數位身分識別證（New eID），在版面上公開的個人資料採最小化進行設計，晶片所儲存的個人資料與現行紙本身分證相同，不會儲存其他資料。同時個人其他隱私資料（如父母姓名、配偶姓名等）會加密保護儲存，使用時需經民眾同意，並輸入自行設定的密碼後，取用機關才可向內政部申請該資訊。

以下將請教您使用數位身分識別證（New eID）的預期看法，1 代表非常不同意，7 代表非常同意，請您依真實的想法回答下列問題。

題目	選項
30. 對我而言，學習如何運用數位身分識別證很容易	1 非常不同意 ・・・・・・ 7 非常同意
31. 我認為數位身分識別證的操作是簡單且易懂的	1 非常不同意 ・・・・・・ 7 非常同意
32. 對我而言，熟練地使用數位身分識別證是很輕鬆的	1 非常不同意 ・・・・・・ 7 非常同意
33. 數位身分識別證有助於縮短我搜尋公共服務的時間	1 非常不同意 ・・・・・・ 7 非常同意
34. 數位身分識別證有助於提高我所獲得的公共服務品質	1 非常不同意 ・・・・・・ 7 非常同意
35. 整體而言，我認為使用數位身分識別證是有益的	1 非常不同意 ・・・・・・ 7 非常同意
36. 透過數位身分識別證授權政府機關使用我的個人資料，可能會產生預期之外的負面後果	1 非常不同意 ・・・・・・ 7 非常同意

DOI:10.6814/NCCU202000421

題目	選項
37. 透過數位身分識別證授權政府機關使用我的個人資料，有很高的機率會導致損失	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
38. 整體來說，透過數位身分識別證授權政府機關使用我的個人資料是有風險的	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
39. 當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的性別、年齡、婚姻狀況等個人資料	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
40. 當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我過去的使用紀錄	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
41. 當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的醫療與健康資訊	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
42. 當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的銀行與財務資訊	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意

以下將請教您對政府在運用民眾個人資料時的看法，1 代表非常不同意，7 代表非常同意，請您依真實的想法回答下列問題。

題目	選項
43. 我擔心政府擁有監控網路活動的權力	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
44. 我擔心政府擁有監控網路活動的能力	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
45. 我擔心我在網路上的活動紀錄會受到政府的審查	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
46. 我相信政府會運用安全的技術來管理我的個人資料	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
47. 當我的個人資料被濫用時，我可以取得政府相關單位的協助	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
48. 我相信政府會在適當的法律授權下來運用我的個人資料	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
49. 政府機關所提供的線上交易服務是值得信任的	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
50. 我相信政府機關會維護我的最高利益	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意
51. 整體來說，政府機關是值得信任的	1 非常不同意 ・ ・ ・ ・ ・ 7 非常同意

DOI:10.6814/NCCU202000421

附錄二 次數分配表[36]

構面：CPE 應對效能			
選項/題項	我有能力可以管理自己的個人資料	我可以遵循預防措施來保護個人資料	每當需要時，我都可以採取預防措施來保護自己的隱私
	次數（百分比）		
1 非常不同意	12（1.6%）	8（1.1%）	9（1.2%）
2	25（3.4%）	12（1.6%）	22（3.0%）
3	94（12.7%）	63（8.5%）	89（12.0%）
4	99（13.3%）	96（12.9%）	117（15.7%）
5	226（30.4%）	269（36.2%）	238（32.0%）
6	178（24.0%）	193（26.0%）	180（24.2%）
7 非常同意	109（14.7%）	102（13.7%）	88（11.8%）
總計	743（100.0%）	743（100.0%）	743（100.0%）

[36] 次數分配表內的數值為未經加權的原始資料。

DOI:10.6814/NCCU202000421

構面：SEL 自我效能			
選項/題項	我可以防止他人非法存取我的個人資料	我可以防止個人資料洩漏造成的詐騙或身分盜用等損失	整體而言，我可以保護個人資料的安全
	次數（百分比）		
1 非常不同意	35（4.7%）	30（4.0%）	14（1.9%）
2	95（12.8%）	77（10.4%）	43（5.8%）
3	190（25.6%）	166（22.3%）	129（17.4%）
4	155（20.9%）	148（19.9%）	172（23.1%）
5	155（20.9%）	183（24.6%）	227（30.6%）
6	72（9.7%）	89（12%）	105（14.1%）
7 非常同意	41（5.5%）	50（6.7%）	53（7.1%）
總計	743（100.0%）	743（100.0%）	743（100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：CAP 應對評價			
選項/題項	我可以自行決定是否授權個人資料給政府機關	我可以掌握授權給政府機關的個人資料範圍	整體而言，我對於個人資料的授權有充分控制權
	次數（百分比）		
1 非常不同意	13 （1.7%）	29 （3.9%）	22 （3.0%）
2	37 （5.0%）	63 （8.5%）	54 （7.3%）
3	87 （11.7%）	164 （22.1%）	132 （17.8%）
4	110 （14.8%）	135 （18.2%）	148 （19.9%）
5	220 （29.6%）	191 （25.7%）	195 （26.2%）
6	164 （22.1%）	92 （12.4%）	107 （14.4%）
7 非常同意	112 （15.1%）	69 （9.3%）	85 （11.4%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：VUL 感知脆弱性			
選項/題項	我的個人資料可能會不經我的同意被分享給第三方	我的個人資料可能會被用於服務提供的用途之外	我的個人資料可能會被非法的使用
	次數（百分比）		
1　非常不同意	22 （3.0%）	13 （1.7%）	15 （2.0%）
2	15 （2.0%）	12 （1.6%）	17 （2.3%）
3	30 （4.0%）	30 （4.0%）	46 （6.2%）
4	66 （8.9%）	56 （7.5%）	97 （13.1%）
5	198 （26.6%）	227 （30.6%）	211 （28.4%）
6	195 （26.2%）	199 （26.8%）	179 （24.1%）
7　非常同意	217 （29.2%）	206 （27.7%）	178 （24.0%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：SEV 感知嚴重性			
選項/題項	當個人資料洩漏時，我的隱私可能會受到侵犯	當個人資料洩漏時，可能會造成我在金錢上的損失	整體而言，我認為個人資料洩漏是個嚴重的問題
	次數（百分比）		
1 非常不同意	1 （0.1%）	2 （0.3%）	2 （0.3%）
2	2 （0.3%）	5 （0.7%）	2 （0.3%）
3	9 （1.2%）	33 （4.4%）	11 （1.5%）
4	38 （5.1%）	94 （12.7%）	34 （4.6%）
5	152 （20.5%）	220 （29.6%）	118 （15.9%）
6	223 （30.0%）	176 （23.7%）	168 （22.6%）
7 非常同意	318 （42.8%）	213 （28.7%）	408 （54.9%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：RIAP 風險評價			
選項/題項	授權個人資料給政府機關，對我來說是件很敏感的事	授權個人資料給政府機關，可能會讓我的個人隱私在網路上被其他人搜尋到	整體來說，將個人資料授權給政府機關會造成隱私問題
	次數（百分比）		
1 非常不同意	6 （0.8%）	6 （0.8%）	5 （0.7%）
2	17 （2.3%）	26 （3.5%）	16 （2.2%）
3	85 （11.4%）	86 （11.6%）	88 （11.8%）
4	151 （20.3%）	130 （17.5%）	174 （23.4%）
5	199 （26.8%）	182 （24.5%）	164 （22.1%）
6	137 （18.4%）	139 （18.7%）	141 （19.0%）
7 非常同意	148 （19.9%）	174 （23.4%）	155 （20.9%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：FNW 財務報償			
選項/題項	透過數位身分識別證可以讓我申請到更多的社會福利補助	透過數位身分識別證可以節省我申請公共服務時的費用	對我而言，使用數位身分識別證具有經濟上的效益
	次數（百分比）		
1 非常不同意	34（4.6%）	11（1.5%）	16（2.2%）
2	49（6.6%）	16（2.2%）	22（3.0%）
3	128（17.2%）	51（6.9%）	72（9.7%）
4	175（23.6%）	112（15.1%）	144（19.4%）
5	199（26.8%）	236（31.8%）	238（32%）
6	94（12.7%）	187（25.2%）	148（19.9%）
7 非常同意	64（8.6%）	130（17.5%）	103（13.9%）
總計	743（100.0%）	743（100.0%）	743（100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：PER 個性化服務			
選項/題項	數位身分識別證可以提供適合我的個人化公共服務	數位身分識別證可以提供我想要的公共服務資訊	數位身分識別證可以為我量身打造更多的個人化公共服務
	次數（百分比）		
1 非常不同意	8 （1.1%）	10 （1.3%）	15 （2.0%）
2	17 （2.3%）	15 （2.0%）	26 （3.5%）
3	61 （8.2%）	70 （9.4%）	81 （10.9%）
4	144 （19.4%）	156 （21.0%）	167 （22.5%）
5	234 （31.5%）	237 （31.9%）	216 （29.1%）
6	181 （24.4%）	159 （21.4%）	151 （20.3%）
7 非常同意	98 （13.2%）	96 （12.9%）	87 （11.7%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：COMP 服務兼容性

選項/題項	數位身分識別證可以與我的工作緊密結合	數位身分識別證適合運用在我的工作上	數位身分識別證可以提高我的工作效率
	次數（百分比）		
1 非常不同意	35（4.7%）	44（5.9%）	60（8.1%）
2	47（6.3%）	48（6.5%）	68（9.2%）
3	152（20.5%）	176（23.7%）	164（22.1%）
4	200（26.9%）	219（29.5%）	203（27.3%）
5	168（22.6%）	146（19.7%）	148（19.9%）
6	89（12.0%）	65（8.7%）	60（8.1%）
7 非常同意	52（7.0%）	45（6.1%）	40（5.4%）
總計	743（100.0%）	743（100.0%）	743（100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：EE 預期投入			
選項/題項	對我而言，學習如何運用數位身分識別證很容易	我認為數位身分識別證的操作是簡單且易懂的	對我而言，熟練地使用數位身分識別證是很輕鬆的
	次數（百分比）		
1 非常不同意	12（1.6%）	13（1.7%）	11（1.5%）
2	11（1.5%）	9（1.2%）	11（1.5%）
3	66（8.9%）	76（10.2%）	65（8.7%）
4	147（19.8%）	178（24.0%）	175（23.6%）
5	208（28.0%）	229（30.8%）	220（29.6%）
6	180（24.2%）	144（19.4%）	161（21.7%）
7 非常同意	119（16.0%）	94（12.7%）	100（13.5%）
總計	743（100.0%）	743（100.0%）	743（100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：BEN 隱私利益			
選項/題項	數位身分識別證有助於縮短我搜尋公共服務的時間	數位身分識別證有助於提高我所獲得的公共服務品質	整體而言，我認為使用數位身分識別證是有益的
	次數（百分比）		
1 非常不同意	15 （2.0%）	14 （1.9%）	12 （1.6%）
2	12 （1.6%）	22 （3%）	20 （2.7%）
3	61 （8.2%）	74 （10.0%）	61 （8.2%）
4	152 （20.5%）	172 （23.1%）	171 （23.0%）
5	216 （29.1%）	224 （30.1%）	210 （28.3%）
6	181 （24.4%）	156 （21.0%）	168 （22.6%）
7 非常同意	106 （14.3%）	81 （10.9%）	101 （13.6%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：RISK 隱私風險			
選項/題項	透過數位身分識別證授權政府機關使用我的個人資料，可能會產生預期之外的負面後果	透過數位身分識別證授權政府機關使用我的個人資料，有很高的機率會導致損失	整體來說，透過數位身分識別證授權政府機關使用我的個人資料是有風險的
	次數（百分比）		
1 非常不同意	5 （0.7%）	8 （1.1%）	4 （0.5%）
2	9 （1.2%）	34 （4.6%）	23 （3.1%）
3	74 （10.0%）	121 （16.3%）	75 （10.1%）
4	181 （24.4%）	227 （30.6%）	199 （26.8%）
5	228 （30.7%）	180 （24.2%）	220 （29.6%）
6	123 （16.6%）	91 （12.2%）	114 （15.3%）
7 非常同意	123 （16.6%）	82 （11.0%）	108 （14.5%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：ATT 資料授權意願

選項/題項	當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的性別、年齡、婚姻狀況等個人資料	當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我過去的使用紀錄	當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的醫療與健康資訊	當我有個人化服務需求時，我願意透過數位身分識別證，授權政府存取我的銀行與財務資訊
	次數（百分比）			
1 非常不同意	27（3.6%）	33（4.4%）	20（2.7%）	103（13.9%）
2	25（3.4%）	43（5.8%）	33（4.4%）	84（11.3%）
3	74（10.0%）	103（13.9%）	54（7.3%）	150（20.2%）
4	164（22.1%）	166（22.3%）	138（18.6%）	166（22.3%）
5	255（34.3%）	217（29.2%）	238（32.0%）	146（19.7%）
6	133（17.9%）	126（17.0%）	159（21.4%）	60（8.1%）
7 非常同意	65（8.7%）	55（7.4%）	101（13.6%）	34（4.6%）
總計	743（100.0%）	743（100.0%）	743（100.0%）	743（100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：GIC 政府監控疑慮			
選項/題項	我擔心政府擁有監控網路活動的權力	我擔心政府擁有監控網路活動的能力	我擔心我在網路上的活動紀錄會受到政府的審查
	次數（百分比）		
1　非常不同意	5 （0.7%）	5 （0.7%）	8 （1.1%）
2	23 （3.1%）	28 （3.8%）	31 （4.2%）
3	55 （7.4%）	53 （7.1%）	71 （9.6%）
4	111 （14.9%）	119 （16.0%）	121 （16.3%）
5	184 （24.8%）	186 （25%）	171 （23.0%）
6	146 （19.7%）	142 （19.1%）	138 （18.6%）
7　非常同意	219 （29.5%）	210 （28.3%）	203 （27.3%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：REG 風險管理機制			
選項/題項	我相信政府會運用安全的技術來管理我的個人資料	當我的個人資料被濫用時，我可以取得政府相關單位的協助	我相信政府會在適當的法律授權下來運用我的個人資料
	次數（百分比）		
1　非常不同意	34 （4.6%）	51 （6.9%）	50 （6.7%）
2	56 （7.5%）	61 （8.2%）	61 （8.2%）
3	96 （12.9%）	117 （15.7%）	94 （12.7%）
4	173 （23.3%）	202 （27.2%）	194 （26.1%）
5	185 （24.9%）	164 （22.1%）	201 （27.1%）
6	108 （14.5%）	92 （12.4%）	86 （11.6%）
7　非常同意	91 （12.2%）	56 （7.5%）	57 （7.7%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

構面：TOG 政府信任			
選項/題項	政府機關所提供的線上交易服務是值得信任的	我相信政府機關會維護我的最高利益	整體來說，政府機關是值得信任的
	次數（百分比）		
1 非常不同意	38 （5.1%）	64 （8.6%）	57 （7.7%）
2	43 （5.8%）	60 （8.1%）	62 （8.3%）
3	93 （12.5%）	120 （16.2%）	93 （12.5%）
4	215 （28.9%）	195 （26.2%）	197 （26.5%）
5	215 （28.9%）	175 （23.6%）	196 （26.4%）
6	97 （13.1%）	84 （11.3%）	99 （13.3%）
7 非常同意	42 （5.7%）	45 （6.1%）	39 （5.2%）
總計	743 （100.0%）	743 （100.0%）	743 （100.0%）

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421

附錄三 控制變項重新編碼表

變項名稱	原有數值	重新編碼方式
性別	1 男性 2 女性	重新編碼為男性=1、女性=0的虛擬變數
年齡	1 20至29歲 2 30至39歲 3 40至49歲 4 50至59歲 5 60歲及以上	直接視為順序尺度分析
教育程度	1 小學及以下 2 國、初中 3 高中、職 4 專科 5 大學及以上	直接視為順序尺度分析
居住地區	1 北部地區 2 中部地區 3 南部地區 4 東部與離島地區	重新編碼為3組虛擬變數，參照組為「北部地區」。
隱私外洩經驗	1 無 2 有	重新編碼為有隱私外洩經驗=1、無隱私外洩經驗=0的虛擬變數
收入	1 28000以下	直接視為順序尺度分析

DOI:10.6814/NCCU202000421

變項名稱	原有數值	重新編碼方式
	2 28001元~39000元 3 39001元~49000元 4 49001元~59000元 5 59001元~70000元 6 70001元~80000元 7 80001元~94000元 8 94001元~111000元 9 111001元以上	
政黨認同	1 國民黨 2 民進黨 3 新黨 4 親民黨 5 臺灣團結聯盟 6 時代力量 7 台灣民眾黨 8 中立及看情形 9 無反應及其他政黨	將國民黨、新黨、親民黨重新編碼為「泛藍政黨」，將民進黨、臺灣團結聯盟重新編碼為「泛綠政黨」，將其餘選項重新編碼為「中立及其他政黨」。 重新編碼後可得「泛藍政黨」、「泛綠政黨」與「中立及其他政黨」三個選項，再重新編碼為2組虛擬變數，參照組為「中立及其他政黨」。

資料來源：本研究自行整理。

DOI:10.6814/NCCU202000421