資訊隱私侵害行爲意圖之研究

A Study of Information Privacy Intrusion Behavioral Intention

任文瑗
僑光技術學院資訊管理系
台中市西屯 40724 僑光路 100 號
denise@ocit.edu.tw

范錚強
中央大學資訊管理系
桃園縣中壢市 32001 中大路 300 號
ckfarn@mgt.ncu.edu.tw

許通安
中原大學資訊管理系
桃園縣中壢市 32023 中北路 200 號
tahsu@mis.cycu.edu.tw

摘要

資訊社會爲了提供更多元的個人化服務，蒐集、交換與儲存個人隱私資料的現象充斥在現實生活中。電子商務和電子化政府等資訊社會發展的背後，人民的資訊隱私權經常受到某種程度的威脅與傷害。保護資訊隱私權是維護資訊社會正常運作的必要條件，維護資訊隱私權就是維持資訊社會的秩序。侵害資訊隱私權的行爲會影響資訊社會的秩序並妨害資訊社會的發展，因此資訊隱私侵害行爲之相關議題相當值得探討與研究。本研究擬以法律觀點對個人資料隱私權之侵害所規範的行爲作爲研究範疇，透過理性選擇理論、計畫行爲理論探討大專學生侵害資訊隱私權的行爲意圖，並以實徵研究的結果分析影響侵害資訊隱私之行爲意圖的因素。

關鍵詞:理性選擇理論、計畫行爲理論、資訊隱私權、資訊隱私侵害行爲。

Abstract

In order to provide more customized services, the growing cyber society continues to expand activities in collecting, storing, searching, and exchanging private personal data. As electronic commerce and e-government services develop, the privacy of people's personal information is easily threatened. The protection of personal information is essential to maintaining the stability fundamental to a well-functioning cyber society. Since information privacy intrusion hinders the development of cyber society, any issue related to information privacy intrusion is worth exploration. Employing both the theory of planned behavior and rational choice theory, this study explores the intention to intrude upon people's private data

and identifies and analyses significant factors influencing information privacy intrusion behavior among college students.

Keywords: Rational Choice Theory, Theory of Planned Behavior, Information Privacy, Information Privacy Intrusion.

壹、緒論

資訊社會中的資訊隱私權(Information privacy)是一項被認爲重要，卻又容易被忽視的議題。保護資訊隱私權是維護資訊社會安全的必要條件；然而，受到龐大的政治控制、經濟利益與個人私慾等箝制，資訊隱私權相關議題未能得到資訊社會應有的重視與關注。侵害隱私權除了會改變公領域、私領域與人我之間的界限，甚至可能對個人、社會與國家帶來無法控制或彌補的傷害，例如：勞委會首例員工因轉寄電子郵件而被開除的案例，是聯電董事長曹興誠透過電子郵件寄發「致員工一封信」(該信件沒有註明不得對外透露)，被 200 多名員工將此郵件傳給親朋好友。由於該信件被媒體大肆報導，引發曹興誠不快，進而在未發放資遣費的情況下開除 10 名員工[2]。在資訊社會中，我們經常將自己的活動以電磁記錄方式散佈在各地，例如：出生、就醫、交易等記錄，亦被收錄在不同單位的資料庫。然而，網路社會的匿名性、跨國性、自治性、網路普及性與表達特殊性等，衍生諸多資訊隱私權的侵權行爲態樣[3]。我們不僅擔心個人的隱私權受侵害，更擔憂我們對個人資訊的自我決定權已慢慢消失，因爲資訊的普及與即時等特性，削減個人對自身資訊的主動掌控能力，這是資訊隱私權的最大隱憂。

Williams and McShane[67]指出，人類的行爲相當複雜，很難被過於簡單的理論所解釋，因此在引用理論的過程中，必須要經過系統觀察和小心的邏輯推演，才能對目前的人類行爲作更深入探討。過去許多資訊管理文獻在探討使用資訊科技的侵害行爲時，經常以不當行爲、不符道德期待的行爲作爲研究標的，較少採用法律觀點或犯罪學理論探討個人資料隱私權的侵害行爲。因此，本研究以法律觀點，透過社會心理學理論與犯罪學理論探討資訊隱私侵害行爲的意圖。希冀實證研究的結果能進一步解釋何種因素能夠有效抑止資訊隱私侵害行爲的意圖，此乃本研究之研究動機。

貳、文獻探討

一、資訊隱私權

Gormley[34]認爲隱私權有四個基本理念：(1)個人性格的表達，強調人類特質的權利；(2)個人自治權，個人擁有思想、行動與決定的自由；(3)個人有規範自身資訊，以及控制與其他人交往的能力；(4)個人擁有秘密、匿名與獨處的權利。隱私權的定義有不少版本與說法，基本上各學說均強調「人有權獨處，不被打擾」的精神[65]，傳達隱私權不可侵犯的基本信念。綜合 Westin[66]、Clarke[22]與 Agranoff[8]對資訊隱私權的定義，本研究對資訊隱私權的定義如下：

(1)資料蒐集：特定人、團體與機關等，必須在合法且必要的情況，才得以蒐集個人資料，而且在使用個人資料時，必須受到一定程度的規範。(2)資料正確性：

個人擁有存取檔案資料，以及更正錯誤資料的權利。(3)資料私密性：任何人、團體或組織，針對於自身之資料，得以自己決定，何時、何地、如何及在何種程度內，將個人資料傳達給他人的權利。

資訊隱私權隱含於隱私權內涵的一部份，因爲資訊隱私權是隱私權的子集合。爲了更清楚地表達資訊隱私權與隱私權的差異，相關的說明簡述如下：(1)資訊隱私權的範疇較明確，資訊隱私權的內涵與範疇比較明確，其基礎也比較穩，例如：個人資訊保護法第三條清楚規定個人資訊被保護的範圍。(2)資訊隱私權較積極，傳統隱私權強調個人的私密生活不要被侵擾，較偏重在身體之生活空間的保護，對於靜態之個人資訊的保護比較不週延、消極。相較之下，資訊隱私權提供人民請求保護個人資料的權利，當人民的個人資料被蒐集、被利用、或被傳輸時，人民享有被告知的權利，同時人民也有權要求停止、或刪除這一類不當行爲權利。(3)資訊隱私權較主動，人民的隱私權被侵害，可以請求法院排除妨害及損害賠償，其權利屬於事後性質，因此隱私權的權利被視爲被動性質。相較之下，資訊隱私權所賦予的積極性權利，人民可以決定自身資料的運用、檢測與修改，進以維持個人資料的正確性，甚至包括他人對自身資料之無理由取得與使用，以及因而導致的危險之防止[1]。

資訊隱私權被侵害類型有五種類型[5, 7]，如表一所示。若以組織層級（Firm level）、個人層級（Individual level）來檢視這五種類型，有些類型屬於組織對個人的侵權行爲，有些類型屬於個人對個人的侵權行爲，亦有些是兩者皆是，相關說明如下所示：

1. 組織層級（Firm level）

   較常發生在組織層級的侵權類型有下列三類：(1)通訊內容隱私權的侵害，經常被應用在司法單位、ISP 業者與僱主等，通常是對特定人士的個人資料或行爲進行監控。(2)新興科技對隱私權的侵害，排除網路使用者的主動行爲，多數被應用在企業網站，通常是在網路使用者不知情的情況下，以資訊工具記錄個別網路使用者的行爲，侵犯個人的資訊隱私權，例如：特洛依木馬程式對資訊隱私權是極具傷害性的軟體。(3)匿名隱私權的侵害，爲了減少犯罪偵查的阻礙，網站管理者要求使用者對自己言論負責的共識已形成，多數人能接受網站管理者的善意考量。

2. 個人層級（Individual level）

   常見之個人層級的侵權行爲有「個人資料隱私權的侵害」、「個人屬性隱私權的侵害」兩種。兩者之中，又以侵害個人資料隱私權的灰色空間較大，因爲被侵害者不一定能很清楚確定本身的個人資料是否已被侵犯，有時甚至侵犯他人資訊隱私權時亦不自知。由於個人屬性隱私權的侵害則是較清楚、明確，例如：在網路上公佈他人隱私，這部份較強調被侵權者之個人屬性的隱私權。

個人資料隱私權的侵害項目共計五種，「濫發電子廣告信」是最普遍、最常見的侵權行爲，通常是組織層級用來進行商業活動，而且這種侵權行爲在立法與執法方面有較大的彈性空間與不確定性，因此不列入本研究的範圍。有關「散佈侵害隱私權之軟體」與「侵入他人系統獲取資料」的侵權行爲，牽涉到較高的資訊科技專業知識，一般民眾對這類侵權行爲的認知較有限。爲減少調查研究誤差發生的機率，這二種侵權行爲亦不列爲研究範圍。至於「個人資料的商業化」與「不當洩漏他人資料」侵權行爲，一般人可能因爲工作場所、環境便利或對資訊隱私權的認知不足等狀況，較有機會涉及上述的

侵權行爲，或是較常從報章雜誌接觸上述侵權行爲的新聞事件，對這類型之資訊隱私侵權行爲較不陌生。因此，擬以這二項侵權行爲作爲本文的研究範圍。

表一　資訊隱私權被侵犯的類型

類型	項目	較常侵害之層級
通訊內容隱私權之侵害	網路監聽	組織
	電子郵件監看	
個人資料隱私權之侵害	個人資料的商業化*	組織 個人
	濫發電子廣告信	
	散佈侵害隱私權之軟體	
	侵入他人系統以獲取資料	
	不當洩漏他人資料*	
個人屬性隱私權之侵害	網路視訊	個人
	行爲的監視	
匿名隱私權之侵害	禁止網路匿名的形式，造成對匿名隱私權的侵害。	組織
新興科技對隱私權之侵害	網頁瀏覽器的 Cookies 蒐集造成隱私權的侵害	組織
	Pentium III 電腦晶片中加入識別序號之爭議	
	Office 97 電腦軟體公司蒐集特殊電腦認證資訊	
	RealNetworks 秘密蒐集消費者個人資料	

*：研究範圍

資料來源：侵權類型與項目歸納整理自簡榮宗[7]；邱惠雯[5]

二、資訊隱私侵害行爲意圖

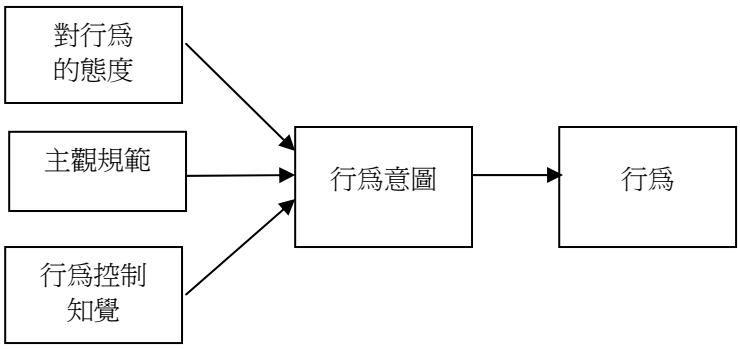
不同社會的道德價值、文化、倫理、規範與法律皆有其不同的觀點與期許，任何偏差行爲亦沒有固定的行爲模式，但是每個社會皆將妨礙他人生活、異於社會期待、造成他人痛苦、社會成長停滯等行爲視爲偏差行爲，某些破壞社會秩序與公共安全的偏差行爲，甚至被視爲犯罪行爲。行爲的認定與社會規範息息相關，尤其是歷經時空、環境等改變後，社會規範會受到相當程度的衝擊與改變。當法律有變更，代表個人所享有的法律保障亦有所變化，例如：電腦科技發展的初期，法律對於軟體的重製行爲並沒有清楚的規範，但是現今軟體的重製行爲已被法律明文限制。這種現象間接說明違法行爲的認定隨著社會環境的變化亦有調整。

「個人資料商業化的侵權行爲」、「不當洩漏他人資料的侵權行爲」是本文的研究範圍，上述侵權行爲均是法律明文規範的違法行爲，可以被認定爲犯罪行爲。然而，由於本研究著重於探討社會規範、態度等因素對資訊隱私侵害行爲意圖的影響，不擬直接定義上述活動爲犯罪行爲，因此以侵害行爲定義上述二種侵權行爲。因此，本研究對「資訊隱私侵害行爲」的定義是：

在沒有通知當事人或獲得當事人同意之前，以不當行為方式將他人的隱私資料應用在特定目的之行為。

三、計畫行爲理論(Theory of Planned Behavior, TPB)

計畫行爲理論主張個人對特定行爲的態度、主觀規範與行爲控制知覺等構念，會影響個人的行爲意圖，而且行爲意圖會影響行爲。多年來，TPB 理論已被廣泛應用在醫療、行銷、教育、心理、管理與資訊倫理等領域。TPB 理論的構念，分述如下：(1)對行爲的態度，係指個人對特定行爲的正面或負面之感覺。(2)主觀規範，係指個人從事某項特定行爲時所預期的社會壓力，這個社會壓力的主要來源是重要關係人（例：父母、師長等）與參考團體（例：朋友、同儕等）等。(3)行爲控制知覺，強調執行某特定行爲時，感受容易或困難的程度，例如：感受到有利的機會、資源（能力、技能等），個人對於該行爲的控制認知會越高，行爲的意圖會越強，行爲意圖與實際行爲的關係就越穩定；反之，則相反[11]。(4)行爲意圖，係指個人從事某特定行爲之意圖的強弱程度。(5)行爲，可以從個人對某特定行爲的意圖預測得知。如圖一所示，對行爲的態度、主觀規範、行爲控制知覺等三項變數影響行爲的意圖。



圖一　計畫行爲理論 [11]

由於多數行爲均存在某種程度的不確定性，Ajzen 因此提出「行爲控制知覺」構念，表達個人行爲受到自我控制（內在因素）與便利性（外在因素）的影響。Ajzen[10]認爲，「行爲控制知覺」與「自我效能」這兩項構念的組成要素相當接近；Bandura[13]認爲，自我效能涵蓋層面比 Ajzen 的行爲控制知覺更完整。Manstead and Eekelen[50]的實徵研究指出，「自我效能」變數可以用來作爲行爲控制知覺的替代變數。過去不少實徵研究[14, 52, 24, 6]證實自我效能構念可以更有效預測個人的行爲。透過上述的觀點與文獻，本研究擬以「資訊隱私自我效能」構念取代「行爲控制知覺」構念，探索影響資訊隱私侵害行爲意圖的因素。「資訊隱私自我效能」構念的定義，如下所示：

在特定情境下，資訊隱私自我效能是尊重、保護他人資訊隱私權之能力的信心判斷。

三、理性選擇理論(Rational choice theory)

根據犯罪學理論類別、意涵[67, 27]，犯罪學理論可分爲三類：(1)鉅觀理論，強調犯罪和社會結構之間的關係；(2)微觀理論，解釋人們爲什麼會變成犯罪者；(3)中介理論，整合鉅觀理論、微觀理論的觀點。犯罪學微觀理論的理性選擇理論經常被用來解釋人的犯罪行爲與動機，因此本研究擬以犯罪學微觀理論的理性選擇理論，探討影響資訊隱私侵害行爲意圖的因素。

犯罪學理論主張犯罪行爲是自由意志(Free-well)、理性(Rationality)選擇的結果。犯

罪行爲是理性的行爲抉擇，個體評估犯罪行爲帶來的利益大於成本，才會付諸行動。近年來，已經有不少文獻引用理性選擇理論探討電腦犯罪相關行爲，例：賽門鐵克公司的駭客入侵行爲意圖研究報告[33]、美國司法部的塑膠貨幣詐欺研究[54]、未來犯罪趨勢研究報告[12]與資訊安全與犯罪機會[68, 69]等，顯示理性選擇理論已逐漸被應用在電腦犯罪行爲的研究。

Clarke and Cornish[23]與 Cornish and Clarke[26]認爲，不同的犯罪類型會有不同的選擇，因此在分析犯罪行爲的抉擇時，應該根據犯罪事件特定性(Offence specific)與犯罪者的特定化(Offender specific)來進行。犯罪事件特定性，係指犯罪事件的建構，主旨在於說明每種犯罪型態都有其特定的報酬、風險與特殊技巧。其次，犯罪者的特定化，係指犯罪者不是隨機從事特定犯罪行爲，亦即犯罪者從事特定犯罪行爲之前，是經過仔細的考量，例如：成本、利益、動機、需求等，均是犯罪者考量的重點。“獲利越大、風險越少”是犯罪者決定犯罪的基本原則。

行爲是自由意志、理性選擇的結果，個人在進行任何一項活動之前，均會理性評估該行爲能替自己帶來何種利益，以及可能付出何種成本。Piliavin et al.[58]指出，犯罪的成本顯著影響犯罪行爲，該研究的成本有二項，一項是正式成本，係指被逮捕的風險、法律制裁的風險等；另一項是非正式成本，係指自我的制裁（行爲後的罪惡感、恥辱等）、家人與朋友的制裁（失去家人與朋友）、社會的制裁（未來合法工作機會的減少）等[38]。除了成本的評估，利益的評估也是潛在犯罪者的考量因素。利益的評估有二項，一項是外在利益，係指從侵害行爲獲得利益、報酬與資源[26]；另一項是內在利益，係指透過侵害行爲獲得刺激感、成就等滿足[35, 56]。綜觀上述，本研究擬以「利益的評估」與「成本的評估」構念探討個體的資訊隱私侵害行爲意圖是否受到利益與成本評估的影響。

參、研究設計

資訊隱私侵害行爲的研究，很難直接對受訪者衡量「行爲」，許多不當行爲的研究常以衡量「行爲意圖」作爲行爲的替代變數，本研究亦不例外。本研究的主旨反映當事人在有意識地情況下，系統化的應用已擁有的資訊，完全自我控制的決定是否從事資訊隱私侵害行爲，這種行爲意圖是經過理性的考量。至於行爲未經理性評估者，則不是本研究所欲解釋與分析的對象。本文的研究設計採用模型比較(Competing models)方式探討資訊隱私侵害行爲的影響因素，分析變數之間因果關係的變化情形，進以瞭解資訊隱私侵害行爲的意圖。

一、研究構念

Ajzen[9]認爲行爲控制知覺與行爲意圖之間的關係，取決於行爲或所處的情境，因爲行爲意圖轉換成行爲時，需考量到個人或所處環境可能造成的影響。根據計畫行爲理論、理性選擇理論，研究模型透過「對資訊隱私侵害行爲的態度」、「主觀規範」、「資訊隱私自我效能」、「利益的評估」與「成本的評估」等研究變數，探討這些變數如何影響資訊隱私侵害行爲的意圖，相關研究構念之定義請參考表二。

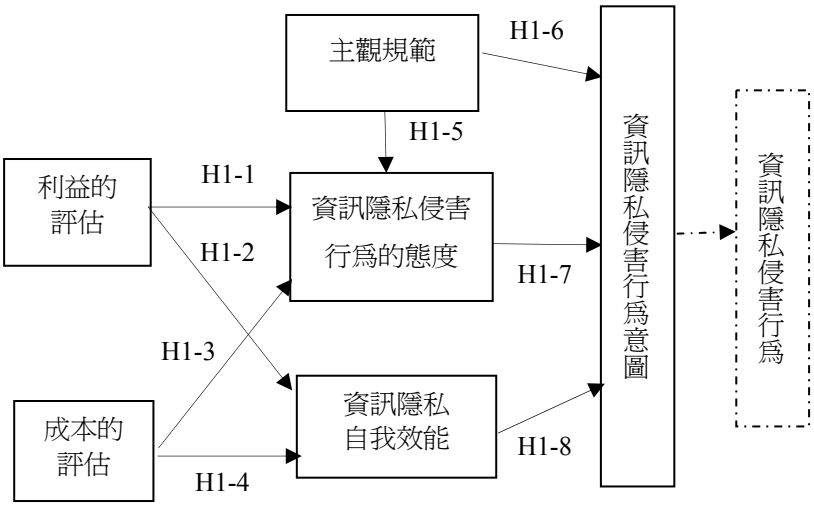
表二　影響資訊隱私侵害行爲意圖的構念定義

研究構念	定義
對資訊隱私侵害行爲的態度	對於資訊隱私侵害行爲的正面、負面的感覺。
主觀規範	從事資訊隱私侵害行爲時預期的社會壓力。
資訊隱私自我效能	尊重、保護他人資訊隱私權之能力的信心程度。
利益的評估	資訊隱私侵害行爲所能帶來內在利益與外在利益的滿意程度。
成本的評估	爲資訊隱私侵害行爲付出正式成本與非正式成本的嚴重程度。
資訊隱私侵害行爲意圖	欲從事資訊隱私侵害行爲之意圖的強弱程度。

二、研究模型

（一）研究模型一

行爲規範階段可分爲兩個階段：第一階段是從眾多習俗與規則之中，選擇適切的行爲規範；第二階段是思考爲什麼這些習俗或規則是好的、是對的。多數人以不違背上述二者方式來決定個人的行爲。然而，爲了欲求的結果，並不是所有人們都以最道德的思維方式決定個人行爲[44, 28]。研究模型一如圖二所示，「資訊隱私侵害行爲意圖」是依變數，「利益的評估」、「成本的評估」與「主觀規範」是自變數，「對資訊隱私侵害行爲的態度」、與「資訊隱私自我效能」爲該模型的中介變數，探索上述影響因素對資訊隱私侵害行爲的影響情形。



圖二　研究模型一

（二）研究假說：研究模型一

DeConick and Lewis[28]認爲人們爲了得到欲求結果，可能會以成本、利益分析來決定行爲，而非以最道德的方式來決定行爲。理性選擇理論認爲利益是犯罪行爲的重要指標之一[26]，例如：Peace et al.[57]之盜版軟體行爲的實徵研究結果證實，對盜版行爲的態度、主觀規範、行爲控制知覺構念均是盜版軟體的關鍵因素，個人對盜版行爲的態度，間接受到軟體價值的影響，而且軟體價值越高，對盜版行爲的態度就越正向。因此，本研究認爲在高利益的誘因下，侵害他人資訊隱私權的態度會趨強，說明利益的評估越高，對資訊隱私侵害行爲的態度會越正向、持肯定態度。因此推導假說如下：

假說 1-1：利益的評估越高，對資訊隱私侵害行爲的態度越正向。

Ajzen[11]認爲現實生活中，某些行爲並非可被意志控制，不少行爲都有相當程度的不穩定性。本研究認爲當資訊隱私侵害行爲的結果，被評估能帶來高利益，且所處的情境又提供行爲所需要（如金錢、時間、精力等）的資源，環境層面與行爲層面會影響個人對於尊重、保護他人資訊隱私權的信心程度。換言之，在高利益的誘因下，尊重、保護他人資訊隱私權的信心會轉弱，亦即利益的評估越高，資訊隱私自我效能會較弱。因此推導假說如下：

假說 1-2：利益的評估越高，資訊隱私自我效能越弱。

Kreie and Cronan[46]、Bommer et al. [18]與 Leonard et al. [47]等研究結果顯示，個人對行爲信念與行爲結果的評價會受到法律環境的影響。Peace et al.[57]研究指出，刑罰的嚴厲程度越高，個人對盜版軟體的態度就越負向。本研究認爲行爲經過理性的評估，正式成本（法律制裁、刑罰嚴重程度、被逮捕風險等）與非正式成本（自我制裁、社會制裁等）會影響當事人對資訊隱私侵害行爲的態度，例如：認爲將他人隱私資料商業化的行爲極具傷害性，而且司法單位與社會的制裁很嚴厲，會對資訊隱私侵害行爲持負向的態度。相反的，如果認爲將他人隱私資料進行商業化的行爲是沒有傷害性，而且司法單位與社會的制裁很寬鬆，會對資訊隱私侵害行爲持正向的態度。因此，在高成本的嚇阻下，侵害他人資訊隱私權的態度會趨弱。換言之，成本的評估越高，對資訊隱私侵害行爲的態度會越負向、持反對的態度。因此推導假說如下：

假說 1-3：成本的評估越高，個人對資訊隱私侵害行爲的態度越負向。

資訊隱私自我效能是個人尊重、保護他人資訊隱私權的信心程度，如果從事資訊隱私侵害行爲必須付出相當的成本（正式成本與非正式成本），在高成本的嚇阻作用下，個人爲了減少被法律制裁、或社會制裁的風險，因此尊重、保護他人資訊隱私權的信心會轉強。換言之，對資訊隱私侵害行爲的成本評估若越高，尊重他人資訊隱私權的信心程度會較強，因此推導假說如下：

假說 1-4：成本的評估越高，資訊隱私自我效能越強。

Shepherd and O’Keefe [61]、Shimp and Kavas[62]、Vallerand et al.[64]等研究指出，對特定行爲的主觀規範會影響其態度。Chang[20]的軟體盜版行爲與 Hsu and Kuo[42]的保護資訊隱私權研究指出，個人感受到的主觀規範會影響當事人對特定行爲的態度。就資訊隱私侵害行爲而言，如果重要關係人與參考團體不支持資訊隱私侵害行爲，資訊隱

私侵害行爲的主觀規範會比較強，個人因爲預期該行爲會遭受較大的社會壓力（主觀規範強），對資訊隱私侵害行爲持反對態度，因此推導假說如下：

假說 1-5：主觀規範越強，對資訊隱私侵害行爲的態度越負向。

軟體盜版行爲意圖[57, 20, 30]、網路入侵行爲意圖[33]與資訊倫理行爲意圖[16, 18, 48]等文獻，均以對行爲的態度構念預測資訊科技的不當行爲意圖。就資訊隱私侵害行爲而言，對資訊隱私侵害行爲的態度呈負向者，代表個人不接受資訊隱私侵害行爲，其價值觀認爲這種行爲具傷害性，對這種行爲的接受程度較低，其態度會影響個人的意圖，並將此意圖轉化爲不從事侵害他人資訊隱私權的行爲。根據上述的文獻與討論，顯示資訊隱私侵害行爲的態度會影響該行爲的意圖。因此推導假說如下：

假說 1-6：對資訊隱私侵害行爲的態度越負向，資訊隱私侵害行爲意圖越弱。

長久以來，主觀規範對於行爲意圖一直扮演相當重要的角色，例如：知識分享的行爲意圖[17]、網路商品購買意願[39]等。若以使用資訊科技的不當行爲而言，軟體盜版行爲意圖[57, 20, 30]、在網際網路上隱瞞個人資訊的行爲意圖[49]等均引用主觀規範預測個人的行爲意圖。就資訊隱私侵害行爲而言，主觀規範呈現負向，代表重要關係人與參考群體支持、不反對資訊隱私侵害行爲，當事人從事該行爲時所承受的社會壓力較小。根據上述的文獻與討論，顯示主觀規範會影響資訊隱私侵害行爲的意圖。因此推導假說如下：

假說 1-7：資訊隱私侵害行爲的主觀規範越強，資訊隱私侵害行爲意圖越弱。

Hill et al.[40]與 Wood and Bandura[70]研究證實，自我效能會影響個人執行某特定行爲的意圖。許孟祥等[6]實徵研究指出，資訊隱私倫理效能反應個人對於保護他人資訊隱私的自信心。本研究認爲，每個人的能力、可享用資源與機會均不相同，對於特定行爲帶來的利益收獲與成本支出均有不同的評估。就資訊隱私侵害行爲而言，資訊隱私自我效能越強者，較有信心控制自我的行爲，保護他人資訊隱私權的行爲意圖會較強。根據上述的文獻與討論，顯示資訊隱私自我效能會影響資訊隱私侵害行爲的意圖。因此推導假說如下：

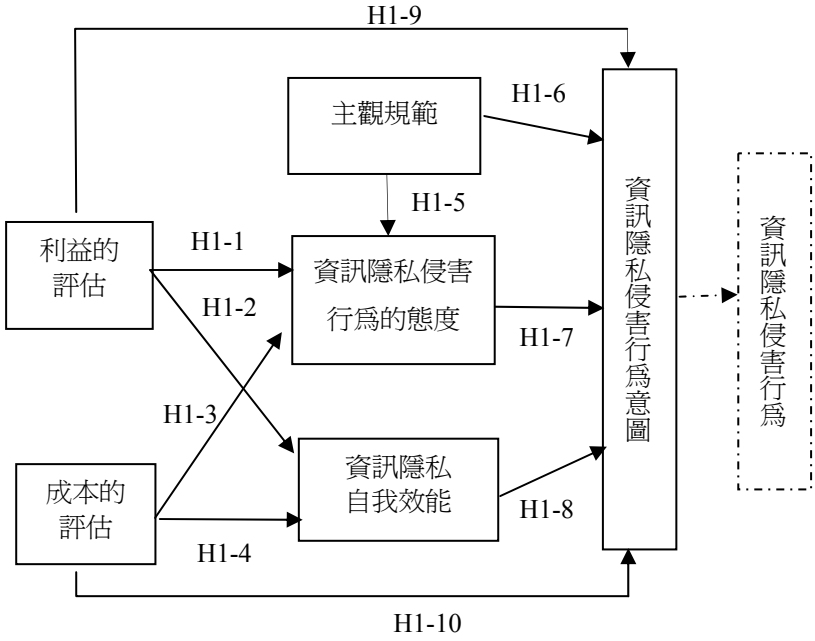
假說 1-8：資訊隱私自我效能越強，資訊隱私侵害行爲意圖越弱。

（三）研究模型二

模型二與模型一的最大差異是「利益的評估」與「成本的評估」對「資訊隱私侵害行爲意圖」有直接的影響作用，亦即模型二比模型一多出二個研究假說，分別是假說 2-9 與假說 2-10。本研究希望透過實徵資料驗證這二項假說，試圖瞭解「利益的評估」與「成本的評估」是否直接影響資訊隱私侵害行爲的意圖。

Hunt and Vitell[43]認爲道德問題的評估可以分爲道義論(Deontological evaluation)和目的論(Teleological evaluation)的角度來看待道德行爲。若以道義論觀點探討行爲，道義論較著重人們是否有欺騙、撒謊、不公平等負面的行爲舉止；若以目的論觀點探討行爲，目的論較著重成本利益分析(Cost/benefit analysis)，以成本利益分析道德上的行爲[28]。Hunt and Vitell[43]認爲，爲了得到想要的結果，人們不一定採取最道德的方案執行其行爲，例如：人們較常以目的論評估行爲，而非以道義論來評估行爲[44, 28]。對資訊隱私

侵害行爲而言，人們是不是也以成本利益分析方式來評估行爲，值得進一步瞭解與探討。



圖三　研究模型二

（四）研究假說：研究模型二

理性選擇理論認爲利益、機會與風險的多寡是犯罪行爲的重要指標，因此本研究認爲「利益的評估」是當事人衡量資訊隱私侵害行爲結果的利害得失指標之一。利益是影響侵害行爲意圖的重要因素[53, 55, 57]。利益的評估包括帶來金錢、報酬的外在利益，以及帶來成就感、滿足感的內在利益。Hunt and Vasquez-Parraga[44]研究指出，如果不當行爲產生的正面結果（獲得利益、好處等）大於負面結果（欺騙、傷害等），人們會降低對此行爲不道德的看法。就資訊隱私侵害行爲而言，人們在從事該侵害行爲之前會經過理性的考量，並評估該行爲能爲自己帶來多少利益。如果能帶來高利益，可能會降低對該侵害行爲不道德的看法，甚至將該行爲合理化，而產生較強的行爲意圖。根據上述的文獻與討論，顯示利益的評估會直接影響資訊隱私侵害行爲的意圖。因此推導假說如下：

假說 2-9：利益的評估越高，資訊隱私侵害行爲的意圖越強。

Gottfredson and Hirschi[36]認爲，當情境有利於犯罪時，犯罪行爲自然就會發生。「成本的評估」也是當事人衡量資訊隱私侵害行爲結果的利害得失指標之一。Bommer, et al.[18]與 Kreie and Cronan[46]認爲法規環境會影響個人的倫理決策；Christensen and Eining[21]指出刑罰可以抑制軟體盜版行爲。成本的評估包括帶來被逮捕、被法律制裁的正式成本，以及自我制裁、親朋制裁或社會制裁的非正式成本。就資訊隱私侵害行爲而言，人們在從事該侵害行爲之前會經過理性的考量，並評估要爲該行爲承擔多少正式成本（法律制裁等）與非正式成本（社會制裁等）。評估之後，如果必須爲資訊隱私侵害行爲付出較高的成本，會對該行爲的意圖產生嚇阻效果，資訊隱私侵害行爲的意圖會轉弱。根據上述的文獻與討論，顯示成本的評估會直接影響資訊隱私侵害行爲的意圖。

因此推導假說如下：

假說 2-10：成本的評估越高，資訊隱私侵害行爲的意圖越弱。

根據上述相關文獻推論出研究模型一與研究模型二，所有的研究假說整理如表三所示。

表三　模型一與模型二的研究假說

模型一	模型二	研究假說
H1-1	H2-1	利益的評估越高，個人對資訊隱私侵害行爲的態度越正向。
H1-2	H2-2	利益的評估越高，資訊隱私自我效能越弱。
H1-3	H2-3	成本的評估越高，個人對資訊隱私侵害行爲的態度越負向。
H1-4	H2-4	成本的評估越高，資訊隱私自我效能越強。
H1-5	H2-5	主觀規範越強，對資訊隱私侵害行爲的態度越負向。
H1-6	H2-6	對資訊隱私侵害行爲的態度越負向，資訊隱私侵害行爲意圖越弱。
H1-7	H2-7	資訊隱私侵害行爲的主觀規範越強，資訊隱私侵害行爲意圖越弱。
H1-8	H2-8	資訊隱私自我效能越強，資訊隱私侵害行爲意圖越弱。
	H2-9	利益的評估越高，資訊隱私侵害行爲的意圖越強。
	H2-10	成本的評估越高，資訊隱私侵害行爲的意圖越弱。

三、變數衡量

研究模型有五項研究變數，變數的衡量指標及問卷問項之設計過程，均根據理論基礎及相關文獻作爲研究設計的基礎（參表四）。研究設計主軸是讓受訪者先閱讀單一情境劇本（個人資料的商業化、不當洩漏他人資料），隨即請受訪者回答情境故事的問項，以瞭解個人在特定情境下，何種因素影響資訊隱私侵害行爲的意圖。相關之研究變數的衡量，說明如下：

1. 對資訊隱私侵害行爲的態度：IT 倫理行爲意圖研究[47, 20]對態度的操作化定義，是徵詢受訪者對特定行爲的感受，例如：正面的感受（可接受、合理、沒有傷害性等）、負面的感受（不接受、不合理、傷害性等）二個信念。本研究依據此測量工具衡量個人的態度，包括：個人認爲資訊隱私侵害行爲是無傷害性、可以被接受、正當且合理等態度。透過 Likert 七點尺度，若答題分數越高表示受訪者接受資訊隱私侵害行爲；反之，則相反。
2. 主觀規範：依據測量工具衡量個人的主觀規範，包括：我的家人會贊成、我的師長會支持、我的朋友不會反對資訊隱私侵害行爲。透過 Likert 七點尺度，若答題分數越高表示受訪者認爲重要關係人支持資訊隱私侵害行爲；反之，則相反。
3. 資訊隱私自我效能：許孟祥等[6]針對資訊隱私發展倫理效能量表，以不看、不取得、不分享與不圖利四個構面衡量資訊隱私自我效能。本研究根據欲研究的情境劇本適當修改該量表的問項，並將這十題測量題項按四個構面計算平均值，用來評估特定情境下受訪者的資訊隱私自我效能。問項以 Likert 七點尺度，若答題分數越高表示受訪者比較有信心控制自我的行爲，較尊重他人的資訊隱私權；反之，則相反。

4. 利益的評估：利益評估的構面，外在利益的問項，包括可能獲得的好處、機會與報酬等問項[26]；內在利益的問項，包括獲得刺激的快感、成就感、朋友的尊重等問項[36, 56]。根據六題測量題項，按內在利益與外在利益構面計算其平均值，用來測量特定情境下受訪者對資訊隱私侵害行爲可能帶來利益的評估。透過 Likert 七點尺度，若答題分數越高表示受訪者認爲資訊隱私侵害行爲可以爲自己帶來報酬與成就感；反之，則相反。
5. 成本的評估：成本評估的構面，正式成本，包括受害人的報案、司法單位的執法、法律制裁等問項；非正式成本，包括影響未來的前途、罪惡感與失去家人、朋友等問項[38]。根據七題測量題項，按正式成本與非正式成本構面計算其平均值，用來測量特定情境下受訪者對資訊隱私侵害行爲可能付出成本的評估。透過 Likert 七點尺度，若答題分數越高，表示受訪者認爲資訊隱私侵害行爲並不會被法律、社會制裁等；反之，則相反。
6. 資訊隱私侵害行爲意圖：行爲意圖是行爲的重要指標[31]，代表個人欲從事資訊隱私侵害行爲意願的強弱程度。透過 Likert 七點尺度，若答題分數越高，表示受訪者之資訊隱私侵害行爲意圖越強；反之，則相反。

表四　研究變數、衡量構面及問卷設計對照表

研究變數	構面	量表來源
對資訊隱私侵害行爲的態度	沒有傷害性	[47, 20]
	可以被接受	
	正當且合理	
主觀規範	我的家人會贊成	[9]
	我的師長會支持	
	我的朋友不會反對	
成本的評估	正式成本	[38] 本研究
	非正式成本	
利益的評估	內在利益	[26, 35, 56] 本研究
	外在利益	
資訊隱私自我效能	不看	[6]
	不取得	
	不分享	
	不圖利	
資訊隱私侵害行爲意圖	意圖之強弱程度	[31]

四、問卷調查與資料分析步驟

Bachman et al.[15]與 Reidenbach and Robin[59]認爲多數人對問卷的敏感問項(Dirty

questions)不願表達個人真實的想法，這種現象容易造成研究誤差。如果改採情境故事(Scenario-based vignettes)方式讓受訪者投射在情境故事的情況下回答問項，可以減緩受訪者刻意配合或迴避問項的困擾。因此，許多涉及道德、倫理行為意圖等研究，經常採用或改編情境故事的方式進行實徵研究[47, 41, 37, 32]。因此，本研究的情境劇本參考Dejoie et al.[29]情境兩難故事，將欲探討之個人資料的商業化、不當洩漏他人資料等侵權行為編撰為二個情境故事。

同一受訪者如果填答兩個情境故事的問項，可能造成副作用(Side-effect)，因此本研究所有受訪者只回答一個情境故事的問項。研究對象在北、中、南三區各選一至二所學校作為研究取樣的主要來源。為了方便日後對研究樣本進行無差異性分析，因此採用便利抽樣，以合作意願較高的學校老師為主要樣本學校，此亦為本研究的限制之一。

本研究資料分析包含下列步驟：首先，進行樣本背景資料的敘述性統計分析，信度檢定採 Cronbach's α 計算。接著，以探索性因素分析法作為建構效度的衡量；以相關分析法作為研究變數之間區別效度的衡量。在完成信度、效度的檢測後，採 LISREL 統計軟體的結構模式分析法（SEM）檢定研究構念對「資訊隱私侵害行為意圖」的影響。

肆、資料分析

一、樣本分析

本研究實際發出 800 份問卷，實際回收 762 份，扣除答題不全等廢卷外，有效回收 632 份，有效樣本之回收率達 83%。回收問卷的樣本特性如表五所示。為確保回收問卷的樣本具母體代表性，本研究以學生個人資料比較不同情境回收的樣本是否具顯著差異。變異數同質性檢定（Test of homogeneity of variances）的結果顯示，不同情境的樣本資料在研究構念上符合同質性要求，代表回收的樣本資料具有一定程度的母體代表性。

表五　研究樣本回收一覽表（樣本數：632）

樣本特徵	類別	個人資料的商業化	不當洩漏他人資料
性別	男	41.5%	39.5%
	女	58.2%	60.5%
職業	學生	83.9%	83.2%
	在職學生	16.1%	16.8%
年齡	20 歲以下	31.9%	49.5%
	21-25 歲	57.6%	43.6%
	26-30 歲	8.2%	6.2%
	31-35 歲	1.2%	0.0%
	36-40 歲	0.3%	0.3%
	40 歲以上	0.6%	0.3%
教育程度	專科	5.0%	12.7%
	大學	90.4%	82.1%
	研究所	4.7%	5.2%
樣本數量		341	291

二、研究量表的檢測

進行假說驗證與分析構念間的關係之前，必須確認研究構念的測量題項和測量尺度具備良好的建構效度及信度。Sethi and Carraher[60]指出，不當的量表設計，即使資料分析結果顯示各構念間具有相當程度的共變性，這種研究結果的正確性亦是令人質疑。因此，本研究以收斂效度、構念效度與信度檢測量表的品質，確保測量工具有相當程度的效度和信度。

表六　研究變數的相關係數、探索性因素分析與 Cronbach's α 值

變數		ATT	SN	SE	BHB	PL	INT	特徵值	解釋變異量%	Cronbach's α
對資訊隱私侵害行爲態度	ATT	1						2.324	77.478	0.841
主觀規範	SN	0.322**	1					2.157	71.911	0.780
資訊隱私自我效能	SE	-0.076	-0.192**	1				7.674	62.570	0.901
利益的評估	BHB	0.177**	0.399**	-0.238**	1			4.427	68.665	0.826
成本的評估	PL	0.195**	0.417**	-0.174**	0.451**	1		4.052	63.702	0.790
資訊隱私侵害行爲意圖	INT	0.497**	0.226**	-0.173**	0.154**	0.177**	1	4.626	77.098	0.910

**表示相關係數在0.01水準下，雙尾檢定爲顯著

本研究採用探索性因素分析法(Exploratory factor analysis)，針對每一變數，逐一檢測所使用之量表的測量題項是否擁有單構面尺度的良好品質。經探索性因素分析，表六顯示每個測量題項的因素負荷量均大於 0.5，而且每一變數均能收斂爲同一因素構面，表示本研究所使用的測量題項擁有單構面尺度的良好品質。

表六顯示，各變數間的相關係數均達顯著水準 $p< 0.01$。本研究變數之間的相關係數均不爲 0，顯示變數之間的確存在某種實質上的關係，代表研究量表具有相當程度的判別效度。另外，表六 Cronbach's α 顯示，各變數的信度均大於 0.7，均具有可接受的信度水準，顯示研究量表具有良好的信度。

三、競爭模型與假說檢定

根據假說一、假說二研究模型的契合度指標、疊代次數與期望交叉效度等指標，選出最佳研究模型後，逐一檢定最佳研究模型變數之間的關係

（一）競爭模型

競爭模型的選擇可以從 LISREL 的參數估計結果與模型契合度指標進行研究模型的判斷與分析。邱皓政[4]指出，採用 LISREL 的 ML 法（最大概似法）時，疊代(Iterations)次數較多時，代表資料不易聚合，研究模型與實際資料間有相當大的差距。Browne and Cudeck[19]對於競爭模型也提出一項指標，該指標是期望交叉效度指標(Expected cross-validation index; ECVI)，這項指標可以用來作爲診斷模型的複核效化(Cross-validation)的指標，ECVI 越小，代表該模型契合度的波動性越小，即代表該模型

較佳；ECVI 越大，代表該模型契合度的波動性越大，代表該模型較不理想。本研究依循上述的參數估計結果與模型契合度指標，判斷研究模型一與研究模型二，選擇最佳的研究模型之後，再檢定該模型的假說。

（二）研究假說的實質關係

根據總體樣本的資料，以 LISREL 統計軟體結構模型分析法(SEM)的模型契合度指標、EVCI 指標值與疊代次數等檢定研究模型一與模型二，選出最佳模型後，再進行研究假說之實質關係的檢定。

1. 研究模型一

表七研究模型一之檢定結果顯示，卡方自由度比（χ^2/df）是 3.688，p 值是 0.000，非集中化參數估計值 NCP 是 75.264，平均概似平方誤根係數 RMSEA 是 0.065，小於 0.08 判斷值。另外，GFI、AGFI、NFI、NNFI、CFI 等契合度指標皆大於 0.90，而疊代次數是 10 次，顯示模型一具有理想契合度。Kettinger and Lee[45]曾建議卡方自由度比小於 5 是可接受的範圍，Browne and Cudeck[19]與 Marsh[51]曾指出，大型樣本量的卡方值不太適合做爲模型契合度指標。因此，檢定模型時應參考其他的契合度判斷指標，如果契合度指標能達到顯著水準，即表示研究模型具有理想的契合度。

表七 模型一與模型二之比較 （樣本數：632）

契合度指標	契合度判斷值	模型一	模型二	假說內容	模型一路徑係數
χ^2		103.26	99.622	利益→態度	0.09 (1.38)
df		28	26	利益→效能	-0.36** (-3.85)
χ^2/df	<5	3.688	3.831	成本→態度	0.17** (2.71)
NCP		75.264	73.622	成本→效能	0.00 (-0.05)
GFI	>0.90	0.968	0.969	主觀→態度	0.54** (9.28)
AGFI	>0.90	0.938	0.935	態度→意圖	0.44** (8.33)
NFI	>0.90	0.948	0.972	主觀→意圖	0.09 (1.91)
NNFI	>0.90	0.970	0.963	效能→意圖	-0.21** (-4.95)
CFI	>0.90	0.981	0.979	解釋力(R^2)	33%
RMSEA	<0.08	0.065	0.067	註：括弧內是 t value	
疊代次數	較少者爲佳	10	17		

2. 研究模型二

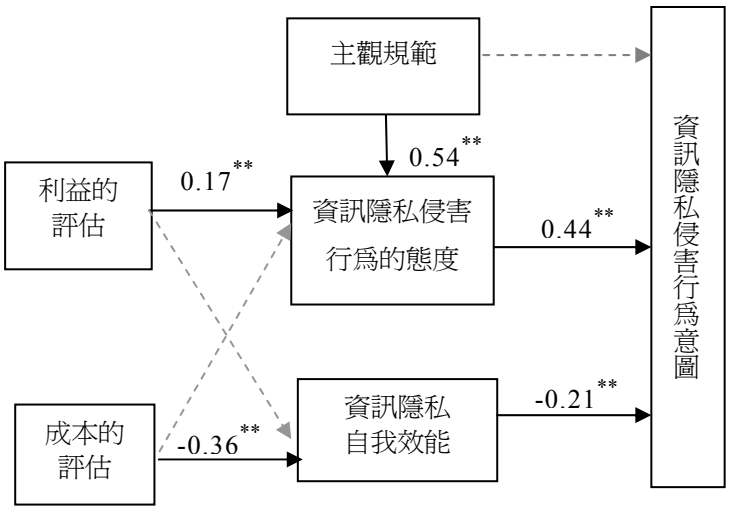
研究模型二的利益評估與成本評估變數不僅直接影響資訊隱私侵害行爲態度與資訊隱私自我效能，同時也直接影響資訊隱私侵害行爲的意圖。表七研究模型二之檢定結果顯示，卡方自由度比（χ^2/df）是 3.831，p 值是 0.000，非集中化參數估計值 NCP 是 73.622，平均概似平方誤根係數 RMSEA 是 0.067，小於 0.08 判斷值。另外，GFI、AGFI、NFI、NNFI、CFI 等契合度指標皆大於 0.90，而疊代次數是 17 次，顯示模型二亦具有理

想契合度。

3. 模型一與模型二的比較

表七顯示，模型一卡方自由度比（χ^2/df）是 3.688，比模型二的 3.381 小，模型一優於模型二。接著，進行契合度指標的判斷，NCP 與 RMSEA 的判斷值越小越好，模型一與模型二各有一次較佳判斷值的表現。GFI、AGFI、NFI、NNFI、CFI 等契合度指標應大於 0.90，在上述的比值當中模型一比模型二多出一次較佳判斷值，在這部份模型一優於模型二。另外，在疊代次數上，模型一的次數較少，又再一次有優於模型二的表現。根據 ECVI 指標，再檢視模型一與模型二在 ECVI 指標的表現，檢視結果發現兩個模型的 ECVI 指標均是 2.074。換言之，這兩個模型契合度的波動情形相似，沒有顯著的差異。

由於模型一卡方自由度比值較低、疊代次數較少、契合度指標值表現較佳等，模型一與模型二的競爭結果，證實模型一是契合度較佳的研究模型。因此，進行模型一的假說檢定，至於模型二的假說則不會進行實質關係的檢定。



圖四　資訊隱私侵害行爲意圖模型的變數間關係

四、假說一的檢定

研究模型一共計有八個假說，圖四與表八顯示檢定結果有五項假說達到顯著水準（t 值 > 1.96），該模型的五項變數對於資訊隱私侵害行爲意圖的累積解釋力爲 33%。如表八所示，假說 1-5 的路徑係數(0.54)最大，顯見主觀規範對資訊隱私侵害行爲態度的影響效果最大，其次依序是態度對意圖(0.44)、利益對資訊隱私自我效能(-0.36)、資訊隱私自我效能對意圖(-0.21)、成本評估對態度(0.17)。

表八的假說檢定結果顯示，假說 1-2 獲得支持，如果利益的評估越高，個人尊重他人資訊隱私權的信心程度越低。假說 1-3 獲得支持，如果成本評估越高，代表個人評估司法、社會等對侵權行爲的制裁是較寬鬆，對該侵害行爲的態度會比較支持、不反對。假說 1-5 獲得支持，如果主觀規範越高，代表重要關係人與次要參考團體越不接受資訊

隱私侵害行為，個人會比較不接受資訊隱私侵害行為。假說 1-6 獲得支持，對資訊隱私侵害行為的態度越正向，從事該侵害行為的意圖越強。假說 1-8 獲得支持，資訊隱私自我效能越正向，代表尊重他人資訊隱私權的信心越強，從事資訊隱私侵害行為的意圖會較弱。

表八　假說一的檢定結果

	假說內容	檢定結果
H1-1	利益的評估越高，個人對資訊隱私侵害行為的態度越正向。	不顯著
H1-2	**利益的評估越高，資訊隱私自我效能越弱。**	**顯著**
H1-3	**成本的評估越高，個人對資訊隱私侵害行為的態度越負向。**	**顯著**
H1-4	成本的評估越高，資訊隱私自我效能越強。	不顯著
H1-5	**主觀規範越強，對資訊隱私侵害行為的態度越負向。**	**顯著**
H1-6	**對資訊隱私侵害行為的態度越負向，資訊隱私侵害行為意圖越弱。**	**顯著**
H1-7	資訊隱私侵害行為的主觀規範越強，資訊隱私侵害行為意圖越弱。	不顯著
H1-8	**資訊隱私自我效能越強，資訊隱私侵害行為意圖越弱。**	**顯著**

伍、討論

研究模型的結構化分析結果顯示，資訊隱私侵害行為意圖之模型一與模型二的競爭結果，模型一比模型二略勝一疇。模型實質關係中，【成本評估→資訊隱私侵害行為態度】與【利益評估→資訊隱私自我效能】均達顯著水準。研究結果說明，如果認為資訊隱私權的侵權行為結果，所招致的懲罰、制裁是寬鬆，當事人支持、不反對資訊隱私侵害行為的態度會較強。另外，在利益評估方面，如果認為資訊隱私權的侵權行為結果，能為個人帶來相當的報酬與利得等誘惑，當事人尊重、保護他人資訊隱私權的信心會降低。換言之，本研究的假說 1-2「利益的評估越高，資訊隱私自我效能越弱」與假說 1-3「成本的評估越高，個人對資訊隱私侵害行為的態度越負向」，皆獲得實徵上的支持。

根據統計結果，【主觀規範→態度】的路徑係數大於【態度→行為意圖】，代表主觀規範對個人之態度有相當重要的影響效果，這種情形亦說明主觀規範對於該侵害行為意圖具有間接的影響效果。主觀規範雖然沒有直接影響資訊隱私侵害行為的意圖，但是卻會間接的影響該侵害行為的意圖，因為重要關係人或次要參考團體不反對資訊隱私侵害行為，這種支持資訊隱私侵害行為的意見會直接影響當事人的態度；支持侵害行為的態度進而產生從事資訊隱私侵害行為的意圖。這種檢定結果說明，重要關係人與次要參考團體的意見與態度，會直接、正向影響到當事人對資訊隱私侵害行為的態度。以上的分析說明假說 1-5「主觀規範越正向，對資訊隱私侵害行為的態度越負向」獲得實徵的支持。

【資訊隱私自我效能→行為意圖】亦達到顯著水準。由於資訊隱私自我效能是尊重他人資訊隱私權的信心程度，如果該信心程度越低，對於資訊隱私侵害行為的意圖會越強。換言之，資訊隱私自我效能越強，該侵害行為意圖越弱。以上的分析說明假說 1-8

「資訊隱私自我效能越強，資訊隱私侵害行爲意圖越弱」獲得實徵的支持。

陸、結論

透過實徵資料檢驗假說，研究結果證實資訊隱私侵害行爲的態度會受到利益評估、主觀規範的影響，而且主觀規範的影響效果超越利益評估。這代表個體身邊的重要關係人、次要參考團體的價值、期待等，能顯著地影響個體對資訊隱私侵害行爲的態度。這項研究結果顯示，尊重他人資訊隱私權的觀念要擴及全民，因爲如果多數的社會成員均能尊重他人的資訊隱私權，我們每一個人都可以影響我們身邊的親朋好友，擴大主觀規範的影響力，引導個體有尊重、保護他人的資訊隱私權的態度。另外，研究結果亦證實，成本評估會影響個體對保護他人資訊隱私權的信心程度，本研究認爲如果司法單位嚴格制裁侵犯他人資訊隱私權的行爲，可以強化個體的資訊隱私自我效能，提升個體尊重他人資訊隱私權的能力。雖然資訊隱私侵害行爲的意圖受到態度、自我效能的直接影響；然而，主觀規範、利益評估與成本評估卻間接影響到個體的態度與自我效能，實不容小覷。

人類是社會動物，社會環境提供指導人類行爲的文化價值和定義，人類的行爲就是社會環境的產物。爲進一步改善資訊社會環境，本研究對政府單位、資訊教育、企業與個人等提出下列三項建議：(1)政府機構，持續修訂電腦犯罪之相關法律，司法機關應多加強刑事科學的電腦犯罪鑑識能力與數位証據的取得，抑制侵權行爲等活動，減少資訊犯罪對社會造成的傷害。(2)資訊教育，法律較著重於事後之懲罰或補救，若能從教育著手，做事前的防範，對資訊社會秩序的維護具積極性的意義。倫理是行爲的指導準則；資訊化社會須要資訊倫理規範個人使用資訊的行爲。資訊倫理教育的提供，不應侷限於校園內的資訊倫理教學，甚至應擴大至整個資訊社會的每一成員。誠如研究結果所示，父母、師長與同儕等重要關係人的期許，會影響個人對資訊隱私侵害行爲的態度。若能透過資訊倫理教育教導社會成員尊重他人的資訊隱私權，對資訊社會秩序的維護應具有積極性意義。(3)企業與個人，所有使用電腦的個人、企業應有尊重、保護他人資訊隱私權的共識，爲資訊社會的秩序盡一份棉薄心力。

資訊社會的匿名性、流動性正在改變人際、家庭、社會的結構，這些結構的變遷正在重新改寫社會活動。因此，我們期許未來能有更多學者透過科際整合方式，對資訊社會所衍生的不當行爲進行更深入的研究。

參考文獻

[1] 朱柏松，“隱私權概念之衍變及其損害防止立法之動向”，*法學叢刊*，34 卷 2 期，1989：頁 89-102。

[2] 自由電子新聞網，“轉寄郵件遭開除 聯電寒蟬效起”，*自由電子新聞網*，2001/7/7, http://www.libertytimes.com.tw/2001/new/jul/7/today-e5.htm

[3] 林雅惠，“資訊隱私權之重塑－以行動商務爲例”，*科技法律評論*，一卷一期，2004：頁 93-122。

[4] 邱皓政，結構方程模式：LISREL 的理論、技術與應用，台北：雙葉書廊，2003。

[5] 邱惠雯，網際網路使用行爲之限制─從隱私權保護觀之探討，國立中正大學犯罪防治研究

所碩士論文，2002。

[6] 許孟祥、郭峰淵、林杏子、朱彩馨、游佳萍，“個人資訊隱私：倫理效能之量表的發展與驗證”，*中山管理評論*，九卷三期，2001：頁 373-394。

[7] 簡榮宗，網路上資訊隱私權保護問題之研究，東吳大學法律研究所碩士論文，1998。

[8] Agranoff, M.H., “Controlling the Threat to Personal Privacy: Corporate Policies Must Be Created,” *Journal of Information Systems Management*, (8), 1991: pp. 48-52.

[9] Ajzen, I., “The Theory of Planned Behavior,” *Organizational Behavior and Human Decision Process*, (50), 1991: pp. 179-211.

[10] Ajzen, I., “Attitude Structure and Behavior,” in *Attitude Structure and Function*, A.R. Pratkanis, S.J. Breckler, and A.G. Greenwald (Ed.), NJ: Lawrence Erlbaum Associates, 1989.

[11] Ajzen, I., “From Intentions to Actions: A Theory of Planned Behavior,” in *Action-Control: from Cognition to Behavior*, Heidelberg: Springer, 1985.

[12] Association of British Insurers, “Future Crime Trends in the United Kingdom,” *General Insurance Research Report No.7*, <http://www.abl.org.uk>, 2000.(Accessed April 10, 2005).

[13] Bandura, A., *Self-Efficacy: the Exercise of Control*, NY: W. H. Freeman, 1997.

[14] Bandura, A. and Jourden, F.G., “Self-Regulatory Mechanisms Governing the Impact of Social Comparison on Complex Decision Making,” *Journal of Personality and Social Psychology*, (60:6), 1991: pp. 941-951.

[15] Bachman, R., Paternoster, R. and Ward, S., “The Rationality of Sexual Offending: Testing A Deterrence/Rational Choice Conception of Sexual Assault,” *Law and Society Review*, (26), 1982: pp. 343-372.

[16] Banerjee, D., T.P. Cronan, and T.W. Jones, “Modeling IT Ethics: A Study Of Situational Ethics,” *MIS Quarterly*, (22:1), 1998: pp. 31-60.

[17] Bock, G.W., R.W. Zmud, Y.G. Kim, and J.N. Lee, “Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate,” *MIS Quarterly*, (29:1), 2005: pp. 87-111.

[18] Bommer, M., C. Gratto, J. Gravander, and M. Tuttle, “A Behavioral Model of Ethical and Unethical Decision Making,” *Journal of Business Ethics*, (6:4), 1987: pp. 265-281.

[19] Browne, M. W. and Cudeck, R., “Alternative Ways of Assessing Model Fit,” in *Testing Structural Equation Models*, Kenneth Bollen and J. Scott Long, (Eds.), Sage Publications, Newbury Park, CA, 1993: pp. 136-192.

[20] Chang, M.K., “Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior,” *Journal of Business Ethics*, (7:16), 1998: pp. 1825-1834.

[21] Christensen, A. and Eining, M., “Factors Influencing Software Piracy: Implications for Accountants,” *Journal of Information Systems*, (5:1), 1991: pp. 67-80.

[22] Clarke, R., “International Privacy Concerns Confirm the Case for Intervention,” *Communications of the ACM*, (42), 1999: pp. 60-67.

[23] Clarke, R. and Cornish, D., “Rational Choice,” in R. Paternoster and R. Bachman (Ed), *Explaining Crime and Criminals: Essays in Contemporary Criminological Theory*, LA: Roxbury

Publishing Company, 2000.

[24] Compeau, D.R. and Higgins, C.A., "Computer Self-Efficacy: Development of A Measure and Initial Test," *MIS Quarterly*, (19:2), 1995: pp. 189-211.

[25] Cornish, D.B. and Clarke, R.V., *The Reasoning Criminal: Rational Choice Perspectives on Offending*, NY: Springer-Verlag, 1986.

[26] Cornish, D. and Clarke. R., "Understanding Crime Displacement: An application of Rational Choice Theory," *Criminology*, (25), 1987: pp. 933-947.

[27] Cullen, F.T. and Agnew, R., *Criminological Theory: Past to Present*, 2nd(Ed), LA: Roxbury Publishing Company, 2002.

[28] DeConick, J.B. and Lewis, W.F., "The Influence of Deontological and Teleological Considerations and Ethical Climate on Sales Managers' Intentions to Reward or Punish Sales Force Behavior," *Journal of Business Ethical*, (16), 1997: pp. 497-506.

[29] Dejoie, R., G. Fowler, and D. Paradice, *Ethical Issues in Information Systems*, MA: Boyd and Fraser publishing company, 1991.

[30] Eining, M.M. and Christensen, A.L. "A Psycho-Social Model of Software Piracy: The Development and Test of A Model," in: R. Dejoie, G. Fowler, D. Paradice (Eds.), *Ethical Issues in Information Systems*, MA: Boyd and Fraser, 1991.

[31] Fishbein, M. and Ajzen, I., *Beliefs, Attitude, Intentions and Behavior: An Introduction to theory and Research*, MA: Addition-Wesley, 1975.

[32] Gattiker, U. E. and Kelley, H., "Morality and Computers: Attitudes and Differences in Moral Judgments," *Information Systems Research*, (10:3), 1999: pp. 233-254.

[33] Gordon, S. and Ma, Q., "Convergence of Virus Writers and Hackers: Fact or Fantasy?" *Symantec Security Response*, http://www.symantec.com, 2003. (Accessed March 28, 2005).

[34] Gormley, K., One Hundred Years of Privacy, *Wisconsin Law Review*, 1992: pp. 1335-1408.

[35] Gottfredson, M.R. and Hirschi, T, *A general theory of crime*, CA: Stanford University Press, 1990.

[36] Gottfredson, M.R. and Hirschi, T., *A general theory of crime*, CA: Stanford University Press, 1990.

[37] Gowthorpe, C., J. Blake, and J. D., "Testing the Bases of Ethical Decision-Making: A Study of the New Zealand Auditing Profession," *Business Ethics: A European Review*, (11:2), 2002: pp. 143-156.

[38] Grasmick, H.G. and Bursik, R.J., "Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model," *Law and Society Review*, (24), 1990: pp. 835-861.

[39] Hansen, T., J.M. Jensen, and H.S. Solgaard, "Predicting Online Grocery Buying Intention: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior," *International Journal of Information Management*, (24:6), 2004: pp. 539-550.

[40] Hill, T., N.D. Smith, and M.F. Mann, "Role of Efficacy Expectations in Predicting the Decision to Use Advanced Technologies: The Case of Computers," *Journal of Management*, (16), 1987: pp. 337-313.

[41] Hsu, M.H. and Kuo, F.Y., "An Investigation of Volitional Control in Information Ethics," *Behavior and Information Technology*, (22:1), 2003: pp. 53-63.

[42] Hsu, M.H. and Kuo, F.Y., "The Effect of Organization-Based Self-Esteem and Deindividuation on Protecting Personal Information Privacy," *Journal of Business Ethics*, (42:4), 2003: pp. 305-321.

[43] Hunt, S. D. and Vitell, S. J., "A General Theory of Marketing Ethics," *Journal of Macromarketing*, (6:1), 1986: pp. 5-16.

[44] Hunt, S.D. and Vasquez-Parraga, A.Z., "Organization Consequences, Marketing Ethics, and Sales Forces Supervision," *Journal of Marketing Research*, (30), 1993: pp. 78-90.

[45] Kettinger, W.J. and Lee C.C., "Perceived Service Quality and User Satisfaction with the Information Services Function", *Decision Sciences*, (25:5/6), 1994: pp. 737-765.

[46] Kreie, J. and Cronan, T.P., "Judging What Is Ethical or Unethical: There Are Differences Between Men and Women," *Communications of the ACM*, (41:9), 1998: pp. 70-76.

[47] Leonard, L.N.K., T.P. Cronanb, and J. Kreiec, "What Influences IT Ethical Behavior Intentions-Planned Behavior, Reasoned Action, Perceived Importance, or Individual Characteristics?" *Information and Management*, (42), 2004: pp. 143-158.

[48] Loch, K.D. and Conger, S., "Evaluating Ethical Decision Making and Computer Use," *Communications of the ACM*., (39:7), 1996: pp. 74-83.

[49] Lwin, M.O. and Williams, J.D., "A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online,".*Marketing Letters*, (14:4), 2003: pp. 257-272.

[50] Manstead, A.S.R. and Eekelen, S.A.M. van, "Distinguishing Between Perceived Behavioral Control and Self-Efficacy in the Domain of Academic Achievement Intentions and Behaviors," *Journal of Applied Social Psychology*, (28:15), 1998: pp. 1375-1392.

[51] Marsh, H. W., "Confirmatory Factor Analysis Models of Factorial Invariance: A Multifaceted Approach," *Structural Equation Modelling*, (1:1), 1994: pp.5-34.

[52] Martocchio, J.J., "Effect of Conceptions of Ability on Anxiety, Self-Efficacy, and Learning in Training," *Journal of Applied Psychology*, (79:6), 1994: pp. 819-825.

[53] Moores, T. T. and Dhaliwal, J., "A Reversed Context Analysis of Software Piracy Issues in Singapore," *Information and Management*, (41:8), 2004: pp. 1037-1042.

[54] Newman, G.R., "Check and Card Fraud," *Problem-Oriented Guides for Police Problem-Specific Guides Series No. 21*, U.S. Department of Justice.
<http:// www.cops.usdoj.gov>, 2004. (Accessed April 08, 2005).

[55] Nunes, J.C., C.K. Hsee, and E.U. Weber, "Why Are People So Prone to Steal Software? The Effect of Cost Structure on Consumer Purchase and Payment Intentions," *Journal of Public Policy and Marketing*, (23:1), 2004: pp. 43-53.

[56] Paternoster, R. and Nagin, D.S., "Enduring Individual Difference and Rational Choice Theories of Crime," *Law and Society Review*, (27:3), 1993: pp. 476-495.

[57] Peace, A.G., D.F. Galletta, and J.Y.L. Thong, "Software Piracy in the Workplace: A Model and

Empirical Test," *Journal of Management Information Systems*, (20:1), 2003: pp. 153-178.

[58] Piliavin, I., R. Gartner, C. Thornton, and R. Matsueda, "Crime, Deterrence and Rational Choice," *American Sociological Review*, (51), 1986: pp. 101-119.

[59] Reidenbach, R.E. and Robin, D.P., "Some Initial Steps Toward Improving the Measurement of Ethic," *Journal of Business Ethics*, (7:11), 1988: pp. 871-881.

[60] Sethi, V. and Carraher, S., "Developing Measures for Assessing the Organizational Impact of Information Technology: A Comment on Mahmood and Soon's Paper," *Decision Science,* (24:4), 1993: pp.867-877.

[61] Shepherd, G.J. and O' Keefe, D.J., "Separability of Attitudinal and Normative Influences on Behavioral Intentions in the Fishbein-Ajzen Model," *The Journal of Social Psychology*, (122), 1984: pp. 287-288.

[62] Shimp, T.A. and Kavas, A., "The Theory of Reasoned Action Applied to Coupon Usage," *Journal of Consumer Research*, (11), 1984: pp. 795-809.

[63] Siegel, L.J., *Criminology*, West Publishing, 1992.

[64] Vallerand, R.D., Deshaies, P., Cuerrier, J., Pelletier, J.G., and Mongeau, C., "Ajzen and Fishbein's Theory of Reasoned Action as Applied to Moral Behavior: A Confirmatory analysis," *Journal of Personality and Social Psychology*, (62), 1992: pp. 98-109.

[65] Warren, S. D. and Brandeis, L. D. (1890), "The Right to Privacy," *Harvard Law Review*, 5, 193.（轉引自林雅惠, 2004）

[66] Westin, A.F.(1967), *Privacy and Freedom*, NY: Atheneum.

[67] Williams, F.P. III, and McShanee, M.D., *Criminological Theory*. NJ: Prentice-Hall, 1988.

[68] Willison, R., "Considering the Offender: Addressing the Procedural Stages of Computer Crime in an Organizational Context," Working Paper Series. Department of Informatics of Copenhagen Business School, <http://web.cbs.dk>, 2000. (Accessed April 10, 2005).

[69] Willison, R., "The Unaddressed Problem of Criminal Motivation in IS Security: Expanding the Preventive Scope Through the Concept of Readying," Working Paper Series. London: London School of Economics. <http://w3.msi.vxu.se>, 2001. (Accessed April 10, 2005).

[70] Wood, R. and Bandura, A., "Task, Domain, and General Efficacy: A Reexamination of the Self-Efficacy Scale," *Psychological Reports*, (72), 1989: pp. 423-432.

附錄A：問卷的情境故事

【個人資料商業化】情境故事

學生輔導中心透過問卷調查欲進一步瞭解學生的生活壓力，該問卷上有學生的個人隱私資訊，例如：姓名、性別、身份證字號、電話、住址等。學生輔導中心委託心理系王教授分析全校 8,000 位同學的問卷資料。明莉是王教授的助理，負責輸入這 8,000 份問卷的資料。

明莉的舅舅是一家補習班老闆，舅舅認爲學生的個人基本資料有助於招生工作，舅舅向明莉索取學生個人資料。因此，明莉利用處理問卷的機會，複製了所有問卷的資料，將資料交給舅舅。

【洩漏他人資料】情境故事

宗憲是某大學 BBS 的版主兼網站管理人，菲哥是其同寢室的哥兒們。菲哥在 BBS 上認識了一位署名爲「神

隱少女」的網友，兩人相談甚歡，菲哥想要進一步認識對方，無奈對方不願意透露真實姓名及聯絡電話。菲哥於是要求宗憲將神隱少女登錄在 BBS 的個人資料透露給他。宗憲認爲幫好友追求女朋友也是美事一樁，就將神隱少女的真實姓名、聯絡電話、就讀學校與上網相關記錄等個人資料給了菲哥。

附錄B：問卷內容

- 採 Likert 七點尺度，，分數由 1 至 7，分別從「非常不同意」到「非常同意」。

對資訊隱私侵害行爲的態度

情境的行爲是沒有傷害性(ATT1)；情境的行爲是可以被接受的(ATT2)；情境的行爲是正當且合理(ATT3)。

主觀規範

我的家人會贊成情境的行爲(SN1)；我的師長會支持情境的行爲(SN2)；我的朋友不會反對情境的行爲(SN3)。

成本的評估

正式成本(FPL)

報案的可能性很低(FPL1)；檢調單位的執法情形是寬鬆的(FPL2)；只會受到法律上輕微的制裁(FPL3)；不會影響情境主角的未來前途(FPL4)。

非正式成本(PL)

家人、朋友更喜歡我(PL1)；不會讓我有良心不安、罪惡感等感覺(PL2)；不會令我感到羞愧(PL3)。

利益的評估

內在利益(IBH)

提升我在朋友間的地位(IBH1)；獲得成就感(IBH2)；獲得刺激的快感(IBH3)。

外在利益(OBH)

獲得報酬(OBH1)；獲得到利益(OBH2)；獲得到好處(OBH3)。

資訊隱私侵害行爲意圖

從事資訊隱私侵害行爲的意願(INT1, INT2, INT3)

- 採 Likert 七點尺度，，分數由 1 至 7，分別從「非常沒信心」到「非常有信心」。

資訊隱私自我效能。

不看、不取得、不分享、不圖利等四構面，共計十題。