探討資訊與通訊科技下的情境盜版預防

林杏子
國立高雄大學
資訊管理學系
cathy@nuk.edu.tw

吳盛
南台科技大學
資訊管理系
shengwu@mail.stut.edu.tw

林芳羽
國立高雄大學
資訊管理學系
fanyu92@gmail.com

摘要

隨著資訊科技的進步,網際網路上的數位內容越趨多元、豐富。許多調查例如全球軟體調查、產業競爭力或經濟效益等皆指出數位盜版在資訊世代依然是值得持續觀察的議題。本研究首先由調查報告說明盜版議題的重要性，以及降低盜版的益處，凸顯事前預防盜版的誘因。因此，本研究將以情境預防的觀點切入，藉由瞭解不同策略，針對現代資訊與通訊科技(ICT)場域的數位盜版現象發展出情境預防方法。

本研究在文獻理論探討部份,根據過去相關研究，以及新聞時事、研究調查報告與文獻回顧等，加以彙整成為不同的預防數位盜版方法。透過事前犯罪機會降低的方法，來抑止數位盜版行為。期盼能對數位內容業者與使用者提出一些建議和參考。對於業者，可以藉由不同方法來進行數位內容的防護，且能理解使用者的需求。而對於使用者能知曉在數位環境上存在相關規範，以及提供合法的其他方案來使用其所需的數位內容。

關鍵字：數位盜版、情境盜版預防、資訊與通訊科技

1. 前言

1.1 研究背景

隨著資訊科技的快速進步,使得人們在網際網路上的活動更加頻繁、多元。然而在數位化環境下的著作權侵害—數位盜版，仍在持續蔓延中。由於軟體、音樂、遊戲、電子書等的數位內容，透過網際網路可以與他人進行傳輸、完整地快速重製，科技技術的進步讓數位盜版變得便利，相對地也造成了影響。根據國際唱片業交流基金會 (International Federation of Phonographic Industry, IFPI)(2010) 指出非法的音樂檔案分享，讓全球的唱片收益從 2004 年至 2009 年呈現逐年下降 30%。而在台灣，新聞局指出 (2010) 流行音樂在 1990 年代曾創造出華語市場 123 億元的產值，但近年面臨音樂科技的快速進步，以及盜版侵權行為的影響下，在 2009 年唱片業產值僅達 14.7 億元。且在學術研究上，透過實徵調查發現非法音樂檔案分享，使得音樂唱片的收益下降 (Zenter, 2003; Norbert, 2006)。由上述數據可以發現音樂唱片在數位盜版的侵害下所受到的衝擊，以及所造成的經濟層面影響。

1.2 研究動機與目的

在降低盜版上，商業軟體聯盟 (Business Software Alliance, BSA)的資料可以發現從 2006 年開始台灣在軟體盜版率表現上的呈現逐年降低。儘管呈現軟體盜版率的降低，但其實仍有改善的空間，像是朝美國 (20%) 或日本 (21%) 來努力。在警政統計通報 (2010) 顯示在 2008-2009 年間，警察機關查緝侵害著作財產權案件從 6,093 下降至 5,542 件。其實持續降低盜版的益處其實很多，像是經濟學人 (The economist) (2009) 在「2009 年 IT 產業競

爭力評估」報告中指出，若要在資訊科技產業保有競爭力，必須具備開放的商業環境與完善的法規制度，健全的智慧財產權保護措施對於產業發展相當重要。且從國家經濟發展層面來看，BSA (2010) 在一份降低盜版的經濟益處中，經由數據與公式指出，(1) 若在未來四年內降低 10%的軟體盜版率，將可能增加當地產業創造 1420 億美元的經濟活動，同時增加將近 50 萬個高科技產業職缺，以及創造將近 320 億美元的稅收。(2) 若盜版率下降很快時，則經濟成長會越快速，舉例而言，法國在四年期間的前兩年達到降低軟體盜版 10%，促進了 37%的經濟相關活動與稅收。(3) 假使研究中的 42 個國家降低軟體盜版的速度越快，可望在 2013 年帶來 1930 億美元的經濟活動，以及 430 億美元的稅收。在這項降低盜版的經濟影響研究中，可以發現是以事前預防觀點來提高盜版降低的誘因，告知如果在未來四年可以達到持續降低，不僅增加國家經濟的發展，且可能增加個體的就業機會。「預防勝於治療」，不單只靠法律訴訟來達到嚇阻的作用，應該以積極的預防角度來達到抑止盜版。

綜上所述，本研究目的在於探討資訊與通訊科技中關於數位盜版的議題，以瞭解如何透過情境預防來減少使用者從事盜版行為。

2. 文獻探討

情境預防 (situational prevention) 是以降低犯罪機會的概念來防範犯罪的發生，(1) 是針對特定形式的犯罪、(2) 涉及對於直接環境的管理、設計與操弄，以達到更具系統化和持久的預防方法、(3) 讓潛在犯罪者對於犯罪感到更困難、有風險，且報酬與藉口的減少 (Clarke, 1997)。企圖讓潛在犯罪者感到無法輕易進行犯罪，讓他們知覺很少或沒有機會可乘，來達到在犯罪行為前的預先阻止。

過去有學者將情境預防運用至盜版研究議題上 (Morris, 2004; 徐百欽，2006; Brookson et al., 2007)。Morris (2004) 在資訊與通訊科技 (information and communication technologies, ICT) 中的網路犯罪 (netcrime) 探討，即以情境預防觀點進行使用者觀點的探討，其中也包含數位盜版的預防探討。在軟體盜版研究上，徐百欽 (2006) 運用五大情境預防技術進行預防軟體盜版的研究。透過情境式問卷實徵發現在增加風險與移除辯解藉口的抑止效果最為有效。而在數位盜版研究中，Brookson et al. (2007) 在歐洲電信標準協會 (european telecommunications standards institute, ETSI) 發表的ICT白皮書提及，數位盜版相關的內容偷竊 (content theft)，包含像是音樂與電影的檔案分享、複製或分享軟體，以及轉錄CD與DVD進行免費分享等皆屬於ICT的內容犯罪行為。而數位盜版的預防策略上，Brookson et al. (2007) 認為在增加困難度與增加風險較能達到防範的可能。可能的防護方法有兩點，第一為透過加密技術防止數位內容遭受攔截或被轉賣。第二為數位版權管理 (digital right management, DRM) 允許付費的使用者觀看，防止進行複製分享給他人。

情境預防主要有五個主要的策略分別為增加困難度、增加風險、降低報酬、降低情境刺激、移除辯解藉口，各別策略將於後續章節分別說明。

2.1 增加困難度

增加困難度指的是當個體在進行不當行為前，知覺面臨到具有困難(difficulty) (Clarke, 1998) 或麻煩的限制存在，必須投入更多的心力 (effort)(Clarke & Eck, 2005)、時間、金錢才能接近到目標物，

而使其放棄從事該行為。Clarke & Eck (2005) 認為增加困難度是情境預防中最基本的類別，卻也是最重要的類別。而數位盜版也屬於財產權犯罪之一，透過增加困難度來約束盜版的技術中，像是軟體光碟上的防盜拷技術，即是用來避免使用者進行重製來對抗軟體盜版 (Gopal & Sanders, 1997)。即使在Anckaert et al. (2004) 的研究中認為軟體防護技術無法提供適當地防護。然而Brookson et al. (2007) 在ICT環境的數位內容防護中表示，如果犯罪是一件困難的事情時，可以嚇阻許多潛在罪犯，因為他們沒有所需的技術，或沒有意願付出所需的時間。因此當個體在進行盜版前，若知覺到所面臨的這項技術或防護有其困難度的存在時，能夠發揮制止踰矩行為的作用。且數位盜版已經非由燒錄實體光碟，而是直接透過網路進行資訊的傳輸與複製，形成廣泛的盜版散佈 (Djekic & Loebbecke, 2007)。

2.2 增加風險

增加風險 (Increase the risks) 代表的是提高個體知覺到從事某項不當行為的負面後果與發生的可能性，當負面結果的發生可能性越高，則風險越高，會促使個體放棄從事該不當行為。Bauer (1960) 在提出知覺風險 (perceived risk) 即提及，由於個體無法考量其行為所有可能的後果，因此當個體對於行為沒有知覺到風險存在時，其決策即無法被它所影響；若當個體認知風險存在時，會透過自身主觀的知覺來進行判斷，以降低其認知風險。透過提高個體的知覺風險，使其知覺存在負向後果且具有發生的可能性，以影響個體的盜版決策。在盜版議題的知覺風險使用上，Tan (2002) 以財務、績效、社交、起訴 (prosecution) 等四項相關風險來衡量購買盜版軟體的意圖，其中起訴風險代表盜版者違反著作權法律時，可能會有被版權所有者提出民事訴訟 (civil action) 的風險存在，而研究結果顯示四項風險皆顯著影響個體的購買意圖。Gerlach et al. (2009) 在跨國盜版研究中，即以訴訟風險 (litigation risk)、損害風險 (damage risk)、心理風險進行研究，研究發現上述三項風險負向影響自陳盜版行為。Liao et al. (2010) 則使用財務、社交、起訴與心理風險進行軟體盜版的研究，結果顯示被起訴風險負向影響盜版軟體的使用意圖，而心理風險負向影響盜版軟體的使用態度。而BSA (2011) 指出盜版光碟上常會暗藏惡意病毒或木馬程式，可能會使得個人電腦遭到程式攻擊、個資外洩的風險；以及在註冊盜版軟體網站時，可能會將個人電腦暴露在危險的網路環境，且個人資料可能遭有心人士盜用、轉賣。

在增加風險的方法上，利用監視或監督，像是透過增加看守者 (watchers) 以約束個體的不當行為 (Brantingham et al., 2005)。Brookson et al. (2007) 認為在ICT的環境下，被追蹤偵查的風險是增加的，因為使用者的任何舉動都會受到監控。例如利用IP位址進行使用者追蹤 (Morris, 2004)。

2.3 降低報酬

降低報酬 (reduce the rewards) 是透過降低犯罪目標物的價值，讓潛在犯罪者知覺從事不當行為所需要投入的成本，與其預期獲得的目標物相較之下，所得到的好處是較少的，進而放棄從事不當行為。

過去在軟體盜版研究中，即發現財務價值 (financial value) 是影響消費者購買

盜版軟體的原因之一 (Moores & Dhillon, 2000)。但也有研究發現消費者購買盜版並非僅考量到財務面的價格考量，還包含像是尋求新奇等因素 (Wang et al., 2005; Ang et al., 2001; Cheng et al., 1997)。由上述可以發現軟體盜版的報酬不僅只有價格上的考量，像是滿足個人對於盜版軟體的好奇也是報酬之一。而Kwong & Lee (2001) 在數位音樂盜版的研究中表示，數位內容符合數位資訊的特性，當分享給他人使用後，並不會降低產品的品質，原始的數位檔案與複製品並沒有存在差異。意謂著當個體得到一份盜版物時，不僅獲得該數位盜版內容，且可以透過拷貝與他人進行分享。在Gunter (2009) 的研究中曾提及，數位盜版讓個體不需付出金錢即可免費獲得盜版物，且會與他人分享其得到的報酬。由上述可以發現，盜版所得到的報酬不僅可以自己使用，也可以與他人進行分享，當盜版產生的報酬增加時，則盜版不當行為也隨著增加。

2.4 降低情境刺激

降低情境刺激 (reduce provocations) 代表的是降低或避免個人受到情境而產生的情緒所影響，使其不會從事不當行為。Wortely (2001) 認為情境不僅提供潛在犯罪者對於不當行為預期成功與否的資訊，同時也是刺激不當行為產生的原因，因為當個體處在會促使壓力或喚醒反社會回應 (anti-social response) 的環境時，即有可能產生踰矩行為。Brantingham et al. (2005) 提及像在網路聊天室網友之間產生紛爭或有不當內容交談時，可以透過版主或管理者的角色加以制止，避免讓情境促發不當行為的產生。

2.5 移除辯解藉口

移除辯解藉口 (remove excuses) 是要讓潛在犯罪者對於其不當行為進行道德判斷，避免合理化 (rationalize) 行為來擺脫罪惡感與羞愧感 (Clarke & Eck, 2005)。Brantingham et al. (2005) 認為移除辯解藉口即是讓潛在犯罪者對於其不當行為難以使用「我不知道」、「我找不到」等說法來作為脫罪藉口，藉由提倡遵守法律讓潛在犯罪者清楚其不當行為可能違法，而政府部門即利用犯罪防治的教育宣導工作，來清楚告知民眾法律或規範的存在。

上述五項情境預防策略皆可用來降低盜版，達到事前預先的行為禁止。透過不同策略的應用，使得在盜版對抗的方法上更顯多元，且涵蓋範圍更廣。期望能在數位盜版情境預防的探討過程中，能由業者、使用者、政府等不同角度找尋適當的盜版預先阻止方法。

3.研究方法

本研究根據Clarke 的五項情境預防策略，來發展不同策略下的數位盜版預防方法，將其運用於對抗數位盜版。透過相關研究探討、新聞案例、調查報告等資料，彙整出各別的數位盜版預防方法，以及發展出五項策略的情境劇本。由不同策略的角度來了解，何者較能發揮抑止數位盜版的行為。

研究步驟會先探討五種策略下的各別情境預防方法，透過具體的方法來了解對抗盜版的相關應用。因此本研究會以彙整的方式來發展預防數位盜版的情境方法。接著會進行研究劇本的發展，用意在於數位盜版為敏感議題，因此受測者可能會隱藏真實答案。而情境式劇本 (scenario based

vignettes) 經常運用於探討敏感性議題的研究，為了減緩填答者可能會隱藏真實的答案，透過劇本的情境設計讓受測者能夠貼近實際的情境 (Harrington, 1996)。透過劇本得以讓研究者在既定的情境下進行研究，且可以避免讓填答者對於研究問卷感到被研究者所威脅 (Rossi & Nock, 1982)。Shore et al. (2001) 認為情境式的問卷可以讓個體的軟體盜版這種複雜的行為得以被捕捉。

4.數位盜版情境預防方法

根據 Clarke & Eck (2005) 對於不同情境策略下的預防方法，本研究彙整當代資訊與通訊科技下的數位盜版預防方法。

4.1 增加數位盜版的困難度

4.1.1 目標物強化

以強化目標物來增加困難度是要讓個體無法輕易、有效率地卸除犯案目標物的防護。Morris (2004) 在網路犯罪 (netcrime) 的研究中認為，廠商在設計其產品時，就應以安全防護觀點出發，在設計中排除犯罪 (designing out crime) 來進行數位產品內容的防護，像是對於數位內容檔案增加防盜機制，一旦有心人士企圖入侵防盜保護時，廠商可以先將數位內容相關檔案的服務暫時離線，避免遭到盜版拷貝。在數位盜版的應用上，像是軟體光碟上的防盜拷技術 (Gopal & Sanders, 1997; 徐百欽，2006)，以及透過加密或干擾技術避免線上影音或廣播遭到側錄 (Brookson et al., 2007) 等技術強化資訊內容保護，避免被使用者輕易地盜拷。近年推出的藍光光碟片 (blue ray disc) 其防盜拷技術即是以先進加密標準 (advanced encryption standard) 為著稱，與過去光碟片上的單一加密技術，存在更高的破解困難度。此外，藍光光碟上所搭載的區域碼[1]，區碼可避免跨國間的盜版平行輸入，例如在美國買的藍光光碟內容，無法使用大陸的播放器播放收看。

4.1.2 控制通道

或稱為存取控制 (access control) (Newman & Clarke, 2003)，透過通道的控制來避免個體進入到其無權入內的空間。在實體的控制通道上，像在出入海關所進行的盜版抽查，一旦發現有盜版內容則會受罰。Morris (2004) 認為在網路環境裡，若需要得到某項數位資源時，個體必須連結至一個網絡 (network)，才能進行存取的動作，而通道控制即是僅讓擁有權力的人進行存取的動作，其餘則無法進行連結。像是企業內部不同階層的員工擁有不同的身份權限，以避免讀取到機密資料 (徐百欽，2006)。透過帳號與密碼以及不同身份權限的方式，是一般網路上進行通道控制最常使用的方式。此外，像是要取得線上音樂服務時 (如：KKBOX)，使用者在登入帳號、密碼後，才能進入線上平台所提供的音樂串流通道，在這串流服務中，使用者透過付費可以合法聆聽音樂。而學術網路對於點對點 (point to point) 軟體的網路連接埠是採取封閉、拒絕連接，故無法在學網內存取到P2P軟體上的資源。

4.1.3 監視出口

或稱為入侵偵測 (intrusion detection)(Newman & Clarke, 2003)，藉由監視出入口的紀錄作為可供日後查閱的歷史

[1] A 區包括有北美洲、中美洲、南美洲、日本、台灣、南韓、香港、澳門及東南亞；B 區包括歐洲、格陵蘭、法國殖民地、中東、非洲、澳大利亞及紐西蘭；C 區則包括印度、俄羅斯、大陸(不包括香港、澳門)、孟加拉、尼泊爾、巴基斯坦及南亞等。

資料，以及在出口確認個體是否有權進出。透過監視進行紀錄，凡走過必留下痕跡的概念。Brookson et al. (2007) 即以電腦或伺服器的日誌檔作為使用者動作紀錄，若有觸法則以日誌檔為證。以及像是透過偵測網路流量來觀察使用者是否在進行不適當的資源下載，一旦發現網路流量過高時，則中斷存取中的連結。此外像是使用軟體必須登入註冊碼，即使個體在取得且安裝盜版軟體後，但沒有經由付費授權即無法得到註冊碼 (徐百欽，2006)。在防毒軟體的更新服務中，若使用者沒有透過合法付費使用，即使有安裝防毒軟體，也無法進行防毒更新。部份線上遊戲 (如星海爭霸等) 會透過線上註冊來確認使用者是否安裝正版遊戲，若是安裝盜版版本則無法進行線上連線功能。以上的例子皆是監視出口的作用，日誌檔與流量紀錄皆是作為使用者的動作歷史紀錄，而軟體的註冊碼、更新服務或線上註冊則是用來確認使用者有權使用。

4.1.4 轉移犯罪者

讓原先是犯罪的事情，讓罪犯者轉移到可被接受的區域執行 (Clarke, 1998)。在近年的駭客大會即是讓駭客可以大展身手但不違法的活動，像是Pwn2Own駭客大賽即是讓駭客對於指定的瀏覽器或智慧型手機廠商中，進行入侵或破解的競賽。在這類的活動中即是讓廠商與使用者間進行互動交流，可以讓駭客進行發揮，也可以讓廠商知道在資訊防護技術的漏洞所在。對於某些作業系統 (如微軟、麥金塔等) 若未經授權使用或分享是違法的行為，但對於開放原始碼的作業系統 (如Linux) 使用是不需付費的。Shang et al. (2008) 在音樂檔案分享的研究中發現，當個體越知道可以自由使用、修改、散佈免費軟體 (freeware) 時，越會影響其倫理上的判斷。意謂著使用者知道其擁有的消費者權力，即使存在需經由付費的版權軟體，但也存在著使用者可以合法、自由使用的免費軟體。

4.1.5 控制工具與武器

指的是在可能發生犯罪的場所，先要求個體交出犯罪工具或武器。應用於數位環境時，像是在學術網路內即有禁止使用P2P軟體的規定，即使P2P軟體原意是用來分享網路上的開放資源，但後來遭到使用者進行未授權的資源分享，故學術單位考量到頻寬的使用以及保護智慧財產權的立場，明文禁止使用P2P軟體。

4.2 增加數位盜版的風險

4.2.1 延伸監視

指的是除了個體本身對於目標物的防護外，也擴大利用目標物周遭的人、事、物，來增加對於目標物的防護。在軟體盜版的應用上，像是在光碟片上的區域碼，若光碟上為美國的區域碼，則無法在其他區域的播放器來光觀賞內容。區域碼不僅防止盜版光碟的跨國平行輸入，且幫助判斷盜版物的輸入來源 (徐百欽，2006)，一旦知道其輸入來源，可以增強對該區域輸入貨物的檢查。以及在販售正版軟體的包裝上加裝無線射頻辨識系統 (radio frequency identification, RFID)，以防止遭到竊取 (Brookson et al., 2007)。在上述例子中區域碼與RFID標籤皆屬於延伸的監視者角色，可以透過其線索進行犯罪的追蹤。此外，企業內的員工也可以扮演延伸監督者的角色，例如BSA所推出的上班族自保行動，即是透過員工來監督企業的盜版使用，避免員工成為企業的共犯。

4.2.2 協助自然監視

自然監視代表強化環境或犯罪目標物的特性進行監控，提高犯罪被發現的可能性，以增加犯罪者被查緝的風險。運用在軟體盜版時，像是Surf Watch、New Nanny、Cybersitter等網路安全軟體原先是應用在防止個體觀看不適合瀏覽的網站，依照其原有的監視特性可以用來警告或封鎖使用者瀏覽可能提供盜版資訊的網站 (徐百欽，2006)。以及像在網路聊天室內，若有使用者出現問題或不當行為，其他使用者可以通報服務提供者 (Morris, 2004)。舉例像在日本音樂著作權協會 (Japanese Society for Rights of Authors, Composers and Publishers, JASRAC) 即與Youtube進行協議，若有使用者上傳版權影片，可經由使用者或版權擁有者進行檢舉通報，再由Youtube進行審核查定影片是否侵權，若是侵權則移除該影片內容，若使用者侵權行為超過三次即刪除其帳號。透過網站服務業者或網路服務提供業者的舉發通報，即是當使用者瀏覽到不適當內容時，即可協助業者進行移除的動作來達到自然監視。The Telegraph (2011) 表示在英國所推動的數位經濟法案 (digital economy act, DEA) 即針對盜版下載的使用者進行查緝，透過與網路服務業者進行著作權的執法合作，當發現使用者侵害著作權時，會發出訊息來警告使用者，若一年內沒有減少70%的非法下載行為，網路服務業者將減慢其上網存取速度，甚至暫停使用者上網存取的動作。以及日本電氣股份有限公司 (Nippon Electric Company, NEC) 研發線上影像辨識比對技術，若有使用者企圖將版權影片上傳到影音網站 (像是Youtube、Yahoo) 時，經由此套技術與正版影像資料庫比對後，可以加以攔截使用者版權影片的上傳 (自由時報，2010)。影像辨識技術即是在使用者進行上傳時的盜版攔截，強化了對於上傳內容的監視。此外像是在公用電腦安裝還原程式，透過還原程式來避免其他使用者跟隨使用盜版。

4.2.3 降低匿名性

或稱為認證授權 (authenticate identity)(Newman & Clarke, 2003)，降低匿名即是進行身份的確認，避免個體利用匿名進行不當行為。運用在網路環境裡，像是利用數位簽章 (digital signatures) 或數位認證 (digital certificates) 來降低匿名性，避免駭客進行偽裝，躲避被查緝的風險 (Morris, 2004; Brookson et al., 2007)。此外，像是無線網路必須透過帳號、密碼登入才能使用，即是避免無線網路遭到冒用或盜用。

4.2.4 使用區域管理者

增加區域的管理者目的在於多一層監督看守的防護，其中，員工也可以作為監督的角色，以增加犯罪的監控。而在盜版防範的方法中，像台灣各地區的夜市可能有盜版攤商的出入，唱片業者即組成巡邏隊以增加盜版攤商被查緝的風險 (徐百欽，2006)。以及在各學術單位的計算機中心，對於學生的網路使用也扮演監督的角色，一旦學生有侵權或違規的情形即會施以懲罰。上述的盜版巡邏隊與校內的計算機中心皆是扮演看守者的角色，來降低盜版行為。

4.2.5 增強正式監控

即是要讓個體感受到犯罪嚇阻的作用，增加被查緝或被逮捕的風險，正式監控的角色像是由機關單位的警察、保全，或監視器、測速照相機等；例如警察會透過路口監視器進行犯罪監控 (Clarke &

Eck, 2005)。運用在網路環境，像是入侵預警系統即是用來避免病毒或駭客進行數位內容盜取 (Morris, 2004)。像在數位內容版權保護上，由電腦軟、硬體公司所組成的信任運算團隊 (trusted computing group) 即透過版權控管來增強軟體的註冊監控(徐百欽，2006)。以及在增加困難度的監視出口中相同的概念，對於公用電腦的日誌檔或流量監控皆是進行使用者的動作紀錄，若有異常即可以此為監視憑據，來終止使用者動作 (Brookson et al., 2007)。在我國，專職處理網路相關犯罪調查的單位為刑事警察局偵九隊，若有違反著作權的盜版情形，會經由通報偵九隊進行查緝。由業界組成的單位像是查緝軟體盜版的BSA、查緝音樂盜版IFPI等，對於使用者侵權會採取法律制裁手段。此外像在校園內，若有同學違反智慧財產權，會予以教育輔導並要求加入校園智財權大隊，一起推廣校園智財權觀念。

4.3 降低數位盜版之報酬

4.3.1 隱藏目標

將容易成為犯罪目標物的財產進行藏匿，使其不會暴露在明顯易取得的地方，避免潛在犯罪者受到誘惑。在降低報酬的方法應用上，像是透過串流服務滿足使用者進行線上影音的收聽或觀賞，卻沒有實際擁有該份音樂檔案 (徐百欽，2006)。以及像是要求使用者關閉藍牙連結，即是避免有心人士透過藍牙連線來窺探可供盜取的數位內容(Brookson et al., 2007)。而嵌入式系統 (embedded system) 可作為隱藏數位內容的技術之一，將數位內容搭載於快閃記憶卡 (flash card) 內，與硬體一同進行組裝來達到隱藏目標物，如此一來可以保護智慧財產權與商業營業秘密 (Winzenried, 2010)。透過嵌入式系統的應用，將數位內容與軟體系統搭載於機器內，只提供介面供使用者使用，如此一來使用者無法接觸到數位內容。

4.3.2 移除原目標

即是將情境中的目標物轉換到其他方法或環境，讓個體不能直接接觸到目標物。在電腦遊戲的應用上，遊戲廠商智冠研發半即時互動角色扮演遊戲，以單機版的遊戲搭配網路功能，即使使用者取得盜版遊戲安裝程式，但若沒有取得遊戲序號則不能與其他玩家進行線上連線遊戲 (徐百欽，2006)。此外，部份線上遊戲 (如星海爭霸) 即便玩家取得盜版安裝程式，但仍無法進行安裝遊玩。

4.3.3 辨別財產權

辨別財產權的目的在於分辨目標物是否為合法授權的財產物，或是能夠用來辨別財產的擁有者。在辨別財產的方法中，微軟公司在其軟體產品包裝貼上真品證明書 (certificate of authentic, COA) 來辨別其為正版、合法的產品，避免使用者買到盜版軟體 (徐百欽，2006)。Newman & Clarke (2003) 認為線上環境的辨別財產權，可以透過告知使用者版權所有的資訊，使其知道該數位內容受到版權保護。像是在電子書或文件上的浮水印應用，Adobe提供作者使用Digimarc版權保護的設定，作者可以將其著作增加數位版權資訊來告知該文件是受到版權保護的，因此若是未經授權的複製或列印該文件檔案時，版權浮水印都會被保留下來。

4.3.4 擾亂市場

當犯罪者得到目標物時，會透過市場進行交易，而擾亂市場像是讓犯罪目標物在

市場變得較沒有價值。在預防盜版的擾亂市場方法上，像是正版軟體透過降價來擾亂原有的市場價格，或以優惠的方案吸引使用者，以及提出拍賣二手正版軟體的建議，來達到市場的流通 (徐百欽，2006)。在手機數位內容服務的應用上，像是小型遊戲—憤怒鳥 (anger bird) 起初必須透過付費才能遊玩所有關卡，但在盜版氾濫的情形下，開放使用者免費下載遊戲，使得盜版遊戲的版本在相較之下，失去其盜版下載該遊戲程式的價值。

4.3.5 否定利益

即是否認個體不當行為所得到的目標物價值，讓個體知覺到目標物可能無法帶來好處，甚至可能成為犯罪的證據。在否定數位盜版的方法中，以色列的科技公司所研發的音樂光碟片可以在一般音響正常播放，但若是要進行光碟內容複製或燒錄時，其干擾機制會讓盜拷的音質出現雜訊。此外，像是微軟會透過宣導正版軟體的優點，來說明盜版可能導致電腦病毒感染與無法進行更新服務 (徐百欽，2006)。Sony對於其遊戲服務像是主機型的PS3以及掌上型電玩—PSP的使用者表示，若對於硬體主機進行越獄 (jailbreak) 下載盜版內容，不但不能獲得Qriocity免費服務，甚至會開始取締盜版使用者。由於部份遊戲必須經由線上服務 (PlayStation network for life, PSN) 來取得更新，若是使用者將遊戲主機進行越獄改裝，可能會因為越獄導致主機封鎖不能遊玩，或是在取得盜版遊戲內容後，成為未經授權的違法行為證據。

4.4 降低數位盜版之情境刺激

4.4.1 降低挫折與壓力

指的是避免個體受到焦躁情緒的影響，導致其出現不當行為。而在預防盜版的應用上，像是學生族群可能無法負擔軟體費用，因此軟體公司會對學生族群推出透過分期付款、電腦套裝購買優惠等方法，以避免學生因無法負擔正版軟體費用的壓力，而轉向使用盜版軟體 (徐百欽，2006; Brookson et al., 2007)。以及學校的公用電腦會提供正版軟體讓學生使用，使其不需煩惱軟體的來源取得，可以合法正當地在校內使用軟體。此外，像是許多軟體公司都會推出不同作業系統 (例如：Windows、Linux等) 相容的軟體版本，避免應用程式無法使用而造成使用者感到困擾。

4.4.2 避免爭吵

指的是避免個體之間有不一致的現象而產生了紛爭。像是國內線上音樂服務市場，即統一一致的收費標準上，國內像是KKBOX、Ezpeer等線上音樂平台每月皆是收費149元，避免不同音樂平台間出現收費不一的現象。

4.4.3 降低情緒喚醒與誘惑

指的是避免潛在犯罪者因為情境，而喚起了對於犯罪感到興奮、刺激等情緒或誘惑的影響，進而減少其從事不當行為的可能 (Clarke & Eck, 2005)。Kwong et al. (2003) 在購買盜版音樂的研究中發現，當個體反對企業的態度越高，則購買盜版音樂的行為意圖越高。意謂著個體的盜版行為意圖會受到其反企業情緒影響，徐百欽 (2006) 即建議若企業善盡社會責任，可以減少使用者對於大型企業的反感情緒，像是反微軟、反蘋果的社團。此外，廠商對於駭客的越獄行為應避免喚醒其反抗的挑戰心態，像是Sony對於駭客提出法律控告行動，但Kinect卻以軟性疏導讓駭客可以自

行設計創作，反而讓Kinect上的應用更有創意。

4.4.4 中和同儕壓力

指的是緩和或抵銷同儕之間對於從事不當行為的影響，避免群聚而相互影響。由於同儕的影響在過去盜版相關研究中皆指出，當同儕的盜版涉入程度越高，則個體會有較高的可能經常從事盜版 (Higgins, 2005; Higgins, et al., 2006; Gunter, 2009)。可以發現在求學階段，同儕對於個體所發揮的影響力很深，Skinner & Fream (1997) 在大學生電腦犯罪的研究中，即發現個體受到其重要社會團體—家庭成員與同儕所影響，兩者皆顯著影響個體的盜版軟體行為，其中，學生學到非法電腦活動是來自於電子討論版 (bulletin board)，說明了線上的同儕組織是學生學習電腦犯罪的對象之一。徐百欽 (2006) 認為若能與同儕產生對於某位偶像的認同或喜愛時，可以中和同儕之間對於盜版行為的看法，或像是政府鼓勵對於盜版「勇於說不」的口號，來緩和同儕相處之間對於盜版的需求。而經濟部智慧財產局對於不同年級的學生推廣校園著作權的概念，藉由教育宣導來鼓勵學生尊重智慧財產權，透過教育宣導的方法，來改善同儕之間對於盜版的看法。

4.4.5 防止模仿

避免潛在犯罪者藉由學習、觀察不當行為的方法或步驟，進而從事仿效。以及學生若觀察到教師從事非法電腦活動時，學生會有較高的可能從事相關不當行為 (Clarke & Eck, 2005; Skinner & Fream, 1997)。而家庭對於從事盜版的影響，即發現家庭成員的非法電腦活動會正向顯著影響個體從事盜版 (Skinner & Fream, 1997)。而網站內容分類制度目前在台灣仍是採取自治的傾向，像在美國的網際網路娛樂軟體顧問委員會 (Recreational Software Advisory Council on the Internet, RSAC) 即提供網站系統的內容分級服務[2]，透過分級制度來阻隔孩童瀏覽到不當內容網站，像是誤導智慧財產權觀念的內容 (徐百欽，2006)。而Brookson et al. (2007) 認為若有網站遭到駭客入侵時，不要清楚告知使用者駭客行為的相關細節，避免有心人士進行仿效。如同美國家庭安裝V晶片的應用，在我國的家長為了防止家中孩童或青少年瀏覽到不良網站，會使用中華電信所推出的守門員來防堵瀏覽不當內容。

4.5 移除數位盜版之辯解藉口

4.5.1 設立規範

透過明確的規定或章程，來避免潛在犯罪者利用模糊、不明確的漏洞來進行不當行為。Newman & Clarke (2003) 認為若規則是不確定，且無法明確執法時，潛在犯罪者即會利用這項模糊來從事電子商務上的不當行為。Morris (2004) 則表示由於網際網路的全球特性，使得在電腦濫用 (例如：駭客行為、侵害智慧財產權等) 處於違法灰色地帶，普遍缺乏法律規範，像是使用點對點音樂下載軟體KaZaA的使用者，即可能是在沒有察覺到其使用是違法的行為。在數位盜版的防治上，若能透過規則法條的建立，讓潛在犯罪者無法規避其責任，像是推動「杜絕盜版與教育法案 (The Piracy Deterrence and Education)」、「誘使侵害著作權法案 (The Inducing Infringement of Copyright)」等，藉由清楚的法條內文，明確限制使用者的盜版行為 (徐百欽，2006)。在數位音樂播放器與電腦

[2] 內容分級共有五個層級，由階級零到階級四，階級越高則代表越不適合孩童進行瀏覽。

軟體在使用前通常會有畫面來警告盜版音樂或軟體是違法行為的警語，明確告知使用者盜版是觸法的行為，避免人們用藉口表示不知道非法複製是有罪的 (Brookson et al., 2007)。在校園中，對於學生宿舍內的網路管理辦法中，會明文規定每位學生的網路流量限制，以確保學術網路上的資源合理使用，若違反則處以網路停權；情節重大則處以學生獎懲辦法來懲處。

4.5.2 張貼告示

指的是藉由公告或提醒的方式，讓使用者難以忽略有規則或警示的存在。應用在對抗盜版的方法上，像是許多軟體公司或業界組成的聯盟 (如BSA、IFPI等) 都有提供民眾上網檢舉盜版使用，藉由公告正確的智慧財產權知識來告知使用者支持正版。美國電影協會 (Motion Picture Association of America, MPAA) 曾推出全民捕盜行動，透過舉動活動來鼓勵民眾檢舉盜版電影光碟，藉以提醒使用盜版是違法的 (徐百欽，2006)。Brookson et al. (2007) 則建議在使用者進行網路使用前，為了讓使用者將電腦網路用在合法存取上，清楚告知電腦日誌檔紀錄的規範，以達到提醒的作用；像在企業內，為預防員工在公司電腦下載、安裝盜版軟體，故會讓員工簽署網路使用安全政策，透過政策的宣佈作為告誡員工小心不要違反。透過使用前的禁止動作告知，讓潛在犯罪者清楚知道進行違法盜版存取，是遭到禁止的。此外，在校園內的影印機周遭會發現有張貼尊重智慧財產權的警語告示，即是用來提醒使用者不要成為侵害著作權的一份子。在電影播映前的著作權所有警語，即是用來告知民眾意識到該部電影是受到著作權人所保護的，若違反其使用規範將有可能面臨侵權的法律訴訟。

4.5.3 激發良心意識

藉由提醒使用者的意識避免個體忽略規範的存在，目的並非在於改變違法的態度，而是在可能犯罪的情境裡，給予使用者適時的規範提醒。Brookson et al. (2007) 建議在潛在犯罪者企圖進行非法存取時，在其上傳或下載頁面彈出反盜版文宣來增強其良心意識的告知，發揮適時的提醒作用。IFPI曾在2002年發起全華人音樂界的「404反盜版大遊行」，藉由號招電影、音樂等相關產業工作者來進行反對盜版的呼籲，透過「支持正版、重燃希望」的盜版光碟回收活動以及當天廣播全面停播流行音樂等行動，來對盜版提出沉默的抗議，且期盼民眾能夠支持正版創作。也有歌手[3]透過歌詞來訴說對於音樂盜版的沈痛陳述。激發良心意識即是透過軟性訴求，企圖喚醒民眾拒絕從事盜版行為，

4.5.4 促使遵守規範

即是在使用者可能產生不當行為前，提供合法的解決方案，鼓勵使用者遵從。徐百欽 (2006) 提出兩種應用於防止盜版的方法，其一是微軟在其作業系統的自動更新功能中，加入了Windows genuine advantage的軟體驗證程序，盜版用戶會在更新重新開機後，出現非正版用戶的字樣來提醒使用者改用正版，且提供「就地合法」方案來促使使用者購買正版序號。以及藉由智慧財產權的推廣讓使用者知道存在其他合法使用的選擇，像是創用CC (Creative Common) 即推廣不同的使用授權條款，讓使用者在遵守規範的情況下，合法使用像是音樂、圖片、文章等網路素材，促使使用者之間以善意換取善意。以及自由軟體鑄造場 (Open Source Software

[3] 歌手林俊傑即以「盜」這首歌來訴說音樂盜版對於創意的傷害，企圖喚醒民眾對於正版好音樂的支持。

Foundry, OSSF) 即提供使用者可單純使用自由軟體的權力，但若是營利或散佈使用，則必須告知創作者。透過這些方法讓使用者知曉在遵守版權使用的規範中，仍有不同的方案可供選擇，即使不付費仍可合法使用。

4.5.5 控制藥物與酒精

控制可能使人失去或混淆日常意識或察覺的犯罪間接物，來避免個體從事不當行為。徐百欽 (2006) 認為此方法中的藥物與酒精概念類似犯罪的催化物，一旦使用可能會使得個人察覺或認知對於觸法較無警覺。在防範實體盜版上，不需經由電腦即可使用的光碟對拷機即可能成為盜版的催化物，然而若是正版光碟則對拷機將無法運作，避免使用者進行盜版拷貝使用。

5. 數位盜版預防劇本之設計

本研究植基於上述各項資訊與通訊科技下的數位盜版預防，再輔以時事新聞與真實案例來發展五項抑止數位盜版的情境劇本。

5.1.1 情境劇本1：增加困難度

情境劇本1：增加困難度(如表1所示)，主要是要突顯出劇中人物小高的兩難在於，購買正版的遊戲需要花費二千元，而另一方面，如果想破解該款遊戲，亦具有一定程度的困難性，因此，透過本劇本將可觀察到對於困難度的知覺是否會抑止小高繼續從事該款遊戲的破解。

表 1 情境劇本 1：增加困難度

小高對於線上遊戲—**星海爭霸 2** 感到興趣，在一次偶然機會下，他獲得一日遊戲序號的星戰體驗包，但體驗過後即無法連線進行遊玩。然而，小高還是想要繼續玩星海爭霸 2，可是購買整套遊戲需要 1950 元，若要嘗試破解其防盜保護程式可能有其**困難度存在**，再加上遊戲本身也不斷地推出更新版與防作弊保護，小高看著網友的討論留言暗自思考該如何是好。

5.1.2 情境劇本2：增加風險

情境劇本2：增加風險(如表2所示)，主要是要突顯出劇中人物小珍的兩難在於，得知學長姐已經因為使用Foxy抓MP3而被懲處，而如果改用目前流行的其他管道如Badongo、megaupload等來下載，會不會也有被抓到的風險。因此，透過本劇本將可觀察到對於風險的知覺是否會抑止小珍繼續從事盜版音樂的下載。

表 2 情境劇本 2：增加風險

小珍聽聞曾經有學長姐在宿舍使用下載軟體 Foxy 抓音樂 MP3，而被台灣唱片業者追查到，在通報學校計算機中心後，被予以停權禁止上網且記過懲處。而現在校園內不能使用 Foxy 等 P2P 下載軟體，小珍在想如果改用論壇或免費空間 (如 Badongo、megaupload 等) 來下載盜版，**不知道會不會也被查緝**呢…..

5.1.3 情境劇本3：降低報酬

情境劇本3：降低報酬(如表3所示)，主要是要突顯出劇中人物艾玲的兩難在於，從網路上抓到的盜版軟體能加速她個人的專案工作，而專題提早完成，就可以得到老師給予的獎勵。而另一方面，如果被發現使用盜版軟體，則成員的成績會被處以零分，不但沒得到預期中的報酬—好成績，反而還有可能被當掉。因此，透過本劇本將可觀察到對於使用盜版會降低報酬

的知覺是否會抑止艾玲使用盜版軟體來完成專案。

表 3 情境劇本 3：降低報酬

蕭老師指導一組資訊管理系統開發專題的團隊，他告訴這個團隊，「遲交作業會被扣分，**早交的學生將會得到獎勵**。不過，**使用盜版軟體則成績將以零分計算**」。同時，蕭老師也身兼管理電算中心的職位，允許他們使用電腦教室的設備來完成專案。然而，其中一名成員艾玲，將網路上抓到的盜版軟體安裝在電算中心的電腦裡，卻沒告知其他成員，因為艾玲覺得這套軟體可以**加速她個人的專案工作**，早交的話，還可以獲得獎勵。另一名成員小美發現這件事後，馬上提醒艾玲，**「**你知道**這樣做會讓妳自己和小組成員得不到好成績，如果因此還被當掉，就更得不償失了」**。

5.1.4 情境劇本4：降低情境刺激

情境劇本4：降低情境刺激(如表4所示)，主要是要突顯出劇中人物小莉的兩難在於，她若是繼續使用盜版軟體，會在每次開機時出現黑色畫面，不但無法獲得持續更新服務，且工具列會出現「非正版用戶」的字樣，似乎是在時時刻刻的提醒她正在使用盜版軟體。因此，透過本劇本將可觀察到對於此一軟體工具列反覆出現的「非正版」字樣是否會促使小莉停止使用盜版軟體，以減少每次使用盜版軟體擔心受怕的感覺。

表 4 情境劇本 4：降低情境刺激

某天小莉關機時，發現電腦一如往常的又在進行更新安裝，之後她開機時卻驚覺電腦桌布整個變成黑色畫面，並出現「**您可能已經成為盜版軟體的受害者**」字樣，同時在工具列也出現「**非正版用戶**」的圖示。**小莉感到十分震驚，立刻緊張地打電話給好友小歐詢問**。小歐告訴小莉說：這是微軟用來偵測用戶所使用的作業系統是否為正版；如果是正版用戶的話，才能夠繼續進行其他的線上更新服務；而這也是在提醒盜版用戶小心成為駭客或病毒攻擊的對象。於是小歐正好利用這次機會請小莉以積極正確的態度來支持正版，如此一來可以**安心使用正版軟體，也可以減少每次開機看到黑色畫面感到擔心害怕的感覺。**

5.1.5 情境劇本5：移除辯解藉口

情境劇本5：移除辯解藉口(如表5所示)，主要是要突顯出劇中人物小浩的兩難在於，雖然可以幫忙學弟妹安裝盜版軟體，但小芳的提醒又使得小浩不得不面對自己這樣行為的違法性。因此，透過本劇本將可觀察到對於移除辯解藉口的知覺是否會抑止小浩繼續幫學弟妹安裝盜版盜體。

表 5 情境劇本 5：移除辯解藉口

小浩在開學期間幫忙學弟妹購買並組裝電腦，有學弟妹私下要求小浩提供完整功能的盜版軟體。小浩覺得以自己的功力，要幫學弟妹安裝他們想要的軟體只是舉手之勞。這件事情被好友小芳知道後，好心地提醒小浩「**不要仗著自己有能力就去幫忙學弟妹安裝盜版軟體**，你記得我們之前上過的資訊倫理課程有提過盜版有**著作權法、刑法與民法上的責任** (註 1)，你可別拿幫忙學弟妹**來當作自己盜版的藉口阿!」**。 註 1：著作權法第 91 條：侵害他人著作財產權，處三年以下有期徒刑、拘役，或併科新臺幣七十五萬元以下罰金。刑法第 358 條：破解電腦之保護措施處三年以下有期徒刑、拘役，或併科新臺幣十萬元以下罰金。民法第 184 條：因故意或過失，不法侵害他人之權利者，負損害賠償責任。

5.2 前測與先導研究對象

本研究的先導研究先與四位專家 (一

位資訊管理領域的教授與兩位碩士生) 逐一進行討論、修正其中的字句適切，採納專家意見以期提昇情境劇本的內容效度。接著進行情境劇本確認的準確度試測，藉由受測者閱讀情境後，視其能否將對應狀況填入所設計的五項情境類別：「增加困難度」、「增加風險」、「降低報酬」、「降低情境刺激」、「移除辯解藉口」。在探討數位盜版研究議題裡，多是以大學生為對象居多，原因在於大學生對於在網路上進行盜版下載較為普遍能夠接受(Gopal & Sanders, 2000; Kwong & Lee, 2002; Higgins, 2007)。因此研究盜版議題時，會認為大學生是適合的母體對象。

5.3 情境盜版預防劇本之準確度分析

本研究的情境劇本準確度分析結果發現，總情境正確率為70.08% (N=123)，而分成資管系 (n=73) 與非資管系學生 (n=50) 其正確率分別為70.68%與69.2%。在「增加困難度」與「降低情境刺激」的情境中，兩組學生答對率都較高 (平均有85%)。而針對準確度較低的「降低報酬」、「移除辯解藉口」兩項劇本，本研究也與專家學者重新修正劇情，以提升全部五套劇本的精確性。

6. 結論與限制

本研究透過情境預防觀點的探討與了解，即是希望提供不同方法來對抗數位盜版。期望所提出的這些方法可以規範使用者的盜版行為，使他們感到無法進行、或感到行為很容易會被發現，而放棄從事盜版，來達到犯罪的預先阻止。透過理論的釐清與預防數位盜版技術的彙整，本研究所發展的情境劇本，以及不同的數位盜版預防方法，皆可作為後續數位盜版研究的劇本。

透過文獻探討的過程，可以發現並非每項情境預防策略皆適合運用於數位盜版。Brookson et al. (2007) 認為不同情境預防的方法能否適用於在ICT相關犯罪上，必須由辨別現存的成功實例，來視其運用的可能性。因此可以發現在數位盜版情境預防上，部份的預防方法即可能不太適用，像是控制藥物與酒精。然而情境預防所涵蓋的範圍，除了過去盜版研究常運用的增加風險以外，更包含了增加困難度、降低報酬、降低情境刺激與移除辯解藉口的預防數位盜版策略，都是可供後續相關研究延伸的部份。但由於許多資訊科技相關知識是僅限於資訊科系或從事人員才知曉的應用，像是自由軟體/免費軟體、免費的創用CC 資源等，故一般民眾對於相關瞭解與法規認識，除了可以透過政府進行的宣導推廣方式，可以透過校園宣導或網路宣傳來讓使用者知道除了進行盜版方式，仍擁有其他方法可供其選擇。

由於本研究僅進行情境預防的基礎理論探討，並綜和過去情境預防應用於盜版的研究加以整理，結合時事案例與調查報告後，歸納出不同情境預防策略下的數位盜版情境預防方法。並進行五項情境劇本的準確度確認，來判斷填答在不同的劇本中能否正確的判斷出其屬於何種情境預防策略。未來研究可實際根據本研究所出的五套劇本並應用於盜版行為的模型實徵研究，以進行情境盜版預防 (Situational Piracy Prevention) 的延伸探討。

致謝

本論文經費來源由國科會計畫編號NSC 95-2416-H-390-013提供。

參考文獻

[1] 徐百欽，以情境預防觀點探討台灣大學生軟體盜版之意志與非抑制控制研究（碩士論文），取自 http://ir.nuk.edu.tw:8080/ir/handle/310360000Q/424，2006。

[2] 商業軟體聯盟，洩個資風險大，中央社新聞網，取自 http://tw.news.yahoo.com/article/url/d/a/110322/5/2ohtv.html，2011。

[3] 商業軟體聯盟，全球軟體盜版調查，取自 http://portal.bsa.org/globalpiracy2009/pr/pr_taiwan.pdf，2009。

[4] 商業軟體聯盟，盜版影響研究：降低軟體盜版的經濟益處，取自 http://portal.bsa.org/piracyimpact2010/index.html，2010。

[5] 國際唱片業交流基金會，IFPI 數位音樂報告，取自 http://www.ifpi.org/content/library/DMR2010.pdf，2010。

[6] 新聞局提出台灣流行音樂發展行動計畫，中廣新聞網，取自 http://news.cnyes.com/Content/20100624/KC9XCVP2JVDBJ.shtml，2010。

[7] 經濟學人，風暴中的復原力：2009 IT 產業競爭力評估，取自 http://portal.bsa.org/2009eiu/，2009。

[8] 資策會產業情報研究所，2009 年台灣網友網路娛樂行為，取自 http://mic.iii.org.tw/intelligence/pressroom/pop_pressfull.asp?sno=214&type1=2，2009。

[9] 澳洲新聞公司 (News.com.au) 和市場調查公司 (CoreData)，2010 年澳洲非法下載調查，取自 http://www.news.com.au/old-t3chnol0gy/download-culture/why-do-australians-choose-illegal-downloads/story-fn58oolp-1225863649562，2010。

[10] 警政統計，侵害智慧財產權通報。取自，http://www.stat.gov.tw/ct.asp?xItem=15440&CtNode=3647&mp=4，2009。

[11] A. Zentner, Measuring the effect of file sharing on music purchases. *Center for the Analysis of Property Rights and Innovation*, 2003, 5, 1-49.

[12] Attributor, U.S. Book Anti-Piracy Research Findings. Retrieved from http://attributor.com/blog/book-piracy-costs-study, 2010.

[13] B. Anckaert, B. DeSutter, K. De Bosschere, Software piracy prevention through diversity. Proceedings of the 4th ACM Workshop on Digital Rights Management, Washington, DC, USA, 2004, pp. 63-71.

[14] B. Shore, A. R. Venkatachalam, E. Solorzano, J. M. Burn, S. Z. Hassan, & L. J. Janczewski, Soft-lifting and piracy: Behavior across cultures. *Technology in Society*, 2001, *23*(4), 563-581.

[15] B. Tan, Understanding consumer ethical decision making with respect to purchase of pirated software. *The Journal of Consumer Marketing*, 2002, 19, 2(3), 96-111.

[16] C. Beccaria, Essay on crimes and punishments (H. Paolucci, Trans). New York, NY: Macmillan, 1985. (Original work published 1764).

[17] C. Brookson, G. Farrell, J. Mailley, S. Whitehead, D. Zumerle, ICT product proofing against crime, ETSI White Paper, 2007, 5, pp. 1-33.

[18] C. Liao, H. N. Lin, Y. P. Liu, Predicting the use of pirated software: A contingency model integrating perceived risk with the theory of planned behavior. *Journal of Business Ethics*, 2010, 91, pp. 237-252.

[19] D. B. Cornish, R. V. Clarke, Opportunities, precipitators and criminal decisions: A reply to Worteley's critique of situation crime prevention (Vol. 16). In M. Smith & D. B. Cornish (Eds.). *Theory for Situational Crime Prevention, Crime prevention Studies*. Monsey, NY: Criminal Justice Press, 2003.

[20] G. E. Higgins, B. D. Fell, A. L. Wilson, Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies*, 2006, 19, pp. 3-22.

[21] G. E. Higgins, Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior*, 2005, 26, 1-24.

[22] J. Cooper, D. M. Harrison, The social organization of audio piracy on the internet. *Media, Culture & Society*, 2001, 23, pp. 71-89.

[23] J. H. Gerlach, F. Y. B. Kuo, S. L. Cathy, Self sanction and regulative against copyright infringement: A comparison between U.S. and China college students. *Journal of the American Society for Information Science and Technology*, 2009, *60*(8), pp. 1687-1701.

[24] J. Jacoby, L. B. Kaplan, The components of perceived risk. In Proceedings of the Third Annual Conference of the Association for Consumer Research, Association for Consumer Research, 1972, pp. 382-393.

[25] M. J. Norbert, The impact of digital file sharing on the music industry: An empirical analysis. *Topics in Economic Analysis & Policy,* 2006, *6* (1), pp. 1-28.

[26] N. Lim, Consumers' perceived risk: Sources versus consequences. *Electronic Commerce Research and Applications,* 2003, *2*(3), 216-228.

[27] O. Winzenried, Anti-piracy protection for embedded systems. Embedded Security. Retrieved from: http://www.wibu.com/files/pressestimmen/ECE-Magazine%20Oktober-2010-wibusystems.pdf, 2010.

[28] O. Winzenried, Anti-piracy protection for embedded systems. Embedded Security. Retrieved from: http://www.wibu.com/files/pressestimmen/ECE-Magazine%20Oktober-2010-wibusystems.pdf, 2010.

[29] P. Djekic, C. Loebbecke, Preventing application software piracy: An empirical investigation of technical copy protections, *Journal of Strategic Information Systems*, 2007, 16, pp. 173-186.

[30] P. H. Rossi, & S. L. Nock, Measuring social judgments: The factorial survey approach, 1982 (Vol. 23, pp. 563-581). *Technology in Society*. Beverly Hills, CA: Sage Publications.

[31] P. L. Brantingham, P. J. Brantingham, W. Taylor, Situational crime prevention as a key factor in embedded crime prevention. *Revue canadienne de*

criminology et de justice penale, 2005, pp. 307-317.

[32] R. A. Bauer, Consumer behavior as risk taking. Proceedings of the American Marketing Association, eds. Robert, S. Hancock, 1960, pp. 389-398.

[33] R. Newman, R. V. Clarke, Superhighway Robbery, Preventing e-commerce crime. United Kingdom, UK: Port Willan Publishing, 2003.

[34] R. V. Clarke, D. B. Cornish, Rational choice. In R. Paternoster & R. Bachman (Eds.), *Explaining Criminals and crime: Essays in contemporary criminological theory* (pp. 23-42), Los Angeles, CA: Roxbury, 2001.

[35] R. V. Clarke, J. E. Eck, Crime analysis for problem solvers in 60 small steps. *Office of Community Oriented Policing Services*, U.S. Department of Justice, 2005, pp. 1-60.

[36] R. V. Clarke, Situational crime prevention: Successful case studies. (Ed.) Albany, NY: Harrow and Heston, 1992.

[37] R. V. Clarke, Situational crime prevention: Successful case studies. (2nd ed.) Albany, NY: Harrow and Heston, 1997.

[38] R. V. Clarke, The theory and practice of situational crime prevention. Retrieved from University of Rutgers, School of Criminal Justice, 1998.

[39] R. Wortley, A classification of techniques for controlling situational precipitators of crime. *Security Journal*, 2001, *14*(4), 63-82

[40] R.V. Clarke, 25 Techniques of Situational Crime Prevention. Retrieved from www.popcenter.org/conference/.../2004/25_TechniquesClarke.ppt, 2004.

[41] S. J. Harrington, The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 1996, pp. 257-278.

[42] S. Morris, The future of netcrime now: Part2—responses. Home Office Online Report, 2004.

[43] T. C. H. Kwong, & M. K. O. Lee, Behavioral intention model for the exchange mode internet music piracy. Proceedings of the 35th Annual International Conference on System Sciences, 2002.

[44] The Telegraph, Digital Economy Act: Rushed anti-piracy laws delayed until 2012. Retrieved from: http://www.telegraph.co.uk/technology/news/8391308/Digital-Economy-Act-rushed-anti-piracy-laws-delayed-until-2012.html, 2002.

[45] W. D. Gunter, Internet scallywags: A comparative analysis of multiple forms and measurements of digital piracy, *Western Criminology Review*, 2009, 10(1), pp. 15-28. (http://wcr.sonoma.edu/v10n1/Gunter.pdf).

[46] W. F. Skinner, A. M. Fream, A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency, 1997, 34, pp. 495-518.