資通安全法律案例宣導彙編

第 12 輯

行政院國家資通安全會報技術服務中心編印

中華民國 104 年 12 月

序

現今社會之資訊科技蓬勃發展，資訊流通快速，資訊應用層面更是無遠弗屆。無論民眾日常生活、企業發展或是政府運作，隨處可見資訊科技之影響及其帶來之龐大效益。然而，資安威脅態樣更趨複雜多元，各界在擘畫及推動資訊技術發展之同時，對於背後所潛藏之風險自是不可輕視。有鑑於資訊技術對於國家發展之重大影響，行政院於102年12月核定「國家資通訊安全發展方案(102-105年)」，其中即明白揭櫫「強化國家資安政策，建立安全資安環境」、「完備資安防護管理，分享多元資安情報」、「奠基資安技術能量，整合科技實務應用」及「擴大資安人才培育，加強國際資安交流」4大策略目標。配合此項重大政策之推展，資安法治意識之形塑及推廣更顯得刻不容緩。

「行政院國家資通安全會報技術服務中心」(以下簡稱技服中心)長期推動我國資通安全基礎設施工作，自 91 年起著手規劃「資通安全法律案例宣導彙編」，並於 104 年邁入第 12 輯。在 104 年內容編排上，仍維持以「資訊保護」、「資訊公開」、「資訊監察」及「資訊應用」為四大主軸，收錄近期重要時事案例，透過法律概念剖析及 CNS 27001(資訊安全管理系統國家標準)觀念宣導之結合，提升讀者對於組織系統安全之正視與關注。

第 12 輯為增加資安案例素材之豐富性與實用性，特別收錄國外重要爭議事件，包括美國電郵門事件、歐盟法院對安全港協議之認定、美國人事行政局洩密案等重要事件，均提供自我國法制角度出發之精闢解析，期帶領讀者了解國際之趨勢脈動。

誠摯希望本案例彙編，能多為各界利用，並成為政府機關與社會大眾進行資訊安全法治教育時之重要參考教材，進一步建構良好的法律和管理觀念。

行政院國家資通安全會報 技術服務中心

劉培文主任 謹識

編者序

國家資訊安全體系之建構向來是各界注目的重點工作，多年來行政院資通安全辦公室與行政院國家資通安全會報技術服務中心在實踐此項任務上不遺餘力、令人感佩。

為協助此項工作，本所長期投入「資通安全法律案例彙編」編輯與撰寫，希望從法律與管理之角度切入，帶給國人即時、豐富且實用的資安法律資訊，協助資安意識之建立及宣導。在這段時間當中，國際環境、資通技術快速變化，國內重要資安法律也接連修正，因而資安法治推廣工作的進行自然也必須加緊腳步。

今年所發行的「資通安全法律案例」(第 12 輯)，除了國內近期的新聞時事外，特別擴大收錄國際間發生的資安重要事件。在內容的編排上，分為「資訊保護」、「資訊開放」、「資訊監察」及「資訊應用」四個構面。其中，在「資訊保護」部分，除了國內重要時事外，尚包括美國人事行政局洩漏個資案、電郵門事件、美國證交會提告竊密案、勒索軟體攻擊等重大事件。在「資訊開放」部分主要討論政府開放資料及其條款設計之議題。在「資訊監察」部分，主要介紹「永遠開啟」(always on)電子產品對於隱私的潛在侵害與因應方式。最後，在「資訊應用」部分，則分析電子票證及數位金融之新興發展趨勢。在這些案例的編寫過程，特別邀請安侯企業管理股份有限公司謝昀澤副總經理協助提供資訊，針對案例重點及法律分析內容，搭配 CNS 27001 的重點內容進行管理提要，希望能夠協助讀者提綱挈領，迅速掌握資安防護之重點方向。

最後，團隊期待能夠透過今年所精心選出的案例，重新啟發讀者對於資安事件的思考及討論，讓「資通安全法律案例彙編」能夠持續成為資訊安全法制領域的園地，持續孕育資訊安全法治意識之發展。

國巨律師事務所

朱瑞陽合夥律師謹識

說明

壹、本案例彙編分為以下類別：

一、資訊保護 (Security)

01 個人資料保護法

02 國家機密保護法

03 營業秘密法

04 刑法

05 醫師法

06 智慧財產權相關法律

二、資訊公開 (Disclosure)

01 政府資訊公開法

三、資訊監察 (Monitors)

01 通訊保障及監察法

四、資訊應用 (Application)

01 電子簽章法

02 電信法

貳、本案例編碼共 8 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年份三碼及上述各小類之編碼兩碼，最後兩碼為該小類中之第幾篇案例。例如：S1040101，即代表資訊保護類 104 年度之個人資料保護法第一則案例。

目次

壹、　資訊保護(Security)

一、個人資料保護法

類別：資訊保護【**案號：S1040101**】

銀行寄錯近 2 萬人帳單，遭金管會裁罰 400 萬元

【焦點話題】

某銀行委託廠商列印並寄送客戶房屋擔保借款繳息清單，但寄發帳單前未具有嚴謹驗證及控管機制，導致 104 年 2 月有高達 1 萬 9,991 名該銀行客戶，收到他人房屋擔保借款繳息對帳單，導致客戶房屋座落地、房貸餘額及還款金額等資料發生外洩疑慮；且該行迄至接獲客戶反映後，始察覺寄給客戶之繳息清單為第三人資料，未能於第一時間發現錯誤，進而採取有效之補救措施。

金融監督管理委員會(以下簡稱金管會)調查後進一步發現，該銀行在民國(下同)102 年就有類此缺失，當時是寄錯 40 多名客戶的扣繳憑單，故銀行認為情節尚屬輕微而未通報金管會。因此，金管會認為該銀行已連續發生兩次類似缺失，且至今未能有效改善，故依銀行法裁處 400 萬元罰鍰[1]。

【資料來源：蘋果日報 104/6/10】

【重點摘要】

1. 機關委託廠商從事印製與寄送含有個人資料之帳單或通知文件，應有檢核資料正確性之管理機制。

---

[1] 銀行法第 45-1 條第 3 項規定：「銀行作業委託他人處理者，其對委託事項範圍、客戶權益保障、風險管理及內部控制原則，應訂定內部作業制度及程序；其辦法，由主管機關定之。」金管會依前項授權訂定金融機構作業委託他人處理內部作業制度及程序辦法第 6 條第 1 項規定：「專責單位應執行之事項如下：…三、督導受委託機構內部控制及內部稽核制度之建立及執行。」。本案中，金管會認為該銀行未善盡對受委託機構監督之責，故以違反銀行法第 45 條之 1 第 3 項規定，依同法第 129 條第 7 款規定，核處新臺幣 400 萬元罰鍰。

2. 機關發生個資外洩，除依相關安全維護管理辦法通報主管機關外，應採取應變措施並持續改善。

【法律觀點】

金管會依個人資料保護法(以下簡稱個資法)授權，於 102 年 11 月 8 日訂定發布「金管會指定非公務機關個人資料檔案安全維護辦法」(以下簡稱安全維護辦法)，明確規範金融控股公司、銀行業及保險業等金融機構，在個人資料蒐集、處理及利用作業過程應採取的適當安全維護事項。安全維護辦法第 8 條要求金融機構委託他人蒐集、處理或利用個人資料時應訂定程序，對於廠商執行業務加以監督並將內容約定於雙方契約[2]。因此，本案例中，銀行委託廠商印製與寄送客戶房屋貸款對帳單，涉及將客戶資產與財務狀況等個人資料委託廠商處理與利用，對於廠商執行業務應依法進行監督，例如銀行在產製當期帳單清冊時，應有一定管控措施；且廠商完成印製後，銀行亦應採取適當方式，抽樣檢查寄件名條所涉個資當事人資料，與通知內容是否相符，以維護客戶資料正確性。

再者，金融機構依前開安全維護辦法，負有於發生個資遭竊取、竄改、毀損、滅失或洩漏等事故後，通報金管會之義務[3]，以利金管會能夠即時掌握個資外洩風險，並監督金融機構後續應變與預防措施之執行。本案例中，該銀行於首次發生帳單作業疏失，致當事人個資有遭不當利用疑慮時，未依安全維

[2] 安全維護辦法第 8 條：「非公務機關應就下列事項，訂定個人資料之管理程序：...六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第 8 條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。」另參個資法施行細則第 8 條第 2 項關於監督事項規定，指出：「監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第 12 條第 2 項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。」

[3] 安全維護辦法第 6 條第 2 項：「非公務機關遇有重大個人資料安全事故者，應即通報本會；其所研議之矯正預防措施，並應經公正、獨立且取得相關公認認證資格之專家，進行整體診斷及檢視。前項所稱重大個人資料安全事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益之情形。」

護辦法通知金管會，雖未遭主管機關逕以違反個資法第 27 條並依第 48 條予以裁罰[4]，然而，銀行於事故後，若未依個資法施行細則第 12 條規定改善內部管理程序[5]，以防止後續作業方式再出現類似疏失，即可能違反非公務機關依個資法相關規定應採取適當安全維護措施之義務。

【管理 Tips】

就本案中某銀行委託廠商列印含有個人資料的文件，該銀行在提供廠商資料前，應先進行組織內部資料檢核作業，在確認資料正確後，始提供給廠商利用並要求委外廠商採取一定之確認或檢核作業。於此同時，組織亦應於委外廠商在列印或其他利用過程進行監控、審查與稽核措施，以避免違反個人資料保護法之情事發生。

一旦組織或其委外廠商不幸發生個資事故，除了要依循既定的管道通報相關單位及主管機關外，並應依照現行的個人資料保護法，查明事件發生的原因後通知當事人。因此就本案中，某銀行得知委外廠商發生個資事故時，除應通報主管機關外，應該要迅速且確實找出事故發生的原因，並且依法通知相關的當事人。

---

[4] 個資法第 27 條第 2 項規定：「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」同法第 48 條規定：非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣(市) 政府限期改正，屆期未改正者，按次處新臺幣 2 萬元以上 20 萬元以下罰鍰：四、違反第 27 條第 1 項或未依第 2 項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」因此，非公務機關若有違反第 27 條情事，主管機關得先命限期改正。再參法務部 104 年 3 月 30 日法律字第 10403503590 號要旨：「個人資料保護法第 27、48 條規定參照，如非公務機關發生個人資料外洩事件時，目的事業主管機關仍應就該非公務機關有無違反上述相關規定，依個案具體情形審酌是否符合處罰構成要件，不得僅因非公務機關未依通報機制向目的事業主管機關為通報，即逕予裁罰。」

[5] 個資法施行細則第 12 條：「本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.15.2.1 供應者服務之監視與審查

組織應定期監視、審查及稽核供應者服務交付。

A.16.1.2 通報資訊安全事件

應循適切之管理管道，儘速通報資訊安全事件。

A.16.1.5 對應資訊安全事故之回應

應依文件化程序，回應資訊安全事故。

A.16.1.6 由資訊安全事故中學習

應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性或衝擊性。

類別：資訊保護【**案號：S1040102**】

欠債變色狼，債主貼文肉搜惹議

【焦點話題】

蔡姓男子在「新竹人」的臉書社團，張貼一則「南寮之狼」的警告貼文，揭露「在逃色狼」的姓名與照片姓名，並提醒婦女小心，貼文最末還附上連絡電話，宣稱「找到必有重賞」。

文章在社群網站上轉載，引發大量網友關注與討論。但警方調查發現，該貼文內容係蔡姓男子自行捏造，因為照片人物為其債務人，積欠百萬元債務又失聯已久，因此蔡姓男子才想利用網友發動人肉搜索。

【資料來源：民視新聞 104/6/16】

【重點摘要】

1. 在公開網站上揭露他人姓名與照片等具有識別性資料，可能構成特定目的外利用他人個資。
2. 未循法律途徑，而任意捏造犯罪事實訴求人肉搜索，致他人受有名譽損害時，恐負刑責。

【法律觀點】

我國個人資料保護法(以下簡稱個資法)明定，除「自然人為單純個人或家庭活動之目的」，或是「在公開場所或公開活動中且未與其他個人資料連結之影音資料」[1]以外，任何公務機關或非公務機關─包含自然人在我國蒐集、處理及利用個人資料，均適用個資法。因此本案中，蔡姓男子非基於個人或家庭生活目的，透過社群網站公開他人具有識別性的姓名與照片等個資，使

[1] 個人資料保護法第 51 條第 1 項：「有下列情形之一者，不適用本法規定：一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料 。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」

該社群網站成員均可檢視其債務人之資料，即屬於個資法上的利用行為[2]，而應適用個資法之規定。

又，蔡姓男子係基於借貸關係而取得個資受害人資料，本應於契約關係與行使法律權利等特定目的範圍內進行利用。而今蔡姓男子在社群網站公開其債務人之個人資料，以不實指控發動人肉搜索，恐已逾越特定目的範圍，且造成個資受害人困擾，若未符合個資法所定正當事由之一[3]，將可能因違法從事特定目的外利用而負有刑責[4]。

再者，蔡姓男子在多數人可得見聞的社群網站，指稱其債務人為「南寮之狼」，依一般社會通念，此一事實將侵害該債務人名譽，導致個資受害人受到該社群網站多數成員的負面評價。因此，蔡姓男子在社群網站散布個資受害人資料之行為，可能同時構成刑法加重誹謗罪[5]。從此一案例，民眾在臉書貼文時，應注意揭露他人資料，是否符合原初蒐集目的之合理範圍，或於特定目的外利用時是否具備合法事由，以避免觸法而負有法律責任。

【管理 Tips】

組織在公告資料時，應考量援引資料的正確性。如係使用其他單位所提供的資料，需要標示資料的來源或出處，並且不可逕行修改內容或陳述與事實不

---

[2] 個人資料保護法第 2 條：「本法用詞，定義如下：四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。五、利用：指將蒐集之個人資料為處理以外之使用。」

[3] 個人資料保護法第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、經當事人書面同意。」

[4] 個人資料保護法第 41 條第 1 項：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。」

[5] 刑法第 310 條：「意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處 1 年以下有期徒刑、拘役或 5 百元以下罰金。散布文字、圖畫犯前項之罪者，處 2 年以下有期徒刑、拘役或 1 千元以下罰金。」

符的言論。組織在取得單位以外的個人資料時，應先內部確認這些資料取得之必要性，以及取得範圍與目的間，是否具有合理關聯性並符合比例原則。

若組織揭露的資料涉及個人資料時，除應比對揭露的資料與原先提供的資料是否一致，並經過一定覆核機制，避免人員誤用或是捏造相關事實以外，同時應考量將個人資料予以遮蔽或去識別化，避免個人資料被不當或過度的揭露或使用，降低管理上的風險。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊保護【**案號：S1040103**】

美國人事管理局再傳 2,150 萬筆個資外洩，局長下台

【焦點話題】

美國人事管理局(Office of Personnel Management, OPM)在民國(下同)年 104 年 6 月對外證實該局遭到駭客攻擊，有 420 萬筆的前任與現任員工個人資料外洩。人事管理局嗣於同年 7 月初，表示調查期間發現另一起相關攻擊行動，造成約有 2,150 萬筆的個資受到影響，其中有 1,970 萬名是申請人的背景調查。該局提供的背景調查服務，是為協助政府機關判斷潛在員工即申請人的個性與可靠度，調查資料範圍涵蓋犯罪紀錄、教育背景、工作經驗及住址，部分尚包含詢問申請人親友或僱主的徵詢紀錄，以及涉及公共信任或是國家安全的調查。

美國人事管理局面臨的兩起個資外洩事件，已成為美國政府史上最大的駭客攻擊事件，曝露出美國聯邦政府系統上的漏洞風險，該局已與美國電腦緊急應變中心及聯邦調查局合作展開調查。連續駭客攻擊事件，迫使人事管理局局長遞出辭呈並已獲准。

【資料來源：iThome 104/6/17】

【重點摘要】

1. 新興駭客攻擊鎖定保有大量敏感資料的政府資料庫，機關應強化資訊防護能力。
2. 機關發生大規模個資外洩後，應採取應變措施並與相關單位橫向聯繫，以釐清攻擊來源並降低損害。

【法律觀點】

隨著資通訊技術發展，資訊網路已深入應用到全球各國政治、經濟、軍事、科技及文化等多個領域。然而，網路安全威脅亦層出不窮，透過釣魚方式散布病毒、植入木馬程式竊取機密及發動分散式阻斷服務攻擊等網路犯罪活動趨於猖獗，且基於政治或敲詐牟利考量的集團式操作型態更為頻繁，對於各國政府維護本身資訊資產與機密安全，均帶來嚴峻挑戰。

在我國，政府機關就公務人員檔案依個人資料保護法相關規定，應採取適當安全維護措施之義務，尤其此類人事檔案基於國家忠誠與職務分配考量，可能含有人員犯罪紀錄與健康檢查等具有敏感性之特種個資，更應強化設備安全，以避免遭他人不當利用，而成為打擊國家安全的工具。

再者，我國國家資通安全會報為掌握政府機關及公民營事業機構資安事件，強化雙向通報與緊急應變處置，訂有「國家資通安全通報應變作業綱要」(以下簡稱本綱要)，若政府機關發現發生資安事件，符合本綱要定義的影響等級時，應立即至國家資通安全通報應變網站進行登錄，提供事件細節、影響等級、支援申請及資安紀錄等資訊，以利主管機關能透過通報系統即時督導事件處理，並評估有無請求外部支援之需求[1]。因此，我國政府機關若發現有大量個資外洩情事時，除應依個資法採取補救或應變措施以外，亦應注意有無依本綱要辦理通報作業之必要。

【管理 Tips】

組織如有使用資料庫或保有大量機敏資料的情形，除了採取一般的資安防護外，另建議定期執行整體的資安檢測，例如網路活動檢測、網路設備、伺服

[1] 「國家資通安全通報應變作業綱要」第 3.1 條規定：「各級政府機關(構)發現資安事件後除應循內部程序上報外，並須於 1 小時內，至通報應變網站通報登錄資安事件細節、影響等級及支援申請等資訊，並評估該事件是否影響其他政府機關(構)或重要民生設施運作，需橫向通知本會報政府資通安全組相關分組。（二）如因網路或電力中斷等事由，致使無法上網填報資安事件，須於發現資安事件後 1 小時內，與技術服務中心聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。（三）進行資安事件處理，『4』、『3』級事件須於 36 小時內完成復原或損害管制；『2』、『1』級事件須於 72 小時內完成復原或損害管制。（四）完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件處理辦法及完成時間。

器及終端設備檢測、網站安全檢測及安全設定檢測等項目，藉由進一步技術性的檢測，找到可能資安弱點或發生風險的所在，並針對檢測的內容加以修正及改進，以避免有心人士藉由技術上的漏洞，藉機取得相關的資料。

組織如有發生資訊安全事故時，須依循相關規定進行通報作業。除了要進行內部通報，以防止事態的蔓延及擴大以外，另外需要通報上級主管機關，同時視個案決定是否需要研擬對外說明的新聞稿。如組織所發生的資訊安全事件涉及個人資料外洩或遭竊取，則須一併考量個資法規定，在查明事件原因後告知當事人。

同時，除了解決個案問題外，組織也要嘗試找到問題核心，並適切處理。在本案中，因這起資安事故，而發現另一個案件是有關連性的，甚至影響範圍更大。因此，一旦發現資安事故時，需要找到問題根因，確實處理並從中經驗學習，以降低同樣事故發生之可能性。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.6.1.4 與特殊關注方之連繫

應維持與各特殊關注方或其他各專家安全論壇及專業協會之適切聯繫。

A.12.6.1 技術脆弱性管理

應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。

A.16.1.2 通報資訊安全事件

應循適切之管理管道，儘速通報資訊安全事件。

A.16.1.6 由資訊安全事故中學習

應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性或衝擊。

類別：資訊保護【**案號：S1040104**】

app 遭駭 企業暫停查詢功能

【焦點話題】

因應行動載具之熱潮，日前有國內公司開發出可供查詢交易紀錄及卡片餘額的行動應用程式(簡稱 app)。不過，此項新的 app 隨即成為駭客攻擊目標；依據該公司在事件發生後之描述，攻擊事件發生之際湧入 9-10 萬筆卡號登入 app，且絕大多數為錯誤碼，顯示攻擊者可能以測試方式登入系統。

攻擊事件爆發之後，該公司已先行暫停 app 查詢功能，改由實體店面提供查詢服務。其後，公司出面澄清所有用戶資料存放於後台系統之中，而不是存放在非記名式的行動載具或 app 中，因而在此攻擊事件中尚未發生個資外洩或遭竊之情形。不過，為釋除各界疑慮，該公司正在加快腳步研擬如何強化 app 的卡片登入安全驗證機制，以提升對於資訊安全的保護。

【資料來源：工商時報 104/5/16】

【重點摘要】

1. 非記名式之行動載具或卡片，其卡號本身無法直接用來識別特定個人，但如與其他消費資料結合，則有可能透過間接方式識別，因而仍屬於個資。
2. 駭客如藉由 app 的卡片登入安全驗證機制或其漏洞，以連線至系統後台竊取交易資料，恐構成刑法無故侵入電腦罪。

【法律觀點】

為規範個人資料之蒐集、處理及利用，避免人格權受侵害，並促進個人資料之合理利用，我國訂有個人資料保護法(簡稱個資法)。其中，針對「個人資料」之定義實為本法的重點之一，其指自然人之姓名、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。簡單來說，個人資料必須是與自然人有關之資料，不包括法人資料在內。此外，個人資料必須可以用來識別個人，不論是透過直接或間接方式，均包含在內；而依個資法施行細則第 3 條規定，所謂得以間接方式識別，指「保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人」。就本案而言，參酌法務部 102 年 12 月 18 日法律字第 10100100770 號函之意旨[1]，無記名卡片之卡號，無法據此識別持卡人之身分，原非屬個人資料；然而，此等資訊如與其他消費資訊結合時，則有可能得以間接方式進行識別特定個人，而有個資法之適用。因此，倘違反規定而蒐集、處理或使用此種個資時，仍有可能觸犯個資法第 41 條規定，最高可處以 5 年有期徒刑。

另一方面，因應資訊時代之發展，各項資料(包含個人資料)往往透過電腦或網路進行存取或處理，因而電腦及網路無疑成為駭客或資訊竊取者攻擊的熱點之一；此時對於侵害資料之行為，除了可依個資法規定請求民事賠償外[2]，尚可透過刑法妨礙電腦使用罪章加以制裁。就本案而言，駭客透過app隨機輸入他人卡號，以連線方式進入系統後台，應屬無故輸入他人帳號密碼入侵電腦設備，且主觀上具有侵害他人的故意，因而將構成刑法第 358 條[3]無故侵入電腦罪，最高可處以 3 年有期徒刑；至於針對無故取得後台資料之部分，由於此等資料屬於電子紀錄，如致生損害於公眾或他人者，駭

[1] 法務部 102 年 12 月 18 日法律字第 10100100770 號函：「個人資料保護法第 2 條、個人資料保護法施行細則第 3 條等規定參照，如記名悠遊卡、金融卡、信用卡卡號等可間接識別持卡人身分，持卡人為自然人者，仍屬個人資料，又尚不得因可間接識別持卡人身分之卡號加密後而尚未解密前，無遭側錄盜刷風險，或機關沒有持卡人其他詳細個人資料檔案可供比對，即認非屬個資法所稱個人資料。」

[2] 個人資料保護法第 29 條規定：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第六項規定。」

[3] 刑法第 358 條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

客將另外構成刑法第 359 條[4]無故取得他人電磁紀錄罪，最高可處 5 年有期徒刑。

【管理 Tips】

就本案而言，雖然是無記名卡片，但因為此種卡片之特性，很容易結合其他資訊(例如消費資訊)，而符合個資法中的間接識別個資。組織應就其保護的資料，鑑別是否有潛在形成間接識別的個人資料，若有就需要與其他個人資料進行同樣的保護。

登入使用者的身分鑑別，除了以最常用的密碼進行管控外，也可以依照所取得資料的重要性，分別賦予不同的身分鑑別方式(如一次性密碼、生物辨識等)。簡言之，權限管控作業是資訊安全業務中的重要環節，如果權限管控無法有效執行，發生資訊安全事件的機率就會相對提高。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.9.4.2 保全登入程序

當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。

A.9.4.3 通行碼管理系統

通行碼管理系統應為互動式，並應確保嚴謹通行碼。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

[4] 刑法第 359 條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

類別：資訊保護【**案號：S1040105**】

最大偷情網站遭駭，3,700 萬筆個資恐外洩

【焦點話題】

全球最大偷情網站《Ashley Madison》日前發表聲明，坦承公司資料庫遭到駭客入侵，致使高達 3,700 萬名會員個資可能外洩，包括姓名、信用卡資料及裸照等資訊。《Ashley Madison》於 2014 年推出徹底刪除個人資料之付費服務，只要會員付費即可完全刪除其個人資料(包括信用卡付費等資料)。然而，在此項服務推出不久後，一個名為 The Impact Team 之駭客組織入侵該網站，宣稱該項徹底刪除資料的服務完全無效，並要求 Avid Life Media(以下簡稱 ALV，即《Ashley Madison》母公司)立刻永久關閉旗下偷情網站，否則將公開其客戶資料。

ALV 聲明其已和政府當局合作調查並掌握駭客資料。《Ashley Madison》則於聲明中表示，目前已透過法律專家及系統安全人員調查此次駭客攻擊事件，試圖找出攻擊的起源、性質及範圍。ALV 並且聲明該公司一直對於客戶隱私有嚴格之安全監控，將會繼續確保業務的安全。

【資料來源：蘋果日報 104/7/20】

【重點摘要】

1. 網站經營者對其保有之個人資料，應提供當事人行使刪除之權利，並應於蒐集個資時，明確告知其行使方法。
2. 網站經營者如未採取適當安全維護措施，致使個人資料被竊取或不當使用，除網站經營者能證明無故意或過失外，被害人得依法請求民事損害賠償。

【法律觀點】

資訊隱私權雖沒有明文列舉於憲法條文中，但司法院大法官釋字第 585 號指出，基於人性尊嚴、個人主體性的維護以及人格發展的完整，隱私權是不可或缺的基本權利，而為憲法第 22 條所保護[1]。至於具體的保護規定，如民法第 195 條侵害人格權之侵權行為責任[2]、刑法上的妨害秘密罪章[3]，及個人資料保護法(以下簡稱「個資法」)相關規定。其中，個資法主要係為規範個人資料之蒐集、處理及利用，避免人格權受侵害，並促進個人資料之合理使用而訂定。為保障民眾的資訊自主權，個資法第 3 條規定乃賦予當事人對其個人資料可向保有機關行使刪除權，使已儲存之個人資料自個人資料檔案中消失[4]；公務機關或非公務機關向當事人蒐集個人資料時，並應將當事人得行使刪除權及其行使方式，向當事人明確告知[5]。除因執行職務或業務所必須(例如，法令規定或契約約定有保存期限等)，或經當事人書面同意者外，倘若個人資料蒐集之特定目的消失或期限屆滿時，機關即應主動或依當事人之請求，刪除、停止處理或利用該個人資料[6]。是以，如本案發生在

---

[1] 憲法第 22 條：「凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障。」

[2] 民法第 195 條第 1 項：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

[3] 刑法第 315 條至第 319 條。

[4] 個人資料保護法第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」個資法施行細則第 6 條第 1 項：「本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。」

[5] 個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

[6] 個人資料保護法第 11 條第 3 項：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」個資法施行細則第 21 條：「有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由。」

我國，當事人無庸以付費方式，即可要求網站經營者刪除其個人資料。

此外，公務機關與非公務機關應採取技術上或組織上的適當安全措施，避免個資被竊取、竄改、損毀、滅失或洩漏，並應以與所欲達成之個人資料保護目的間，具有適當比例為原則[7]。就本案而言，網站經營者既提供徹底刪除個人資料之付費服務，即有必要就相應之安全措施採取更高的標準。如其因未能採取適當安全措施，因而造成主機被駭致使消費者個資外洩，應盡速執行事件通報或應變措施[8]，並調查個資事件之原因，以控管或降低損害範圍。除非網站經營者能夠證明其無故意或過失，否則此時消費者可依個資法第29 條向其請求民事損害賠償，對於因裸照等個資外洩等所造成的非財產上損害，亦得請求慰撫金[9]。

【管理 Tips】

就本案中，主要涉及應刪除的客戶資料卻沒有依照規定徹底執行。在平日業務中，組織應重視記錄生命週期管理(如保護、刪除)，如為需要刪除之項目，務必確認資料已適當移除。此外，應同時注意，經刪除之資料是否尚有其他備份，此備份亦應做同樣之刪除處理。應同時注意的是，除就資料刪除應落實相關執行規定外，對於硬碟、磁帶或光碟之報廢等，也需要將相關媒體進行實體破壞、消磁或是規格化作業，以確保應移除的資料不會被不當利用。

---

[7] 個人資料保護法第 18 條：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」第 27 條第 1 項：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」個人資料保護法施行細則第 12 條：「本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」

[8] 個人資料保護法施行細則第 12 條第 2 項第 4 款。

[9] 個人資料保護法第 29 條：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第六項規定。」

組織另需特別注意，遇有當事人依照個資法第 3 條規定請求刪除資料時，應先確認當事人身分無誤，而後將資料確實刪除或銷毀。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.8.3.2 媒體之汰除

當不再需要媒體時，應使用正式程序加以安全汰除。

A.18.1.3 紀錄之保護

應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊保護【**案號：S1040106**】

帳單亂催繳，判賠男子 3 千元

【焦點話題】

一名張姓男子行經高速公路收費站時，因繳費機帳戶餘額不足扣款失敗，共計積欠 6 筆通行費用。張姓男子原須於民國 103 年 1 月 27 日前繳納完畢，惟其遲至同年 2 月 12 日始繳清款項；在這段期間當中，由於〇〇公司門市人員之疏忽，該筆款項並未正確入帳及銷帳，致使張姓男子持續接到催繳通知，甚至被國道公路警察以同年 1 月 28 日起違規為由開單處罰。案件發生後，張姓男子先至〇〇公司門市請求協助查詢繳費情形，惟因一時找不到繳費收據而遭到拒絕。

張姓男子認為此項事件造成自己名譽受損，家庭因此爭吵不斷，因而向法院提起訴訟，請求〇〇公司賠償新臺幣 30 萬元。經由審理，一審判決判命〇〇公司賠償張姓男子 3,000 元，〇〇公司不服提起上訴，二審法院之理由雖有不同，惟仍維持同一判決結果。

【資料來源：103/9/7 中時電子報】

【重點摘要】

1. 組織應自行確保組織營運資訊之正確性，遇客戶異議或投訴時，負有盡速調取內部留存資料，以查明事實真偽之注意義務。
2. 倘因組織營運資訊之錯誤，對客戶或消費者造成財產或精神上損害，對於客戶或消費者所受損害應負有損害賠償責任。

【法律觀點】

私人權利受到侵害或發生糾紛時，通常可透過民事法律相關規定來保障權利。就本案之情形，張姓男子係主張〇〇公司之催繳行為，對其名譽造成

侵害，此情形原則上可依民法第 184 條第 1 項前段規定請求損害賠償[1]，如屬情節重大者，另可就所受非財產上之損害，依民法第 195 條規定請求精神慰撫金[2]。除此以外，由於張姓男子與○○公司間簽訂有「電子收費服務契約」，因而○○公司之錯誤催繳行為，已涉及違反契約義務，因而張姓男子尚可依民法第 227 條及第 227 條之 1 規定[3]，主張契約上的損害賠償責任。

在本案，張姓男子乃依上開規定向○○公司請求賠償 30 萬元。在一審判決中，法院認為○○公司固因門市員工疏失而未將款項正確入帳與銷帳，惟 6 張違規罰單事後均已銷單，張姓男子並無財產上損害，因而無法就其財產上損害請求賠償；至於家庭失和部分，由於該結果與○○公司疏失行為間欠缺因果關係，因而張姓男子亦無法請求慰撫金。然而，○○公司曾在一審審理過程中，主動提出願意「補償」張姓男子 3,000 元，故一審法院判決○○公司應給付張姓男子 3,000 元[4]。

其後，○○公司提起上訴。二審法院認為張姓男子業已繳費，惟○○公司仍直接對交通部臺灣區國道高速公路局，間接對國道公路警察局為不實陳述，此種不實陳述所傳達之資訊，有表彰張姓男子經催繳仍不願繳款之意思，可能讓第三人聽聞而對張姓男子之誠實、信用產生質疑，進而使其在社會上之評價受到貶損，因而認為○○公司應就其疏失行為對張姓男子造成之損害，「賠償」3,000 元[5]。本案一、二審之判決理由雖有不同，惟其

---

[1] 民法第 184 條第 1 項：「因故意或過失，不法侵害他人之權利者，負損害賠償責任。故意以背於善良風俗之方法，加損害於他人者亦同。」

[2] 民法第 195 條第 1 項：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

[3] 民法第 227 條：「因可歸責於債務人之事由，致為不完全給付者，債權人得依關於給付遲延或給付不能之規定行使其權利。因不完全給付而生前項以外之損害者，債權人並得請求賠償。」同法第 227-1 條：「債務人因債務不履行，致債權人之人格權受侵害者，準用第 192 條至第 195 條及第 197 條之規定，負損害賠償責任。」

[4] 參臺灣士林地方法院 103 年湖簡字 574 號民事判決。

[5] 參台灣士林地方法院 103 年度簡上字第 171 號民事判決。

判決結果皆認為〇〇公司應負民事責任。是以，組織應建立相關機制，以確保客戶資訊之即時性與正確性，並於客戶異議或投訴時，盡速調取內部留存資料，以查明事實真偽，否則一旦發生疏失行為，致客戶受有經濟損害，或其社會評價受到貶損時，將可能因此負有民事責任。

【管理 Tips】

就組織而言，必須要確保所提供資料的正確性，尤其是所提供之資料，與法律條文或契約有關時，更應特別注意。如果發現已經提供不正確之資料，須盡速將資料更正並尋求補救，以避免造成彼此雙方的權益損失。

以本案為例，如有發生資料錯誤導致影響當事人權益時，除了要將資料即時更正外，同時也需要將相關案例及改善措施，做為後續教育訓練的教材，以避免日後再度發生相同的事件，亦可增加日常作業控管的參考。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.3 紀錄之保護

應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

類別：資訊保護【**案號：S1040107**】

公布分析數據爆爭議，軟體開發業者提出解釋

【焦點話題】

A 公司日前針對某商品推出行銷活動，開放民眾於某日凌晨撥打電話訂購商品。活動舉辦當日，A 公司訂購電話專線完全塞爆，某產品順利在數小時內銷售一空。在這同時，軟體開發商 B 公司在知名社群網站上，公布用戶在活動期間撥打電話搶購該商品的相關數據，以 12 小時內訂購電話被撥打次數約 250 萬為計，平均一人就撥打了 126 次電話。B 公司原本希望搶搭新聞話題為自己造勢，沒想到卻意外自爆 B 公司擅自存留與分析用戶去電紀錄，包括發話端與受話端之時間、地點、當時網路環境及手機型號等資料，反倒令用戶驚覺自己隱私遭到侵害，因而引發輿論撻伐。事發之後，B 公司解釋其存留與分析用戶去電紀錄乃是為了過濾不明電話，避免用戶誤撥惡意電話；而針對隱私條款與政策說明不清之處則承諾將會改進，並將致力強化用戶隱私之保障。

【資料來源：自由時報 104/9/5】

【重點摘要】

1. 電話撥打時間、地點及電話型號等，屬於社會活動範疇中之資料，而有個人資料保護法之適用。
2. 組織透過應用程式或其他工具收集用戶資訊，並分析用戶行為，應事先告知並符合蒐集個資之其一事由，否則將涉及隱私權或個人資料之侵害。

【法律觀點】

有關本案所涉及之「發話端之時間地點、受話端之時間地點、當時網路環境及手機型號」等資料，是否屬於個人資料，依照法務部歷來函釋見解，因此等資料可透過與其他資料結合或連結而達到間接識別之效果，性質上屬於社會生活範疇之個人資料，而應符合個人資料保護法(以下簡稱個資法)之相關規定[1]。

在本案中，B公司可否留存與分析用戶去電紀錄等資料，除應視其行為是否依個資法第 8 條規定為明確告知[2]，並符合同法第 19 條第 1 項規定個資蒐集或處理之法定事由外[3]，如涉及特定目的外利用時，尚應取得經當事人書面同意，或符合同法第 20 條第 1 項規定之其他各款事由[4]。此外，個人資料之蒐集、處理或利用，並應尊重當事人之權益，

---

[1] 法務部法律決字第 10303506500 號函：「判斷住家或行動電話號碼是否為得以直接或間接方式識別特定個人，無一致性標準，宜從個案審認。倘蒐集之資料型態已可識別電話號碼屬某學校學生，雖在電話行銷時未直接指名道姓，但一經揭露仍足以識別為特定人，要難謂非個人資料保護法適用對象」、法務部法律字第 10203502260 號函：「個人資料保護法第 2、51 條等規定參照，蒐集者如能將行動電話號碼與其他資料對照、組合、連結而得識別特定個人，即屬個人資料而有該法適用，又行動電話用戶蒐集、處理及利用個人資料行為，如係基於自然人單純為個人活動目的而為者，則無該法適用。」，再參法務部法律決字第 10100122870 號函：「電腦處理個人資料保護法第 3 條等規定參照，該法所稱『個人資料』係指足資識別特定個人之資料，是否足資識別特定個人，宜就具體個案事實審認，如非得足資識別特定個人者，則亦無該法適用。」

[2] 個資法第 8 條第 1 項：「公務機關或非公務機關依第 15 條或第 19 條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」個資法施行細則第 16 條規定：「依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。」

[3] 個資法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。五、經當事人書面同意。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」

[4] 個資法第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危

依誠實及信用方法為之，並與蒐集之目的具有正當合理之關聯[5]。對此，B公司雖曾公告隱私政策與相關條款，惟其內容對於資料種類並未逐一清楚指明，也沒有完整告知蒐集目的與利用用途，更非對客戶以個別方式進行告知[6]，因而B公司就此等資料之蒐集、處理及利用之適法性，是否與原蒐集目的間具有合理關聯，以及該利用是否符合特定目的，恐衍生爭議。B公司之利用行為一旦被認定為侵害個資，且對用戶造成損害時，恐須負民事賠償責任。

另 B 公司以「此等資料均已去識別化」為由作為抗辯，試圖減輕外界疑慮，惟 B 公司對於個資之蒐集、處理或利用，若不符法定事由，或與蒐集目的間不具正當合理關聯時，尚不會因 B 公司係以去識別化方式公布統計資料，即可脫免相關責任，併予說明。

【管理 Tips】

就本案而言，B 公司使用的應用系統記錄用戶電話撥打時間、地點等資訊，由於上述資料符合個人資料的定義，因而應遵守個資法相關規範。為確保當事人的權益，在蒐集個人資料時，應依照相關法令進行告知，並依照所

害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、經當事人書面同意。」

[5] 個資法第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」，另參照法務部法律決字第 10300631830 號函之要旨節錄：「非公務機關對個人資料之蒐集或處理，應有特定目的並符合個人資料保護法第 19 條各款規定所稱法定情形之一；如為特定目的外利用則應符合同法第 20 條但書各款事由之一。除應符合個資法規定外，非公務機關可否蒐集或處理個人資料，應視有無其他法律規定為依據。」，以及法務部法檢字第 10304504440 號函之要旨節錄：「資料蒐集、處理或利用仍應受『必要範圍』及『正當合理關聯』限制。」。

[6] 參照法務部 102 年 1 月 21 日法律字第 10103111060 號函、102 年 2 月 25 日法律字第 10100669890 號函、102 年 7 月 3 日法律字第 10203507170 號函參：「法務部非公務機關依本法第 19 條規定蒐集個人資料時，應『明確告知』當事人上開條文所列應告知事項。又上開規定所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之(本法施行細則第 16 條參照)，亦即任何足以使當事人知悉或可得知悉之方式，均屬之。此一告知並未要求當事人須簽署相關文件，亦未限制不得與其他文件(例如契約)併同為之。惟為達到『明確告知』之目的，蒐集者仍應以個別通知之方式使當事人知悉，不得以單純擺設(張貼)公告或上網公告之概括方式為之，而需足以使當事人知悉或可得知悉該公告內容之方式」。

告知的目的進行個人資料的利用，除非符合法律規定外，不得從事逾越原先告知目的範圍以外的利用。如果未依照既定的程序執行，恐有違反個資法等相關規定。

就實務面而言，組織如果因開創新種業務而需蒐集個人資料，在設計作業流程時，就必須要將個人資料的蒐集、處理及利用等，一併納入考量。組織在考量新種業務時，宜取得法務等相關人士的意見，並且經過核可後，才可正式蒐集個人資料，如果有與蒐集目的不符合的利用，亦不具備其他得為特定目的外利用的法定事由時，必須要取得當事人的同意後才可以執行，以避免個人資料的不當蒐集與利用。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可以識別資訊之隱私及保護。

類別：資訊保護【**案號：S1040108**】

社群軟體利用會員資料寄發邀請信，以 1,300 萬達成和解

【焦點話題】

美國某社群網站以「先社交、再求職」為訴求，提供社交網路服務，會員在該網站建立個人檔案後，能透過網站認識相近領域背景的人士，或針對與其他會員合作經驗撰寫評論意見等。該社群網站推出「增加連結」(Add Connection)功能，在會員同意下，利用會員個人通訊錄以會員名義發送信件給聯絡人，表示「我想把妳/你加入我的專業網絡」，以邀請他們加入該社群網站。若收件人仍未申請社群網站帳號，該社群網站會再以會員名義追加寄發兩封提醒信件，引發會員不滿。

遭到社群網站以其名義後續寄發邀請信的會員，主張他們只有同意該社群網站寄送首次邀請信，但並未明確同意該社群網站後續得再寄發邀請通知，甚至在邀請通知中使用會員姓名與照片。因此，會員主張社群網站此利用行為，並未得到會員同意，且會員亦未因社群網站此宣傳方式而獲得任何回饋，遂在美國提起團體訴訟。該社群網站同意以 1,300 萬元達成和解，經該社群網站以電子郵件通知符合資格的美國會員，均可請求賠償，但符合和解資格的會員人數增加，導致每位會員獲得賠償金額低於 10 美元，故該社群網站同意再追加 75 萬美元和解金。

【資料來源：The Guardian 104/10/7】

【重點摘要】

1. 社群網站未經明確告知會員並經其同意，即利用其個資以會員名義重複寄信予第三人，恐有不當利用的爭議。
2. 因同一事件而受害之多數個資當事人，得授權由財團法人或公益社團法人提起損害賠償訴訟，以團體訴訟方式降低訴訟勞費。

【法律觀點】

依我國個人資料保護法(以下簡稱個資法)規定，此類社群網站除有符合法定免為告知事由以外，應於首次向會員蒐集資料時，告知個人資料蒐集目的、類別，以及利用期間、地區、對象及方式等事項[1]。故依我國個資法規定，社群網站若有利用會員個人通訊錄資料，並以會員名義寄送邀請通知予聯絡人時，應告知會員有此利用方式；社群網站若告知有利用會員資料從事服務宣傳使用，但未說明有此利用方式，恐有違反告知義務或有違合理關聯暨比例原則之疑慮。若社群網站係基於會員服務目的而蒐集會員資料，亦未告知有其他目的或未另行取得會員同意，而使用於其他目的時，例如社群網站逕自利用會員個資，基於行銷本身服務的目的，而以會員名義寄發邀請信件給第三人，即可能構成違法特定目的外利用，而負有民刑事法律責任[2]，並可能遭到主管機關裁罰[3]。因此，未來我國社群網站或應用服務若欲開發此類服務，應確認本身個資蒐集告知事項說明內容，是否充分說明資料利用方式，以保障會員決定是否使用各該功能之資訊自主權。

本案中，該社群網站是與提起訴訟的會員達成和解，而依我國個資法修正新增的團體訴訟制度，亦有助於因同一原因事實受有損害的多數受害人集體求償。依我國個資法規定，因同一事件受有損害的個資當事人，若達 20

---

[1] 個資法第 8 條：「公務機關或非公務機關依第 15 條或第 19 條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。有下列情形之一者，得免為前項之告知：一、依法律規定得免告知。二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。三、告知將妨害公務機關執行法定職務。四、告知將妨害第三人之重大利益。五、當事人明知應告知之內容。」

[2] 個資法第 29 條：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」、個資法第 41 條：「違反...第 20 條第 1 項規定...足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。意圖營利犯前項之罪者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」

[3] 個資法第 27 條：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣(市）政府處新臺幣 5 萬元以上 50 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：三、違反第 20 條第 1 項規定。」

人以上將其訴訟實施權授與特定團體時，得由該團體其代表個資當事人進行訴訟[4]。個資法新增團體訴訟機制的目的，在希望發揮規模經濟效益，降低個別個資當事人自行循求救濟時的勞費成本。附帶說明，依我國個資法，本案中社群網站若因不當利用會員個資，致多數會員受有損害時，除非社群網站因其不當利用行為之所得超過 2 億元以上，否則對於同一原因事實造成多數當事人權利受侵害之事件，損害賠償上限為 2 億元[5]。

【管理 Tips】

組織在使用個人資料時，必須確保其使用目的，與當初經同意之蒐集目的相同，不得逾越授權使用目的而為利用。就本案而言，該社群網站在未經當事人同意的狀況下，使用其個人資料邀約其他人員加入會員，此項行為已經違反個資法相關規定。

組織內部於蒐集資料前，必須確認目的為何，並且在法律所規範的範圍內執行。若需要進一步利用個人資料時，應重新檢視當初蒐集、利用或處理之目的與範圍，如涉及目的外之利用或已超出當初所告知之蒐集範圍時，則須再度取得當事人同意。組織針對個人資料的再利用，宜建立相關審查程序，確保個人資料檔案均為合法使用，避免因為使用目的與蒐集目的不符而違反相關法令。

【相關標準】

ISO 27001：2013(CNS 27001)

A18.1.1 適用之法規及契約的要求事項之識別

---

[4] 個資法第 34 條第 1 項：「對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。」

[5] 個資法第 29 條第 2 項適用第 28 條第 4 項：「對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣 2 億元為限。但因該原因事實所涉利益超過新臺幣 2 億元者，以該所涉利益為限。同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第 3 項所定每人每一事件最低賠償金額新臺幣 500 元之限制。」

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊保護【**案號：S1040109**】

歐盟法院認定安全港協定無效，震撼跨國資料傳輸作業

【焦點話題】

某社群網站蒐集歐盟用戶資料後儲存在位於愛爾蘭的分支機構，再轉傳至美國總公司伺服器，此舉讓美國情治機構得以直接在美國監控所有歐盟公民的社群網站檔案。某位奧地利使用者不滿，向愛爾蘭個資主管機關主張，美國對於傳輸至該國的歐盟公民個資保護不足，但愛爾蘭主管機關基於安全港協議(Safe Harbor agreement)，認定美國為能確保傳輸資料受到適當保護的第三國，而駁回該使用者請求。本案上訴至愛爾蘭高等法院，高等法院為釐清歐盟執委會與美國間簽署之安全港協議，有無排除該國主管機關調查美國企業是否採取適當安全措施，或排除主管機關禁止資料傳輸的權限，將本案提交歐盟法院(European Court of Justice)裁決[1]。歐盟法院認定，縱使美國經歐盟執委會依 2000 年生效的安全港協議，認定為能夠確保適當個資保護的國家，但歐盟 28 個國家個資主管機關仍得依該國法令，監督第三國企業組織蒐集與利用該國民眾個資的情形，若有違反，則依該國個資保護規定論處法律責任。再者，歐盟法院進一步指出，安全港協議允許美國政府機關得向企業取得歐盟公民個人資料檔案，對於歐盟公民隱私權保護顯有不足，故認定無效。

此判決嚴重衝擊美國企業與歐盟間跨國個資傳輸作業，部分業者抨擊此舉將衝擊網路廣告服務或跨國企業業務經營，並危害數位經濟發展，因企業無法確認跨國資料處理作業能否符合歐盟各國規定，而面臨不確定性。美國與歐

[1] Court of Justice of the European Union, PRESS RELEASE No 117/15, The Court of Justice declares that the Commission’ s US Safe Harbour Decision is invalid, available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (latest visited:2015/11/5)

盟已花費將近兩年商議修正安全港協定，而今該協定經歐盟法院宣告無效後，將加重雙方商議時程的壓力。

【資料來源：New York Times 104/10/6】

【重點摘要】

1. 歐盟法院判決認為，縱使歐盟執委會認定第三國對於接收個資能夠確保適當保護程度，仍未限制各會員國個資主管機關得依其本國法令，自行監督調查個資跨國傳輸作業之權限。

2. 依歐盟法院判決，各會員國得要求美國企業蒐集、處理及利用該國民眾個資時須遵守其內國相關規範，可作為我國主管機關斟酌有無限制國際傳輸必要之參考。

【法律觀點】

歐盟個資保護指令規範會員國傳輸個人資料至第三國時，該第三國必須確保具有適當保護程度，而第三國是否達到適當保護程度，應從個資傳輸作業相關情形、資料性質、利用期間及該國法律規範情形等面向加以評估。若經歐盟執委會認定，第三國未能達到適當保護程度時，會員國得採取必要措施，以禁止個資傳輸至該國[2]。因此，為釐清美國是否為該指令所稱具有適當保護程度，而能接受位於歐盟地區各機關組織所傳輸個人資料的第三國，以便雙方跨國資料交換作業順暢運作，安全港協議即在此背景下產生[3]。然而，鑒於近來美國情治機構透過社群網站或雲端服務業者，大量取得歐盟公民個人資料檔案，引發歐盟法院認定美國法令實務運作，尚不足

[2] Article 25, DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (latest visited:2015/11/5)

[3] 美國企業組織得自願加入美國歐盟安全港計畫，自願參與該計畫的企業組織必須遵守安全港架構相關要求並公開承諾遵守。詳細資料可參考 U.S.-EU Safe Harbor Overview, available at http://www.export.gov/safeharbor/eu/eg_main_018476.asp (latest visited:2015/11/5)

充分保障歐盟公民個資安全，進而認定安全港協議無效，各會員國個資主管機關均得本於職權，針對與美國機關組織間跨國資料之處理利用，是否符合該國個資法令，進行監督或調查。

我國個人資料保護法(以下簡稱個資法)第 21 條第 3 款[4]，亦有類似規定，授權中央主管機關於「接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞時」，得限制非公務機關將個人資料傳輸至第三國，以保護我國民眾個資安全，違反者將負有刑事責任並遭到主管機關裁罰[5]。例如國家通訊傳播委員會於 101 年 9 月 25 日，即以「大陸地區之個人資料保護法令尚未完備」，而限制通訊傳播事業將所屬用戶之個人資料傳遞至大陸地區[6]。歐盟法院就本案判決，並非要求會員國逕為禁止本國機關組織傳輸個資至美國，而是否認安全港協議具有「排除會員國主管機關監督跨國資料傳輸處理作業」的效力。因此，歐盟會員國後續如何處理美國社群網站或科技巨擘處理歐盟公民個資的爭議，即值得觀察，並可作為我國主管機關規範個資國際傳輸的參考。

【管理 Tips】

組織在面對個人資料國際傳輸的議題時，應該思考是否有個資國際傳送的必要性；如有需要時，應留意其資料接收的國家是否定義個資保護各項規定並要求落實執行，如有必要將個人資料或其他資訊放置於第三方時，組織應在其與第三方簽訂之合約中明確定義，並且將此些資料或資訊之傳送途徑、儲存方式及業務持續等，盡可能地加以標註或說明，特別是包括監

[4] 個資法第 21 條：「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國(地區)傳輸個人資料規避本法。」

[5] 個資法第 41 條：「違反...中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。意圖營利犯前項之罪者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」、同法第 47 條：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣 5 萬元以上 50 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：四、違反中央目的事業主管機關依第 21 條規定限制國際傳輸之命令或處分。」

[6] 國家通訊傳播委員會民國 101 年 9 月 25 日通傳通訊字第 10141050780 號令。

督管理及檢核的方式，以強化資訊安全的事前保障。

此外，組織需要進一步考量，如果管轄的單位有個資國際傳送的情形，應如何要求其傳送的國家或地區落實個資保護作業，同時如何確保這些國家或地區執行的情形。對於相關的合約規定及要求，組織也可以對業務執行單位進行實際查核，或要求業務單位提出第三方查核報告，確認已依照當地的法令及合約之要求執行。

【相關標準】

ISO 27001：2013(CNS 27001)

A13.2.2 資訊傳送協議

協議應闡明組織與外部各方間營運資訊之安全傳送。

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

二、國家機密保護法

類別：資訊保護【**案號：S1040201**】

公務即時 LINE，洩密也能賴？

【焦點話題】

拜科技進步所賜，即時通訊軟體(例如 skype 及 Line 等)越來越夯，這個工具不僅在一般企業組織或社群中受到歡迎，也成為政府機關提升公務聯繫效率的新幫手。在提升公務聯繫效率的同時，即時通訊軟體的潛在風險也引發討論。例如，某公務人員曾將首長批示意見透過 Line 對外傳送，造成消息不當曝光；又例如因某公務群組遭駭客入侵，促使機關自我檢討公務聯繫作業，甚至自此嚴禁「機密公文」以即時通訊方式傳遞。

面對公務聯繫效率及資訊安全保護的兩難，曾有議員質疑通訊軟體存有潛在風險，部分政府單位早已禁用通訊軟體。更深度的問題是，與一般公文不同，即時通訊所傳送的訊息無須依法進行存檔及列管，也無從追查，未來恐成了洩密和弊案的溫床。

【資料來源：聯合報 104/4/18】

【重點摘要】

1. 公務人員線上進行公務討論聯繫時，應注意資訊安全與通訊內容之機密性。
2. 公務人員利用行動裝置從事公務討論時，應進行資料備份與加密防護，並注意該裝置遺失或廢棄之資料處理。

【法律觀點】

隨著網路及行動應用的蓬勃發展，越來越多民眾喜歡使用即時通訊軟體聊

天、甚至會將他作為討論或交辦工作的工具。針對利用即時通訊軟體處理公務的作法，目前已有政府單位訂定技術性或細節性規範加以因應。整體來看，這些規範大抵可分為「軟體安裝與設定」、「群組管理」及「資訊傳遞」三個部分。針對「軟體安裝與設定」，使用即時通訊軟體進行公務討論時，應先進行密碼設定及管理，並就裝置進行相關安全環境設定，這部分其實與一般電腦安全並無二致。針對「群組管理」，先依據公務需求不同成立各類群組，再依此設定分組原則及成員資格，而後由群組管理者(組長)本於管理權限進行群組加入或退出之審核；在此模式下，如果不具有加入群組資格，即無法進入該群組而有後續接觸公務資訊的機會，藉以降低公務資訊外流的風險。至於「資訊傳遞」則為資安風險控管之關鍵點，在做法上，公務資訊如涉及機密性、資訊安全及隱私事項，一律不得以即時通訊軟體傳輸，原則上就不可能會有透過即時通訊軟體傳輸或外洩的機會。其次，針對非屬機敏性之公務資訊，如果涉及公文檔案傳遞，另應同時注意符合公文公開作業原則等規定。

此外，為俾利公務資訊的後續使用、舉證、追蹤等，公務人員對於重要資料，應注意備份存放；針對重要資料，例如含有大量個人資料檔案，應以密碼或加密措施保護。而為避免公務資訊在無意間外洩，在丟棄任何儲存資訊之電子媒介時(例如，光碟片及隨身碟等)，應先將儲存資訊刪除，並徹底消磁或銷毀至無法解讀的程度。並且，在任何公開之新聞群組、論壇、社群網站或公布欄中，應特別注意不可透漏任何公務機密相關之細節。

公務人員如有違反上開規定，將依政府機關人事相關規章面臨行政懲處。如涉及重要之公務機密外洩事件，不論出於故意或過失，可能構成刑法洩漏公務秘密罪[1]，最重可處以三年有期徒刑。如洩漏者屬國家機密時，更可依國家機密保護法規定，處一年以上七年以下有期徒刑[2]。在提升公務聯繫效率

[1] 刑法第 132 條第 1 項及第 2 項：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。」

[2] 國家機密保護法第 32 條：「洩漏或交付經依本法核定之國家機密者，處一年以上七年以下有期徒刑。因

的同時，對於潛在的資安風險必須格外謹慎，以免因一時的無心之失，反而為自己增添無謂的牢獄之災。

【管理 Tips】

在本案中，組織在導入或使用行動式設備時，應訂定相關政策規範，其中應包括：可在行動設備中使用的工作項目、資料儲存方式、行動設備需具備的保護設施、資料傳送要點，及資料銷毀的程序等。此外，組織應採取相關配套措施以管控風險，並透過教育訓練、宣導或公告注意事項等方式，讓員工明瞭設備使用範圍、限制及相關安全規則；必要時，對於違反使用規範之員工應有相當內部懲處措施，以兼顧行動辦公需求並同時落實對於機敏資訊的保護。

另一方面，針對就行動式設備的資料，組織應定期執行備份作業；如有包含機敏性資料，尤其應考量機敏性資料加密的方式，以避免機敏性資料被其他未經授權的人員取得。此外，組織應明確告知員工，如授權的行動設備遺失時，務必要進行內部通報，以防止損害擴大。對於使用的行動設備，如有報廢或汰換之需求，應先將原有資料備份到新的裝置，而後刪除原有資料或破壞原有行動設備，以避免資訊安全事件的發生。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.6.2.1 行動裝置政策

應採用政策及支援性之安全措施，以管理使用行動裝置所導致之風險。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及

過失犯前項之罪者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。第一項之未遂犯罰之。」

程序之適切認知、教育及訓練，並定期更新。

A.7.2.3 懲處過程

應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。

A.12.3.1 資訊備份

應依議定之備份政策，定期取得資訊、軟體及系統的影像備份複本，並測試之。

A.13.2.1 資訊傳送政策及程序

應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。

類別：資訊保護【**案號：S1040202**】

海軍中尉誤碎機密文件 未違反國家機密保護法確定

【焦點話題】

謝姓現役海軍中尉任職海軍中正基地蘇澳通信隊時，代理督導機密文件清點作業的江姓中尉區隊長認為，通信機密文件外面所套的牛皮紙袋多已破損而不利清點，曾要求他進入密件庫，為所有機密文件退除舊的牛皮紙袋，並更換為透明塑膠資料袋。在更換的過程當中，謝姓中尉漏未替核定為軍事機密的「國軍第〇號密譯辨證法編號〇」(簡稱本案密件)更換新袋，而將其夾在舊牛皮紙袋中，整疊攜出，交由正在值班的不知情蔡姓二兵負責碎紙，致使本案密件毀損。其後，陳姓上尉督導通信機密文件清點作業時，赫然發現本案文件遺失，幾經調查發現其早已被碎為紙屑。軍方單位以涉犯國家機密保護法第 35 條第 2 項之過失毀損國家機密罪，將謝姓中尉移送法辦。

針對本案，一審法院認定，本案文件並未依國家機密保護法核定為國家機密，因而謝姓中尉誤碎文件行為，並不構成前開犯罪。其後經檢察官提起上訴，日前經二審法院認定原審判決沒有不當，維持無罪判決。

【資料來源：自由時報 104/7/08】

【重點摘要】

1. 對於涉及國家安全或利益而有保密必要之公務文件，應依法報請國家核定機密，並強化對於該文件的保護。
2. 銷毀公務文件前，應確認其是否經核定為國家機密；除因戰爭、暴動或事變而非予銷毀無法保護外，銷毀國家機密前應先解密，否則可能涉犯毀損國家機密相關犯罪。

【法律觀點】

為建立國家機密保護制度，確保國家安全及利益，我國訂有國家機密保護法(以下簡稱本法)。然而，並非機敏性公務資訊都屬於本法保護的客體；必須是基於國家安全或利益而有保護必要，且經核定機密等級的資訊[1]，才是所謂「國家機密」。

經核定為國家機密的資訊，不論是絕對機密、極機密或機密，在知悉、持有、使用、收發、傳遞、保管、複製、移交、銷毀及解除等作業，法令上都有非常嚴謹的規定。例如，國家機密之知悉、持有或使用，必須取得書面授權或核准[2]，且國家機密之收發、傳遞、使用、持有、保管、複製及移交，應依其等級分別管制[3]；如有違反規定而有洩密之情形，無論故意或過失，可能涉犯本法第 32 條第 1 項或第 2 項犯罪，最高可處以 7 年有期徒刑。另，國家機密經解除機密後始得依法銷毀[4]；國家機密因戰爭、暴動或事變之緊急情形，非予銷毀無法保護時，得由保管機關首長或其授權人員銷毀後，向上級機關陳報[5]；違反前開規定而毀損國家機密者，無論故意或過失，可能涉犯本法第 35 條第 1 項或第 2 項犯罪，最高可處以 5 年有期徒刑。

就本案而言，謝姓中尉將公務密件交由蔡姓二兵碎紙的行為，在法律上屬於「毀損」之行為。而謝姓中尉之所以囑託他人碎紙，是他沒有注意到該公務密件仍夾在舊牛皮紙袋中，因而主觀上可能具有過失。然而，本案關鍵在於，謝姓中尉交由他人碎紙的公務文件，當時僅依「軍事機密與國防秘密種類範圍等級劃分準則」核定為軍事機密，而沒有同時依「國家機密保護法」核定為國家機密，因而還不是法律上所謂的「國家機密」。因此，本案一審判決[6]認為，謝姓中尉固然誤碎本案文件，惟該文件件並未依國家機密保護法核定

[1] 國家機密保護法第 2 條規定：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」

[2] 國家機密保護法第 14 條。

[3] 國家機密保護法第 15 條第 1 項。

[4] 國家機密保護法第 15 條第 2 項。

[5] 國家機密保護法第 16 條。

[6] 臺灣宜蘭地方法院 103 年度軍易字第 1 號判決。

為國家機密，所以他的過失行為並不成立過失毀損國家機密罪。其後經檢察官提起上訴，日前經二審法院[7]仍維持同一見解。

【管理 Tips】

有關組織文件銷毀的議題，特別是機密文件，從管理面的角度而言，不光是只有現行使用的文件需要保護，組織必須了解到從資料生命週期之各個階段，都有可能被有心人士拿來利用，因此從文件的產製、傳送、儲存到銷毀，也需要因應文件內容及其機密等級之不同，考量可能涉及的風險並相應採取管理機制，而有差異性的處理方式，以防止文件管理不當導致重要資訊外洩，以降低事故發生的機率。

本案涉及海軍中尉誤將公務文件銷毀，此類事件發生主因在於未確實依據資訊分級採取相應保護措施。因此，組織除定義一般、密、極機密的資訊機敏等級分類方式以外，對於每一種類文件所涉及之階段，包括蒐集使用、保管傳送、揭露或銷毀等，都必須訂定明確的規範，並向組織所屬人員進行宣導，且配合適時抽核以強化認知，防止因不明瞭文件分類處理的方式，而造成資訊安全事件再次發生。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.8.2.1 資訊之分級

資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

[7] 臺灣高等法院 104 年度軍上易字第 1 號判決。

A.8.2.2 資訊之標示

應依組織所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

類別：資訊保護【**案號：S1040203**】

電郵門事件延燒，希拉蕊交出私人信件伺服器

【焦點話題】

美國民主黨總統候選人希拉蕊於 2015 年 3 月驚爆電郵門事件(Emailgate)，據悉她在 2009 年至 2013 年間擔任國務卿一職期間，未曾使用美國政府配發的公務信箱，而是使用伺服器設在自家的私人郵件帳戶，收發與儲存相關公務信件，恐有違反聯邦檔案法相關規定，引發爭議。事件發生一週後，希拉蕊親自出面說明，強調使用私人信箱收發郵件是貪圖方便，但絕無不法。其後，希拉蕊為平息輿論質疑並回應公眾監督聲浪，在同年 8 月決定將私人信箱 6 萬 2,320 封往返郵件中，涉及公務事務的 3 萬餘封電子郵件提交予國務院檢視。

儘管希拉蕊提交的電子郵件資料內容，尚有待聯邦調查局進一步分析是否涉及國家機密，但美國情報體監察長(Inspector General of Intelligence Community)表示，在國務院允許他調查的電子郵件範圍中，已發現五封機密文件，當中還有兩封是絕對機密，且都未明確標註分類機密等級。監察長指出「有些文件應該被標註機密，且透過受保護的系統傳送，可是顯然沒有。」國務院保守估計，至少有上百封郵件是屬於機密文件。

【資料來源：風傳媒 104/8/12】

【重點摘要】

1. 公務人員以其私人信箱傳輸涉及公務的內容，即可能因私人電子郵件系統未有適當安全防護措施，而違反機關資訊安全管理規範，並提高機密外洩之疑慮。
2. 公務人員以私人電子郵件信箱收發涉及公務內容，可能規避機關主管監督，

並導致公務執行紀錄無法確實保存或配合調閱，而有礙檔案保存與備查。

【法律觀點】

美國於 1950 年通過的聯邦檔案法[1]，要求政府官員應妥善記錄並保存涉及決策、程序及機關重要活動等相關紀錄，美國總統歐巴馬嗣於 2014 年簽署通過總統暨聯邦紀錄法修正草案(Presidential and Federal Records Act Amendments of 2014)，該法修正後已明確定義所謂聯邦紀錄包含電子或數位格式，並要求聯邦政府官員若非以公務電子郵件系統傳送資料時，須同時副本至公務信箱，或於寄送後 20 日內將原信件轉寄至公務信箱[2]，以保存該信件紀錄並確實揭露相關公務活動。鑒於希拉蕊擔任國務卿期間，聯邦法令並未明確禁止官員使用私人信箱[3]，然而美國國家檔案局(National Archives and Records Administration)於 2011 年電子紀錄管理規定中的「電子郵件紀錄管理之其他要求」[4]，已規定「允許職員使用非由機關維運的電子郵件系統收發信件」的機關，必須確保以其他郵件系統收發的聯邦紀錄，能夠由該機關本身檔案管理系統歸檔保存，希拉蕊擔任國務卿期間顯然未遵守該規範。而希拉蕊卸任後，聯邦法令進一步明文要求官員須將涉及公務內容的紀錄，須於指定期限內提供機關存檔備查，以致希拉蕊電郵門事件是否違反當時聯邦關於紀錄保存的規定，引發爭議。

---

[1] 44 U.S. Code § 3101 - Records management by agency heads; general duties.

[2] Presidential and Federal Records Act Amendments of 2014, Sec 2209: Disclosure requirement for official business conducted using non-official electronic messaging accounts.

[3] 美國國家檔案局於 2013 年 9 月公告「機關職員管理電子郵件帳號等聯邦紀錄，與避免聯邦紀錄遭未經授權移除之指引」，以供聯邦機關參考。該指引第 5 點指出，聯邦職員不應廣泛使用私人電子郵件帳號從事公務活動，但在公務信箱無法登入的緊急情況，或該職員係私人電子郵件初次接洽等情形，機關得授權使用私人郵件帳號。惟機關職員在此情形，必須確保所有在私人郵件帳號涉及聯邦紀錄的信件收發，符合機關檔案管理作業。查詢自 NARA Bulletin 2013-03, September 9, 2013, available at https://www.archives.gov/records-mgmt/bulletins/2013/2013-03.html (last visited: 2015/10/5)

[4] 36 CFR 1236.22 - What Are The Additional Requirements For Managing Electronic Mail Records?, available at http://www.gpo.gov/fdsys/pkg/CFR-2011-title36-vol3/pdf/CFR-2011-title36-vol3-sec1236-22.pdf (last visited:2015/10/4)

公務機關通常會配發所屬人員使用機關網域的公務信箱，然而因垃圾郵件管理機制或檔案容量上限等因素，公務人員可能仍有使用私人電子郵件收發涉及公務活動信件的情形。而希拉蕊電郵門事件即曝露出政府官員使用私人電子郵件處理公務時，可能發生公務機密保護不足、難以滿足公眾監督需求與政府文書紀錄保存未盡完整等問題。

我國法令雖未明文禁止公務人員使用私人信箱，然而部分機關針對公務電子郵件信箱使用，訂定申請程序與相關使用限制等管理規範，並禁止人員使用公務信箱傳送私人信件[5]，以維護機關資訊安全，且確保公務人員從事公務紀錄能夠完整存檔備查。又依「行政院及所屬各機關資訊安全管理要點」第 27 條[6]，已明文禁止機關人員原則上不得以電子方式傳輸機密檔案，至於有傳輸敏感性資料與文件之必要時，機關所屬人員應採取相當安全防護機制。因此，公務人員以其私人信箱傳輸涉及公務的內容，即可能因私人電子郵件系統伺服器或傳輸過程本身，未有適當安全防護措施，而提高公務機密或其他敏感資料外洩風險，以致違反機關資訊安全管理規範。

另，依我國政府資訊公開法關於「政府資訊」之定義，是指政府機關於職權範圍內作成或取得之各種訊息[7]，因此私人電子郵件是否構成政府資訊，須視個別信件具體內容，是否係基於職權範圍作成或取得而定。再者，信件是否適用檔案法相關規定須統一歸檔，並於法定期間內保存，亦須視信件內容或夾帶檔案，是否涉及機關指定保存的檔案類型。然而，公務人員以私人電子郵件信箱收發涉及公務內容，已可能規避機關主管或公眾監督，並導致公務執行紀錄無法確實保存或配合調閱，恐已違反資訊公開揭

[5]例如司法院、總統府、監察院及臺南市政府環境保護局等均自行訂有機關電子郵件信箱管理要點。

[6]行政院及所屬各機關資訊安全管理要點第 27 條：「各機關應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各機關應視需要以適當之加密或電子簽章等安全技術處理。機關業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。」

[7] 政府資訊公開法第 3 條：「本法所稱政府資訊，指政府機關於職權範圍內作成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息。」

藝的公眾監督意旨，是機關逐步邁向電子化作業環境時，應注意此一資訊管理議題。

【管理 Tips】

組織宜在資訊政策中，明確告知同仁電子郵件的分類及管理，以及釐清得否使用私人郵件信箱處理公務或相關限制。另電子郵件之資料分類等級，應考量電子郵件的內容而加以區隔，如果涉及機敏性資料，檔案宜加密或使用密碼保護，避免因為電子郵件的控管不當，導致電子郵件被未經授權的人員取得。

另就實務作業而言，電子郵件同樣需要依照規定進行備份作業，除了防止系統發生異常狀況時，可以利用備份資料迅速恢復正常作業，同時對於電子郵件的使用，亦應保有適當的進出紀錄與軌跡資料。如果有需要調閱過往郵件紀錄的情形，也必須依照內部的作業程序進行調閱，以確保郵件的使用受到適當的保護，並且能留存完整的資訊。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.5.1.1 資訊安全政策

資訊安全政策應由管理階層定義並核准，且對所有員工及相關外部各方公布及傳達。

A.8.2.1 資訊之分級 A.12.3.1 資訊備份

應依議定之備份政策，定期取得資訊、軟體及系統的影像備份複本，並測試之。

A.13.2.3 電子傳訊

應適切保護電子傳訊時所涉及之資訊。

A.13.2.4 機密性或保密協議

宜識別、定期審查及文件化，以反映組織對資訊保護之需要的機密性或保密協議之要求事項。

三、營業秘密法

類別：資訊保護【**案號：S1040301**】

洩密給中國公司 前工程師被訴

【焦點話題】

兩岸科技產業的競爭局勢趨向白熱化，知名大廠頻頻上演搶人大戰。國內知名光電大廠的員工陳男，離職後前往對岸競爭對手公司任職，並協助挖角老東家的菁英人才。為了獲得賞識，作為爭取薪資或職務的交換條件，該大廠某資深幹部吳男選擇「帶槍投靠」，不顧自己所簽下的保密約定書內容，將被原任職公司列為機密文件的「某新產品製程檢核表」等資料下載，透過電子郵件寄給新東家。全案經原任職公司發現後，報請國內檢調單位處理，檢察官隨即偵結並以違反營業秘密法為由提起公訴。

【資料來源：自由時報 104/4/21】

【重點摘要】

1. 逾越授權範圍而將公司機密資料提供予第三人，將構成營業秘密侵害。
2. 意圖提供機密資料在我國領域外使用，將構成加重犯罪型態，且屬於非告訴乃論罪。

【法律觀點】

對於洩漏機密資料之行為，我國刑法第 317 條[1]原定有妨害工商秘密罪。所謂工商秘密，通常指「工業上或商業上之秘密事實、事項、物品或資料，而

[1] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金。」

非可舉以告人者而言，重在經濟效益之保護[2]」，行為人只要違反法令上或契約上之保密義務，而無故洩漏他人或他公司的工商秘密，即會成立本條犯罪，最重可處一年以下有期徒刑。

我國營業秘密法中原本僅有民事責任相關規定，為因應陸續發生幾起矚目案件，在國內科技產業強烈要求下，我國才於 102 年修正營業秘密法，增定相關刑罰規定，希望能夠藉此有效解決營業秘密犯罪問題。新營業秘密法中的刑罰規定，是刑法妨害工商秘密罪的特別規定，其對於侵害營業秘密行為賦予較高刑度。

所謂營業秘密，必須是「生產、銷售或經營之相關資訊」，且應具備「秘密性」、「經濟性」及「合理保護措施」等三項要件[3]，缺一不可。行為人只要以非法取得、無故洩漏或無權使用之方式侵害他人或他公司的營業秘密，就會構成本法第 13 條之 1[4]侵害營業秘密罪，最高得處以五年以下有期徒刑，並得併科高額罰金。

考量外國經濟間諜對於國內產業發展的強烈危害性，營業秘密法第 13 條之 2[5]特別增設加重規定，對於意圖在外國、大陸地區、香港或澳門使用，而涉犯侵害營業秘密的行為，最高得處以十年以上有期徒刑，並得併科高額罰金。另外，依據同法第 13 條之 3 第 1 項反面解釋，本罪為非告訴乃論罪；

---

[2] 臺灣高等法院 78 年度上易字第 2046 號判決。

[3] 營業秘密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

[4] 營業秘密法第 13 條之 1：「意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處五年以下有期徒刑或拘役，得併科新臺幣一百萬元以上一千萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。二、知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密者。三、持有營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密者。四、明知他人知悉或持有之營業秘密有前三款所定情形，而取得、使用或洩漏者。前項之未遂犯罰之。科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之三倍範圍內酌量加重。」

[5] 營業秘密法第 13 條之 2：「意圖在外國、大陸地區、香港或澳門使用，而犯前條第一項各款之罪者，處一年以上十年以下有期徒刑，得併科新臺幣三百萬元以上五千萬元以下之罰金。前項之未遂犯罰之。科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之二倍至十倍範圍內酌量加重。」

換言之，一經查明犯罪事實，即便被害人並未提出告訴，檢察官仍可提起公訴，法院亦可對之進行判決。

在本案中，吳男與原任職公司訂有保密協議，其違背保密義務而透過電子郵件寄送之方式，無故洩漏原任職公司的「某新產品製程檢核表」等機密資料，同時構成刑法妨害工商秘密罪及侵害營業秘密罪，惟優先適用營業秘密法之刑罰規定。此外，吳男洩漏該機密文件予大陸地區公司，其目的乃是希望提供大陸地區公司使用，因而符合營業秘密法第 13 條之 2 的加重規定，其最高得處以十年有期徒刑。

【管理 Tips】

就本案而言，組織對於具有機密資料應採取一定保護措施。除了要求員工簽署保密協議、建立相關資訊安全政策，以及訂定違反資安政策或規範時之內部調查或裁處流程外，平日應對員工加強宣導機密資料保護之重要性，同時也要向員工明確宣布未經授權揭露機密資料所需擔負的責任及後果。

此外，機敏資料如有內容龐雜且分屬不同權責單位管理使用之情形，組織宜針對個別員工職務內容，設定不同的資料存取權限，並配合日常監控機制，定期進行審核，確保所員工所持有的權限與工作職掌相符合，以減少遭不當利用風險。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.7.1.2 聘用條款及條件

組織與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。

A.7.2.3 懲處過程

應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。

A.7.3.1 聘用責任之終止或變更

應對員工及承包者定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並執行之。

A.18.2.2 安全政策及標準之遵循性

管理人員應以適切之安全政策、標準及所有其他安全要求事項，定期審審查其責任範圍內之安全處理及程序的遵循性。

類別：資訊保護【**案號：S1040302**】

駭客竊取財報炒股　美國 SEC 堅決提告

【焦點話題】

美國證券交易委員會(Securities and Exchange Commission，SEC)對駭客集團提出控告，指出駭客集團以竊取企業財報等未公開資訊之方式，協助他人進行股票交易，獲利逾 1 億美元。依據 SEC 之說法，這起國際級詐騙行動約有 32 名被告參與其中，自 2010 年至今，至少竊取 15 萬筆未公開資訊。就犯罪分工而言，初步分析至少有 2 名國外成員入侵美國特定新聞通訊社之系統，短時間內竊取企業財報調整之新聞稿資訊，並立即由其他成員將所竊得之資訊銷售予美國、法國及俄國等買家，方便其利用該資訊進行股市交易。

SEC 同時指出，此駭客集團通常利用代理伺服器偽裝身分，並假冒為新聞通訊社之員工與顧客，以方便進行資訊竊取。另一方面，集團成員也會透過影片證明自己有能力取得未公開財報，做為招攬買家之手段。整起資訊竊盜事件，駭客與買家以分潤方式拆分不法所得之獲利。

【資料來源：iThome104/8/12】

【重點摘要】

1. 企業尚未對外發布的新聞稿與財報資料，且具有經濟價值時，如已採取合理保密措施，應屬企業之營業秘密。
2. 駭客基於營利目的，以不當手段透過媒體竊取企業營業秘密，在我國將負有侵害營業秘密之刑責及民事懲罰性賠償責任。

【法律觀點】

因應知識經濟時代之產業型態轉變，無形資產占企業資產比重益趨增加，依

據美國知名智慧財產機構Ocean Tomo之調查，在 2015 年 1 月美國S&P 前 500 大企業中，無形資產所佔比例已達 84%[1]，因而無形資產之保護變得非常重要。事實上，營業秘密也是我國企業或組織常常用來保護重要無形資產的方式之依據。按營業秘密法(以下簡稱本法)第 2 條之規定，營業秘密相當多元，舉凡方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊等，都可能包含在內。就本案而言，企業提供予新聞通訊社之財報調整相關資訊，通常不是一般人可以知悉的資訊，而該資訊會影響企業價值因而具有經濟價值，在企業或組織採取合理保密措施(例如，以保密契約要求新聞通訊社在指定時間點前必須保密、不得公開)，則該資訊應符合營業秘密之定義，受到本法相關保護。

在我國，駭客倘透過入侵媒體之方式竊取營業秘密，受害企業或組織通常可以透過民刑事程序來處理。在民事責任方面，營業秘密受侵害時，受害組織得請求排除之 [2]，並向加害者請求負損害賠償責任 [3]。而像駭客攻擊這類的故意侵害行為，法院更可以因被害人之請求，依侵害情節，酌定損害額三倍以下之賠償 [4]，此即所謂懲罰性損害賠償。至於刑事責任方面，依據本法第 13 條之 1 第 1 項第 1 款規定，意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者，最高可處 5 年有期徒刑。應補充說明的是，本法第 13 條之 1 第 1 項第 4 款 [5]另訂有收受營業秘

[1] http://www.oceantomo.com/blog/2015/03-05-ocean-tomo-2015-intangible-asset-market-value/

[2] 營業秘密法第 11 條。

[3] 營業秘密法第 12 條第 1 項前段。

[4] 營業秘密法第 13 條第 2 項本文。

[5] 營業秘密法第 13 條之 1 第 1 項規定：「意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處五年以下有期徒刑或拘役，得併科新臺幣一百萬元以上一千萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。二、知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密者。三、持有營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密者。四、明知他人知悉或持有之營業秘密有前三款所定情形，而取得、使用或洩漏者。」

密罪，如本案買家明知該秘密乃駭客入侵他人系統所竊取而仍買受該資訊之情況，此時買家同樣成立本罪，最高可處 5 年有期徒刑。

【管理 Tips】

就本案而言，駭客取得未發布之財報資料，此等資料雖然不是組織內屬於極機密資訊，惟有心人士一樣可以利用相關資訊以侵害各企業或組織，或藉此獲取暴利。為此，組織應明確了解其資料的重要性，除了以往所定義極機密或機密的資料，尚須考量此等資訊是否曾提供其他外部單位進行利用，並依照資訊內容之不同，對外部單位之利用進行要求及監控，以進行不同程度的保護。舉例而言，組織應於內部先行定義各種資料機密等級，在基於業務需求而提供其他單位使用時，應讓取得資料之單位確實了解該資料在本單位之分類等級，以及需要注意之相關事項，以避免資料取得單位在不明瞭相關資料重要性之情形下，造成資料誤用。

就實務面而言，組織所擁有之機敏資料，尤其是尚未公開資料，需要特別保護，除了一般常用的帳號、密碼的控管方式外，對於某些特定資料的存取，還可以考慮加上一次性密碼、生物辨識等方式進行管控、在存取時全程進行錄影，或是要求兩組以上人員同時輸入密碼，作為對機密資料增加管控的方式。換言之，也就是越重要的資料，需要控管的程序也就越多，透過提高使用者存取資料困難度，來管控資料外洩風險。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.8.2.1 資訊之分級

資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

A.8.2.2 資訊之標示

應依組織所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.9.3.1 秘密鑑別資訊之使用

於使用秘密鑑別資訊時，應要求使用者遵循組織之實務規定。

A.13.2.4 機密性或保密協議

宜識別、定期審查及文件化，以反映組織對資訊保護之需要的機密性或保密協議之要求事項。

四、刑法

類別：資訊保護【**案號：S1040401**】

家裝網路監視器遭駭客入侵，OL 春光外洩

【焦點話題】

臺中一名吳姓女子於網路上團購網路監視器，想要監看家中貓咪的動態，於入浴前卻意外發現鏡頭會跟著她轉動，查看後發現該網路監視器之登入人數為 2 人，趕忙把攝影機插頭拔掉並更換密碼。她與當初團購的朋友聯絡，竟發現 14 個買家中有 3 人都有這個現象。

團購業者表示，這可能是因為使用者沒有更改密碼所導致，由於該款網路監視器不會將使用者的數據上傳儲存伺服器，所以也無法追蹤 IP 位置。專家則研判，可能是網路監視器遭駭客侵入，網路上有不少破解監視器的網站，將各國的監視畫面即時播放，其中也包括臺灣地區。警方表示，如果伺服器設在國外，或是用公共 Wi-Fi 登入，實難以追查。

【資料來源：聯合新聞網 104/7/14】

【重點摘要】

1. 以工具或設備窺視、竊聽他人非公開之活動或身體隱私部位，將構成刑法上之妨害秘密罪。
2. 無故輸入他人帳號密碼，入侵他人之電腦或相關設備，將構成刑法上之妨害電腦使用罪。

【法律觀點】

隨著科技發展，網路已經是日常生活不可或缺之一環，不論是搜尋資料、與朋友聊天，甚至是遠端操作的進行，都日漸普及。然而，正因為網路與我們

生活的關係日益密切，我們的日常活動常在一時疏忽下不慎於網路洩露，導致外人透過網路獲悉我們的隱私資訊。

倘若是因自己之行為而使自己的隱私外洩，或許無法怪罪於他人；但如利用網路的特殊性而侵害他人之隱私，則屬於法律所禁止之事項。司法院大法官釋字第 603 號解釋指出：「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障。」故而，刑法乃於第 28 章以下規定妨害秘密罪章，對於侵害他人隱私權之行為予以處罰。

案例中，該名駭客以破解密碼之方式登入吳姓女子之網路監視器，並且利用網路監視器之設備窺視吳姓女子之私生活，顯無正當理由，利用工具或設備窺視、竊聽吳姓女子非公開之活動、言論、談話或身體隱私部位，已違反刑法第 315 條之 1 規定[1]，可能將面臨 3 年以下有期徒刑、拘役或 30 萬元以下罰金之刑事責任。

再參照最高法院 100 年度台上字第 4780 號刑事判決之見解：「就上述妨害秘密罪旨在保護人民秘密通訊自由及隱私權之觀點而言，此項『非公開之活動』之認定，固應著重於活動者主觀上具有不欲其活動遭他人攝錄之意願或期待；但活動者主觀意願如何，外人不易確知，且該項意願未必恆定不變，若單憑活動者主觀上是否具有不公開之意願，作為認定上述犯罪構成要件(即『非公開活動』)之唯一標準，難謂與罪刑法定及法律明確性原則無違。故仍須活動者在客觀上已利用相當環境或採取適當設備，足資確保其活動之隱密性，始能明確化上述構成要件之內容；不能僅以活動者主觀上對其活動有無公開之意願，作為上述罪名所稱『非公開活動』之唯一內涵。」承上，關於「非公開活動」之認定，應參考客觀之環境予以認定。案例中吳姓女子

[1] 刑法第 315 條之 1 規定：「有下列行為之一者，處 3 年以下有期徒刑、拘役或 30 萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

之活動乃發生於自宅，客觀上自具有隱私期待，駭客利用網路監視器予以窺視之行為，即已破壞吳姓女子對自宅之隱私期待，而違反刑法第 315 條之 1 規定。

再者，案例中之駭客是經由破解密碼之方式，登入吳姓女子之網路監視器，因此該名駭客之行為同時違反刑法第 358 條之規定[2]，而可能面臨 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金之刑事責任。

【管理 Tips】

組織內凡以使用者帳號密碼進行管制作業時，包括一般使用者登錄帳號、應用程式使用者帳號等，在使用者開通或啟用階段，就應提醒使用者變更或重設密碼，同時需限定密碼的長度，並且密碼的內容建議包含英文、數字等複雜性密碼，以強化防護功能。

另外，建議組織提醒使用者定期更新密碼，避免密碼因久未修改或過於簡單，藉以提高遭到駭客破解的風險。

若有久未使用的帳號，應檢視有無將帳號加以停用或刪除之必要，避免有心人士利用這些帳號，未經授權取得相關的資訊。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.9.2.4 使用者之秘密鑑別資訊的管理

應以正式之管理過程控制秘密鑑別資訊的配置。

A.9.2.6 存取權限之移除或調整

所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、

[2] 刑法第 358 條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。

A.9.4.3 通行碼管理系統

通行碼管理系統應為互動式，並應確保嚴謹通行碼。

類別：資訊保護【**案號：S1040402**】

法官認定「死人沒有隱私權」 偷拍遺體生殖器傳 LINE 判無罪

【焦點話題】

甲男某日得知同事乙男往生，前往殯儀館探視時，檢察官在驗屍間相驗，甲男未經檢察官及乙男家屬同意下，隨手拍了一張乙男遺體照片，照片中遺體裸露生殖器，並上傳到 LINE「○○群組」給其餘 68 名同事。乙男弟弟後來得知照片一事，憤而依刑法「妨害秘密罪」提告。檢察官主張甲男涉嫌拍攝「檢察官相驗程序」、「乙男身體隱私部位」，還將照片上傳 LINE 群組「洩漏及散布他人非公開之活動照片」，已觸犯刑法妨害秘密罪。甲男庭訊時坦承拍攝死者屍體照片，並將照片上傳至 LINE 群組，目的是讓同事們確認乙男已身亡，並沒有注意到連隱私部位也一同入鏡。

法官認為，甲男僅拍一張遺體照，並未拍攝檢察官相驗過程，且民法第 6 條「人之權利能力，始於出生，終於死亡」，因此甲男拍攝乙男遺體生殖器並散布，並未觸犯妨害秘密罪，判甲男無罪。

【資料來源：自由時報 104/5/7】

【重點摘要】

1. 死亡者不具權利能力，亦無「非公開之活動」可言，因此拍攝遺體本身並將相片上傳至社群網站的行為，尚不構成刑法妨害秘密罪。
2. 偵查程序中依法執行職務人員之隱私，並非偵查不公開保護的對象，尚不屬刑法妨害秘密罪章所欲保障之範圍。

【法律觀點】

我國大法官在解釋文及其理由書內曾經揭示隱私權用語及其內涵，概以隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴、個人主體性及人格發展之完

整，並為保障個人生活私密領域免於國家及他人侵擾及個人資料之自主控制，而認為其為不可或缺之基本權利，受憲法第 22 條保障[1]。所謂權利能力，亦即法律上之人格，因人之死亡而消滅[2]。就刑法而言，隱私法益亦是指自然人的法益，而不及於死者。因此，除有特別規定，刑法各條文所保護之法益主體，均指生存之自然人而言，不包括死者在內[3]。在本案中，因死者隱私部位不等於遺族之隱私，法院認為拍攝已死之乙男，並不涉及自然人的「非公開之活動」，從而甲男拍攝屍體及散布相片之行為，在道德上雖有可非難之處，但在刑法上尚不成立犯罪[4]。然而，在民事責任上，我國法院實務曾認為，人格權係關於人的價值與尊嚴的權利，遺族對於故人敬愛追慕之情，亦可視同人格上利益加以保護，故行為人如不法侵害他人之人格法益而情節重大者，被害人仍可就其非財產上之損害請求損害賠償[5]。

此外，本案甲男於檢察官相驗乙男屍體時，擅自闖入驗屍間拍照，法院認為從照片來看，甲男並未拍攝到檢察官相驗程序，因而並未以刑法第 315 條之 1 第 2 款之無故竊錄他人非公開活動罪，或第 315 條之 2 第 3 項之散布竊錄內容等罪論處[6]。應注意的是，我國法院實務認為，刑事訴訟法上偵查

---

[1] 參照司法院大法官釋字第 603 號解釋。

[2] 民法第 6 條規定：「人之權利能力，始於出生，終於死亡。」

[3] 如刑法第 247 條規定：「損壞、遺棄、污辱或盜取屍體者，處六月以上五年以下有期徒刑。損壞、遺棄或盜取遺骨、遺髮、殮物或火葬之遺灰者，處五年以下有期徒刑。前二項之未遂犯罰之」，一般或認為本條所保護者為尊敬死者之善良風俗，屬社會法益；又刑法第 312 條規定：「對於已死之人公然侮辱者，處拘役或三百元以下罰金。對於已死之人犯誹謗罪者，處一年以下有期徒刑、拘役或一千元以下罰金。」係為保護死者或係遺族的名譽，亦甚有爭議。

[4] 臺灣基隆地方法院 104 年度訴字第 92 號刑事判決。

[5] 參臺灣台北地方法院 96 年度訴字第 2348 號民事判決，又依民法第 195 條第 1 項：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

[6] 刑法第 315 條之 1 規定：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」刑法第 315 條之 2 規定：「意圖營利供給場所、工具或設備，便利他人為前條第一項之行為者，處五年以下有期徒刑、拘役或科或併科五萬元以下罰金。意圖散布、播送、販賣而有前條第二款之行為者，亦同。製造、散布、播送或販賣前二項或前條第二款竊錄之內容者，依第一項之規定處斷。前三項之未遂犯罰之。」

不公開的相關規定，約束對象為檢察官等於偵查程序依法執行職務之人員[7]，其目的除在維護偵查程序順利進行外，也及於犯罪嫌疑人、被害人或利害關係人之名譽、隱私及安全的保護。至於偵查程序中依法執行職務人員之隱私等，則非偵查不公開規定所欲保護的對象，檢察官及檢察事務官執行公務之行為，也不會構成隱私權範疇，因而不屬於刑法妨害秘密罪章所欲保障之範圍。依此見解，甲男拍攝並散布照片內容，縱令涉及檢察官相驗程序時，亦可能不構成前述妨害秘密罪之刑責[8]。

【管理 Tips】

本案中甲男在未經死者家屬同意下，逕行進入驗屍間並拍攝死者隱私部位後上傳至網路。就實務面中，組織對於存放業務機密或敏感資訊之機敏區域的所在，例如電腦機房、檔案室，或是涉及機敏資訊使用的場所等，都需要限制人員的進出，確實落實門禁管控。而可以考慮採取之措施，例如加裝錄影設備、留存人員進出紀錄，或要求出入人員均須配發識別證等。

另一方面，如人員有臨時進入組織機敏區域的需求，組織應要求由授權人員全程陪同；同時，對於其進入機敏區域後所執行的工作，也應事先確認並為必要限制，避免人員進入後，因為不當操作或是作業疏失，導致對組織造成傷害。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.11.1.2 實體進入控制措施

保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。

---

[7] 刑事訴訟法第 245 條第 1 項規定：「偵查，不公開之。」同條第 3 項：「檢察官、檢察事務官、司法警察官、司法警察、辯護人、告訴代理人或其他於偵查程序依法執行職務之人員，除依法令或為維護公共利益或保護合法權益有必要者外，偵查中因執行職務知悉之事項，不得公開或揭露予執行法定職務必要範圍以外之人員。」

[8] 臺灣高等法院臺中分院 103 年度上易字第 1316 號刑事判決。

A.11.1.5 於保全區域內工作

應設計並施行於保全區域內工作之程序。

類別：資訊保護【**案號：S1040403**】

投奔敵營還盜用老東家帳密　房仲被訴

【焦點話題】

甲男原擔任知名房屋仲介直營店副店長，其去(103)年 3 月離職後直接在對街經營房屋仲介加盟店。老東家房仲業者發現去年 3 月至 7 月間，其付費購買之地籍資料網站查詢費用暴增 15 萬元，懷疑帳號密碼遭竊因而向警方報案。

警方循線查出使用該帳密之 IP 位置為甲男開設之新房屋仲介加盟店，惟甲男到案說明時堅稱，其之所以可以登入該付費地籍資料查詢網站，係過去任職時已將帳號密碼儲存於筆電，並非惡意盜用老東家帳號密碼。老東家則主張，甲男過去擔任副店長，故持有地籍資料查詢網站相關帳號密碼，而在甲男離職後已更改地籍查詢網站之帳號密碼，因而應是有內鬼將新帳號密碼提供予甲男使用。老東家要求甲男提供洩密者之身分資料，惟遭甲男拒絕。在雙方不願和解的情況下，檢方依刑法妨害電腦使用罪起訴甲男。

【資料來源：蘋果日報 104/7/28】

【重點摘要】

1. 員工離職後，已無權限使用原任職公司相關資源，故其如以原公司帳號密碼繼續使用資料庫服務，將涉犯刑法無故輸入他人帳密入侵電腦罪之刑責。

2. 公司為妥善維護本身資源，應將資源使用之權限調整納入離職程序環節，並定期更換帳號密碼。

【法律觀點】

近半世紀以來，電腦科技及網路蓬勃發展，與電腦網路相關的新型犯罪型態

隨之出現。基於電腦侵害的犯罪行為態樣不一，其處罰亦有差別。其中，針對無故輸入他人帳號密碼入侵電腦之部分，依據刑法第 358 條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」所謂「入侵」是指未取得他人同意而擅自使用(例如帳密)；至於「無故」，則是指在法律上沒有正當理由(例如，主張依法令行為、業務上正當行為等)。而條文中先後出現二次之「他人」，並沒有限定必須是同一個「他人」。就本案而言，甲男輸入的是老東家的帳號密碼，而入侵的是政府的付費地籍資料網站，仍然可能成立本罪。

在本案例中，甲男既然已經離開原公司，依照社會一般常情，原公司通常不會同意其繼續使用付費查詢地籍資料網站，因此甲男應已無輸入帳號密碼以進入該系統的權限。是以，無論甲男得到新帳號密碼的管道，究竟如同老東家所猜測的由該公司內鬼提供，或是如甲男堅稱是過去任職時將帳號密碼已儲存於筆電當中，只要老東家沒有同意甲男可以繼續使用該帳號密碼，則他輸入該帳號密碼登入地籍資料網站之行為，都會被認定是刑法第 358 所稱之「輸入他人帳號密碼而入侵他人之電腦」。而甲男輸入帳號密碼之行為，乃是出於自己新公司之私用，而這種情形通常無法主張是依法令行為、業務上正當行等，因而仍然構成「無故」。因此，甲男可能構成刑法第 358 條之罪，最高必須面對 3 年有期徒刑。

【管理 Tips】

本案係涉及離職人員使用原公司資源之議題。就實務面而言，當員工職務有異動時，包括人員離職或部門轉調，組織均應將原有權限全部註銷；因此，在部門調動或人員離職的作業程序中，都應該增加資訊單位之管理或確認環節，以達成權限控管之目的，避免人員的工作職掌與使用權限不符。

同時，組織尚需定期執行權限清查作業，將現行使用者帳號全部列出，交相關人員進行覆核，特別是注意防止人員借調、留職停薪、受訓、或離職後卻

仍有使用權限之情形，以確保所配發的權限均為授權使用。此外，組織仍應考量定期進行密碼變更，以避免久未變更密碼，導致其他人員均可利用此組密碼執行相關程式。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.7.3.1 聘用責任之終止或變更

應對員工及約用人員定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效並執行之。

A.9.2.1 使用者註冊及註銷

應實作正式之使用者註冊及註銷過程，俾能指派存取權限。

A.9.2.5 使用者存取權限之審查

資產擁有者應定期審查使用者之存取權限。

A.9.2.6 存取權限之移除或調整

所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。

A.9.4.3 通行碼管理系統

通行碼管理系統應為互動式，並應確保嚴謹通行碼。

木馬駭臺，逾 10 萬支手機每 6 秒回傳個資

【焦點話題】

內政部警政署刑事警察局日前破獲國內首宗智慧型手機簡訊惡意程式詐騙案件。警方調查，從民國 102 年 8 月起，發現國內大批民眾陸續收到詐騙簡訊，例如「聚會相片」、「宅急便通知」、「電費通知」、「快遞簽收單」及「新北市政府警察局通知」等社交工程手法，騙取民眾以智慧型手機點擊連結網址，手機因此遭植入惡意程式，手機會自動發送大量惡意簡訊到其他用戶，造成被害人產生額外電信費用。

電信警察分析中毒的手機發現，詐騙集團利用遭感染手機向電信業者申請小額付款，並操縱該手機發送更多簡訊給通訊錄內親友。民眾除負擔小額付款費用外，還會增加額外大量發送簡訊費用。此惡意程式每隔 6 秒左右更會回傳手機內的個資。因此，民眾若有利用手機登入網路銀行或使用信用卡，帳號密碼也會傳回至詐騙集團架設的伺服器。

警方分析發現，警方發現全臺遭植入木馬惡意程式的智慧型手機最少逼近 10 萬支，單周發送惡意簡訊超過 1,600 萬則，影響範圍相當深遠。

【資料來源：蘋果日報，104/10/12】

【重點摘要】

1. 為降低手機資訊安全風險，民眾本身亦須達到某程度注意義務，避免下載不明軟體或點選簡訊提供的可疑網址，並定期更新手機防毒軟體。
2. 駭客撰寫並散布惡意程式，以入侵他人電腦或其相關設備，除涉及我國刑法妨害電腦罪章以外，亦可能同時構成詐欺、竊取他人營業秘密或違法蒐集他人個資情事等，而負有刑責。

【法律觀點】

隨著科技日新月異，智慧手機成為民眾日常生活中不可或缺的工具，無論通訊、行動支付、透過行動應用程式訂票，或線上查閱資料等，都加深民眾對於手機的依賴程度。然而，行動網路與應用服務趨於普及下，也提升手機感染病毒或遭到惡意程式攻擊的威脅，以致民眾可能因資料遭到竊取，或遭犯罪集團利用手機發送社交詐騙、小額支付驗證等簡訊，而受有損害。因此，為降低民眾手機資訊安全風險，不僅有賴行動應用程式開發者或服務供應商強化行動版作業環境的安全性，提供適當安全程度，避免民眾在使用過程，資料易遭犯罪集團擷取或破解；另一方面，民眾本身亦須擔負某程度注意義務，避免下載不明軟體或點選簡訊提供的可疑網址，並定期更新手機防毒軟體。

就駭客撰寫並散布惡意程式，以入侵他人電腦或其相關設備，除涉及我國刑法妨害電腦罪章以外[1]，視駭客竊取手機資料的內容，更可能同時構成以不法手段竊取他人營業秘密[2]，或不法蒐集他人個資情事[3]等而負有刑責。此外，駭客以木馬程式控制他人手機，並以他人名義偽造同意申辦電信小額付款或確認支付款項之電磁紀錄，亦可能構成刑法上偽造文書；另，駭客以社交工程方法寄發簡訊，誘使民眾點選後誤為提供帳號密碼或直接匯付款項

[1]刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」、「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」同法第 362 條：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

[2]營業秘密法第 13-1 條：「意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處五年以下有期徒刑或拘役，得併科新臺幣 100 萬元以上 1000 萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。」

[3] 個人資料保護法第 41 條：「違反...第 19 條...足生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」

時，尚可能分別構成詐欺取財或詐欺得利罪[4]，若駭客截取民眾收到的帳號密碼開通簡訊，或利用民眾回傳的驗證碼等資料，輸入電腦設備以執行線上授權交易或轉帳，而造成民眾存款金額減少，則另可能構成不法偽造紀錄取得他人財物罪[5]。鑒於我國刑法對此類犯罪手法已有相關規範，有心人士應考量法律風險，避免觸法。

【管理 Tips】

現今社交工程詐騙的管道，已經從傳統的電子郵件，逐步演進到智慧型手機及社群軟體。雖然利用不同的平台與媒介，但基本原理都還是一致，藉由人們的好奇心及對科技的不了解，進而騙取所需的資料，如利用手機簡訊，騙取民眾點選不當連結發送大量簡訊。

組織應將相關社交工程的案例，藉由教育訓練的方式，讓同仁能夠提高警覺，對於來路不明的郵件或是簡訊，不要任意的點選或開啟。如果認為有必要保存的資訊，可以在網路上尋找相關的連結後再進入，而不要直接連結其所附的路徑。

此外，組織應明確的定義，未經授權不得任意安裝軟體。組織內所有軟體的安裝，都必須事先經過測試，確認軟體版本正確以後才可以進行安裝，以防止不肖人員藉由程式的安裝，進而取得未經授權的資料。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之約用人員，均應接受與其工作職能相關的組織政策

[4] 刑法第 339 條：「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處 5 年以下有期徒刑、拘役或科或併科 50 萬元以下罰金。以前項方法得財產上不法之利益或使第三人得之者，亦同。前二項之未遂犯罰之。」

[5] 刑法第 339-3 條：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人之財產者，處七年以下有期徒刑，得併科 70 萬元以下罰金。以前項方法得財產上不法之利益或使第三人得之者，亦同。前二項之未遂犯罰之。」

及程序之適切認知、教育及訓練，並定期更新。

A.12.5.1 對運作中系統之軟體安裝

應實作各項程序，以控制對運作中系統之軟體安裝。

A.12.6.2 對軟體安裝之限制

應建立並實作使用者安裝軟體之管控規則。

資訊保護【**案號：S1040405**】

勒索軟體 CryptoWall 3 已造成 3.25 億美元損失

【焦點話題】

網路威脅聯盟(Cyber Threat Alliance, CTA)在 2015 年 11 月發表一份深入研究 CryptoWall 3 的報告。勒索軟體 CryptoWall 3 有兩大感染途徑，分別是網路釣魚郵件與攻擊套件，在 7 萬個感染案例中約有三分之二是因網路釣魚郵件而受到感染，另有 30%則是駭客透過攻擊套件攻擊受害者。入侵使用者裝置的 CryptoWall 3 會建立與遠端命令暨控制伺服器 C&C(Command and Control Server, C&C)的連線，傳送裝置資訊至 C&C 並加密裝置上的檔案，駭客通常要求受害者支付比特幣，價格從數百美元到數千美元不等，萬一受害者未於指定的時間內匯款，駭客即會將贖金提高到一倍。估計操作 CryptoWall 3 的駭客集團已獲利 3.25 億美元，主要的受害者位於北美市場。

針對加密勒索軟體目前尚未有有效解法，一旦資料被勒索軟體加密，以目前的解密技術及設備能量是無法在能接受的時間範圍解密成功。所以除了確實備份資料外，應從資安意識教育訓練著手。因目前感染加密勒索軟體的途徑，大多是使用者被社交工程郵件攻擊，或是自行在網路上點擊不當惡意連結。唯有提升人員資安意識，方能有效降低被攻擊成功的機率。

【資料來源：技術服務中心整理，104/11/17】

【重點摘要】

1. 駭客撰寫、散布勒索軟體此類惡意程式，並利用此軟體要脅被害人交付財物，可能構成刑法上入侵電腦設備、變更電磁紀錄及恐嚇取財罪。
2. 因應勒索軟體根本之道為強化使用者資安意識，並配合定期資料備份，以

提升本身資料遭到惡意毀損或滅失時之因應能力。

【法律觀點】

駭客攻擊手法日新月異，除入侵電腦系統竊取資料或癱瘓系統服務以外，目前駭客更發展出勒索軟體，以社交工程或其他方式誘騙使用者下載該軟體後，就能遠端操控使用者所屬裝置並將該裝置內的資訊進行加密，導致使用者無法存取或使用，而必須依駭客指示交付財物換取解密，以「贖回」檔案資訊。若使用者無法破解又不願付款，或駭客取款後未依約解密時，使用者恐怕無法再使用該資訊或必須重建資訊系統，而蒙受重大損失。

就駭客撰寫並散布勒索軟體此類惡意程式，以入侵他人電腦或其相關設備，或變更檔案內容致無法讀取時，除涉及我國刑法妨害電腦罪章以外[1]，駭客基於營利目的，透過勒索軟體造成對於使用者所保有資訊完整性與可用性的威脅，迫使使用者交付財物，亦可能同時構成刑法上恐嚇取財罪[2]，而負有刑責。

目前勒索軟體受害人遍及個人與企業用戶，然而鑒於勒索軟體付款機制精密而難以追查，且自行解密恐耗費時日而緩不濟急，因此根本之道仍是強化使用者資安意識，避免下載可疑軟體檔案，並配合定期資料備份，以提升本身資料遭到惡意毀損或滅失時之因應能力。

[1]參刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」、「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」，同法第 362 條：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」、同法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

[2] 刑法第 346 條：「意圖為自己或第三人不法之所有，以恐嚇使人將本人或第三人之物交付者，處 6 月以上 5 年以下有期徒刑，得併科 1000 元以下罰金。以前項方法得財產上不法之利益，或使第三人得之者，亦同。前二項之未遂犯罰之。」

【管理 Tips】

勒索軟體通常會將檔案加密，導致檔案無法正常使用。為防範勒索軟體對於組織之危害，在日常資安教育訓練中，就應該對組織內的同仁加強宣導，無論電子郵件、即時通訊或是社交軟體之來源管道為何，對於陌生的訊息都必須避免任意開啟，而在未經查證下也應該儘量避免直接點選所附的連接，因為這些錯誤的方式都是容易遭受勒索軟體感染的原因。

在日常作業層面，組織應定期檢視現有的備份作業是否完整與依照既定計畫進行備份。此項工作如能確實執行，當遭受勒索軟體攻擊時，便能迅速將舊有的資料復原，避免因資料缺乏導致組織之正常作業停擺。而因應這種新型態的攻擊模式，組織應定期接收相關的技術更新，明瞭目前常用的攻擊方式，以及其對於企業影響之層面與程度。如發現資安管理措施有需要強化的地方，建議組織及早進行部署，或是增加監控的頻率，以確保組織資訊效能可正常運作。

【相關標準】

ISO 27001：2013(CNS 27001)

A.7.2.2.2. 資訊安全認知、教育及訓練

組織所有員工及相關之約用人員，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練、並定期更新。

A.12.3.1 防範資料漏失

應依據議定之備份政策，定期取得資訊、軟體及系統影像備份，並測試之。

A.17.2.1 資訊處理設施之可用性

應對資訊處理設施實作充分之多重備援，以符合可用性要求。

資訊保護【**案號：S1040406**】

詐騙集團盜帳號，知名網路討論區籲改密碼

【焦點話題】

知名網路討論區中，提供買賣二手商品的「市集」專區，近日疑遭詐騙集團刊登多項假商品販賣訊息，站方前天緊急發出公告，表示近期不少網友帳號遭盜用，除新增機制防堵，也提醒會員更改所使用的帳號密碼。

根據知名網路討論區之公告，該站認為遭盜帳號的會員，是因和其他網站使用相同的帳號密碼，因其他網站帳號密碼外洩，才導致該站的帳號也被盜用。該網站已推新制防堵，會員若要在「市集」刊登販賣商品資訊，需登錄手機門號以簡訊驗證才能刊登商品。

資安廠商顧問表示，盜取帳號密碼最常見是用釣魚手法，藉發送偽造的官方信件等騙取帳號密碼，或在用戶電腦中植入木馬程式側錄，提醒民眾注意。

【資料來源：蘋果日報，104/10/25】

【重點摘要】

1. 使用者應妥善保管帳號密碼及定期變更，並注意網路安全，避免帳號密碼遭有心人士利用。

2. 業者對於網站應採取符合當時科技或專業水準可合理期待之安全性，以降低使用者帳號密碼被盜用，並有效控制損害發生風險。

【法律觀點】

在虛擬的網路世界裡，為辨識並確認使用者身分，多係由使用者於網站上註冊帳戶，並設定密碼後，作為登入之驗證機制。由於使用者登入不同網站均須輸入其於該網站註冊之帳號密碼，許多使用者為管理方便，常常將所有網站之帳號與密碼設定為相同，以避免忘記密碼而無法登入網站，造成一旦有

心人士透過釣魚、植入木馬程式或社交工程等方式取得他人帳號密碼後，即可使用該帳號密碼登入其他網站，進而盜用使用者身分而為不法行為，而造成其他民眾損害。

本件案例中，行為人盜用使用者的帳號密碼登入該知名網站討論區，不論行為人取得該帳號密碼之來源為何，在未獲得使用者授權或沒有正當理由之情況下，均屬於刑法第 358 條[1]所指「無故輸入他人帳號密碼，而入侵他人之電腦或相關設備」之情況，而涉有刑事責任。另行為人盜用使用者帳號密碼而於討論區刊登多項假商品訊息，因行為人係利用得識別使用者之代號，佯以刊登相關訊息，亦構成偽造私文書罪[2]。

有關知名網站討論區之責任，依我國實務見解，如業者已善盡各項告知與提醒義務，並提供各項防護措施，防範駭客入侵，而得認符合當時科技或專業水準可合理期待之安全性時，對於使用者之損害即不負賠償責任[3]。是以，使用者之帳號密碼被盜用雖非網站業者所導致，惟如網站業者未採取符合當時科技或專業水準可合理期待之安全性時，恐有應負損害賠償責任之虞。雖然如此，使用者仍應妥善保管帳號密碼及定期變更，並應注意網路安全性問題，避免帳密遭盜用所衍生之爭議。

【管理 Tips】

本案使用者因沒有正確使用密碼，導致有心人士取得帳號密碼而移做其他使用。就實務作業而言，使用密碼管控是最基本的資訊安全控制措施，除了使

---

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

[2] 刑法第 210 條：「偽造、變造私文書，足以生損害於公眾或他人者，處 5 年以下有期徒刑。」、第 220 條第 2 項：「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。」

[3] 士林地方法院 94 年湖簡字第 299 號判決意旨：「本件被告在原告聲稱帳號被盜情事之前已盡各項告知及提醒義務，並提供各項防護措施，防範駭客入侵，更積極地以『終極密碼行動』認證原告之基本資料及密碼，使該帳號僅有知悉密碼、帳號之原告方能通過認證而登入遊戲，故應認被告於提供線上遊戲服務時，業已符合當時科技或專業水準可合理期待之安全性。是以，原告依據線上遊戲契約、消費者保護法第 7 條、民法第 184 條等規定，請求被告賠償 131,500 元，即無理由。」

用者帳號至少需要使用密碼登錄外，同時還需要限制密碼最少長度。此外，密碼最好是文字、數字夾雜使用，並定期進行密碼變更作業，以避免因為密碼過於單純，或是久未更新，導致密碼遭盜用。

組織針對密碼管控，最好的方式就是在伺服器或應用系統上進行設定，利用自動化的方式強迫使用者使用強度較高的密碼。另，組織除應制定與公布相關密碼使用規則，尚需提醒同仁，不可將帳號、密碼分享給其他人使用，或是將使用者帳號密碼張貼在電腦四周，以避免密碼外洩，並且不要利用相同一組的帳號密碼，登錄於不同的應用系統環境，以避免導致其他的應用系統遭有心人士使用。

【相關標準】

ISO 27001：2013(CNS 27001)

A.9.1.1 存取控制政策

存取控制政策應依據營運及資訊安全要求事項、建立文件化及審查之。

A.9.2.1 使用者註冊及註銷

應實作正式之使用者註冊及註銷過程，俾能指派存取權限。

A.9.3.1 秘密鑑別資訊之使用

於使用秘密鑑別資訊時，應要求使用者遵循組織之實務規定。

A.10.1.1 使用密碼式控制措施之政策

應發展及實作政策，關於資訊保護之密碼式控制措施的使用。

駭客以監視器攝影機組成殭屍網路，發動 DDoS 攻擊

【焦點話題】

資安業者 Imperva 發現一個由監視器攝影機組成的殭屍網路，而且駭客利用此一殭屍網路，針對某一雲端服務發動了分散式阻斷服務攻擊(DDoS)，突顯了物聯網時代所面臨的安全問題。

連網的監視器攝影機是目前物聯網殭屍網路最常見的媒介，因為監視器攝影機可說是目前最普遍的物聯網裝置之一。此次 Imperva 所發現的監視器攝影機殭屍網路約由 900 台裝置組成，他們攻擊一個大型雲端服務中較少被使用的服務，該服務在全球約有數百萬用戶，而尖峰攻擊流量為每秒 2 萬次的請求。

業者建議消費者在安裝路由器、無線基地台或是監視器攝影機時，別忘了更改裝置的預設密碼，以防遭駭客輕易破解。

【資料來源：iThome，104/10/23】

【重點摘要】

1. 駭客以殭屍網路癱瘓網路設備，致他人受損害時，恐構成無故干擾他人電腦罪而負有刑事責任。
2. 服務供應商提供物聯網相關應用服務時，應注意資訊安全保護，尤其是密碼設定或變更，避免駭客癱瘓網路而中斷服務，而造成損害。

【法律觀點】

所謂分散式阻斷攻擊(Distributed Denial of Service attack, DDoS)，乃是利用分散於不同地方的多部電腦主機，發送大量偽造來源地址的封包，癱瘓受害者所在的網路電腦主機伺服器，導致無法服務正常的使用者。此種攻擊

手法的目的不在於篡改或竊取資料，而是癱瘓系統主機致其無法正常作業，過去即曾有多家電子商務業者遭到攻擊而癱瘓。

近年來物聯網(Internet of Things, IoT)掀起另一波革命。物聯網透過高度整合的全球網路，把所有事物與人全部連結在一起，並透過感測器與軟體連接到物聯網平台，這些資訊成為寶貴的巨量資料，並造就許多新興商業模式，帶來更便利的生活。例如，透過智慧型手機可以隨時控制家中的電器，在炎熱的夏天即可在抵達家門前開啟冷氣。

然而，物聯網的發展，也面臨資訊安全的威脅，本案例駭客以殭屍網路癱監視攝影機，即突顯物聯網所面臨之資訊安全議題。依我國刑法第 360 條規定[1]，無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致公眾或他人發生損害時，將構成無故干擾電腦罪。若因中斷物聯網服務，而導致他人受有損害時，亦應負民事損害賠償責任[2]。

物聯網的發展，雖為許多創新商業模式帶來商機，但在發展的過程，仍應注意資訊安全保護，並應採取符合科技水準的保護措施，以避免遭受惡意攻擊致服務中斷，而造成損害並影響客戶權益。

【管理 Tips】

在物聯網時代，除了作業環境或是應用系統外，權限控管的範圍也必須擴大到與網路相連接的各項設備。因外，在安裝路由器、無線基地台、監視錄影機或其他相關設備時，應考量是否設置密碼作為控管措施。而對於廠商所提供的預設密碼，組織務必記得更改，在預設密碼之變更上，亦應儘量使用較為複雜的密碼規則。因為預設密碼如未變動或採取過於簡單的密碼規則，都會使有心人士容易取得或破解密碼之方式，因而對於此一環節需要特別審慎留意。

---

[1] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[2] 民法第 184 條第 1 項：「因故意或過失，不法侵害他人之權利者，負損害賠償責任。故意以背於善良風俗之方法，加損害於他人者亦同。」

【相關標準】

ISO 27001：2013(CNS 27001)

A.9.2.3 具特殊存取權限之管理

應限制及控制具有特殊存取權限之配置及使用。

A.9.4.3 通行碼管理系統

通行碼管理系統應為互動式，並確保嚴謹之通行碼。

五、醫師法

類別：資訊保護【**案號：S1040501**】

美國食藥署發布指引，釐清對於行動醫療應用程式之管理態度

【焦點話題】

鑒於行動應用程式發展快速，與其對於公眾帶來的潛在效益與風險，美國食品藥物管理署(US Food & Drug Administration)於104年2月發布關於行動醫療應用程式的指引文件[1]，以提供製造商、銷售商及其他業者了解其管理方式。美國食藥署將醫療應用程式分為三大類，一是不符合聯邦食品、藥物及化妝品法下關於「裝置」(device)定義者，食藥署就此類應用程式尚無管理權限；二是符合該法關於裝置定義，但對於公眾僅有低度風險，三是應用程式運作非如預期時，其功能對於病患安全將造成風險者，後兩類將受到食藥署的監督審查。

美國食藥署指出，依說明或廣告文件等內容，若應用程式顯示用於診斷、治癒、減輕症狀或預防疾病時，就會認定屬於裝置。但為避免過度管制影響產業創新，食藥署對於僅有低度風險的醫療應用程式，例如提供病患管理並追蹤健康資訊的簡易工具、提供病患取得健康情形或治療資訊等應用程式，在執行上將裁量從寬管理，以降低製造商行政遵循成本，並建議相關製造商在設計開發與修正過程，應遵循良好實務守則。

【資料來源：InformationWeek 104/3/3】

[1] US Food & Drug Administration, Mobile Medical Applications：Guidance for Industry and Food and Drug Administration Staff, Document issued on February 9, 2015, available at http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm263366.pdf (latest visited:2015/11/4)

【重點摘要】

1. 我國衛生福利部參考歐美規範，發布「醫用軟體分類分級參考指引」，以供產業界開發產品、申請查驗登記之參考，並讓使用單位了解醫用軟體之管理。

2. 程式開發商或服務供應商應確保醫療行動應用程式，符合當時科技或專業水準可合理期待之安全性，並對個資之保存採取適當安全維護措施。

【法律觀點】

在健康照護領域，行動應用程式為促進智慧照護服務的重要關鍵，無論是強化各種醫療器材運作效率或品質管控，建立行動裝置與應用服務平台間的連結機制以延伸服務範圍，或是提供病患以該行動應用程式分析健康資料等，都可見行動應用程式扮演重要角色。因此，服務供應者從行動應用程式的開發、運作、修正到終止服務等各生命週期階段，均應確保其安全性與可用性，以避免影響使用者權益。我國醫療器材管理辦法第 2 條規定，原本即將醫療器材依據風險程度分為三級[2]，而在藥事法授權訂定之藥物優良製造準則中，亦強調醫療器材之安全性議題，此對於新興醫用軟體類之醫療器材也有適用。衛生福利部為說明新興醫用軟體之分類分級管理，並提供產業界開發產品、申請查驗登記之參考，即參考歐美等國的管理規範，於 104 年 4 月 14 日發布「醫用軟體分類分級參考指引」[3]，將醫用軟體[4]依「是否符合藥事法第 13 條醫療器材定義」、「是否宣稱具診斷、治療功能或協助診斷、治療」等原則，判斷是否納入醫療器材進行管理。例如依該

---

[2] 醫療器材管理辦法第 2 條：「醫療器材依據風險程度，分成下列等級：第一等級：低風險性。第二等級：中風險性。第三等級：高風險性。」

[3] 衛生福利部食品藥物管理署公告「醫用軟體分類分級參考指引」，查詢自 http://www.fda.gov.tw/TC/siteListContent.aspx?sid=310&id=12109&chk=e9332177-b2b6-4823-90f9-9cbfb331efdb&param=pn%3D1%26sid%3D310#.VjsB67crLIU (最後檢索日：2015/11/5)

[4] 該指引所稱「醫用軟體」，泛指蒐集、儲存、分析、顯示、轉換人體健康狀態、生理參數、醫療相關紀錄等處理軟體，使用場所涵蓋醫療院所、個人居家使用及遠距醫療照護，而「醫用軟體」判定屬醫療器材管理者，在此則稱為「醫療器材軟體」。

指引說明，行動應用程式若作為一般民眾日常生活的健康管理用途，例如顯示、傳輸、保存個人健康指標的測量值，或執行飲食紀錄、熱量消耗、偵測步數或動作週期等，因未涉及疾病之診斷或治療，故不以醫療器材列管；但如該軟體可用以處理醫療器材產生的資料，如電子血壓計、血糖計等醫療器材附屬專用之訊號處理或傳輸軟體，則屬醫療器材。

部分醫療相關行動應用程式，在我國雖無庸依醫療器材管理辦法向主管機關申請查驗，但若該行動應用程式係直接提供服務予消費者時，依我國消費者保護法規定，程式開發商或服務供應商應確保此類應用程式，在提供服務時，符合當時科技或專業水準可合理期待之安全性，否則將對消費者負有損害賠償責任[5]。再者，若行動應用程式涉及蒐集使用者可得識別的個人資料時，服務供應商依個人資料保護法規定，應採取相當技術上適當安全維護措施[6]，例如具有身分檢核機制以防止未經授權者存取，或是有相當防護技術以避免駭客透過該應用程式竊取使用者資料等。

【管理 Tips】

當資訊科技跨足不同產業時，組織需要注意符合相關法令，以及考量到未來執行狀況。組織針對資訊業務新種應用，建議將相關要求一併列入資訊安全考量範圍中，以行動醫療應用程式為例，醫療器材必須充分考量安全性議題，而資訊安全乃是其中重要環節之一；因此，對於行動醫療應用程式之研發與應用，從最基礎的權限管控開始，到程式開發、撰寫、檢測及修補，乃至於網路安全，這些都是在行動裝置應用時需要加以考量的面向。另組織宜建立程式撰寫的規範，此規範包括各種平台程式撰寫規則，以及所禁止使用的程式語法，以防止 SQL Injection 等較為常見的網路攻擊方式，並須在規範中要求開發人員依照撰寫規則進行程式開發。關於程式開

[5] 消費者保護法第 7 條第 1 項：「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。」

[6] 個人資料保護法第 27 條第 1 項：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

發，現行的程式規範除了參考軟體工程建置架構外，同時還會考量駭客常會使用的攻擊方式，或是已發現的程式漏洞，避免相關語法的撰寫。對於需要更新的程式，也應經過檢測後才可以執行程式變更。同時，要針對目前新興科技，適時地修正相關規定及內容。

此外，組織應對資訊作業的運用定期實施教育訓練，除了需要讓一般業務承辦人員知道未來發展的走向，也要讓相關作業人員知道資訊科技的管控及注意事項。組織惟有及早將資訊安全概念傳遞給相關人員，並且適時調整，才能使新興科技發揮到最大的功用。

【相關標準】

ISO 27001：2013(CNS 27001)

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之約用人員，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.14.2.1 保全開發政策

應建立軟體及系統開發之規則，並應用至組織內之開發。

A18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

六、智慧財產權相關法律

類別：資訊保護【**案號：S1040601**】

影片收進播放清單違法？智財局要找業者聊聊

【焦點話題】

台北市一名張姓男大學生在 103 年 10 月間，把在影音網站 YouTube 看完的國片電影「聽說」及「天后之戰」影片，收藏進播放清單，影片的兩家代理商發現後，控告張姓男大學生違反著作權法。後經士林地檢署認為張姓男大學生並無違法，但張姓男大學生因纏訟而苦，在不起訴處分前，即以新台幣 2 萬元與代理商和解，最後以代理商撤告終結。

經濟部智慧財產局(以下簡稱智財局)說明，影片來源是正版或盜版難以分辨，觀看盜版影片及把影片加入播放清單的網友並沒有重製，也沒有做新的公開傳輸行為，因此不違反著作權法。

獲知媒體報導後，代理商於臉書上發文指責智財局毀掉音樂產業，並聲明強調沒有濫告張姓男大學生，對此智財局表示，近期內將找兩家代理商好好溝通正確的著作權法概念。

【資料來源：自由時報 104/5/26】

【重點摘要】

1. 網友利用影音網站服務製作播放清單之行為，係以超連結方式提供網站上的影音檔案，不涉及重製或公開傳輸他人著作。
2. 影片遭網友非法上傳至影音網站的著作權人，得依著作權法規定向影音網站要求取下，以降低侵害。

【法律觀點】

影音網站匯集眾多種類影片及音樂檔案，為一龐大的影音資料庫，而成為廣受網路使用者歡迎的娛樂管道。又為了讓使用者依照個人喜好及需求播放影音，影音網站更提供使用者自行製作播放清單的功能，使得影音服務使用上更為多元。然而，使用者「製作」播放清單之行為，是否屬於著作權之重製或公開傳輸，或是進一步侵害著作權，仍有爭議。

本件張姓男大學生將電影收藏至自己的播放清單中，而被代理商控告侵害重製權與公開傳輸權，違反著作權法。然而，民眾單純於影音網站點選瀏覽影音，並無涉及重製與公開傳輸之利用著作行為，而不會有侵害著作財產權的問題。而播放清單之功能，其性質上是屬於以超連結方式提供網站上的影音檔案，同樣不會涉及重製與公開傳輸之利用行為。此外，一般播放清單之製作者，大部分是為自己聆賞之方便而將相關影片連結納入其播放清單，並不具有向公眾提供之主觀意思，亦難以認定使用者有幫助公開傳輸之意思。但如果使用者是自己主動將盜版影片傳輸至影音網站，或是明知為盜版影音，主觀上意圖向大眾提供該影音而將其傳輸至影音網站等行為，主管機關認為此行為將涉及重製、公開傳輸等利用行為，而有侵害他人著作財產權之可能[1]。

為了鼓勵網路服務提供者與著作財產權人合作，共同遏止網路侵權，著作權人得循著作權法第 6 章之 1 規定建構的「通知及取下」機制，要求網路服務提供者迅速移除流通之侵權資料，以降低侵權資料在網路上之流傳對於著作財產權人造成之損害。以提供部落格、討論板、網路拍賣或影音瀏覽等服務的資訊儲存服務提供者為例[2]，依著作權法第 90 之 7 條規定，如其符合對使用者涉有侵權行為不知情，未直接自使用者之侵權行為獲有財產上利

[1] 經濟部智慧財產局 104 年 1 月 28 日「以瀏覽或播放清單方式觀賞 YOUTUBE 網站影片之著作權問題說明」新聞稿、104 年 5 月 29 日電子郵件字第 1040529 號函。

[2] 著作權法第 3 條第 1 項第 19 款：「十九、網路服務提供者，指提供下列服務者：.....(三) 資訊儲存服務提供者：透過所控制或營運之系統或網路，應使用者之要求提供資訊儲存之服務者。」

益，且經著作權人或製版權人通知其使用者涉有侵權行為後，立即移除或使他人無法進入該涉有侵權之內容或相關資訊者等要件者，即可免除民事賠償責任[3]。從而，此類網路服務提供者藉由配合著作財產權人取下侵權資訊之行為，亦可免除與上傳侵權資料的網友負共同侵權責任之風險，藉此落實網路環境之著作權保護。

【管理 Tips】

就本案而言，組織應就使用第三人著作權等部分，建立內部政策及作業規範，包括權利範圍、權利歸屬、合法使用、違反時之處理或懲處流程等議題。

鑒於網路資源取得日益便利與豐富下，組織在下載或利用各樣網路著作時，應先透過內部作業程序進行，例如確認智慧財產權歸屬，並釐清使用方式是否符合著作權人授權範圍等，以避免負有侵害他人智慧財產權之法律責任。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.18.1.2 智慧財產權

應實作適切程序，以確保遵循與智慧財產權及專屬軟體產品使用之相關之法律、法令、法規及契約的要求事項。

[3] 著作權法第 90 之 7 條：「有下列情形者，資訊儲存服務提供者對其使用者侵害他人著作權或製版權之行為，不負賠償責任：一、對使用者涉有侵權行為不知情。二、未直接自使用者之侵權行為獲有財產上利益。三、經著作權人或製版權人通知其使用者涉有侵權行為後，立即移除或使他人無法進入該涉有侵權之內容或相關資訊。」著作權法第 90 之 4 條第 1 項：「符合下列規定之網路服務提供者，適用第九十條之五至第九十條之八之規定：一、以契約、電子傳輸、自動偵測系統或其他方式，告知使用者其著作權或製版權保護措施，並確實履行該保護措施。二、以契約、電子傳輸、自動偵測系統或其他方式，告知使用者若有三次涉有侵權情事，應終止全部或部分服務。三、公告接收通知文件之聯繫窗口資訊。四、執行第三項之通用辨識或保護技術措施。」

類別：資訊保護【**案號：S1040602**】

網路公布搭訕信件內容，女子要賠搭訕男子 1 萬 1

【焦點話題】

一名女子逛書店回家後，在包包內發現一張寫有 e-mail 和想要認識她等語的紙條，女子好奇而寫信問對方是誰。男子自稱「小帥帥」，詢問女子的住處和基本資料，女子拒絕回答，對方卻以許多情緒性言語回應。女子被罵的莫名其妙，因此在 PTT 發表「在高雄遇到神經病！！」一文，附上紙條照片、男子的 e-mail 帳號與 e-mail 的內容。後來有網友提供在其他書局發生過同樣事件的影片，女子也一併加入其發表的文章，提醒其他女性小心。男子發現後，陸續對女子與網友提出公然侮辱、殺人未遂等刑事告訴，但均不成立。男子又另提民事訴訟，主張女子侵害其人格權、著作人格權及著作財產權。一般人格權部分，法院認為女子是對可受公評之事發表評論，發表之內容無法特定男子是何人，亦未直接披露足以識別其個人之資料，並沒有侵害男子之人格權。但侵害著作權方面，法院認為電子郵件是具有原創性之文字著作，受著作權法之保護。女子公開電子郵件侵害男子著作人格權及著作財產權，應負損害賠償責任，並判賠新台幣 1 萬 1 千元。

【資料來源：蘋果日報 104/9/16】

【重點摘要】

1. 著作只要有最低程度的創意，可認為作者的精神作用已達到相當程度，足以表現其個性或獨特性，著作權法即予保護。
2. 信件具有著作權，如為非法公開或未經當事人同意而公開，恐違反著作權法規定而負有民事責任。

【法律觀點】

依著作權法第 3 條第 1 項第 3 款規定，著作的定義是「屬於文學、科學、藝術或其他學術範圍之創作」，又依經濟部智慧財產局對於著作權的保護提出「四必一沒有」的五個要件[1]：(1)必須是人類精神力作用的成果；(2)必須經「表達」而外顯；(3)必須獨立創作且具有「創作性」：只要有最低程度的創意，可認為作者的精神作用已達到相當程度，足以表現其個性或獨特性，就給予保護，此為「美學不歧視原則」；(4)必須屬於文學、科學、藝術或其他學術範圍：指相對於「實用性」，創作需具有「文藝性」，價值在所不論；(5)不屬於著作權法第 9 條的類型[2]。以這五個要件來檢視書信，不論是著名作家還是普通人寫的信，基於美學不歧視原則，都屬於著作的範疇。本案法院即係認為電子郵件將男子思想表現出來，顯現其個性或獨特性，具有最低程度的創意，是具有原創性的著作。

因此，在本案中男子對電子郵件享有著作權的保護。依著作權法，若是侵害著作人格權將依第 85 條負損害賠償責任[3]，侵害著作財產權則依第 88 條負損害賠償責任[4]。雖然本案的被告女子主張她是依著作權法第 52 條[5]及第 55 條[6]規定的合理使用，但這兩條均以「已公開發表之著作」為要件。本

---

[1] 經濟部智財局，著作權基本概念，https://www.tipo.gov.tw/ct.asp?xItem=219594&ctNode=7561&mp=1，(最後瀏覽日期：2015 年 10 月 5 日)

[2] 著作權法第 9 條第 1 項：「下列各款不得為著作權之標的：一、憲法、法律、命令或公文。二、中央或地方機關就前款著作做成之翻譯物或編輯物。三、標語及通用之符號、名詞、公式、數表、表格、簿冊或時曆。四、單純為傳達事實之新聞報導所作成之語文著作。五、依法令舉行之各類考試試題及其備用試題。」

[3] 著作權法第 85 條第 1 項：「侵害著作人格權者，負損害賠償責任。雖非財產上之損害，被害人亦得請求賠償相當之金額。」

[4] 著作權法第 88 條第 1 項前段：「因故意或過失不法侵害他人之著作財產權獲致版權者，負損害賠償責任。」

[5] 著作權法第 52 條：「為報導、評論、教學、研究或其他正當目的之必要，在合理範圍內，得引用已公開發表之著作。」

[6] 著作權法第 55 條：「非以營利為目的，為對觀眾或聽眾直接或間接收取任何費用，且未對表演人支付報酬者，得於活動中公開口述、公開播送、公開上映或公開演出他人已公開發表之著作。」

案e-mail僅在兩造之間傳遞，並未公開發表[7]，亦無同法第 15 條第 2 項的推定公開發表的情形[8]，因此法院認為女子公布信件內容非屬合理使用。

本案判決一出受到許多外界的批評，也有人質疑保障此類信件的內容是否符合著作權法保護文化發展的立法目的，惟本案當事人已表示考慮提起上訴，故仍有待觀察二審法院見解。

【管理 Tips】

就本案而言，信件是受到著作權法保護。在實務作業中，除非是已取得當事人授權外，否則就他人受著作權保護之著作，尚不得自行對外首次公開或從事逾越合理使用範圍的利用行為。就管理層面如何降低組織利用著作時侵害他人智慧財產權的法律風險，可思考在利用該資訊前，增加事前審核的機制，亦即由專責人員進行權利盤點與授權範圍檢核，以確保所揭露的資料，均為授權範圍內的使用，除有助於組織遵守法令規範要求外，亦能進一步避免資料遭到不當揭露。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.18.1.2 智慧財產權

應實作適切程序，以確保遵循與智慧財產權及專屬軟體產品使用相關之法律、法令、法規及契約的要求事項。

A.18.1.3 紀錄之保護

應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

A.18.1.4 個人可識別資訊之隱私及保護

[7] 著作權法第 3 條第 1 項第 15 款：「公開發表：指權利人以發行、播送、上映、口述、演出、展示或其他方法向公眾公開提示著作內容。」

[8] 著作權法第 15 條第 2 項：「依第 11 條第 2 項及第 12 條第 2 項規定，由雇用人或出資人自始取得尚未公開發表著作之著作財產權者，因其著作財產權之讓與、行使或利用而公開發表者，視為著作人同意公開發表其著作。」

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私與保護。

類別：資訊保護【**案號：S1040603**】

歐盟法院認定網站所有權人得限制使用者基於商業目的擷取網站資料

【焦點話題】

荷蘭公司 A 以自動化程式，擷取廉價航空公司 B 網站上的航班資料，作為本身經營網路比價服務使用。B 公司表示，此舉違反其禁止使用者基於商業目的使用網站資料的服務條款；而 A 公司則主張依歐盟資料庫指令，可自由運用他人資料庫中屬於單純事實部分的資料。

歐盟法院受理本案後，認為廉價航空公司B網站提供的航班資料，尚無法受到著作權法或資料庫特別權利的保護，並進一步肯定當網站經營者就其本身資料內容，無法透過智慧財產權排除他人未經授權使用時，仍得以服務條款限制其他企業以擷取方式自動抓取、蒐集網站資料的行為。故法院裁決認定廉價航空公司B得以服務條款，禁止A公司以自動化程式抓取網站資料後轉為商業使用[1]。

【資料來源：OUT-Law.com 104/1/15】

【重點摘要】

1. 航空公司提供查詢的航班資料，雖不受歐盟資料庫指令適用範圍或受著作權法保護，但航空公司得以服務條款，限制使用者的利用行為。
2. 歐盟法院認定使用者以自動化程式擷取網站資料，恐違反網站服務條款而負賠償責任，此將影響自動比價服務開發與巨量資料應用。

[1] Case C-30/14, preliminary ruling on Ryanair Ltd v. PR Aviation BV, 15 January 2015, see http://curia.europa.eu/juris/document/document.jsf?docid=161388&doclang=EN (last visited: 2015/10/05)

【法律觀點】

依歐盟資料庫指令(Directive 96/9/EC)[2]，資料庫內容本身屬事實資訊時，雖不受著作權保護，但資料庫本身就資料選擇或編排具有精神創作性時，可受著作權保護；另外，若資料庫所有人就資料的取得、確認或呈現，在質量上係耗費相當時間精力與技術建置時，該指令亦賦予其所有權人享有特別的資料庫權利(Sui Generis Database Rights)，享有特別資料庫權利者，除在特定情形時不得限制使用者抽繹或再利用資料以外[3]，得禁止他人以任何方法或形式將資料庫之全部或部分重要內容，移轉於其他資料媒介。因此，本案歐盟法院裁決即是針對在歐盟資料庫保護指令架構下，對於資料庫內容本身不受著作權法保護，亦不符合資料庫特別權利保護要件的資料庫所有者，認定其仍得依一般契約關係，以網站服務條款限制使用者擷取資料庫內容，從事逾越特定目的的利用。

這項歐盟法院裁決對於有從第三方蒐集、擷取資料自行使用的業者，尤其是透過網路爬蟲或其他自動化程式，從各家資料來源網站抓取資料，提供分析或加值應用服務的資訊服務業者，無寧造成重大影響。因為依歐盟法院見解，資料來源網站縱使無法基於著作權，排除此類業者未經事先授權的利用行為，仍能夠以服務條款限制他人從事特定目的外利用。故資訊服務業者為確保資訊供應穩定並降低法律風險，恐須與資料來源網站簽訂授權協議，避免資料來源網站以違反契約條款請求損害賠償，或採取拒絕連線等排除侵害手段。

---

[2] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

[3] Article 9, Member States may stipulate that lawful users of a database which is made available to the public in whatever manner may, without the authorization of its maker, extract or re-utilize a substantial part of its contents:(a) in the case of extraction for private purposes of the contents of a non-electronic database; (b) in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved; (c) in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure.

我國並未基於資料庫建立耗時費力而賦予其特別權利，資料庫為資料的集合體，依我國著作權法屬於編輯著作，因此只有在資料選擇及編排具有創作性時，資料庫設計或架構本身受著作權法保護[4]。至於資料庫內容本身，是否受著作權法保護則須個別認定，若資料屬於不具有創作性的新聞事實或我國法令，即不受著作權法保護[5]。但資料庫所有者對於使用者擷取網站中不受著作權保護的內容，雖無法以著作權排除侵害，惟使用者之利用行為如涉及榨取其他事業努力成果、造成網站系統設備干擾或違反網站服務條款，致生他人損害時，資料庫或網站所有者仍可能依其他法律循求救濟[6]。歐盟法院此裁決即指出，資料來源網站在特定情形下，得以契約條款限制使用者抽繹或再利用資料，我國實務見解是否採納仍有待觀察，但此歐盟法院見解勢必促使某些以抓取其他網站資料提供資訊加值服務的業者，為避免動輒遭到網站拒絕連線或請求賠償，而須重新思考其經營策略，並評估尋求授權或建立合作夥伴關係的成本。

【管理 Tips】

由於科技進步日新月異，組織在推動業務時，需要了解新種科技對業務的影響。網路爬蟲程式是否允許使用，或是可以使用的範圍，除了必須符合法令與資料利用相關契約條款的要求外，組織也應該定期檢視科技的影響，並決定原有的作業方式是否需要調整。要思考新科技對業務的影響，避免因為不了解法令或科技，而導致業務的執行出現與實際斷層的情況。

組織以網站方式提供他人利用本身資訊服務時，宜先行評估此類資訊是否

---

[4] 著作權法第 7 條：「就資料之選擇及編排具有創作性者為編輯著作，以獨立之著作保護之。編輯著作之保護，對其所收編著作之著作權不生影響。」

[5] 著作權法第 9 條：「下列各款不得為著作權之標的：一、憲法、法律、命令或公文。二、中央或地方機關就前款著作作成之翻譯物或編輯物。三、標語及通用之符號、名詞、公式、數表、表格、簿冊或時曆。四、單純為傳達事實之新聞報導所作成之語文著作。五、依法令舉行之各類考試試題及其備用試題。前項第一款所稱公文，包括公務員於職務上草擬之文告、講稿、新聞稿及其他文書。」

[66] 公平交易法第 25 條：「除本法另有規定者外，事業亦不得為其他足以影響交易秩序之欺罔或顯失公平之行為。」刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

符合我國著作權或營業秘密保護範圍，以利訴諸此類法令保護本身保有的資訊，另組織亦得透過網站服務條款，明確約定使用者利用範圍與方式，以利組織於使用者利用行為違反網站服務條款時，得採取終止服務、排除侵害或請求違約損害賠償等方式，以維護自身權益。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.3 紀錄之保護

應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

A.18.2.2 安全政策及標準之遵循性

管理人員應以適切之安全政策、標準及所有其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。

貳、資訊公開(Disclosure)

一、政府資訊公開法

類別：資訊公開【**案號：D1040101**】

臺北市政府開放資料加值應用，將修正再授權規定

【焦點話題】

臺北市政府過去雖開放資料供民眾「加值應用」，但民眾若要將這些資料再重製分享出去，還需填寫授權書。為了實現開放政府之目標，臺北市政府近日擬修改「臺北市政府資料開放使用規範」，取消這項「再授權」規定，並擴大資料開放之範圍，未來可加值應用的資料類型，將包括不具原創性、不需收費、不受「著作權法」保護或已逾保護期限的資料等；且 APP 開發者也可進行商業使用。

市府人員透露，資訊局也想與交通局合作，討論是否要開放 YouBike 租借站及捷運站人流等統計數據，再由民間發展成 APP，當然這些資訊都要去除個人資料；若相關技術持續開展，將可實現開放政府理念。

【資料來源：自由時報 104/5/6】

【重點摘要】

1. 與人民權益攸關之施政、措施及其他有關之政府資訊，應以主動公開為原則，並應在符合相關法令之前提下，建構便利人民進行加值應用之環境。
2. 公務員於公開政府資訊同時，仍應留意這些資訊是否有法定應不予公開或限制公開之事由，避免觸法而受行政裁罰。

【法律觀點】

政府資訊公開向來被視為檢視政府施政是否透明，以及評估國家民主化程度的重要指標，而在大數據(Big Data)時代，其意義又不僅止於此。近年來，

隨資通訊科技的發展，各國逐漸推動資料開放，將政府資訊之原始資料(raw data)對外提供，使民眾得進行編輯、分析、公開傳輸或為其他利用方式，並作為開發各種產品或應用服務之基礎，臺北市政府更已於 100 年仿效新加坡方式建立簡易開放資料平臺，目前資料目錄包含 192 項以上資料集，並提供線上預覽、檔案下載及應用程式介面(Application Programming Interface, API)介接等多種服務模式。然而，由於現行「臺北市政府資料開放使用規範」要求人民於取得政府資訊後，須取得臺北市府書面同意，方得重製、改作、編輯、散布或轉讓[1]，距離「開放政府」仍有一段距離。

進一步說，政府資訊既泛指政府機關於職權範圍內作成或取得之訊息[2]，至少於數據統計等資料方面，除了在資料的選擇和編輯具創作性者屬編輯著作外[3]，原則上並無智慧財產權可言，是以此類資訊於公開之後，即無再對後續之加值應用予以管控之必要。而不具原創性、不受著作權法保護或已逾保護期限的資料，於本質上言，過往對於此類資料要求須取得臺北市府書面之再授權同意，始得重製或改作等，實屬多餘之限制，且有礙於應用程式開發者在大數據時代之發展。

然而，政府資訊公開亦非全無限制，除應遵循各級政府資料開放的相關規範外[4]，另依政府資訊公開法之規定，政府機關內部單位之擬稿或其他準備作業，或者公開將侵害個人隱私、職業上秘密或著作權人之公開發表權者，均屬法律明定不得公開之資訊[5]，倘若公務員不慎將此類資訊公開或提供，即

---

[1] 臺北市政府資料開放使用規範第 7 條：「本府資料開放智慧財產權歸屬於本府，除依本規範所約定之方式進行加值應用外，非經本府事前書面同意，使用者不得任意重製、改作、編輯、散布或轉讓，亦不得使第三人為上述之行為。」

[2] 參政府資訊公開法第 3 條：「本法所稱政府資訊，指政府機關於職權範圍內作成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息。」

[3] 著作權法第 7 條第 1 項：「就資料之選擇及編排具有創作性者為編輯著作，以獨立之著作保護之。」

[4] 如「行政院及所屬各級機關政府資料開放作業原則」、「臺北市政府資料開放使用規範」及「新北市政府電子資料公開作業要點」等。

[5] 政府資訊公開法第 18 條第 1 項：政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。二、公開或提供有礙犯

可能面臨懲戒或懲處之行政制裁[6]。除此之外，如政府資訊中有部分不得公開，部分應公開時，則為使人民取得政府資訊之權利，不致受到過度限制，政府機關仍應將不得提供之資訊予以遮蔽後，再行公開或提供，俾符法制[7]。

【管理 Tips】

就本案而言，與人民有關的政府資訊，應主動公開為原則。因此，就組織而言，特別是政府機關，應先將其所具有之資訊進行定義及分類；凡與民眾有關之資訊，在不涉及國家安全或機關業務機密的考量下，原則上應加以公開；因此，組織應進一步規劃資訊公開之對象、範圍、方式、程序及期限等，以利民眾查詢、使用。

應予注意的是，機關所具有之資訊中，可能並不涉及國家安全或機關業務機密，但卻涵蓋他人之個人資料或營業秘密；就此情形，組織對於資訊公開或加值運用之政策及作業規範應審慎考量，透過限制公開或透過適當遮蔽之方式來進行，以避免因為資料公開而牴觸個人資料保護法、營業秘密法等法令之規定。

罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者。三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。四、政府機關為實施監督、管理、檢 (調) 查、取締等業務，而取得或製作監督、管理、檢 (調) 查、取締對象之相關資料，其公開或提供將對實施目的造成困難或妨害者。五、有關專門知識、技能或資格所為之考試、檢定或鑑定等有關資料，其公開或提供將影響其公正效率之執行者。六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。七、個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。八、為保存文化資產必須特別管理，而公開或提供有滅失或減損其價值之虞者。九、公營事業機構經營之有關資料，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。」

[6] 政府資訊公開法第 23 條：「公務員執行職務違反本法規定者，應按其情節輕重，依法予以懲戒或懲處。」

[7] 政府資訊公開法第 18 條第 2 項：「政府資訊含有前項各款限制公開或不予提供之事項者，應僅就其他部分公開或提供之。」

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.8.2.1 資訊之分級

資訊應依其法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

類別：資訊公開【**案號：D1040102**】

政府資料開放授權條款可轉為創用 CC 4.0 授權

【焦點話題】

行政院國家發展委員會(以下簡稱國發會)於 104 年 7 月 27 日發布新版政府資料開放授權條款第 1 版，藉以取代 102 年 4 月 26 日所訂定之舊版授權條款。參與新版條款訂定的中央研究院資訊科技創新研究中心資深顧問表示：「行政院國發會符合國際開放定義的第一版政府資料開放授權條款終於上線！自此以後中央政府釋出資料的利用規則，悉以條款來論，而不用擔心平臺規範可能隨時遭到變更」。

另外，本次改版重點在於釐清著作權利用範圍與相關限制，明確約定授權不會撤回，並容許使用者不限時間、地域及目的之利用，且允許再轉授權，必要時得直接轉換為國際通用的 Creative Commons BY 4.0(以下簡稱創用 CC BY 4.0)此開放授權條款，進行利用。由於創用 CC BY 4.0 的通用性較廣，有助於達到多源共工的大數據加值應用。

【資料來源：iThome 104/8/9】

【重點摘要】

1. 我國政府資料開放授權條款修正後，已明訂與「創用 CC 授權姓名標示 4.0 國際版本」相容。
2. 採取開放授權條款有助於降低授權門檻與使用成本，進一步促進政府開放資料後續加值利用。

【法律觀點】

依我國著作權法規定，著作權歸屬於著作權人所有，因此對於尚在著作財產權保護期間的作品，從事合理使用範圍以外的著作利用行為時，利用者

均需事先取得著作權人的授權。但這樣的規範架構對於希望著作能獲得快速流通分享，甚至歡迎他人逕為改作、共同激盪創意的著作權人而言，反而造成阻礙。因此，美國非營利組織Creative Commons提出「保留部分權利」(Some Rights Reserved)的相對思考與作法，透過「姓名標示」、「非商業性」、「禁止改作」及「相同方式分享」等四大授權要素的排列組合，提供六種開放授權條款[1]，任何人只要遵守著作權人所設定的授權條件下，即可自由使用以創用CC授權的著作，俾以藉由自願分享且授權條件明確的機制，促進內容資源的交流分享。

因此，我國政府開放資料平台即因應國際上鼓勵開放授權的風潮，在政府資料開放授權條款明訂「本條款與『創用CC授權姓名標示 4.0 國際版本』相容」[2]，採取相對更為寬鬆的授權條款，亦即任何人只要標註授權機關或其指定名稱，無論其利用需求屬於出版、付費軟體服務等營利行為，或有進一步編寫、修改情形等，均可自由運用。是以，我國政府開放資料平台上之資料集，若循新版條款釋出，所有利用者只要符合授權條件即可自行利用，無庸再尋求機關授權，有助於降低授權門檻與使用成本，並能進一步促進政府開放資料後續加值利用。惟在新版授權條款下，利用者應注意在使用政府機關釋出的資料集時，應依「顯名聲明」要求之方式，明確標示原資料提供機關之相關聲明[3]，以避免未能符合授權條件，而有回歸到該

[1] Creative Commons 所提供的公眾授權條款，台灣稱為「創用 CC」授權條款，自 92 年由中央研究院資訊科學研究所支援，依據臺灣著作權法規範轉化為在地化版本。關於創用 CC 授權要素與六大條款內容介紹，參閱「台灣創用 CC 計畫」，檢索自 http://creativecommons.tw/explore。

[2] 政府資料開放授權條款第 1 版第 4 條：「四、版本更新及授權轉換(一)本條款如有修正，依舊條款提供之開放資料，於新條款公告時，使用者得選擇採用新條款利用。但原資料提供機關，於提供開放資料時，已訂明其使用之特定版本條款者，不在此限。(二)本條款與「創用 CC 授權姓名標示 4.0 國際版本」相容，使用者依本條款利用開放資料，如後續以「創用 CC 授權姓名標示 4.0 國際版本」規定之方式利用，視為符合本條款之規定。」

[3] 新版授權條款第 3 條：「(二)使用者利用依本條款提供之開放資料，及後續之衍生物，應以符合附件所示『顯名聲明』要求之方式，明確標示原資料提供機關之相關聲明；未盡顯名標示義務者，視為自始未取得開放資料之授權。」，附件所示顯明聲明方式為：「提供機關 / 單位 [年份] [開放資料釋出名稱與版本號] 此開放資料依政府資料開放授權條款 (Open Government Data License) 進行公眾釋出，使用者於遵守本條款各項規定之前提下，得利用之。政府資料開放授權條款：http://data.gov.tw/?q=principle」。

利用方式是否符合著作權法上合理使用之疑慮。

【管理 Tips】

就實務面而言，因新版授權條款較舊版為寬鬆，組織在建置相關程序時，務必確認新、舊法規之差異性，而後予以適用。從另一個角度來看，在新版條款下，組織開放資料之使用頻率，勢必高於過往，因而組織如何確保提供資料的正確性，即更顯得重要；因為一旦提供不正確的資料，就有可能不斷地被錯誤引用。是以，組織在開放資料運用時，一定要增加並優先執行資料正確性的確認步驟，以確保組織的公信力。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織、應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.2 智慧財產權

應實作適切程序，以確保遵循與智慧財產權及專屬軟體產品使用相關之法律、法令、法規及契約的要求事項。

參、資訊監察(Monitors)

一、通訊保障及監察法

類別：資訊監察【**案號：M1040101**】

程式「永遠開啟」 隱私對話全都錄

【焦點話題】

美國一家非營利組織「電子隱私資訊中心」(Electronic Privacy Information Center)日前致函美國司法部與聯邦貿易委員會，表示許多越來越普遍的「永遠開啟」(always on)電子產品，可以秘密錄下使用者在家裡的談話內容，此功能可能侵犯個人隱私，同時也可能觸犯禁止非法監聽的聯邦法律。

電子隱私資訊中心在信中指出，Google 的 Chromium 瀏覽器含有可以定期擷錄私人對話的程式碼，當使用者利用電腦的內建麥克風講話時，Chromium 瀏覽器經常會從旁「聆聽」，一旦聽到使用者講到「好的，Google」(OK Google)字句，Chromium 瀏覽器便會啟動聲控功能，將使用者聲音轉換成文字以進行搜尋。這意味著 Chromium 瀏覽器可能是在未獲使用者同意下，甚至是使用者根本不知情的狀況，讓使用者在私密環境中遭到錄音。微軟(Microsoft)推出的聲音與動作記錄器 Kinect，以及亞馬遜(Amazon)推出的 Alexa 聲控電腦程式等，也都因為具有類似的錄音功能而被電子隱私資訊中心點名。

電子隱私資訊中心要求美國司法部與聯邦貿易委員會對具有「永遠開啟」功能的電子產品展開全面調查，從法律層面探討使用者權益是否遭受侵犯，並且了解被側錄的語音資料是否被廠商儲存。

【資料來源：中央社 104/7/18】

【重點摘要】

1. 瀏覽器或通訊軟體未經告知或取得使用者同意，逕自錄音作為分析使用，已侵害使用者隱私，引發疑慮。

2. 依我國通訊保障及監察法，產品服務提供者未取得通話任一方同意，逕為擷取通訊內容，恐負有刑責。

【法律觀點】

維護人性尊嚴與尊重人格自由發展，是自由民主社會十分重要之精神。關於秘密通訊自由，已於我國憲法第 12 條中明確規定[1]，而隱私權雖未在憲法明文列舉，但基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障[2]。我國通訊保障及監察法(以下簡稱通保法)之制定，即係基於確保國家安全及維持社會秩序，並保障人民秘密通訊自由及隱私權不受非法侵害[3]等目的。

依照通保法之定義，一般民眾日常生活的言論及談話，以有事實足認其對通訊內容有隱私或秘密之合理期待者，即可稱為通訊[4]。又通訊監察係以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之，但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材[5]。本案提及的Google Chromium網頁瀏覽器，即是透過電腦內建麥克風側錄，並擷取使用者特定聲音指令後，觸發聲控功能，而進一步以程式將語音轉換成文字傳輸到網頁上進行搜尋，因而其可能符合前述通訊監察之定義。

又依照通保法所規定，監察者若獲得通訊之任一方事先同意，且並非出於不法目的，則相關的監察行為將不被處罰[6]。本案所提及之電子產品服務提供

---

[1] 中華民國憲法第 12 條：「人民有秘密通訊之自由。」

[2] 參照大法官釋字第 603 號解釋文。

[3] 通訊保障及監察法第 1 條：「為保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。」

[4] 通訊保障及監察法第 3 條：「本法所稱通訊如下：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。二、郵件及書信。三、言論及談話。前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」

[5] 通訊保障及監察法第 13 條第 1 項：「通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」

[6] 通訊保障及監察法第 29 條：「監察他人之通訊，而有下列情形之一者，不罰：一、依法律規定而為者。

者，雖然所提供之服務多是作為輔助搜尋或是娛樂之用，但在使用者對於其使用電腦設備及相關應用服務時與他人進行之對話內容，具有合理隱私期待時，若產品服務提供者明知未經通訊任一方事先同意，或是完全不告知使用者即進行監察，將使用者的聲音轉換成文字以進行網路搜尋，將會讓使用者的隱私權和秘密通訊自由受到侵害，而可能構成通保法第 24 條第 1 項的違法監察他人通訊罪[7]。除了通保法的規範外，電子產品服務提供者無故利用工具或設備窺視、竊聽，或以錄音、照相、錄影或電磁紀錄竊錄使用者非公開之活動、言論、談話或身體隱私部位者時，亦有可能成立刑法第 315 條之 1 的妨害秘密罪[8]。

科技的進步帶來許多好處，特別是聲控功能增添了日常生活的便利和趣味。然而，私人語音和對話仍屬於人民隱私，產品服務提供者仍應注意自己對使用者通訊內容的處理和記錄，是否獲得使用者同意，以及須有妥善管理方式，避免侵害人民基本權利以及觸犯法律相關責任。

【管理 Tips】

組織購入軟體時，必須先在採購前檢視相關報告及技術文件，確認是否符合功能需求，以及是否有洩漏資訊或個人隱私之風險。如發現該軟體有洩漏組織資訊或個人隱私之可能時，應立即與軟體開發廠商討論及採取相對應的控管機制或其他補償性控制。其次，在正式上線前，組織必須要求硬體、網路及其他相關人員再次確認軟體是否符合現行資訊安全規範，以避免軟體安裝或使用後發生資料外洩情事而不自知。

二、電信事業或郵政機關 (構) 人員基於提供公共電信或郵政服務之目的，而依有關法令執行者。三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

[7] 通訊保障及監察法第 24 條第 1 項：「違法監察他人通訊者，處五年以下有期徒刑。」

[8] 刑法第 315 條之 1 規定：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

此外在組織購入軟體後，仍應定期執行弱點掃描作業，如果有掃描出來屬於高風險的項目，則一定要進行程式修補作業，以確保系統程式均有適當的更新。如弱點掃描的結果，與原先開發的程式有相衝突或牴觸的地方，在合約可行的範圍內，應要求廠商進行程式修正作業，以避免因程式設計不當而導致組織產生資訊安全事件。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.12.6.1 技術脆弱性管理

應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。

A.14.1.1 資訊安全要求事項分析及規格

資訊安全相關要求事項，應納入新資訊系統或既有資訊系統之強化的要求事項中。

A.14.2.2 系統變更控制程序

應藉由使用正式之變更控制程序，以控制開發生命週期內之系統變更。

A.14.2.5 保全系統工程原則

保全系統之工程原則，應予建立、文件化、維護及應用於所有資訊系統實作工作。

A.14.2.7 委外開發

組織應監督及監視委外系統開發活動。

肆、資訊應用(Application)

一、電子簽章法

類別：資訊應用【**案號：A1040101**】

電子票證款項可移轉至電子支付帳戶，立院三讀通過

【焦點話題】

隨著新興科技的應用逐漸改變支付模式，並配合電子支付機構管理條例施行，立法院於民國(下同)104 年 6 月 9 日三讀通過電子票證發行管理條例部分條文修正。新法明定電子票證發行機構與電子支付機構業務得相互兼營；另外，新法開放記名式電子票證持卡人能將儲值款項，移轉至其電子支付帳戶。

然而，基於洗錢防制考量，該條例規定能夠進行款項移轉的電子票證，限於記名式，且款項僅能移轉至同一持卡人的電子支付帳戶，至於移轉金額上限與條件，則授權主管機關訂定。舉例來說，民眾王先生在記名式悠遊卡中儲值 1,000 元，未來王先生在符合法令規定條件與限額下，能將該筆款項移轉至其電子支付帳戶，作為線上消費扣款使用。此修正方向有助於提供民眾更多元的支付管道。

【資料來源：聯合報 104/6/9】

【重點摘要】

1. 電子票證發行機構得經主管機關許可，兼營電子支付業務，不受專營限制，有助於促進支付服務多元化。
2. 新法修正後，准許記名式電子票證款項得移轉至電子支付帳戶，以在落實使用者身分確認機制且防制洗錢活動下，提升支付工具間交互運用效益。

【法律觀點】

近年來隨者電子商務發展活絡，消費者之消費模式與支付工具也發生劇烈的

改變，多數消費者已經可使用信用卡或第三方支付[1]帳號儲值款項，在網路上購買各類生活用品，甚至在實體商店付款時，習慣以悠遊卡、一卡通或以手機應用程式連結第三方支付帳號或信用卡資訊等方式扣款支付。因此，金融監督管理委員會(以下簡稱金管會)為扶植我國電子商務產業發展、保護消費者權益，並促進國內支付服務創新，研訂完成電子支付機構管理條例(以下簡稱電子支付條例)，並於 104 年 5 月 3 日施行，故向主管機關取得許可經營的電子支付機構，就能夠以網路或電子支付平臺為中介，提供消費者代理收付網路交易款項、儲值及帳戶間資金移轉等服務[2]，使我國消費者關於網路支付方式，除購買商家電子禮券點數、透過網路開立儲值支付帳戶扣款[3]或線上刷卡等以外，有更多樣選擇。

鑒於電子支付條例開放電子支付機構得兼營電子票證業務[4]，以促進跨業兼營效益，因此本次電子票證發行管理條例(以下簡稱電子票證條例)部分條文

---

[1] 依經濟部公司行號營業項目代碼表，就第三方支付服務業之營業項目為「從事配合金融機構及履約相關條件，並與銀行合作，取得信用卡特約商店資格，提供電子商務(含行動商務)買賣雙方收付擔保之中介機制之行業」；至於營業項目電子支付業之訂議內容，為「依電子支付機構管理條例規定，以網路或電子支付平臺為中介，接受使用者註冊及開立記錄資金移轉與儲值情形之帳戶，並利用電子設備以連線方式傳遞收付訊息，於付款方及收款方間經營下列業務之公司。但僅經營代理收付實質交易款項，且其保管代理收付總餘額未逾主管機關規定之一定金額者，不包括之： 一、代理收付實質交易款項。 二、收受儲值款項。三、電子支付帳戶間款項移轉。 四、其他經主管機關核准之業務」。電子支付條例制定發布後，依該條例第 3 條規定，若僅經營代理收付實質交易款項業務，且保管使用者代理收付款項之一年日平均餘額未超過新臺幣 10 億元，不屬於電子支付業務，因此一般資訊服務業者仍可經營第三方支付服務。

[2] 電子支付條例第 4 條第 1 項：「本條例所稱電子支付機構，指經主管機關許可，以網路或電子支付平臺為中介，接受使用者註冊及開立記錄資金移轉與儲值情形之帳戶(以下簡稱電子支付帳戶)，並利用電子設備以連線方式傳遞收付訊息，於付款方及收款方間經營下列業務之公司。但僅經營第一款業務，且所保管代理收付款項總餘額未逾一定金額者，不包括之：一、代理收付實質交易款項。二、收受儲值款項。三、電子支付帳戶間款項移轉。四、其他經主管機關核定之業務。」

[3] 參考金管會 102 年 8 月 30 日金管銀票字第 10240002940 號函准予備查訂定發布之銀行受理客戶以網路方式開立儲值支付帳戶作業範本，該範本係為配合電子商務及網路交易代收代付服務之發展，規範銀行受理客戶以網路方式開立儲值支付帳戶之作業審核程序及其配套管理措施，以利消費者透過該儲值支付帳戶完成線上支付。

[4] 電子支付條例第 9 條：「電子支付機構經主管機關依電子票證發行管理條例之規定核准者，得兼營電子票證業務。」

修正草案，亦配合納入開放兼營規定[5]，以利業者能夠兼容不同支付工具特色，提供消費者更為便捷創新的服務。尤其此次電子票證條例修正，開放記名式票證持卡人得將儲值款項移轉至其電子支付帳戶[6]，有助於電子票證機構透過此方式拓寬網路消費通路。

惟電子票證機構為避免持卡人款項遭到盜用並降低資金非法移轉風險，受理款項移轉服務前，應確認持卡人與電子支付帳戶持有人是否同一，以及持卡人是否有為移轉款項意思。因此，電子票證機構應採取一定檢核方式確認持卡人身分、指定帳戶及其款項資料。若於網路環境受理持卡人提出前開申請，電子票證機構應依電子簽章法規定，取得消費者同意以電子文件為表示方法[7]，並配合保存相關電磁紀錄軌跡資料，以依電子票證條例規定妥善維護消費者相關交易紀錄之完整性[8]。

【管理 Tips】

依本案而言，電子票證發行機構提供使用者將記名式電子票證款項，移轉至其電子支付帳戶之服務時，就使用者身分識別作業應有明確的作業程序，例如於註冊程序時即確實掌握使用者身分，在使用者申請款項移轉或指示扣款時，則須能以適當方式確認使用者身分及其權限，以確實維護使用者權益。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.9.2.1 使用者註冊及註銷

---

[5] 電子票證條例第 7 條第 1 項：「發行機構以股份有限公司組織為限；除本條例另有規定或經主管機關依電子支付機構管理條例規定許可兼營電子支付機構業務者外，應專業經營電子票證業務。」

[6] 電子票證條例第 5 條之 1 第 1 項至第 3 項：「發行機構發行記名式電子票證，符合一定條件者，得依持卡人指示，將儲存於記名式電子票證之款項移轉至同一持卡人之電子支付帳戶。主管機關得限制前項移轉款項之金額；其限額，由主管機關定之。第一項所定一定條件，由主管機關定之。」

[7] 電子簽章法第 4 條第 1 項：「經相對人同意者，得以電子文件為表示方法。」

[8] 電子票證條例第 22 條：「發行機構應依主管機關及中央銀行之規定，申報業務有關資料。發行機構發行電子票證應保存持卡人交易帳款明細資料，至少保存五年，並提供其查詢之服務。前項明細資料應充分揭露交易日期、使用卡號、交易項目、交易金額、交易設備代號及幣別等項目。」

應實作正式之使用者註冊及註銷過程，俾能指派存取權限。

A.9.2.2 使用者存取權限之配置

應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。

A.9.2.3 具特殊存取權限之管理

應限制及控制特殊存取權限之配置及使用。

類別：資訊應用【**案號：A1040102**】

毛揆：打造數位化金融環境 3.0，推動金融創新

【焦點話題】

行政院長毛治國今在行政院會聽取金融監督管理委員會(以下簡稱金管會)「打造數位化金融環境 3.0」報告後表示，網際網路興起及行動通訊時代的來臨，帶動商業模式的創新，金融服務必須順應科技發展的趨勢，方能掌握商機。故請金管會持續關注數位化金融發展情形，適時檢討修正相關措施，營造有利金融產業的環境，並協助金融服務業強化數位科技的應用能力，以推動金融創新，為臺灣金融產業奠定新的發展利基。

金管會表示，規劃推動「打造數位化金融環境 3.0」計畫，從鼓勵創新網路金融服務、推動金融巨量資料分析應用、普及行動支付與第三方支付應用等方面三管齊下，目的在掌握數位化發展趨勢，以提升金融產業的競爭力。目前推動措施包括調整法規規範、並開放線上申辦信貸、投保、行動支付等服務、開放設立電子支付機構、開放經營股權性質群眾募資平台等。未來將朝研議放寬金融業轉投資金融科技產業限制、研究開放純網路銀行、持續推動大數據應用與金融資料開放等方向進行。

【資料來源：行政院新聞傳播處 104/7/9】

【重點摘要】

1. 金融機構提供民眾使用行動裝置應用程式，以執行電子銀行、消費、儲值及第三方支付等金融服務時，應採取安全控管措施，確保程式安全。
2. 金融機構提供予民眾使用的行動應用程式，若未適當採取防護與安全控管機制，恐違反消費者保護法或個人資料保護法相關規定，依法應對民眾負賠償責任。

【法律觀點】

隨著科技發展，網路通訊與智慧型行動裝置日益普及，促進各類食衣住行育樂資訊與相關服務的行動應用程式快速發展，並進而強化民眾對於行動裝置的依賴度。為滿足民眾對金融服務行動化之需求，並因應行動生活趨勢，金管會自民國 103 年起推動「打造數位化金融環境 3.0」計畫，就是希望藉由主管機關發揮引導的效果，協助金融服務業推動金融創新，以營造有利發展數位金融之環境。

然而，數位金融環境應建立在資訊安全的基礎上，尤其伴隨金融服務行動化趨勢，民眾透過行動裝置執行業務申辦或交易，雖可享有服務提供的即時與便利，但資料傳輸安全與相關紀錄完整留存亦為影響民眾信賴的重要課題。對此，金管會已督促中華民國銀行商業同業公會全國聯合會(簡稱銀行公會)訂定「金融機構提供行動裝置應用程式注意事項」，規範金融機構以行動應用程式提供電子銀行、消費、儲值、第三方支付等金融業務時應注意事項，包含銀行若採取空中傳輸(Over the Air)方式，讓使用者下載敏感性資料至其行動裝置時，應配合以密碼等方式確認使用者身分，且敏感性資料本身應採取加密或亂碼化等相關機制，以有效防範相關資料被竊取。因此，金融機構在開發行動應用服務時，即應注意上開注意事項對於資料安全與保密的要求。

若金融機構提供予民眾使用的行動應用程式未適當採取防護與安全控管機制，銀行除因該產品或服務「未能符合當時科技或專業水準可合理期待之安全性」，而依消費者保護法對民眾所受損害負賠償責任以外[1]，若進一步因該金融機構未盡採取適當安全防護措施，致造成民眾個人資料遭竄改、

[1] 消費者保護法第 7 條：「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。商品或服務具有危害消費者生命、身體、健康、財產之可能者，應於明顯處為警告標示及緊急處理危險之方法。企業經營者違反前二項規定，致生損害於消費者或第三人時，應負連帶賠償責任。但企業經營者能證明其無過失者，法院得減輕其賠償責任。」

竊取、外洩或其他不當利用時，民眾亦得依個人資料保護法之規定向該金融機構請求損害賠償[2]。

【管理 Tips】

就本案而言，金融機構提供行動應用程式，除在程式開發及撰寫上需要融入安全設計概念外，由於涉及多數一般使用者的利用，因而對於登入權限的管控及網路的安全性，也都需要一併考量。其次，考量行動裝置使用的便利性，除密碼外，也可以考慮再加入生物辨識或其他身分辨識的方式，以避免行動裝置遺失導致的交易糾紛。又，在網路層面，除了考量網路的可連結性外，應特別留意異常狀況的處理，例如不尋常的登錄時間或登錄方式，並採取事先預警機制且再確認相關資訊。整體而言，在開發新種資訊業務時，除方便性及創新性外，資安基本防護的考量絕對不可缺少。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.9.4.2 保全登入程序

當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。

A.9.4.3 通行碼管理系統

通行碼管理系統應為互動式，並應確保嚴謹通行碼。

A.10.1.1 使用密碼式控制措施之政策

應發展及實作政策、關於資訊保護之密碼式控制措施的使用。

A.10.1.2 金鑰管理

[2] 個人資料保護法第 27 條第 1 項：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」、同法第 29 條第 1 項：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

應發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命週期。

A.13.1.2 網路服務之安全

應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外提供。

A.13.2.1 資訊傳送政策及程序

應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式之通訊設施之資訊傳送。

A.13.2.3 電子傳訊

應適切保護電子傳訊時所涉及之資訊。

自我評量

7 月分自我評量

是非題：(每題十分)

1. （O） 銀行委託廠商印製與寄送客戶房屋貸款對帳單，涉及將客戶資產與財務狀況等個人資料委託廠商處理與利用，對於廠商執行業務即應依法進行監督。【資料保護 S1040101】

   解析：金管會指定非公務機關個人資料檔案安全維護辦法第 8 條規定。

2. （X） 「作業委外」即表示相關的責任也同時委外。除非有特別必要，否則可以不用特別監督。【資料保護 S1040101】

   解析：「作業委外」並非表示相關的責任也同時委外。對於委外廠商，仍應負責督導管理。

3. （X） 公務資訊不分性質，一律可以用即時通訊軟體傳輸。【資料保護 S1040201】

   解析：公務資訊如涉及機密性、資訊安全及隱私事項，盡量避免以即時通訊軟體傳輸。

4. （X） 如涉及重要之公務機密外洩事件，只有在故意之情形，才可能構成刑法洩漏公務秘密罪。【資料保護 S1040201】

   解析：如涉及重要之公務機密外洩事件，不論出於故意或過失，可能構成刑法洩漏公務秘密罪，最重可處以三年有期徒刑。

5. （O） 政府資訊既泛指政府機關於職權範圍內作成或取得之訊息，至少於數據統計等資料方面，除了在資料的選擇和編輯具創作性者屬編輯著作外，原則上並無智慧財產權可言。【資料公開 D1040101】

解析：政府資訊除非具有創作特性，否則原則上並不具有智慧財產權。

選擇題：(每題十分)

1. （2） 以下哪個項目不是營業秘密的必要要件？(1)秘密性。(2)公益性。(3)經濟性。(4)合理保護措施。【資料保護 S1040301】

解析：所謂營業秘密，指「生產、銷售或經營之相關資訊」，且應具備「秘密性」、「經濟性」及「合理保護措施」等。

2. （3） 利用影音網站服務製作播放清單，是否屬於著作權法的重製或公開傳輸他人著作?(1)是，因為播放清單是將想看的影片再編輯收藏，屬於重製；(2)是，因為播放清單是對公眾公開的，屬於公開傳輸他人著作；(3)不是，因為單純為自己聆賞之方便點選瀏覽影音，不屬於重製或公開傳輸他人著作；(4)不是，因為播放清單沒有傳輸功能。【資料保護 S1040601】

解析：利用影音網站服務製作播放清單之行為，係以超連結方式提供網站上的影音檔案，不涉及重製或公開傳輸他人著作。

3. （1） 假設著作權人在影音網站上看到盜版侵權影音，下列影音網站與著作權人的權益，何者正確?(1)著作權人可以通知影音網站，請影音網站取下盜版侵權影音；(2)目前著作權法沒有相關規定；(3)著作權人可以直接控告影音網站；(4) 影音網站無法避免與上傳侵權資料的網友負擔共同侵權責任。【資料保護 S1040601】

解析：影片遭網友非法上傳至影音網站的著作權人，得依著作權法規定向影音網站要求取下，以降低侵害。而網路服務提供者藉由配合著作財產權人取下侵權資訊之行為，亦可免除與上傳侵權資料的網友負共同侵權責任之風險。

4. （4） 請問以下何者並非金融機構發生個資外洩事故後，依法應採取之措施?(1)通報金管會；(2)採取補救措施並以適當方式通知受害當事人；(3)持續改善；(4)召開股東會。【資料保護 S1040101】

解析：金融機構依個資法規定，應於事故發生後採取補救措施並通知受害當事人，且需依個資法施行細則第 12 條要求持續改善內部作業，另依「金管會指定非公務機關個人資料檔案安全維護辦法」，金融機構尚負有通報金管會之義務。

5. （3） 電子票證發行機構提供記名式票證持卡人，將儲值款項移轉至其電子支付帳戶時，請問以下何者不是電子票證發行機構應採取措施?(1)確認持卡人身分(2)確認持卡人款項移轉意思(3)暫停持卡人交易活動(4)留存交易記錄。【資料保護 A1040101】

解析：電子票證機構為避免持卡人款項遭到盜用並降低資金非法移轉風險，受理款項移轉服務前，應確認持卡人與電子支付帳戶持有人是否同一，以及持卡人是否有為移轉款項意思，並依法保存相關紀錄。

自我評量檢測成果評分說明

得分	溫馨提醒
100 分	資安小博士非您莫屬
80 分~90 分	小粗心，別灰心
60 分~70 分	釐清觀念，滿分到手
40 分~50 分	再接再厲，繼續努力
20 分~30 分	牛刀小試，再來一次

8 月分自我評量

是非題：(每題十分)

1. （X） 臉書社團網頁或粉絲團屬於個人生活空間的延伸，所以無論貼文的隱私權限是否設定公開，揭露他人個資都無個資法適用? 【資料保護 S1040102】

解析：非基於個人或家庭生活目的，透過臉書社團公開他人具有識別性的姓名與照片等個資，使該臉書社團成員均可檢視個資受害人資料，屬於個資法利用行為，原則上有個資法適用。

2. （X） 聲控瀏覽器或通訊軟體為強化功能。可以在未經告知或取得使用者同意的狀況下，擷取、錄製使用者語音內容作為分析使用【資料監察 M1040101】

解析：瀏覽器或通訊軟體若未經告知或取得使用者同意，逕為擷取、錄製使用者語音內容作為分析使用，若涉及蒐集處理使用者個資，恐有違法蒐集個資疑慮；另若使用者對該段談話具有合理隱私期待，則另可能涉及刑法上竊錄或非法監聽疑慮。

3. （X） 隱私權並非我國憲法明文保護的權利，因此若竊錄他人非公開活動而有侵害他人隱私時，行為人只負有民事責任，沒有刑責風險【資料保護 S1040402】

解析：就竊視、竊聽他人非公開活動等行為，刑法已有明文之處罰規定，是以侵害他人隱私之行為，仍可能須負擔刑事責任。

4. （O） 公務機關依法辦理文件銷毀時，若文件內容經核定為國家機密，機關辦理銷毀前應先解密。【資料保護 S1040202】

解析：依國家機密保護法第 15 條第 2 項規定，國家機密經解除機密後始得依法銷毀。

5. （X） 所有機敏性公務資訊都屬於國家機密保護法所規範的客體，即所謂「國家機密」。【資料保護 S1040202】

解析：並非機敏性公務資訊都屬於本法保護的客體；必須是基於國家安全或利益而有保護必要，且經核定機密等級的資訊，才是所謂「國家機密」。

選擇題：(每題十分)

1. （3） 民眾於臉書等社交網站公開他人個資時，若夾帶不實指控或影射用語而有侵害他人名譽時，可能同時構成刑法以下何罪？(1)強制罪；(2)無故輸入他人帳密罪；(3)加重誹謗罪；(4)毀損債權罪。【資料保護 S1040102】

解析：公開他人個資並侵害他人名譽，致當事人受到社會大眾負面評價，可能同時構成刑法加重誹謗罪。

2. （2） 若政府機關發現系統主機遭駭客入侵，並導致入口網連線服務中斷時，依國家資通安全通報應變作業規定，應盡快至何處登錄資料以進行通報？(1)行政院科技部；(2)國家資通安全通報應變網站；(3)總統府；(4)國家安全局。【資料保護 S1040203】

解析：若政府機關發現發生資安事件符合本綱要定義的影響等級時，應立即至國家資通安全通報應變網站進行登錄，提供事件細節、影響等級、支援申請及資安紀錄等資訊，以利主管機關能透過通報系統即時督導事件處理。

3. （3） 1. 公務機關保有公務員人事檔案的系統，若遭駭客入侵致個資外洩時，以下關於公務機關法律責任敘述，何者正確？(1)外洩原因是因遭第三人攻擊，公務機關無任何法律責任；(2)個資受害人為公務員，對於公務機關無求償權；(3)公務機關若未盡適當安全維護，對個資受害人負賠償責任；(4)公務機關無個資法適用，不負法律責任。【資料保護 S1040203】

解析：公務機關如因未採取適當安全維護措施導致駭客入侵而遭竊取個人資料時，恐應依個資法第 28 條規定，對當事人負損害賠償責任。

4. （1） 若電子產品服務提供者未取得通話任一方同意，擅自竊聽擷取通訊內容，除了可能負有通訊保障及監察法上的違法監察他人通訊刑責之外，還可能觸犯刑法何罪？(1)妨害秘密罪；(2)詐欺罪；(3)普通竊盜罪；(4)強制罪。【資訊監察 M1040101】

解析：除了通保法的責任外，電子產品服務提供者無故利用工具或設備窺視、竊聽使用者非公開之活動、言論、談話或身體隱私部位者時，側錄私人活動或談話亦有可能成立刑法第 315 之 1 條的妨害秘密罪。

5. （1） 刑法對於侵害他人隱私的行為設有處罰之規定，但拍攝他人以下何種活動較不可能構成刑法上的犯罪？(1)在街上示威遊行；(2)在更衣室換衣服；(3)在自己的房間睡覺；(4)在餐廳上廁所。【資料保護 S1040402】

解析：在街上示威遊行並無合理隱私期待，即使予以拍攝，亦不致侵害其隱私，自不構成刑法上之犯罪。

自我評量檢測成果評分說明

得分	溫馨提醒
100 分	資安小博士非您莫屬
80 分~90 分	小粗心，別灰心
60 分~70 分	釐清觀念，滿分到手
40 分~50 分	再接再厲，繼續努力
20 分~30 分	牛刀小試，再來一次

9 月分自我評量

是非題：(每題十分)

1. （X） 我國在政府資料開放授權條款明訂「本條款與『創用 CC 授權 姓名標示 4.0 國際版本』相容」，因此未經資料釋出機關書面同意，使用者不得自行利用。【資訊公開 D1040102】

   解析：我國政府開放資料平台即因應國際上鼓勵開放授權的風潮，在政府資料開放授權條款明訂「本條款與『創用 CC 授權 姓名標示 4.0 國際版本』相容」，採取相對更為寬鬆的授權條款，只要符合顯名聲明原則，使用者即可自行利用該資料集。

2. （O） 依我國個資法規定，網站經營者於蒐集、處理我國會員個人資料時，除有依法免為告知情事以外，應以適當方式讓會員知悉關於行使當事人權利，包含請求停止蒐集、利用或刪除等權利之方式?【資料保護 S1040105】

   解析：依個資法第 8 條規定，個資蒐集主體應告知當事人依該法第 3 條規定得行使之權利及方式。

3. （O） 員工離職後，在原任職公司尚未關閉其帳號權限前，均可基於個人創業目的，繼續使用原任職公司的相關資源，包含客戶名單與內部資料庫。【資料保護 S1040403】

   解析：員工離職後，已無權限使用原任職公司相關資源，故其如以原公司帳號密碼繼續使用資料庫服務，恐涉刑責。另建議公司為妥善維護本身資源，應將資源使用之權限調整納入離職程序環節。

4. （X） 企業提供予新聞通訊社之財報調整相關資訊，反正馬上就要公布，所以無論如何該資訊都不可能構成營業秘密。【資料保護 S1040302】

解析：企業提供予新聞通訊社之財報調整相關資訊，若屬於企業經營資訊且非為一般人所知悉者，而該資訊通常會影響企業價值而具有經濟價值，如企業或組織已採取合理措施(例如，要求新聞通訊社在指定時間點前必須保密、不得公開)，則該資訊應符合營業秘密之定義，而受到營業秘密法保護。

選擇題：(每題十分)

1. （1） 以下何者是使用政府開放資料平台上，由機關以新版開放資料授權條款第 1 版釋出資料集時，應遵守的授權條件?(1)標示授權機關的顯名聲明。(2)徵詢國家發展委員會書面同意。(3)平台上資料集完全不可私自利用。(4)政府機關釋出資料可以自由利用，完全沒有限制。【資訊公開 D1040102】

解析：在新版授權條款下，利用者應注意在使用政府機關釋出的資料集時，應依「顯名聲明」要求之方式，明確標示原資料提供機關之相關聲明。

2. （3） 以下何者不是以行動應用程式提供電子銀行、消費、儲值及第三方支付等金融業務時，為防範使用者資料遭竊取的安全控管措施？(1)提供使用者下載敏感性資料前須確認使用者身分；(2) 敏感性資料本身應採取加密；(3)全面禁止以空中傳輸方式下載敏感性資料。(4)提醒使用者在行動裝置上安裝防毒軟體。【資訊應用 A1040101】

解析：銀行若採取空中傳輸(Over the Air)方式，讓使用者下載敏感性資料至其行動裝置時，應配合以密碼等類方式確認使用者身分，且敏感性資料本身應採取加密或亂碼化等相關機制，以有效防範相關資料被竊取。

3. （1） 依個資法第 3 條規定，下列哪項不是當事人可以行使的權利？(1)請求付費；(2)請求停止蒐集、處理或利用；(3)請求刪除；(4)請求閱覽。【資料保護 S1040105】

解析：依個資法第 3 條規定，當事人對於個人資料可以行使的權利，包括：(1)查詢或請求閱覽；(2)請求製作給予複製本；(3)請求補充或更正；(4)請求停止蒐集、處理或利用；(5)請求刪除。

4. （1） 有關企業秘密之管理及保護，以下敘述何者錯誤？(1)企業所有資訊都屬於營業秘密；(2) 基於業務需求而提供其他單位使用時，應讓取得資料之單位確實了解該資料在本單位之分類等級；(3)針對資料機密與重要程度採取相應控管機制；(4)企業對於他人竊取其營業秘密之行為，可以依法向法院請求酌定損害額以上之賠償。【資料保護 S1040302】

解析：依我國營業秘密法對於營業秘密的定義，須非一般人可得知悉，且該資訊具有經濟價值，並經企業或組織採取合理保密措施的資訊，始受營業秘密法保護。

5. （3） 有關非公務機關不法蒐集他人個人資料之民事賠償責任，下列敘述何者正確？(1)故意不法蒐集他人個人資料，始負民事賠償責任；(2)過失不法蒐集他人個人資料，其賠償責任可以減半；(3)非公務機關不法蒐集他人個人資料者負損害賠償責任。但能證明其無故意或過失者，不在此限；(4)過失不法蒐集他人個人資料，無庸負任何賠償責任。【資料保護 S1040104】

解析：個人資料保護法第 29 條規定：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第六項規定。」

6. （3）有關我國個人資料保護法上之個人資料，下列敘述何者正確？(1)只有特種個資才受保護；(2)只有可以直接識別個人身分之資料才受保護；(3)凡是可以識別個人身分之資料，無論是透過直接或間接方式，都會受到保護；(4)經主管機關公告之個人資料類別才受保護。【資料保護 S1040104】

解析：依據個人資料保護法第 2 條第 1 款，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。

自我評量檢測成果評分說明

得分	溫馨提醒
100 分	資安小博士非您莫屬
80 分~90 分	小粗心，別灰心
60 分~70 分	釐清觀念，滿分到手
40 分~50 分	再接再厲，繼續努力
20 分~30 分	牛刀小試，再來一次

10 月分自我評量

是非題：(每題十分)

1. （X） 民眾負有自行妥善保存收據繳款紀錄或其他憑證的紀錄，除非民眾能透提出確切證據，否則組織遇客戶異議或投訴時，無庸先行調取內部留存資料，以查明事實。【資料保護 S1040105】

解析：組織應建立相關機制，以確保客戶資訊之即時性與正確性，並於客戶異議或投訴時，盡速調取內部留存資料，以查明事實真偽，否則一旦發生疏失行為，致客戶受有經濟損害，或其社會評價受到貶損時，將可能因此負有民事責任。

2. （X） 因應資訊時代來臨，並為加速行政作業效率，無論檔案是否經核定為機密，公務人員均可使用電子郵件傳輸且無庸特別加密？【資料保護 S1040203】

解析：依「行政院及所屬各機關資訊安全管理要點」第 27 條，已明文禁止機關人員原則上不得以電子方式傳輸機密檔案，至於有傳輸敏感性資料與文件之必要時，機關所屬人員應採取相當安全防護機制。

3. （X） 資料庫為各種資料的集合，資料庫本身呈現、檢索或資料挑選等設計，均不受我國著作權法保護？【資料保護 S1040603】

解析：資料庫為資料的集合體，依我國著作權法屬於編輯著作，因此只有在資料選擇及編排具有創作性時，資料庫設計或架構本身受著作權法保護。

4. （X） 公務機關因帳務資料未更新而錯誤寄發催款通知給民眾時，無論內容正確與否，民眾都無法主張名譽或信用受損？【資料保護 S1040404】

解析：因機關疏失而錯誤寄發的催款通知，有表彰當事人經催繳仍不願繳款之意思，可能讓第三人聽聞而對當事人誠實、信用產生質疑，進而使其在社會上之評價受到貶損，因此在此情形，民眾得向機關請求非財產上損害賠償。

5. （X） 小明寫完一封文情並茂的情書後，將情書寄給小美，寄送行為構成著作權法上所謂的公開發表？【資料保護 S1040602】

解析：所謂公開發表，依著作權法第 3 條第 1 項第 15 款：「指權利人以發行、播送、上映、口述、演出、展示或其他方法向公眾公開提示著作內容。」信件僅在兩方之間傳遞，並不是向公眾公開提示，並非公開發表。

選擇題：(每題十分)

1. （4） 請問以下何者是公務人員以私人電子郵件寄發涉及公務活動訊息，可能衍生的問題?(1)私人電子郵件系統伺服器防護不足，提高機密外洩風險；(2)電子郵件未依機密等級適當加密，提高機密外洩風險；(3)公務執行紀錄無法確實保存或配合調閱；(4)以上皆是。【資料保護 S1040203】

解析：公務人員以其私人信箱傳輸涉及公務的內容，即可能因私人電子郵件系統未有適當安全防護措施，而違反機關資訊安全管理規範，並提高機密外洩之疑慮；且以私人電子郵件信箱收發涉及公務內容，可能規避機關主管監督，並導致公務執行紀錄無法確實保存或配合調閱，而有礙檔案保存與備查。

2. （3） 請問資料庫所有人權若欲限制他人，以自動化程式擷取資料庫所屬個別資料內容從事商業利用，採取以下何種方式較有理由？(1)資料屬於不具有創作性的新聞事實時，得依著作權法主張排除侵害；(2)資料內容為我國法規命令時，得依著作權法主張排除侵

害；(3)使用者利用行為違反網站服務條款，得終止服務；(4)主張使用者偽變造資料庫電磁紀錄而涉有刑責。【資料保護 S1040603】

解析：當資料庫內容本身屬於不具有創作性的新聞事實或我國法令，即不受著作權法保護 。但資料庫所有人雖無法以著作權法限制使用者不當利用行為，在使用者之利用行為如涉及榨取其他事業努力成果、造成網站系統設備干擾或違反網站服務條款，致生他人損害時，仍可能依其他法律循求救濟。

3 （2） 以下何者為民眾維護手機資訊安全的可行方式？(1) 看到不明簡訊所附網址，趕快點開確認內容；(2)定期更新手機防毒軟體；(3)手機不會被植入木馬程式，因此可以大量下載各種應用軟體；(4)維護手機資訊安全是手機製造廠商的義務，與民眾完全無關。【資料保護 S1040203】

解析：為降低民眾手機資訊安全風險，民眾本身亦須達到某程度注意義務，避免下載不明軟體或點選簡訊提供的可疑網址，並定期更新手機防毒軟體。

4 （1） 下列何者是受到著作權法保護的著作？(1)私人信件;(2)國家考試的題目；(3)政府公文；(4)交通號誌。【資料保護 S1040602】

解析：依著作權法第 9 條第 1 項：「下列各款不得為著作權之標的：一、憲法、法律、命令或公文。二、中央或地方機關就前款著作做成之翻譯物或編輯物。三、標語及通用之符號、名詞、公式、數表、表格、簿冊或時曆。四、單純為傳達事實之新聞報導所作成之語文著作。五、依法令舉行之各類考試試題及其備用試題。」選項 2、3、4 分別為第 9 條第 1 項的第 5 款、第 1 款、第 3 款。而私人信件則是作者精神的產物，可表彰其個性或獨特性，應為著作權所保護的著作。

5. （3） 軟體開發商若欲蒐集用戶撥打電話的資料從事分析，應遵守以下何項事項，是符合我國個資法規定?(1)通訊紀錄非屬個人資料，軟體開發商得自行蒐集，不受限制；(2)軟體開發商並非我國個資法適用行業；(3)軟體開發商蒐集用戶資料應符合個資法第 19 條其一事由並向用戶告知；(4)通訊紀錄為特種個資，軟體開發商不得蒐集。【資料保護 S1040106】

解析：電話撥打時間、地點及電話型號等，屬於社會活動範疇中之資料，因此軟體開發商蒐集此類資料應遵守個資法相關規定；又軟體開發商蒐集用戶資訊，並分析用戶通訊行為時，依法應事先告知並符合蒐集個資之其一事由。

自我評量檢測成果評分說明

得分	溫馨提醒
100 分	資安小博士非您莫屬
80 分~90 分	小粗心，別灰心
60 分~70 分	釐清觀念，滿分到手
40 分~50 分	再接再厲，繼續努力
20 分~30 分	牛刀小試，再來一次

11 月分自我評量

是非題：(每題十分)

1. （X） 因同一事件而受害之多數個資當事人，若欲循團體訴訟方式降低個別起訴請求賠償的勞費成本，僅能將訴訟實施權授與政府機關。【資料保護 S1040108】

解析：依我國個資法修正新增的團體訴訟制度，因同一事件受有損害的個資當事人達 20 人以上時，得將訴訟實施權授與符合特定資格的財團法人或公益社團法人，由其代表個資當事人進行訴訟。

2. （X） 醫療軟體與實體裝置有所不同，故我國醫療器材管理規範未涵蓋醫用軟體或應用程式？【資料保護 S1040501】

解析：依我國衛福部食藥署發布之「醫用軟體分類分級參考指引」，經考量「是否符合藥事法第 13 條醫療器材定義」、「是否宣稱具診斷、治療功能或協助診斷、治療」等原則，認定該軟體屬於醫療器材者，將納入醫療器材進行管理。

3. （X） 為保障營業自由與國際貿易發展，我國主管機關無論在任何情形，均不得禁止我國組織機構將個人資料傳輸至第三國？【資料保護 S1040108】

解析：我國個資法第 21 條第 3 款，授權中央主管機關於「接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞時」，得限制非公務機關將個人資料傳輸至第三國，以保護我國民眾個資安全。

4. （O） 行為人盜用使用者的帳號密碼登入網站，在未獲得使用者授權或沒有正當理由之情況下，將可能構成無故輸入他人帳密罪？【資料保護 S1040405】

解析：行為人盜用使用者的帳號密碼登入網站，不論行為人取得該帳號密碼之來源為何，在未獲得使用者授權或沒有正當理由之情況下，均屬於刑法第 358 條所指「無故輸入他人帳號密碼，而入侵他人之電腦或相關設備」之情況，而涉有刑事責任。

5. （O） 駭客以殭屍網路癱監視攝影機，恐構成無故干擾他人電腦罪而負有刑事責任？【資料保護 S1040406】

解析：以我國刑法第 360 條規定 ，無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致公眾或他人發生損害時，將構成無故干擾電腦罪。因此，駭客以殭屍網路癱監視攝影機，致他人受有損害時，即可能構成該罪。

選擇題：(每題十分)

1. （4） 關於個資法規定，因同一原因事實，造成多數當事人權利受侵害事件之損害賠償,以下說明何者正確?(1)合計最高總額以新臺幣 5 億元為限；(2)無論人數多寡，每人每一事件最低賠償金額均為 500 元；(3)原因事實所涉利益超過賠償上限時，仍以賠償上限為準；(4)以上皆非。【資料保護 S1040108】

解析：依個資法第 28 條規定，對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受每人每一事件最低賠償金額新臺幣五百元之限制。

2. （4）關於醫用軟體可能適用的法律規範，以下何者正確？(1)程式開發商提供應用程式給消費者時，依消保法應確保服務當時科技或專業水準可合理期待之安全性；(2)應用程式涉及蒐集病患個資時，服務供應商依個資法應採取相當技術上適當安全維護措施；(3)醫用軟體涉及疾病診斷或治療時，可能受醫療器材管理辦法之規範；(4)以上均屬正確。【資料保護 S1040501】

解析：服務供應者從行動應用程式開發、運作、修正到終止服務各生命週期階段，均應確保其安全性與可用性，依程式功能、目的及使用對象等，判斷是否適用消保法、個資法及醫療器材管理辦法之規定，以維護使用者權益。

3. （3）駭客透過勒索軟體將受害人電腦檔案加密，向受害人要求支付一定財物。若受害人拒絕支付贖金，就無法使用或存取檔案。此行為可能構成我國刑法上何罪？(1)洩漏業務上知悉工商秘密罪;(2)偽造變造通貨、幣券罪；(3)恐嚇取財罪；(4)侵占遺失物罪。【資料保護 S1040405】

解析：駭客基於營利目的，透過勒索軟體造成對於使用者所保有資訊完整性與可用性的威脅，迫使使用者交付財物，亦可能同時構成刑法上恐嚇取財罪，而負有刑責。

4. （2）鑒於受害人資料一旦被勒索軟體加密，以目前的解密技術及設備能量，恐怕難以在短時間內解密成功。為防範勒索軟體威脅，請問以下何者並非有效方式？(1)強化人員資安意識教育訓練；(2)學習人身安全防衛術；(3)避免點選不明電子郵件或連結；(4)資料異地備份。【資料保護 S1040405】

解析：目前勒索軟體受害人遍及個人與企業用戶，然而鑒於勒索軟體付款機制精密而難以追查，且自行解密恐耗費時日而緩不濟急，因此根本之道仍是強化使用者資安意識，避免下載可疑軟體檔案，並配合定期資料備份，以提升本身資料遭到惡意毀損或滅失時之因應能力。

5. （3） 行為人盜用使用者的帳號密碼登入網站，請問關於網站責任，以下何者正確? (1)此為行為人個人行為，網站完全沒有任何責任；(2)無論網站是否已採取安全維護措施，只要使用者帳號遭盜用，網站均須負責；(3) 若網站已採取防護措施，符合當時科技或專業水準可合理期待之安全性時，無庸負責；(4)帳號密碼遭盜用為使用者管理不當，網站沒有任何責任。【資料保護 S1040406】

解析：依我國實務見解，如業者已善盡各項告知與提醒義務，並提供各項防護措施，防範駭客入侵，而得認符合當時科技或專業水準可合理期待之安全性時，對於使用者之損害即不負賠償責任。

自我評量檢測成果評分說明

得分	溫馨提醒
100 分	資安小博士非您莫屬
80 分~90 分	小粗心，別灰心
60 分~70 分	釐清觀念，滿分到手
40 分~50 分	再接再厲，繼續努力
20 分~30 分	牛刀小試，再來一次