編 者 序

在 21 世紀資通訊科技蓬勃發展上，網際網路所帶起的資訊革命已風起雲湧，一日數變。由於資訊科技開放、自由、易於使用等特性，讓網路已成為個人、組織、政府間訊息交換、傳遞的重要管道，民眾的生活型態與商業模式也因此產生了重大變革。但隨著各行各業加深資訊化應用的同時，電腦及資訊設備應用的安全風險也隨之提高：諸如國家機密、商業資訊外洩，網路入侵、駭客攻擊、個人資料遭盜用，甚至是色情、誹謗言論的散播等等，以及不當或違法的資訊應用態樣，輕則影響個人權益、社會安定，重則危及國家安全。

綜觀各國之相關資訊應用的整備度已成為國際組織衡量國家競爭力的重要指標，而安全的議題更成為各國政府高度重視並積極構思強化的面向。我國在民國 90 年 1 月由行政院通過「建立我國通資訊基礎建設安全機制計畫」，成立行政院國家資通安全會報，開啟了政府有計畫推動我國資通安全建設之路。透過政府、企業及學界的努力，資訊安全的概念已逐漸為民眾所了解，惟多數民眾至今仍將資安概念侷限於軟硬體設備的採購與安裝，而疏忽了對整體資訊應用安全

意識的強化，使得有心人士有機可乘。要如何喚起民眾資安風險意識，並建立安全無虞的資訊應用環境，遂成為現階段政府推動電子化的重要目標。

為協助政府及社會各界了解網路應用可能衍生的安全議題，建立完整的法律概念，行政院研考會特委託財團法人資訊工業策進會科技法律中心摘錄近一年來廣受矚目的國內外案例，希望透過對實務案例的分析與說明，建立各界對網路資訊應用應有的法治觀念，提高民眾風險意識。鑑於資通安全議題涉及的層面甚廣，如何透過管理手段降低應用風險，消弭犯罪於無形，亦為國家資通安全法制建設重要的一環。本案例手冊本次納入實務相關管理建議供各界參考，誠摯希望透過本案例手冊的說明與分析，為我國資通訊環境應用法制宣導略盡棉薄之力。

財團法人資訊工業策進會科技法律中心 撰稿
行政院國家資通安全會報技術服務中心 謹誌

目　錄

壹、電腦與網路犯罪

一、妨害電腦使用

【案號：1101】

你的無名小站，被無名氏竄改資料了嗎？

【資料來源：台北地方法院 95 年度訴字第 1543 號】

事件描述

周女與羅女原係好友，因細故心生嫌隙，周女先後二次未經羅女同意，使用其帳號、密碼登錄羅女在無名小站所申請的網站，刪除、變更網頁內容，且刊登不堪入目的描述與援交訊息，供不特定人上網瀏覽。羅女發現後報警處理，然已嚴重損及其名譽。

法律意見

隨著網路的高度發展，民眾對網路的依賴性愈來愈深，各種傳統或新興的犯罪態樣相繼發生於網路空間中。特別是網路具有散布迅速與可匿名性之特性，其無遠弗屆的影響力，也讓各類犯罪的影響層面擴大，讓現行法令以及執法單位面臨巨大的挑戰。

為因應網路入侵型犯罪，我國於民國 92 年通過刑法第三十六章「妨害電腦使用」罪章，將包括無故入侵、

無故取得刪除變更電磁紀錄、無故干擾電腦系統、與製作專供犯罪電腦程式等四種犯罪型態納入刑罰規範。本案事實中，周女未經羅女同意，輸入羅女帳號與密碼登錄網站之行為，已明顯觸犯刑法第 358 條入侵電腦罪，得處三年以下有期徒刑、拘役或科或併科十萬元以下罰金；而其刪除、變更羅女個人網頁資料之行為，可該當同法第 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罪，得處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。兩罪數罪並罰，就周女入侵網站進行破壞之行為，即可能被處以高達八年的有期徒刑。

除此之外，周女為損害羅女名譽目的，刊登毀謗羅女之描述與援交訊息，可另成立刑法第 310 條第 2 項的加重誹謗罪，依法得處二年以下有期徒刑、拘役或一千元以下罰金。

在網路虛擬空間中，帳號與密碼成為識別個人身分的重要憑據。雖然當事人事後得以法律途徑尋求救濟，但類似妨害名譽行為，其透過網路所造成的損害實無法具體評估。類似案例另常見於親密愛人共用帳號與密碼，其後因故分手而報復。所有網路使用者宜明瞭於此，妥善保管自己的帳號與密碼，以免造成遺憾。

【案號：1102】

用垃圾郵件「駭」對手只為搶生意

【資料來源：東森新聞網 2004/7/13】

事件描述

2004 年在高雄發生一件兩家距離五十公尺的網咖為搶客源，利用電腦長才而攻擊對方網路系統之案例。經警方追查發現，較晚開幕的網咖老闆曾為另一家網咖系統架設時之工程師，其後自行創業，為了搶客人而扮演電腦駭客，利用寄發大量垃圾郵件手法，意圖癱瘓競爭對手的網路系統，讓其網路傳輸速度變慢，進而影響其生意。

法律意見

本案行為人藉由在一段時間內消耗網站對外頻寬資源，使得頻寬流量擁塞而無法正常提供相關網路服務的一種攻擊方式，又稱為「阻絕服務」（Denial-of-Service，簡稱 DoS)攻擊。

阻絕服務攻擊並不以篡改或竊取主機資料為目的，而

是癱瘓系統主機使之無法正常運作。由於一般網路系統的系統資源(例如記憶體、磁碟空間以及網路頻寬等)有限，有心人士可以根據部分網路系統或相關通信協定設計或實作上的漏洞，在短暫時間內透過傳送大量且密集的封包至特定網站，使該網站無法立即處理這些封包而導致癱瘓，讓正常用戶無法連上該網站而被阻絕在外。這種攻擊對網站設備本身而言並不具破壞性，只是造成系統無法即時處理所傳送的大量指令而停滯或當機。

為嚇阻此類阻絕式攻擊事件的發生，我國於增訂刑法第 36 章妨礙電腦使用罪章時，特別加入第 360 條無故干擾他人電腦與相關設備罪，若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，依本罪之規定，得處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。本案中的網咖店老闆為了搶生意，故意透過傳送大量垃圾郵件方式，試圖癱瘓競爭對手網路之行為，即可能觸犯本條規定。

【案號：1103】

下載新版 MSN？當心變成殭屍電腦

【資料來源：資安人 2006/1】

事件描述

2006 年 1 月出現了一種「蘭迪斯變種 F」病毒(Backdoor.Landis.f)，它偽裝成流行的網上聊天工具 MSN8.0 的測試版本，自動向 MSN 上的好友名單發送 MSN8.0 新版發布的消息，誘騙其他人點擊隨附網址，該網址指向一個仿冒微軟公司的下載網站，用戶只要從這個網站下載運行「MSN8.0 測試版」，電腦就會中毒，成為遭駭客得以遠端控制的殭屍電腦，除了可能被盜取個人隱私資訊外，也可進一步被做為其他犯罪的工具或跳板。

法律意見

所謂「電腦病毒」，在技術上來說，是一種會自我複製的電腦程式執行檔：有些電腦病毒於程式被執行時，會破壞檔案資料、重新格式化電腦硬碟，有些電腦病毒會暗藏指令，自動運行電腦擁有者所不知道的功能

，或竊取資料，或修改應用程式，干擾整個電腦系統的運作等等。就算病毒未發作，它也可能佔據電腦系統中的記憶體空間，並尋找機會自行繁殖複製，使電腦運算變得遲緩。

近年來透過資安教育的宣導與資安軟體廠商在技術方面的努力，關於電腦病毒感染造成大規模損害的新聞已經少見。目前實務上較具危害性的病毒，為具有後門功能的智慧型病毒。這類程式的設計通常具有針對性，或針對特定對象(如金融服務業)，或針對特定系統程式漏洞、應用環境不斷地變種，再搭配社交工程，利用人性的弱點散布，一般網路使用者甚難察覺與防範。而中毒後的電腦，則常被用來當作跳板，作為掩飾駭客身分或隱藏攻擊來源的屏障。

從法律層面而言，只要當事人能證明因病毒散布而造成的損害、能確認施放病毒或入侵者身分，均可以透過法律求償；我國更為了遏止此類惡性程式的製作，特別於刑法第 362 條訂有「製作專攻犯罪電腦程式罪」。惟病毒或木馬程式的散布，往往透過大量的跳板轉接，實務上欲發現病毒製作者或入侵者的真實身分可說相當困難；而在跳板雙方當事人均可能為受害者的情況下，相關侵權行為的損害賠償責任更難釐清。

網路環境雖然危機四伏，但也不需因噎廢食。只要每位網路使用者都能具有資訊安全風險意識，不隨意開啟、接收或下載來路不明的檔案，並善用資安工具，定期進行資安防護工作，才可能避免成為別人犯罪的幫凶，保護自己也保護別人。

【案號：1104】

自動更新的病毒專攻台灣區

【資料來源：Digitimes 電子時報 2006/10/2】

事件描述

「防毒軟體會自動更新最新的病毒碼，以防止病毒與惡意程式的攻擊」是眾所周知的常識，現在這樣的動作連病毒也學會了。2006 年 1 月出現的新型態巴克雷病毒(W32.Bacalid)，在成功入侵電腦後，會自動連回網路檢視病毒本身有沒有最新的版本，而後自動上網更新最新的攻擊模式，偽裝變身以規避掃毒程式。目前似乎只有在台灣地區以及使用繁體中文的作業系統環境中發現該病毒蹤跡。

法律意見

資安防護工作，如同「官兵捉強盜」，一直以來是與時間賽跑的工作。新品種病毒與木馬程式的不斷出現，已讓定期更新程式碼、根據通報下載補丁程式成為機關(構)網管人員強化資安防護的例行性工作，然而這樣的安全防護模式已不足以因應多變的網路環境。巴

克雷病毒的出現，其靈活的變身攻擊模式，凸顯了機關(構)應對網管人員強化專業的重要性。概善用市售的防毒軟體固然有助於阻絕病毒，降低損害發生的可能性，但過份倚賴掃毒程式，卻可能形成網管工作上的盲點。例如本案自動更新病毒的發現，實有賴於專業網管人員對封包流量與連線紀錄檢視時的敏銳度才可能致。

關於連線紀錄的保存議題，目前除了第二類電信事業管理規則對網路連線服務提供者(Internet Access Provider)有所規範外，並未見於其他法律。但為了協助機關(構)做好資安防護工作，仍建議機關(構)依據自身需求，參考「行政院及所屬各機關資訊安全管理要點」，建立機關(構)的資訊安全紀錄保存與稽核制度，定期或不定期進行稽核作業，並禁止任意刪除及修改系統中之稽核紀錄檔案；其中最重要者，仍是建立機制，強化網管人員之專業，避免定期或不定期的稽核檢視工作流於表面而不自知。

【案號：1105】

Freedom 程式讓設計者沒有 freedom

【資料來源：台灣 FTP 聯盟 2006/8/30】

事件描述

刑事局於 2006 年 8 月破獲「Freedom」穿越封鎖線駭客程式案，嫌犯為知名銀行資訊室電腦工程師，聲稱純為友人解決電腦被公司設限、上班時不能上網聊天「打發無聊」的問題而撰寫此程式，不知觸法。由於此程式著重隱藏及穿透防護功能，被認定是有攻擊性的木馬程式，警方依妨害電腦使用罪將他送辦。

法律意見

企業或機關(構)進行網管的第一步，即是根據使用者的身分進行權限設定，並分層管理，或藉此限制特定應用軟體的使用權限，或避免無權限者得以接取到具有機密或敏感性的資料。近年來，更由於網路已成為病毒散布、資料外流的重要管道，有越來越多的企業或機關(構)會對內部員工的網路應用行為加以設限，會刻意封鎖如 MSN、Skype 等即時通訊軟體，或限制電

子郵件的收發，甚至是禁止上網。即使如此，高階主管的電腦使用權限仍相對比基層員工高。

本案中的「Freedom」穿越封鎖線程式，據報載，即是利用此分層設限的機制，讓組織內部具有較高權限主管的電腦(代稱A)被植入程式後，其他原本沒有上網權限的電腦(代稱B)得藉由已被該程式控管的電腦A轉介上網，使原有的系統保護管制措施形同虛設，遂其協助使用者達到上網之目的。

從技術層面言，此程式的運作涉及到破解電腦保護措施(刑法第358條)、植入遠端控制程式(刑法第359條)、干擾系統依正常指令運作的穩定性(刑法第360條)，從而此程式的設計者，可構成刑法第362條之「製作專供犯罪電腦程式罪」；不論是供自己或他人使用，只要對公眾或他人造成損害時，可處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

簡而言之，當事人不管是為滿足成就感而挑戰、測試他人設置之資安防護措施，或是單純好奇想驗證自己製作程式能力，或是想宣洩對社會或組織的不滿，或如同本案例，僅純粹為自己或親朋使用之便利而製造具有入侵、破壞、干擾功能之電腦程式時，應留意這

類程式的執行或散布是否可能對他人或公眾造成損害，否則將有觸法可能，程式設計者不可不慎。

二、網路犯罪

【案號：1201】

網路釣魚，願者上鉤？

【資料來源：卡優新聞網 2007/1/5】

案例事實

2007 年 1 月有不肖集團以聯 X 銀行網站為樣本，製作與聯 X 銀行首頁相同的網頁，並以該銀行名義發出數十萬封以「銀行系統轉換，重新登錄」為標題的電子郵件，要求銀行用戶點選郵件末隨附的極相似網址，上網重新確認帳號及個人密碼。當用戶連上該偽冒網站時，即被植入木馬，竊取個人密碼及信用資料；歹徒隨後更利用相關資料盜領存款、盜開支票，甚至複製信用卡詐欺取財。

法律意見

所謂網路釣魚，英文為 Phishing，與 Fishing 發音相同，主要因為早期是以盜撥電話來詐騙財物，所以將「Phone」和「Fishing」兩字結合為 Phishing。現在則是指利用網站連結、電子郵件、即時通訊等工具，誘騙網友進入與企業或組織網站相似的網頁，騙取帳

號或是植入木馬程式，更進一步詐取受害人的財物。這類犯罪由於具有經濟上的誘因，已迅速成為目前國內外嚴重的詐欺犯罪態樣。

由於資訊化社會的發展，許多的文字或圖像都已經電子化，並相當程度足以表示其用意之證明，法律上即將其擬制為「文書」，適用文書保護之相關規定。以本案為例，行為人以商家名義向不特定多數人發送電子郵件之行為，即可能構成我國刑法的第 210 條偽造準文書罪；郵件內含偽造首頁及偽冒網址之行為，即可能違反了著作權法第 91 條，侵害網頁著作人重製權，也可能涉及使用他人商標中之文字作為來源之標識，成立商標法第 62 條的侵害商標權罪。

關於竊取帳號密碼的部分，不論是網友誤入極為相似的網站而輸入帳號密碼，或行為人透過木馬程式竊取，有可能成立刑法第 359 條取得電磁記錄罪。最後，行為人以竊得之帳號、密碼進入銀行網站，進而將被害人帳戶內存款轉走之行為，視行為的階段性，可能成立刑法第 358 條之無故入侵罪，也可能成立第 339-3 條之電腦詐欺罪，分別為 3 年與 7 年以下的刑責。如歹徒用以製作偽卡，可構成刑法第 201-1 條的偽造支付工具罪，可處 1 年以上、7 年以下有期徒刑。

網路釣魚詐欺多是利用人性弱點進行誘騙，或要求收信人及時回覆、或提供虛假網址連結誤導被害人。面對層出不窮的犯罪手法，消費者對於網路之應用要有所警惕，除應定期更新安全防護軟體及更新瀏覽器漏洞修正外，更要謹慎小心，不要輕信不明的電子郵件，或隨意點擊廣告連結，並儘可能注意加註防釣安全標章(Sign-in Seal)，以確保擁有安全的網路使用環境而免於受騙。

【案號：1202】

在網路賭博就可逃過一劫？

【參考資料：民視新聞網 2007/1/20】

案例事實

政府的運動彩券雖仍在規劃階段，但事實上民間早就大賭特賭。2007 年 1 月警方接獲線報破獲了一個網路賭博集團，該集團專賭美國職籃 NBA，每注最少一萬元，才開張一個月，賭金將近千萬元。

法律意見

近年來，台灣已逐漸開放公益目的的博奕遊戲，如大樂透或台灣彩券，但民眾仍須注意的是，刑法仍未將賭博罪予以除罪化，參與未經政府許可的賭博遊戲，仍屬於犯罪行為。

就本案事實分析，提供網站的業者因同時提供不特定多數賭客進入該網站賭博，其行為可能構成刑法第 268 條之聚眾賭博罪。或許有賭客會以為，只要網站不設在台灣地區，便可規避我國刑責，但根據刑法第

4 條規定，「犯罪之行為或結果，有一在中華民國領域內者，為在中華民國領域內犯罪」，因此，縱使網站架設在國外，但使用者或操作者在我國領域內從事犯罪行為，我國政府仍有審判權。

【案號：1203】

色情資訊土石流

【資料來源：聯合新聞網 2007/3/07】

案例事實

檢警於台北縣偵破一販賣色情光碟案，行為人利用知名網站成立「女友的私房相簿」家族網頁，張貼色情圖片並販售色情光碟，這些色情光碟中包含賓館、廁所偷拍，甚至還有未滿 18 歲的「幼幼片」。行為人為了達到宣傳網站的效果，還徵得妻子同意，將兩人性交的自拍畫面拷貝成色情光碟販售。

法律意見

所謂網路色情，指在網際網路上公開張貼或散布裸露、猥褻或低俗不雅的文字、圖片、聲音、動畫與性交易資訊。但何為猥褻？何為低俗不雅？由於憲法保障民眾的言論自由權，且對猥褻、色情等的認定標準亦會隨社會發展、風俗變異而有所不同，其界線甚難釐清。雖然如此，考量兒童及少年之心智發展未臻成熟，國家採取適當管制措施以保護兒童及少年免於被

迫從事任何非法之性活動或性引誘，至為重要。此亦為聯合國兒童權利公約所宣示普世價值之基本人權。

本案例首先值得討論者，即為這些色情圖片的來源取得問題。如所謂的「幼幼片」為行為人自行拍攝、製作，或引誘、媒介使未滿 18 歲之人被拍攝、製作相關圖畫、錄影帶、影片、光碟、電子訊號或其他物品時，行為人無疑該當兒童及少年性交易防制條例第 27 條之「拍攝製造猥褻物品罪」，得處六個月以上五年以下，或一年以上七年以下有期徒刑。若其來源係以廁所、賓館偷拍方式取得，涉及無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動或身體隱私部位者，可構成刑法第 315-1 條之「妨害秘密罪」，得處三年以下有期徒刑、拘役或三萬元以下罰金。

若不涉及來源問題，則本案行為人張貼、散布、播送、公然陳列或販賣色情光碟之行為，另構成刑法第 235 條之販賣猥褻物品罪，與兒童及少年性交易防制條例第 28 條之散布或販賣姦淫猥褻物品罪，得處三年以下有期徒刑。

為避免讓未成年人接觸到不該接觸的色情資訊，我國已於 2004 年 4 月 26 日公布實施「電腦網路內容分級

處理辦法」,要求平台提供者與內容提供者需就其內容標示分級標誌，並設置管理員以及時發現、及時移除不當資訊。即便如此,網路過濾和分級制度皆非萬能，仍應仰賴學校、家庭和社會三方面的配合，建立兒童及青少年正確的性觀念，才可能有效遏止網路色情對於兒童及青少年的危害。

【案號：1204】

轉寄誹謗郵件有罪

【資料來源：中國時報 2007/04/28】

案例事實

南部某家知名冷飲店一再遭人惡意中傷，在電子郵件、網路留言版或聊天室上經常發現有詆毀性的文章，包括「該家冷飲店的飲料含有茶精、添加代糖，吃多會致癌」等內容，該公司摘錄 30 多封網路留言及相關轉寄電子郵件後報請台南市刑大偵辦，警方詢問幾位措辭嚴重且強烈的行為人到案說明後移送地檢署。

法律意見

網路是一個匿名的虛擬空間，似乎每個人都可以在網路上想做什麼就做什麼，也因其具有訊息散布快速、使用者得匿名的特性，有不少網友誤以為實體社會的法律、道德或倫理的界線在網路虛擬空間可以不用遵守而無所顧忌的發表言論，因此網路上流傳的各種言論內容可謂千奇百怪。例如早年流傳的「某公司所生

產的衛生棉會長蟲」或「XX 公司所販售的雞肉為基因雞」、「XX 醫院的醫生罔顧人命」等等，網友在收到或看到這樣的訊息或文章後覺得感同身受，或覺得有必要伸張正義，提醒親友注意，往往不加思索地將文章再次轉寄出去，殊不知此等行為可能觸犯了法律。

依目前實務見解，行為人透過網路將涉及妨害名譽內容的郵件轉寄給大量連絡人時，可被認定「顯有散布於眾」的意圖，可構成刑法第 310 條的誹謗罪「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，處一年以下有期徒刑、拘役或五百元以下罰金」。又，如果網友為取信於人，隨附說明圖片或文字並透過網路傳送，此時可成立第 310 條第 2 項之加重誹謗罪；即使謠言不是由行為人首先發表，只要行為人在收到謠言後又轉寄出去，也可能構成此罪。

建議網友處理這些真假難辨的電子郵件時，在未經查證前最好不要轉寄予他人，萬一這些消息是錯誤的，甚至是有心人惡意散布以打擊對手時，轉寄者也許只是出於好心想提醒親朋好友，卻可能因此須負擔法律責任。當然，轉寄者或許可以提出抗辯，表示並沒有犯罪故意，但依照民法第 195 條，此等行為若侵害了他人的名譽或信用，恐怕仍須負起民事損害賠償責

任。網友在轉寄類似郵件時宜謹慎。

【案號：1205】

恭喜你得標！小心網路劫標客

【資料來源：大紀元 2006/7/9】

案例事實

台中市有名女子在知名拍賣網站上以 3400 元標得一部中古相機，結標後隔天便收到自稱是賣主寄發的得標確認電子郵件，便依信中留下的手機號碼聯絡對方，對方要她將貨款匯到指定帳戶，即可收到貨品。買家依指示將錢匯進賣家帳戶後，卻遲未收到商品，再次與對方聯絡卻無任何回音，直到重新查看信箱，又發現了真正賣主的確認信後，才知上了網路劫標客的當。

法律意見

網路交易自 2005 年起遭劫標集團擾亂至今，已逾 4,000 件無法偵破，嚴重危害網路交易安全。根據警方的統計,近年來網路詐騙案件逐年呈倍數成長,2006 年 1 月至 8 月，警方受理網路詐騙案達 4,600 餘件，是 2004 年的兩倍，也超越了 2005 年的 3,800 件，顯

見網路已成為詐騙集團從事犯罪的新管道。

網路劫標多半是發生在下列情形：劫標客通常會盯上快結標商品的出價者，等商品結標後，利用與真賣家極為相似的帳號，或者提供與賣家一模一樣郵件帳號，佯稱賣方而發給買方得標通知信，要求轉帳到某帳戶；信的內容多半以出國、出差等理由，要求買家儘早匯款，並強調因此將另外給予折扣。劫鏢客同時也可能通知買家，稱其因為電話或手機故障，請買家勿以電話聯絡等，以延遲犯罪被發現的時間。

從法律觀點，雖然這類犯罪的手法千變萬化，但其行為可概括論以刑法第 339 條之詐欺罪，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，或得財產上不法之利益者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。

網路拍賣雖然便利，但在保障自身權益考量下，建議喜好網路拍賣的網友可以選擇「見面交易」或「貨到付款」方式，或選擇利用拍賣網站提供的交易認證機制，以降低詐騙風險。若堅持郵寄取貨，建議網友對結標商品頁面的資訊應多加留意，並於匯款前主動跟賣家聯絡，確認收到的匯款資料是否正確無誤，以保

護自身權益。

【案號：1206】

虛擬竊盜，實體制裁

【資料來源：卡優新聞網 2006/11/09】

案例事實

某位 19 歲的電腦高手，利用網路入侵他人電腦，取得網友的遊戲帳號、密碼後，以竊取到的帳號和密碼登入遊戲伺服器，並將他人遊戲角色中所有的珍貴裝備與寶物轉移給自己遊戲中的角色。警方循線查獲後，將該名青少年移送法辦。

法律意見

網路遊戲玩家因為遊戲中竊取他人的虛擬寶物而衍生的官司時有所聞。根據內政部警政署偵辦電腦犯罪案件的成果報告，網路竊盜案件已躍升為排行榜第一名，其中絕大部分是虛擬寶物的竊盜案件。

竊取寶物的行為雖然發生在虛擬遊戲世界中，但仍可構成犯罪而受到刑法的制裁。就本案事實分析，行為人入侵他人電腦的行為，即違反了刑法第 358 條「無

故入侵電腦罪」，最高可處三年以下有期徒刑、拘役或併科十萬元以下罰金。行為人以竊得之帳號密碼登入遊戲伺服器，進而移轉其他玩家之虛擬寶物給自己遊戲中的角色，有可能構成刑法第 359 條「無故取得他人電磁記錄罪」；但也有見解認為，行為人藉由輸入不正確指令而獲得不法利益，可構成刑法第 339-3 條「不正使用電腦詐欺罪」，最高可處七年以下有期徒刑。

有鑑於線上遊戲發展快速，衍生問題不斷，遊戲廠商卻往往片面以「定型化契約約款」或「遊戲管理規則」排除己身責任，經濟部於 2005 年初修訂有「線上遊戲定型化契約範本」，針對虛擬貨幣或寶物被盜取之糾紛設計出一套保護機制條款，除要求業者應於此類糾紛發生時，積極介入玩家與第三人間，協助釐清事實真相外，更要求業者應維持消費者相關電磁紀錄保存之完整，至少保留 30 日之遊戲歷程提供玩家參閱。

有效解決線上遊戲糾紛，可說是遊戲產業發展的關鍵。透過契約條款明確區分玩家與遊戲公司的責任歸屬外，仍建議遊戲公司應加強設備的安全性，而玩家亦應定期更新防毒軟體及執行更新系統，建立保護虛擬財產的觀念，於發生糾紛後積極主張自己的權利，如此才能使遊戲回歸娛樂面的意義。

【案號：1207】

部落格分享音樂，違反著作權法？

【資料來源：聯合新聞網 2006/10/10】

案例事實

國內盛行網路部落格(Blog)文化，部落格作者常以文章配上優美的音樂，以豐富自己的文章及網誌內容，然而多數的部落格作者可能不知道，在部落格內分享音樂，其實有觸法危險。各地方法院判決相繼出現，網友應提高警覺。

法律意見

部落格作者在網誌內以音樂搭配自己的文章，或提供音樂檔案供他人聆聽、轉貼，這些互動、分享的機制原本是網誌文化盛行的原因之一。但部落格作者卻可能因為上載分享的音樂使用量過大，而難以主張著作權法中的合理使用。雖然部落格作者被判刑的刑期通常不重，且可易科罰金，但是這樣的判決結果確實為部落格文化投下一個震撼彈。

從法律層面分析，部落格作者上傳音樂於網路空間或透過超連結與網友大量分享歌曲檔案的行為，可能構成著作權法第 91 條第 1 項之重製罪。其將音樂放在網誌內，供不特定網友點選聆聽的行為，則違反了第 92 條的公開傳輸而侵害著作財產權之規定。所謂的「公開傳輸」，係指以有線電、無線電之網路或其他通訊方式，藉聲音或影像或公眾提供或傳達著作內容，包括使公眾得於其各自選定之時間或地點，以上述方法接收內容。因此，部落格作者設置音樂檔案，也許只是想方便自己聆聽，但因網際網路的特性，已使部落格內容置於公開傳輸或接受的狀態而觸法。

依目前各地方法院就部落格作者侵權案的判決結果，部落格作者利用別人的音樂著作，但未取得其音樂著作權人授權的行為，一旦遇到音樂著作權人主張其權益時，部落格作者雖無商業行為，仍恐無法主張合理使用，而被認定為有罪。建議部落格作者在提供分享機制時應審慎之。

貳、資訊安全管理

一、無線網路與新興科技

【案號：2101】

悠遊無線應注意安全

【資料來源：大紀元 2006/2/14】

事件描述

2006 年 2 月 14 日刑事局破獲國內第一例利用無線溢波盜刷信用卡之犯罪。該犯罪集團為逃避、干擾警方追查，四處以租屋方式尋找可盜用之無線溢波，或暫住可接收無線網路的飯店，再上網盜刷信用卡購物，不法獲利至少數百萬元以上。

法律意見

隨著寬頻網路環境的普及，無線網路設備價格的下降，民眾已可輕易且自由自在地在許多公共場所及家中使用無線網路，享受隨時飆網的便利。不過此種新興的上網模式，也為機關(構)網路安全的維護工作帶來困擾。概在有線網路環境下，網管人員還可藉由對有線區域內的設備掌控進行管理，但行動載具搭配無線網路，打游擊式的上網態樣，確實容易讓網管人員無所適從。有機關(構)乾脆禁止使用無線網路，但即

使如此，來自隔壁大樓或街上便利商店的無線溢波，可能仍讓網管人員防不勝防。

在台灣，民眾自行架設小型無線基地台的情形相當普遍。或許有些人不介意讓別人借用多餘頻寬，但出借者仍必須留意，未經管理的無線溢波容易成為有心人士混淆辦案或逃避犯罪查緝的途徑。本案即是網路新興科技被利用以逃避犯罪追緝的案例。

從法律層面分析，行為人如果是透過破解保護措施方式進入他人無線網路時，此時已違反刑法第 358 條之無故入侵電腦相關設備罪。而行為人上網盜刷信用卡之行為，也違反了刑法第 339-3 條之詐欺罪，可處以七年以下有期徒刑。

無線上網技術雖然帶給民眾隨時上網的便利，卻不可避免遭犯罪集團濫用，輕則佔用頻寬、干擾網路穩定度，重則散布病毒、惡意攻擊、甚至竊取機密隱私資料，造成難以彌補的損失。建議架設有無線基地台的民眾應重視無線溢波管理之問題，做好基礎安全防護，一方面以加密方式限制無線網路接取權限，另一方面透過指定無線網卡方法，限制特定無線網卡才能接收，以防範有心人士之犯罪行為。

【案號：2102】

美國「黑色世界」盯上全球網路

【資料來源：新華網 2006/7/19】

事件描述

為打擊恐怖份子利用網路電話逃避犯罪追查，美國聯邦調查局在一項名為「黑色世界」專案中進行大規模的秘密監控行動。該計畫要求所有網路硬體製造商提供支援通訊監察的升級技術，且只要美國聯邦通信委員會（FCC）認為涉及公共利益時，則擴大至對商業網路服務的監聽。當人們透過即時通訊軟體，如 MSN 或 Google talk 和遠方朋友通話時，談話內容等資訊可能即透過網路傳到聯邦調查局手中。

法律意見

電信科技的日新月異是有目共睹，其中價格便宜的網路電話已成為世界潮流和民眾需求。特別在全世界各國積極投入推動與建設有線、無線的寬頻網路，挾著基礎設施完備及價格優勢，網路電話將更為普及。然而網路電話的安全監管問題，也開始困擾各國政府。

網路電話(Voice over Internet protocol,VOIP)依其是否使用電信號碼資源，分為 E.164(有核配門號)及非 E.164(未核配門號，亦即 PC to PC 之網路電話)二類。以目前技術，使用點對點技術之非 E.164 網路電話較不容易進行管理。但為確保先進的通信技術不會成為犯罪活動溫床，相關執法單位仍汲汲致力訂定一套有效的通訊監察規範。如前述案例，美國司法部即要求 FCC 應根據「法律執行通訊協助法」，強制網路服務業者提供服務時，必須確保該服務得被執法單位進行有效的通訊監察。我國政府亦然。

除政府犯罪防制議題外，企業在應用 VoIP 工具時也必須審慎思考此新技術對資訊安全管理帶來的衝擊。一般使用者通常認為只要插入 VoIP 裝置，即可享受到更彈性的電話使用環境與節費效益。然而 VoIP 技術直接應用在以傳輸資訊封包為主要功能而建置防禦的既有資訊系統時，卻可能造成安全隱憂，特別在流量管控與通話品質維護等議題上。企業如何制定好的安全防護策略，在防堵外部駭客入侵、內部機密外洩的同時，不讓防火牆、入侵偵測系統等所謂 Housekeeping 工具的應用阻斷語音封包的即時傳輸，影響 VoIP 話質；在提供高速傳輸環境，維護語音資料傳輸暢通的同時，不致給予駭客利用指令進行阻絕服務式攻擊的機會

等，這些都是 VoIP 進一步推廣應用必須思考的議題。

【案號：2103】

電子生物護照的安全疑慮

【資料來源：中時電子報 2007/1/1】

案例事實

在國際恐怖主義籠罩下，世界先進國家(如美國、英國、新加坡)紛紛全面換發電子生物護照，將民眾的生物特徵資訊寫入微晶片中。然而據了解，英國所使用的生物護照竟於兩週內被德國一家安全公司的電腦專家破解。

法律意見

所謂「電子生物護照」，即是在新護照中裝置一小片「無線射頻辨識系統」(RFID)晶片，晶片中儲存護照持有人的姓名、國籍、出生日期、出生地等資訊，以及個人生物特徵(如指紋、臉型及虹膜等)。美國、英國政府當局即表示，這些高科技護照的運用將有助於縮短到訪者入海關檢查時間，並可有效防範護照偽造，保

障邊境安全。

雖然如此，透過 RFID 技術在護照防偽功能上的好處是否大於護照持有者就其個人資料安全上的威脅，一直仍為各方爭議中。各國的人權團體無一不擔心 RFID 晶片為駭客所破解，個人資料因而被側錄，造成資料外洩，甚至供以犯罪之用。

個人資料的管理及保護預計是 RFID 在電子生物護照應用上最受爭議的議題。有感於國際應用電子生物護照趨勢，我國政府也於 2007 年提出護照條例修正草案，擬賦予政府發行晶片護照之法源依據。然而，政府對於蒐集民眾生物特徵後的個人資料如何保護議題，似仍未見明確之說明。相關爭議，就如同我國先前因政府換發身分證擬強制錄存指紋之爭議一般；該案並已經司法院作成釋字第 603 號解釋。

根據釋字第 603 號解釋意旨，憲法對資訊隱私權之保障並非絕對，國家得於符合憲法 23 條規定意旨之範圍內，以法律明確規定對之予以適當之限制。亦即，政府如果確定將發行電子晶片護照，應注意：應以法律明定其蒐集之目的；個人生物資料之蒐集應與重大公益目的之達成具有密切必要性與關聯性；應明文禁止

法定目的外之使用；而最重要者，主管機關應配合當代科技發展，對所蒐集之檔案採取組織上與程序上必要之防護措施。

我國「電腦處理個人資料保護法」對政府蒐集民眾個人資料的安全管理規範，僅見於個資法第 17 條，要求公務機關應指定專人依相關法律辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。另包括若公務機關違反本法規定，致當事人權益受損者，則應依個資法第 27 條負損害賠償責任。此種規範方式，實不足以回應釋字第 603 號所揭示的個人資料保護原則。政府後續在推動電子生物護照時，實應強化法源，在組織上與技術上建立更安全的防護機制並建立透明的稽核機制，納入公眾參與，才可能消弭電子生物護照帶來的個人資料管理疑慮。

二、個人資料保護

【案號：2201】

市長候選人病歷資料外洩事件

【資料來源：自由電子報 2006/08/25】

事件描述

94 年底縣市長選舉之際，中部地區爆發胡姓市長候選人遭對手陣營公布病歷事件。其後檢方認為公布病歷資料之涉案人並未直接參與診療被害人，該案以不起訴處分偵察終結。病歷來源之醫療機構的管理責任為本文探究之焦點。

法律意見

電腦應用已經成為民眾生活、工作的重要部分，事關民眾健康之醫療機構近年亦大力推動醫療資訊、病歷電子化的工作。依據衛生署 93 年訂定「醫療機構實施電子病歷作業要點」規定，所謂電子病歷是以電子文件方式製作、保存之病歷；該要點並規定醫療機構應設置經適當訓練之人員，以確保電子病歷之安全。

在上述案例中，胡姓被害人遭公布之病歷為 A 醫院所

有，依據「電腦處理個人資料保護法」(以下簡稱個資法)的規定，A 醫院即應做好保護措施，不讓病歷外洩。不過值得注意的是，目前個資法所規範之範圍僅限於經電腦處理之個人資料，若非經電腦處理之個人資料(如手寫紙本)則不在本法保護範圍中。

本案分析上第一步值得探究者，為被洩漏之資料是否為電腦列印之病歷複製本：若不是，則無現行個資法適用；若是，則 A 醫院對病患病歷外洩即應負個資法責任。其次，電子病歷既為個資法所保護的客體，醫療機構有防止資料被竊取、竄改、毀損、滅失或洩漏之義務。亦即，依據個資法第 28 條規定，A 醫院對於病歷外流乙事應負舉證責任，證明醫院本身無故意或過失，否則對於病患因此所受之損害應負民事上的損害賠償責任。

為強化對民眾資料隱私權之保障，個資法修正草案目前正在立法院審議中，未來將更名為「個人資料保護法」，將規範主體擴大到所有公務機關及非公務機關；同時擴大保護客體，不再以經過電腦處理的個人資料為限，即便是未經電腦處理的個人資料亦加以保護。保有個人資料檔案之機關(構)，未來只要因管理疏忽造成資料外洩，依法都需負擔法律責任，不可不慎。

【案號：2202】

信用卡資料外洩事件

【資料來源：自由電子報 2006/12/13】

事件描述

2006 年底國道警察偵破堪稱南部歷來規模最大的信用卡偽造、盜刷集團，逮捕「南部偽卡教父」主嫌黃 X 吉在內共 15 名嫌犯；該集團以派員應徵加油站短期工讀生之方式趁隙盜錄信用卡內碼，以製作偽卡進行盜刷。

法律意見

消費者使用信用卡消費已成為一種常見的付費方式，但隨著信用卡消費的普及，伴隨而來的是使用信用卡隱藏的風險--盜刷。回顧近年新聞事件，偽卡集團常透過詐騙民眾、購買銀行行員竊取之信用卡資料或對消費場所刷卡機進行側錄之方式，取得他人信用卡卡號、內碼等資料偽造信用卡。

本案中犯罪集團成員為了達成製作偽卡之目的，於加油站側錄消費者信用卡，以供偽卡集團使用之行為，已經明顯成立刑法第 204 條意圖供偽造、變造信用，而製造、交付或收受各項器械、原料、或電磁紀錄之構成要件，依法得處二年以下有期徒刑，並得併科五千元以下罰金。而製作偽卡以供使用者，則違反了刑法第 201-1 條偽造支付工具罪之幫助犯，最高得處以一年以上、七年以下的有期徒刑。此外，側錄他人信用卡資料之行為，同時違反了「電腦處理個人資料保護法」中對於「對於個人資料檔案為非法輸出、干擾、變更、刪除」之規定，依據個資法第 34 條規定，可處三年以下有期徒刑、拘役或科新臺幣五萬元以下罰金。

為避免個人信用卡遭側錄，建議平日應妥善保管皮夾及信用卡，並不隨意將信用卡交給他人，或離開自己視線，以降低卡片被側錄或商店重覆刷卡的風險。一旦信用卡遺失，或發現有不正常之情況時，應立即聯繫發卡銀行通知，或完成掛失手續，避免造成損失。同時，消費者於簽單時，應再三確認簽帳單之內容與張數，並於平日養成保留簽帳單和核對帳單的習慣，才能第一時間發現異常的交易項目，保護自身權益。

三、資訊作業委外

【案號：2301】

你有病，因為我上網查的到！

【資料來源：大紀元 2003/12/24】

事件描述

2003 年有民眾發現,只要在 Yahoo!奇摩網站的搜尋引擎鍵入參與中央健保局氣喘計畫的醫院或醫師姓名，即可連線進入健保局的病人案件管理系統，包括參與病患之姓名、出生年月日、身分證字號、電話、地址甚至配偶資料等都一覽無遺。更可由其他選項，查尋到醫師的個人資料及對病患的處置檢查報告等等，完全無須憑證或帳號，引起全國的關注與恐慌。

法律意見

在成本及效益的考量下，資訊委外的概念已成為主要潮流，各國政府與民間企業均愈來愈仰賴「委外」來達成降低營運成本、提升經營效率與效益。然而，若層出不窮發生的個人資料外洩事件所追溯的源頭，是具有公權力之行政機關所為之委外行為時，政府的形象、人民對政府的信心，恐怕會大受影響。政府資訊

服務委外的安全控管已成為各國不得不重視的課題。

所謂「政府業務委託民間辦理」之概念，係指國家或地方公共團體之事業或事務，不由國家或地方公共團體直接處理，而為達成行政任務之要求，由行政機關保留必要監督權限後，將之委託與民間企業、團體或私人代為處理。惟須注意者，機關(構)與受託處理事務之團體或個人間仍須負一定的連帶責任，機關(構)不可能因業務委外而免除監督責任。例如電腦處理個人資料保護法（以下簡稱個資法）第 5 條即明確說明，受公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人。

因此一旦發生資料外洩事件，如案例中參與計畫相關人士的個人資料因欠缺安全機制導致外洩時，資料主體當事人即可選擇依個資法第 27 條,或依參與計畫簽訂之契約關係，對機關(構)請求損害賠償；機關(構)在賠償當事人後，得再依委外契約，向廠商就其損失求償。另外，廠商如在處理資訊業務時，因故意或過失侵害當事人之人格權，當事人也可另依民法向廠商請求財產及非財產上的損害賠償。

為落實政府資訊委外作業時的安全管理，建議政府應

慎選有信用之資訊服務提供廠商，並妥善研議委外契約條款：應把「安全」列為契約主要標的；明確要求廠商應提供的資訊安全等級，且資訊安全的保障應包含資料機密性、完整性及可取用性之聲明；要求廠商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；要求服務提供商之資訊安全標準應不低於機關本身；要求廠商在委外合約中加列人員保密條款、簽訂保密切結書，必要時，要求政風人員參與協助委外廠商的安全查核工作等，以落實資安查核工作。

【案號：2302】

誰向詐騙集團洩漏我的個人資料？

【資料來源：台北地方法院 95 年度簡字第 620 號】

事件描述

法務部調查局接獲受害人投訴，渠等經常接獲行銷電話或信件，造成生活困擾，懷疑個人資料遭外洩並遭他人不當使用。經法務部調查後發現，受害人等資料外洩係肇因於 A 汽車股份有限公司離職員工甲。甲在 A 公司任職期間，擁有 A 公司受委託使用 B 公司相關車籍資料庫之帳號密碼，離職後未經 A、B 公司或當事人之同意，擅自使用該帳號密碼進入 B 公司資料庫，下載車籍資料並販售與他人牟利。

法律意見

隨著科技資訊化的快速發展，大多數的企業在降低成本、達到經濟規模考量下，都有服務委外的需求。根據 2006 年 6 月 Forrester Research 研究顯示，2011 年歐洲光是軟體委外市場將達 275 億歐元，平均年複合成長率將達 10%。特別在不斷推陳出新的資訊技術

領域，如銀行、證券、保險業、電信甚至醫療院所等，都普遍將資訊技術委託專業，以節省自行運作單位成本，進而提昇同業間競爭力。

然而，近年來不斷發生企業委外個人資料外洩，進而衍生後續被歹徒利用以進行詐騙、恐嚇等行為可知，企業委外仍應重視對客戶資料保護的承諾。

從法律層面分析，離職員工甲因已無合法權限使用 A 公司的伺服器主機與 B 公司之資料庫，其未經同意使用帳號密碼的行為，已違反刑法第 358 條入侵電腦罪，可處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。其下載車籍資料之行為，則另違反電腦處理個人資料保護法第 34 條規定，意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法輸出，致生損害於他人者，處三年以下有期徒刑、拘役或科新臺幣五萬元以下罰金。

企業委外成為最常造成客戶資料外洩的緣由，多是離職或在職員工有心竊取或無意洩漏，為保護企業客戶資料安全，建議企業在委外時，應特別注意在委外合約中須加列人員保密條款，並思考將保密義務延長到離職後一段期間，並加強人員控管及資料分級，從內

控和外控雙管齊下，期使委外風險降至最低。

四、系統與人員管理

【案號：2401】

某國防單位驚爆共諜案

【資料來源：ET today 2005/08/10】

事件描述

某國防單位莊姓少校涉嫌利用職務之便，將電訊密碼賣給男子黃 X 中，案經國防部高等軍事法院審理後，被告莊嫌無期徒刑並褫奪公權終身。

法律意見

某國防單位為我國重要情報機關，主要任務為對國際政經、大陸電訊與共軍電子情報偵蒐、研判，為國家戰略、技術及預警情報中重要的來源。日前傳出洩漏情資事件，顯示資訊安全維護工作除了完善的「電腦安全」維護外，「人員控管」亦是重要的一環。近年資訊安全的概念已經逐漸發展出資訊資產分級的概念，針對不同人員設定不同的使用者權限並記錄系統中資料存取的情況，期能對人員進行安全控管。

自法規層面觀之，過去施行多年的「妨害軍機治罪條

例」已於 93 年 1 月明令廢止，今日我國法規中對於秘密保護之法規，除了刑法之「國防秘密」、「國防以外之公務秘密」外，尚有國家機密保護法「國家機密」、及陸海空軍刑法之「軍事機密」且均列有罰則。上述案例中被告莊姓軍官因涉嫌利用職務上之機會竊取並洩漏軍事之電訊密碼等資訊，除了觸犯刑法「洩漏交付國防秘密罪」及國家機密保護法中「洩漏或交付經核定之國家機密罪」外，亦直接違反陸海空軍刑法中第 20 條「洩漏交付軍事機密罪」、第 21 條「洩漏交付職務上持有或知悉之機密罪」等重罪。

資訊安全維護工作是個人、民間單位與政府機關(構)必須共同面對的課題。在進行資訊安全維護工作時，除了提升電腦系統安全外，對於人員安全的控管亦需一併加以考量。而任何人若企圖竊取、洩漏、交付各式應秘密之資訊，終將面臨上述諸多法規帶來的牢獄之災。

【案號：2402】

離職員工竊取電子郵件

【資料來源：刑事局新聞快訊，2007/5/25】

事件描述

2007 年 3 月刑事局接獲報案，XX 科技公司之電腦遭不明人士入侵，竊取該公司重要商業機密等資料。經查為曾任職於該公司之陳姓員工，離職後自行成立與該公司性質雷同的電子商務公司，因商業競爭之故，竊用該公司現任員工帳號、密碼入侵公司資料庫，並取得該公司競標國外廠商訂單，獲利初估超過 500 萬元。

法律意見

基於資訊安全及網路管理之考量，多數公司會分配每名員工一組內部系統之帳號密碼及電子郵件供處理公司事務之用；員工離職後，除非有特殊情況，否則解釋上，該員工即沒有再使用該帳號密碼之權限，當事人若仍使用該帳號密碼進入公司系統，即可能有違法之虞。

本案中，陳姓員工不論是使用離職前公司配給自己的帳號及密碼，或是冒用他人名義，以同事的帳號密碼登入公司系統，其行為都可構成刑法第 358 條「無故輸入他人帳號密碼入侵電腦」之規定，可處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

其次，陳姓員工擅自入侵公司資料庫竊取商業機密等資料的行為，可能構成刑法第 359 條之無故取得電磁紀錄罪，依法得處五年以下有期徒刑、拘役或或科或併科二十萬元以下罰金，也可能構成刑法第 317 條的洩漏工商秘密罪。此外，公司也可根據營業秘密法請求民事上的損害賠償。

單靠法律的規範不足以嚇阻犯罪的發生。當電腦已成為多數公司賴以生存的基礎元素時，為避免公司電腦系統因人員流動而受到侵害，建議公司應制定一套安全機制，於員工離職後應立即取消其帳號、權限。從本案例觀之，該公司雖已取消陳姓員工的帳號，但陳姓員工仍得以社交工程手法取得其他員工的帳號密碼，此恐為員工資安風險意識不足之所致。如何強化人員權限控管，要求員工使用優質密碼設定(例如密碼設定應超過八個字元，且含有文數字及符號)，不輕易洩漏帳號密碼，並定期更新密碼等，均是公司網管必

要注意事項。最後，不論是檢視資料存取記錄，或是依據不同資料的機密程度設定資料回溯時間，甚至進一步追蹤員工帳號、密碼是否在合法時間內被使用，是否出現不正常資料存取等，都有利於資料外洩管控及強化系統資料安全，企業主管可酌情使用相關工具。

參、法條附錄

一、 案例引用相關法令彙編

案號	引用法令名稱及條款
1101	刑法第 358 條、第 359 條、第 310 條第 2 項
1102	刑法第 360 條
1103	刑法第 362 條
1104	行政院及所屬各機關資訊安全管理要點第 10 點
1105	刑法第 358～360 條、第 362 條
1201	刑法刑法第 201-1 條、第 210 條、刑法第 339-3 條、刑法第 358～359 條、著作權法第 91 條、商標法第 62 條
1202	刑法第 4 條、刑法第 268 條
1203	刑法第 235 條、第 315-1 條、兒童及少年性交易防治條例第 27 條、第 28 條、電腦網路內容分級處理辦法
1204	刑法第 310 條、民法第 195 條
1205	刑法第 339 條
1206	刑法第 339-3 條、刑法第 358～359 條、線上遊戲定型畫契約範本
1207	著作權法第 91 條、第 92 條

2101	刑法第 339-3 條、第 358 條
2102	無
2103	電腦處理個人資料保護法第 17 條、第 27 條
2201	電腦處理個人資料保護法第 28 條、醫療機構實施電子病例作業要點第 3 點、第 9 點
2202	刑法第 201-1 條、第 204 條、電腦處理個人資料保護法第 34 條
2301	電腦處理個人資料保護法第 5 條、第 27 條
2302	刑法第 358 條、電腦處理個人資料保護法第 34 條
2401	刑法第 109 條、國家機密保護法第 32 條、陸海空軍刑法第 20 條、第 21 條
2402	刑法第 317 條、第 358 條、第 359 條

二、 刑法（節錄）

條款	條文內容
第 201-1 條	意圖供行使之用，而偽造、變造信用卡、金融卡、儲值卡或其他相類作為簽帳、提款、轉帳或支付工具之電磁記錄物者，處一年以上七年以下有期徒刑，得併科三萬元以下罰金。 行使前項偽造、變造之信用卡、金融卡、儲值卡或其他相類作為簽帳、提款、轉帳或支付工具之電磁記錄物，或意圖供行使之用，而收受或交付於人者，處五年以下有期徒刑，得併科三萬元以下罰金。
第 204 條	意圖供偽造、變造有價證券、郵票、印花稅票、信用卡、金融卡、儲值卡或其他相類作為簽帳、提款、轉帳或支付工具之電磁紀錄物之用，而製造、交付或收受各項器械、原料、或電磁紀錄者，處二年以下有期徒刑，得併科五千元以下罰金。 從事業務之人利用職務上機會犯前項之罪者，加重其刑至二分之一。
第 210	偽造、變造私文書，足以生損害於公眾或

條款	條文內容
條	他人者，處五年以下有期徒刑。
第 220 條	在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以為表示其用意之證明者，關於本章及本章以外各罪，以文書論。 錄音、錄影或電磁記錄，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。
第 235 條	散布、播送或販賣猥褻文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處兩年以下有期徒刑、拘役或科或併科三萬元以下罰金。 意圖散布、播送、販賣而製造、持有前項文字、圖畫、聲音、影像及其附著物或其他物品者，亦同。 前兩項文字、圖畫、聲音或影響之附著物及物品，不問屬於犯人與否，沒收之。
第 268 條	意圖營利，供給賭博場所或聚眾賭博者，處三年以下有期徒刑，得併科三千元以下罰金。
第 310	意圖散布於眾，而指摘或傳述足以毀損他

條款	條文內容
條	人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或五百元以下罰金。 散布文字、圖畫犯前項之罪者，處兩年以下有期徒刑、拘役或一千元以下罰金。 對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。
第 315-1 條	有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金： 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。
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。
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

條款	條文內容
	，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。 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。
第 339-3 條	意圖為自己或第三人不法之所有，以不正方式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、變更記錄，而取得他人財產者，處七年以下有期徒刑。 以前項方法得財產上不法之利益獲使第三人得之者，亦同。
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、拘役或科或併科十萬元以下罰金。
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記錄，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。

條款	條文內容
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，至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。
第 361 條	對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
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、拘役或科或併科二十萬元以下罰金。

三、 電腦處理個人資料保護法（節錄）

條款	條文內容
第 1 條	為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。
第 2 條	個人資料之保護，依本法之規定。但其他法律另有規定者，依其規定。
第 3 條	本法用詞定義如左： 一、個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。 二、個人資料檔案：指基於特定目的儲存於電磁紀錄物或其他類似媒體之個人資料之集合。 三、電腦處理：指使用電腦或自動化機器為資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理。 四、蒐集：指為建立個人資料檔案而取得個人資料。

條款	條文內容
	五、利用：指公務機關或非公務機關將其保有之個人資料檔案為內部使用或提供當事人以外之第三人。 六、公務機關：指依法行使公權力之中央或地方機關。 七、非公務機關：指前款以外之左列事業、團體或個人： （一）徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。 （二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。 （三）其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。 八、當事人：指個人資料之本人。 九、特定目的：指由法務部會同中央目的事業主管機關指定者。
第 4 條	當事人就其個人資料依本法規定行使之左列權利，不得預先拋棄或以特約限制之： 一、查詢及請求閱覽。 二、請求製給複製本。

條款	條文內容
	三、請求補充或更正。 四、請求停止電腦處理及利用。 五、請求刪除。
第 5 條	受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人。
第二章　公務機關之資料處理	
第 7 條	公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之： 一、於法令規定職掌必要範圍內者。 二、經當事人書面同意者。 三、 對當事人權益無侵害之虞者。
第 8 條	公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用： 一、法令明文規定者。 二、有正當理由而僅供內部使用者。 三、為維護國家安全者。 四、為增進公共利益者。

條款	條文內容
	五、為免除當事人之生命、身體、自由或財產上之急迫危險者。 六、為防止他人權益之重大危害而有必要者。 七、為學術研究而有必要且無害於當事人之重大利益者。 八、有利於當事人權益者。 九、當事人書面同意者。
第 9 條	公務機關對個人資料之國際傳遞及利用，應依相關法令為之。
第 10 條	公務機關保有個人資料檔案者，應在政府公報或以其他適當方式公告左列事項；其有變更者，亦同： 一、個人資料檔案名稱。 二、保有機關名稱。 三、個人資料檔案利用機關名稱。 四、個人資料檔案保有之依據及特定目的。 五、個人資料之類別。 六、個人資料之範圍。 七、個人資料之蒐集方法。

條款	條文內容
	八、個人資料通常傳遞之處所及收受者。 九、國際傳遞個人資料之直接收受者。 一〇、受理查詢、更正或閱覽等申請之機關名稱及地址。 前項第五款之個人資料之類別，由法務部會同中央目的事業主管機關定之。
第 11 條	左列各款之個人資料檔案，得不適用前條規定： 一、關於國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益者。 二、關於司法院大法官審理案件、公務員懲戒委員會審議懲戒案件及法院調查、審理、裁判、執行或處理非訟事件業務事項者。 三、關於犯罪預防、刑事偵查、執行、矯正或保護處分或更生保護事務者。 四、關於行政罰及其強制執行事務者。 五、關於入出境管理、安全檢查或難民查證事務者。 六、關於稅捐稽徵事務者。

條款	條文內容
	七、關於公務機關之人事、勤務、薪給、衛生、福利或其相關事項者。 八、專供試驗性電腦處理者。 九、將於公報公告前刪除者。 一〇、為公務上之連繫，僅記錄當事人之姓名、住所、金錢與物品往來等必要事項者。 一一、公務機關之人員專為執行個人職務，於機關內部使用而單獨作成者。 一二、其他法律特別規定者。
第 12 條	公務機關應依當事人之請求，就其保有之個人資料檔案，答覆查詢、提供閱覽或製給複製本。但有左列情形之一者，不在此限： 一、依前條不予公告者。 二、有妨害公務執行之虞者。 三、有妨害第三人之重大利益之虞者。
第 13 條	公務機關應維護個人資料之正確，並應依職權或當事人之請求適時更正或補充之。 個人資料正確性有爭議者，公務機關應

條款	條文內容
	依職權或當事人之請求停止電腦處理及利用。但因執行職務所必需並註明其爭議或經當事人書面同意者，不在此限。 個人資料電腦處理之特定目的消失或期限屆滿時，公務機關應依職權或當事人之請求，刪除或停止電腦處理及利用該資料。但因執行職務所必需或經依本法規定變更目的或經當事人書面同意者，不在此限。
第.14 條	公務機關應備置簿冊，登載第十條第一項所列公告事項，並供查閱。
第 15 條	公務機關受理當事人依本法規定之請求，應於三十日內處理之。其未能於該期間內處理者，應將其原因以書面通知請求人。
第 16 條	查詢或請求閱覽個人資料或製給複製本者，公務機關得酌收費用。 前項費用數額由各機關定之。
第 17 條	公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防

條款	條文內容
	止個人資料被竊取、竄改、毀損、滅失或洩漏。
第三章 非公務機關之資料處理	
第 26 條	第十二條、第十三條、第十五條、第十六條第一項及第十七條之規定，於非公務機關準用之。 非公務機關準用第十六條第一項規定酌收費用之標準，由中央目的事業主管機關定之。
第四章 損害賠償及其他救濟	
第 27 條	公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。 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，並得請求為回復名譽之適當處分。 前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。

條款	條文內容
	基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。
第 28 條	非公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。 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五項之規定。
第 29 條	損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。
第 30 條	損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。
第五章 罰則	
第 33 條	意圖營利違反第七條、第八條、第十八

條款	條文內容
	條、第十九條第一項、第二項、第二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金。
第 34 條	意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法輸出、干擾、變更、刪除或以其他非法方法妨害個人資料檔案之正確，致生損害於他人者，處三年以下有期徒刑、拘役或科新臺幣五萬元以下罰金。
第 35 條	公務員假借職務上之權力、機會或方法，犯前二條之罪者，加重其刑至二分之一。
第 36 條	本章之罪，須告訴乃論。
第 37 條	犯本章之罪，其他法律有較重處罰規定者，從其規定。