機密維護常識彙編（１００年９月份）

＊某市政府烱站擺擺烏龍，民眾個資外洩

壹、案例事實：

某市政府法規會，也就是主管消費者保護的機關網站，把民眾申請國賠的資料，全部開放提供檢索，不但個人身分資料全都查得到，就連就醫紀錄都被貼在網站上。

當市民想申請國賠，而進入某市政府法規會網站時，在全文檢索中隨意輸入查詢字眼，就會出現一筆民眾的案例資料，不只是文字陳述，就連車禍照片與當事人就醫紀錄，全都一覽無疑，還有民眾的身分證就這樣顯示在網站上。某市市議員質疑，主管消費者保護的法規會，竟然成了洩密個人資料的兇手。法規會則表示是外包資訊廠商，忘記把資料加密，才導致民眾的個人資料全都露，已經請廠商趕工補救。

貳、法律探討：

一、最近常常發生個人資料外洩的新聞，除有購物頻道的消費者因業者外洩個人資料，而遭到詐騙集團鎖定行騙外，政府機關處理民眾的個人資料，也有疏忽的時候。除上面案例所提到的某市政府法規會，發生外洩民眾申請國賠的資料外，同時間也發生某縣政府網站，外洩原住民學生個人資料的情形，顯見目前對於個人資料的保護還不夠落實，所以連政府機關也有發生洩漏民眾個人資料的情形。

二、目前我國對於個人資料的保護，是以「電腦處理個人資料保護法」為規範。其中規範的對象即包括公務機關。以本案而言，某市政府法規會即是受「電腦處理個人資料保護法」規範之公務機關，而依「電腦處理個人資料保護法」第17條規定，應負有防止個人資料被竊取、竄改、毀損、滅失或洩漏之義務。由於某市政府法規會之管理不當而洩漏民眾個人資料者，應負起賠償民眾權益損失的責任，如果民眾名譽受損，依法更可請求回復名譽的適當處分（例如登報道歉）。

三、「電腦處理個人資料保護法」自民國84年公布施行以來，已經有十餘年，雖然對於個人資料的保護發生一定的功效。然而從這個案例看起來，公務機關對於民眾個人資料外洩的情形，特別是外包廠商的控管與責任分擔，都有強化的空間。所謂「徒法不足以自行」，也就是說，即使法律規範非常清楚，但是對於不遵守法律的行為，法律本身仍然有時而窮。因此對於個人資料的保護，仍然需要政府機關與企業及民眾等的支持。

四、另外，由於目前「電腦處理個人資料保護法」適用的範圍僅及於以「電腦處理」 的個人資料；而規範對象之非公務機關部分亦有限制，並非所有涉及個人資料處理的企業都有適用，故其保護的範圍比較狹窄。目前修法的研議，已經針對這幾個方向為放寬的規劃，相信修法通過以後，對於個人資料的保護將更為周到。

（資料來源：行政院國家資通安全會報技術服務中心）

貳、法律探討：

一、最近常常發生個人資料外洩的新聞，除有購物頻道的消費者因業者外洩個人資料，而遭到詐騙集團鎖定行騙外，政府機關處理民眾的個人資料，也有疏忽的時候。除上面案例所提到的某市政府法規會，發生外洩民眾申請國賠的資料外，同時間也發生某縣政府網站，外洩原住民學生個人資料的情形，顯見目前對於個人資料的保護還不夠落實，所以連政府機關也有發生洩漏民眾個人資料的情形。

二、目前我國對於個人資料的保護，是以「電腦處理個人資料保護法」為規範。其中規範的對象即包括公務機關。以本案而言，某市政府法規會即是受「電腦處理個人資料保護法」規範之公務機關，而依「電腦處理個人資料保護法」第17條規定，應負有防止個人資料被竊取、竄改、毀損、滅失或洩漏之義務。由於某市政府法規會之管理不當而洩漏民眾個人資料者，應負起賠償民眾權益損失的責任，如果民眾名譽受損，依法更可請求回復名譽的適當處分（例如登報道歉）。

三、「電腦處理個人資料保護法」自民國84年公布施行以來，已經有十餘年，雖然

對於個人資料的保護發生一定的功效。然而從這個案例看起來，公務機關對於民眾個人資料外洩的情形，特別是外包廠商的控管與責任分擔，都有強化的空間。所謂「徒法不足以自行」，也就是說，即使法律規範非常清楚，但是對於不遵守法律的行為，法律本身仍然有時而窮。因此對於個人資料的保護，仍然需要政府機關與企業及民眾等的支持。

四、另外，由於目前「電腦處理個人資料保護法」適用的範圍僅及於以「電腦處理」的個人資料；而規範對象之非公務機關部分亦有限制，並非所有涉及個人資料處理的企業都有適用，故其保護的範圍比較狹窄。目前修法的研議，已經針對這幾個方向為放寬的規劃，相信修法通過以後，對於個人資料的保護將更為周到。（轉載於臺灣宜蘭監獄政風室）

＊洩漏國防以外之秘密罪

壹、案情摘要：

甲○○為某縣政府某局處技士，負責協助河川巡防，並配合某縣政府各單位聯合稽查取締勤務，竟將該府 97 年 11 月營建廢棄土及土方洩聯合取締小組稽查日程表漏予業者知情，使業者事先避免行駛稽查路線，以致該府稽查行動無法克盡全功。案經臺灣○○地方法院檢察署檢察官依刑法第 132 條第 1 項洩漏國防以外秘密罪起訴，及該縣政府 99 年第 5 次考績委員會會議以一次記二大過免職在案。

貳、法律探討

一、刑法第 132 條第 1 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。（洩漏國防以外之秘密罪）

二、按公務員服務法第 4 條第 1 項規定:「公務員有絕對保守政府機關機密之義務，對於機密事件無論是否主管事務，均不得洩漏，……。」。又行政院 99 年 1 月 22 日修正發布生效前之文書處理手冊七十八、（一）規定:「各機關員工對於本機關任何文書，除經特許公開者外，應遵守『公務員服務法』第 4 條之規定，絕對保守機密，不得洩漏。」查某縣政府 97 年○○月○○日府環稽字第 0000000000 號函雖未列「密」等級，惟依上開規定，甲○○仍負有保守秘密，

不得洩漏之義務。況該函內容為事涉敏感之取締稽查行程，縱形式上未以密件辦理，實質上仍屬應保密之事項，甲○○為參與營建廢棄土及土方聯合取締小組稽查人員，更當知相關稽查行程事涉敏感應行保密。(資料來源：公務人員保障暨培訓委員會/保障案件決定書查詢系統)

＊勾結員警盜賣個個資，檢方起訴不法集團

壹、案例事實：

熊姓女子所組成的個資盜賣集團，涉嫌自民國 95 年起從縣市警察局等單位購賣個資，再販賣給徵信業者。台北地檢署偵查終結，將熊○○等 8 人依違反個資法等罪起訴。

檢方表示，熊女自 95 年起開始販賣個資，每筆消息收受新台幣 1,500 元至 2 萬 8,000 元不等的費用，每月收入達 10 萬元至 15 萬元。96 年 9 月間，熊女委託曾○○利用分局內的「內政部警政署戶役政查詢系統」，查詢 5 名民眾的個資後，販賣給徵信業者。熊女又在 97 年 4 月間與謝○○談妥調取個資價碼，謝○○隨後假藉辦案名義，向電信業者調閱 3 支行動電話的通聯紀錄。(資料來源：中央社 *98/12/9*)

貳、法律探討：

一、依電腦處理個人資料保護法第 8 條之規定，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。且須有法律所列情況，始能為目的外使用。警員基於辦案需求，可以透過「內政部警政署戶役政查詢系統」查詢民眾戶籍資料，應屬於增進公共利益，可作為特定目的外的利用。

二、本案例中警員洩漏個人資料及熊女不法蒐集並利用個人資料的情況，依照電腦處理個人資料保護法第 33 條之規定，可處 2 年以下有期徒刑、拘役或科或併科新台幣 4 萬元以下罰金。另警員因係利用職務上的方法，加重其刑至二分一。此外，民眾若因此受有損害時，也可以依照電腦處理個人資料保護法第 27 條規定，請求國家賠償。

(資料來源：行政院國家資通安全會報技術服務中心)

＊資安名詞的認識

一、防毒軟體/反病毒軟體：

指安裝於電腦內的一種程式，用於檢查入侵電腦的病毒、蠕蟲、木馬與惡意程式。當防毒軟體掃描到病毒時，會進行清除、隔離或刪除等動作，以防止病毒破壞系統。防毒軟體通常具有監控、識別、病毒掃描、郵件掃描和自動升級等功能，有的防毒軟體還帶有數據恢復等功能。

二、電腦病毒：

電腦病毒與醫學上所提的病毒大多具有不斷「自我複製」及「感染」的狀況，只是電腦病毒所感染的對象是電腦系統。通常它會寄存在可執行的檔案(*.COM，*.EXE)之中，或者是軟、硬碟的開機磁區啟動部份，隨著作業系統載入記憶體而同時執行這個病毒程式，因此獲得系統控制權。電腦病毒的創作者會針對電腦病毒程式進行修改，讓電腦病毒更具有破壞性，像目前來說，電腦病毒除感染執行的檔案(EXE)外，也演變為會感染 Office 軟體(例如:文件巨集病毒等)。

三、資料加密標準：

Data Encryption Standard 是一種被廣泛使用的資料加密方法。DES 起源於 1977 年美國 IBM 公司發展的區塊加密方法，且被美國國家標準局公布為資料加密標準。此外，DES 亦被制定於 ANSI X3.92、X3.106 標準、FIPS 46 等標準。目前約有 72 萬億，或者更多可能的加密金鑰可供使用。對於每一個給定的訊息，加密金鑰會從此巨大的金鑰庫中隨機挑選。傳送者與接收者必須知道相同的私密金鑰才能進行加解密。DES 利用 56-bit 的祕鑰於每一個 64-bit 的資料區塊進行加密。在 56-bit 的祕鑰輸入後，會額外產生 16 組子金鑰(subkey)。雖然這算是「強」的加密方法，然而以現有科技的計算能力，單一的 DES 有可能於 24 小時內被「破解」，因此有許多公司採用「三重 DES」，意指使用連續三個金鑰。過去的二十多年來，DES 一直在資訊安全扮演著重要的角色。它被廣泛的應用在商業、軍事、秘密通訊、身分認證等各方面上。DES 現在已經不被視為安全的加密演算法，因為它使用的 56-bit 秘鑰過短，以現代計算能力，24 小時內即可能被破解。也有一

些分析報告提出了該演算法的理論上的弱點。由於 DES 有安全上的疑慮，且加密算法並非牢不可破，美國標準技術局(NIST)已表示 DES 不會重新認證為標準，其更換意見書正在接受中。該標準最近已被高級加密標準(AES)所取代。

四、後門程式：

後門程式通常係指「不明的遠端人士未經系統管理員之允許，且利用不正當的手法」進入電腦系統中，並且可能偷走個人資料、機密資訊等，甚至可以隨心所欲地操控您的電腦，通常不明的遠端人士會透過電子郵件、IRC 或其他方式將後門程式植入使用者電腦中。目前 Windows 上常見的後門程式有 Netbus、Netspy、Netbuster、BirdSpy 等等。

五、網路犯罪：

網路犯罪為利用電腦或網路工具從事犯罪活動。網路犯罪可以藉由許多形式發生於任何時間、地點發生。例如：藉由下載非法的音樂檔案竊取銀行帳戶資料、散佈病毒或商業機密、竊取個人資料等。常見的網路犯罪手法為網路釣魚(phishing)和網址轉嫁(pharming)，這兩種手法都是誘騙使用者連到假網站，要求使用者輸入相關資料，以取得使用者個人資訊，如：使用者帳號、密碼、電話號碼、信用卡卡號等。

六、惡意軟體：

為軟體中含有惡意程或意圖之一般統稱。惡意程式包括：病毒(Virus)、蠕蟲(Worms)、木馬程式(Trojan Horse)、間碟軟體(Spyware)、廣告軟體(Adware)、疆屍網路(Botnet)等。惡意軟體會在未明確提示用戶或未經使用者許可的情況下，於使用者電腦或其他終端機上安裝執行，侵犯合法使用者權益的軟體。惡意軟體具有下列特徵行為：(1)採用多型技術手段，強行或秘密安裝，並抵制卸載。(2)強行修改使用者軟體設定，如：瀏覽器主頁(綁架網頁)設定變更。(3)強行彈出廣告，或其他佔用系統資源的行為。(4)有侵害使用者資訊和財產安全的潛在因素或隱憂。(5)與病毒聯合侵入用戶電腦。(6)停用防毒軟體或其他電腦管理程式做更進一步的破壞。(7)未經用戶許可、利用使用者疏忽或缺乏相關知識，秘密收集使用者

個人資訊、秘密和隱私。

七、間諜軟體：

Spyware 是間諜軟體的意思，也就是說未經使用者同意就私自放置於使用者電腦中的一支程式或是軟體，通常免費的軟體會暗藏 Spyware 程式，這意味當使用者電腦若啟動 Spyware 的話，將會讓不明人士可藉由 Spyware 將使用者電腦中上的資料「偷偷搬出門」，且利用網際網路將資料傳到遠方不明的伺服器中。這些資料有可能是使用者真實名字、IP、瀏覽過的網站與停留的時間、下載哪些檔案、上網的總時數、信用卡帳號及電腦硬碟的檔案資料等。

八、RSA：

Gnutella 網路屬於一種點對點(p2p)的分享網路，允許使用者於不同的網路進行檔案分享。然而，每一個使用者必須連結到一個類似 Server 的「ultrapper」，「ultrapper」包含已連線使用者的檔案分享清單，讓使用者能夠從數百台甚至數千台的連線電腦中搜尋檔案。Gnutella 是一種網路協定，而不是實際的程式。因此，從 Gnutella 網路中存取其他電腦，您的電腦必須安裝 p2p 軟體以支援 Gnutella。幸運的是許多 p2p 軟體都是可利用的共享軟體且可透過網際網路進行下載。

九、SubSeven：

SubSeven 是一套後門程式，會將自己安裝到系統上，不僅可讓駭客於受害電腦上做調整與設定，還能以多種方式進行感染 。SubSeven 也稱為 Backdoor-G 或 Sub7，由一名 Mobman 的駭客所撰寫的，SubSeven 通常會附在新聞群組的檔案當中，並且藏在電子郵件的檔案中散佈出去。它本身分為 Client 與 Server 兩個部分，因為變種繁多，有許多的使用方法，有的可以附在別的程式上，有的可以單獨存在。Server 部分會以 email 或連結方式讓別人下載使其中毒，Server 開始執行後，會與駭客所設定的 IP (當然是駭客自己的電腦）Client 開始聯繫，駭客可藉此做鍵盤記錄，以偷取密碼、觀看使用者的電腦、操控被害者的電腦硬體及進行一些破壞性的動作。

十、反網路釣魚工作小組：

APWG 為來自全世界各地超過 1600 家公司組成的國際組織。目的是打擊利用網路釣魚進行詐欺與竊取個資等行為。該組織提供網路釣魚相關訊息、安全產品與法律方面的協助。網址:http://www.antiphishing.org/。

十一、網路釣魚：

網路釣魚(Phishing)是網路上在常見的社交工程，特別是利用 email 來欺騙，Phishing 並不是一個新的攻擊手法，然而發生的頻率卻在過去幾年中逐漸增加。通常網路釣魚(Phishing)的方式是讓使用者收到一封標題是某帳戶資訊更新的郵件，其信件內容裡有提供一個仿冒 P 某網頁的連結並要求使用者由此連結登入這個仿冒網頁去輸入帳號及密碼來更新使用者資訊，這個仿冒網頁便會記錄使用者帳號密碼，接著再將網頁導向真實的 Paypal 網頁，令使用者在不知不覺中就被盜取了密碼。

十二、複合型病毒：

複合型病毒是一種具有開機型病毒以及檔案型病毒的特性。它們除了會傳染 *.COM，*.EXE 檔，也可以傳染磁碟的開機系統區（BootSector）。由於他可以同時感染兩種程式檔案的特性，使得這種病毒具有相當程度的傳染力，一旦被感染且發作後，其破壞的程度將會非常可怕。

十三、巨集病毒：

巨集病毒是最常感染的是 Word、Excel 等有提供巨集功\能的軟體，它主要是利用軟體本身所提供的巨集能力來設計病毒。而巨集病毒是常見的是以 Visual Basic 程式語言撰寫而成，所以相當容易製作。於使用檔案期間，巨集病毒可在不同時間，例如，當開啟、儲存、關閉或刪除檔案時散播病毒。

十四、千面人病毒：

千面人病毒主要是在於當它們每繁殖一次，就會產生一組新的病毒程式以便傳染到系統別的地方去，這樣的繁殖方式會讓掃毒軟體無法防到已變種後的病毒，雖然它們的的特性都很類似，實際上可能感染檔案不同，是被認定為二種

以上的病毒。

十五、特洛伊木馬程式：

特洛伊木馬程式與特洛伊木馬病毒不同點在於特洛伊木馬程式不會像電腦病毒一樣會感染其他檔案。此指特洛伊木馬程式是不明人士利用電子郵件或是經由些特殊管道進入使用者的電腦系統中，將「特洛伊木馬程式」植入電腦系統中，然後伺機執行惡意行為（例如格式化磁碟、竊取檔案或密碼等），會被植入特洛伊木馬程式的原因，也有可能來自使用者自己下載位受信任網站下的程式、檔案或軟體，而特洛伊程式則寄存在這些未被信任的程式內，當這類程式被執行時，特洛伊程式也跟著被執行，進而進行破壞。

十六、特洛伊木馬病毒：

所謂特洛伊木馬病毒係指使用者開啟電子郵件之不明附件檔案等行為後，使得病毒被啟動並感染電腦系統中相關程式及軟體(例如:EXE、COM 等執行檔)，當使用者再次執行已被感染的執行檔後，則造成特洛伊木馬程式被啟動，可能會自動連線至遠端不明之電腦，自動傳回系統相關資料(例如:管理員密碼、個人資料等)，電腦駭客也可能此一管道進入電腦系統進行破壞。

十七、蠕蟲病毒：

蠕蟲病毒(Worm Virus)本身就是一種電腦病毒的變種，它可以在感染電腦後或是在電腦之間複製它本身，並且透過電腦可傳輸檔案或資訊的功\能自動進行複製，蠕蟲病毒會利用一些媒介大量的自我複製。例如，蠕蟲病毒可利用使用者郵件通訊錄將病毒傳給在通訊錄的每個人，若收到郵件的人未經查證就執行將會造成感染，並且又利用相同手法傳遞病毒，從而發生大量網路流量的連鎖效應，降低整個企業網路和網際網路的速度。

（資料來源：行政院國家資通安全會報技術服務中心）