電腦網路隱私權之探討

施學琦　徐濟世　趙福源

國立雲林技術學院資訊管理技術系
台灣省雲林縣斗六市大學路三段123號
e-mail: shihhc@mis.yuntech.edu.tw

摘要

隱私權所代表的，乃是對個人的一種尊重。在民主法治的國家裡，尊重隱私權，乃是每位國民所應具備的基本素養。台灣學術網路乃一教育性網路，其目的，應不僅限於資訊的傳輸，亦包含對於使用者的適當教育，使其養成良好的習慣，並建立其正確的觀念。在教育性的網路裡，倘若缺乏明確的隱私權政策，很容易誤導使用者，以爲隱私權無關緊要，當此種態度被帶入商業性網路時，甚至可能影響對商業機密之保護，而此種負面印象一旦形成，將影響國際對我國之投資意願。時值我國政治更民主，社會更開放，經濟更自由，並積極成立亞太營運中心之際，隱私權的問題，值得重視。本論文即以台灣學術網路爲背景，探討一些可能發生的侵害隱私權的行爲，並舉出一些使用者爲保護自己的隱私權而可能採取的自力救濟措施，及這些自力救濟措施所可能帶來的影響；藉著這些探討，本論文希望能提昇學術網路對隱私權的重視，並促使明確的隱私權政策的制定。

1. 前言

隱私權的目的，並非在保護罪犯，使其免受法律的制裁；其所代表的，乃是對個人的一種尊重。隱私權的需要，人人皆有，譬如，當居家時，對於房門與窗簾的使用，又譬如，當寄信時，對於信封的使用，均是行使隱私權的一些例子。隱私權的行使，並不代表行使隱私權的個人，有難以告人的祕密，或正在進行不法的行爲。在民主法治的國家裡，尊重隱私權，乃是每位國民所應具備的基本素養。

由於台灣學術網路的建立，網路的使用，在學校與研究機構間日趨普及。目前台灣學術網路連接的範圍已包括大學院校、研究單位、將近半數的專科學校、及少部份的高中職、國中小，教育部並計畫以台灣學術網路爲基礎，逐步擴充爲「教育與研究網路」[2]。隨著台灣學術網路的擴充，使用者亦不斷增加，如何使眾多的使用者，在彼此尊重的前提下，共同發揮網路的最大效益，實爲重要課題。

現行的台灣學術網路使用規範，雖有部份條文與隱私權有關，惟略顯含糊。以下列舉二個屬於假設性質，但依據現行的使用規範卻無法明確回答的例子：（1）學校的學生事務處是否可以拆閱學生的電子郵件？如果可以，在何種情況下才算可以？（2）學校的老師是否可以在學生不知情的情況下，觀察學生在網路上的行爲，作爲研究資料的來源？

對於一個負有教育任務的學術網路而言，網路的使用，應不僅限於資訊的傳輸，亦包含對於使用者的適當教育，使其養成良好的習慣，並建立其正確的觀念。在這樣的網路環境裡，倘若缺乏明確的隱私權政策，很容易誤導使用者，以爲隱私權無關緊要，當侵犯他人的隱私權時，亦誤以爲無傷大雅。或許，在學術網路裡，隱私權的確無關緊要，侵犯隱私權也的確無傷大雅；但是，當一個不曾建立正確隱私權觀念的網路使用者，離開學習的環境，進入商業性網路時，是否能夠適時的建立正確的隱私權觀念？當一個國家的商業性網路，其使用者泰半皆缺乏隱私權觀念時，其網路秩序是否會受到影響？當一個國家的商業性網路，空有優良的硬體建設，卻缺乏良好的網路秩序時，是否仍能吸引來自國際的使用者？這些問題，值得深思。

本論文即在探討台灣學術網路中，一些與隱私權有關的問題，其結構如下：第2節是對隱私權作進一步的探討；第3節是簡述台灣學術網路的目的及其所提供的服務；第4節是列舉台灣學術網路中，一些可能發生的侵害隱私權的行爲；第5節是舉出一些使用者爲保護自己的隱私權而可能採取的自力救濟措施；第6節是討論這些自力救濟措施所可能帶來的影響；第7節是結論。

2. 隱私權

處身於一個分工細密、環環相扣的現代社會，個人很難離群而索居。基於彼此共同生活的需要，每個人不可避免的，都會或多或少的向他人揭露一些有關自身的資訊。當由隱私權的角度，來探討有關個人資訊揭

露的問題時，眞正值得注意的，並不是被揭露的資訊其數量的多寡，而是以下幾點：（1）在揭露這些有關個人的資訊時，是否有徵詢當事人的意願？是否在當事人不知情的狀態下所爲？（2）當資訊被揭露出來後，是否會在違反當事人意願，或其不知情的狀態下，做二手甚至多手的傳播？（3）在傳播的過程中，是否有扭曲原始資訊的情形發生？

以上提出的幾點，其答案的是與否，並不足以判斷行爲的善與惡，是與非。某些行爲，在多數的情況下，不能得到多數人的認同，但在特定的情況下，卻能爲大眾所接受，譬如，擅拆他人信件，通常會被認爲是不道德的行爲，但是，相同的行爲，當行爲人由一般人轉變爲執法人員，當其目的，由滿足個人的好奇心，轉變爲維護社會治安，當其方式，由擅自行動，轉變爲經過合法授權時，其評價，也就有了截然不同的轉變。因此，提出以上幾點的目的，僅在藉此探討，與個人有關的資訊，是否有可能藉著電腦網路，透過以上幾點，逐漸脫離當事人的掌握，而無遠弗屆的傳播？又若果眞如此，則當事人是否有可能運用自己的力量，來加強對隱私權的保護？而這種自力救濟的行爲，又會帶來何種衝擊？藉著這些探討，希望能提昇對學術網路中隱私權的重視，並進而促使明確的隱私權政策的制定。

3. 台灣學術網路

台灣學術網路是一個全國性的電腦網路，是在民國七十九年，由教育部電子計算機中心及各主要國立大學所共同建立，其目的有四[1]：（1）支援台灣地區學校間之教學研究活動，（2）支援研究機構間之教學研究活動，（3）相互分享資源，（4）相互提供合作機會。爲達成這些目的，台灣學術網路提供許多項服務，一些常用的服務包括：

（1）電子郵件（e-mail）：透過這項服務，寄件者能夠將所欲傳遞的訊息，經由網路，傳送給一位或多位的收受者。每封電子郵件中，均包含寄件者的電子郵件地址，以表明其身份；亦包含收受者的電子郵件地址，以便訊息能夠一站接一站地傳送給收受者。電子郵件在送抵收受者的節點後，先存放於系統的電子郵箱（electronic mailbox），等待收受者讀取。收受者閱畢後，可視需要，或將電子郵件保存於其個人的電子郵箱中，或另行存檔，或轉寄他人。

（2）遠程簽入（telnet）：透過這項服務，使用者可以由目前所在的節點，經由網路，簽入另一個節點，並使用其服務。

（3）遠程檔案傳輸（FTP）：透過這項服務，使用者可以在本地的系統，與遠方的系統間，進行檔案的傳輸。

（4）全球資訊網（World Wide Web）：透過這項服務，使用者可以藉瀏覽程式（browser）之助，以超文件（hypertext）的方式，瀏覽全世界公開的文字、影像、聲音與動畫。

（5）小田鼠查詢（Gopher）：較全球資訊網稍早出現的另一個強大的整合性資訊系統。

4. 網路上可能發生的侵害隱私權行爲

本節擇要列舉台灣學術網路中，一些可能發生的侵害隱私權的行爲。此類行爲可再區分爲三子類：第一子類是直接的侵害，指的是在當事人不知情，或違反其意願的情況下，揭露有關其個人的資訊的行爲；第二子類是多手的傳播，指的是在當事人不知情，或違反其意願的情況下，做二手甚至多手的傳播；第三子類是資訊的扭曲，指的是在當事人不知情，或違反其意願的情況下，扭曲原始的資訊。

4.1 直接的侵害

此類行爲可再細分爲非惡意的，與惡意的。

4.1.1 非惡意的直接的侵害

本分節探討非惡意的，對隱私權的直接侵害。

首先探討遠程簽入服務。這種服務能夠讓使用者由一個節點，遠程簽入另一個節點。當使用者合法的簽入某遠程節點後，便能運用一些合法的工具，得知許多有關其他使用者的資訊。譬如，在Unix系統上，能夠輕易的知道，目前有那些使用者由何處正簽入本節點，這些使用者目前正在執行那些程序（process）；也能知道，某位使用者在何時，由何處最後一次簽入本節點，及這位使用者是在何時，最後一次閱讀電子郵件，是否有任何尚未閱讀的電子郵件；甚至能知道，所有使用者過去是在何時，由何處簽入本節點的所有資料。

再者，如果在被簽入的節點中，有部份使用者對自己的檔案未加以適當的防護，則遠程簽入者可以進入這些使用者的檔案，加以觀察或修改，這種現象，就好比某人敞開自家的大門，令人得以入內參觀或翻弄一般。

接著探討電子郵件。如同一般的信

件，電子郵件也有可能被非收件人的其他人所拆閱。本分節談的是合法的情況，不合法的情況留待下分節再談。網路上的每一個節點，都會有一位或數位的管理者，這些管理者具有極高的權限，幾乎能夠閱讀節點中的所有檔案（除非檔案已被加密，看了等於沒看），因此，這些管理者也能夠不留絲毫痕跡的拆閱使用者的所有電子郵件。由於節點的設備與網路的設備通常並非使用者所自有，而是由學校或研究單位所提供，因此，純以法律的觀點而言，節點的管理者極有可能確實具有拆閱使用者電子郵件的權力。本論文所重視的，並非法律上的權力，而是使用者是否事先有被告知。如果，使用者在事先已經知道其電子郵件有可能會被拆閱，卻仍然願意使用這項服務，那是使用者自願以一些隱私權來換取其通信上的便利，旁人自然不需妄加干涉；但是，如果管理者未善盡告知之責，即逕行拆閱，即使管理者具有法律上的權力，在道德上，卻也並非全無可議之處。

另外，由於電子郵件包含寄件人的姓名與網路地址，在某些特殊的情況下，也可能會造成隱私權的侵害。譬如，某單位的員工掌握了上級長官瀆職的明確證據，並利用電子郵件加以揭發，但是不幸這封電子郵件被攔截，並且由於眞實身份暴露，而遭到嚴厲的報復。又譬如，某單位的員工利用Usenet News發表與其服務單位立場相左，但代表其眞實心聲的聲明，由於電子郵件顯示其眞實身份，而影響其日後的升遷。諸如此類的例子，均可視爲對隱私權的侵害。

接下來探討網路上的記錄。使用者透過網路所進行的所有活動，都有可能會被記錄下來。這些活動包括了電子郵件、遠程簽入、遠程檔案傳輸、全球資訊網、小田鼠查詢等，一切活動都有可能被記錄下來。有時記錄中所記載的只是對方節點的名稱，有時記錄中所記載的同時包括對方節點與其使用者。通常，這些記錄是被用來做一些統計性的分析，藉以幫助管理者對資源作更有效的運用。這裡，本論文所重視的，亦是使用者是否事先知情。有些伺服器在記錄前會先徵詢使用者的意願，譬如一些遠程檔案傳輸的伺服器，若使用者不願意留下記錄，可以立刻離開；但有些伺服器，並不會事先徵詢使用者的意願，因此，許多時候，使用者是在不知情的狀況下留下了記錄。

再下來探討網路的安全性管制。維護網路的安全性，以保護絕大多數守法的使用者，是一項非常重要的課題，這點在下一個次節將會提到。絕大部份的時間，安全性與隱私權是攜手並進的，意即安全性的加強對隱私權的保護有正面的作用，但是，某些安全性的措施，亦有可能對隱私權造成侵害。一個明顯的例子，是監視的功能。監視有二種作用：（1）觀察網路上的活動，找出可疑的跡象，以判斷是否有壞份子嘗試侵入；（2）當有壞份子已經侵入時，監視被用來觀察侵入者的手法，藉以找出其入侵的路徑，以及其已經造成的損害。監視是一種非常有力的工具，許多時候，監視是瞭解侵入者的重要方法，譬如，Venema[9]曾經記載如何以監視來觀察某侵入者，而Cheswick[5]也記載同一名侵入者如何被引誘進入貝爾實驗室的系統，並在嚴密保護措施下被仔細觀察的經過。但是，問題是，如何在安全性與隱私權間取得一個平衡，如何防止安全性措施的濫用，這是必需審愼考量的。

4.1.2 惡意的直接的侵害

本分節接著探討惡意的，對隱私權的直接侵害。

如同社會並非完美無缺，在網路上，也有一些壞份子，專門惡意的侵入他人的系統，造成巨大的損害，一個著名的例子，是1988年的Internet Worm。不可否認的，網路上的許多服務，爲這些壞份子，提供了可資利用的途徑。Farmer與Venema[10]曾舉例說明許多看似無害的網路服務，在這些壞份子手中，卻成了極具價值的犯罪工具。在其文章裡，有許多的實例，可以供系統管理者來查核系統的安全性；然而，這些實例也提供了壞份子入侵系統的指南，其結果如何，端視何人先執行這些實例而定。並且，Farmer與Venema合作發展了一套名爲SATAN的程式，能夠有系統的找出系統安全性上的弱點，對於系統管理者而言，極具價值；但是，由於SATAN可以透過匿名遠程檔案傳輸服務而取得，壞份子也可以使用SATAN找出系統的安全性弱點，作爲入侵系統的參考。在Internet上，具有與SATAN類似意味，並且能透過匿名遠程檔案傳輸服務而取得的程式還有許多，如COPS、Crack等。由於此類程式被置於公開領域，且其儲存位置很容易透過檢索工具而得知，因此，系統安全性的確實強化，便成爲當務之急。

在終端使用者意識高漲的今日，許多系所，或其下的單位，已經架設了自己的子網路，連上了校園網路，連上了台灣學術網路，也連上了Internet。這是一個可喜的現象，說明台灣的使用者，已充份明瞭網路的必要性與便利性，對於將來學術研究的發展，有非常正面的影響。但是，不可否認的，如果學校在連接台灣學術網路時，沒有訂定適當的安全性政策，如果校園網路內的

各子網路漫無節制的提供所有的網路服務，如果各節點的管理者對已知的系統弱點與入侵手法毫無所悉，那麼，至少有二點值得憂心：

（1）當一個壞份子侵入某節點後，可以利用許多方法，取得節點管理者的權限，當其成功後，節點中一切的檔案（包括電子郵件），都任其處置，從而造成該節點隱私權的嚴重侵害。

（2）只要壞份子侵入某個節點，無論是否取得節點管理者的權限，都可以用一種稱爲吸納（sniffing）的方法，擴大侵入的範圍。由於網路共用的特性，使得節點在實際上能夠收聽到其子網路中所傳送的所有訊息。吸納程式（sniffer），便是利用這種特性，使其能夠在網路上監聽或攔截訊息。吸納程式的取得，並不困難，實際上，有許多的吸納程式，能夠直接透過匿名遠程檔案傳輸服務而取得[11]。這是由於吸納程式對於網路的管理，特別是網路的偵錯，有很大的助益；但是，如果吸納程式是由壞份子在被侵入的節點所執行，當其尚未取得節點管理者的權限時，能夠攔截由被侵入的節點所發出的所有訊息，當其已經取得節點管理者的權限後，更能夠攔截整個子網路上的所有訊息。在被攔截的訊息中，可能包括使用者在使用遠程簽入時，透過網路所傳輸的簽入密碼（password），以及其他如電子郵件之類的私密性資料。因此，當壞份子侵入節點並執行吸納程式時，一般使用者的隱私權已經受到嚴重的侵害，而藉著不當取得的簽入密碼，壞份子所侵入的範圍益形擴大，更可能會造成隱私權的進一步被侵害。

以上的探討指出，對隱私權惡意的、直接的侵害，是由壞份子的入侵而來。而壞份子的入侵，則是藉安全性的疏失而爲。故欲避免對隱私權惡意的、直接的侵害，唯有加強整個網路中所有節點的安全性。

4.2 多手的傳播

一些涉及隱私權的資訊，可能會在違反當事人意願，或其不知情的狀態下，做二手甚至多手的傳播。一個明顯的例子，是電子郵件轉寄（forward）功能的濫用。當收件人收到電子郵件後，可以毫不費力的將該電子郵件轉寄給其他人，而其他人又可以毫不費力的將該電子郵件再轉寄給更多的其他人。問題是，該電子郵件的原始寄件人是否知情，又是否同意。此類行爲，應予以適當的規範。

另一個明顯的例子，與網路上的記錄有關。第一個值得關心的問題，是節點所保存的記錄，是僅限節點的直接管理單位使用，譬如某個系，或僅限節點管理單位的上一層組織使用，譬如某個學院，或是會被轉給外界的第三者使用，譬如情治單位。第二個值得關心的問題，是記錄的保管方式是否研嚴密，是毫無保護，任何人皆可存取，或是略具保護，唯有特定人方可存取，或是嚴格保護，不但唯有特定人方可存取，並且有加密。第三個值得關心的問題，是一般使用者是否知道第一個與第二個問題的答案。

實際上，目前所探討的題目，與資料監視（dataveillance）[6]有密切的關係。所謂資料監視，指的是有系統的運用個人資料系統，對一位或多位人員的行動或通訊，進行調查或監督。大多數人可能都不願意自己的一舉一動，受到一個無所不在的特定單位的監視。Clarke[6]曾爲這樣一個無所不在的特定單位，提出三個要件：（1）必需有許多的個人資料系統，每一個系統均依據特定目的而搜集資料；（2）這些個人資料系統必需透過網路連結在一起；（3）資料必需能相當一致的加以辨識。如果以這三個要件，來看目前所探討的網路記錄的問題，可以發現，第一個與第二個要件均已滿足，而第三個要件藉著分散式異質性資料庫技術[3]的發展，也可以得到滿足。因此，資料監視使用者在網路上的一舉一動，就技術面而言，已不再困難，所剩下的屏障，是（1）這些分散各處的網路記錄，是否願意對外開放，與（2）執行資料監視的成本效益比，是否值得。

假設所有的屏障均已去除，資料監視已經開始執行，對隱私權究竟會造成何種影響？首先，有關個人的記錄可以加以整合，監視者可以清楚的知道，某特定個人在何時由何處進入某節點做了某事，個人的一舉一動，都有完整記錄；其次，當某特定個人在網路要求某項服務時，監視者可以依據該員過去的行動記錄，來決定是否提供該項服務；再者，當某特定個人試圖在網路上進行超越權限的行動，譬如試圖進入一個無權進入的子目錄，無論是有意或無意，都可能觸發對其進行進一步的調查；最後，監視者可以依據過去的經驗，定出某特定類別使用者的特徵，再依據這些特徵，過濾出一些符合特徵的使用者，而採取進一步的行動。

Schwartz與Wood[8]所進行的一項研究，爲上述最後一類的作法，提供了一個例證。他們在全球的十五個節點對電子郵件的寄件人與收件人加以記錄，然後以啓示圖形演算法對寄件人與收件人所形成的圖形進行分析，在不涉及信件內容，只分析通訊模式的情況下，其方法能夠相當準確的找出具有相關興趣的電子郵件使用者。Schwartz與Wood的方法有一點很值得注意，那就是即使

電子郵件已經經過加密的處理，其方法仍然能夠對電子郵件的使用者進行分類。

本論文認爲，科技本身並沒有善與惡的區別，問題是在人們如何使用科技。資料監視可以被用來遏止壞份子在網路上的活動（在某種程度上），使網路成爲一個更安全的地方；也可以使人在毫無防備的情況下，蒙上不白之冤。資料監視可以找出對某領域有特殊興趣的專家學者，促成彼此交流，以加速研究的進展；資料監視也可以亂按帽子，在當事人不知情的狀況下，將其列入黑名單。在科技突飛猛進的今日，重要的問題是，如何明智的使用科技。

4.3 資訊的扭曲

一些涉及隱私權的資訊，可能會在傳播的過程中，被有意無意的扭曲。一個明顯的例子，是電子郵件轉寄功能的扭曲。當收件人收到電子郵件後，可以將該電子郵件竄改後再轉寄給其他人，而其他人又可以將該電子郵件再竄改後再轉寄給更多的其他人。這種行爲不但侵害隱私權，還有故意傳播不實訊息之嫌。

另一個明顯的例子，與網路上的記錄有關。第一個值得注意的問題，是記錄的竄改。譬如，某使用者可能從來沒有進入過某個節點，卻被記錄成曾經進入，可能從來沒有存取過某個檔案，卻被記錄成曾經存取。記錄的竄改，不一定是節點的管理者所爲，亦有可能是別有用心的第三者。第二個值得注意的問題，是殘缺記錄的傳播。記錄的殘缺可能會造成判斷的偏頗，譬如，在許多節點拒絕揭示其網路記錄，而僅有部份節點願意揭示的情況下，彙總而成的記錄的價值，必需加以謹慎的評估。

5. 一些自力救濟的方法

本節所介紹的自力救濟方法，均與電子郵件有關。

隨著電子郵件的普及，一些與電子郵件相關的問題也逐漸受到重視。第一個問題與電子郵件的特性有關，第參節曾提到，電子郵件是一站接一站地傳送給收受者，第肆節第一子節的第乙分節亦曾提到，吸納程式能夠在網路上攔截包括電子郵件在內的訊息。如果電子郵件不幸遭人攔截，可能發生的情況有許多，以下僅列出二種：（1）攔截者的目的在獲悉電子郵件的內容，故在檢視電子郵件後，不加任何更動即再傳送給收受者；（2）攔截者的目的在變更電子郵件的內容，當其成功的更動電子郵件後，即再傳送給收受者。

針對以上的疑慮，Zimmerman發展了一套名爲PGP的程式[7]，PGP混合了傳統加密法與公開金匙加密法來化解第一個疑慮，其方法如下：（1）在發信時，PGP會（a）壓縮信件，（b）隨機產生一個金匙（key），（c）用步驟b所得的金匙以IDEA（International Data Encryption Algorithm）法將明文加密，（d）將步驟b所得的金匙，用收件人的公開金匙（public key），以RSA法加密，並附加於步驟c所得的密文前，（e）將步驟d所得的密文傳送給收件人；（2）在收信時，PGP會（a）以收件人的秘密金匙（private key）解開金匙，（b）用步驟b所得的金匙解開密文，（c）解壓縮。

PGP化解第二個疑慮的方法如下：（1）在發信時，PGP會（a）以單向赫序函數對訊息產生一個128位元長的訊息摘要（message digest），（b）以寄件人的秘密金匙將訊息摘要加密，（c）將步驟b所得的數值簽章（digital signiture）連同訊息一併傳送給收件人；（2）在收信時，PGP會（a）以寄件人的公開金匙解開數值簽章得到訊息摘要，（b）再對所收到的訊息算一次訊息摘要，（c）比對步驟a與步驟b的訊息摘要。

由於PGP最初是在美國發展，且美國政府禁止未經許可的密碼軟體出口，因此在台灣將無法合法的使用美國版的PGP，但是有一些合法的國際版PGP，可以透過匿名遠程檔案傳輸服務而取得。

第二個與電子郵件相關的問題，是曾在第4.1.1節所提及的，有關電子郵件的署名問題。電子郵件上的署名究竟會不會爲其寄件人帶來某種程度的迫害，是一個見仁見智的問題，而電子郵件究竟應不應該署名，也是一個議論紛紜的問題。對匿名權的支持者而言，匿名權與民主制度的運作息息相關，爲確保人們匿名使用電子郵件的權利，因而有匿名再郵寄者（anonymous remailer）的出現。匿名再郵寄者所做的，是在收到電子郵件後，除去寄件人的眞實姓名與網路地址，換上假名與假地址後，再傳送給收件人。電子郵件的使用者可以運用一連串的匿名再郵寄者來確保絕對的匿名，意即先將其電子郵件寄給第一個匿名再郵寄者，第一個匿名再郵寄者將其轉給第二個匿名再郵寄者，第二個匿名再郵寄者將其轉給第三個匿名再郵寄者，一個接一個，直到最後一個匿名再郵寄者將其轉給收件人。

6. 自力救濟的影響

PGP之類的程式的目的，是在保障通

信雙方的隱私權，其立意非常良好，其手段也非常有效。但正因爲這類程式太過有有效，反而帶來一絲潛在的困擾。試想，當第三者（特別是執法人員）必需知道信件內容，以保障多數人的利益，卻無法破解密文時，會不會反而造成社會的困擾？有鑑於此，美國政府在1993年提出了引起爭議的金匙寄管（key-escrow）加密法[4]，其構想是採用一個未經公開的Skipjack演算法來執行加密，由於Skipjack所產生的密文應該很難破解，因此得以保障訊息的內容不致洩漏，但是，在必要時，經過授權許可的人員可以藉著同時取得一些分開保管的金匙，來破解加密所用的金匙，從而破解密文。當然，如果密文是透過其它加密法而產生，即使執法人員取得了那些分開保管的金匙也是毫無助益，因此，金匙寄管加密法最引人爭議的一點，便是它必需排除其它加密法的使用，才能達到最終的效益。本論文不願評斷金匙寄管加密法的構想，也無法預測金匙寄管加密法的最終命運，但是，現代資訊社會的每一份子，應該嘗試開始思考密碼學的意義，以及將來該走的方向。

另一個自力救濟方法所帶來的影響，也值得思考。匿名電子郵件帶來的，究竟是轉機？還是危機？如果，匿名電子郵件帶來的，是勇於表達意見，勇於嘗試意見，是注重意見的內容而非發表意見的個人或團體，那麼，整個社會將會更開放、更民主；但是，如果匿名電子郵件是被用來脅迫恐嚇他人，或散佈不實謠言，那麼，整個社會將會變的更黑暗、更混亂。在許多匿名再郵寄者已經設立，匿名電子郵件已經成爲事實的今日，匿名的意義與影響值得深思。

7. 結論

本論文概括性的探討了台灣學術網路中，一些與隱私權有關的問題，而這些問題的解決，首先有賴於適當法律的制定，以明確的規定網路中隱私權的範圍與適用時機，惟法律的制定，必需遵守憲法第十二條所定：「人民有秘密通訊之自由」的原則。

對於法律尚未涵蓋的範圍，台灣學術網路管理委員會似乎可以在其下成立專責之網路隱私權委員會，負責隱私權政策的制定與宣導，而各學校及研究單位，亦可成立關心隱私權的社團性組織，一方面宣導隱私權的重要性，一方面隨時注意與隱私權有關之各種現象，促請網路隱私權委員會解決。

台灣學術網路爲一教育性網路，除研究發展最新之通訊科技外，亦應教導對人類基本價值之尊重，以培養健全之國民。一個國家，若只擁有最新的科技，卻普遍缺乏對隱私權之尊重，甚至因此而影響對商業機密之保護，是否仍能長期繼續吸引跨國性企業之投資，頗值得思考。時值我國政治更民主，社會更開放，經濟更自由，並積極成立亞太營運中心之際，隱私權的問題，值得重視。

8. 參考文獻

[1] 陳文生、尹清海，"台灣學術網路（TANet）現況簡介，"*教育部電子計算機中心簡訊*，8311期，pp.3-15，83年11月。

[2] 曾憲雄、劉金和，"資訊化教育環境新藍圖，"*教育部電子計算機中心簡訊*，8311期，pp.45-57，83年11月。

[3] M.W. Bright, A.R. Hurson, and S.H. Pakzad, "A taxanomy and current issues in multidatabase systems," *Computer*, vol. 25, no. 3, pp.50-60, Mar. 1992.

[4] L.J. Camp, "Cryptography policy needs another look," *IEEE Spectrum*, vol. 31, no. 6, pp.15-16, Jan. 1994.

[5] W.R. Cheswick, "An evening with Berferd, in which a cracker is lured, endured, and studied," *Proceedings of the Winter USENIX Conference*, Jan. 1992.

[6] R.C. Clarke, "Information technology and dataveillance," *Communications of the ACM*, vol. 31, no. 5, pp.498-512, May 1989.

[7] A. Noor, "PGP: pretty good privacy," *Unix Review*, vol. 13, no. 2, pp.31-38, Feb. 1995.

[8] M.E. Schwartz and D.C.M. Wood, "Discovering shared interests using graph analysis," *Communications of the ACM*, vol. 36, no. 8, pp.78-89, Aug. 1993.

[9] W. Venema, "TCP wrapper: network monitoring, access control, and booby traps," *Proceedings of the Third Usenix UNIX Security Symposium*, Sep. 1992, pp.85-92.

[10] D. Farmer and W. Venema, "Improving the security of your site by breaking into it," ftp://ftp.win.tue.nl/pub/security/admin-guide-to-cracking.101.Z.

[11] "Sniffer FAQ" http://iss.net/~iss/sniff.html