科技法學評論，1 卷，頁 1（2004）

網際網路法發展趨勢特別報導*

王明禮[a1]　李界昇[a2]　周威秀[a3]　林三元[a4]
林明儀[a5]　林郁菁[a6]　林夢平[a7]　張睿元[a8]
雷雅雯[a9]　蔡惠如[a10]　蕭　敏[a11]

摘　要

伴隨著資訊通訊科技的急速進展與網路社群的快速演化，網際網路法（Cyberlaw）也在短短十來年內歷經不少變化，致學者們常有跟不上腳步之嘆。本特別報導的目的，就是要對本領域的重大發展做一概括性的介紹。從網際網路的管制結構，到智慧財產權、言論與內容管制、隱私權及網路犯罪及社會衝擊等主題，我們都嘗試從最新的案例發展、立法動態及學說與理論的演變等層面加以報導，並提供初步的分析，冀望能給有心瞭解網路法最新動態的各界先進一個實用的鳥瞰圖。

關鍵字：網際網路、網路法、智慧財產權、言論自由、隱私權

---

* 這篇特別報導是一項集體創作的成果。參與的成員大部分是 2003 年下半年在交通大學科技法律研究所修習 Cyberlaw 課程的同學。

a1 交通大學科技法律研究所助理教授。
a2 台灣積體電路股份有限公司工程師，交通大學科技法律研究所學生。
a3 執業律師，交通大學科技法律研究所學生。
a4 台中地方法院法官，交通大學科技管理研究所科技法律組博士生。
a5 交通大學科技法律研究所學生。
a6 交通大學科技法律研究所學生。
a7 交通大學資訊管理研究所科技法律組博士生。
a8 交通大學科技法律研究所學生。
a9 交通大學科技法律研究所學生。
a10 台北地方法院法官，交通大學科技管理研究所科技法律組博士生。
a11 晶豪科技股份有限公司法務經理。

Cite as: 1 Tech. L. Rev. 1 (2004)

Cyberlaw Special Report

Ming-Li Wang, Jason Jieh-Sheng Lee, Kelly Chou, San-Yuan Lin, Ming-Yi Lin, Yu-Ching Lin, Meng-Ping Lin, Richard Jui-Yuan Chang, Ya-Wen Lei, Grace Huei-Ju Tsai, Karen Min Hsiao

Abstract

Cyberlaw has made tremendous progress in recent years, following the footsteps of the technology and community that define its mission. Legal scholars in the field often lament that what you teach today will be outdated tomorrow, with only slight exaggeration. This special report aims to introduce the latest development in the field through the discussion of recent cases, legislative activities, and theoretical progresses covering topics of infrastructure, intellectual properties, speech and content regulation, privacy, cybercrime and social impact.

Keywords: Internet, Cyberlaw, intellectual property, freedom of speech, privacy

1. 前言

從一個實驗性產品，到社會大眾日常生活中不可或缺的一部分，網際網路（Internet）的崛起，見證了科技發展對人類生活的影響。而在短短幾年中，「網際網路法」（Cyberlaw）從一個看似標新立異的概念，成爲許多法學院的常設課程，則見證了網際網路對人類社會帶來的改變幅度。

網際網路法固然是個年輕的學門，變化卻非常快速。某些十年前的重大爭議，現在已經逐漸有了公論，取而代之的則是一些全新的議題。有些議題歷久彌新，但也發生了不少變化。這篇特別報導的目的，乃是要爲這個新興法領域的發展現況做一點整理，提供關心網際網路及相關法律發展的各界先進一個基本的瞰圖。

本文主要分爲五大部分。首先，我們介紹有關管制結構面的最新理論，然後進入幾個主要議題：智慧財產權、言論與內容管制、隱私權及網路犯罪。限於篇幅與能力，有許多主題不得不割愛，包括電子商務及競爭法有關的部分。

2. 網際網路的規範架構

網際網路的開端僅係美國國防部的一個研究計畫（ARPANet），其目的是爲了發展一個用「封包交換」（packet switching）代替「線路交換」（circuit switching）的通訊網路，以降低戰爭對通訊系統的威脅。1981 年 TCP/IP 通訊協定（Transmission Control Protocol/Internet Protocol）一統天下，成爲網際網路的基本通訊協定，網際網路也開始日漸茁壯。連接到網際網路上的電腦快速增加，很快的就超越一般地理疆界的限制，也因此引發了該如何管理網際網路的爭議。其中，在結構面的論戰，可以分爲兩個階段。

2.1 第一階段——管轄權爭議

2.1.1 基本問題

在這樣的發展脈胳下，早期的重要爭議是「誰有權管網際網路？」當時許多網路使用者認爲，網際空間（Cyberspace）是一個跨越國界的虛擬社會，實體世界裡的政府組織，均不能、也缺乏正當性，獨自有效地管理網路世界。代表性的人物包括 David Johnson 與 David Post 兩位法學者。在一篇著名的論文裡，他們力主以電腦螢幕爲網際空間的彊界，承認網路世界的自力性[1]。當然，反對的學者也不在少數[2]。

在網際網路基本上是個學術網路，網路使用者同質性高的時代，Post 等人的理論自然引起廣泛的共鳴。基於對學術社群的尊重，早年美國政府也的確對網路世界採取放任的態度，所以這類的辯論概念性高於政策實用性。但是當商業活動開始出現在網路空間，網路使用者的成色日趨多元，使用糾紛急速增加時，實體世界的政府必須對網際網路加以管理的壓力也越來越大[3]。基於保護本國人民及維護國家主權的立場，許多國家乃採取本國法優先的強硬立場。

2001 年的 Yahoo! v. LICRA et al.[4]案就是一個典型案例。二位法國公民於 2000 年去函 Yahoo，要求其停止於美國拍賣網站上登載納粹物品供售未果，便依法國之納粹符號法向法國法院起訴。法國法院認爲陳列系爭物品的網站雖在美國，但仍可被法國的網路使用者接觸，因此有法國法的適用，而判決命 Yahoo 須盡一切必要方法阻止法國境內之網友使用其美國網站上的

1 David R. Johnson & David G. Post, *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

2 例如，Goldsmith 教授就認為 Johnson 與 Post 等人低估了傳統法律機制處理司法管轄爭議的功能；Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

3 馮震宇，〈論網路商業化所面臨的管轄權問題（下）〉，《資訊法務透析》，頁 20（1997）。

4 Yahoo! v. LICRA et al., 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

納粹製品拍賣服務。原告乃於美國另行起訴，請求法院宣告該法國法院判決因違反美國憲法對言論自由的保障而不可執行，結果獲准。法、美二國之法院皆認對此事件具有管轄權，卻做出大相逕庭之判決結果。

2.1.2 網域名稱與商標之競合——實體世界法規範的勝利

雖然各國對於網路空間的管轄問題仍有岐見，對於某些議題的解決共識則已逐漸成型。最明顯的例子莫過於網域名稱（domain name）註冊人與商標所有人間之權利衝突問題。商標所有人希望將網域名稱視爲其商標權的延伸，視搶先註冊與其商標相同或近似之網域名稱者爲可鄙的網路蟑螂（cybersquatter）。但另一方則認爲網域名稱僅是網際網路上的一種位址識別方式，有如地址中的路名一般，不具商品的表徵性，網際網路行之有年的「先到先贏」政策應受尊重。商標法制的屬地性加深了此問題的複雜性。只有少數的商標具有普世的知名度，也只有少數的公司有財力在世界各國註冊其商標。到底誰才有權在全球性的「.com」網域註冊其商標呢？

經過數年的協商與協調，如今一個統一的處理模式已然成形。主管網際網路網域名稱政策的 ICANN（Internet Corporation for Assigned Names and Numbers），於 1999 年通過「網域名稱爭端解決政策」（Uniform Domain Name Dispute Resolution Policy, UDRP）[5]與及相伴的「解決規則」（rules for UDRP）[6]。前者乃所有域名註冊人皆須遵守之政策，而後者則爲「爭端解決機構」[7]受理糾紛案件時所須依循之規則，各機構並得參酌其自行訂定之補

---

5 ICANN, The Uniform Domain Name Dispute Resolution Policy, *at* <http://www.icann.org/dndr/udrp/policy.htm> (approved Oct. 24, 1999). *See also* Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy, *at* <http://www.icann.org/udrp/udrp-schedule.htm> (updated Feb. 5, 2002).

6 *See* ICANN, Rules for Uniform Domain Name Dispute Resolution Policy, *at* <http://www.icann.org/dndr/udrp/uniform-rules.htm> (approved Oct. 24, 1999).

7 目前 ICANN 已承認之爭端解決機構有五：ADNDRC、CPR、eRes、NAF 與 WIPO；*See* ICANN, Approved Providers for Uniform Domain-Name Dispute-Resolution Policy, *at*

充規則。根據 UDRP，只要 1.註冊人之域名與申訴人之商標或服務標章相同或近似致生混淆；2.註冊人對系爭域名無合法利益；3.系爭域名於惡意下被註冊並使用[8]，則已註冊之域名就會被取消。

ICANN 的這項政策，某程度等於將商標權延伸到網域名稱上。各地區性的註冊機構與爭端處理機構，也大致上都採用同樣的政策。美國 1996 年通過的「反網路侵占消費者保護法」（Anti-Cybersquatting Consumer Protection Act）[9]基本上也是同樣立場。雖然學界與網友間仍有反對聲浪[10]，但整體而言大勢已定。實體世界證實它的確有能力將其法規範延伸到網路空間之中。

2.2 第二階段——程式碼與法律的互動

如果第一階段的主要爭點在於「實體世界的法律能不能、應不應適用到網路世界」，那麼第二階段則在於「什麼樣的社會控制機制最適合網路世界」。這個階段的領導學者則非史丹佛大學法學院的 Lessig 教授莫屬。他指出，實體世界的法律及其他社會規範，背後其實都有一些自然界的事實基礎——Lessig 稱爲「控制的架構」（architectures of control）。例如，證人之所以得以在訴訟程序裡發揮功能，是因爲人有一定的辨識能力和記憶力。如果自然沒有賦予人類記憶力，證人就毫無用處[11]。我們平常之所以不太注意這個明顯的事實，是因爲它已存在太久，而被視爲理所當然。

早期的網友也經常將網際網路的一些特性視爲理所當然。例如，許多人誤以爲網際網路自然而然就是一個「自由」的世界。事實上，這些自由卻是

<http://www.icann.org/dndr/udrp/approved-providers.htm> (updated Mar 1, 2002).

8 URDP §4(a).

9 15 U.S.C. §1125(d).

10 *See* Jessica Litman, *The DNS Wars: Trademarks And The Internet Domain Name System*, 4 J. SMALL & EMERGING BUS. L. 149, 163 (2000).

11 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 31-32 (1999).

網路設計者有意無意選擇的結果。網際空間是由許多程式碼（code）所建構而成，程式碼就是網路世界的「大自然」。但與實體世界的大自然所不同的是，程式碼是人寫的，也是可變的[12]。程式碼的可操控性爲網路世界的社會控制機制帶來新的局面。網路的架構可以被設計成自由開放，也可以封閉獨裁；可以保障隱私權，也可以方便監控；可以促進言論自由，也可以箝制言論。今天網際網路的許多特性，不論好壞，都不是天生註定，而是選擇的結果。

在網際網路的發展初期，這些選擇可能是個別的程式設計師所爲，也反應出程式師社群的某些特質，如崇尚自由開放。但值得我們警惕的是，政治人物與商業利益正逐漸學會如何操控程式碼。法律，作爲社會控制的一種機制，至少在民主國家是經過一定的正當程序才能通過。而且，在必要時我們還可以選擇拒絕遵守（只要我們準備承擔可能的法律後果）。相對的，程式碼的控制卻不一定經過慎思熟慮，或顧及大眾的利益，對一般人（相對於程式高手）而言卻可能更直接、更具不可抵抗性。

Lessig 教授這種「程式碼爲網路世界重要的控制要素」的理論，很快就成爲網際網路法的主流，而且爲許多議題的辯證提供一個重要的思考角度。

3. 智慧財產權

自從網際網路發達以來，有關智慧財產權——尤其是著作權——的爭議就一直不斷。在出版、音樂、電影等產業的強烈反應下，各國政府和 WTO 迅速地通過立法來加強對著作權人的保障。其中，最顯著的發展就是美國在 1998 年通過的「數位千禧年法」（Digital Millennium Copyright Act, DMCA）[13]。該法提供給著作權人一項重要的勝利——增加對「著作權管理

[12] 人當然也可以操弄自然，但人對自然的控制力顯然遠為不足。

[13] Pub. L. No. 105-304 (1998).

資訊」（copyright management information）[14]及「著作權保護系統」（copyright protection systems）[15]的保護，爲「數位權利管理」（digital rights management, DRM）科技的使用背書，但也引發許多新的爭議。

然而，有關的爭議並未因此而平息。隨著寬頻網路的日漸普及與「點對點傳輸技術」（peer-to-peer technology, P2P）的發展，盜版著作在網路上益加盛行。錄音產業尤其深感威脅，極欲剷除 P2P 科技。在轟動一時的 Napster 案裡，美國錄音產業公會（Recording Industry Association of America, RIAA）固然成功地迫使 P2P 始祖 Napster 公司終止其服務，卻無力阻止 P2P 的熱潮。

另一方面，越來越多的學者與公益團體對著作權保護不斷擴張的趨勢感到憂心，認爲對保護智慧財產權的原始目的——鼓勵創作發明——將造成反效果。因此，主張智慧財產權保護體制應重新檢討的呼聲此起彼落。代表性的事件則是去年美國的 Eldred 案及開放原始碼運動。

3.1 P2P 與音樂盜版案件

傳統的網路傳輸以「主從式」（client-server）架構爲主，也就是由伺服器端按使用者之要求將資料傳送至使用者端[16]。相對的，P2P 傳輸架構則是直接於使用者間建立連線，也就是讓每個終端節點同時扮演伺服端與使用者端的角色。在主從式架構下，伺服器的數量遠少於使用者，伺服器本身的處理能力及其對外頻寬往往成爲瓶頸所在。相形之下，P2P 模式充份運用廣大使用者的電腦與頻寬，對網路上的瓶頸有一定程度的疏解作用。其最大的弱點，則在於伺服端數量眾多、分散且不穩定（大部分一般使用者的電腦不會 24 小時開機），如何讓使用者隨時掌握資料來源的分布狀態，就成了 P2P

14 17 U.S.C. §1202.

15 17 U.S.C. §1201.

16 William Fisher & Christopher Yang, *Peer-to-Peer Copying*, <http://cyber.law.harvard.edu/ilaw/P2P.html>(Nov. 18, 2001).

應用的重大關鍵。

讓 P2P 一夕揚名的 Napster 公司，就是靠著建立一強大的中央伺服器，負責爲所有使用者硬碟裡所儲存且願意提供的 MP3 檔案加以索引，好讓使用者得以很容易地查知可以從何處下載哪一首歌曲。一時之間，Napster 成爲音樂 MP3 檔案交換的天堂及錄音業者的眼中釘，終於導致 Napster 被法院命令停止服務的下場。

爲了避免重蹈 Napster 的覆轍，後 Napster 時代的 P2P 軟體，多改採所謂「無階式的 P2P」（tierless P2P）或「純粹 P2P」（pure P2P）架構。放棄了 Napster 式的集中式索引服務，這些新一代的 P2P 讓參與的各節點互相做索引，以避免軟體提供者成爲盜版行爲的共犯。Gnutella、Grokster、StreamCast Networks 與 Kazaa 等均是著例。

3.1.1 早期發展

雖然不是使用 P2P 技術，MP3.COM 案[17]卻是網際網路有關之音樂盜版案件的始祖。被告 MP3.COM 公司擅自將許多音樂著作以 MP3 的形式重製置於伺服器上，並藉以提供「My.MP3.com」之服務。其內容包含兩種類型：

1. Beam-it Service：客戶必須事先登錄其合法擁有的 CD，然後就能從被告網站下載 MP3 來聽。

2. Instant Listening Service：客戶向與被告合作之線上商店購買 CD 後，即可從被告網站下載 MP3 來聽，不必等 CD 寄到家。

因爲 MP3.COM 的服務具商業性質，且不具「轉換」（transformation）的特性，法院拒絕了被告合理使用的抗辯。此案也開啓了 RIAA 與 MP3 音樂傳播者之間戰爭的序幕。

記取了 MP3.COM 的教訓，Napster 自己並未提供任何 MP3 供使用者下

17 RIAA v. MP3.com, 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

載。如前所述，它所提供的是集中式的索引和軟體。該軟體扮演的角色如下：

1. 將使用者電腦上的 MP3 檔案建立索引，並將該資訊送回 Napster 公司的中央資料庫。

2. 讓使用者得以檢索該資料庫。

3. 向他使用者請求特定檔案。

4. 提供他使用者所請求的檔案。

因爲 Napster 公司本身並未從事任何重製音樂著作物的行爲，也未經手任何 MP3 檔案的傳輸（此等傳輸只發生在兩個使用者之間），因此自認並未侵害任何人的著作權。原告 A&M Records 等唱片公司卻不以爲然，起訴主張 Napster 應負間接侵權責任（secondarily liability，含輔助侵權 contributory infringement 及代理侵權 vicarious infringement）[18]，經美國聯邦第 9 巡迴上訴法院判決 Napster 敗訴確定。法院認爲 Napster 有意地鼓勵並協助使用者侵害原告之著作權，並對於使用者之侵權行爲有實質上之幫助。加上 Napster 因使用者之侵權行爲而直接獲利，且對彼等行爲有監督管理之能力[19]。

3.1.2 新的挑戰——無階性P2P架構

Napster 的失敗促成了無階性 P2P 的興起，此時一家獨大的情形已經不再。Gnutella、Grokster、Music City Networks、KaZaa、eDonkey 等群雄並起，且這些軟體的發展者也散布世界各地，使得有關的法律關係更加複雜。全球的唱片業者也只好分別在世界各地提起訴訟，企圖撲滅這股 P2P 的風潮。其中有些訴訟已經結束，有些仍在進行之中，我們擇要整理如下：

3.1.2.1 FastTrack

---

18 A&M Records v. Napster, 239 F. 3d 1004 (9th Cir. 2001).

19 惟地方法院之禁制令範圍過廣，故上訴巡迴法院予以修正為 Napster 只有在明知或可得而知使用者之侵權行為卻又未防止其發生時，始負輔助侵權責任，且僅於 Napster 未致力管理其系統而避免使用者侵權行為時，始負代理侵權責任。

Kazaa 創始者之一 Niklas Zennström 所開發的軟體技術 FastTrack，因採用 supernode 的技巧提昇無階式 P2P 的效率，很快成了最受歡迎的 P2P 系統。利用 FastTrack 技術開發軟體的有 Kazaa、Grokster 與 MusicCity Networks 等公司。爲了進一步增加自身的「訴訟免疫力」，Zennström 還利用了一些企業手法，包括將 Kazaa（原是一個荷蘭公司）的資產移轉給一個在南太平洋島國 Vanuatu 註冊的公司 Sharman Networks（以下簡稱 Sharman）。其網站原設在丹麥，後移至澳洲。FastTrack 的技術本身則移轉給一個在愛沙尼亞註冊的公司。這種複雜的安排，增加了唱片業提起侵權訴訟的困難度，也增加了法律——包括實體法和程序法——適用上的困擾。

和 FastTrack 有關的訴訟有多起，分別由不同的唱片業者在荷蘭、美國和澳洲等地所提起。除了澳洲的部分正由雪梨的聯邦法院審理中外，美國部分已有初步判決，而荷蘭部分則已在 2003 年底有了終局裁判。

荷蘭阿姆斯特丹地方法院於 2001 年底判決，以 Sharman 應採取必要措施以防止使用者侵害著作權爲由，認定 Sharman 侵害著作權，並要求 Sharman Networks 公司移除該網站。但上訴法院於 2002 年 3 月間判決廢棄地方法院判決，認爲 Kazaa 具有如交換笑話或個人照片等實質上合法用途，故被告無須爲使用者之侵害著作權行爲負責[20]。該判決經荷蘭最高法院於 2003 年 12 月 19 日判決維持而確定[21]。

---

20 Anupam Chander, Next Stop, Kazaakhstan?: The Legal Globe-trotting of Kazaa the Post-napster Filing Sharing Company (Oct. 24, 2002), *at* <http://writ.corporate.findlaw.com/commentary/20021024_chander.html>; Magdalena Heim-Smith, Peer-to-Peer File Sharing Since Napster (Fall 2002), *at* <http://gsulaw.gsu.edu/lawand/papers/fa02/heim-smith/#a24>; Eric Bangeman, Kazaa wins in European file-sharing court battle, *at* <http://www.arstechnica.com/news/posts/1071870117.html> (Dec. 19, 2003).

21 參見羅明通，〈P2P 資源共享架構之傳輸及重製在著作權法上之評價——兼論折衷式與無階式（NO-TIER）P2P 之技術差異〉，《月旦法學雜誌》，94 期，頁 212、219（2003）; Chander, *supra note* 20; Heim-Smith, *supra note* 20; Anthony Deutsch, *supra note* 14; Eric Bangeman, *supra note* 20.

另一方面，在美國加州提起的 Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.[22]一案，於 2003 年 4 月間經美國加州區聯邦地院判決，認爲被告等對於使用者之侵權行爲既無任何積極且實質之幫助，且無權也無法控制其使用者的行爲，因此不負輔助或代理侵權責任。本件原告業已提起上訴，預計今年將有進一步的結果。

3.1.2.2 Gnutella

Gnutella 屬於最純粹的無階式 P2P 系統，因爲它連 supernode 也沒有。所有的檔案搜尋都通過各終端節點以接力的方式傳遞。在前述的 Grokster 案中同列被告之一的 StreamCast Networks 公司（以前稱爲 MusicCity Networks，其軟體名稱爲 Morpheus），起初和同案其他被告同樣採用 FastTrack 技術，後來則改投 Gnutella 陣營[23]。採用同技術的還有 LimeWire 與 BearShare 等軟體。在 Grokster 案中，法院將兩個技術同等看待，認爲均不構成侵權。

3.1.2.3 轉向攻擊

目前看來，P2P 業者的「轉型」是成功的。利用無階式的設計，業者在釋出軟體後對使用者的行爲無任何的參與，因此連間接侵權責任也沒有。另一方面，新一代 P2P 軟體也放寬了得交換的檔案種類，而不再限於 MP3，因此得以理直氣壯地主張其軟體有許多正當的用途——例如用來交換使用者自己用數位相機拍攝的照片。許多學者也積極主張 P2P 技術所具備之開放與自由之特質，原爲網際網路發展所期許之最初目標，不應輕易扼殺[24]。

鑑於這樣的發展，除了繼續在 Grokster 案尋求上訴外，唱片業者也開始移轉打擊的目標——改以使用者爲訴追的對象。從 2003 年開始，RIAA 已

22 259 F. Supp. 2d 1029 (C.D. Cal., 2003).

23 *Id*. at 1032.

24 *See, e.g.*, LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 134-141 (2001); Fisher & Yang, *supra note* 16; SIVA VAIDHYANATHAN, COPYRIGHTS AND COPYWRONGS, 181 (2003).

經向許多 P2P 使用者提起侵害著作權之訴[25]，希望藉此殺雞儆猴。但此舉也多少冒著得罪消費者的風險，因此其後續發展仍有待觀察。

3.1.3 本土案例——ezPeer[26]和Kuro[27]

EzPeer 和 Kuro 分別爲全球數碼公司和飛行網公司的產品，其經營方式與 Napster 雷同。以 ezPeer 爲例，會員購買 P 點即可於個人電腦內安裝、使用 ezPeer 軟體，藉以連結全球數碼公司網站所管理之伺服器主機，將會員之電腦內 MP3 格式之音樂檔案資訊上傳至全球數碼公司的「檔名索引伺服器」，以供其他會員查詢。一旦查詢到所欲下載之 MP3 檔案，就可以自已連線會員電腦中下載。

士林地方法院檢察署檢察官於 2003 年 12 月初分別將 ezPeer 及 Kuro 之負責人及少數會員，以涉嫌違反著作權法第 91 條第 1 項、第 92 條第 1 項、第 94 條規定提起公訴，並請求對各該公司科以同法第 101 條第 1 項、第 94 條第 1 項所規定的罰金。

在美國，Napster 是被判應負間接侵權的責任。但我國著作權法並無類似條款，檢察官基本上是以共同正犯的方式將各該公司及其負責人起訴。這兩個案件將是國內在 2004 年最受矚目的著作權法案件。

3.1.4 和解與合作

雖然影音業者與 P2P 業者及其使用者之間的訴訟仍在如火如荼地進行之中，彼此的敵意也仍深，但最近也逐漸地出現一些和解甚至進一步合作的跡象。美國蘋果電腦的 iTunes 就獲得許多大唱片公司的支持，重新開張的

---

25 *See, e.g.*, Carrie Kirby, *RIAA Goes After 532 Unnamed File Sharers*, SAN FRAN. CHRON., Jan. 22, 2004, at B-1, <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/01/22/BUGJD4EP2O1.DTL>.

26 台灣士林地方法院檢察署檢察官 91 年度偵字第 10786 號、92 年度偵字第 4559 號起訴書。

27 台灣台北地方法院檢察署檢察官 92 年度偵字第 16389、21856 號起訴書。

Napster 也提供合法的音樂供下載[28]。Altnet 和 Sharman 也在規劃一以 Kazaa 爲基礎之安全商業 P2P 服務，使付費之客戶得以散布經授權的音樂、電影與遊戲檔案[29]。作者需要創作誘因，而公眾則期待以最少的交易成本接觸創作，如能設立某種機制，公眾可以合理但有價地接觸各種著作，將是創造雙贏的契機。

3.2 數位權利管理與存取控制

3.2.1 DRM與DMCA

除了利用訴訟手段來嚇阻盜版行爲外，各數位出版產業也努力發展新科技來保障其智慧財產，數位權利管理的相關技術乃應運而生。首先是所謂的「科技保護措施」（technological measures）。CD 雖然給音樂錄音產業帶來空前的收益，但因 CD 的規格沒有內建任何防拷機制，使得它也成爲盜版——包括盜版 CD 和網際網路上的盜版傳輸——的主要對象。經過這個教訓，DVD（Digital Versatile Disc）及其他新的數位內容技術——電子書、SACD 等——都特別強調科技保護措施的使用。以 DVD 爲例，出版者得選擇用 CSS（Content Scramble System）技術加內容加密，而所有的 DVD 播放設備——不論是硬體還是軟體——都得先取得 CSS 的授權，而且不得將解碼後的內容以數位的方式輸出。可錄式 DVD 的空白片，不論是哪一種規格，都保留一個特定區域爲唯讀狀態，以防止一對一的直接對拷。

除了防拷之外，CSS 也是區域播放控制（Regional Playback Control, RPC）的基礎。RPC 使商業電影出版商得以控制 DVD 發行的區域，而禁止不在發行區域裡的觀眾（事實上是設備）無法播放該 DVD。這種限制只有

---

28 Benny Evangelista, *The Music Revolution Has Arrived: Itunes, Napster 2.0 Make Downloading Songs Easy and Legal*, SAN FRAN. CHRON., Feb. 8, 2004, at E-1, <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/10/20/BUGJG2E8IF1.DTL>.

29 Paul Korzeniowski, *The Future of P2P File-Sharing Networks*, TECHNEWSWORLD, Dec. 4, 2003, *at* <http://www.technewsworld.com/perl/story/32305.html>.

某一區域的觀眾才能觀賞特定影片的手法，正是 DRM 的一種初級應用。更進一步的 DRM，則可以對授權的範圍——對象、時間、地點、權利內容等——做更細緻的切割，而分別要求不同的對價[30]。爲避免科技保護措施遭破解，美國重量級的著作權團體進一步遊說國會於 DMCA 中加入對著作權管理資訊及科技保護措施的保護[31]。

3.2.2 相關案例

在 Universal City Studios, Inc. v. Corley[32]一案中，一位挪威少年 Jon Johansen 與同夥運用反向工程（Reverse Engineering）的技術破解了 CSS，並將其破解程式碼 DeCSS 發布在網頁上。Eric Corley 因在其著名的駭客雜誌「2600」的網頁上介紹此事，並連結至提供 DeCSS 的網頁而遭八大影業公司起訴[33]。被告本身並未利用 DeCSS 從事任何盜版行爲，但仍被判違反 DMCA 的「反非法流通」（anti-trafficking）條款[34]。Johansen 本身則於 2003 年底經挪威上訴法院判決無罪後，因控方放棄上訴而確定[35]，因爲挪威的著作權法並不禁止破解保護機制的行爲[36]。

第二個案例是 2001 年的普林斯頓大學電腦科學教授 Edward Felten 事件[37]。RIAA 希望仿效電影業與消費性家電業者的科技保護協議，乃成立

---

30 *See, generally*, Lessig, *supra note* 24, at 177-217.

31 17 U.S.C. §1201, 1202 (2000).

32 Universal v. Corley, 273 F. 3d. 429 (2d Cir. 2001).

33 Corley 本來在其網站上直接提供該程式讓人下載，受警告後乃加以移除，但仍提供超連結。

34 所謂 anti-trafficking，指的是非法進口、提供、流通規避科技保護措施的技術、產品、服務等。*See* 17 U.S.C. §1201(a)(2), 1201(b)(1).

35 *See* BBC News, Film firms lose DVD piracy battle, *at* <http://news.bbc.co.uk/1/hi/technology/3371975.stm> (Jan. 6, 2004).

36 *Id.*

37 *See generally* EFF, Felten v. RIAA, *at* <http://www.eff.org/IP/DMCA/Felten_v_RIAA/> (visited Jan. 20, 2004).

Secure Digital Music Initiative（SDMI），進而設定一技術標準，能夠與製造廠商協議將一種稱爲的加密保護措施置入設備中。爲了證明 SDMI 的有效性，SDMI 空開徵求能破解其加密技術的挑戰者。Felten 的團隊成功找到了 SDMI 的缺失，並打算在學術研究會議上發表他的研究。RIAA 乃以訴訟威脅 Felten 不得發表，後者則起訴請求確認他有發表學術論文的自由。因 Felton 爲著名學府的教授，此事件經媒體報導後引起社會大眾對唱片業者的不滿。因此 RIAA 立刻改口，表示他們無意干涉學術自由。

第三個案例是俄國電腦工程師 Dmitry Skylarov 事件[38]。Skylarov 的程式可破解 Adobe 電子書閱覽器（Adobe eBook reader）上的科技保護措施，因此在網際網路上廣爲流傳。2001 年間美國利用 Skylarov 到美國參加學術研討會之際將其逮捕。該項行動受到人權團體的關注，也因 Skylarov 的外國身分受到國際矚目。2001 年底，Skylarov 獲准保釋出獄回國，交換條件則是他必須作證指控他的雇主 Elcomsoft 公司。最後該俄國公司也在 2002 年底被判無罪[39]。

3.2.3 主要爭點

3.2.3.1 對研究與創新的影響

DMCA 的「反規避」條款[40]將數位內容的著作權爭論帶進另一個層次。支持者主張該法是爲符合世界智慧財產權組織（World Intellectual Property

---

38 *See generally* EFF, EFF "Intellectual Property: Digital Millennium Copyright Act (DMCA): U.S. v. ElcomSoft & Sklyarov" Archive, *at* <http://www.eff.org/IP/DMCA/US_v_Elcomsoft/> (updated Mar. 13, 2003).

39 *See* Yochi J. Dreazen, *Russian Company Passes First Test Of Copyright Law*, WALL ST. J., Dec. 18, 2002, at B4.

40 17 U.S.C. §1201. 關於科技保護措施的保護其實有兩個條款：anti-circumvention 和 anti-trafficking，嚴格講只有前者才是「反規避」條款，後者則可譯為「反非法流通」。但就此處的討論而言，兩著沒有區別的必要，故併以「反規避」條款稱之。國外有關之文獻也經常如此。

Organization, WIPO）的「著作權條約」（WIPO Copyright Treaty, WCT）[41]和「表演與錄音物公約」（WIPO Performances and Phonograms Treaty, WPPT）[42]之要求而立。反對者則指出 WCT 僅要求「適當之法律保障及有效之法律救濟規定」[43]，而 DMCA 卻過於嚴格且涵蓋範圍過廣[44]。

學者特別指出，DMCA 的科技保護措施保障條款，將著作權的保護從傳統的「利用控制」（use control）帶到「接觸控制」（access control）的層次[45]。這是一種空前的變革，應該需要更周詳的考慮與更多的公眾討論。尤其是，對抗傳統的著作權侵害指控，行爲人得以主張「合理使用」以爲抗辯。但因反規避條款的規範對象——規避科技保護措施——本身不是一種著作權的侵害，所以不能主張合理使用。除了該條所定的法定例外之外，行爲人沒有其他的合法抗辯[46]。換句話說，即使行爲人對特定著作的特定利用有權主張合理使用，但如果該著作受到科技保護措施的保護，該行爲人仍然不能因此主張其規避行爲的合法性。

至於 DMCA 本身提供的七項例外條款[47]，則有過於狹隘之嫌。舉例來說，若是有著作權人懷疑某件加密的產品藏有侵害該著作權人權利的作品，則此著作權人唯一能找出答案的方法就是規避該產品的科技保護措施來檢視

41 *See* WCT article 11, 12 (Dec. 20, 1996), <http://www.wipo.int/clea/docs/en/wo/wo033en.htm>.

42 *See* WPPT article 18, 19 (Dec. 20, 1996), <http://www.wipo.int/clea/docs/en/wo/wo034en.htm>.

43 *Id.*

44 *See, e.g.*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999), <http://www.sims.berkeley.edu/~pam/papers/Samuelson_IP_dig_eco_htm.htm>.

45 *See, e.g.*, Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure For Rights Management Systems*, 15 HARV. J.L. & TECh. 41 (2001).

46 Samuelson, *supra note* 44, at 537-543.

47 *See* 17 U.S.C. §1201(d)-(j).

原始材料。但就算其懷疑事後獲得證實，他仍然違反了 DMCA[48]。更何況這些例外條款對一般人效益也很有限，因爲一般使用者沒有能力自行規避科技保護措施，而必須倚賴他人的工具，可是製作或提供此等工具本身也是被禁止的[49]。

此等爭論的核心爲合理使用在著作權法中的角色。如果我們把合理使用當成科技不夠發達時不得已的措施，那麼隨著科技的進步，合理使用的角色逐漸式微也就不值得我們憂心。換句話說，如果過去在圖書館影印一本書裡的一頁構成合理使用，只是因爲在紙張時代，要將一本書拆開出售有困難，那麼在電子書的時代，所謂「書」可以很容易地分開一頁一頁賣，那麼就不必再容許合理使用的存在。

相反地，如果我們認爲合理使用是著作權法制裡的一項重要制度，是爲了平衡著作權人對其著作的壟斷性控制，是爲了維特一個健康的「公共領域」（public domain），以作爲進一步研究與創新的基礎，那麼隨著科技進步，著作權人利用科技保護措施進行接觸控制的能力越強，我們反而需要更積極地維護合理使用的權利。

3.2.3.2 對隱私權的影響

由於網路時代的 DRM 可以讓廠商輕易地蒐集使用者的各種資訊——例如讀者的閱讀習慣，使讀者喪失匿名性，因此也有學者提出可能侵害隱私權的警訊[50]。因爲此種先進的 DRM 尚不普遍，因此一般人的感受並不強烈。但以近年來網際網路上有關 cookies 及商業網站蒐集與濫用消費者資訊所引起的關切來看，將來 DRM 對隱私權的威脅並不容輕視。

3.2.4 我國及歐盟的立法進展

48 Samuelson, *supra note* 44, at 543.

49 Burk & Cohen, *supra note* 45, at 49-50.

50 *See, e.g.*, Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).

我國於 2003 年 6 月 6 日通過的著作權法修正案中，增訂了權利管理電子資訊保護規定[51]，然而與 DMCA 有異曲同工之處的科技保護措施卻未經通過。在歐盟方面，其 2001 年著作權指令（Copyright Directive）[52]同樣禁止規避由著作權人所採用的科技保護措施或非法流通規避工具[53]。但與美國的 DMCA 不同的是，該指似乎只禁止商業性的規避行爲與工具，且在得允許的例外條款上和美國規定不同[54]。然因該條款的真義仍有爭議，各會員國會如何加以落實仍有待觀察[55]。但至目前爲止，各會員國實施的腳步緩慢[56]。

3.3 著作權保護期間爭議

Eldred v. Ashcroft[57]案所涉及是和 DMCA 同年通過的另一飽受批評的法案——著作權期間延長法（Sonny Bono Copyright Term Extension Act, CTEA）[58]。該法廣被譏爲專爲米老鼠而設，因爲 Disney 公司對米老鼠的著作權原應於 2003 年到期，因而對該法案的推動不遺餘力[59]。

---

51 參見著作權法第 3 條第 1 項第 17 款，第 80 條之 1，第 90 條之 3 及第 96 條之 1。

52 Council Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (*hereinafter* EU Copyright Directive).

53 *See id.*, article 6(2). 但學者指出該條文義不明，所謂「商業性」是用來修飾整個子句，還是只有最後一個項目仍有爭議；Brian W. Esler, *Protecting the Protection: A Trans-Atlantic Analysis of the Emerging Right to Technological Self-Help*, 43 IDEA 553, 596 (2003).

54 EU Copyright Directive, article 6(4).

55 Esler, *supra note* 53, at 598-604.

56 該指令規定會員國應在 2002 年 12 月 22 日前立法落實該指令；article 10. 但歐洲執委會（European Commission）發現只有希臘和丹麥在該期限前達成，而另有四個在 2003 年間完成，其他則仍未執行；*See* EC Press Release, Commission Acts to Ensure Eleven Member States Implement EU Laws, Dec. 17, 2003, *at* <http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1752|0|RAPID&lg=EN>.

57 123 S. Ct. 769 (2003); rehearing denied, 123 S. Ct. 1505 (2003).

58 Pub. L. 105-298, 11 Stat. 2827 (1998).

59 *See, e.g.*, Robert Patrick Merges & Glenn Harlan Reynolds, *The Proper Scope of the Copy-*

原告主張美國著作權保護的法源——憲法第 8 條第 8 款——規定著作權保護是爲了「促進科學與藝術」（to promote the progress of science and useful arts），而且必須限定保護期間[60]。因此，著作權的保護期間不應無限期延長。如果延長，則必須有助於憲法所設定之目的。反之，如果延長太多，以致妨害公共領域的成長，反而對進一步的創新造成負面影響，則這樣的延長就是違憲。同時，因著作權保護也構成對言論自由的限制，因此太長的保護期間也違反第 1 增補條款對言論自由之保障。

然而美國聯邦最高法院在 2003 年判決認爲該法的合憲性。其主要理由是該法雖將著作權保護期間延長二十年，但仍符合憲法所要求的「限定期間」。至於到底多長的保護期間才不致妨害鼓勵創新的憲法目標，則屬立法裁量的範圍。而只要是合憲的著作權保護，就不生違反憲法對言論自由保障問題[61]。

3.4 開放原始碼運動

在著作權保護與公共利益的角力裡，「開放原始碼運動」（open source movement）稱得上是另闢蹊徑——它利用著作權法所提供的保護，來建構公共使用的空間。它的興起和網際網路的發達有很密切的關係，而它的發展，則爲思索網路空間和智慧財產權相關法制的未來的有識之士，提供了許多值得玩味的線索[62]。

3.4.1 開放原始碼運動簡介

---

right and Patent Power, 37 HARV. J. LEGIS. 45, 53-54 (2000).

60 U.S. CONST. art. I § 8, cl. 8.

61 本案另有 Stevens 與 Breyer 兩位大法官提出不同意見書，基本上贊成原告的見解；123 S. Ct. 769, 790-815 (2003).

62 *See generally*, Lessig, *supra note* 24, at 49-72.

3.4.1.1 源起

開放原始碼運動源自於一個需要解決軟體瑕疵的程式設計師 Richard Stallman[63]。在電腦發展初期，程式的原始碼通常隨硬體提供，而使用者也經常幫忙除錯或改良軟體。因此當有一天，某印表機廠拒絕繼續提供驅動程式的原始碼時，Stallman 生氣了。他認爲該程式包含了許多使用者——包括他自己——的心血結晶，如今卻被據爲己有。而且，缺乏原始碼，他就不再能自行修改軟體，即使是芝麻大的問題都必須倚賴原廠商解決[64]。

於是 Stallman 於 1985 年成立了「自由軟體協會」（Free Software Foundation），大力鼓倡軟體原始碼必須開放的理念。這樣的理念在網際網路初期崇尚分享的氣氛下廣爲接受，加上特殊設計的公眾授權條款，確保了他人衍生創作的回饋機制，排除私人在公眾資源上搭便車的可能，因此吸引了更多具有共同理想的程式設計師自願加入，形成一個互惠合作的社群。1991 年經赫爾辛基大學生 Linus Torvalds 貢獻出一套作業系統的核心後，進入另外一個階段，在採用公眾授權條款的號召下，許多程式設計師自願無償地投入可觀的心力，經過多年群策群力之後，產生了足以和微軟 Windows 系統相抗衡的 Linux 系統，而受到各方的注意。

開放原始碼特殊之處在於，每個人都可以無償取得程式碼，並加以修正或改良。對於衍生著作在權利歸屬與限制上，不同授權條款有著不同的規定，有的只要求維持原始的著作人格權，而允許對衍生著作進行商業上的用途[65]。但許多則要求衍生著作必須再以同樣的授權條款無償地回饋到開放原

63 Stallman 是開放原始碼運動中傳奇人物之一。當年為 MIT 研究員，其後曾隱居一年半載，以 10 多萬行程式打造出廣為流通的編譯器 GCC，為其後自由軟體的開展打下良好基礎。

64 *See* Lessig, *supra note* 24, at 52-54.

65 如 BSD 版本的授權條款。對衍生著作如不設限，可能為商業軟體所吸收、改良，而在市場上形成原開放原始碼開發計畫的競爭對手，因此，一般多採用類似 GPL 的授權模式，再加以調整。

始碼社群中，其中最重要的首推 GNU Public License（GPL）[66]。GPL 允許別人取得原始碼後可以自行修改，以符合自己的需求，但如果再散布衍生著作，則必須受到相同 GPL 條款的規範將改良成果再公布出來。在授權條款中，這種達到藉由著作權法及契約來確保衍生著作維持在公眾領域中的做法，有人稱之爲 copyleft，以示與傳統的 copyright 有別，而後續連鎖效應中保有相同授權條款的特性，則有人以 viral 稱之[67]。

在 GPL 之後，開放原始碼運動中因不同軟體開發計畫有著不同的授權考量，而需要各式各樣的授權契約，加上最初運動中標舉著「自由軟體」容易產生「免費軟體」的誤解[68]，增加商業軟體公司加入的疑慮，於是有「開放原始碼協會」成立，並制定「開放原始碼定義」[69]，凡符合定義中十項基本要求者，就可以稱之爲開放原始碼模式下的軟體。其中比較重要的規定即包括：必須開放程式的原始碼、必須可以自由散布原始碼、允許衍生著作在相同的條款下再散布出去、不可對特定使用族群或領域設限等[70]。

3.4.1.2 優勢

和封閉式的軟體開發方式相比，開放原始碼陣營特別強調兩點優勢：

1.軟體的安全性[71]

在軟體複雜度與日俱增的情況下，利用其瑕疵進行擴散的電腦病毒時有所聞，而網路的普及，也讓電腦上的資料可能未經查覺即流通出去，一般大眾每天使用的各種軟體是否安全，其實有待質疑。開放原始碼在這裡所代表

66 細節請參見 GNU, Frequently Asked Questions about the GNU GPL, *at* <http://www.gnu.org/licenses/gpl-faq.html> (updated Feb. 26, 2004).

67 Viral 取其「如病毒般快速擴散」之意，其利弊分析可參閱 Christian H. Nadan, *Open Source Licensing: Virus or Virtue?*, 10 TEX. INTELL. PROP. L.J. 349 (2002).

68 因其英文為“free software”。

69 Open Source Initiative, The Open Source Definition, version 1.9, *at* <http://opensource.org/docs/definition.php> (visited Mar. 2, 2004).

70 *Id.*

71 有關開放原始碼軟體與軟體安全及電腦犯罪的關係，在 6.2 續有討論。

的意義，在於資訊透明後所提高的安全性，程式設計師占人口比例上雖然不高，但因「只要注視目光夠多，臭蟲就無所遁形」[72]，其所形成的社群扮演著關鍵性的少數。原始碼的公布有如陽光法案，在一切透明之後，軟體中蓄意植入對使用者不利功能的機會將下降，即使一旦發生，相關社群也能發揮把關的效果[73]。相對之下，現行封閉式的軟體則一切仰賴原廠軟體公司的品質與服務。

對國家安全而言，如果無法完全掌控並檢驗所使用的軟體，則資訊戰的佈署無異於一座沙灘上的碉堡，許多國家大力採用開放原始碼的理由在此，微軟「分享原始碼」（shared source）計畫的著眼點也在此。但因「分享原始碼」所分享的對象有限，是否能達到藉外力協助爲系統安全把關的效果仍有待觀察。

2.數位鴻溝的跨越

對許多開發中國家而言，開放原始碼軟體有另外一層的吸引力。除了軟體成本低廉外，也有機會讓技術生根，而每年花在購買專屬軟體或廠商強迫升級的費用，則可以轉投入研發或基礎建設的設立。目前有 25 個國家提出 70 多個有關自由軟體之法案、政策及聲明，歐盟在建立電子化政府及資訊交換平台上，也特別提出詳盡的「遷徙指南」[74]，說明相關單位應如何以開放原始碼的軟體取代現有的專屬軟體。

---

72 原文為“Given enough eyeballs, all bugs are shallow.”，由 Open Source Initiative 創始人 Eric Raymond 所提出，他將其稱為 “Linus’s Law”；See Eric Steven Raymond, Release Early, Release Often, a section in his online treatise The Cathedral and the Bazaar, Revision 1.57, *at* <http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ar01s04. html> (Sept. 11, 2000).

73 例如曾有人試圖在 Linux 新版的系統核心中植入安全漏洞，但隨即被其他社群成員發現而移除；Kevin Poulsen, Linux Kernel Backdoor Blocked, *at* <http://www.theregister.co.uk/content/55/33855.html> (posted Nov. 7, 2003).

74 INTERCHANGE OF DATA BETWEEN ADMINISTRATIONS, THE IDA OPEN SOURCE MIGRATION GUIDELINES, <http://europa.eu.int/ISPO/ida/export/files/en/1618.pdf> (Nov. 8, 2003).

3.4.1.3 擴展

基於開放原始碼模式的優點及隨手可得的大量資源，許多國家除努力導入並擴大應用外，並進一步加強合作，例如中國大陸、韓國及日本宣布將共同開發一套以開放原始碼爲主的作業系統，以取代 Windows 系統。在國內，產官學界發起「阿里山計畫」，希望以五年時間推動 Linux 系統，經濟部則設立「自由軟體入口網站」[75]，作爲推廣開放原始碼的平台。

開放原始碼的精神也正逐步擴大到軟體社群之外。例如，爲了擴大公眾自由創作空間，Creative Commons 這個組織參考開放原始碼的公眾授權模式，制定同樣以分享爲出發點的 Creative Commons License（簡稱 CC License），用來規範文字、影像、音樂等各種媒介下著作權人的權利與義務，並賦予創作者選擇調整授權條款的彈性[76]。在台灣，中央研究院資訊所已領軍加入相關合作[77]，從事相關授權條款的本土化及推廣工作。

3.4.2 法律議題

目前與開放原始碼運動相關的訴訟，以 SCO v. IBM 一案最受注目。IBM 近幾年投注可觀人力在開放模式主流系統 Linux 上，作爲其降低軟體成本往顧問服務業轉型的利器，因而影響了包括 SCO 在內 Unix 廠商的獲利。因此 SCO 於 2003 年對 IBM 提起訴訟，指控其侵害著作權、營業秘密、違反授權合約及構成不公平競爭，並求償數十億美元。SCO 主張 Linux 之快速成長，實因 IBM 違反授權合約將其專屬的程式碼流入開放原始碼社群中之故。SCO 並試圖挑戰開放原始碼模式賴以運作的公眾授權條款，主張 GPL 等的強制回饋條款沒有法律上的拘束力。因其潛在影響極大，SCO 案在開放原始碼社群中引起軒然大波。其後對使用 Linux 的客戶散發警告函

75 自由軟體入口網站，*at* <http://www.oss.org.tw> (visited Mar. 23, 2004).

76 Creative Commons, *at* <http://creativecommons.org/> (visited Mar. 23, 2004).

77 台灣正體中文 iCommons 討論網站，*at* <http://www.openfoundry.org/icommons/> (Nov. 29, 2003).

的動作，更讓另外一家 Linux 主力廠商 Red Hat 決定加入戰局。最近微軟也被發現私下以金援的方式鼓勵 SCO 興訟，更使得本案成爲開放與封閉兩種軟體產業模式的一次大對決[78]。

另外一個值得觀察的是軟體專利對開放原始碼運動的影響。軟體專利及商業方法專利對促進資訊科技及產業的進步是否有正面幫助？一直是爭論不斷的議題[79]。有人建議從制度面改革，以符合軟體生命週期較短、技術需要累積漸進的特性[80]，也有人直接建議縮短軟體專利保護的年限[81]。在現行制度下，開放原始碼社群視軟體專利爲潛在的地雷區。一則對專利局因缺乏前案而生的審查品質感到荒謬，二則在程式設計師無償貢獻原始碼的情況下，不可能自行負擔申請費用。而且，專利制度的設計以保護爲目的，跟開放原始碼運動以分享爲初衷並不相容，使得軟體專利在開放原始碼運動中一直如芒刺在背，而相關社群卻又遲遲無法有效地正面以對。近年來，微軟在軟體專利方面的申請案持續攀升，並間接迫使 WIPO 放棄將開放原始碼列爲討論議題[82]，以微軟在開發中國家屢屢失利於 Linux 系統來說，有人憂心封閉原始碼廠商將透過失衡的專利制度抑制開放原始碼運動的發展。

---

78 *See* Steve Lohr, *Microsoft Said to Encourage Big Investment in SCO Group*, N.Y. TIMES, Mar. 12, 2004, at C5, <http://www.nytimes.com/2004/03/12/technology/12soft.html>.

79 *See, e.g.*, FEDERAL TRADE COMMISSION, TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY (2003)（認為就軟體界而言，競爭的強化比專利制度更能促進資訊界的創新，其中並將開放原始碼模式列為有效替代方案之一), <http://www.ftc.gov/os/2003/10/innovationrpt.pdf> (accessed Mar. 23, 2004)。

80 *See, e.g.*, Dan L. Burk & Mark A. Lemley, *Is Patent Law Technology-Specific?*, 17 BERKELEY TECH. L.J. 1155 (2002).

81 *See, e.g.*, Lessig, *supra note* 24, at 260.

82 去年 8 月，微軟資助的團體向美國州部門及專利局代表遊說，以開放原始碼有礙技術的創新與經濟成長為由對 WIPO 施壓，迫使取消原本將開放原始碼納入議題的計畫，學者 Lessig 的批評可參見<http://www.lessig.org/blog/archives/001436.shtml> (visited Mar. 23, 2004)。

3.4.3 國內產業的機會

台灣在全球資訊產業的版圖中占有一席之地，特別是在硬體方面表現突出。從上游的 IC 設計、晶圓製造、封裝測試、零組件組裝、主機板，到各式各樣的消費性電子產品，如筆記型電腦、液晶電視、DVD 光碟機等，產業在激烈競爭與群聚效益的綜效中，持續提升市場占有率。而近年來，硬體產業更逐漸將製造部分轉移到勞力成本更低的區域，往設計代工及其他附加價值更高的方向升級，相對於硬體產業，軟體產業不僅相形見絀，而且在印度及中國大陸等崛起後，亦有轉型的壓力。在這樣的情況下，如何善用開放原始碼所帶來的機會？除了推動軟體中文化或開發以中文處理爲核心的技術外，或許還可從產業特性加以思考：

1.擴大開放程式碼可執行的硬體範圍：目前 Linux 系統面臨的問題之一在於可支援的硬體相對較少，台灣作爲硬體設計製造的主要基地，如能主動對 Linux 等開放原始碼系統增加支援，應有助於開放原始碼運動的推展，並間接增加市場影響力。對於硬體在驅動程式方面，則需要軟體人才的加入。

2.降低軟體成本：資訊家電的應用範圍隨著網路而擴大，硬體廠商有機會附加各種軟體的功能提高整體系統的價值，如軟體部分可有效運用低成本的開放原始碼[83]，則有助於在微利時代下提高獲利的可能。

4. 內容管制與言論自由

網際網路基本上是一個溝通的工具，訊息傳遞的基本架構（infrastructure）。因此，在網路上流通的「內容」，雖然不見得有著作權，甚至不見得構成「著作」，但除了完成無法意會的「純資料」之外，幾乎都是某種形式的「言論」。也因此，在網路社會裡，和言論有關的困擾或糾紛特別多，也就不足爲奇。但也因涉及言論自由，任何打擊「不當」內容的企圖——只

83 如內嵌式系統核心 eCos 採用開放原始碼模式，亦逐漸形成開發社群，詳見 eCos, *at* <http: //sources.redhat.com/ecos/>(visited Mar. 23, 2004).

要是由國家發動的——都必須通過憲法的檢驗。尤其在網際網路發源地、使用人數最多、對任何問題的處理都洞見觀瞻的美國，言論自由更是最重要的基本人權。這樣的價值取向，深植整個網路社群。當我們在分析相關法律議題時，也就不能脫離這樣的社會脈絡。

回顧網際網路法的發展足跡，我們可以看到一些有趣的轉折。在一方面，網路色情一直是政府和衛道人士所頭痛的問題。另一方面，早期引起激烈爭執的誹謗問題，已經逐漸退燒[84]，大體上只留下一個尾巴——關於匿名言論的價值與可容忍性。相反的，早期普遍認爲是小問題的「垃圾電郵」（spam）[85]，則成了今天人人喊打的過街老鼠。

4.1 網路色情

色情一直是最善於利用各種新興媒體的內容形態，網路的匿名性提供使用者更多接觸色情的機會，因此網路色情的歷史和網際網路本身幾乎一樣久。有鑒於網路色情對未成年人的不良影響，各國均試圖立法加以防堵。

在進一步討論之前，有兩個前提問題必須先加以釐清。首先是關於「猥褻」（obscenity）與「色情」（pornography）的差別。在一般的討論中，這兩個概念似乎並沒有太明確的區分。但色情其實應是猥褻的上位概念，色情不見得構成猥褻，而只有猥褻才受刑法的制裁。我國如此，美國也如此。第二個問題是有關尚未構成猥褻程度之色情言論（以下簡稱色情言論或色情）對社會的害處。有人認爲根本就無害，國家不必也不應做任何管制，任由家

84 主要可能是因為涉及語言的障礙及言論的效果，妨害名譽的糾紛很少跨國界，只要事實——行為人與行為態樣——能夠確定，適用各國原有的法律並無沒有太大困難。而因各國執法機關的電腦及網路技術都已大幅提升，在事實的偵查上也比過去有效率得多。

85 spam 其實沒有很明確的定義，更沒有統一的中文翻譯。spam 不僅可能以電子郵件的形式出現，也可能以 Usenet 上的文章或其他方式出現，比較嚴謹的翻譯應為「垃圾訊息」。但因本文討論以 email spam 為主要對象，且各種有關 spam 的管制法令，也多僅以 email spam 為對象，所以採取「垃圾電郵」之譯名。

長們自行決定如何教育其子女即可。另一方面，某些女性主義者認爲色情對社會上普遍存在的性別歧視具有強化的作用，因此主張政府應全面管制[86]。本文以下的討論則是站在通說的立場，認爲色情雖屬未成年者不宜，但國家無權過問成年人的接觸。

4.1.1 屢敗屢戰的美國國會

1996 年美國國會通過 Communications Decency Act（CDA），因屬全球第一個針對網路色情的立法，而格外受到矚目。其中最受爭議的條文於 1997 年美國聯邦最高法院宣告違憲[87]，媒體廣爲報導，應爲多數人所熟悉。

隨後，美國國會檢討 CDA 被宣告違憲的原因後，在 1998 年通過 Child Online Protection Act（COPA）。COPA 將管制範圍限縮在 WWW 上所顯示的資訊，且僅針對商業性的傳輸。同時，COPA 也放棄 CDA 受到最多攻擊的要件——不雅（indecency），而改採「對未成年人有害的資訊」（material that is harmful to minors），並以盡可能和 Miller test 接近的方式加以定義[88]。所謂「未成年」的年齡標準也降低爲 17 歲[89]。

COPA 通過後，一些反 COPA 的民間組織立刻在它尚未生效前就起訴挑戰其合憲性[90]。賓州東區聯邦地院認爲該法有可能無法通過嚴格審查基準的檢驗，因此發布初步禁制令（preliminary injunction）[91]，禁止該法的執行。

---

86 請參閱，CATHARINE A. MACKINNON, FEMINISM UNMODIFIED: DISCOURSES ON LIFE AND LAW, 10-15, 127-133 (1987). Mackinnon 為女性主義中宰制理論（dominance approach）的代表，認為色情是男性霸權下男性的利益（sexual access to women）的一種形式，將女性物化與商品化，而強化社會上的性別歧視（sexual discrimination），故主張所有的色情均應禁止。

87 Reno v. ACLU, 521 U.S. 844 (1997).

88 *See* 47 U.S.C. § 231(e)(6) (2000).

89 47 U.S.C. § 231(e)(7) (2000).

90 該法案規定自法案通過日起 30 日後生效；Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 §1406 (1998)。

91 ACLU v. Reno, 31 F. Supp. 2d 473 (1999). 當時尚在 Clinton 政府時代，因此由當時的

經政府上訴後，第 3 巡迴上訴法院維持該禁制令，但基於不太一樣的理由。上訴法院援引最高法院在 CDA 案裡的見解，認爲根據該法的定義，對未成年人有害與否必須「依當代社群標準」來認定，但依當時的科技水準，網站不可能按地理區域來區隔使用者，結果將被迫以當代最保守的社群標準來自我設限，否則就可能違法。法院認爲如此的立法方式範圍太廣[92]。

政府再上訴後，聯邦最高法院推翻了該項見解，認爲單單採用「當代社群標準」這樣的要件來定義「對未成年人有害的資訊」，並不必然導致違憲的結果。最高法院認爲 COPA 和 CDA 不同，雖然後者也同樣在所謂「顯然令人厭惡」的定義裡使用「當代社群標準」這樣的概念，但 CDA 最大的問題是它的打擊範圍實在太大，所以法院特別擔心這樣的立法方式，可能使政府利用最保守社區的言論尺度來限制全國言論。COPA 的打擊範圍小得多，所以就沒有這層顧慮[93]。最高法院不願意冒然評斷 COPA 的合憲性，選擇將全案發回給上訴法院審理。這次上訴法院仔細地檢討 COPA 的各項要件，以及所應適用的司法審查原則，最後仍然認爲原告有獲勝的可能，而維持原禁制令[94]。目前全案又回到最高法院手中，預計在 2004 年將有進一步的結果。

在有關色情管制的論戰中，不斷有人提出讓家長自行安裝過濾軟體才是正途。在 CDA 一案裡討論其所採取的手段是否過當時，最高法院也肯認過濾軟體可能同樣有效，又不會對成年人構成不當的限制[95]。因此，當發現直接管制色情傳播源似乎難關重重後，美國國會試著在 2001 年的 Children's Internet Protection Act（CIPA）採取另一種管制手段——強制安裝過濾軟

司法部長 Reno 代表政府擔任被告。

92 ACLU v. Reno, 217 F. 3d 162 (2000).

93 Ashcroft v. ACLU, 535 U.S. 564 (2002). 法院認為，「當代社群」在此指的是自網路上接收訊息的觀眾所在地區的社群，因為 COPA 限縮了適用範圍，故此一標準並不使之違憲。

94 ACLU v. Ashcroft, 322 F. 3d 240 (2003).

95 Reno, 521 U.S. at 844-845.

體，對象則是接受聯邦補助的中小學和圖書館[96]。

美國圖書館協會（American Library Association）領銜提起違憲之訴。美國聯邦最高法院的複數意見（plurality）認爲圖書館有選擇所收藏圖書內容的裁量權，且此裁量權在該館所提供網路服務的內容篩選亦同。但是囿於經費人力與時間等現實因素，欲一一過濾網站內容絕無可能。是以，事先裝設阻止接觸的程式雖可能阻斷成年人接觸有價值的色情言論，在兩相權衡下，仍宜認爲 CIPA 之要求不違憲[97]。其次，由於 CIPA 是以限制補助的方式進行管制，未直接限制成年人的任何權利，且圖書館服務內容非公共論壇（public forum），因而政府應擁有較大的管制裁量權，故 CIPA 不違憲[98]。

4.1.2 我國的最新發展

針對網路色情的問題，政府在近年做了以下的努力：

4.1.2.1 兒童及青少年性交易防制條例新增「網路援交」條款

兒童及青少年性交易防制條例係爲防制、消弭以兒童少年爲對象的性交易事件而制定[99]。其中第 29 條係援助交際條款，爲防制以兒童、少年爲主體的援助交際。該條於 1999 年修法時，將網路援交行爲納入規範。該條所謂「足以引誘、媒介或暗示或其他促使人爲性交易之訊息」的判斷，最高法院認爲應依社會一般人之標準客觀爲之[100]。

此外，本條修正前，依一最高法院刑庭會議決議，屬結果犯，須產生性交易之結果方得成立[101]。經修正後，已不再以實際發生性交易結果爲要

96 美國的學校和圖書館，即使是公立的，也是隸屬於州或地方政府，而非聯邦政府，因此即使不考慮言論自由的問題，聯邦法也不能直接強制彼等安裝過濾軟體。

97 *See* U.S. v. American Library Ass'n, Inc. 123 S. Ct. 2297, 2303-2307 (2003).

98 *See id.* at 2307-2309.

99 兒童及青少年性交易防制條例第 1 條。

100 參見最高法院 92 年台上字第 2305 號判決。

101 參見最高法院 87 年度第二次刑事庭會議決議。

件[102]。例如於網際網路上聊天室中之對話，如可「使其他上網瀏覽該項聊天主題之不特定人，均能輕易明瞭被告渴求性交易的意圖，形同刊登暗示性交易之廣告訊息」，即有本條之適用[103]。

4.1.2.2 「網站內容分級制度」的推動

2003 年 5 月，兒童及少年福利法公布施行，第 27 條規定電腦網路應分級。新聞局希望網路服務業者能自發性地爲網站內容分級，現正邀請國內主要的網路服業者簽署自律公約。但電腦網路上之內容遠較傳統媒體多樣，如何執行仍待觀察。

此外，2003 年國內也出現一個高度爭議性的案件——何春蕤案。刑法第 235 條之目的在規範散布猥褻物品之行爲。1999 年，爲因應網路色情資訊的泛濫問題，修正本條文，將散布物標的內容增加了「聲音、影像」，散布行爲亦增加「播送」。以推動女性主義運動著名的中央大學何春蕤老師在其「性／別研究室」網站上，有關「性解放」議題的網頁中，置有介紹「動物戀」之網頁，其中提供連結至某國外有關動物戀的網站，其上提供有人與動物性交之圖片[104]，遭立委曾蔡美佐和勵馨基金會等十多個團體告發涉嫌觸犯刑法猥褻罪，嗣後台北地檢署檢察官以本條文起訴，引起社會對色情、猥褻與性別議題的關注[105]。

因該案不僅涉及學術研究與言論自由，且涉及刑法第 235 條所謂「散布」等行爲的構成要件如何解釋的問題，有可能成爲我國在網路色情管制上的重要案例。

4.2 垃圾電郵

102 參見最高法院 92 年度台上字第 2139 號。。

103 參見台灣彰化地方法院 91 年訴字第 1125 號判決。

104 請參閱，台灣台北地方法院檢察署 92 年度偵字第 23213 號起訴書。

105 請參閱，王己由、高有智，〈人獸交圖片官司 何春蕤論辯 社運團體聲援〉，《中國時報》，2004 年 1 月 17 日，<http://news.chinatimes.com.tw/Chinatimes/newslist/newslist-content/0,3546,110503+112004011700061,00.html>。

如果說網路色情的問題令家長們憂心，那麼垃圾電郵大概是絕大多數網路使用者共同的困擾[106]。本文將分別從立法解決與技術解決兩個層面，說明相關的最新發展。

4.2.1 法律途徑

我國目前尚無針對垃圾電郵的立法，但垃圾電郵對網路資源造成的浪費，已經引起 ISP 的不滿，要求立法的呼聲不小。但據報載，法務部認爲垃圾電郵與隱私權無涉，不宜在由其主管的「電腦個人資料保護法」中規範[107]，因此我國未來立法動向仍不明。相對的，許多其他國家或地區已開始立法管制垃圾電郵，以下將擇要介紹。

4.2.1.1 美國

從 1997 年內華達州開始[108]，截至目前爲止，至少已有 36 州制訂管制垃圾電郵的法律[109]。在聯邦方面，則在 2003 年底通過延宕了 6 年的「垃圾電郵控制法」（Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, CAN-SPAM Act of 2003）[110]終於獲得參、眾兩院表決通過，並自 2004 年元旦起生效，其效力凌駕於各州之垃圾電郵管制立法。

在管制對象上，垃圾電郵控制法自限於「未經索取的商業電郵」

106 *See, e.g.,* PEW INTERNET PROJECT, SPAM: HOW IT IS HURTING EMAIL AND DEGRADING LIFE ON THE INTERNET, (2003), <http://www.pewinternet.org/reports/toc.asp?Report=102>.

107 劉鳳琴，〈垃圾郵件不涉隱私，無法規範〉，《中國時報》，2004 年 3 月 23 日，<http://news.chinatimes.com/Chinatimes/newslist/newslist-content/0,3546,110503+112004032300062,00.html>。但包括歐盟在內的許多國家或地區，但是從保護隱私權的觀點出發來管制垃圾電郵；參見 4.2.1.1 以下之介紹。

108 DAWN ESTES & BHAVEENI PARMAR, SPAM, SPAM AND MORE SPAM 7, Paper for 16th Annual Computer And Technology Law Institute, May 29-30, 2003, <http://www. gardere.com/Content/hubbard/tbl_s31Publications/FileUpload137/640/Estes_Spam.pdf>.

109 *See* Spam Laws: United States: State Laws, *at* <http://www.spamlaws.com/state/index.html> (visited Mar. 23, 2004).

110 Public L. No. 108-187, <http://thomas.loc.gov/cgi-bin/query/D?c108:6:./temp/~c108ztGml::>.

（unsolicited commercial electronic mail, UCE），也就是以從事商業廣告或推銷商品、服務爲主要目的之電子郵件，至於建立在既有交易關係上之電子郵件（例如產品之升級、進行中的服務），則排除在管制範圍之外。在管制手段上，垃圾電郵控制法採取所謂「選擇不接受」（opt-out）之模式，允許發信者得在未獲得許可之情形下寄送商業電郵，但當收件者表示不願繼續收到商業電郵時，寄件者即不得再寄發商業電郵。

爲降低收件者或 ISP 辨識商業電郵之成本，垃圾電郵控制法規定除非在事前已取得收件者的同意，寄件者必須於信件中清楚標示該信件係屬商業電郵。其次，爲尊重收件者的選擇權，使收件者有得以拒絕商業電郵寄送之途徑，該法案要求信件中必須具有使收件者「選擇不接受」之機制，包含寄件者有效之電郵地址，抑或其他得以讓收件者在網際網路上表示拒絕之機制，且此等「選擇不接受」之機制至少必須維持 30 日之有效性。該法案亦要求寄件者標示有效之實體郵遞地址，而寄送商業電郵者在收受收件者回絕之表示後，於 10 個工作日內必須將該位寄件者自收件名單中移除。該法案也要求具有猥褻或色情內容之商業電郵必須附加明確之警告標示，否則將受有刑事責任之追究。

爲進一步避免使用者必須對垃圾電郵逐一表示拒絕接受的麻煩，該法也授權美國聯邦貿易委員會（Federal Trade Commission, FTC）比照 2003 年剛成立的「請勿來電資料庫」（do-not-call registry），建置一個「拒收垃圾電郵資料庫」（do-not-spam registry）。針對違法的業者，垃圾電郵控制法授權 FTC、各級檢察官及 ISP 起訴追究各種民、刑事責任，但個別之電郵使用者則無此項權力。

目前美國各界對新法反應不一。支持者抱持樂觀之態度，認爲立法之成效雖仍有待觀察，至少是好的開始，然而部分反垃圾電郵團體批評該法案所採取「選擇不接受」之立法模式，使寄件者取得一次合法發送垃圾電郵的機會，將迫使收件者花費昂貴之成本裝設反垃圾電郵之各項裝置，以杜絕垃圾

電郵之騷擾[111]。最近已有數家大型的 ISP 依該法提起訴訟[112]，未來發展值得密切注意。

4.2.1.2 歐盟

「電子商務指令」（E-Commerce Directive）[113]是歐盟第一項直接適用於垃圾電郵之立法，該指令第 7 條課與寄件者對於 UCE 應予標示的義務。2003 年 10 月底生效的「隱私及電子通訊指令」[114]則採取更爲嚴格之「選擇接受」（opt-in）立法模式，要求會員國內之直銷業者在未經索取的情形下以自動撥話機、傳真機、電子郵件、簡訊傳送訊息時，必須事先徵得接收訊息者的明示同意。例外有二：第一，倘若從事商品、服務交易之自然人或法人係遵從歐盟「隱私保護指令」（Directive 95/45/EC）之規定自其顧客處取得電子聯絡管道，在取得者蒐集此等聯絡方式時，曾賦予顧客拒絕之機會，且顧客亦未拒絕將該聯絡管道提供使用的情形下，取得者得使用該聯絡方式推銷相似的商品或服務；第二，在收件者並非是自然人的情形下，該指令第 13 條第 5 款雖要求會員國保障非自然人用戶之利益，然而各會員國仍保有選擇採取「選擇拒絕」立法模式之權利，又該指令第 13 條第 4 款禁止寄件者隱藏或僞裝身分，亦要求寄件者提供日後可供收件者爲拒絕表示之有效地址。批評者認爲，垃圾電郵對於自然人及非自然人用戶所造成之困擾應屬相同，是以歐盟「隱私及電子通訊指令」對於非自然人用戶所開啓之例外，將使非自然人用戶遭受極大之損害。

111 *See, e.g.*, Coalition Against Unsolicited Commercial Email Press Release, Nov. 25, 2003, *at* <http://en2.wikipedia.org/wiki/Can_Spam_Act_of_2003> (visited Mar. 23, 2004).

112 *See* Jonathan Krim, *EarthLink, AOL Allege Spamming Networks*, WASH. POST, Feb. 19, 2004, at E01 <http://www.washingtonpost.com/wp-dyn/articles/A52951-2004Feb18.html>.

113 Council Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.

114 Council Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (*hereinafter* E-Privacy Directive).

4.2.1.3 澳洲

澳洲之「垃圾電郵法」（Spam Act 2003）[115]將於 2004 年 4 月 11 日生效，該法將所謂之垃圾電郵定位爲未經請求的商業電子訊息，包含未經請求之商業電郵、簡訊和其他電子訊息，且該等電子訊息必須與澳洲有所關聯，亦即，必須是在澳洲境內所發送，抑或自海外傳送至澳洲境內。「垃圾電郵法」採取「選擇接受」（opt-in）之立法模式，除非事先獲得接收訊息者之許可，不得傳送或唆使他人傳送商業電子訊息，而「許可」除包含收受訊息者之明示同意外，尚包含由收件者的行爲、寄件者與收件者間所存之商業或其他關係，而可合理推知收件者同意的情形。該法案要求所有商業電子訊息必須含有正確、清楚之寄件者資訊，且此等訊息至少必須維持自寄件日起算 30 日的有效期間，此外，尚要求所有商業電子訊息均含有可供收件者日後表示拒絕之機制。「垃圾電郵法案」亦禁止任何人提供、取得或使用專供在網頁上自動蒐集電郵地址的軟體，並禁止寄件者對以上開方式取得的名單寄送垃圾商業電子訊息。在立法之執行方面，「垃圾電郵法案」設有扣押、禁止發送的保全規定，並明訂民事損害賠償責任及刑事處罰規定。

4.2.1.4 日本

日本管制垃圾電郵之法律「特定電郵送信適正化法」（特定電子メールの送信の適正化等に関する法律）[116]於 2002 年 7 月 1 日生效，採取「選擇拒絕」（opt-out）的立法模式，將「特定電郵」定義爲未經受件者同意或索取，基於廣告目的而自行寄送的郵件，寄信者於寄送「特定電郵」時，必須標示該信件具有廣告之性質，以及寄件者之姓名、住所、寄送者寄信用的電郵地址暨收信用的電郵地址，再者，寄件者必須將收件者享有選擇拒絕權之事實告知收件者，倘若收件者已向寄件者爲拒絕之表示，寄件者日後即不得再對之寄送未經索取的廣告電郵，此外，當垃圾電郵已導致電信業者系統的

115 <http://scaleplus.law.gov.au/html/comact/11/6735/rtf/1292003.rtf> (accessed Mar. 23, 2004).

116 <http://www.soumu.go.jp/joho_tsusin/top/pdf/meiwaku_01.pdf> (accessed Mar. 23, 2004).

障礙時，電信業者有權拒絕傳送該等垃圾電郵。

4.2.1.5 跨國垃圾電郵之問題

以立法管制垃圾電郵面臨最大之挑戰爲跨國垃圾電郵之問題，由於網際網路無實體國界的特性，電子郵件之傳送不受限於傳統國界疆域，而各國對於垃圾電郵所持態度不一，多數國家尚未制訂管制垃圾電郵之法令，縱使在採取立法管制之國家中，立法的模式亦有寬嚴不一之別，濫發垃圾電郵者即可規避不利於自己之法令，縱使不論管轄權之問題，各國對於境外濫發垃圾電郵之人在實際上仍難以追究其責任，立法的執行顯有重大困難存在。

4.2.1.6 合憲性的疑慮

從美國州法之施行經驗，管制垃圾電郵立法可能遭遇合憲性之挑戰，在具體案件中，垃圾電郵寄件者經常提出之抗辯即爲此等立法已違反美國憲法之州際通商條款（Dormant Commerce Clause）以及第 1 增補條款（First Amendment）。前者涉及美國聯邦與州之間分權的界限，與他國人民關係不大。但有關言論自由的部分就值得注意。可以預期的是，未來「垃圾電郵控制法」亦可能受到美國憲法言論自由條款之挑戰。

美國國會於 1991 年間制訂「電話消費者保護法」（Telephone Consumer Protection Act of 1991），禁止使用電話傳真機、電腦或其它設備發送任何未經索取的廣告，部分行銷業者曾以「電話消費者保護法」違反美國憲法第 1 增補條款爲由提起訴訟。結果，加州之上訴法院在 Kaufman v. ACS Systems, Inc.[117]一案中判定「電話消費者保護法」並未違憲。另外，美國聯邦貿易委員會（Federal Trade Commission, FTC）於 2003 年間曾推動「請勿來電」登記資料庫（do-not-call registry），禁止業者在未經允許之情形下對已登記者進行電話行銷。一些電話行銷業者立即對 FTC 提起訴訟。初審的美國科羅拉州地方法院法官於 2003 年 9 月判決，認爲「請勿來電」之登記僅針對營利的行銷電話，而未提供國民拒絕接受非營利性組織來電的機會，此

117 Kaufman v. ACS Systems, Inc., Cal Ct App, July 22, 2003, 14 ILR (P&F) 514.

種差別待遇並無正當理由存在，侵害電話行銷公司之言論自由權，進而禁止上述「請勿來電」登記的進行。FTC 隨即提起上訴，第 10 巡迴上訴法院於一週後迅速裁定，廢棄下級法院的禁令，准許 FTC 繼續進行「請勿來電」之登記[118]，但該案的實體爭議目前仍未獲得最終之決定。在可預見之將來，倘若 FTC 依據「垃圾電郵控制法」建置「勿濫發郵件」（do-not-spam）的登記名冊，類似之爭議可能再度引發。

4.2.2 技術解決途徑

垃圾電郵逐漸成爲問題之初，多數使用者採用消極的「手動刪除法」對付，也就是自行把垃圾電郵刪除。反應比較激烈的，則使用「報復法」，回敬病毒或郵件炸彈（email bomb）——以程式自動產生的巨量電子郵件灌爆對方的系統——給作者。

最受看好的技術解決方式則是「過濾法」——設定過濾條件以自動刪除垃圾電郵。過濾的條件分兩大主流系統——針對內容或針對寄件者。前者主要是設定一些關鍵字——垃圾電郵裡經常出現而正常訊息少用者——來加以過濾，後者則依賴使用者自行建立的「黑名單」——垃圾電郵發信者名單資料庫。但業者很快就發展出迴避的方法，一方面經常變換發信人的姓名與電郵地址，另一方面爲其促銷訊息做更好的僞裝，增加關鍵字設定的困難。

經過長期的挫折，以寄件者爲封鎖對象的過濾系統近年來終於有了顯著的突破，也就是 MAPS 的發明。MAPS 是 Mail Abuse Protection System 的簡稱，也是新一代垃圾電郵過濾系統的始祖。有鑑於電郵地址雖能任意造假，IP 地址及電郵傳遞路徑卻不容易僞裝，MAPS 系統建立一組「黑洞名單」（blackhole lists）的資料庫，專門收錄垃圾電郵的發源地——包括垃圾電郵業者本身的網路節點以及主動或被動爲垃圾電郵業者提供服務的網路服務業者或郵件伺服器。此外，充份利用網際網路的互動性，MAPS 總部鼓勵一般

118 Caroline E. Mayer, *Court Says Do-Not-Call List Can Be Enforced*, WASH. POST, Oct. 8, 2003, at A01 <http://www.washingtonpost.com/wp-dyn/articles/A58828-2003Oct7.html>.

使用者提供所收到的垃圾電郵，經過自動化的處理，就可以在最短的時間更新黑洞名單，令黑洞名單的有效性大爲提高[119]。

MAPS 起初將黑洞名單提供給大眾免費使用[120]，不論是個人還是整個 ISP，都可以利用 MAPS 的黑洞名單來過濾垃圾電郵。然而，不同之組織對於「垃圾電郵」之定義並非一致，且黑名單亦可能封鎖合法之寄件者，從而對於解決垃圾電郵之成效上亦有其限制。

上述措施，不但未能有效增加垃圾電郵發信者之成本，甚至將防止接收垃圾電郵之成本轉由收件方或網際網路服務提供業者負擔，發信者之濫發行爲自不致有所改變，由於網際網路使用者及服務提供業者對於防堵垃圾電郵的挫敗經驗，要求政府以立法管制之呼聲逐漸升高。

4.2.3 最佳解決方式仍然待尋

我們必須承認，僅仰賴科技或立法管制之方式並無法使人們免於遭受垃圾電郵的侵襲，上開方式均各有其限制及困難，部分經濟學者試圖以市場機制解決問題，認爲關於寄送電子郵件的計價方式影響寄件者之行爲，價格將有助於寄件者衡量其寄送郵件之需求及願意付出之價格，亦有助於收件者瞭解閱讀信件之收益，依據目前網際網路服務提供業者採行之計價方式，對於寄件者而言，多寄出一封電子郵件之邊際成本幾乎趨近於零，部分研究顯示從量計價之方式應可解決垃圾電郵的問題，亦可將防堵垃圾電郵之難題由收件者移轉至寄件者[121]。

依上所述，解決垃圾電郵確屬不易之事，自從垃圾電郵之問題浮現後，電郵使用者、網際網路服務提供業者甚至各利益團體莫不致力於尋求解決之

119 *See generally,* David Post, *Of Blackholes and Decentralized Lawmaking in Cyberspace*, 2 VAND. J. ENT. L. & PRAC. 70 (2000).

120 MAPS 後來已改成收費制，但現在網路上有許多類似的免費服務。

121 *See, e.g.*, Robert E. Kraut, Shyam Sunder, Rahul Telang & James Morris, Working Paper, Pricing Electronic Mail to Solve the Problem of Spam, *at* <http://www.heinz.cmu.edu/~rtelang/Pricing%20Email.pdf> (accessed Mar. 23, 2004).

道，然而成效並無預期之顯著，當其他途徑均無法達成目標後，以立法管制之聲浪逐漸增高，目前有越來越多的國家相繼投入以立法管制垃圾電郵之行列，藉由民、刑事責任之課與，立法者期盼得以增加寄件者的成本，而改變其濫發商業電郵之行爲，以達到降低垃圾電郵之效果，實際成效如何，尚須進行持續的觀察，由於許多管制垃圾電郵之立法於 2004 年開始施行，因此未來之一、二年是觀察施行成果之絕佳時機。

5. 隱私權

近年對網際網路隱私權影響最重大的事件和網路並沒有太直接的關係，而是發生於 2001 年的 911 恐怖攻擊事件。911 改變了許多美國人對國家安全和個人自由的態度，而變得比以前樂意接受政府的情治監控。以對抗恐怖主義爲名，美國政府也不客氣地通過許多新的措施，其中有些和網路使用者的隱私權有密切的關係。除此之外，我們也將報導網路匿名性及國內個人資料保護法的最新發展。

5.1 情治監控與網路隱私權

5.1.1 911的震撼

911 發生前，情治監控已是網際網路上一個熱門話題。其中最顯著的事件乃 2000 年先後爆發的 Carnivore 事件和 Echelon 事件。前者指的是美國聯邦調查局（Federal Bureau of Investigation, FBI）所設計的一個封包檢視（packet sniffing）裝置，安裝在 ISP 的機房，過濾所有進出的訊息。經媒體報導後，引起軒然大波。美國許多知名 ISP 紛紛表示他們尚未安裝，也不會配合安裝[122]。美國國會立刻舉行聽證，進行調查[123]，FBI 則趕緊澄清該工具

122 *See, e.g.*, Vanessa Hua & Bob Egelko, AT&T Wins Appeal on Net Access, S.F. Exam., June 23, 2000, at B1 <http://www.sfgate.com/cgi-bin/article.cgi?file=/examiner/archive/2000/06/23/BUSINESS464.dtl>.

只是用來幫助他們進行合法的監聽[124]。

和 Carnivore 相較，Echelon 的規模與對個人隱私的影響更爲驚人。Carnivore 只是美國 FBI 的一個犯罪偵查工具，其使用必須遵守尚稱嚴謹的美國司法偵查程序。只因美國 ISP 所承載的網際網路通訊量在全世界無出其右，對許多外國資訊的流通而言——例如由台灣傳給歐洲的電子郵件，美國也是必經之地，所以其存在才會引起全球的矚目。相對的，Echelon 則是赤裸裸的情報蒐集系統。它的設置遍布全球各地，參與的國家包括美、英、澳等國家，只是至今美、英兩國尚拒絕承認其存在。據瞭解，Echelon 主要監聽的對象爲無線——包括地面及衛星——通訊，其存在已有相當時日，只是一直到 2000 年才被媒體發現而已[125]。

正當一般民眾及網友對情治監控感到憂心時，911 的發生改變了整個態勢。規模空前的恐怖攻擊，使許多先進國家的人民對國家安全的重要性有新的體會。一時之間，輿論和民意對國家進行情治監控的容忍度大爲提高。以美國爲首的許多西方國家紛紛基於國家安全的理由，加強對國內外的情報活動。

5.1.2 美國愛國者法

美國 2001 年的「愛國者法」（Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, USA PATRIOT Act），就是在這個背景下通過。雖然當時也有少數民權團體如 ACLU、EPIC 等提出警告，主張不應過度犧牲對基本人權的保障，但在當時的政治氣氛下，愛國者法的通過勢不可擋。

愛國者法對網路隱私權的影響，主要表現在執法機關與情治機關權限的

123 *See* D. Ian Hopper, *House Grills FBI on E-Mail Surveillance*, S.F. EXAM., July 25, 2000, at A6 <http://www.sfgate.com/cgi-bin/article.cgi?file=/examiner/archive/2000/07/25/NEWS13188.dtl>.

124 Donald M. Kerr, Congressional Statement on Carnivore Diagnostic Tool, <http://www.fbi.gov/congress/congress00/kerr090600.htm> (Sept. 6, 2000).

125 *See, e.g.*, Tom Zeller, *Cloak, Dagger, Echelon*, N.Y.TIMES, July 16, 2000 <http://www.nytimes.com/library/review/071600echelon-review.html>.

擴張。在 911 之前，美國聯邦對通訊監察主要有三個法律：

1. The Omnibus Crime Control and Safe Streets Act of 1968, Title III[126]：本法主要規範傳統意義的「監聽」（wiretap），也就是直接截取通訊的內容。因爲對當事人隱私權的影響最大，因此所要求的程序保障也最嚴格——必須要基於適當理由（probable cause）向法院申請核准方可。

2. The Electronic Communications Privacy Act（ECPA）[127]：這個 1986 年通過的法律，對所謂「位址紀錄器」（pen register 及 trap & trace devices）的使用設有特別規定，其所要求的程序較前述的監聽申請程序來得鬆，雖然仍得向法院申請核准，但不必有適當理由。換句話說，只要是由有權的執法人員申請，法院就一定要准。

3. The Foreign Intelligence Surveillance Act（FISA）[128]：1978 年通過，主要針對情報與反間。依本法，對「外國勢力」（foreign power）及其「代理人」的通訊監察行動，原則上只要司法部長的授權即可，程序上的要求鬆得多。

愛國者法並沒有對這個架構做根本性的更動。但它鬆動了有關通訊監察的許多程序上的安全瓣：

1. 擴大 FISA 的適用範圍：FISA 程序本來只能用在對外國勢力及其代理人的通訊監察行動，現在則可用來對付「內國恐怖份子」（domestic terrorists）。

2. 擴張位址紀錄器的適用範圍：ECPA 所謂的位址紀錄器，乃是針對傳統電話而設計，所得到的資訊相當於我們一般理解的雙向通話紀錄——打進與打出的時點與對方號碼。愛國者法將其擴大適用到網路通訊上，而且授權紀錄的資訊不僅限於來源地與目的地，尚包括路由（routing）和其他和訊息傳輸有關的資訊。簡單講，只要不是通訊的內容本身，都可以用 ECPA 的授

126 18 U.S.C. § 2510-2522.
127 18 U.S.C. § 2701.
128 50 U.S.C. § 1801-1811, 1841-1846.

權來加以蒐集[129]。

3. 放寬監聽的許可要件及其內容的公開要件：如前所述，在各種通訊監察的形式中，監聽屬於侵入性最高的，也因此傳統上需要最嚴格的授權程序。愛國者法爲監聽增加了一項合法要件，允許在發生「電腦入侵」（computer trespassing）的情形下，執法有關人員（agents acting under color of law）得在得到電腦主人的同意下，截取入侵者的通訊內容[130]。

4. 執法機關現在可以利用法院只做形式審查的證人傳票，向 ISP 請求更多的資訊。

5. 將「秘密搜索」（sneak-and-peak search）明文化並擴大其適用範圍：美國法院實務上原就允許在某些特定情形下，執法人員可以先搜索、後告知。愛國者法將其明文化，並對此種搜索令之核發要件給予較大的彈性。

5.1.3 歐盟的發展

相對於美國而言，歐盟一向較注重對隱私權的保護。歐盟於 2002 年通過隱私及電子通訊指令[131]，基本上仍然不脫過去幾個相關指令所建立的基調。但基於反恐勢力——特別是美國——的壓力，該指令特別允許（但不強迫）會員國立法規定電子資料的保存年限[132]。除此之外，歐盟和美國對於隱私權的保護程度仍存有許多岐異，內部各國意見也仍不一致。傳統上，戰後德國和法國對人民隱私權保護最力，但因 911 中某些恐怖份子曾在德國及其他歐盟國家內活動或募款，這些國家如今面臨必須加強對內情治監控的國內外壓力。

---

129 18 U.S.C. § 3121(c).

130 18 U.S.C. § 2511(2)(i).

131 E-Privacy Directive, *supra note* 114.

132 *Id*. art. 15(1). 該指令基本上是朝進一步強化隱私權保護的方向走。但歐盟有關隱私權的指令，一向比較集中在有關對抗企業對個人資料的不當利用，而少觸及國家情治活動的問題，本指令也不例外。

5.1.4 台灣

台灣於 1999 年通過通訊保障及監察法，將行之有年的監聽行爲法制化，但據瞭解，目前該法並沒有被用來對網際網路上的資訊截取之用。實務上乃是依一般的搜索扣押程序來取得網路有關資訊。

5.2 匿名性

網路世界有一個迷人的特色——匿名性。在許多場合，使用者可以放情高談闊論，而不必揭露真實身分。這樣的特性，是好是壞，迭有爭議。高度的匿名性與較低的言論責任是一體的兩面。躲在千奇百怪的代號背後，蓄意散發恐嚇、誹謗或各種不實言論的人，所在多有。另一方面，網路的匿名性的確有鼓勵發表的作用，許多社會邊緣人因此得以在網路上覓得知音並盡情宣洩。因此，自有網際網路以來，匿名言論究應予以容忍甚至鼓勵，還是應該加以壓抑甚至禁止，就成了爭執不休的話題。本文無力對此議題進行深入的分析與討論，但將介紹網路誹謗侵權訴訟當紅的被告——無名氏（John Doe），以最新的案例探討網路匿名言論的法律地位。

5.2.1 控告無名氏——新的法律策略

言論自由不代表不負言責，即令在對言論自由保護最徹底的美國，也是如此。如果涉及刑責——例如誹謗罪、妨害國家機密罪等，自有檢察官發動偵查。因檢察官得動用公權力來進行蒐證的工作，想要發現發言者的真實身分，自然比一般人容易得多。

但如果涉及民事責任，受害者想要主張權利的第一個難題，就是如何得知加害者的真實身分。早期的嘗試乃是改對 ISP 提起訴訟，要求 ISP 爲其使用者所發表的匿名言論負責。其立論的基礎是網際網路宛如大眾傳播媒體，ISP 扮演出版者的角色，應善盡言論過濾的工作。著名 ISP 如 Compuserve[133]

133 *See* Cubby Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1995).

和 Prodigy[134]等都曾因此遭到控告。但因這種主張和 ISP 的特性實不相符，對網路的發展也有負面的影響，因此法院的判決及後來的 CDA 皆排除了 ISP 這項過濾審查的責任[135]。

在最新的發展中，原告方改變策略，以對「無名氏」提起訴訟的方式，要求法院對該匿名者使用之網路供應商（ISP）發出「證人傳票」（sub-poena duces tecum），強制 ISP 揭露該匿名者之真實身分。典型的案例如 1998 年，HealthSouth 公司對 Krum 的訴訟[136]中，該公司控告一位在 Yahoo 的財經討論版上發表不利言論的無名氏，後來藉由法院發出證人傳票得知被告之真實身分爲 Peter Krum。諸如此類的法律訴訟策略之後大量的出現[137]。

令人玩味的是，這類型案件的原告，在提出這些訴訟時，往往不以得到巨額的賠償金爲其主要目的。因爲其所控訴的無名氏，往往只是不具資力的一般民眾，甚至只是毫無能力負擔任何賠償的年輕電腦網路使用者[138]。這種民事訴訟行動多半僅是象徵性的動作，以嚇阻類似事件的持續發生爲主要目的[139]。有的時候，原告的目的只是在找出公司內部的「爆料者」（whistle blower），以便加以懲處。因此，有人以 CyberSLAPP（SLAPP, strategic litigation against public participation）稱呼此類案件。

基於這樣的發展，一些人權團體開始關注此類案件的發展，以免言論自由受到不當的壓抑。美國法院也嘗試要建立一套平衡的檢驗標準，來決定是

134 *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL323710 (NY Sup. Ct. May 24, 1995).

135 47 U.S.C. § 230 (Supp. III 1999).

136 *See* Complaint, HeathSouth Corp. v. Krum, No. 98-2812 (Pa. C.P. Centre County, filed Oct. 28, 1998).

137 *See* Lyrissa Barnet Lindsky, *Silencing John Doe: Defamation and discourse in cyberspace*, 49 DUKE L.J. 855, 859 (2000); *See also* EFF, Cyberslapp/John Doe Cases, *at* <www.eff.org/Privacy/Anonymity/#cases> (visited Mar. 23, 2004).

138 *See* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability as Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1645 (1995).

139 *See* Lyrissa Barnet Lindsky, *supra note* 137, at 860.

否要揭露網路匿名言論發表者的真實身分。在 2001 年的 Doe v. 2TheMart.com, Inc.[140]一案中，承審的華盛頓州西區聯邦地院發展出四個檢視原則：1.原告之請求是否基於誠信（good faith）而無不當之企圖；2.匿名者身分是否與核心爭點有關；3.匿名者身分是否爲原告主張直接相關且必要的資訊（directly and materialy）；4.是否有其他資源可得到此必要資訊[141]。在同年的 Dendrite International, Inc. v. Doe 一案[142]中，法院更進一步的要求，原告必須針對每一個匿名言論者明白列舉其認爲有傷害部分，並確實盡力通知被告揭示身分的請求，同時必須給予其合理的機會反對這項請求。

5.2.2 網路匿名權的立法保護

爲了避免針對網路匿名言論作策略性訴訟的風氣日益蓬勃，除了法院的判例之外，立法權也逐漸重視相關的立法措施，以保護廣大的網路使用者。

加州率先於 1992 年通過「反 SLAPP 法」，被告方只要證明其言論與公共事務相關，或原告無充份之證據證明其主張有成立之可能性，即可對抗原告揭示身分之請求[143]。在 Global Telemedia International, Inc. v. Doe 一案[144]中，法院首度將本法之保護範圍延伸到網路匿名案件。原告雖然主張被告言論乃對其商譽毀損，無關公眾利益，但法院認定反 SLAPP 法應擴充適用至商業事件相關言論的保護，同時，大企業如 GTMI 之行爲也屬於公共利益的一部分。這項延伸是網路匿名保護的一大里程碑[145]。目前，除了加州之外，

140 *See* Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088 (W.D. Wash., 2001).

141 *Id*. at 1095.

142 *See* Dendrite Intern., Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

143 *See* Cal. Civ. Proc. Code §425.16(b)(1) (West Supp. 2001).

144 *See* Global Telemedia International, Inc. v. Doe, 132 F. Supp. 2d 1261 (C.D. Cal. 2001).

145 *See* Margo E. K. Reder & Christine Neylon O'Brien, *Corprate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking the Identity Ofanonymous Empolyee Internet Posters*, 8 MICH. TELCOMM. & TECH. L. REV. 195, 202-204 (2002), *available at* <http://www.mttlr.org/voleight/Reder.pdf >.

另有 16 州有相似的立法，另有許多州有類似的立法計畫[146]。

在 2003 年 6 月，加州眾議院通過了 1143 號法案[147]。這項法案由 EFF 推動，加大柏克萊分校法學院學生起草的法案[148]，主要是針對加州的民事訴訟法進行修正，最主要的目的是：增加了接到證人傳票的匿名發表者提出反證，進行防禦的時間；同時將加州的判例法成文化，使法院在相關案件時，必須要仔細審查匿名者的憲法權利。目前該法案正在加州參議院審議之中。

5.2.3 DMCA與網路匿名權的衝突

由於在企圖打擊新一代 P2P 軟體一事上屢遭挫敗，RIAA 於 2002 年中開始採取新的策略——對利用 P2P 網路分享具著作權之音樂檔案的使用者進行法律追訴。經過一年多的準備，RIAA 於 2003 年 9 月發動第一波攻勢，對 261 位個人網路用戶提出告訴，後續行動仍在持續進行中。

RIAA 透過軟體搜尋，找出在 P2P 網路上分享盜版音樂檔案的使用者，記錄其在 P2P 軟體中的使用者帳號及 IP 位址，再透過如 ARIN 之類的軟體查出該 IP 位址的擁有者，並據以向法院聲請對彼等——ISP、大學、公司等——發出證人傳票，要求提供該使用者之真實身分。RIAA 此舉的法律依據是 DMCA 一廣受爭議的條款——侵權者身分揭露請求傳票（Subpoena to Identify Infringer）[149]。和前面 5.2.1 所提到的證人傳票不同，此處傳票申請者連向「無名氏」提起訴訟都不必，只須依同條第(c)款的規定，向 ISP 發出

146 這是 2001 年的資料，包括 Colorado、Delaware、New York、Massachusett 等州；*See* Richard Raysman & Peter Brown, *Discovering the Identity of Anonymous Internet Posters*, N.Y.L.J., Sept. 11, 2001, <http://cyber.law.harvard.edu/stjohns/anon-net.html>; *see also* Margo E. K. Reder & Christine Neylon O'Brien, *supra note* 145, at 204.

147 California Assembly Bill 1143, <http://www.leginfo.ca.gov/cgi-bin/postquery?bill_ number=ab_1143&sess=CUR> (visited Mar. 23, 2004).

148 Janet Gilmore, Law students draft Internet privacy bill, *at* <http://www.berkeley.edu/news/media/releases/2003/05/05_privacy.shtml> (press release May 5, 2003).

149 17 U.S.C. § 512(h).

侵權通知，並給法院一份宣誓書（sworn declaration），保證該傳票的目的僅只爲了取得侵權者的真實身分，且僅只作爲保護著作權之用[150]。RIAA 主張這類聲請僅爲法院行政程序，無須提出證據證明該請求支持其本案的實體主張，亦無須通知使用者該聲請的存在或給予反對之機會，更不須法官對匿名者之憲法權利作檢視[151]。

目前已有部分 ISP 選擇公開其用戶之身分，但亦有許多 ISP 要求法院撤銷這類證人傳票的效力[152]，其中最受注目的是 RIAA v. Verizon Internet[153]案。經過一年多的纏訟，哥倫比亞特區巡迴上訴法院於 2003 年底裁定，贊同被告 Verizon 的立場，認爲第 512 條第(h)款所規定的傳票，只能用於同條第(b)至(d)款的 ISP，也就是只有當 ISP 本身的伺服器上有其使用者所存放的侵權物件時，方得請求。在 P2P 的情形，所分享的檔案縱使有侵害著作權的嫌疑，因並未利用 ISP 的伺服器存放檔案，ISP 純粹扮演通道（conduit）的角色，因此沒有第 512 條第(h)款適用的餘地[154]。對於發展，RIAA 計畫以對無名氏提出控訴的方法作爲其下一步的法律手段。希望在訴訟繫屬之後，能以進一步的證據，由法院發出證人傳票，達到揭示該使用者身分之目的，同時對他進行侵權告訴。

6. 網路犯罪

講到網路犯罪，近年來最令人頭痛的大概非病毒和駭客攻擊莫屬。以下將介紹各國最新的相關立法與案例。

---

150 *Id*.

151 *See* Defendant Jane Doe's Motion to Quash at 1, RIAA v. Boston College (D. Mass. 2003) (Misc. Act. No. 1:03-MC-10210-JLT), <http://www.eff.org/IP/P2P/20030926_jane_doe.pdf> (accessed Mar. 23, 2004).

152 *See generally*, EFF, RIAA v. The People, *at* <http://www.eff.org/IP/P2P/riaa-v-thepeople.php> (visited Mar. 23, 2004).

153 351 F.3d 1229 (DC. C. 2003).

154 *Id*.

6.1 各國立法例

6.1.1 美國

美國聯邦刑法和州法對於利用網路傳送電腦病毒，或不正入侵、損害政府機關之電腦、網站等行爲，皆已列爲處罰對象。自 1978 年起美國佛羅里達州即通過「佛羅里達州電腦犯罪法」，隨後其他各州亦紛紛相繼頒布該州之電腦犯罪法。聯邦法案中，最重要的是 1984 年頒布的「電腦詐欺和濫用法」（Computer Fraud and Abuse Act, CFAA）。該法頒布之初，僅將聯邦政府電腦內及金融機構內之資訊列爲保護客體。美國國會於 1986 年修改並擴張保護客體爲「與聯邦利益有關之電腦」（federal interest computer）。於 1996 年再次修正時，保護客體再次修正爲「受保護之電腦」（protected computer）之概念，涵蓋範圍擴大及於所有與州際或國際商務有關之電腦系統[155]。該法案內容後被納入美國聯邦法典 18 USC §1030。

CFAA 對於非法入侵設有 5,000 美元的損失下限。單一入侵事件所造成的損失如果低於此下限，則不構成犯罪。這個下限的設置，一方面是本於微罪不舉的精神，一方面則是避免有限的執法資源浪費在輕微的入侵事件上。經過數次修正之後，CFAA 的保護對象幾乎已涵蓋所有美國境內的電腦，如果沒有這項下限，那麼許多單純的惡作劇也將構成犯罪，顯然失之過苛。但該下限也造成法律適用上的困難。因爲該法並未清楚定義何種花費屬於該條所謂的「損失」。愛國者法即針對此點加以釐清，舉凡損害鑑定、系統或資料重建等費用，以及營業上的損失等，都可列入該條所謂的損失。如果有多部電腦同時受到攻擊，其所受損失還可以相加。此舉等於大幅擴張 CFAA 的打擊範圍。

愛國者法也再度擴大保護對象至外國的電腦。換句話說，如果美國的駭

155 Edmund B. (Peter) Burke, *The Expanding Importance of The Computer Fraud and Abuse Act*, GIGALAW Jan. 2001, *at* <http://www.gigalaw.com/articles/2001-all/burke-2001-01-all.html>.

客入侵它國的電腦，也有可能受 CFAA 的制裁。有疑問的是，如果是外國的駭客繞道美國的設備入侵外國的電腦，是否也有該法的適用[156]。

6.1.2 歐洲網路犯罪防制公約

歐洲理事會（Council of Europe）於 2001 年 11 月 8 日經第 106 屆部長會議通過「網路犯罪防制公約」（Convention on Cybercrime）[157]，並自同月 23 日起開放簽署。由於該公約經過長達 4 年的草擬協商階段，又是全球第一個有關網路犯罪的公約，簽約國除了歐洲理事會的會員外，還包括了美、日等重量級的網際網路大國，因此備受矚目。但因公約規定必須有 5 個以上的國家——包括至少 3 個歐洲理事會的會員國——批准，才開始生效。因此，一直等到 2004 年 3 月，立陶宛國會批准之後，該公約才正式於同年 7 月 1 日起對已批准的國家——阿爾巴尼亞、克羅埃西亞、愛約尼亞、匈牙利和立陶宛——生效。

基本上，網路犯罪公約主要在將網路犯罪做初步的類型化，並就各類型提供基本的構成要件與最低的保護標準[158]：1.侵害電腦資料及系統之秘密性（confidentiality）、完整性（integrity）及可利用性（availability）之犯罪[159]；2.與電腦相關之犯罪（computer-related offences）[160]；3.與內容相關

156 Bill Reilly, *The Impact of the USA Patriot Act on Network Security Practice*, J. INTERNET L., Mar. 2002, at 1, <http://packetstormsecurity.nl/papers/legal/patriot.doc> (accessed Mar. 23, 2004).

157 Convention on Cybercrime, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=&CL=ENG> (visited Mar. 23, 2004).

158 馮震宇，〈網路犯罪與網路犯罪條約（上）（下）〉，《APIPA 智權情報網》（2002.7.31.）<http://www.apipa.org.tw/Article/Article-ViewADA.asp?intADAArticleID=88&strSortTarget=adaCreateDate>。

159 包括非法接觸（illegal access）、非法截取（illegal interception）、資訊干擾（data interference）、系統干擾（system interference）及設備濫用（misuse of devices）；Cybercrime Convention art. 2-6.

160 包括與電腦相關之偽造（forgery）及詐欺（fraud）；*Id.* art. 7-8.

之犯罪 （content-related offences）[161]；4.關於侵害著作權及著作鄰接權之犯罪（offences related to infringements of copyright and related rights）[162]。

6.1.3 台灣

過去我國刑法並未對電腦上所做儲存的資料加以定位，因此對於僞造、變造、毀損或竊盜他人電腦中資料之行爲皆無法可適用。於 1997 年 9 月刑法修正時，於第 220 條第 2 項規定「文書」亦包括「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，足以爲表示其用意之證明者」，正式將電磁紀錄列入準文書之範圍。從此，凡侵入他人電腦系統篡改毀損資料，致生損害於他人的行爲，即可依刑法第 352 條「毀損文書罪」論處。

該次修正固然大致上解決了以電磁紀錄爲犯罪客體的傳統犯罪，但對於以電腦或網路本身爲攻擊對象之行爲，則仍未加以規範。以病毒攻擊爲例，如因此造成資料的毀損，固然處罰有據，但若只是單純地令電腦當機而未對資料造成影響，就有爭議。網際網路上令人頭痛的駭客攻擊行爲，是否應加以處罰？若是，又應以何爲據？也是爭執不休的問題。鑑於此類案件日益頻繁，造成個人生活上之損失益趨擴大，立法院終於 2003 年 6 月於刑法新增妨害電腦使用罪專章，以規範電腦犯罪行爲及保護之對象[163]。依新法，舉凡無故入侵他人電腦，或無故干擾他人電腦或相關設備（如網路設備）致生損害者，最高可換來三年的牢獄之災[164]，駭客攻擊行爲不再無法可罰。

新法亦新增「破壞電磁紀錄罪」[165]，以處罰「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」之行爲。曾經

161 *Id*. art. 9.
162 *Id*. art. 10.
163 刑法第 36 章「妨害電腦使用罪」。
164 刑法第 358、360 條。
165 刑法第 359 條。

轟動一時的「天幣竊盜」案，即遭法院依本條定罪[166]。此外，針對電腦病毒等惡意之電腦程式，程式撰寫者與使用者可能不同之情形，新法也增訂「製作專供電腦犯罪之程式罪」[167]，以處罰此類程式的撰寫者。除非犯罪的客體是公務機關之電腦或相關設備，或犯前述之「製作專供電腦犯罪之程式罪」，否則本章之犯罪屬告訴乃論，以節省國家有限之偵查及司法資源[168]。

經由此次修正，我國在電腦犯罪方面的實體規定，確已符合國際趨勢。相形之下，我國對於執法機關的蒐證權限規範卻仍相當模糊。爲兼顧犯罪偵查、人民通訊自由及隱私的不同需求，參考網路犯罪防制公約，在程序法的層次做更仔細的規範，對於網路上各類證據加以定義、分類，並建立更明確的蒐證程序，可能是未來可以思考的方向[169]。

6.2 替代途徑——從結構面著手

電腦程式碼中永遠有臭蟲，無法完美的除錯即會引發安全漏洞。欲避免被駭客攻擊的關鍵，首重資訊安全與自我防衛的本領。提昇個人的安全觀念加強自我防衛意識、研訂安全的預防策略，以及研發安全防範軟體以強化資訊系統的安全性，是目前各國正積極提昇網路安全的做法。以我國爲例，行政院於 2001 年通過「建立我國通資訊基礎建設安全機制計畫」[170]，設立國內資訊安全專責機構「國家資通安全會報」[171]，下設「國家資通安全應變中心」、「技術服務中心」及數個工作組，包括「網路犯罪工作組」，希望多

166 台北地方法院 92 年簡字第 3842 號判決。

167 刑法第 362 條。

168 刑法第 363 條。

169 吳兆琰，〈新興網路犯罪法制議題分析及因應——以歐洲理事會「網路犯罪防制公約」為中心〉，《資策會科技法律透析》，頁 48（2003）。

170 建立我國通資訊基礎建設安全機制計畫，<http://www.moj.gov.tw/chinese/c_rule_sys_point0-3.aspx> (visited Mar. 23, 2004).

171 國家資通安全會報，*at* <http://www.nicst.nat.gov.tw/group/application/nics/index.php> (visited Mar. 23, 2004).

管齊下，以維護國家資通訊安全。

除了加強系統管理者及網路使用者對安全防衛的重視外，Katyal 教授則建議從環境面著手，某個程度重建現實世界的四個自然防護架構——自然監視（Natural Surveillance）、私有領域（Territoriality）、建立社群（Building Communities）與目標保護（Target Protection）[172]。在現實世界中，人眼所及之處就是一種自然的防護；私人財產制有助劃清人我界限與「入侵」的起點；群聚生活可以發揮鄰里間守望相助的效果；有時候私人也會針對特別的安全弱點採取特別保護措施——如鐵窗。這些有意無意的措施或社會結構都有防制犯罪的效果。

在網路世界也是如此。例如，開放原始碼的電腦軟體可以藉許多人的眼睛共同找安全漏洞。但網際網路的開放性也會吸引侵入者與犯罪。因此，在某些領域，適當的建立身分認證及網路門禁可能可以發揮如現實世界中地界與社群的犯罪防制效果[173]。Katyal 也特別指出，系統管理者及網路使用者的角色固然重要，許多官方的電腦犯罪防制計畫也不斷宣導防火牆等機制的必要性，但過猶不及，太嚴格的目標保護措施，會像太多鐵窗一般，有時會造成反效果。有效的法律與有力的執法，將有助於減少網路鐵窗的副作用[174]。

7. 尚難評估的社會衝擊——代結論

網際網路是個年輕的科技，它對社會的影響，顯然需要更長時間的觀察才有辦法論斷。我們在此只是整理幾個重要的討論，提供關心網路社會發展的各界先進一些思考的角度。

首先是關於「全球化」（globalization）。不論如何定義，全球化正在發生之中是個不爭的事實，現代資通訊科技——尤其是網際網路——對其發

172 Neal Kumar Katyal, *Digital Architecture As Crime Control*, 112 Yale L.J. 2261, 2262 (2003).

173 *Id*. at 2268-2279.

174 *Id*. at 2280.

生扮演重要的推手角色，也是不爭的事實。有問題的是，這個全球化的世界將建在何種架構之上？這樣的社會結構，又是讓誰得利？隨著網際網路逐漸融入我們日常生活的一部分，網路世界和實體世界的分野將越來越模糊，網路法與「一般法」的界限可能會逐漸淡化，而網路法所帶給我們的重要啓示——特別是社會架構與社會控制之間的關係——則可能滲入到其他的法學領域中。

如 Friedman 教授所說，我們常用「地球村」這個名詞來形容今天全球化的世界，其實是有一點誤導作用，因爲今天的地球，和「村」一點都不像。交通的距離可能拉近了，訊息傳遞的速度可能變快了，但這個世界可不點也沒有傳統村莊的小巧與單純[175]。在這個超級複雜的聚落裡，網際網路究竟會塑造什麼樣的人際關係，則是值得仔細觀察的。悲觀者如 Sunstein 教授，即提出「網際網路可能造成群體極化」的隱憂[176]。所謂「群體極化」（group polarization），指某種團體內的成員，最初的思考形態與觀念上具有的某個特定傾向，在經過團體內的討論與意見交流後，其觀念逐漸朝著原本傾向的方向繼續強化，變得愈來愈確信與堅持，最後形成極端的觀點。舉例來說，假設一個原本觀念上有些許種族歧視傾向的人，置身於一個相同觀點的團體中，經過與其他成員的討論及相互肯定，最初輕微的種族歧視傾向，在團體內可能逐漸形成一種極端的確信與堅持，甚至將之視爲真理。

Sunstein 教授指出，民主的真諦在討論（deliberation），而有意義的討論應避免只有單一觀點的交流，以免自我盲目與偏頗。然而，近來由於傳播選擇遽增，產生了資訊超載的現象——太多選擇、太多話題、太多觀點，使得「資訊過濾」（information-filtering）成爲必要的手段。網際網路讓資訊過濾更容易，但可能太容易了，而導致一個危機，就是很多人可能不自覺地就讓自己被全然同質的觀點所包圍，變得主觀，也毫無機會去修正、調整自

175 Lawrence M. Friedman, *Erewhon: The Coming Global Legal Order*, 37 STAN. J. INT'L L. 347, 364 (2001).

176 CASS R. SUNSTEIN, REPUBLIC.COM, 51-88 (2002).

己所持的立場[177]。而網路世界裡結社的方便性，使得這種現象更容易從個人層次提昇至團體層次，而形成群體極化。他以種族岐視組織近年來利用網際網路大幅擴張組織爲例，說明這種顧慮並非杞人憂天。

知名作家 Brin 則提出另一個有意思的理論。他指出科技（不只是網際網路）正在把我們的社會往透明化的方向推進——不論我們喜歡與否。和個人有關的資訊正在快速累積與傳播之中，這是無法抵擋的趨勢。Brin 主張這是好事，也和網際網路透明開放的精神相符。與其因隱私權的顧慮而阻止別人蒐集你的資料，不如反過來鼓勵（或至少容許）大家互相蒐集資料。因此社會越透明，每個人就更需要爲自己的言行負責，豈不美哉[178]？

對此，Lessig 有一個發人深省的回應[179]。Lessig 指出，所謂「責任」（accountability）是相對於社會規範（social norms）而言。只有當我們對一個特定社會的規範有信心的時候，責任才是一件美事。如果我們同時在許多不同的社會（社群）中生活，所謂的責任往往成爲強勢社群將其價值觀強加在別的社群身上的藉口。

從一個「特別報導」的角度，我們很慶幸不必在此對這些論戰判斷是非。如果大家覺得這些討論有點意思，我們的目的就達到了。

參考文獻

英文書籍

BRIN, DAVID, TRANSPARENT SOCIETY (1998).

ESTES, DAWN & PARMAR, BHAVEENI, SPAM, SPAM AND MORE SPAM 7, Paper for 16th Annual Computer And Technology Law Institute, May 29-30, 2003 <http://www.gardere.com/

177 *Id*. at 56-57.

178 *See*, DAVID BRIN, TRANSPARENT SOCIETY (1998).

179 Lessig 其實有兩個回應，此處只介紹其中一個。*See* Lessig, *supra note* 11, at 153.

Content/hubbard/tbl_s31Publications/FileUpload137/640/Estes_Spam.pdf>.

FEDERAL TRADE COMMISSION, TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY (2003), <http://www.ftc.gov/os/2003/10/innovationrpt.pdf> (accessed Mar. 23, 2004).

INTERCHANGE OF DATA BETWEEN ADMINISTRATIONS, THE IDA OPEN SOURCE MIGRATION GUIDELINES, <http://europa.eu.int/ISPO/ida/export/files/en/1618.pdf> (Nov. 8, 2003).

LESSIG, LAWRENCE, CODE AND OTHER LAWS OF CYBERSPACE (1999).

_____, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001).

MACKINNON, CATHARINE A., FEMINISM UNMODIFIED: DISCOURSES ON LIFE AND LAW (1987).

PEW INTERNET PROJECT, SPAM: HOW IT IS HURTING EMAIL AND DEGRADING LIFE ON THE INTERNET, (2003), <http://www.pewinternet.org/reports/toc.asp?Report=102>.

SUNSTEIN, CASS R., REPUBLIC.COM (2002).

VAIDHYANATHAN, SIVA, COPYRIGHTS AND COPYWRONGS (2003).

中文論文

吳兆琰，〈新興網路犯罪法制議題分析及因應——以歐洲理事會「網路犯罪防制公約」爲中心〉，《資策會科技法律透析》，頁 48（2003）。

馮震宇，〈網路犯罪與網路犯罪條約（上）（下），《APIPA 智權情報網》（2002.7.31.）<http://www.apipa.org.tw/Article/Article-ViewADA.asp?intADAarticleID=88&strSortTarget=adaCreateDate>。

英文論文

Branscomb, Anne Wells, *Anonymity, Autonomy, and Accountability as Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1995).

Burk, Dan L. & Cohen, Julie E., *Fair Use Infrastructure For Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001).

Burk, Dan L. & Lemley, Mark A., *Is Patent Law Technology-Specific?*, 17 BERKELEY TECH. L.J. 1155 (2002).

Burke, Edmund B. (Peter), *The Expanding Importance of The Computer Fraud and Abuse Act*,

Gigalaw Article, Jan. 2001, <http://www.gigalaw.com/articles/2001-all/burke-2001-01-all.html>.

Carrie Kirby, *RIAA Goes After 532 Unnamed File Sharers*, SAN FRAN. CHRON., Jan. 22, 2004, at B-1, <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/01/22/BUGJD4EP2O1.DTL>.

Cohen, Julie E., *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. Rev. 981 (1996).

Dreazen, Yochi J., *Russian Company Passes First Test Of Copyright Law*, WALL ST. J., Dec. 18, 2002, at B4.

Esler, Brian W., *Protecting the Protection: A Trans-Atlantic Analysis of the Emerging Right to Technological Self-Help*, 43 IDEA 553 (2003).

Evangelista, Benny, *The Music Revolution Has Arrived: Itunes, Napster 2.0 Make Downloading Songs Easy and Legal*, SAN FRAN. CHRON., Feb. 8, 2004, at E-1, <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/10/20/BUGJG2E8IF1.DTL>.

Fisher, William & Yang, Christopher, Peer-to-Peer Copying, <http://cyber.law.harvard.edu/ilaw/P2P.html> (Nov. 18, 2001).

Friedman, Lawrence M., *Erewhon: The Coming Global Legal Order*, 37 STAN. J. INT'L L. 347 (2001).

Gilmore, Janet, Law students draft Internet privacy bill, *at* <http://www.berkeley.edu/news/media/releases/2003/05/05_privacy.shtml> (press release May 5, 2003).

Goldsmith, Jack L., *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

Hopper, D. Ian, *House Grills FBI on E-Mail Surveillance*, S.F. EXAM., July 25, 2000, at A6 <http://www.sfgate.com/cgi-bin/article.cgi?file=/examiner/archive/2000/07/25/NEWS13188.dtl>.

Hua, Vanessa & Egelko, Bob, *AT&T Wins Appeal on Net Access*, S.F. EXAM., June 23, 2000, at B1<http://www.sfgate.com/cgi-bin/article.cgi?file=/examiner/archive/2000/06/23/BUSINESS464.dtl>.

Johnson, David R. & Post, David G., *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

Katyal, Neal Kumar, *Digital Architecture As Crime Control*, 112 YALE L.J. 2261 (2003).

Kerr, Donald M., Congressional Statement on Carnivore Diagnostic Tool, <http://www.fbi.gov/

congress/congress00/kerr090600.htm> (Sept. 6, 2000).

Kraut, Robert E., Sunder, Shyam, Telang, Rahul & Morris, James, Working Paper, Pricing Electronic Mail to Solve the Problem of Spam, *at* <http://www.heinz.cmu.edu/~rtelang/Pricing%20Email.pdf>.

Krim, Jonathan, *EarthLink, AOL Allege Spamming Network*s, WASH. POST, Feb. 19, 2004, at E01.

Litman, Jessica, *The DNS Wars: Trademarks And The Internet Domain Name System*, 4 J. SMALL & EMERGING BUS. L. 149 (2000).

Lohr, Steve, *Microsoft Said to Encourage Big Investment in SCO Group*, N.Y. TIMES, Mar. 12, 2004, at C5, <http://www.nytimes.com/2004/03/12/technology/12soft.html>.

Lyrissa Barnet Lindsky, *Silencing John Doe: Defamation and discourse in cyberspace*, 49 DUKE L.J. 855 (2000).

Mayer, Caroline E., *Court Says Do-Not-Call List Can Be Enforced*, WASH. POST, Oct. 8, 2003, at A01 <http://www.washingtonpost.com/wp-dyn/articles/A58828-2003Oct7.html>.

Merges, Robert Patrick & Reynolds, Glenn Harlan, *The Proper Scope of the Copyright and Patent Power*, 37 HARV. J. LEGIS. 45 (2000).

Nadan, Christian H., *Open Source Licensing: Virus or Virtue?*, 10 TEX. INTELL. PROP. L.J. 349 (2002).

Post, David, *Of Blackholes and Decentralized Lawmaking in Cyberspace*, 2 VAND. J. ENT. L. & PRAC. 70 (2000).

Poulsen, Kevin, Linux Kernel Backdoor Blocked, *at* <http://www.theregister.co.uk/content/55/33855.html> (posted Nov. 7, 2003).

Raymond, Eric Steven, Release Early, Release Often, a section in his online treatise The Cathedral and the Bazaar, Revision 1.57, *at* <http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ar01s04.html> (Sept. 11, 2000).

Raysman, Richard & Brown, Peter, *Discovering the Identity of Anonymous Internet Posters*, N.Y.L.J., Sept. 11, 2001 <http://cyber.law.harvard.edu/stjohns/anon-net.html>.

Reder, Margo E. K. & O'Brien, Christine Neylon, *Corprate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking the Identity Ofanonymous Empolyee Internet Posters*, 8 MICH. TELCOMM. & TECH. L. REV. 195 (2002), *available at* <http://www.mttlr.org/ volleight/Reder.pdf>.

Reilly, Bill, *The Impact of the USA Patriot Act on Network Security Practice*, J. Internet L., Mar. 2002, at 1 <http://packetstormsecurity.nl/papers/legal/patriot.doc>.

Samuelson, Pamela, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999), <http://www.sims.berkeley.edu/~pam/papers/Samuelson_IP_dig_eco_htm.htm>.

Zeller, Tom, *Cloak, Dagger, Echelon*, N.Y. TIMES, July 16, 2000 <http://www.nytimes.com/library/review/071600echelon-review.html>.

其他

Creative Commons, *at* <http://creativecommons.org/> (visited Mar. 23, 2004).

eCos, *at* <http://sources.redhat.com/ecos/> (visited Mar. 23, 2004).

EFF, Cyberslapp / John Doe Cases, *at* <www.eff.org/Privacy/Anonymity/#cases> (visited Jan. 20, 2004).

EFF, EFF "Intellectual Property: Digital Millennium Copyright Act (DMCA): U.S. v. Elcom-Soft & Sklyarov" Archive, *at* <http://www.eff.org/IP/DMCA/US_v_Elcomsoft/> (updated Mar. 13, 2003).

EFF, Felten v. RIAA, *at* <http://www.eff.org/IP/DMCA/Felten_v_RIAA/> (visited Jan. 20, 2004).

EFF, RIAA v. The People, *at* <http://www.eff.org/IP/P2P/riaa-v-thepeople.php> (visited Mar. 23, 2004).

GNU, Frequently Asked Questions about the GNU GPL, *at* <http://www.gnu.org/licenses/gpl-faq.html> (updated Feb. 26, 2004).

Open Source Initiative, The Open Source Definition, version 1.9 <http://opensource.org/docs/definition.php> (visited Mar. 2, 2004).

Spam Laws, *at* <http://www.spamlaws.com/state/index.html> (visited Mar. 23, 2004).

台灣正體中文 iCommons 討論網站，*at* <http://www.openfoundry.org/icommons/> (visited Nov. 29, 2003).

自由軟體入口網站，*at* <http://www.oss.org.tw> (visited Mar. 23, 2004).

國家資通安全會報，*at* <http://www.nicst.nat.gov.tw/group/application/nics/index.php> (visited Mar. 23, 2004).