行政院所屬各機關因公出國報告
（出國類別：九十一年度公務人員出國專題研究）

刑法妨害電腦使用罪章之立法研究

服務機關：法務部
出國人職稱：檢察官
姓名：葉奇鑫
出國地區：美國
出國期間：九十一年五月二十四日至九十一年十一月二十三日
報告日期：九十二年十月三十日

自　序

民國九十一年是我人生中一個重要的轉戾點。

這一年，我很榮幸被法務部推薦參加人事行政局公務人員出國專題研究甄試，而且很僥倖地，順利通過了英語能力測驗，獲得許多公務員夢寐以求的機會：公費出國進修半年。

放榜後的第一個煩惱，是究竟要出國當「學生」？還是當「訪問學者」？當學生最大的好處是：有教授鞭策，讀書不會偷懶，學問底子可以從基礎打起；缺點則是：美國學費高，必須自己補貼學費（人事行政局補助款爲五千五百美金，筆者因此自己吸收了約七千美金之學費差額），另外，半年內不可能拿到學位，如果在乎學位，將來還必須想辦法再到美國進修一次。相反的，當訪問學者的好處則是沒有繁重的課業壓力，可以專心研究自己有興趣之主題，回國後也不必考慮是否要再到美國拿學位的問題，缺點則是：如果自制力不夠，有可能虛度時日而沒有太大的收穫。

我的自制力不算太差，但過去在業務上經常感嘆自己比較法學之基礎不夠，往往碰到美國法律或判例即感到束手無策，因此面對這千載難逢的進修機會，我還是毅然決定到美國法學院當個乖學生。

放榜後第二個煩惱是如何選擇學校，我獲選的研究題目爲「網路及智慧財產權犯罪之防治與查緝實務」，由於放榜時已是十二月中旬，而美國名校之申請截止期限多在隔年一月中旬，時間上非常急迫（若當訪問學者則無此申請時間之壓力），所幸，有一所在智慧財產權領域享有盛名之研究所 Franklin Pierce Law Center，申請手續相當簡單，甚至不需要推薦信，於是在四月中旬，我順利地拿到了法學碩士班（L.L.M.）之入學許可，準備體驗人生中第一次留學經驗。

到了美國，只能用眼界大開來形容，除了文化與生活習慣的截然不同外（飲食大概是讓我最難適應的一環），美國法學院紮實的訓練課程，和美國教授認真的治學與教學態度，更讓我受益匪淺。爲了趕上功課進度，我終日埋首書堆，印象中，自己從不曾如此賣力地讀書！

回國後，剛好碰上著作權法修正草案和刑法妨害電腦使用罪章草案之立法，由於我國著作權法已逐漸向美國著作權法傾斜，而電腦犯罪立法，世界各國更是以美國馬首是瞻，於是去年苦讀所學剛好都能派上用場，對國家之栽培能學以致用，略盡棉力，確是人生一大樂事。

本出國報告之第一部分，就是刑法妨害電腦使用罪章之立法研究，該草案係筆者於出國前所草擬，而於回國後見證該草案之通過，筆者特別摘記該草案之立法過程重點，並輔以比較法之研究，以供關心電腦犯罪立法者之參考。第二部分則是美國司法部電腦犯罪與智慧財產權處（CCIPS）簡介翻譯，該份文件記敘美國司法部刑事司（相當於筆者目前服務之單位：法務部檢察司）如何於 1991 年成立由五名檢察官組成之「電腦犯罪組」(Computer Crime Unit)，並逐漸發展成目前有四十名專業檢察官之「電腦犯罪與智慧財產權處」，該處目前業已成爲領導全世界網路犯罪立法之重要機構，包括歐洲網路犯罪公約，該處亦著力甚深，該處之成功經驗，頗值吾人借鏡。第三部分則是美國智慧財產權立法簡介翻譯，此份文件很扼要地勾勒出美國智慧財產權法律體系，與智慧財產權刑事處罰條文之演進過程，特別是美國政府對於智慧財產權犯罪之態度，從純粹之民事救濟逐漸轉爲輔以刑事追訴，亦值我國參考。

最後，我要特別感謝蔡司長碧玉與洪副司長光煊之提攜，讓我能在電腦犯罪與智慧財產權領域有所發揮，並能有機會實現出國進修之夢想，謹記於此，以表謝忱。

摘　要

本出國報告之第一部分，就是刑法妨害電腦使用罪章之立法研究，該草案係筆者於出國前所草擬，而於回國後見證該草案之通過，筆者特別摘記該草案之立法過程重點，並輔以比較法之研究，以供關心電腦犯罪立法者之參考。第二部分則是美國司法部電腦犯罪與智慧財產權處（CCIPS）簡介翻譯，該份文件記敘美國司法部刑事司（相當於筆者目前服務之單位：法務部檢察司）如何於 1991 年成立由五名檢察官組成之「電腦犯罪組」（Computer Crime Unit），並逐漸發展成目前有四十名專業檢察官之「電腦犯罪與智慧財產權處」，該處目前業已成爲領導全世界網路犯罪立法之重要機構，包括歐洲網路犯罪公約，該處亦著力甚深，該處之成功經驗，頗值吾人借鏡。第三部分則是美國智慧財產權立法簡介翻譯，此份文件很扼要地勾勒出美國智慧財產權法律體系，與智慧財產權刑事處罰條文之演進過程，特別是美國政府對於智慧財產權犯罪之態度，從純粹之民事救濟逐漸轉爲輔以刑事追訴，亦值我國參考。

關鍵字：電腦犯罪、網路犯罪、刑法妨害電腦使用罪章、虛擬寶物、歐盟網路犯罪公約

目　錄

我國刑法電腦犯罪修正條文之立法比較及實務問題研究

作者：葉奇鑫[1]

壹、 前言

為因應高科技時代層出不窮之電腦犯罪案例，我國刑法曾於民國八十六年十月八日公布修正及增訂共計九個條文（以下簡稱：八十六年電腦犯罪條文）[2]，該次修法及時解決了當時司法界處理電腦犯罪案例時，法律適用上之困境，對於近五年來電腦犯罪查緝實務之發展，確實有重大貢獻。惟近年來因網路快速發展，電腦犯罪手法不斷翻新，為有效規範新型態之電腦犯罪，並使我國電腦犯罪之法律規範能符合世界先進國家之標準[3]，法務部於九十年五月邀集產官學界代表共同組成「法務部防制電腦（網路）犯罪相關法規研究小組」（以下簡稱電腦犯罪法規研究小組），歷經一年多之理性辯論，逐步將共識形成具體草案文字[4]。該草案經行政院審查後會銜司法院送立法院審議，立法院於九十二年六月三日三讀通過本草案[5]， 總統並於九十二年六月二十五日公布。至此，我國刑法新增第三十六章「妨害電腦使用罪」章（簡稱電腦犯罪專章），專以處理狹義之電腦犯罪[6]。

---

[1] 本文作者為交通大學電子工程系畢業，東吳大學法律研究所碩士，現職法務部檢察司調辦事檢察官，電子信箱：simon061@ms3.hinet.net

[2] 修正條文計有四條：刑法第二百二十條、第三百一十五條、第三百二十三條、第三百五十二條。增訂條文則有五條，分別為：第三百一十八條之一及之二、第三百三十九條之一至之三。

[3] 法務部於本次修法之初，即確立以歐洲網路犯罪公約為本次立法之重要參考方向，參見電腦犯罪法規研究小組九十年十二月二十七日會議記錄，「刑法有關電腦（網路）犯罪研修資料彙編」，第八十六至八十七頁。另關於歐洲網路犯罪公約與我國相關法律（實體法部分）比較表，亦請參見上開彙編第三百一十三至三百二十頁。

[4] 關於法務部防制電腦（網路）犯罪相關法規研究小組前後共十一次會議之完整會議記錄、各草案版本及外國參考資料等，均收錄於「刑法有關電腦（網路）犯罪研修資料彙編」，九十二年十二月，法務部印製。

[5] 修正條文及立法理由之電子檔，可於「立法院全球資訊網」（網址：http://www.ly.gov.tw/ly/index.jsp）之「法律資料庫」檢索，或於法務部部內網站首頁下載。

[6] 一般而言，廣義之電腦犯罪係指以電腦為工具犯傳統型犯罪，例如：網路詐欺、網路色情等。而狹義電腦犯罪則指以電腦或網路為攻擊標的之犯罪，例如：駭客入侵、電腦病毒等

筆者因職務關係有幸全程參與修法過程，且鑒於新修正電腦犯罪條文將對我國實務審理電腦犯罪案件之法律適用將產生重大影響，因此不揣學識淺陋，爲文將修法重點與各方先進共享，除期發揮拋磚引玉之效果外，並願藉此文對所有參與本法案之先進表達由衷之感謝。

貳、 我國電腦犯罪實體法之體系與架構

傳統刑法於訂定搶奪、強盜、竊盜等諸多財產犯罪行爲態樣及刑度時，係以有體物之保護爲思考基礎，進而以不法腕力之有無，及其他可能造成人身危險之因素（例如：夜間、攜帶凶器、結夥人數等）來區分罪名與刑度，此與電腦網路犯罪決勝於千里之外之無形犯罪特質，本質上有極大之不同，故世界各先進國家均以獨立之電腦犯罪條文規範電腦犯罪行爲。我國八十六年電腦犯罪條文基本上仍係架構於傳統刑法之基礎上發展，除創設電磁紀錄之概念且將準文書之範圍擴張至電磁紀錄外（刑法第二百二十條），並將電磁紀錄擬制爲動產（原刑法第三百二十三條），使電磁紀錄得以藉傳統刑法之竊盜罪、侵占罪（刑法第三百三十八條準用）、詐欺罪（刑法第三百四十三條準用）、搶奪及強盜罪（刑法第三百三十四條之一準用）獲得保護。本次修法則因考量電腦已成爲日常生活之重要工具，電腦使用安全、電磁紀錄支配權及電腦系統效能等應已成爲值得獨立保護之法益，因此設立專章獨立保護上開法益，又由於電腦安全等法益於新法中已受到充分保護，因此本次修法同時刪除八十六年電腦犯罪條文中將電磁紀錄擬制爲動產之規定，以避免發生法條競合之情形，並進而將法律問題簡化，以受攻擊客體係有體物或無體物爲區分標準，如爲有體物（例如：搶奪磁片或竊取電腦），則以傳統刑法評價，如爲無體物（如駭客入侵網站並竊取電磁紀錄），則以電腦犯罪專章處理。以下謹逐條說明新增之刑法第三十六章妨害電腦使用罪章。

參、 妨害電腦使用罪章逐條釋義與問題探討

一、章名：妨害電腦使用罪

如前所述，本章係以狹義電腦犯罪，亦即以電腦或網路爲攻擊標的之行爲作爲規範對象。本章章名原擬爲「電腦犯罪」，惟從立法技術之角度來看，刑法章名向以「某某罪」爲名，例如：殺人罪、傷害罪或竊盜罪等，並未有「某某犯罪」之章名體例，因此於草案研擬過程中又仿英國 Computer Misuse Act，將章名改爲

「濫用電腦罪」[7]。惟學者認爲：「濫用」一詞係指有權使用者超越正當合理使用之情形，與本章目的係保障他人電腦使用之不受侵害不符[8]。故最後以甘添貴及靳宗力教授所提議之「妨害電腦使用罪」爲章名[9]。

另，有學者主張電腦一詞似不足以涵蓋網際網路空間之部分[10]。更有專家認爲：網路爲電腦連結而成，網路犯罪爲電腦犯罪之一種類型，電腦犯罪與網路犯罪之定義與範圍有所不同[11]。上開對電腦犯罪及網路犯罪之區分，固非無見。惟如從外國之經驗來看，所謂電腦犯罪(Computer Crime)與網路犯罪(Cybercrime)之區隔，卻非如此絕對。據美國學者於二００一年二月十日，分別從 Westlaw 及 Findlaw 法律資料庫搜尋之結果，均顯示美國法院判決並未使用 Cybercrime 一字，惟於 Westlaw 中則可查得九十四個使用 Computer Crime 一詞之法院判決[12]。又美國最重要之網路犯罪政策單位：美國司法部「電腦犯罪與智慧財產權處」（CCIPs）之全稱爲"Computer Crime" and Intellectual Property Section，並非使用 Cyber Crime。但歐洲網路犯罪公約(Convention on Cybercrime)則使用 Cybercrime 一詞爲名，新近諸多國際會議亦經常使用 Cybercrime 一詞[13]。由此可見，於國際上，Computer Crime 或 Cybercrime 均有人使用，其間之區別並非涇渭分明。況本法保護之客體並不限於網路上之電腦，亦包含單機電腦，因此本章雖未使用「網路」，而係以「電腦」爲名，應無不妥。

二、無故入侵他人電腦（刑法第三百五十八條）

刑法第三百五十八條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有

---

[7] 參見電腦犯罪法規研究小組九十一年三月一日會議記錄，「刑法有關電腦（網路）犯罪研修資料彙編」，第一百三十一頁。

[8] 參見電腦犯罪法規研究小組九十一年五月二十日會議記錄，靳宗立教授之發言，「刑法有關電腦（網路）犯罪研修資料彙編」，第二百三十一頁。

[9] 同前揭註，第二百三十頁至第二百三十三頁。

[10] 同前揭註，第二百三十頁。

[11] 參見吳芙如檢察官著，「網路犯罪之管轄權」，收錄於 2003 網路犯罪與智權保護研討會論文集，第二十一至第二十二頁。

[12] *See* Ralph D. Clifford, Cybercrime-The Investigation, Prosecution and Defense of a Computer-Related Crime, page 1. (2001)

[13] 例如：APEC 今年七月二十一日至二十五日於泰國曼谷舉辦之「亞太經濟合作網路犯罪立法及執法能力建構會議」(Cybercrime Legislation and Enforcement Capacity Building)。香港大學近年定期舉辦之網路犯罪高峰會（Cybercrime

期徒刑、拘役或科或併科十萬元以下罰金。」本條保護法益係電腦之使用安全，如使用人能合理期待其電腦具有高度之安全性，而該安全性卻因爲他人之無故入侵行爲而遭受破壞，行爲人即可能該當本罪。使用人能合理期待其電腦具有高度安全性之情形可概分爲二：

（一）設有保護措施：使用人已爲其電腦設有密碼（例如：一般個人電腦系統均具備之 BIOS 密碼、作業系統密碼或螢幕保護程式密碼等），或已安裝其他類似之保護措施（例如：在高階筆記型電腦或 PDA 可見到的指紋或聲紋開機辨識系統等），上開密碼及保護措施原足以阻絕他人無故使用電腦，以確保電腦之安全性，但卻因爲行爲人以盜取之密碼或破解保護措施之方法入侵，此行爲縱使未生實質損害（例如：行爲人只把玩電腦一會兒即自行離去），該電腦之安全性亦已受到破壞與挑戰，行爲人已該當本條之罪。

（二）系統漏洞：使用人原能合理期待電腦係處於安全狀態（最常見之情形爲網路上之電腦），但卻因爲他人無故利用系統之漏洞而遭到入侵，此種情形雖然使用人未設有保護措施，但因爲在正常使用情形下，他人應該無法進入並使用其電腦，使用人因此得以合理期待電腦之安全性，如因行爲人利用系統漏洞而遭到入侵，行爲人亦可能該當本罪。

由上述分析可知，本條適用之關鍵在於使用人對其電腦安全性是否能有合理之期待，故如電腦未設有密碼，或雖設有密碼，但使用人輸入密碼開機後因故離開時，卻未再設密碼保護，因而遭到他人輕而易舉地不必使用任何密碼或破解手法即得以無故使用其電腦，此類情形原則上均不成立本罪。

又本條所稱之保護措施，與著作權法本次修正草案所列之科技保護措施（Technological Protection Measures ）[14]概念並不相同，最主要之差別在於保護之目的與對象不同，前者爲限制電腦之使用，後者則爲限制著作之利用，所以如果在自己所有之電腦上安裝某廠牌軟體時，利用破解軟體規避輸入註冊碼之科技保護措施，此行爲人可能違反著作權法，但卻不構成本罪，因爲該電腦乃行爲人所有，行爲人並沒有破壞任何人之電腦安全。惟因本次著作權法修正草案於九十

Summit）等，均使用 Cybercrime 一詞。

[14] 智慧財產局本次提出之著作權法修正草案中關於科技保護措施之定義與規定，文字大致上與美國著作權法 17 U.S.C. §1201 規定相同。

二年六月五日立法院朝野協商時，科技保護措施之條文已被刪除[15]，因此今年六月六日三讀通過之著作權法並未將科技保護措施納入規範，法律適用上暫時沒有混淆之虞。

二、無故取得、變更、刪除電磁紀錄（第三百五十九條）

刑法第三百五十九條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」本條保護之法益爲電磁紀錄之支配權。由於本條已將電磁紀錄直接列爲保護之對象，因此於電磁紀錄被無故刪除之情形，不須再考慮電磁紀錄是否符合文義性而符合「準文書」之要件。又此次修法已將電磁紀錄擬制爲動產之規定刪除（刑法第三百二十三條），故於無故取得他人電磁紀錄之情形，亦無須考慮傳統竊盜罪之「破壞他人持有並進而建立自己持有」之構成要件，法律適用上均較爲單純。實務上目前常見之虛擬寶物竊盜案件，未來亦將不再論以竊盜罪，而改論以本罪。

三、無故干擾他人電腦（第三百六十條）

刑法第三百六十條規定：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致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。」本條保護之法益爲電腦系統之效能。本條精神上與原刑法第三百五十二條第二項「干擾他人電磁紀錄罪」相近，本次修正之目的在於釐清干擾之方式限於電腦程式或其他電磁方式[16]，又原刑法第三百五十二條第二項保護之對象爲「電磁紀錄之處理」，新法則改爲「電腦或其相關設備」。本條文適用上之關鍵在於判斷行爲人之干擾行爲是否已「致生損害於公眾或他人」，故常見之

---

[15] 筆者因職務關係，亦全程見證著作權法草案朝野協商過程。立法委員於朝野協商時刪除著作權法草案中關於科技保護措施之相關條文，其主要理由即爲：著作權法草案之科技保護措施，於刑法第三百八十五條中已經規定，勿庸再予重複規定。筆者認爲：科技保護措施立法與否，當屬可供社會公評事項，惟如以刑法第三百五十八條已有重複規定爲由，而刪除該草案科技保護措施之條文，則爲對於刑法第三百五十八條之誤解。

[16]原刑法第三百五十二條第二項干擾電磁紀錄罪，並未將攻擊方式明確界定，造成文義射程太廣，例如：毀損鍵盤、螢幕等毀損硬體之方法，可能干擾電磁紀錄之處理，拔除排線接頭雖未毀損硬體，亦可能干擾電磁紀錄之處理，實則上開例子均屬對有體物之攻擊行爲，應以傳統刑法之毀損罪評價即已足。以上例子均請參見甘添貴教授著，體系刑法各論，第二卷，第四百九十二頁，二０００年四月初版。

垃圾郵件、掃描通訊埠等行爲，因尚未「致生損害」[17]，原則上均未構成本罪。又法院目前審理虛擬寶物竊盜案例所適用之法條，見解並不統一，有法官除認爲除構成竊盜罪與詐欺得利罪外，尚構成原刑法之干擾電磁紀錄罪，此見解於現行法固非無據，惟於新法公布施行後，此見解恐須變更，因爲輸入他人帳號密碼進而移轉竊取虛擬寶物，均爲原遊戲平台提供之功能，此種行爲嚴格說來並未影響系統之效能，所發生之損害乃係因伺服器之電磁紀錄被變更所致，而此部份已有前述之刑法第三百五十九條可資規範。至於極具爭議性之遊戲外掛程式，是否該當本條？亦應視其是否「致生損害」而定，以練功程式爲例，如果該程式係以正常遊戲節奏自動操作角色進行練功或尋寶，此種程式並未影響到系統效能，應不該當本罪，反之，如果該程式係以非常誇張之密集封包傳送方法「加速」練功，此種程式會造成伺服器超過負荷而當機，因而致生損害，如行爲人主觀上亦對此種損害之發生有所預見，則可能（並非一定）該當本罪。至於影響系統效能到什麼程度方能認爲是致生損害，很難量化，必須透過實務逐步累積案例。

四、公務機關電腦之加重規定（第三百六十一條）

刑法第三百六十一條規定：「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。」本條係爲加強保護公務機關電腦所設之加重規定，字義上並不難解，有疑問者爲告訴乃論與否之問題。本條之立法方式十分類似傷害直系血親尊親屬罪（刑法第二百七十七條、第二百八十條），雖然第二百八十七條並未規定傷害直系血親尊親屬罪是否須告訴乃論，但我國實務向來見解認爲：傷害直系血親尊親屬罪性質上爲傷害罪之刑度加重，因此仍屬告訴乃論[18]。惟本條之立法原意，原本即欲將之列爲非告訴乃論罪，於立法院司法委員會一讀審查時，立法委員亦曾就此罪是否宜採告訴乃論進行詢答，後結論同意採非告訴乃論，故審查會之審查報告中亦補充本條之修正理由略謂：「至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法」。由於立法意旨已明示於立法理由，本條自應解爲非告訴乃論之罪，而不應援引實務上對刑法第二百八十條之解

---

[17] 關於掃描通訊埠之行爲，美國地方法院曾以並未造成損害爲由判決無罪。Scott Moulton and Network Installation Computer Services, Inc. v. VC3 (N.D. Ga. November 6, 2000)。

[18] 參照十九年上字第一九六二號判例要旨。

釋認第三百六十一條爲告訴乃論。

五、製作惡意電腦病毒程式（第三百六十二條）

刑法第三百六十二條規定：「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。」本條係處罰製作「專供犯本章之罪」之惡意程式之行爲，由於構成要件已將該類程式限定於「專供犯本章之罪」之電腦程式（典型之例爲：電腦病毒程式及後門程式），且本條文尚以實害之發生爲要件，故本條文適用情形著實相當有限，以台灣近六、七年來所查獲之電腦犯罪案例觀察，只有極少數個案（例如：車諾比病毒案件）符合本條之構成要件而已，由於本條在構成要件上相當嚴格，應不至於對軟體產業或學術研究產生影響。

六、告訴乃論（第三百六十三條）

刑法第三百六十三條規定：「第三百五十八條至第三百六十條之罪，須告訴乃論。」由於科技法律向具爭議性，特別是網際網路源於崇尚學術自由之大學及研究中心，因此「網路公民」向以自由、共享爲標榜，甚至有人主張網路空間係一獨立之虛擬新社會，應免於國家統治[19]。故以刑罰約制電腦及網路犯罪之界限應如何拿捏，亦成爲本次修法過程中辯論最多之焦點。爲避免國家司法權過度介入網路虛擬空間，且爲使有限之司法資源能集中於偵辦重大網路犯罪，故本章之罪除第三百六十一條及第三百六十二條之外，其餘之罪均採告訴乃論。

肆、以國際標準檢視本次修法

一、歐洲網路犯罪公約

由於世界各國皆意識到網路犯罪問題之嚴重性，因此國際間乃在歐洲執委會率先倡議，與歐洲議會之主導下，在二００一年十一月二十三日在布達佩斯通過第一個國際性網路犯罪公約[20]。歐洲網路犯罪公約簽署國計有美國、日本、加拿大、南非四個非歐洲議會成員國，及歐洲議會成員中之三十三個國家，而其中已

---

[19] 關於網路法律之探討，請參考劉靜怡教授譯，「網路自由與法律」，Lawrence Lessig，商周出版，二００二年七月二十九日初版。

[20] 關於網路犯罪公約，請參閱馮震宇教授著，「網路犯罪與網路犯罪公約（上）（下）」，月旦法學教室第四期第一百二十四頁至第一百三十六頁、第五期第一百一十五頁至第一百二十四頁，二００三年四月、五月。

經批准生效者僅有阿爾巴尼亞、克羅埃西亞和愛沙尼亞等三個國家[21]，但誠如美國司法部 CCIPs 處長瑪莎女士（Martha Stansell-Gamm）於「亞太經濟合作網路犯罪立法及執法能力建構會議」中演講時指出：歐洲網路犯罪公約應爲世界各國網路犯罪立法之下限，而非上限（It's a floor, not a ceiling）[22]。故歐洲網路犯罪公約實已經成爲國際間審核各國電腦犯罪相關立法之標準，我國本次電腦犯罪專章之修法亦應以歐洲網路犯罪公約加以檢驗，以符合國際網路犯罪之立法趨勢。

二、APEC 電腦犯罪立法調查

爲瞭解 APEC 各經濟體電腦犯罪之立法情形，APEC 於二００二年底對各經濟體發出問卷調查(SURVEY OF CYBERCRIME LEGISLATION)[23]。該份問卷係以歐洲電腦犯罪公約爲範本，共列出三十一項問題，其中與實體法有關者共有十一項，而與狹義電腦犯罪有關者則有下列五項[24]，美國 CCIPs 並彙整分析各經濟

---

[21] 參見 Convention on Cybercrime / Chart of signatures and ratifications，http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (latest visited Oct. 14, 2003)。

[22] 該會議係於二００三年七月二十一至二十五日於泰國曼谷舉辦，該會議共分成三大主題，第一主題（Session #1）即爲「打擊網路犯罪之法律架構」（Legal Frameworks For Combating Cybercrime）。第一主題共分成二日討論（七月二十二日及二十三日），筆者受邀於七月二十二日下午擔任 Speaker，介紹我國網路犯罪之立法進度，刑事警察局偵九隊李相臣隊長則受邀於七月二十三日上午擔任 Speaker，介紹我國網路犯罪之查緝情形。該次會議之內容請參見「亞太經濟合作網路犯罪立法及執法能力建構會議」出國報告，報告人：戚難先、盧玲朱、葉奇鑫、李相臣。

[23] 我國之問卷係由電信總局轉法務部檢察司，再由筆者與慶啓人檢察官共同填寫。問卷內容請參閱：
http://www.apjii.or.id/apec/Country%20Surveys/ChinaSurvey.htm (latest visited Oct.14, 2003)

[24] 其他六項屬廣義電腦犯罪者分別爲：（六）Offences relating to Computer related forgery (such as the alteration or deletion of computer data with the intent that it be acted on for legal purposes as if it were authentic)、（七）Offences relating to computer related fraud (such as by dishonestly attempting to gain money or property by altering computer data)、（八） Offences relating to the creation, possession, or distribution of child pornography、（九）Offences related to infringements of copyright and related intellectual property rights、（十）Attempt and aiding or abetting in respect of the above computer related offences（十一）Corporate liability in respect of the above computer related offences 。參見前揭註網址

體之立法情形如下[25]：

（一）非法接觸電腦罪（Offences relating to illegal access to a computer）

1、本項目之依據爲歐洲電腦犯罪公約第二條，我國現行刑法中與之對應者爲第三百五十八條。

2、問卷說明：本項目係指禁止單純之未經授權入侵電腦之行爲，例如：電腦駭客等。

3、美方分析意見：全部經濟體均有某種程度之立法，以規範此種犯罪。但某些經濟體在規範時仍有範圍限制，例如：只限於接觸電腦程式或資料時才犯罪，或者必須規避某種限制接觸之保護功能才犯罪。

4、本文分析意見：我國刑法第三百五十八條即屬美方所指「規範時仍有範圍限制，例如：必須規避某種限制接觸之保護功能才犯罪」之情形，惟此部分其實是我國立法政策選擇後之結果，於草擬條文時即經過充分討論，當時與會專家學者多認爲：如果未經授權或無故使用他人電腦即構成本罪，處罰範圍可能太廣，對社會將造成衝擊，因此刻意將電腦之範圍限定在已經設有保護措施之電腦，或雖未設有保護措施，但正常使用情形並不會被入侵之電腦[26]。

（二）非法擷取電子通訊罪（Offences relating to illegal interception of electronic communications）

1、本項目之依據爲歐洲電腦犯罪公約第三條，我國現行刑法中與之對應者爲第三百五十九條，另如果擷取之電子資料涉及通訊內容，尚可能涉及通訊保障及監察法。

2、問卷說明：本項係禁止非法之網路監聽。

3、美方分析意見：許多經濟體並未特別針對電子通訊監聽立法，電子通訊之監聽是否等同於電話監聽，而受一般電話監聽法律之規範？美國特別對此提出質疑。

4、本文分析意見：查我國刑法第三百五十九條中之「無故取得」，於解

---

[25] 以下美方分析意見部分，均請參見「亞太經濟合作網路犯罪立法及執法能力建構會議」出國報告第九至第十頁。

[26] 參見電腦犯罪法規研究小組九十一年三月二十二日會議記錄，「刑法有關電腦（網路）犯罪研修資料彙編」，第一百六十五至第一百七十二頁。

釋上應當包含以有線或無線方式擷取電磁紀錄；又我國實務上向認通訊保障及監察法包含網路監聽，而違法監聽者，依該法第二十四條規定，可處五年以下有期徒刑。故我國雖未直接針對電子通訊監聽立法，仍應認無此項漏洞。

（三）干擾電腦資料罪（Offences relating to interference with computer data）

1、本項目之依據爲歐洲電腦犯罪公約第四條，我國現行刑法中與之對應者爲第三百五十九條。

2、問卷說明：本項目係指禁止未經授權干擾電腦資料或電腦程式，例如：損害資料正確性、刪除資料、使合法使用者無法使用電腦資料等行爲。

3、美方分析意見：大部分經濟體均訂有某種程度之干擾罪，且大部分經濟體並不將非法使用列爲本罪之要件，這是好現象。

4、本文分析意見：我國刑法第三百五十九條雖未使用干擾一詞，惟對於電腦資料（我國法稱電磁紀錄）之保護範圍大致相同，故應符合本項標準。

（四）干擾電腦系統罪（Offences relating to Interference with a computer system）

1、本項目之依據爲歐洲電腦犯罪公約第五條，我國現行刑法中與之對應者爲第三百六十條。

2、問卷說明：本項目禁止未經授權干擾電腦系統，例如：關閉電腦系統、妨礙電腦系統正常運作、使合法使用者無法使用電腦系統等行爲。

3、美方分析意見：許多經濟體有立法規範干擾電腦系統罪，但有部分經濟體只處罰干擾電腦資料之行爲，而未特別規範針對電腦系統之干擾行爲。

4、本文分析意見：查我國刑法第三百六十條即係以電腦或其相關設備爲保護客體，並無美方所指之情形，應符合本項標準。

（五）濫用裝置罪（Offences relating to misuse of devices）

1、本項目之依據爲歐洲電腦犯罪公約第六條，我國現行刑法中與之對應者爲第三百六十二條。

2、問卷說明：本項目係禁止生產、散布、販售或持有可以犯上開罪之裝置，例如：帳號密碼、可用以入侵之軟體工具及非法監聽程式（Sniffers）等。

3、美方分析意見：許多經濟體並未特別針對生產、散布、販售或持有

可以犯上開罪之「裝置」立法處罰，部分經濟體僅處罰移轉（transfer）使用裝置（access devices）之行爲。

４、本文分析意見：查我國刑法第三百六十二條僅處罰製作專供犯本章之罪之電腦程式，就行爲而言，並未規範到散布、販售及持有等行爲，就工具種類而言，我國法僅限於電腦程式，並不包括帳號密碼等，範圍確實較歐洲網路犯罪公約要求之標準狹窄許多。然本項目之立法其實仍具爭議性，世界各國軟體業者對本項目之立法亦多所疑慮，本法規範範圍雖然遠較歐洲網路犯罪公約之要求狹窄，但於草擬過程中，仍有委員強烈反對刑法第三百六十二條，認爲本條會對國內軟體產業及學術研究造成不利之影響[27]。甚至美國 CCIPs 處長瑪莎女士於泰國會議中亦坦言：「美方亦花了許多時間精力與軟體產業溝通，以解除軟體業界對此立法之疑慮。」又歐洲網路犯罪公約第六條第三項亦規定：電腦密碼、使用碼（access code）或類此資料之部分，簽署國可保留不立法，可見關於帳號密碼之部分更具高度爭議性。故我國未來就裝置濫用部分如欲全面採取歐洲網路犯罪公約之標準，必須廣納雅言，事先與軟體產業及學術研究單位充分溝通，以避免反彈與誤解。

三、小結

本次電腦犯罪專章修法雖仍未完全符合歐洲電腦犯罪公約之要求，但較之修法前，已有相當大之進步，在 APEC 經濟體中，亦已屬先進之實體法。我國接下來應重新檢視並修法者，應爲網路犯罪程序法之部分，惟因程序法部分已超越本文所探討之範疇，擬另文論述之。

伍、虛擬寶物竊盜案件之新舊法比較問題

在本次刑法修正前，雖然有少數意見認爲不應以刑法處罰虛擬寶物之竊盜行爲[28]，惟法院實務上幾乎均肯認虛擬寶物爲電磁紀錄，而依刑法第三百二十三

---

[27] 參見電腦犯罪法規研究小組九十一年四月三日會議記錄，「刑法有關電腦（網路）犯罪研修資料彙編」，第一百九十至第一百九十七頁。

[28] 是否應以竊盜罪處罰目前實務常見之虛擬寶物竊盜行爲，實務界曾有不同價值觀之精采辯論，內容詳見：九十二年二月二十一日法務部法檢字第０九二０八０

條將電磁紀錄擬制爲動產之規定，虛擬寶物之竊盜已構成刑法第三百二十三條、第三百二十條之竊取他人電磁紀錄罪。由於本次刑法修正已將刑法第三百二十三條中電磁紀錄擬制爲動產之規定予以刪除，故竊取他人虛擬寶物之行爲，於刑法修正後即無法再適用竊盜罪處罰，而必須改以刑法第三百五十八條、第三百五十九條之規定處罰[29]。

比較有疑問者，乃虛擬寶物竊盜之行爲時點係於刑法修正前，而裁判時點卻於刑法修正後之情形，此情形涉及新舊法之比較問題，且筆者觀察新近實務判決，對於此種犯罪行爲之新舊法比較，似有不同見解，有認爲比較新舊法之結果，因新法將此種犯罪改列爲告訴乃論之罪，故以新法較爲有利於行爲人，適用新法判決[30]。亦有認爲因新法第三百五十九條所定之罰金刑（二十萬元）高於刑法第三百二十條之罰金刑（五百元），比較新舊法之結果，應以舊法較有利於行爲人，而適用舊法判決[31]。

關於行爲後刑罰法律有變更時，究應如何適用法律，我國刑法係採「從新從輕之原則」，亦即原則上適用裁判時之新法，但裁判前之舊法有利於行爲人時，例外適用裁判前之舊法[32]。至於裁判時之新法與裁判前之舊法何者較爲有利之比較，應依照刑法第三十五條之規定：「主刑之重輕，依第三十三條規定之次序定之。同種之刑，以最高度之較長或較多者爲重。但最高度相同者，以最低度之較長或較多者爲重。除前二項規定外，刑之重輕參酌前二項標準定之。不能依前二項標準定之者，依犯罪情節定之。」依上開規定觀之，舊法似較有利於行爲人。

惟如行爲後法律之訴追條件（告訴乃論與否）有所變更[33]，則此是否屬於刑

0六九六號函。該函可於「法源法學資料檢索系統單機版/刑法/第三百二十條/法律問題」中檢索查閱。

[29] 一般而言，竊取虛擬寶物之行爲可分爲三階段，第一階段爲取得被害人之帳號密碼，第二階段爲登入遊戲伺服器，輸入被害人之帳號密碼，第三階段則爲操作被害人帳號中之角色，並將該角色中之虛擬寶物移轉給自己或第三人之角色。第二階段於修法前並無法可罰，第三階段實務通說則以竊盜罪處罰。修法後，第二階段可能觸犯刑法第三百五十八條，第三階段則可能觸犯刑法第三百五十九條。

[30] 參見臺灣板橋地方法院九十二年度易字第一八八八號刑事判決。

[31] 參見臺灣高等法院九十二年度上易字第一二一二號刑事判決。

[32] 刑法第二條第一項規定：「行爲後法律有變更者，適用裁判時之法律。但裁判前之法律有利於行爲人者，適用最有利於行爲人之法律。」

[33] 竊盜罪爲非告訴乃論之罪，刑法第三百五十八條及第三百五十九條則爲告訴乃論之罪。

法法律之變更而有新舊法比較之問題？又應如何加以比較？臺灣高等法院研究意見認爲：告訴權之行使、撤回固屬國家刑罰權得否發動，即刑事訴訟之訴追條件具備與否之刑事程序問題，雖程序應從新，惟某種行爲應否劃歸屬告訴乃論之罪，因事涉國家刑罰權得否據以發動所依憑之內容及其範圍之界定，乃具實體性質，就此層面而言，對某種犯罪行爲是否得以發動國家刑罰權予以制裁，恒宥於該類型化之犯罪是否屬告訴乃論之罪，並受制於告訴權人是否行使告訴權或撤回告訴，準此，告訴權之行使、撤回與否，並非得以單純之程序問題視之。此因事涉國家刑罰權其內容及範圍之劃定，仍應認係法律有變更，而有比較新舊法之適用。又新舊法比較之結果，以對國家刑罰之發動所做一定限制之規定，較有利於行爲人，亦即以劃定爲告訴乃論之罪之規定爲較有利於行爲人[34]。上開研究意見顯認爲：行爲後法律之訴追要件有所變更，仍有新舊法比較之適用，且以告訴乃論規定之法律爲較有利於行爲人。由此觀之，新法反較有利於行爲人，應適用新法裁判，筆者亦較贊同此見解。

陸、結語

自歐洲網路犯罪公約簽署後，該公約已成爲世界各國網路犯罪立法之重要標準，我國在網路犯罪實體法部分，因本次電腦犯罪專章之補充，已大致能符合國際標準，我國相關主管機關應立即以該國際標準重新檢視網路犯罪程序法之部分，以使我國網路犯罪程序法之部分亦能臻國際水準。

司法審理網路犯罪案件時，除條文之文義解釋外，亦同時面對真實空間與虛擬空間基本價值觀之衝突與挑戰，本次修正條文之適用與解釋，仍有賴司法人之智慧與經驗累積，以釐清法律適用之界限。限於篇幅，筆者僅能簡述至此，如有未盡之處，敬請各方先進不吝賜教。

---

[34] 參見司法院(八九) 廳刑一字第００八三七號函，司法周刊第九八三期第三版。

美國司法部電腦犯罪與智慧財產權處
在打擊網路相關犯罪與智慧財產權侵害之角色
The Role of the Justice Department's Computer Crime & Intellectual Property Section in Combating Internet-Related Crime and the Infringement of Intellectual Property Rights

撰文：電腦犯罪與智慧財產權處 (CCIPS)
華盛頓美國司法部

編譯：葉奇鑫

美國司法部背景資料
Background on the U.S. Department of Justice

美國司法部於 1789 年根據美國國會的一項法案成立，由美國司法部長執掌管理。司法部的使命是：“根據律法規定執行法律並保護美國的利益；確保公衆安全免受國外和國內的威脅；提供聯邦政府在預防和控制犯罪領域的領導地位；對有違法行爲者尋求公正的懲罰……並確保爲所有美國人提供公平、公正的司法管理。”（本“使命宣言”以及其他有關司法部的背景資料均可在 http://www.usdoj.gov 查詢而得。）

The United States Department of Justice was created by an act of Congress in 1789 and is led by the Attorney General of the United States. The mission of the Department of Justice is: "To enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; ... and to ensure fair and impartial administration of justice for all Americans." (This Mission Statement, as well as other background information on the Department of Justice, can be found at http://www.usdoj.gov.)

司法部由許多機構組成，包括聯邦調查局 (FBI)、緝毒署 (DEA)、監獄管理局以及 94 個聯邦檢察署（即“美國檢察官辦事處”，分佈在美國 50 個州以及美屬領地，其任務是對違反聯邦法律的行爲提出起訴）。位於首都華盛頓的司法部總部由若干部門組成，各負責不同的任務主題，如民權司、稅務司、環境與自然資源司、刑事司。

The Department has many components, including the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Bureau of Prisons, and ninety-four federal prosecuting offices (or "U.S. Attorneys' Offices") located throughout the fifty states and the U.S. Territories, which prosecute violations of federal law. The headquarters of the Department of Justice, located in Washington, D.C., is comprised of a number of divisions, organized around various subject matters, such as the Civil Rights Division, the Tax Division, the Environment and Natural Resources Division, and the Criminal Division.

刑事司負責起訴違反美國刑事法的行爲並制訂相關政策。刑事司有特定的處或局專門負責打擊犯罪行爲，例如：欺詐、走私毒品和危險藥物、洗錢、剝削童工、恐怖主義、間諜活動、組織犯罪、貪瀆、電腦犯罪和竊用智慧財產權等。

The Criminal Division is charged with prosecuting violations of U.S. criminal law and developing related policies. It has specific sections or offices that combat criminality such as fraud, trafficking in narcotic and dangerous drugs, money laundering, child exploitation, terrorism, espionage, organized crime, public corruption, and computer crime and theft of intellectual property.

司法部電腦犯罪與智慧財產權處的誕生
Creation of DOJ's Computer Crime & Intellectual Property Section

雖然在 1969 年就發明了網路，但是美國的執法機構直到 1986 年才開始全面打擊重大的網路犯罪活動。那一年，因爲帳目上 0.75 美元的差異，使得當時身爲大學電腦管理員的加州天文學家 Clifford Stoll 發現了有人入侵大學的電腦。由於涉及的金額很小，Stoll 未能引起美國執法機構對此事的關注。在根本沒有政府的協助下，他發現電腦的入侵者竟是一個身在德國、曾由蘇聯格別烏付錢讓他盜竊美國軍事機密的駭客。這個案例證明，在有電腦犯罪活動的情況下，資料的機密性就和金錢的損失同樣地重要。（Stoll 在他於 1989 年出版的《The Cuckoo's Egg》[1]一書中講述了這個故事。）

Although the Internet was invented in 1969, law enforcement in the United States did not begin to comprehensively fight major Internet crime until 1986. That year, a $0.75 accounting discrepancy led a California astronomer, Clifford Stoll, to discover an intruder in a University computer for which he was the administrator. Because of the small monetary value involved, Stoll had difficulty interesting U.S. law enforcement in the matter and, essentially without government assistance, he discovered that the source of the intrusion was a hacker located in Germany who had been paid by the Soviet KGB to steal U.S. military secrets. This case demonstrated that, with a computer crime, confidentiality of data can be as important as monetary loss. (Stoll tells this story in his 1989 book, "The Cuckoo's Egg.")

此後相繼發生的幾個事件有助於喚醒了美國執法機構對於透過網路犯罪活動的威脅引起注意。舉例來說，1988 年，一個大學學生 Robert Morris, Jr. 開發出一種程式，即“蠕蟲”（病毒）。設計程式的目的在於滲入電腦、自我繁衍直到耗盡電腦的所有可用記憶體，從而使電腦停機，藉此方式攻擊網路上的所有電腦。在不到 48 個小時內，這一病毒就損壞了大約 6200 台電腦，造成 9800 多萬美元的損失。在 1987 到 1989 年間發生的第三個事件是一個地方電話公司的電腦被稱爲“末日兵團”(LOD) 的駭客團體侵入。該團體利用侵入能力來更改和中斷了當地的電話服務。考慮到通訊設施的極其重要性，LOD 入侵網路對正在興起的電腦革命顯示了嚴重的威脅。同時，Morris 病毒和 LOD 兩個案例也證明，在電腦犯罪中，使用電腦的重要程度可能是舉足輕重。

[1] 台灣翻譯爲「捍衛網路」，天下文化民國八十五年出版。

Several subsequent events aided in further awakening U.S. law enforcement to the threat of crime committed via the Internet. For example, in 1988, a university student named Robert Morris, Jr. developed a program, or "worm," designed to attack computers throughout the Internet by penetrating a computer, propagating itself until it consumed all available computer memory, and thereby shutting down that computer. In fewer than forty-eight hours, this worm crippled approximately 6,200 computers and caused over $98 million in damage. A third event was the penetration of the computers of a regional telephone company, from 1987 to 1989, by a hacker group known as the "Legion of Doom" (LOD), which used this ability to alter and disrupt local telephone service. Considering the critical importance of communication facilities, the LOD network intrusions exposed serious threats to the emerging computer revolution, and both the Morris Worm and LOD cases demonstrated that, with a computer crime, the availability of a computer can be of vital importance.

雖然這三個案例都得到了成功的處理，但是，到 1989 年年底已經很明顯：新興的電腦和電信技術會對執法團體提出新的挑戰。電腦在日常生活中不斷擴大的使用範圍和日益增長的網路使用以及其他網路社區的發展，不僅僅改變著我們的生活方式，也同時在改變犯罪分子的行動方式。在認識到這一點之後，美國政府開始制定一項綜合性計劃，旨在預測這些改變以及因此而產生的挑戰，並應對這些改變和挑戰。

Although these three cases were handled successfully, it was clear by the end of 1989 that emerging computer and telecommunications technologies would pose new challenges for the law enforcement community. The widespread integration of computers into our daily lives and growing use of the Internet and other networked communications were not simply changing the way we lived, but changing the way criminals operated. Recognizing this, the U.S. government began to develop a comprehensive program to anticipate and respond to these changes and resulting challenges.

1990 年，司法部刑事司向司法部長提出了“電腦犯罪提案”，其中包括以下目標：確定電腦犯罪問題的範圍；實行對檢察官的培訓；在處理電腦犯罪案件時，實施機構之間的合作；針對國際電腦犯罪威脅，制定國際性反應方式；提出意見並提供立法提案來應對電腦犯罪問題；制定一致的政策，讓執法機構能在積極調查和起訴電腦犯罪活動時，能同時保護公民的自由。此提案於 1991 年被採納，並成立了由五名檢察官組成的“電腦犯罪組”。

At the Department of Justice, the Criminal Division proposed to the Attorney General in 1990 a "Computer Crime Initiative," which included as objectives: determining the scope of the computer crime problem; instituting training for prosecutors; facilitating inter-agency cooperation in computer crime cases; developing an international response to the threat of international computer crime; commenting on and offering legislative proposals to address computer crime issues; and formulating coherent policies that allow law enforcement to investigate and prosecute aggressively computer crime while also protecting civil liberties. The initiative was adopted in

1991 and a five-lawyer Computer Crime Unit was created.

然而，就在“電腦犯罪單位”開始在聯邦層次上強調電腦和網路犯罪問題後不久，又有另一種形式的相關犯罪行爲被添加到這個新單位的任務之中。隨著上一世紀 90 年代的進展，創造出越來越多的數位式智慧財產權（如商業軟體、流行音樂、好萊塢電影、電腦遊戲），且以數位格式銷售。日益增長（不久之後，爆炸性增長）的網路使用，意味著受著作權保護的財產其完善的數位式拷貝可以很低的成本在全世界範圍被大量地散布。因此，在成立後短短幾年內，“電腦犯罪單位”的職責單上就添加了有關智慧財產權刑事法之執法。1996 年，“電腦犯罪單位”被提升成爲司法部的“電腦犯罪與智慧財產權處”(CCIPS)。

However, not long after the Computer Crime Unit began addressing computer and Internet crime at the Federal level, another form of related criminality would be added to this new Unit's mission. As the 1990s progressed, increasing amounts of intellectual property – such as business software, popular music, Hollywood movies, and video games – were being created and sold in digital format. Growing (and, soon, exploding) access to the Internet meant that perfect digital copies of copyright-protected property could be distributed worldwide, at little cost, and in great quantities. Therefore, within a few years of its creation, the Computer Crime Unit also added to its portfolio the responsibilities for criminal enforcement of intellectual property rights. In 1996 the Computer Crime Unit was elevated to become the Computer Crime & Intellectual Property Section (CCIPS) of the Justice Department.

CCIPS 當前的使命
CCIPS's Current Mission

CCIPS 目前擁有四十位檢察官。除此之外，CCIPS 對 94 個美國檢察署的 200 多名聯邦檢察官提供培訓和支援，因此讓這些檢察官能夠專注於處理電腦與智慧財產權犯罪案件。CCIPS 不僅與這些聯邦檢察官密切合作，同時也和政府其他許多領域的代表合作，包括國土安全部、FBI、美國特工處、美國海關署以及全國各州和地方的執法部門。

Today CCIPS has forty lawyers. In addition, CCIPS trains and supports 200 more federal prosecutors throughout each of the 94 U.S. Attorneys' Offices and, in turn, those prosecutors primarily focus on computer and intellectual property crime. CCIPS works closely not only with these federal prosecutors, but also with representatives from many other areas of our government, including the Department of Homeland Security, the FBI, the U.S. Secret Service, the U.S. Customs Service, and state and local law enforcement throughout the country.

CCIPS 的主要使命仍然是與電腦犯罪相關法律之執法（例如，與入侵電腦、攻擊資訊網路、電腦蠕蟲和病毒相關的法律）以及與侵害智慧財產權相關的犯罪活動。這項工作已經擴展到許多相關的領域，例如：

CCIPS's primary mission remains the enforcement of criminal laws relating to computer crimes – such as those relating to computer intrusions, attacks on information networks, and computer worms and viruses – and crimes relating to the infringement of intellectual property rights. This work has expanded into many related areas, such as:

- 打擊利用電腦和網路作爲恐怖分子之間的聯絡工具以及協助此類行爲的國際恐怖主義；
  combating international terrorism, where computers and the Internet are used for communications among terrorists and to facilitate their acts;

- 保護關鍵性基礎設施，如通訊網絡、銀行業以及高度依賴電腦網路並容易受到網路駭客攻擊的應急服務；
  protecting critical infrastructures such as communications networks, banking, and emergency services that rely heavily on computer networks and which remain vulnerable to cyber-attack;

- 當我們與個別國家合作進行特定的跨邊界調查並與多邊團體——如 G-8、歐理會、歐盟、亞太經合組織（即 APEC）以及美洲國家組織——合作的同時，促進並協助國際合作，以制定出更完善的國際法規、政策和方法來打擊國際網路犯罪；
  promoting and facilitating international cooperation as we work with individual countries on specific cross-border investigations and with multilateral groups – such as the G-8, Council of Europe, European Union, Asia Pacific Economic Cooperation (or APEC) forum, and Organization of American States – to develop better international laws, policies and practices to combat international cybercrime;

- 在美國的地方、州和聯邦各層次並在全球衆多國家，培訓調查員和檢察官；
  training investigators and prosecutors at the local, state and federal levels in the United States and in many countries throughout the globe;

- 對於網路犯罪和智慧財產權的立法提出提議並提供意見，對正在草擬新的國家法規的其他國家提供協助；並且
  proposing and commenting on legislation concerning cybercrime and intellectual property, and assisting other countries that are drafting new domestic legislation; and

- 與業界和民間部門的代表合作，確保能夠結合和考量不同的相關觀點。
  working with representatives from industry and the private sector to ensure cooperation and consideration of different relevant viewpoints.

在美國的智慧財產權犯罪起訴
Prosecution of Intellectual Property Crimes in the United States

撰寫：電腦犯罪與智慧財產權處 (CCIPS)
華盛頓美國司法部
www.cybercrime.gov

編譯：葉奇鑫

背景資料
Background

在美國，智慧財產權的重要性——無論是發明、文學或藝術作品、商業機密，還是商業所用符號或設計——從國家建立的初期就已經得到重視。於 1787 年通過的《美國憲法》明確授權美國國會可制定法規，確保作者和發明者就其作品與發現享有有限期間之專有權利，以促進科學和實用性藝術之進步。

The importance of intellectual property – whether it be inventions, literary or artistic works, trade secrets, or symbols or designs used in commerce – has been recognized in the United States since the earliest days of the nation's founding. The United States Constitution, ratified in 1787, expressly authorized the United States Congress to enact legislation to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."

自從 1790 年首次制定聯邦著作權法以來，美國的智慧財產權保護工作主要是由權利持有人自己採取民事行動，而不需要政府的參與。通過這樣的民事行動，權利持有人可收取金錢上的損失（在某些案例中，包括律師費用和實際損失的三倍）以及禁制處分和其他補償來預防侵害行爲繼續發生。

Since the enactment of the first federal copyright legislation in 1790, protection of intellectual property rights in the United States has been accomplished primarily through civil actions initiated by rights holders themselves, without the need for government involvement. Through such civil actions, a rights holder may collect money damages (including, in some cases, attorneys fees and three times his actual losses) as well as injunctive relief and other remedies to prevent the infringing conduct from continuing.

雖然對智慧財產權侵權者的刑事起訴是保護智慧財產權的另一項重要工具，但是，保護智慧財產權最早的刑事法律卻是直到 1897 年才制定出來；但當時的法律依然沒有將侵權行爲作爲重罪懲罰，直到 1982 年才有所改變。然而，過去二十年來，美國智慧財產權刑事法的執行已有大幅度提升，這是各級政府爲應付快速增長的著作權盜版、仿冒商標以及竊盜商業機密等威脅所做的努力之一。

Although criminal prosecution of intellectual property infringers is another essential tool for the protection of intellectual property rights, the first criminal laws protecting intellectual property rights were not enacted until 1897 and, even then, those laws did not punish infringement as a felony until 1982. In the past two decades, however, criminal enforcement of intellectual property rights in the United States has increased dramatically as part of a government-wide effort to meet the rapidly growing threats of copyright piracy, trademark counterfeiting, and theft of trade secrets.

針對智慧財產權犯罪的美國法令基本體制
The Basic U.S. Statutory Framework for Intellectual Property Crimes

根據美國聯邦法的規定，刑事懲罰主要適用於三種類型的盜用智慧財產權：仿冒商標、侵害著作權和竊盜商業機密。在美國，沒有針對侵害專利的刑事懲罰，因爲大家普遍認爲採用民事補償就足以保護專利持有人的權利。

Under United States federal law, criminal penalties are available for primarily three types of misappropriation of intellectual property: trademark counterfeiting, copyright infringement, and theft of trade secrets. There are no criminal penalties in the United States for the infringement of patents, as it is generally perceived that civil remedies are sufficient to protect the rights of patent holders.

仿冒商標
Trademark Counterfeiting

美國商標法旨在保護識別商品和服務的文字和符號。耐克 (Nike) 球鞋上的“彎勾” (swoosh) 和麥當勞餐廳的“M”（金色拱門）都是家喻戶曉的商標範例。如同美國所有智慧財產權一樣，商標權的保護工作主要是權利持有人自己採取的民事行動，而不需要政府的介入。如果要將侵害商標提高到刑事犯罪的等級（在美國的已知罪名爲“交易仿冒商品或服務”），必須符合以下若干要素：首先，被告一定是故意或試圖交易商品或服務。其次，被告一定使用了那些商品或服務的仿冒標記或與那些商品或服務有關的仿冒標記。最後，被告一定知道如此使用的標記是仿造的。符合這些要素且罪行成立之後，法院可能會對各個被告處以最高 10 年徒刑和 2 百萬美元的罰款；或者，若被告是企業，可處以 5 百萬美元的罰款。在《美國法典》第 18 篇第 2320 款中規定了關於交易仿冒商品或服務罪的要件及其刑罰。

United States trademark law protects words and symbols that identify goods and services. The “swoosh” on Nike shoes and the “golden arches” of McDonald’s Restaurants are examples of well-known trademarks. Like all intellectual property rights in the United States, trademark rights are protected largely through private, civil actions initiated by rights holders themselves without the involvement of the government. For a trademark infringement to rise to the level of a criminal

offense – which is known in the United States as "trafficking in counterfeit goods or services" – several elements must be met: First, the defendant must have intentionally trafficked or attempted to have trafficked in goods or services. Second, the defendant must have used a counterfeit mark on, or in connection with, those goods or services. Finally, the defendant must have known that the mark so used was counterfeit. Where these elements are met and the offense is established, the court may impose penalties on individual defendants of up to ten years' imprisonment and a $2,000,000 fine or, for corporate defendants, a $5,000,000 fine. The elements and penalties for the crime of trafficking in counterfeit goods or services are set forth in Section 2320 of Title 18 of the United States Code.

侵害著作權之刑事處罰
Criminal Copyright Infringement

著作權一般保護原始的表達形式，如書籍、劇本、音樂作品、電腦軟體、電影和其他文學或藝術作品。著作權法授予權利持有人對其受保護作品享有某些專屬權利，例如重製權和散布權。

Copyright generally protects original forms of expression, such as books, plays, musical compositions, computer software, movies, and other literary or artistic works. The law of copyright grants rights holders certain exclusive rights with respect to their protected works, such as the rights to reproduce and distribute those works.

如果符合特定構成要件，侵害著作權就是一種聯邦犯罪，可判處達 5 年的徒刑。如果被告故意侵害著作權，且目的是從侵害行爲中獲利，或者如果被告故意且在未經授權的情況下於 180 天內重製或散布了總零售價值超過 1000 美元的受著作權保護作品，被告可被判處達 1 年的徒刑並處以 10 萬美元的罰款。如果被告在 180 天內故意侵害至少 10 份，且總零售價值超過 2500 美元的受著作權保護作品，則被告可能被判處達 5 年的徒刑並處以 25 萬美元的罰款。

Copyright infringement is a federal crime, punishable by up to five years' imprisonment, if certain elements are met. If a defendant willfully infringes a copyright with the purpose of profiting from the infringement, or if the defendant willfully and without authorization reproduced or distributed copyrighted works with a total retail value of more than $1,000 within a 180-day period, then the defendant may be sentenced up to one year in prison and be required to pay a $100,000 fine. If the defendant willfully infringed, within a 180-day period, at least ten copies of copyrighted works having a total retail value of more than $2,500, then the defendant may be sentenced up to five years in prison and be required to pay a $250,000 fine.

雖然侵權行爲的商業或財務動機可提高刑事處罰，但侵權行爲的目的並不一定是要爲了商業利益或私人財務收益才能構成罪行。相反地，如下文的詳細說明（參閱"回應數位時代的挑戰"），無論被告是否從其行動中獲利或意欲獲利，侵權行爲若涉及一定零售價值的受著作權保護作品，就足以符合犯罪要素。此外，零售價值的臨界點是以被侵權的

合法作品之價值來計算，而不是以侵權材料的價值來計算。在《美國法典》第 17 篇第 506 款以及《美國法典》第 18 篇第 2319 款中規定了侵害著作權罪的要件及其懲罰。

Although a commercial or financial motivation for the infringement can enhance the criminal penalties, it is not necessary that the infringement was done for purposes of commercial advantage or private financial gain in order to constitute a crime. Rather, as discussed in greater detail below (see "Responding to Challenges of the Digital Age"), it is enough to meet the elements of the offense that the infringement involved copyrighted works of the requisite retail value, regardless of whether the defendant profited or intended to profit from his actions. Moreover, the threshold of retail value is measured by the value of the legitimate works that are infringed, not by the value of the infringing material. The elements and penalties for the crime of copyright infringement are set forth in Section 506 of Title 17 of the United States Code, and Section 2319 of Title 18 of the United States Code.

竊盜商業機密
Theft of Trade Secrets

美國聯邦政府歷來並不把竊盜商業機密作爲刑事處罰，使保護商業機密的責任落到美國 50 個州的各州政府手中。1996 年，美國國會批准了“經濟間諜法”(Economic Espionage Act)，第一次明確地在聯邦層次上將竊盜商業營業機密的行爲刑罰化。依據“經濟間諜法”，“商業機密”的一般定義爲擁有者採取了合理的措施以保持其機密性，並在公衆未知的情況下衍生出獨立經濟價值的任何形式或類型的財務、技術或其他商業資訊。如果被告意欲將商業機密轉換爲除其擁有者以外的他人的經濟利益，而且被告知道會或意欲用其行爲來傷害商業機密的擁有者，在未經授權的情況下竊盜、複製或以其他方式得到被告知道或相信是商業機密的任何機密，根據此法規即構成聯邦罪。此罪行可處罰達 10 年的徒刑並罰款 25 萬美元。如果犯下竊盜商業機密罪或試圖犯罪的目的是爲了讓某個外國政府、機構或代理得益，處罰可高達 15 年徒刑並罰款 50 萬美元。在《美國法典》第 18 篇第 1831 到 1839 款中規定了“經濟間諜法”的內容。

Until recently, the U.S. federal government did not criminalize trade secrets, leaving the protection of such matters to be handled by each of the individual governments of the fifty constituent states of the United States. In 1996, the U.S. Congress enacted the "Economic Espionage Act" which, for the first time, explicitly criminalized the theft of commercial trade secrets at the federal level. Under the Economic Espionage Act, a "trade secret" is defined generally as any form or type of financial, technical, or other business information that its owner took reasonable steps to keep secret, and which derives an independent economic value from not being known to the public. The statute makes it a federal crime to steal, copy or otherwise obtain without authorization any trade secret that the defendant knows or believes to be a trade secret if the defendant intended to convert the trade secret to the economic benefit of someone other than its owner, and if the defendant knew or intended that his actions would injure the owner of the trade secret. The punishment for this crime can be as high as ten years' imprisonment and a $250,000 fine. If the theft of trade secrets was committed or attempted in order to benefit a foreign

government, instrumentality or agent, the punishment can be as high as fifteen years' imprisonment and a $500,000 fine. The Economic Espionage Act is set forth at Sections 1831 through 1839 of Title 18 of the United States Code.

其他嚴重侵害智慧財產權罪
Other Significant Intellectual Property Crimes

雖然仿冒商標、侵害著作權和竊盜商業機密是美國主要之智慧財產權犯罪的類型，但另外還有數個法規處罰涉及智慧財產權的其他類型犯罪行爲。例如，在某些情況下，故意交易用以粘貼在特定產品（如電影或電腦套裝軟體）上的仿冒標簽是犯罪行爲。類似地，在未經授權的情況下交易實況音樂演出之錄音，也是犯罪行爲。另一項法令“數位千禧年著作權法”(Digital Millennium Copyright Act)，禁止妨礙設計用以限制使用受著作權保護作品的控制機制，並禁止使用和銷售能妨礙控制使用機制或設計用以防止複製受著作權保護作品的控制機制之任何裝置[1]。

Although trademark counterfeiting, copyright infringement and theft of trade secrets are the principal types of intellectual property crime in the United States, several additional statutes criminalize other types of conduct involving intellectual property. For example, in certain circumstances, it is a crime to knowingly traffic in counterfeit labels that are designed to be affixed to particular products such as movies or computer software packaging. Similarly, it is also a crime to traffic without authorization in recordings of live musical performances. Another statute, the Digital Millennium Copyright Act, prohibits the circumvention of controls that are designed to restrict access to copyrighted works, and prohibits the use and sale of devices that enable circumvention of either access controls or controls designed to prevent copying of copyrighted works.

回應數位時代的挑戰
Responding to Challenges of the Digital Age

電腦科技——尤其是網路——的出現，讓個人就能輕易地、廉價且以相對匿名的方式重製和散布受保護的作品。數位作品如音樂光碟、DVD 電影、軟體和 PC 遊戲，現在都能在僅僅幾秒鐘時間內透過電腦網路被傳送到世界各地，而每一份拷貝都可用作具有與原件同樣品質的完美主版。同時，智慧財產權在全球經濟中所起的重要作用也在與日俱增；因此，使得竊盜智慧財產權的經濟價值更高，也更頻繁地發生。爲了因應這些變化所呈現之日益增長的盜版挑戰，世界各國（包括美國）已經擴大並加強其法律體制來對付數位時代的犯罪行爲。美國在這方面的兩項重大發展是 1997 年的“禁止電子竊盜法”（No Electronic Theft，簡稱“NET”）和 1998 年的“數位千禧年著作權法”。

The advent of computer technology – particularly the Internet – has made it extremely easy

[1] 此即我國著作權法草案中之科技保護措施。惟科技保護措施相關條文於九十二年六月六日立法院朝野協商時，並未獲立法委員採納，而全數遭到刪除。

for individuals to copy and distribute protected works inexpensively and with relative anonymity. Digital works such as music CDs, DVD movies, software and PC games are now distributed worldwide over computer networks in a matter of seconds, each copy serving as a perfect master of the same quality as the original. At the same time, intellectual property has become an increasingly important part of the global economy, thereby making its theft more valuable – and more frequent. To meet the growing challenges of piracy that these developments present, nations around the world, including the United States, have expanded and enhanced their legal frameworks for dealing with criminal violations in the digital age. Two significant U.S. developments in this respect are the No Electronic Theft (or "NET") Act of 1997 and the Digital Millennium Copyright Act of 1998.

禁止電子竊盜 ("NET") 法
The No Electronic Theft ("NET") Act

直到最近以前，根據美國法律，區分刑事和民事侵害著作權行爲的中心概念是：要構成刑事罪，其侵權行爲的目的一定是商業或財務得益。然而，在 1994 年的一個法庭案件判決後，美國國會決定侵害著作權刑事罪的利益動機規定在網路時代已經不再適用了。

Until recently, the central concept that differentiated criminal from civil copyright violations under United States law was that, to be a criminal act, the infringement must have been undertaken for purposes of commercial or financial gain. Following a court case decided in1994, however, the United States Congress decided that the requirement of a profit motive for criminal copyright infringement was no longer sensible in the era of the Internet.

在 *LaMacchia*案件中，麻省理工學院的一個學生鼓勵他人將流行軟體未經授權地上載到他在網路上的網站，讓世界各地的其他人可以免費下載。雖然這個學生的行爲導致軟體製造商一百多萬美元的損失，但是，此侵權行爲並不是爲了獲利，他也沒有從他的舉動中得到任何財務上的收益。因爲當時存在的著作權法規定需要有利益動機才能構成罪行，所以儘管他是故意侵權且受害者承受了重大損失，政府依然無法對他的行爲以刑事罪起訴。

In that case, *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994), a student at the Massachusetts Institute of Technology encouraged individuals to upload to his site on the Internet unauthorized copies of popular software to be downloaded by others around the world for free. Although the student's conduct resulted in losses to the software manufacturers of more than $1 million, the infringement was not undertaken for profit and the student derived no financial gain from his actions. Because the copyright law then in existence required a profit motive in order to constitute a crime, the government was unable to prosecute the student criminally for his actions, despite the willfulness of the infringement and the substantial losses to the victims.

1997 年 12 月，美國國會直接針對 *LaMacchia* 一案通過了 "禁止電子竊盜法" 。此項法令修訂了著作權法，去除了構成侵害著作權罪所需要的利益動機規定。現在只要被侵權的作品達到一定的最低法定臨界零售價值，即使不存在利益動機，故意侵害著作權依然

可以是刑事犯罪。這項修正反應的事實是：在數位環境中，未經授權重製和散布權利擁有者的作品，即使犯罪人沒有商業動機，對權利擁有者的傷害並不比由商業化盜版侵權所造成的傷害要輕。

In December 1997, the United States Congress passed the "No Electronic Theft" Act in direct response to the *LaMacchia* case. The statute amended the copyright law to eliminate the requirement of a profit motive for the crime of copyright infringement. Instead, a willful infringement of copyright can now be a criminal offense, even in the absence of a profit motive, as long as the amount of material that is infringed is of sufficient retail value to meet certain minimum statutory thresholds. This change reflects the fact that, in the digital environment, the harm to rights holders from the unauthorized reproduction and distribution of their works is no less significant when committed by individuals who lack a commercial motive than when committed by commercial pirates.

數位千禧年著作權法 ("DMCA")
The Digital Millenium Copyright Act ("DMCA")

數位形式的受著作權保護作品不斷增加，帶來一項重大挑戰：個人可以廉價的數位媒介（如 CD-R、DVD、電腦硬碟等）輕易地複製出受保護作品的完美但未經授權的重製品。權利擁有者嘗試保護其作品免受此類盜版侵害的方法之一，是將保護程式內嵌到數位作品中，以此來控制用戶使用或複製作品的能力。上述的 1998 年 "數位千禧年著作權法" 有助於支援這些保護措施，方法是以刑法處罰妨礙使用控制機制的行爲，以及使用或銷售設計用以妨礙使用和複製控制機制的裝置（如果行爲目的是商業利益或私人財務得益）。美國制定此項法令的目的之一是依據 "世界智慧財產權組織著作權條約" 第 11 條的要求實現美國之義務。該條款規定各簽約方必須 "提供足夠的法律保護和有效的法定補償來對抗妨礙有效科技保護措施之行爲，該等科技保護措施係作者使用來實現其在本條約下之權利。 ....."

A major challenge presented by the ever-increasing availability of copyrighted works in digital formats is the ease with which individuals can make perfect, unauthorized copies of protected works with inexpensive digital media, such as CD-Rs, DVDs and computer drives. One way in which rights holders have attempted to protect themselves from such piracy is to embed their digital works with protections that control the ability of users to access or copy the works. The Digital Millennium Copyright Act of 1998, discussed above, helps preserve these protections by criminalizing the act of circumventing access controls and the use or sale of devices designed to circumvent access and copy controls, when done for purposes of commercial advantage or private financial gain. The United States enacted this statute in part to fulfill its obligations under Article 11 of the World Intellectual Property Organization Copyright Treaty, which requires contracting parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty . . . ."

決定是否起訴
Deciding Whether To Bring A Prosecution

司法部決定是否刑事起訴取決於多種不同的考量，視各個特定案件的事實和情況而定。但一般來說，在民事補償不足以阻止侵權活動或補償受害者的損害，且侵權行爲是故意行爲之案件中，刑事起訴是恰當的。比方說，如果侵權行爲是一個有組織的犯罪企業進行的，民事懲罰對其沒有遏止效果，而他們也只將這種懲罰當作商業成本而已；或者，如果侵權活動對大衆的健康和安全造成重大威脅（例如，僞造的飛機零件、汽車電池或機器之類商品）；或者，如果這是大範圍的侵權行爲，因而造成權利擁有者巨大的損害；在這些情況下，政府可能選擇刑事起訴而不是依靠民事補償來解決問題。

The Department of Justice's decision to bring a criminal prosecution rests on a variety of considerations that depends on the facts and circumstances of each particular case. In general, however, criminal prosecution is appropriate in those cases where civil remedies are inadequate either to deter the infringing activity or to remedy a victim's injuries, and where the infringement is intentional. For example, if the infringement is conducted by an organized criminal enterprise that is undeterred by civil penalties and views such penalties as a mere cost of doing business, or if the infringing activity poses a serious threat to the health and safety of the public (as with such goods as counterfeit airplane parts, car batteries, or medicines), or if the infringement is conducted on a massive scale causing significant harm to the rights holder, the government may choose to prosecute the case criminally rather than rely on civil remedies to address the problem.

當政府決定提出刑事起訴時，並不需要得到受害者或權利擁有者的許可；相反地，政府可以自行決定起訴這樣的案件。儘管如此，在智慧財產權侵害罪的調查和起訴這兩項工作中，政府可能（也經常）需要依賴權利擁有者的協助。這和民事案件不同。在民事案件中，權利擁有者只需要“優勢證據”來證明其權利受到了侵害；但在刑事起訴中，政府必須“高出合理可疑”（這是更嚴厲的證據標準）地證明構成所有構成要件。

When the government decides to bring a criminal prosecution, it does not require the permission of the victim or rights holder to do so and, instead, may bring the prosecution on its own initiative. Nevertheless, the government may (and often does) rely on rights holders for assistance in both the investigation and prosecution of intellectual property crimes. Unlike civil cases, in which the rights holder need only prove by "a preponderance of the evidence" that his rights have been infringed, the government, in a criminal prosecution, must prove all elements of the crime of infringement "beyond a reasonable doubt," which is a more exacting standard of proof.

對侵害智慧財產權罪判刑
Sentencing for Intellectual Property Crimes

在美國，對所有聯邦罪的判刑都受到 1984 年“量刑改革法” 的管制。旨在確立量

刑時的公平性、均衡性和確定性的“判刑改革法”，要求制定強制性的“量刑準則”(Sentencing Guidelines)，以限制聯邦法官在量刑時的自由裁量。這些在1987年首次發佈並定期更新和修訂的“量刑準則”考量每個聯邦罪行的所有相關因素，並且根據被懷疑犯罪人的特性指定一個判刑範圍，若無特殊情況，法官必須在此範圍內作出選擇。

Sentencing for all federal crimes in the United States is governed by the Sentencing Reform Act of 1984. The Sentencing Reform Act, which was intended to establish fairness, proportionality, and certainty in sentencing, called for the creation of mandatory "Sentencing Guidelines" that limit the discretion of federal judges in meting out punishments for crimes. These "Sentencing Guidelines," which were first issued in 1987 and are updated and revised regularly, take into account all relevant factors for each federal crime and, based on the characteristics of the offense conduct in question, prescribe a sentencing range within which the judge must choose, absent exceptional circumstances.

如同所有聯邦罪，依據“量刑準則”對侵害智慧財產權的被告的判刑範圍也會受到特定罪行之各種特徵的影響。特別是侵權的金額價值對量刑的範圍有很大影響。也就是說，在大部分案件中，罪行的判定會以受侵害的合法商品其零售價值來決定，而不是以侵權商品的價值來計算。如果侵權行爲牽涉到製造、進口或上載侵權，或者如果犯罪的目的是利益或商業收益，則刑罰也會提高。其他影響判刑範圍的因素包括：被告在共謀或有組織犯罪企業中扮演領導角色的程度、罪行是否涉及妨礙安全措施或其他特殊技能、被告是否對其行動表示負責等等。

As with all federal crimes, the range of a defendant's sentence for intellectual property infringement under the Sentencing Guidelines will be affected by a variety of specific offense characteristics. In particular, the extent of the sentence is substantially affected by the infringement amount, which is, in most cases, determined by the retail value of the legitimate goods that have been infringed rather than by the value of the infringing goods. The sentence will also be increased if the infringement involved the manufacture, importation, or uploading of infringing items, or if the offense was committed for purposes of profit or commercial gain. Other factors affecting the sentencing range include the extent to which the defendant played a leadership role in a conspiracy or organized criminal enterprise, whether the offense involved circumvention of security measures or other special skills, and whether the defendant demonstrates an acceptance of responsibility for his actions.

執行智慧財產權刑事法是司法部的重要任務
Criminal Intellectual Property Enforcement Is A Department of Justice Priority

司法部已將執行智慧財產權刑事法當成一項優先任務。司法部投注了大量的資源來訓練專門的檢察官，並制定積極的起訴策略來處理不斷增長的盜版和高科技犯罪威脅。司法部確保分佈全美國的九十四個美國檢察署都聘用了專長於此方面的檢察官，而且定期對他們進行電腦和智慧財產權罪起訴訓練。在過去兩年中，司法部在十二個高科技和智慧財

產權犯罪尤其受到注意的檢察署，建立或擴大了“入侵電腦系統和智慧財產權”單位。這些單位由許多專長處理電腦和智慧財產權犯罪的專業檢察官團隊組成，這些檢察官的專業知識有助於司法部跟上在時刻變化中的高科技犯罪性質的步伐。

The Department of Justice has made the criminal enforcement of intellectual property rights a high priority. The Department has committed substantial resources to training specialized prosecutors and developing aggressive prosecution strategies to deal with the growing threat of piracy and high-tech crime. The Department ensures that each of the ninety-four (94) United States Attorney's offices throughout the United States employs prosecutors who specialize and are regularly trained in the prosecution of computer and intellectual property crimes. In the past two years, the Department established or expanded Computer Hacking and Intellectual Property units in twelve United States Attorney's offices nationwide where high-tech and intellectual property crimes are of particular concern. These units are teams of specialized prosecutors focused primarily on computer and intellectual property crimes whose expertise helps the Department of Justice keep pace with the constantly changing nature of high-tech crime.

在位於首都華盛頓的司法部總部有一個“電腦犯罪與智慧財產權處”(CCIPS)，這個辦公室有四十名律師，專門處理電腦與智慧財產權犯罪。CCIPS 的律師起訴網路犯罪和智慧財產權案例、爲其他檢察官和調查人員提供智慧財產權法及搜查和查扣電腦方面的建議和訓練、協調國際執法單位，並擴大努力來打擊世界性的智慧財產權和電腦犯罪，並對新的立法案提供意見和提議。CCIPS 的律師已經與其他國家成功地協調國際性起訴跨越邊界的網路和智慧財產權犯罪，並且定期參與旨在改進對此類全球犯罪的國際性起訴合作的努力。

At its headquarters in Washington, D.C., the Department of Justice maintains its Computer Crime and Intellectual Property Section (CCIPS), an office of forty (40) lawyers who focus exclusively on computer and intellectual property crime. CCIPS lawyers prosecute cybercrime and intellectual property cases, advise and train other prosecutors and investigators in matters such as intellectual property law and searching and seizing computers, coordinate international enforcement and outreach efforts to combat intellectual property and computer crime worldwide, and comment on and propose new legislation. CCIPS lawyers have successfully coordinated international prosecutions of trans-border cyber and intellectual property crimes with other countries and are regularly engaged in efforts to improve international cooperation in prosecuting such crimes worldwide.

司法部與許多執法機構合作調查有關智慧財產權的刑事違法行爲。這些機構包括聯邦調查局 (FBI)、新成立的國土安全部下的移民和海關執行署 (ICE)、美國特工處以及美國郵政部。FBI 和 ICE 這兩個單位內都有專門處理高科技和電腦犯罪（包括智慧財產權罪）的專業部門，這些部門對於數位時代的智慧財產權罪的調查工作提供極其重要的專業知識。

The Department of Justice works with several law enforcement agencies to investigate criminal violations of intellectual property laws. Those agencies include the Federal Bureau of

Investigation (FBI), the Bureau of Immigration and Customs Enforcement (ICE) within the newly-formed Department of Homeland Security, the United States Secret Service, and the United States Postal Service. Both the FBI and ICE have specialized units within their agencies that are dedicated to high-tech and computer crimes, including intellectual property crimes, that provide critically important expertise in investigations of intellectual property crimes in the digital age.

司法部同時也是美國政府一個名爲“全國智慧財產權法執法協調委員會”的多機構組織的共同主持單位之一。該組織的宗旨在於確保在美國政府在國內外智慧財產權執法的協調合作。除了司法部，成員單位還有美國專利和商標局（也是該組的另一個共同主持單位）、國務院、美國貿易代表辦事處、海關委員會和商業部。

The Department of Justice also serves as co-chair of a multi-agency organization of the United States government known as the "National Intellectual Property Law Enforcement Coordination Council." The purpose of this organization is to ensure a coordinated, U.S. government-wide approach to intellectual property law enforcement both domestically and abroad. Along with the Department, the organization consists of the United States Patent and Trademark Office (which is the other co-chair of the group), the Department of State, the office of the United States Trade Representative, the Commissioner of Customs, and the Department of Commerce.

代表性起訴案例
Representative Prosecutions

海盜行動 (Operation Buccaneer)：
Operation Buccaneer:

2000 年 10 月，美國司法部的電腦犯罪與智慧財產權處 (CCIPS) 和美國海關（現爲“移民和海關執法署”）合作，開始一項代號爲“海盜行動”的調查行動，調查目標是大型、國際性線上侵害著作權陰謀。這項陰謀活動是從所謂的“warez scene”產生的，這是網路上的地下文化。在此地下文化中，組織完善的群組會關閉（或“破解”）軟體、電腦遊戲以及數位化電影和音樂的著作權保護裝置，然後將作品的無限量地透過網路傳送到世界各地。Warez 群組彼此互相競賽，欲成爲第一個將最新數位作品“破解”版本發行到 warez scene，這種情況通常在作品尚未在市面上商業化提供以前就出現了。一般來說，warez scene 的成員參與這一活動並不是爲了獲得財務上的利益，而是爲了享有第一個發行特定作品的盛名，以及能夠不付款而得到其他盜版作品的能力。

In October 2000, the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice, together with the U.S. Customs Service (now called the Bureau of Immigration and Customs Enforcement), commenced an investigation code-named "Operation Buccaneer," which targeted a massive, international online copyright piracy conspiracy. The conspiracy arose from the so-called "warez scene," an underground culture on the Internet in which highly organized groups disable (or "crack") copyright protections on software, computer games,

and digitized movies and music and then distribute virtually unlimited copies of those works worldwide over the Internet. Warez groups compete against each other to be the first to release "cracked" versions of the most recent digital works into the warez scene, often before those works are commercially available. Typically, members of the warez scene engage in this activity not for financial profit, but for the prestige of being the first to release a particular work, and for the ability to obtain other pirated works without payment.

2001 年 12 月 11 日，作爲"海盜行動"的一部分，美國各個執法機構以及其他五個國家分別在各自的國家同步進行七十多個電腦和其他數位證據的搜查和查扣行動。這項國際合作執法行動結果共沒收 150 多台電腦系統，其中包含成千上萬份軟體、電影、音樂和電腦遊戲的盜版。由於此現在仍在持續進行中的調查，某些最高階層的 warez 群組中，已有二十五個成員已被判決觸犯重大著作權侵害罪，其中九名已被量處 33 到 46 個月之間不等的有期徒刑。這是有史以來對網路著作權盜版罪所判處的最長徒刑。

On December 11, 2001, as part of Operation Buccaneer, law enforcement agencies in the United States and five foreign countries conducted more than seventy (70) simultaneous searches and seizures of computers and other digital evidence in each of their respective countries. This coordinated international law enforcement action resulted in the seizure of over 150 computer systems containing tens of thousands of pirated copies of software, movies, music and computer games. As a result of the investigation, which remains ongoing, twenty-five (25) members of some of the highest-level warez groups have been convicted of felony copyright crimes, nine of whom received prison sentences of between 33 to 46 months, the longest sentences ever imposed for Internet copyright piracy.

美國 v. Mynaf (United States v. Mynaf)：
United States v. Mynaf:

2003 年 2 月 13 日，加州的 Mohsin Mynaf 因違反多項與著作權有關的法律（包括違反"數位千禧年著作權法"、著作權刑事法和交易仿冒標簽）而被判處監禁在聯邦監獄二十四個月。Mynaf 經營一家錄影帶複製中心，該中心製造了數千卷仿造的電影錄影帶，然後 Mynaf 在加州許多不同地點出售這些錄影帶。除了二十四個月的徒刑外，還規定 Mynaf 支付 20 萬以上美元來賠償受害者。另有三人因協助和煽動 Mynaf 進行非法活動也已被定罪，在等候判刑中。

On February 13, 2003, Mohsin Mynaf of California was sentenced to twenty-four (24) months in federal prison for multiple violations relating to copyright, including Digital Millennium Copyright Act violations, criminal copyright infringement, and trafficking in counterfeit labels. Mynaf operated a videocassette reproduction center that produced thousands of counterfeit movie videocassettes, which Mynaf would then sell at various locations throughout California. In addition to twenty-four (24) months in prison, Mynaf was also required to pay in excess of $200,000 in restitution to the victims. Three other individuals have also been convicted of aiding and abetting Mynaf in his illegal activity and are awaiting sentencing.

美國 v. Min Zhu (United States v. Min Zh)；美國.v. Qiuhui Huang (United States v. Qiuhui Huang)：
United States v. Min Zhu; United States v. Qiuhui Huang:

2003 年 2 月 7 日，紐約的 Min Zhu 和 Qiuhui Huang 被逮捕，並被指控將價值 20 多萬美元的仿造 Louis Vuitton 手提包透過網路拍賣網站 "eBay" 和 "Yahoo!" 賣給全國各地數百名受害者。這兩人各被指控共謀郵件詐欺和仿冒商標，二人各面臨最高二十 年徒刑和 25 萬美元罰款。

On February 7, 2003, Min Zhu and Qiuhui Huang of New York were arrested and charged with selling more than $200,000 worth of fake Louis Vuitton handbags to hundreds of victims across the country through auctions on the Internet auction sites "eBay" and "Yahoo!" Each individual was charged with conspiracy, mail fraud and trademark counterfeiting, and each faces a maximum sentence of twenty (20) years in prison and a $250,000 fine.

美國 v. Nguyen (United States v. Nguyen)：
United States v. Nguyen:

2002 年 10 月，加州的 Tony Minh Nguyen 因製造和交易仿冒 Compaq 電腦記憶體模組而被聯邦起訴並逮捕。根據起訴書，Nguyen 是總部設在加州的一家電腦公司內負責銷售和生產的主任，他指示員工購買過時的 Compaq 記憶體元件，取下元件中的 Compaq 標簽。然後，Nguyen 讓員工將那些 Compaq 標簽又粘貼到非 Compaq 的元件上，創造出外觀幾乎無異於 Compaq 產品的產品。最後，Nguyen 指示員工將這些僞造的零件當真品銷售。Nguyen 面對高達二十 年的徒刑和最高 4 百萬美元的罰款。

In October 2002, Tony Minh Nguyen of California was arrested on federal charges of manufacturing and trafficking in counterfeit Compaq computer memory modules. According to the indictment, Nguyen, a director of sales and production at a California-based computer company, instructed his employees to purchase out-of-date Compaq memory components and remove the Compaq labels from those components. Nguyen then had his employees re-adhere the Compaq labels to non-Compaq memory components, creating a product that would be substantially indistinguishable in appearance from genuine Compaq products. Ultimately, Nguyen directed his employees to sell these counterfeit parts as the genuine article. Nguyen faces a maximum penalty of twenty (20) years in prison and a fine of up to $4 million.