出國報告（出國類別：進修）

# 有關打擊網路犯罪（Cybercrime）法制及國際合作之研究

服務機關：臺灣桃園地方檢察署

姓名職稱：朱哲群檢察官

派赴國家：美國喬治城大學

出國期間：**108** 年 **8** 月 **14** 日至 **109** 年 **3** 月 **30** 日

報告日期：**109** 年 **6** 月 **30** 日

# 摘要

首先，本文將網路犯罪定義為犯罪行為部分或全部涉及使用網際網路之犯罪；其次，以此為基礎蒐集、摘要美國網路犯罪相關判決，並就其相關部分，與我國近期議題：雲端扣押（中華電信 hiBox、楓林網）案件進行比較；網路的出現將國家的邊界模糊化，同時也衍生司法權如何跨境實現的議題，則為本文最後探討之議題。

## 目錄

# 出國報告（出國類別：進修）

## 第一章 前言

### 第一節 目的

筆者於 2019 年獲法務部選派至美國喬治城（Georgetown）大學法學中心進行訪問，研究主題為「有關打擊網路犯罪（Cybercrime）法制及國際合作」。

喬治城大學位於美國首都，即東岸的哥倫比亞特區（District of Columbia），中文世界俗稱華府。華府為美國政治中心，受惠於此，美國三權分立機構－國會、白宮、最高法院－均設立在特區內，喬治城大學因此擁有關注政治及法律議題的第一手資源。最高法院離法學中心步行約十五分鐘可抵達，該校法學院學生在學時，多半以至少要進入大法庭一次聆聽言詞辯論為目標。若遇上熱門議題例如槍枝、墮胎、性別平等，必須要清晨排隊領取號碼牌，甚至前一夜就攜睡袋在外搭帳棚，等待進入大法庭的機會。這都是喬治城法學中心地理位置得天獨厚的緣故。

美國於十七世紀初期成為歐洲殖民地，各殖民地原本即有一定程度的自治權限，在獨立後雖成立聯邦政府，但仍保有其領域內的高權，這項歷史背景使美國國內司法系統分為州及聯邦層級，聯邦法院原則上需要尊重各州法律。美國司法採用普通法（common law）體系，注重個案之背景事實及判決先例（precedent）；加上美國領土幅員廣大，其國內有五十州、哥倫比亞特區，已有五十一套州司法系統，再疊加上聯邦司法系統，繁複程度，不言自明。例如，哥倫比亞特區相較於其他州幅員狹小，因此司法制度設計上只有兩個審級，即 Superior Court（即地方法院）、Court of Appeal（即上訴法院）。但這也代表在美國不同地域的司法案件，因應各地不同的歷史、文化、經濟、法律，帶來不同的

思考，讓想法相互衝擊，經過辯證得出結論。

本文研究方向擬蒐集美國法院有關網路犯罪的判決，一窺美國司法實務上在處理網路犯罪時是如何辯證，並且導入更多技術相關議題，強化法律與技術的連結，作為我國司法系統處理類似案件時之借鏡。

## 第二節 過程

筆者於 2019 年 8 月底抵達法學中心，陸續完成訪問學者註冊、資料庫申請、圖書館登記、識別證核發，可以使用法學中心大部分資源。抵達時是喬治城大學的秋季學期，為完成研究主題，擬定第一學期先初步瞭解美國司法系統，後續再進一步延伸。第一學期有幸旁聽 Craig Hoffman 教授開設的 Introduction to U.S. Legal System；同時也旁聽與研究主題高度相關、由 Mike Songer 教授講授的 Law of Cyberspace。在聖誕假期結束後，第二學期原先有意旁聽 Paul Ohm 教授開設的 Computer Programming for Lawyers，因為在臺灣未曾聽過法學院有程式設計的課程，筆者認為可以作為我國法學教育或法律實務的借鏡。可惜該課程額滿且需要大量實作，無法如願以償，是本次訪問的遺憾之一。後來筆者選定 Thomas Kellogg 教授的 China and International Law、John Facciola 教授的 Evidence 課程進行旁聽，深感收穫豐富，可惜遇上武漢肺炎疫情大流行，美國成為重災區疫情嚴重，筆者提早於 2020 年 3 月結束訪問返國，未能跟完完整的學期課程，是本次訪問的遺憾之二。

# 第二章 網路與犯罪

## 第一節 網路空間[1]

網路空間（cyberspace）[2]的概念是從科幻小說作家 William Gibson 開始流行，他在作品內描述全球的電腦網路創造出一個新世界，是每個國家數十億網路參與者每天共同經歷的一致幻覺，而這股幻覺僅是由具有數學概念的人們所建立。網路空間的「空間」使法律的論述披掛上了一層長遠的陰影，尤其是談論到審判權（jurisdiction）的時候。如果橫跨地球的兩個人可以同步且深刻地互動，或許稱他們的互動是在網路空間發生而非在任何一個他們所處的國家，更為合理。如此的話，特別發展出適用不同物理、領域觀念的網路法，以供實體世界遵循，是一個更妥適的選擇。

## 第二節 網路的發展趨勢

傳統上對於電腦的理解，是可以接受指令或資料，以處理器運算分析，再將結果輸出的電子裝置，我們強調個別電腦的運算能力，不必然須與網路產生連結。但從蘋果公司 2007 年發表第一代 iPhone 以後，智慧型手機／設備的需求如雨後春筍，成長迅速，而行動裝置的特色在於需要與網路連結發揮其最大效用，諸如電子郵件、通訊軟體、社群媒體、影音串流、雲端空間、物聯網（Internet of Things），無一不需要透過網路才能使用上述服務。以臺灣為例，行動通訊數據傳輸量在 2018 年第

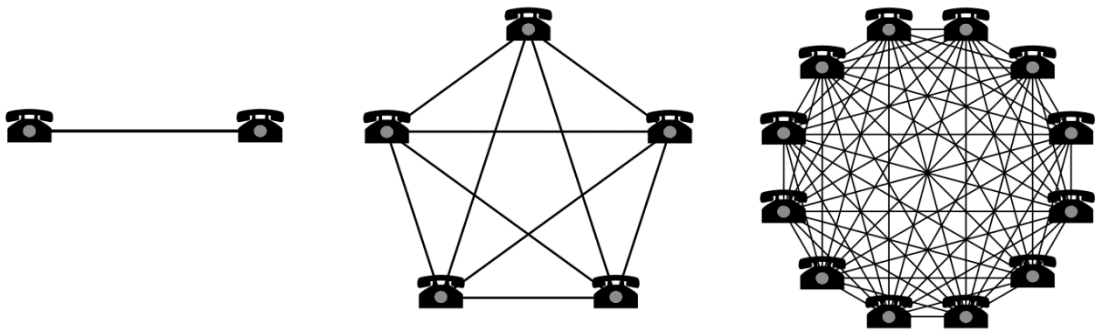
[1] James Grimmelmann, Internet Law: Cases & Problems(9th Edition) 53-54 (2019)

[2] 在英文中 Internet 偏向指涉電腦裝置間的連結能力，Cyberspace 則偏向指涉網民在網路中構築的世界，但現在鮮少有人細緻區分這兩個概念，不論講到 Internet 或 Cyberspace，多半都是指連上網路與他人互動或使用服務。而在中文脈絡下，網路世界／網路空間／網路同樣也難以區分。本文使用「網路空間」是照字面翻譯，不過將它代換成「網路世界」或「網路」，理解上並沒有多大區別。

2 季是 1,199,704.6 Tbytes，但在 2019 年第 2 季時已成長至 1,504,467.5 Tbytes，一年內的成長幅度高達到百分之二十五。[3]由此可見民眾對網路的需求以及深入日常生活的程度。

另外，電腦／行動裝置適用所謂的網路效應（Network Effects），即產品或服務（以下簡稱產品）的價值將會隨著使用者的增加而擴大。簡單的說，就是越多人使用越好。越多人使用同樣的產品，消費者越容易黏著在該產品上，創造更多與他人—不管是實體或者虛擬—的交流機會。如果從預防或偵辦犯罪的角度來看，網路世界建立起複雜的人際關係，也必定隱含或孕育著更多犯罪產生的可能性。質言之，現在如果討論電腦犯罪時，沒有納入當代社會背景，思考網路與電腦如影隨形的連結性，即可能在研討議題時失去大方向。故本文有意排除單純針對離線（off-line）電腦所為的犯罪行為。

圖 1：網路效應示意圖



資料來源：https://en.wikipedia.org/wiki/Network_effect，最後瀏覽：2019/11/11。

## 第三節 網路犯罪的定義

下一個問題是，什麼是網路犯罪？散布病毒破壞作業系統

3 國家通訊傳播委員會，2019 年第 2 季行動通訊市場統計資訊，【線上資料】，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=3773&cate=0&keyword=&is_history=0&pages=0&sn_f=42069，最後瀏覽：2019/11/6。

（operating system），讓你再也無法開機？利用系統在你的電腦植入木馬程式，藉機側錄資料或監視你的一舉一動？使用軟體綁架硬碟，讓你無法開啟重要檔案，以此勒索贖金？或者根本與專業技術無關，在社群網站上誹謗他人？上傳盜版音樂？以虛擬貨幣購買毒品都算是？在理解上，大致可以將網路犯罪區別為①構成要件本身與網路有關，②違反犯構成要件時使用到網路，本文認為前者需要對於科技有一定程度之詮釋及理解，而後者則是傳統犯罪以嶄新手段違反。舉例而言，前者例如：美國聯邦法典集 Title 18 犯罪及刑事訴訟程序（Crimes and Criminal Procedure）§ 2421(a)規定：任何人利用州際間或外國公司的設備、方法，或在該公司內或發揮影響力，擁有、管理、經營互動電腦服務或陰謀或嘗試，意圖行銷或促使與他人的性交易，應被科以罰金、十年以下有期徒刑或兩者兼具。[4]從條文中使用的「互動電腦服務」，可以窺見網路存在的身影。後者例如，例如前述法典集 Title 18 § 875(b)：任何人意圖敲詐他人、事務所、組織、公司金錢或其他有價事物，在州際間或對外國公司傳送任何包含對他人的綁架威脅或傷害威脅的通訊，應被科以罰金、二十年以下有期徒刑或兩者兼具。[5]條文中規定的「傳送（transmit）」，解釋上可以是透過信件、電話，或者是使用網際網路。

如前所述，本文目標是介紹美國與網路有關之案例及其背後議題，不侷限而囊括上開兩者，將「網路犯罪」定義為：犯罪行為部分或全部

[4] 18 U.S.C. § 2421(a)

Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, owns, manages, or operates an interactive computer service (as such term is defined in defined in [1] section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f))), or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person shall be fined under this title, imprisoned for not more than 10 years, or both.

[5] 18 U.S.C. § 875(b)

Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than twenty years, or both.

涉及使用網際網路之犯罪。

## 第四節 網路犯罪的特性

如本文定義，「網路犯罪」係犯罪行為部分或全部涉及使用網際網路之犯罪。如同現實世界保護不同法益所規制的不同罪名，想當然爾，涉及網路的犯罪類型也多如繁星，我們很難擘畫出全面性的特質來描述各種網路犯罪，每種網路犯罪都應有其著重的特點。例如侵害著作權（copyright）的犯罪，我們可能思考民眾觀看未授權影音的串流播放（streaming）是否該當重製、散布，判斷時側重其背後的技術架構，反而網路帶來的人際互動特質並不重要。但無論如何，一旦你使用電腦設備進入了網路世界，你的一舉一動必然電子化而留下數位足跡，不論這些數位足跡是儲存在自己或他人的硬碟當中。從數位足跡，也就是凡走過必定留下痕跡的觀點出發，本文引用以下四種特性：①持續性、②可見性、③擴展性、④可搜尋性[6]來描述網路犯罪的特性。

### 第一項 持續性（persistence）

持續性係指線上表達及內容的耐久性。[7]透過社群媒體傳送的內容通常是恆存的，因為在設計時就考量技術上的持續性，如此才能達成非同步的交流。例如 Alice 在半夜時傳送訊息給 Bob，Bob 隔天早上起床後或就算外出三週後回來，Bob 仍然可以看到 Alice 傳送的訊息，就算 Alice 已經忘了這件事了。持續性意味著透過社群媒體的對話，不再如現實世界一般稍縱即逝，是恆久的，使不同種類的線上互動不僅是短暫的過客。我們可以這麼說，使用者在網路／社群媒體留下的「紀錄」，多到一個前所未有的境界。

---

[6] Danah Boyd, *It's complicated : the social lives of networked teens*, 10-13(2014).

[7] "the durability of online expressions and content." *id*. at 11.

## 第二項 可見性（visibility）

可見性係指見證的潛藏觀眾數量。[8]透過社群媒體，人們可以簡單地向群眾分享，且即使他人與你身處遙遠，你也可以輕易地得知他人的生活，這增加了特定訊息的可見性。更有甚者，人們放在社群媒體上的訊息將被他人輕易的知悉，因為大部分的系統設計上是預設分享給多數人或公開訊息，反而是要求使用者採取積極措施去限制他人對你訊息的閱聽。這點即與實體世界大不相同，在實體世界要想方設法才能讓你的想法呈現在相當數量的觀眾面前。在網路世界，與人互動是預設立場，保持隱私是努力。

## 第三項 擴展性（spreadability）

擴展性係指內容被分享的簡易度。[9] 社群媒體經常被設計成鼓勵使用者傳播訊息，不論是明示或暗示，方法有：連結分享、提供轉載功能轉發文字或圖片、簡化複製貼上流程。因此，使用者在網路上的發文，只要簡單敲擊幾個鍵盤指令，就會散播出去。有些系統會提供簡明的按鈕讓你「轉傳」、「重發」、「分享」文章，針對內容評論或者儲存，就算沒有前述功能，你也可以輕易的複製、下載並單獨轉發出去，這種人們在網路上分享訊息的日常簡易性是無所匹敵的，但同時可能是有威力的及有問題的。擴展性可以是人民政治上團結的利器，也可以是散播謠言的溫床。

## 第四項 可搜尋性（searchability）

可搜尋性係指能夠在網路上找到內容。[10]由於搜尋引擎的興起，人們的傳訊內容通常可以搜尋得到。任何好奇的人都可以查詢資料庫，揭

[8] "visibility: the potential audience who can bear witness." *id*.
[9] "the ease with which content can be shared" *id*.
[10] "the ability to find content." *id.*

開數不盡有關他人的八卦，不論是他人親自發文或第三人的評論。就算一篇文章本來就是規劃在網路上公開，但這不代表發文者有被搜尋引擎以想不到的方式重現文章的意思。搜尋引擎使得原本深思熟慮的網路互動表面化了，因為它們為了迅速找到相關結果，被設計成除去繁雜的背景因素，增加搜尋者只取所需而不考慮前後文的可能性。

# 第三章 美國網路犯罪

## 第一節 無故使用電腦

### 第一項 未經授權的解讀[11]

雖然未經授權存取的法規提及「授權（authrorization）」，彷彿它是一個片段的概念，但在事實上，對電腦未經授權的「存取（acess）」或「使用（use）」有兩條清楚區分途徑。每一種型式對應到電腦的擁有者得以如何規範使用者權限，電腦擁有者可以透過密碼或契約規範使用者權限；同樣地，電腦使用者涉及電腦濫用（misuse）也將以規避密碼基礎的限制，或違反契約基礎的限制呈現。

當擁有者以密碼規範權限，擁有者或其代理人將程式編碼，如此一來，特定的使用者只能在電腦上有一組限制的權限。舉例來說，擁有者可以要求每個使用者開立帳號且設定獨特的密碼，並在每個帳號指定不同的權限，以此為基礎限制每個使用者能造訪什麼部位、做什麼事情。若使用者有超出密碼所賦予的權限，這位使用者必然某種程度上欺騙電腦使得電腦給予使用者更高權限。本文將此種方法分類為密碼規範（regulation by code），因為這種方式依靠電腦密碼建立障壁，阻止使用者有超出他所屬網路的權限。

如果要規避密碼規範，通常使用者會陷入兩種的電腦濫用型式之一。首先，使用者必須使用假身份（false identification）偽裝成擁有更高權限的另一位使用者。舉例來說，使用者可以用另一個人的密碼，欺騙電腦賦予使用者更高的權限，這些高權限本來應該保留給真正的帳號擁有者。如果 A 知道 B 的帳號跟密碼，A 可以登入 B 的帳號並且見

[11] Orin S. Kerr, Cybercrime's scope Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U L. Rev. 1596, 1644-1645, 1649-1650 (2003)

到只有 B 被授權的資訊。

另外，使用者可以利用程式內密碼的弱點，授予使用者更高的權限導致程式管控失能。現在介紹一種所謂緩衝區溢位（buffer overflow）攻擊，這是常見的駭入電腦方式。緩衝區溢位攻擊使得被害者電腦的記憶體緩衝區過度負載，迫使電腦失能並重設成開放給使用者根（root）或高級使用者權限，將導致攻擊者取得對被害電腦的全面控制。有了根權限，攻擊者可以存取任何帳戶跟刪除任何檔案。這種攻擊方式成功規避了密碼對使用者施加的限制…。

第二種擁有者可能會嘗試的路線，是以契約規範（regulation by contract）電腦權限。擁有者可以有條件的開放使用電腦，只要使用者同意遵循某些規則。如果使用者與擁有者／操作者有什麼先存關係，通常是兩者間已有服務條款（Terms of Service）。如果沒有這層關係，那麼多半是以使用條款（Terms of Use）的方式呈現，像是在進入網站前瀏覽確認（click-through）的同意。舉例而言，成人網站要求使用者保證他在存取網站的成人內容時，已經年滿十八歲。最後，這些限制或許是相對隱晦的，並沒有明列在文字當中。

契約規範是一種遠較密碼規範脆弱的管制型式。密碼規範強行阻絕使用者執行被禁止的行為，至少，在沒有被規避的前提之下。作為對比，契約規範則是以一種榮譽系統運作，或者更精確一點，這套榮譽系統以契約法的救濟制度背書。思考成人網站要求使用者表明在進入網站之前已經至少年滿十八歲。一個十七歲的少年要進入網站根本就跟十八歲以上成年人一樣容易，唯一的差別是十七歲少年需要對網站虛偽陳述年齡以進入網站。用一個實體世界的例子類比，密碼規範跟契約規範的差異就像是，讓一個陌生人無法進入屋內，前者是關上跟鎖住門以阻絕陌生人，後者是在一個開放的門前放置標誌，寫著「陌生人勿

入」。

更重要的，契約規範跟密碼規範之間的區別，與其說是一種啟動／關閉的開關，不如說是兩種極端情形的連續狀態。混合兩種概念的例子是存在的。比方說，電腦擁有者設立看似需要帳號、密碼才能存取內容的網站，但實際上你能以任何帳號、密碼組合進入網站。這類網站乍看之下是對使用者進行密碼規範，實際上卻比較像契約規範的系統。然而，在大部分例子裡，電腦擁有者的權限規範無法相對清楚地歸類為密碼規範或契約規範。

問題是，哪種型式足以被確立為未經授權存取？我提議法院應將未經授權存取限制在規避密碼規範。違反契約規範是一項法律議題，但不足以作為有未經授權存取的立論。換句話說，法院應該排除契約基礎的授權理論…。建構未經授權存取，而將規避密碼障礙、違反契約兩者同時納入，是在錯誤的地方劃上界線，這將賦予電腦擁有者過大的權力規範網路使用者做什麼、怎麼做，犧牲不計其數的自由，卻只在隱私及安全上換回些許甚至虛無的回報。

## 第二項 UNITED STATES V. NOSAL[12]

### 壹、背景事實

電腦已經成為我們日常生活不可或缺的一部分。我們用來工作，用來娛樂，有時候我們在工作中用來娛樂。許多雇主採行禁止非公務使用電腦的政策。如果一位員工，違反這項政策即觸犯聯邦刑法？如果是社群網路網站的使用者違背服務條款？這取決於我們解讀 Computer Fraud and Abuse Act（CFAA, 18 U.S.C. § 1030）多廣泛。

David Nosal 過去在 Korn/Ferry 工作，一間執行搜尋公司。很快地

[12] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

在他離開公司以後，他說服還在職的前同事，Becky Christian 跟 Mark Jacobson，協助他開設一間同性質的競爭公司。在職員工用他們自己的登入權限，從公司電腦機密資料庫中下載來源清單、姓名、聯絡訊息，然後將這些資訊轉傳給 Nosal。在職員工有權限登入存取資料庫，但是 Korn/Ferry 有一項政策是禁止外傳這些機密資訊。

政府起訴 Nosal 二十項罪名，包括竊取營業祕密、郵件詐欺、陰謀及違反 CFAA。CFAA 罪名控訴 Nosal 違反 18 U.S.C. § 1030(a)(4)，認為他幫助及教唆 Korn/Ferry 員工意圖詐欺逾越授權存取。

## 貳、法律議題

CFAA 定義逾越授權存取為：未經授權存取電腦，利用該存取獲得或修改電腦內資訊，而存取者未有如此授權獲得或修改（18 U.S.C. § 1030(e)(6)）。這段文字可以從兩個方向解讀：首先，如同 Nosal 的抗辯及地方法院的結論，可以解讀成某人只有存取特定資料或檔案的權限，但卻存取未經授權的資料或檔案—俗稱的駭解（hacking）。比方說，假設員工只有權限存取公司電腦內的產品資訊，但是卻存取顧客資料，則他如果瀏覽顧客名單時構成逾越授權。又或者如同政府主張，文字可以解讀成，某人實體上近用電腦沒有限制，不過侷限在他所能處理資訊的目的內。比方說，員工因為工作需要存取顧客名單，但不能將名單寄給競爭對手。

CFAA 受到政府寬廣的解讀，然而，我們認為 Nosal 的狹義版本更有說服力。國會於 1984 年頒布 CFAA 主要是為了解決日漸嚴重的電腦駭客問題，並認知到故意侵踏他人電腦內檔案的入侵者，至少獲得如何破解電腦系統的訊息。政府同意 CFAA 與電腦駭解有關，這也是為什麼該法禁止未經授權的存取電腦。依照政府的說法，這道禁令著重於駭

解電腦，這也是為什麼法律禁止未經授權存取電腦的原因。接著政府指出，這道禁令適用於駭客，所以「逾越授權存取」禁令必須適用於被授權使用電腦、但卻以未經授權目的使用的人們。然而，對於適用駭客禁令的解讀也可能是：未經授權只適用於外部駭客（從未被授權存取電腦的個人），逾越授權存取則適用於內部駭客（初始存取電腦經授權但取得未經授權資訊或檔案的個人）。這是對於法條文字的完美合理建構，維護 CFAA 專注在駭解而不是將它轉換成全面性的網路秩序監控。

政府的條文建構，將過度擴展而超出設定的電腦駭客範圍，使任何未經授權取得電腦內資訊的使用者入罪化。這將使沒理由懷疑自己正在觸犯聯邦犯罪的一大群普通人成為刑事被告。當然，對於法律的忽略不能開脫，我們可以適當地對於 1984 年的國會，是否明示超出範圍的行為—本質上即屬錯誤，例如破解電腦—應予入罪化進行討論。政府爭執被告已經知悉他們的行為錯誤，應由 1030(a)(4)下的詐欺及實質要件規範，該條文規定：明知且意圖詐欺，未經授權存取受保護電腦，或逾越授權存取，並藉此實現意圖的詐欺及獲取任何有價值之物，除非詐欺的目標及獲取之物只是由使用電腦所組成，以及使用的價值在一年期內不超過五千美元（18 U.S.C. § 1030(a)(4)）。然而，「逾越授權存取」用語在 CFAA 的其他地方，是刑事罪責的基礎未伴隨「意圖詐欺」。例如 1030(a)(2)(C)僅規範逾越授權從受保護電腦取得資訊者。因為「受保護電腦」的定義是被影響或涉及州際商業活動的電腦—對所有連結到網際網路的電腦生效—如此，政府對「逾越授權存取」的闡釋會讓每一件違反私人電腦使用政策成為聯邦犯罪（參照§ 1030(e)(2)(B)）。

自從電腦時代的開啟，員工的心思已經游移，電腦成為耽誤工作的新管道，與朋友聊天、玩遊戲、購物、觀賞運動比賽的精華剪輯。這些雜項早已例行性的被許多電腦使用政策禁止，儘管員工很少能夠維持

紀律，偶爾因為個人目的使用工作電腦。然而，在放寬 CFAA 解讀之下，如此微小的拖延可能成為聯邦犯罪。當然，不太可能因為你在工作電腦上觀看 Reason TV 就一定會被起訴，但有此可能性。雇主若要不遵循合法程序擺脫麻煩員工，就可能以提報到聯邦調查局威脅員工自願辭職。遍地開花、片面決定的犯罪將招致恣意及歧視的執法行動。雇主—員工、公司—消費者間的關係，傳統上是以侵權法及契約法規範。然而，政府提出的 CFAA 闡釋，允許私人操弄他們的電腦使用及人事政策，將這些關係轉變成由刑事法律支配。如果我們允許刑事責任取決於變幻莫測的私人政策—冗長、不透明、易變、鮮為閱讀，將帶來重大的「注意」問題。思考電腦只能公務使用的典型公司政策。到底什麼是「非公務目的」？如果你是用電腦確認公務旅程的天氣狀況？或是為了公司的壘球比賽？還是自己到夏威夷的假期？而且，如果些許的個人使用是被容忍的，員工要如何注意到什麼程度的違反足以觸發刑事責任？

刑事責任若建構在違反私人使用電腦政策上，會翻轉所有無害行為類別成為聯邦犯罪，單純只因為電腦涉入。從前用辦公室電話打電話給家人的員工，將成為罪犯，只因為他們改成寄送電子郵件。員工可以偷偷在工作中閱讀紐約時報的運動專欄，但最好不要造訪 ESPN.com。以及，數獨的愛好者應該堅持紙本謎題，因為從他們工作電腦瀏覽 www.dailysudoku.com 可能讓他們有更多時間在牢房磨練數獨技巧。

寬鬆地建構 CFAA，對於工作場所行為的影響，跟對於每個使用電腦、智慧型手機、iPad、Kindle、Nook、X-box、藍光播放器或其他有網路能力的裝置的人相較起來，根本就是相形見拙。網際網路是經由電腦溝通的管道：每當我們存取網頁頁面、開始下載、在某人臉書牆留言、在 Amazon 購物、在 eBay 下標、發布部落格、在 IMDB 上評分電影、

閱讀 www.NYT.com、觀看 Youtube 影片，以及其他不勝枚舉我們在網路上經常做的事情，我們就是使用電腦對遠端的另一台電腦下指令。我們存取的這些遠端電腦受一系列的私人協議跟政策所管控，然而大部分人們僅僅朦朧的意識到，簡直沒有人閱讀或理解過。

比方說，有一件事並不廣為人知，直到最近大家才發現 Google 禁止未成年人使用他的服務。如果採用政府的闡釋，成千上百的十幾歲或更小者會成為非行少年，而他們的家長、老師則是非行貢獻者。同樣地，Facebook 認為讓任何人登入你的帳號違反他們的服務條款。不過，讓親近的朋友或親戚替你確認電子郵件或使用線上帳戶毋寧是一件相當普遍的事情。有些人可能察覺，如果被發現的話，可能遭受網路服務業者的斥責或不能再使用，但只有很少人想像如此會將他們推向聯邦監獄。或者，考慮五花八門的約會網站，他們的使用條款禁止不正確或誤導訊息。又或者 eBay 跟 Craigslist，他們的使用條款規定上傳物品分類不適當是一種違規行為。在政府提議的 CFAA 解讀之下，在 Craigslist 上傳政策禁止販售的物品，或描述自己「高富帥」但實際上矮又宅，你將贏得一件帥氣的橘色囚服。

今天，我們不需要決定是否國會可能以違反公司或網站的電腦使用政策，認定刑事責任。相反的，我們認為在 CFAA 的用語「逾越授權存取」並未延伸到違反使用限制。如果國會要將誤用行為納入 CFAA 管制，他必須更清楚的表明。狹義的解讀也是一個更合理的文字解讀和立法歷程，總體目標是處罰駭解電腦—規避技術性存取障礙，而不是誤用營業祕密—國會在別處處理的主題。因此，我們做出結論，在 CFAA 的「逾越授權存取」僅限於資訊「存取」限制的違反，而不是「使用」。

因為 Nosal 的同夥擁有公司資料庫的存取及獲得其內資訊的權限，政府的指控未能 18 U.S.C. § 1030(a)(4)符合「未經授權或逾越授權存取」

要件。因此，我們維持地方法院此部分的駁回判決。

## 第二節 性罪犯者與社群媒體[13]

### 第一項 背景事實

北卡羅萊納州於 2008 年頒布法律，經登記的性犯罪前科者，若使用包括像是 Facebook、Tweet 等社群網站，即成立重罪。呈現的問題是，該法能否通過憲法第一修正案言論自由條款的檢驗，以及州政府適用時是否有遵循憲法第四修正案的正當法律程序。

北卡羅萊納州的法律規定一項只針對經登記的性犯罪前科者的重罪：其使用商業社群網路網站，並明知網站允許未成年兒童註冊會員、製作或維護個人頁面（N.C. Gen. Stat. Ann. §§ 14–202.5(a), (e) (2015)）。商業社群網路網站係指符合以下四種要件的網站：第一，營運者從會員費、廣告或其他與網站有關的營業獲得收益（§ 14–202.5(b)）；第二，促使二人或以上以創造友誼、遇見他人或訊息交換等目的進行社會交流；第三，使用者可以製作網頁或個人檔案，其中包含例如姓名、綽號、照片或其他個人資訊，以及連結到其他同在商業社群網路網站的好友個人頁面，或者可以被其他使用者、訪客造訪頁面而與使用者有關的相關人士；第四，它提供使用者或訪客與其他使用者溝通的機制，例如留言板、聊天室、電子郵件或通訊軟體。

以上法律明示兩種例外。條文禁止事項不會延伸到只提供以下一種分散服務的網站：照片分享、電子郵件、通訊軟體、聊天室、留言板平台（§ 14–202.5(c)(1)）。該法也不包含主要目的為促使其會員或訪客間商品或服務商業交易的網站（§ 14–202.5(c)(2)）。依照提供給法院的資料，§ 14–202.5 在北卡羅萊納州適用到約二萬人身上，而州政府已經

[13] Packingham v. North Carolina,137 S.Ct. 1730 (2017).

起訴超過一千位違反該法令的人。

在 2002 年，當時二十一歲的上訴人 Lester Gerard Packingham 是大學生，與一位年僅十三歲的女孩發生性關係，他對於合意猥褻兒童坦承犯罪。因為該罪符合對於未成年人侵害的要件，上訴人被要求登記為性犯罪前科者，這項狀態可能持續三十年或更久的時間。身為一個被登記者，上訴人依據§ 14–202.5 被禁止近用商業社群網路網站。

在 2010 年，州法院駁回了一張對上訴人開出的交通罰單。隨後，他登入 Facebook.com 並在他的個人檔案發文回應：天啊，我是多麼幸運啊！法院駁回罰單甚至沒有開庭？沒有罰錢、不用跑法院、沒有任何花費。向上帝祈禱吧！謝謝老天！同時間，一位 Durham 警察局的成員正在調查他們認為違反§ 14–202.5 的登記者。警官注意到，有一位署名「J.R. Gerrard」的人發表上述聲明，經由確認法院紀錄，他發現發文時間前不久，有一件對上訴人裁罰的交通罰單被駁回。後來取得搜索票取得證據，確認警官懷疑的對象「J.R. Gerrard」就是上訴人。

大陪審團以違反§ 14–202.5 起訴上訴人。上訴人以對他的控訴違背憲法第一修正案為由請求駁回起訴，不過審判法院否決這項請求。上訴人最終被判決有罪並給予緩刑。在審理或判刑的任何時間點，州政府並沒有指控上訴人在網路上有接觸未成年人，或者觸犯其他任何違法行為。

## 第二項 法律議題

憲法第一修正案的一項基本原則，所有人都可以近用任何他們可以發表及傾聽言論的地方，在反思後，再度發言及聆聽。法院總是在空間背景下尋求對發言權利的保護。作為一個基本原則，舉例來說，街道、公園是典型的實現憲法第一修正案的論壇平台。即使在當代，這些地方

依舊是公眾集會慶祝某些觀點、對他人抗議、或單純知悉與調查的必要管道。

在過去辨識哪些地方是最重要交換意見的地方可能有困難（從空間觀點考量），然而，在今日答案是非常明顯的：總體而言，網路空間—網際網路上的廣大民主論壇，以及特定的，社群媒體。百分之七十的美國成年人使用至少一個以上的網路社群服務。其中一個最受到歡迎的是 Facebook，也就是上訴人使用該網站導致他本件的有罪判決。依據本件引用的資料來源，Facebook 有十七億九千萬個活躍使用者，這是將近整個北美洲人口數的三倍。本件是本院首次論述憲法第一修正案與現代網路的關係。因此，在宣告憲法第一修正案對近用廣大的網路作為媒介保護不足之前，本院必須高度謹慎以待。

本件的背景事實使我們必須分析北卡羅萊納州的法律。即使假設該法屬於內容中性而受到中度監督，這些條文仍禁不起考驗。為了通過中度監督，一部法律必須為重大政府利益狹窄地量身訂做，易言之，法律對於言論造成的負擔不能大於所實現的政府合法利益。毫無疑問，本院認知對於兒童的性侵害是最嚴重的犯罪，以及任何有道德良知的人所深惡痛絕的行為。所以立法機關可能通過可行的法律保護兒童及性侵害的被害人。當然，政府不能只是袖手旁觀允許這些邪惡發生。不過，一項可行的合法政府利益，在任何時空背景之下，都不能獨立於所有的憲法保護之外。

解決本案必須作出兩項假設。首先，北卡羅萊納州的法律的廣泛措辭，它可能不只禁止近用一般的社群媒體網站，也可能會適用到略有變

化的 Amazon.com[14]、Washingtonpost.com、Webmd.com。本院不用決定本件法律的精確範圍，如同州政府承認的，已足夠假設本件法律適用在像是 Facebook、LinkedIn、Twitter 這些大眾認識的社群網站。其次，本院的意見，也不應被解讀為禁止州政府頒布比本件法律更加細緻的法案。特定的犯罪行為，即使言論是它們觸犯的方法，也不屬於應被保護的言論。即使這類議題尚未在本院面前，我們假設憲法第一修正案允許州政府頒布特定、量身訂做的法案，禁止性犯罪前科者從事經常是性犯罪前兆的行為，像是接觸未成年人或使用網站蒐集未成人年資訊。這類特別法律是州政府保衛防止性犯罪引起嚴重傷害的第一要務。

即便有這些關於法律範圍及政府利益的假設，本件法律所頒布的禁令已在憲法第一修正案範圍內造成前所未見的負擔。社群媒體允許使用者存取資訊，以及與他人溝通任何在心裡浮現的想法。藉由禁止性前科者使用這些網站，北卡羅萊納州廣泛的打擊，阻擋對於許多人而言，瞭解目前事件、確認聘僱廣告、在現代公共場合發言及聆聽，以及探索人類廣大想法和知識的領域。這些網站，或許，可以是公民讓他們的聲音被聽見的最有力機制。這些網站讓使用網際網路的人，得以成為發聲的倡議者，獲得的響應遠比過去站在臨時演講台上更多。

總而言之，提前關閉對於社群媒體的近用，就是阻卻使用者從事憲法第一修正案的合法權利。認為已經完成審判的人只能使用有限的網站是不平的，即使是被判刑的罪犯—在某些案例中，特別是被判刑的罪

[14] 大法官 Alito 提出的協同意見：以最受歡迎的零售網站 Amazon.com 為例，它允許未成年人使用它的服務，也符合全部§ 14–202.5 所列四個商業社群網路網站的定義。第一，身為商品銷售者，Amazon 無疑地從營運網站獲得收益。第二，Amazon 網站促使民眾社交介紹以交換訊息。當某個人在 Amazon 上買東西，買家可以評論產品、上傳照片，其他買家也可以回應評論。這些產品的訊息交換無疑地落在§ 14–202.5 的定義內。這等同於公車上的乘客相互比較他們購買的產品。第三，Amazon 允許使用者建立個人檔案，用來連結他們上傳購買產品的評論，個人檔案可以包含各式各樣的資訊，包括使用者名稱、電子郵件及照片。第四，評論功能開放來往討論。Amazon.com 滿足最後的條文要件需求。

犯—可以從近用意見的世界得到合法的利益，尤其是如果他們正在尋求改革、合法和應得的生活。

州政府主要的回應是法律效力必須如此廣闊，以達到阻止被判刑的性侵害者遠離脆弱被害人的預防性目的。然而，州政府並沒有證明如此全面性法律是達成目標的必要或合法手段。本件具有指標性意義，本院至今未有案例或決定認同法律可以有如此廣大的效力範圍。州政府引用 Burson v. Freeman, 504 U.S. 191 (1992)作為最接近的類比，在該案中法院支持在投票所一百呎內不得有任何的宣傳活動。不過，這個先例並沒有為州政府的論點提供任何支持。*Burson* 先例中的法律是有限的限制，目的是保護另一項基礎權利—投票權，其背景與憲法傳統一致。該案限制的繁瑣性遠遠小於本件州政府尋求實施的限制。

比較好的類比是 Board of Airport Comm'rs of Los Angeles v. Jews for Jesus, Inc., 482 U.S. 569 (1987)，本院宣告禁止任何在洛杉磯國際機場進行憲法第一修正案活動的法令違憲，因為該法令涵蓋全部受到保護、非干擾式的抗議行為，像是談話、朗讀或穿戴宣傳飾品、象徵性服飾。如果一個禁止在單一機場行使受保護表達權利的法律違憲，舉輕以明重，州政府更不得頒布完全禁止在與現代社會、文化密不可分的網站上行使憲法第一修正案權利的禁令…。北卡羅萊納州最高法院判決違背法令，本件撤銷發回。

## 第三節 兒童色情的網路過濾[15][16]

[15] Center for Democracy adn Technology v. Pappert 337 F. Supp. 2d 606 (E.D. Pa. 2004).

[16] 本判決後續討論架構為美國憲法第一修正案議題，即對於法案對於言論的負擔、該適用何種層級的審查密度、是否過早的言論限制，且前一節性犯罪者與社群媒體之判決論述中，也已經導入介紹言論自由議題，由於筆者主要目的是引入判決中關於技術層面的論述，故省略後續之言論自由議題，以免有重複之感。

## 第一項 背景事實

2002 年 2 月，賓州頒布 Internet Child Pornography Act（Internet Child Pornography Act）。該部法律要求網路服務業者（ISP, Internet Service Provider），經過州檢察長通知後，業者應該移除或阻斷立基於或使用其存取服務的兒童色情內容。這是首次州政府對網路服務業者實施刑事責任，即使業者只是提供網路管道存取兒童色情，與色情內容的來源毫無關係也一樣。

### 壹、Internet Child Pornography Act

本法授權賓州地方檢察官向法院聲請命令，只要提出可信的證明網路內容構成兒童色情，即可要求網路服務業者移除或阻斷立基於或使用其存取的服務。聲請的要件必須表明對象內容的 Uniform Resource Locator（URL，即在瀏覽器網址欄直接輸入地址）。法庭命令的核發，可能只是單方面的聽證，並不會事先通知網路服務業者或網站所有者，也不會對網站所有者發出聽證後的通知。依照法案，一旦有合理證據顯示受到挑戰的內容構成兒童色情，法官將核發命令指示，該等內容應從業者的服務中移除或限制存取。在取得命令後，賓州檢察長會通知相關的網路服務業者並提供一份法庭命令的影本[17]。接著，網路服務業者有五天的時間阻斷特定內容的存取，否則將面臨刑事責任，包括三萬美元以下罰金、七年以下有期徒刑。依照被告州檢察長的說法，法案的目的是保護兒童免於性剝削、性虐待，藉由阻止兒童色情的散布，尤其是透過網路網路散布，以達到法案目的。

[17] 該程序原文係「Informal Notices」，如直接翻譯應為非正式通知，不過本文為行文順暢，視情況稱為命令。

## 貳、如何遵循法庭命令

### 一、實行方法

根據網路服務業者解釋，在大部分的情形，他們嘗試以 IP 過濾或 DNS 過濾的方法遵循命令，這些方法可能單獨或綜合採行。使用 IP 過濾、DNS 過濾或 URL 過濾阻斷透過業者服務存取的內容，只會影響到使用其服務連結網路的使用者。因此，如果網路使用者的服務業者並沒有阻斷網站，則使用者還是能存取到被阻斷的內容。

#### （一）DNS 過濾（DNS Filtering）

要實行 DNS 過濾，業者會在其掌控的 DNS 伺服器輸入註記，防止符合域名（登記於命令內的 URL）的特定網站請求（requests），從伺服器中解析出該網站正確的 IP 位置。上開註記會讓 DNS 伺服器，對符合域名索取 IP 位置的請求，回應以錯誤的地址或錯誤的訊息。沒有請求網站的正確 IP 位置，請求將不會有下一步處理，或根本無法訪問目標網站。

#### （二）IP 過濾（IP Filtering）

要實行 IP 過濾，業者首先要決定特定 URL 對應的 IP 位置。接著，業者會在掌控的路由器設備中註記，阻止全部導向特定 IP 位置的請求。

#### （三）URL 過濾（URL Filtering）

證人 Stern 作證表示，網路服務業者只能透過 URL 過濾遵循政府的阻擋指示。URL 過濾涉及業者必須在其網路系統內，進行額外設備的替換，或在某些情形對現存路由器的重新調校，步驟如下：（a）重組流經其網路系統的網際網路封包；（b）讀取每個 http 網頁的請求（c）如果網頁請求的 URL 符合在黑名單列出的 URL，丟棄或者阻擋該 http 請求。

## 二、過度封鎖（Overblocking）

DNS 過濾會停止被封鎖域名（domain name）下的所有子頁面的請求。因此，如果命令中所列 URL 的域名剛好是虛擬主機服務（web hosting service），該服務的使用者可以在網站下設立獨立的子頁面內容，則 DNS 伺服器的註記就會停止網站下所有獨立頁面的請求，不是只有被列為目標顯示兒童色情的物件。舉例來說，當例如 GeoCities 網站這樣的線上社群，它允許不同使用者在 GeoCities.com 的子頁面下設立網站，一旦被列為目標以後，DNS 過濾就會產生過度封鎖的效果。

IP 過濾更是會導致顯著的過度封鎖。如同證人 Stern 所述，IP 過濾會封鎖大量的無辜網站，以及極有可能因為虛擬主機的關係，封鎖非目標網站。又因為共用 IP 的盛行，IP 過濾會有封鎖無辜網站的情形，如果網路服務業者使用 IP 過濾阻斷特定 IP 位置的存取，則所有在該 IP 位置下代管的網頁都會被阻擋。比方說，為了回應本件命令，網路服務業者 Epix.net 阻斷 IP 位置 204.251.10.203 的存取，同時也阻擋了兩個 Laura Blain 個人網站及其他使用 directNIC 代管服務的網站。

URL 過濾細緻篩選網頁至特定的子頁面，這表示不會有阻斷非目標網站存取的風險。儘管 URL 過濾只會產生最小量的過度封鎖，不過沒有任何網路服務業者現階段有辦法實施這個方法，而 DNS 過濾跟 IP 過濾兩者又會有過度封鎖的疑慮。

## 三、規避方式

### （一）匿名代理伺服器（Anonymous Proxy Servers）

網路使用者如果想隱藏真實身分，可以使用匿名代理伺服器或匿名器。在瀏覽網頁時，這些服務路由所有流經代理伺服器或匿名器的請求，代替將請求送至欲造訪的網站。使用這些服務的請求，在網路服務

業者的路由面前，彷彿他們是被導向到代理伺服器的請求，而不是到使用者真正尋求存取的根本 URL。匿名代理伺服器或匿名器的使用，完全地規避科技阻擋手段：IP 過濾跟 DNS 過濾，兩種網路服務業者所使用遵循命令的方式，且 URL 過濾也有可能被規避。比方說，被網路服務業者 AOL 阻擋的網站，仍然可以使用匿名器 Proxify.com 透過 AOL 服務存取。

### （二）閃避過濾的能力

IP 過濾可以被兒童色情網站的營運者藉由改變 IP 位置閃避。在一個案例當中，檢察長辦公室對 AOL 發出關於某網站的第二次通知，是因為在 AOL 封鎖該網站的 IP 位置以後，AOL 的使用者又得以不同 IP 位置進入該網站。AOL 的作法是再次封鎖第二次通知的 IP 位置。兒童色情網站的營運者也有許多方法可以閃避 DNS 過濾，包括：（1）直接用 IP 位置當作網址，例如網站可以用 IP 位置（一串數字）當作網址而不是以域名的方式如「www.example.com」呈現；（2）修改一部分的域名，再將新的域名超連結發布到廣告、搜尋引擎、新聞群組。

## 第二項 楓林網影音侵權案

### 壹、新聞報載[18]

碩士 33 歲陳男和 32 歲莊男自 2014 年起設立影視追劇網站「楓林網」，透過網路廣告獲取非法利益，涉侵權金額近新台幣 10 億元，刑事局接獲美國電影協會跨海提告將兩男送辦。

刑事局電信偵查大隊今天舉行破案記者會，大隊長陳瑞金表示，非法網站「楓林網（8maple.ru）」利用註冊境外主機架設免費台劇、日劇、

[18]楓林網 2 主嫌遭起底！現金買千萬透天豪宅、開特斯拉，每月海撈 2 百多萬，https://www.storm.mg/lifestyle/2497697，最後瀏覽：2020/5/25。

韓劇、泰劇、中國大陸戲劇及歐美電影等影視頻道，供不特定民眾觀賞，並利用網路廣告點擊率賺取不法利益。

電偵大隊首次和美國電影協會（MPA）跨境合作分享情資和依法蒐證，包括日本內容產品海外流通促進機構（CODA）和多家國內媒體都委任律師提告，統計侵權金額近 10 億元，經報請桃園地檢署檢察官指揮擴大偵辦。

根據調查了解，陳男和莊男兩人為大學和碩士班同窗，兩人熱愛電影又具理工背景，卻因求職不順便合作共設「楓林網」，犯罪時間自 103 年起迄今，月付 30 萬元網路費，單月最高非法獲利可達 200 萬元，近期還耗資現金數千萬元在桃園購買兩棟透天厝作為工作據點，還購置名車特斯拉。

經查兩人此舉涉嫌違反著作權法重製及公開傳輸、公開撥放等犯罪事實，且網站流量高居全國所有盜版網站第 1 名，涉嫌非法竊取台灣、歐美及亞洲各國重要智慧財產。 刑事局歷經約半年時間蒐證追查，目前已掌握「楓林網」相關 28 個網址，其中有 8 個已被提告，警方見時機成熟於 3 月 31 日在桃園市八德區逮捕兩男，並起獲電腦、手機、雲端主機 25 台（加拿大、法國），以及凍結動產資金及不動產 2 筆，價值共約 6000 多萬元。

同時，「楓林網」網站已遭刑事局查禁，兩男依涉違反著作權法送辦，陳男和莊男分別以 50 萬元和 30 萬元交保。

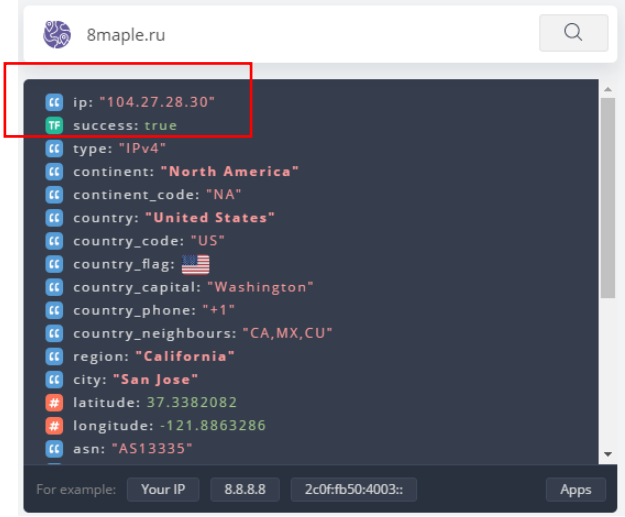
## 貳、楓林網的封鎖方式

筆者於寫作期間，恰巧注意到內政部警政署刑事警察局電信偵查大隊破獲盜版影音網站的新聞。楓林網於 2020 年 3 月 31 日遭查禁後，如果在網路上搜尋楓林網並嘗試點擊進入該網站，只會顯示如下畫面，無法再進一步瀏覽網站的內容。此時，本節介紹的美國判決，使筆者產生聯想，我國執法單位是否在楓林網採取了同樣的過濾方式。

圖 2：瀏覽「8maple.ru」時顯示的頁面（最後瀏覽：2020/5/25）

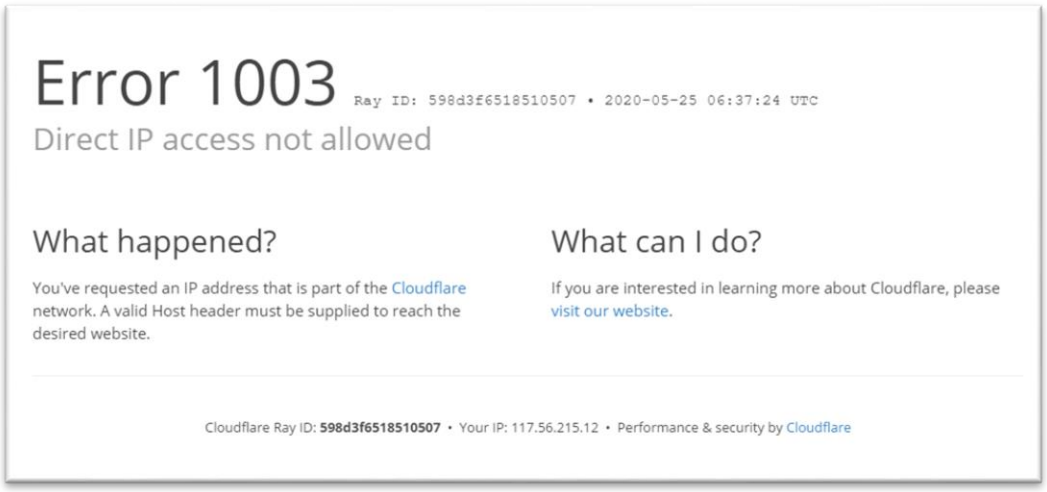

首先，以楓林網的網址「8maple.ru」反查 IP 位置，其 IP 位置為「104.27.28.30」。

圖 3：「8maple.ru」轉換 IP 位置




接著，在瀏覽器網址列輸入「104.27.28.30」，結果顯示錯誤，「8maple.ru」係架設在 Cloudflare 公司的虛擬主機之下，該公司為美國公司，提供網頁基礎設施、網站安全等服務，並無法直接以 IP 位置存取，必須提供標頭檔以特定欲存取網站頁面。

圖 4：網頁顯示不允許直接以 IP 位置存取




如同本節美國判決中記載之技術分析，楓林網既然是採用虛擬主機所架設，所以本件不可能使用 IP 過濾，以免造成過度封鎖，同一虛擬主機下的其他網站均無法被瀏覽。至於 URL 過濾，因為被認為程序上過度繁瑣，現階段網路服務業者難以實施此方法。然而，被阻擋的頁

面明白顯示「The Domain Has Been Sized」，宣稱該網域已被扣押，是否代表刑事警察局電信偵查大隊使用 DNS 過濾技術，阻斷侵權影音繼續在網路上流竄？筆者嘗試以本節美國判決中提到的匿名代理伺服器方法，造訪「8maple.ru」確認是否可以規避網路服務業者審查，結果仍然顯示相同的查禁頁面。如此表示電信偵查大隊其實並未請求我國的網路服務業者，例如中華電信或臺灣固網等業者配合，而是在執行搜索時，直接將警方自行製作的查禁頁面，上傳到虛擬主機中覆蓋原本的楓林網首頁，以防止網友繼續上網觀看侵權影音內容，以此方式保護智慧財產權。筆者認為這間接地透露網路過濾的難度、技術與法律交界處的模糊。

# 第四章 我國網路證據爭議與美國實務發展

## 第一節 中華電信 hiBox 案

### 第一項 hiBox 服務介紹

「hiBox 全能信箱」是中華電信推出的數位服務，以網際網路為基礎，將電子郵件、傳真與簡訊整合在單一數位平台，用戶只要透過電腦、筆記型電腦、平板電腦、手機或行動 app 登入，就可以隨時隨地使用 hiBox 介面進行訊息的收發及觀看。hiBox 服務最大的特色是傳真的數位化，傳統傳真是點對點的定點輸出，收發雙方都必須安裝傳真機，傳真內容則以感熱紙或列印輸出；但如果使用者申請 hiBox 服務，同樣會有一組中華電信配給的傳真電話號碼，不過可以在手邊沒有傳真機的情況下，不論用戶身在何處，只要能連結網路，就可以對他方傳送或收受傳真，並在裝置上即時瀏覽。

圖 5：hiBox 功能示意圖


資料來源：https://hibox.hinet.net/uwc/uwc/homepage_tw/features.html，最後瀏覽：2020/3/11。

## 第二項 hiBox 與賭博罪

### 壹、刑法

我國刑法第 266 條規定：「（第 1 項）在公共場所或公眾得出入之場所賭博財物者，處三萬元以下罰金。但以供人暫時娛樂之物為賭者，不在此限。（第 2 項）當場賭博之器具與在賭檯或兌換籌碼處之財物，不問屬於犯人與否，沒收之。」第 268 條規定：「意圖營利，供給賭博場所或聚眾賭博者，處三年以下有期徒刑，得併科九萬元以下罰金。」此為我國處罰賭博罪之依據。

### 貳、賭博在數位時代的變革

坊間常見的賭博方式是由組頭召集下線及賭客，以臺灣彩券的「今

彩 539」、「大樂透」或香港「六合彩」的開獎號碼作為下注標的，賭客自行選號簽注「二星」、「三星」、「四星」或「特別號」、「全車」等投注方式，並依選號數量支付相對應的投注金。等到每週上述官方的投注標的開獎後，如果賭客簽注號碼有中即可獲得組頭允諾的彩金；相反地，賭客如果沒有簽中任何獎項，所投注之賭金則屬於組頭及下線的利潤。換言之，坊間的賭博是一種組頭與賭客猜測開獎結果的對賭。

組頭與賭客多半不曾謀面，賭客若要下注，通常會寫下簽注號碼傳真給組頭，如此一方面可以快速完成簽注，另一方面也可留下紙本紀錄。為了接收傳真，傳統上組頭通常在家中或另尋地點安裝傳真機，並留存傳真機輸出的簽注紙本。然而，在進入網路時代以後，使用數位傳真的組頭也多了起來，中華電信的 hiBox 服務即為適例。在此情況下，執法機關在偵辦賭博罪時，要取得簽注紀錄即產生困境，畢竟已經不再是實體紙本了，簽注紀錄反而是以電磁紀錄的形式儲存在中華電信的設備之中，傳統的執法單位到組頭家中搜索扣押不再是有效的蒐集證據手段。此時，應該如何取得這些證據，即成為議題。

### 第三項 hiBox 與網路證據

hiBox 在我國引起關注是由於一起賭博案件（臺灣彰化地方法院 105 年度易字第 867 號刑事判決），該案法院以控方從 hiBox 取得的六合彩簽單違反通訊保障及監察法無證據能力為主要理由，判決被告均無罪。檢察官不服提起上訴（臺灣高等法院臺中分院 106 年上易字第 180 號刑事判決），上訴法院認為原審判決理由並無違誤，駁回上訴而判決確定。不過，檢方認為無罪判決的理由有誤，誤認通訊保障及監察法為特別法，不當排除刑事訴訟法關於「扣押」之規定，有判決不適用法則、適用法則不當之違背法令，案經確定，並與統一適用法令有關，

且具有原則上之重要性，依刑事訴訟法第 441 條、第 443 條提起非常上訴。

## 壹、臺灣彰化地方法院 105 年度易字第 867 號刑事判決

### 一、犯罪事實

被告陳昭全、洪文宗於民國 104 年 8、9 月間，共同基於賭博、意圖營利供給賭博場所及聚眾賭博之犯意聯絡，將以被告洪文宗名義申辦之門號「04-1234567」號（下稱本案門號）供作公眾得出入之場所，供真實姓名不詳不特定之多數賭客，向渠等簽賭俗稱「六合彩」之賭博，被告陳昭全再將簽注單以本案門號傳真至上游組頭門號「04-2345678」號電話（上游組頭部分，由檢察官另行偵辦）而賭博財物。其賭法係由賭客先自 01 至 49 共 49 個號碼中任意簽選數個號碼為 1 組，再選擇所謂「二星」、「三星」、「四星」、「特別號」或「全車」等之簽賭方式，並需支付投注金，選定後核對每週香港六合彩之開獎號碼，如賭客所簽選之號碼與開獎號碼之任意 2 個號碼以上相同，即可獲得彩金，賭客如未簽中任何獎項，所投注之賭金悉數歸被告陳昭全、洪文宗所有，藉此方式而獲取利益。因認被告二人共同涉犯刑法第 266 條第 1 項前段之在公眾得出入之場所賭博財物、第 268 條之圖利供給賭場、圖利聚眾賭博罪嫌。

### 二、法律爭議

#### （一）證據：六合彩簽注單影像列印資料如何取得

1.查公訴人提出之六合彩簽注單影像列印資料 324 張，其取得方式，係檢察官向本院聲請調取門號「04-1234567」電話，自 104 年 8 月 1 日起至同年 9 月 17 日止之雙向通聯紀錄，並於調取票聲請書上記載調取之資料包括「接收傳真內容之影像」，但本院核發之通信調取票，

就「調取通信種類」係記載「詳如附件」，而該附件亦僅列載包括上開電話在內共 18 線電話之雙向通聯、使用者資料，並未記載准以調取「接收傳真內容之影像」資料。嗣警方即依檢察官之指揮，持本院核發之調取票向中華電信股份有限公司調閱上開門號使用該公司 hiBox 網路傳真機接收傳真內容之影像，而經中華電信列印交付警方等情，有檢察官調取票聲請書、本院 104 年聲調字第 371 號通信調取票暨附件，及警員職務報告等在卷可參。核此情事，本案警方取得之上揭傳真機簽注單影像列印資料，不無有逸脫本院上述調取票所准許調取之範圍而取得之嫌。

**（二）警方調得之六合彩簽注單影像列印資料之證據能力判斷**

2.稽諸上揭從中華電信 hiBox 網路傳真機截取之六合彩簽注單影像列印資料，其上除有通信時間之資訊外，並有書寫字跡、簽注種類與號碼、簽注支數及名稱代號（即「亮-陳」、「大-全」、「吉全」、「好-全」、「佑→全」等）等意思表示內容，有該等簽注單影像列印資料在卷可參。上開簽注單之通訊方式，係發送方利用電話傳真機將掃描之影像，經由電信線路傳送到中華電信之電腦伺服器儲存，伺服器處理後再透過電信線路傳送到接收方之電信用戶。此通訊方式，核屬通訊保障及監察法第 3 條第 1 項第 1 款所規定：「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信」之通訊；且因該等簽注單上之號碼、文字等內容，係利用中華電信之電信設備發送及儲存，並屬私人間之通信，復查無證據證明警方取得該等傳真通訊內容，曾經得通訊相對人間任何一方之同意，自應認發送方與接收方對該通訊內容具有隱私及秘密之合理期待，是上揭通訊內容為通訊保障及

監察法所保障之通訊。從而欲取得此一通訊內容，自應依同法第 5 條或第 6 條之規定，經法官核發通訊監察書，始得為之。

3.本案警方雖係依調取票而調取上揭簽注單等影像列印資料，惟按通訊保障及監察法第 11 條之 1 第 5 項規定，調取票所得調取之資料為「通信紀錄」及「通訊使用者資料」，依同法第 3 條之 1 的規定，所稱「通信紀錄者」，係指「電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。」；所稱「通訊使用者資料」，則係指「電信使用者姓名或名稱、身分證明文件字號、地址、電信號碼及申請各項電信服務所填列之資料。」足見「通信紀錄」與「通訊使用者資料」，均屬不涉及通信內容之資訊。申言之，調取票所得調取之資訊，係不具通信內容之「通信紀錄」或「通訊使用者資料」，法官核發調取票僅能針對不具通信內容之資訊。倘若聲請調取之資訊係具有通信內容之通訊，因取得具有通信內容之通訊，必須符合通訊保障及監察法第 5 條或第 6 條之要件，且經法官核發通訊監察書，始得為之，此際法官自不得核發調取票，縱然核發，司法偵查機關亦不得執此無效令狀獲取具有通信內容之通訊。如果取得，此「應經法官核發通訊監察書」，卻「未經法官核發」而逕取得之證據，自屬違反通訊保障及監察法第 5 條或第 6 條之規定進行通訊監察所取得之證據，應有同法第 18 條之 1 第 3 項證據排除規定之適用。

4.相對於傳統型態之搜索、扣押等強制處分，通訊監察係屬新型態之強制處分。按諸立法體例，原本應將屬強制處分一環之通訊監察，規範在國家偵查犯罪實施強制處分之基本法律的刑事訴訟法內，但我國立法者係選擇以特別法方式，亦即在刑事訴訟法外，另行制定通訊保障及監察法，以規範有關通訊監察此一強制處分發動之要件及限制，依特

別法優於普通法之原則，通訊保障及監察法乃屬刑事訴訟法之特別法，自應優先適用，法理甚明。是公訴人謂依刑事訴訟法第 133 條之規定，對可得為證據之物，自得命持有上揭簽注單傳真影像資料之中華電信提出，而毋庸法院核發通訊監察書；且依刑事訴訟法第 159 條之 4 第 2 款之規定，該等簽注單為中華電信業務上所製作之紀錄文書，自有證據能力等節，容係誤解上述法律規範之效力優先次序，及傳真機簽注單影像資料之定性（性質上非屬中華電信業務上紀錄之資料，參諸通訊保障及監察法第 3 條之 1 之規定自明）所致，核無足採。

5.公訴檢察官雖另謂依中華電信與用戶簽訂之定型化契約「市內網路業務服務契約」第 45 條之約定，中華電信原則上固對業務上所掌握用戶之相關資料有保密義務，但在有司法機關為偵查犯罪或調查證據所需時，得以提供，而主張系爭列印之簽注單影像資料具證據能力。惟揆諸通訊保障及監察法第 1 條規定「為保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。」之立法目的，即在於保障憲法所賦與人民之秘密通訊自由，與確保國家安全、維護社會秩序之權衡兼顧，故如上所述，國家為偵查犯罪目的而取得通訊內容，必須依據通訊保障及監察法之規定，經法官核發通訊監察書，始得為之。另方面，電信業者相較於電信使用人而言，屬支配通訊設備使用之強者，如不接受其定型化契約內容，即無從使用該電信業者之電信服務，處於弱勢之電信使用人顯然無法與其抗衡，也根本無法與之議訂而修改電信業者提供之定型化契約，而只能照單全收；於此情形，若謂憑定型化契約之上開概括約定，即令電信使用人事先概括同意電信業者得單方將通訊內容提供給偵查機關，而無需視具體個案取得電信使用人之同意，亦無須遵守通訊監察之法官保留原則，此舉將使憲法第 12 條所揭櫫保障之人民有秘密通訊自由成為具文，亦將架空通訊

保障及監察法所規定之法官保留原則。是公訴檢察官此部分之主張，有悖於憲法保障秘密通訊自由與通訊保障及監察法規定之法官保留原則，要無可採。

6.據上所述，本案之傳真機簽注單影像內容列印證據，因未經法官核發通訊監察書而逕行取得，係屬違反通保法第 5 條或第 6 條之規定取得。通訊保障及監察法第 18 條之 1 第 3 項規定：「違反第五條、第六條或第七條規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據或其他用途，並依第十七條第二項規定予以銷燬」。本條項所使用之「監聽行為」一義，究為列舉規定，僅規範監聽行為，而不及於同法第 13 條第 1 項所定之截收、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法？抑或僅屬「通訊監察行為」之例示規定，而包括第 13 條第 1 項所定監聽以外之通訊監察方法？文義上雖非無疑。但本院認為，第 13 條第 1 項規定之通訊監察以「截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法」等各種型態之監察行為，係為因應日新月異之通訊科技所作之例示規定，包括監聽在內，皆屬通訊監察方法，無論何一通訊監察方法，均非經法官核發通訊監察書不可，且各種通訊監察方法所得資訊均為具有隱私期待之通訊，隱密監控之侵害性格並無不同，依相同事物為相同處理之解釋方法，就通訊保障及監察法第 18 條之 1 第 3 項所稱之「監聽行為」，自以例示規定之解釋為妥。再者，如獨獨針對「監聽行為」設立證據排除規定，而其他通訊監察行為不與焉，勢將大大限制該證據排除條款之規範射程，徒使立法美意落空，國家機關將執此以規避證據排除條款，其論理上謬誤甚明。本案警方取得儲存在電信業者電腦伺服器之通訊，該通訊本係以電磁紀錄形式儲存於伺服器上，中華電信應警方所請，將文字、號碼等影像之電磁紀錄輸出列印附

著在紙張之上，成為可供閱讀與解讀之資訊。由此過程觀之，警方獲取通訊之方法與影印既有文字或影像類似，應屬同法第 13 條第 1 項所稱之「其他類似之必要方法」。從而，警方違反通訊保障及監察法第 5 條或第 6 條規定以「其他類似之必要方法」實施通訊監察，該「其他類似之必要方法」亦屬同法第 18 條之 1 第 3 項所稱之監聽行為，是警方上述違反規定取得之本案傳真機簽注單影像列印資料，依該條項之規定，自不得於本案採為證據，應予排除。

## 貳、最高法院 106 年度台非字第 259 號刑事判決

### 一、hiBox 傳真內容是「過去已結束」抑或「現時或未來發生」之通訊內容？

本案 hiBox 傳真內容，結合傳真與電子郵件為線上發送，乃利用電信設備所處理之訊息，固然屬於「通訊」之一種，然既由賭客傳真至被告處，已在其得處置之狀態下，自係「過去已結束」之通訊內容，並非「現時或未來發生」之通訊內容，依上揭說明，當不適用通保法「通訊監察書」之規定。

### 二、執法單位應如何合法取得 hiBox 傳真內容

而「調取票」，規範於通保法，由法官依檢察官或司法警察官之聲請，審查合法後核發之，調取之客體乃通信紀錄或通信使用者資料（非涉及通訊內容），且以「最重本刑 3 年以上有期徒刑之罪」、「有事實足認與本案之偵查有必要性及關連性」等為要件（通保法第 3 條之 1、第 11 條之 1）。本案 hiBox 傳真內容，涉及通訊內容，非屬通信紀錄或通信使用者資料，故不適用通保法「調取票」之規定。誠如前述，偵查機關為犯罪偵查目的而需取得「過去已結束」之通訊內容時，屬資訊隱私權，應回歸適用刑事訴訟法，依刑事訴訟法搜索、扣押相關規定…如比

較「通信紀錄或通信使用者資料」對個人隱私權之侵害程度相對於「過去已結束」之通訊內容較為低，立法者既將前者以法官事前審查核發之令狀（調取票）為原則，後者至少亦應以法官事前審查核發之令狀為原則，才屬妥適（至於調取票與搜索票、扣押裁定之發動門檻要件固然有別，惟此乃立法政策考量，在此不問）。審諸搜索因對於被搜索人隱私權或財產權造成一定程序之干預與限制，基於憲法第 23 條法律保留原則之要求，我國採令狀主義，應用搜索票，由法官審查合法後簽名核發之，目的在保護人民免受非法之搜索、扣押。人民對於「過去已結束」之通訊內容，既享有一般隱私權，且通訊內容往往含有與本案無關之大量個人私密資訊，比其他身體、物件、處所、交通工具等之搜索，其隱私權之保障尤甚，應有法官保留原則之適用，是偵查機關原則上應向法院聲請核發搜索票，始得搜索、扣押（刑事訴訟法第 122 條、第 128 條、第 128 條之 1），方符憲法上正當程序之要求。又 105 年 6 月 22 日修正公布之刑事訴訟法，增訂第 133 條之 1 及第 133 條之 2 規定非附隨於搜索之扣押裁定及聲請程序，偵查機關認有聲請非附隨於搜索之扣押必要時，原則上應向法院聲請核發扣押裁定，其立法理由乃認非附隨於搜索之扣押與附隨於搜索之扣押本質相同，除僅得為證據之物及受扣押標的權利人同意者外，自應一體適用法官保留原則。至修正第 133 條第 3 項（原條文未修正，由第 2 項移列第 3 項）規定提出命令，乃指對於應扣押物之所有人、持有人或保管人，偵查或司法機關得命其提出或交付，如檢察官或法院函請調閱戶政機關有關被告之戶籍口卡，或金融銀行機關有關被告戶頭資金往來明細等。而提出命令，隱含後續之強制處分，受處分人如無正當理由拒絕提出或交付時，通常伴隨著後續之不利處分，即得用強制力扣押（刑事訴訟法第 138 條），此無須事先由法院審查，且無其他要件限制。基此，有主張（如本件非常上訴理由書）

檢察官如認「過去已結束」之通訊內容，屬於本案證據，且為應扣押之物，即可依手段比例原則，分別命扣押物之所有人、持有人或保管人提出或交付，甚而進一步依非附隨搜索之扣押程序，逕以實行扣押之方式取得即可，均無庸向法院聲請扣押裁定（至於該「過去已結束」之通訊內容，如同時得為證據及得沒收之物，依第 133 條之 1 第 1 項之立法理由，仍應經法官裁定，對該通訊內容之一般隱私權之保障已足，故無就此贅述之必要），惟此對人民一般隱私權之保障實有未足。蓋以現今資訊世界，大量仰賴通訊軟體，通訊服務，有大量之隱私儲存於此，如容許偵查機關未經法院之介入，逕行調閱，其侵害隱私至深且鉅，顯違比例原則。且若允許檢察官以提出或交付之方式，即可取得「過去已結束」之通訊內容，則該「過去已結束」之通訊內容之所有人、持有人或保管人如涉及外國網路通訊業者或行動電信業者，其等對於本國不採令狀之提出或交付法制，必先思考該提出或交付之程序是否符合該公司之本國法律（如 FaceBook、Google 業者適用美國法，Line 業者適用日本法），倘該國法律採令狀原則（如前所述之外國立法例均採令狀原則），而我國不採，則業者可能因此拒絕提供該等內容，將有礙檢方對使用通訊科技設備犯罪之偵辦。何況，現今資訊及通訊科技全球化，我國當無閉門造車，自外於先進國家法制之理。準此，修正後刑事訴訟法第 133 條第 3 項（或修正前第 133 條第 2 項）規定「應扣押物」及第 133 條之 1 第 1 項規定「得為證據之物」之扣押客體，基於維護人民一般隱私權、保障其訴訟權益及實現公平法院之憲法精神，應依目的性限縮，而認不及於「過去已結束」之通訊內容。是以，檢察官對於「過去已結束」之通訊內容之非附隨搜索之扣押，原則上應向法院聲請核發扣押裁定，不得逕以提出或交付命令之函調方式取得，方符上開保障人民一般隱私權之旨。

### 參、小結

針對如何取得儲存於 hiBox 服務的傳真內容，實務認為應向法院聲請核發搜索票並扣押證據，或另向法院聲請非附隨於搜索之扣押裁定[19]，不得逕以提出或交付命令之函調方式要求中華電信提出。此作法不僅限於本案起源的 hiBox，往後其他網路業者相類似的服務，只要用戶是將其個人資料儲存其中，而執法單位想要調取之，應均有所適用。從前揭判決的脈絡，本文欲延伸討論三個議題。第一個是數位時代對隱私權帶來的衝擊（如非常上訴所論述：現今資訊世界，大量仰賴通訊軟體，通訊服務，有大量之隱私儲存於此，如容許偵查機關未經法院之介入，逕行調閱，其侵害隱私至深且鉅，顯違比例原則），以及對於偵查作為的影響；第二個是美國法院判斷執法單位要求網路服務業者儲存使用者在其伺服器進出的郵件內容並嗣後提出作為證據，此舉是否合法；第三個是如 hiBox 介紹提到的，用戶可以透過電腦、筆記型電腦、平板電腦、手機登入服務，此時，當執法機關取得這些電子裝置並研判相關證據儲存在其中，應該如何檢視其內容？是否可以命令被告解密而產生不自證己罪議題？以下依序介紹美國實務見解。

## 第四項 美國相關實務判決

### 壹、RILEY V. CALIFORNIA[20]

### 一、背景事實

上訴人 David Riley 因為過期的註冊標籤被警方攔車。在停留的過程中，警方發現 Riley 的駕照已被吊銷。警方因此扣留 Riley 的車輛，另一名警員則依照部門政策對該車盤點搜索。隨後在 Riley 車輛引擎蓋

[19] 吳巡龍（2019），伺服器傳真影像之調取，月旦法學教室，第 197 期，第 25 頁。
[20] Riley v. California, 134 S. Ct. 2473 (2014).

下發現兩把手槍，Riley 立即被以隱藏及裝載槍械被逮捕。一名警員在逮捕 Riley 後，對他進行附帶搜索（search incident to the arrest）並發現與街頭幫派「Bloods」有關的物品，同時也將他長褲口袋內的手機扣押。

依照 Riley 沒有矛盾的主張，該手機是智慧型手機，是一隻具有高端運算能力、大容量儲存空間、與網路連結而有廣泛功能的手機。警方檢閱手機裡的資訊，並注意到有些字句（假設是從文字簡訊或聯絡人名單得知）前註記「CK」字樣，這個標籤警方相信代表著「Crip Killers」，是街頭幫派 Bloods 成員的俗稱。在逮捕過後兩個小時，在警察局一名專精幫派的警探進一步檢查手機的內容。該名警探證稱，他詳細的檢查過 Riley 的手機，因為幫派成員經常對自己持槍的樣子錄影或拍照。雖然有很多東西在這隻手機裡，不過有些檔案特別抓住了警探的目光，包括一群年輕人爭吵時有人叫囂出「Blood」的影片。警方也發現 Riley 站在一台車前面的照片，這台車警方懷疑涉嫌幾個星期之前的槍擊案件。

Riley 最終被認定與該槍擊案件有關，以對有人車輛開槍、使用半自動武器攻擊、殺人未遂等罪名起訴。

## 二、法律議題

例外無令狀的附帶搜索，不只側重於關注在瞬息萬變的逮捕過程中面臨危險的政府利益，也應側重在被警方監管時，被逮捕者所減損的隱私利益。

政府主張對於儲存在手機內的資料的搜索，與這類實體物件的搜索難以區分的。這就像是說騎在馬背上，很難跟前往月球的班機區分開來一樣。兩者都是從地點 A 到地點 B 的途徑，但有一些其他事物足以正當化將他們糾結在一起。現代的手機作為一個類別，跟對於一包香煙、一個錢包、一個提包的搜索，所隱含的隱私權疑慮，大不相同。作

為結論，檢查被逮捕者口袋內容物，並沒有超出逮捕本身可能會適用到實體物品的常識，而造成額外的隱私侵害；不過如果將這個理解延伸到數位資料，就必須另外找出立論基礎。

從一個被逮捕的人身上取得的物品來看，手機不論從質跟量方面都與其他物品不一樣。「手機」這個名詞本身是個容易誤解的用語，許多手機事實上是迷你電腦，只是剛好也有被當作手機使用的功能。手機也可很容易的被稱為相機、影片播放器、名片盒、行事曆、錄音機、圖書館、日記、音樂專輯、電視、地圖或新聞。現代手機其中一個最值得注意的不同特色是他們強大的儲存能力。在現代手機問世之前，對人的搜索限制在物理實體上，而且總體而言只會構成有限範圍的隱私侵害。大部分人們不可能隨身攜帶過去幾個月來所收到的每一封信件、每一張所拍攝的照片、或所閱讀的每一本書、每一篇文章，也不可能有任何如此嘗試的理由。

但是，當議題是手機的時候，對於隱私權可能的侵害就不侷限在實體方面了。目前暢銷的智慧型手機標準的儲存容量是 16Gb（也可以買到最多 64Gb）。16Gb 可以轉換成百萬頁計的文字、數以千計的圖片、或數百個影音檔案。手機有存放不同型態資訊的儲存能力：即使是售價低於二十美元最基本的手機，也會存有照片、圖片訊息、文字訊息、網頁瀏覽歷史、行事曆、上千筆電話簿及其他內容。我們相信，實體的可行性與數位能力之間的鴻溝，在將來只會持續擴大。

手機的儲存能力對隱私的議題有幾項相互關聯的結果。第一，一隻手機收集了許多不同種類的資訊在同一個地方—一個地址、一則筆記、一張處方籤、一份銀行明細、一段影片—這些資訊結合在一起，將比只有單獨紀錄揭露更多訊息。第二，即使只有一個種類的資訊，在手機的助力之下也可能傳達遠比過去的更多。一個個人的整體私密生活可以

透過數以千計標有日期、地點、描述的照片重建，這和在錢包內放入一或兩張你愛的人的照片所是不一樣的。第三，手機上的資料可以回溯到購買的那天，甚至更早。一個人可能在口袋內放一張紙條提醒自己要打電話給 Mr. Jones，不過不像手機例行性的紀錄，他應當不會帶著過去幾個月來跟 Mr. Jones 之間所有的通訊。最後，有一項區別手機與實體紀錄而具有說服力的元素。在數位時代來臨之前，通常人們不會隨身帶著整天經歷過後儲存敏感個人資訊的快取記憶體（cache）。現在，如果有人沒有帶著手機以及其內所蘊含的一切，那麼他將是個例外。根據一份調查，將近百分之七十五的智慧型手機使用者回報大部分時間將他們的手機放在五英呎（按：約一點五公尺）以內；百分之十二承認甚至在淋浴間也會使用手機。十年以前，警方在搜索被逮捕者時，僅偶爾會踩踏到高度私密的物品例如日記，但是這些發現可能是很少且很遙遠的。今日，對較之下，如果說超過百分之九十的美國成人擁有會紀錄幾乎生活中的每個方面—從一般到親暱—的手機，並不誇張。因此，允許警方去掌控檢視例行性基礎下的紀錄，是跟允許他們在偶然案件下搜索一兩個個人物品大大地不同。

儘管儲存在手機的資料光在數量上就足以跟實體紀錄作出區隔，部分類型的資料在質量上也有所不同。舉例而言，一個網路搜尋跟瀏覽歷史可以從一隻有上網功能的手機中被發現，從而揭示了一個個人的隱私利益及顧慮。或許，一筆關於某些疾病症狀的搜尋，可以與頻繁的造訪 WebMD（按：一個美國線上的健康資訊網站）網站對應起來。手機上的資料也可以揭露這個人曾經在何處，歷史位置資訊是許多智慧型手機的標準特色，可以用來重新建構某個人特定的移動路徑，精細到以分鐘為單位，而不是只告訴你在市區內甚至是某特定建築物。

手機上的行動應用軟體，或簡稱 apps，提供了廣泛的工具用來管

理一個人全方位的生活細節資訊。有為了民主黨跟共和黨新聞設計的 apps；有酒類、藥物、賭博成癮的 apps；有分享禱告需求的 apps；有追蹤懷孕症狀的 apps；有規劃你預算的 apps；有各種可以想見的嗜好跟消遣 apps；有改善你生活情趣的 apps。有購買或販賣各種物品的受歡迎 apps，而這些交易紀錄可以無限期的從手機中取得。現在「這東西有個 app（there's an app for that）」慣用語已經是流行詞彙的一部分。平均每個智慧型手機使用者安裝了三十三套 apps，這些匯集在一起將成為手機使用者的生活剪輯。

在 United States v. Kirschenblatt, 16 F. 2d 202 (2nd Cir. 1926) 案件中，曾有這麼一段觀察：搜索一個人的口袋並且用其內含來攻擊他，跟洗劫他家裡的每樣東西找出可以定罪的物品，是兩碼子事。然而，如果這個人口袋裡是一隻手機，那麼這項觀察就再也不適用了。確實，對手機的搜索典型上暴露給政府的，會比對一棟房子竭盡所能搜索的還要更多：一隻手機不只包含以往在家裡會找到的數位形式敏感紀錄，他也包含了要不是手機本身的存在，否則不可能在家中以任何形式存在的廣泛私人資訊。

進一步細緻化受到危害的隱私權利益範圍，現代使用者在手機上檢視的資料可能沒有實際儲存在裝置本身內。將手機視為一個容器，它的內容就能被附帶搜索取出，作為一個初始議題是有一點勉強的。當手機被當作一個觸控螢幕，然後作為從他處存取資料的終端機，此時容器的類比完全被粉碎，這是因為越來越多手機頻繁地被設計成利用雲端運算（cloud computing）的優勢。雲端運算是一種網路連結裝置的能力，來顯示儲存在遠端伺服器內的資料，而非儲存在裝置本身。手機的使用者可能不會經常察覺特定的資訊究竟是儲存裝置內或雲端，而且運作上大體沒什麼差別。此外，同一種資料可能對某個使用者是儲存在手邊

的裝置內，同時另一位使用者則是儲存在雲端。

政府坦承附帶搜索的例外可能無法延伸覆蓋到搜索遠端存取的檔案，也就是說，對儲存在雲端的檔案進行搜索。這樣的搜索很像是在嫌疑人口袋中找到一把鑰匙，並且爭論這樣就允許執法單位打開房屋並且搜索。不過，警方搜索手機資料時通常也不知道他們正在檢視的資訊，是在逮捕時就已經存在手機內，或者剛從雲端內被下載。即便政府承認這樣的問題，所提出的解決方案也不明確。政府建議在搜索裝置之前，可以先斷開它的網路連線—這個方案如同面遠端抹除資料的威脅時一樣，政府也對它的可行性提出辯護。另外，政府提案執法單位發展面對雲端運算議題時可採用的協議。或許是一個好主意，但是建國者們展開革命並不是為了爭取政府單位的協議。搜索遠遠延伸到被逮捕者的實體近身距離的文件及財物以外，是隱私權利益在這裡縮小 *Robinson*[21]先例的一個理由。

除了以 *Robinson* 先例作為論述的直接延伸，政府也提出了在某些情況下，允許無令狀對手機搜索多種的退讓觀點。每一個提案都是有瑕疵的，與法律意旨一般傾向透過規則分類的方式，提供執法單位清晰的指引相違背。政府以前提是官員合理相信手機部分區域內的資訊，可能與犯罪有關，則以此區域為侷限，提出限制手機搜索範圍的規則。這個方法僅僅對官員添加了些微有意義的限制，官員也總是無法進一步區分什麼資訊會在哪裡找到，如此分類將會席捲大量的資訊。政府又以 Smith v. Maryland, 442 U.S. 735 (1979)作為依據，該案中法院支持使用電話公司內的「撥號記錄器」去辨識某個人曾經撥打的電話號碼，並不

[21] United States v. Robinson, 414 U.S. 218 (1973)。該案法院認定即使沒有證據滅失的顧慮，逮捕者也沒有明確證據顯示 Robinson 可能有武裝，對他的搜索仍然是合理的。經由「個案認定」，來決定是否存有理由支持當局對人合法逮捕後附帶搜索，此一概念遭法院否決。

需要令狀，進而認為官員總是被允許搜索一隻手機內的通話紀錄。我們也否決這項政府最後的論點，因為 *Smith* 案件中法院是認定使用「撥號記錄器」不屬於憲法第四修正案中的搜索。除此之外，通話紀錄通常不是只有電話號碼本身，他們也包含了對於個人的識別資訊，例如「我的家」等標示。

最後，言詞辯論時，政府建議一項特別的限制原則，這個論點是如果官員可以合法取得數位時代前同樣的資訊，則在數位時代，官員可以對手機內相對應的部分進行搜索。然而，數位時代前的搜索可能到頭來只是一兩張皮包中的照片，這不能正當化搜索手機中數位相簿中數以千計的照片。某個人隨手將銀行交易明細塞到口袋中，也不能正當化搜索過去五年內每一份的交易明細。更糟的是，這種類比測試將會允許執法單位大範圍搜索手機內的物件，即使現實上人們根本不可能在身上帶著如此多的不同實體資料。以 Riley 的案件來舉例，如果 Riley 在口袋內塞著錄影帶、相簿、地址簿，並帶著它們在街上遊蕩閒晃，根本難以置信。由於前述每一項目（錄影帶、相簿、地址簿）都有數位時代前的先例可以類比，這種作法將導致警方得以搜索手機內全部的物件，這是對於隱私權的重大侵害。除此之外，類比測試將使得法院在決定何種數位檔案可以對應到實體紀錄時，產生劃出一條明確界線的困難。電子郵件可以類比成傳統信件嗎？聲音信件可以等同於電話留言錄音嗎？在官員執行搜索之前，我們根本不清楚他們是如何作出類比決定的，或者法院事後會如何評價官員舉出的類比案例，也不明確。類比測試將使得被告、法庭深陷在不確定的風暴裡。

當然，我們的結論不是在手機裡的任何資訊都豁免於搜索，相反的，是執行這類搜索之前通常需要取得令狀，即便手機是從逮捕後的附帶搜索取得。長久以來累積的案例已經告訴我們，搜索令狀的要件是政

府運作時的重要元素，而非只是警方在追求工作「效率」時對他們造成不便的角色。如同我們上述討論的，近年來科技的進展，反而使向法院取得令狀更加有效率。此外，儘管附帶搜索的例外不適用在手機上，不過在某些情況下是可以正當化對手機無令狀搜索的。一個廣泛被認可的情境是「緊急情狀（exigencies）」，此時執法單位迫切地需要執行無令狀搜索，仍客觀合理的符合憲法第四修正案。這些緊急情狀可能包括在個案裡面避免證據面臨被摧毀，或者是追捕正在逃離的嫌疑犯，還有協助身受重傷或面臨生命威脅的民眾。舉例來說，在 United States v. Chadwick, 433 U.S. 1 (1977)案件中，法院認為附帶搜索的例外不能合理化對一個重達二百磅的提箱搜索，不過值得注意是，如果官員有理由相信這件行李含有造成立即危險的裝置，例如爆裂物，則沒有事先檢查直接將它帶回警局是有勇無謀的舉動。考量到各種緊急情狀例外的可行性，我們不相信執法單位不能找出過往案例中極端的情形作為參考，像是：嫌疑犯正在傳訊給同夥說要引爆炸彈了；或是兒童綁架嫌犯手機內有被害人的位置資訊。此時，被告往往不會爭執這些情況不能正當化對手機資料的無令狀搜索。重點在於，不像附帶搜索的例外，緊急情狀的例外需要法院在每一個案件中檢驗是否符合無令狀搜索的要件。

現代手機不只是另一個方便的科技工具而已。手機所包含的及所揭露的，可能是許多美國人一生的全部隱私。科技讓一個人得以攜帶這些資訊在手邊，並不會讓這些資訊不值得被建國者所追尋的價值保護。對於警方在附帶搜索扣押到的手機，要對他進行搜索有什麼限制，我們的答案很簡單：取得搜索票。

## 貳、UNITED STATES V. WARSHAK[22]

### 一、背景事實

Warshak 擁有並經營 Berkeley 頂級營養品公司，公司產品 Enzyte 是營養補品，宣稱可以增加男性勃起的尺寸。但 Enzyte 的銷售是由一連串的欺騙所支撐，Warshak 跟 Berkeley 虛構顧客調查跟醫學背書，沒有通知或得到顧客同意就登記為月費訂購計畫，且製造虛假交易去隱藏顧客高比例對於 Berkeley 信用卡扣款的爭議。Warshak 被判決郵件詐欺、銀行詐欺、洗錢及其他罪名。他被判處有期徒刑二十五年及沒收超過五百萬美元的不法所得。政府在案件中部分使用從網路服務業者取得的電子郵件來證明他的罪行。

Stored Communications Act（“SCA”, 18 U.S.C. §§ 2701 et seq.）允許政府單位在某些情境下，要求服務提供者揭露電子通訊的內容。電子郵件是 Berkeley 公司重要的人事通訊方式，Warshak 在不同網路服務業者有數個電子郵件帳號，包括向 NuVox Communications 申辦的帳號。在 2004 年 10 月，政府正式地要求 NuVox 保存任何往後從 Warshak 帳號進出的電子郵件內容，NuVox 同意政府的要求並開始保存從 Warshak 帳號進出電子郵件的複製本，這些複製本來在沒有政府要求的前提下，是不會保存的。每次遵照政府的指示，Warshak 都不會被通知他的通訊已經被建檔。在 2005 年 1 月，政府依照§2703(b)取得傳票並迫使 NuVox 交出從去年開始保存的電子郵件；在 2005 年 5 月，政府依照§2703(d)取得單方面法庭命令要求 NuVox 提交 Warshak 帳戶內額外的電子郵件。最後政府總計要求 NuVox 揭露了約二萬七千封電子郵件的內容，這期間 Warshak 並沒有收到任何傳票或命令的通知，直到 2006 年才知

[22] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

悉。

## 二、法律議題

Warshak 爭執政府單方面的無令狀扣押大約二萬七千封他的私人電子郵件，違反了憲法第四修正案的禁止不合理搜索及扣押原則。政府則回應，就算承辦人員在取得郵件時違反了憲法第四修正案，但他們是善意信賴 SCA，該法律允許政府可以取得部分電子通訊而不須經由搜索令。政府也爭執任何假設的憲法第四修正案違反都是無害的。我們發現政府強迫 Warshak 的網路服務業者交出他電子郵件的內容，確實違反了 Warshak 的憲法第四修正案權利。

並不是每項政府行動都是侵略性到涉及憲法第四修正案的議題。憲法第四修正案的保護取決於搜索行為是否在行動中出現。搜索，藝術性的法律名詞，它的歷史布滿著複雜謎題。這個標準再切成兩個細究：第一，調查對象對於被搜索的物件主觀上是否有隱私的期待性？第二，我們的社會認為這種期待是合理的嗎？先探究第一個主觀要件，我們發現 Warshak 顯然期待他的電子郵件會避開外部的監看。如同 Warshak 提出的陳述，他整個事業跟個人生活都包含在被扣押的電子郵件內，即使他的郵件常有敏感性或應受譴責的內容，我們認為 Warshak 不可能希望這些郵件被公開，就像人們鮮少在大眾目光前公開骯髒的洗衣間一樣。

下一個問題是社會大眾是否準備好承認這種期待是合理的。這個問題具有重大意義及長遠後果，因為電子郵件在現代通訊中扮演著不平凡的角色。自從電子郵件的誕生，電話、信件逐漸失去重要性，而網際網路為基礎的通訊則爆炸性地成長，現在人們可以瞬間傳送敏感、親暱的訊息給朋友、家人，甚至是半個地球外的同事。情侶來往甜言蜜語，

業者交流事業，全部都只發生在點擊滑鼠一下的瞬間。商業也開始被電子郵件掌控，線上訂單經常以電子郵件帳號建檔，電子郵件也經常被用來提醒病患、客戶約定的時間。簡而言之，「帳戶」是一個適當的用字來代表組成電子郵件帳號的所有儲存訊息，帳戶代表著使用者的生活。藉由存取某個人的電子郵件，政府人員得到了窺視他人活動的能力。因此，更應取決於政府是否被允許要求商業的網路服務業者提供用戶的電子郵件而沒有啟動憲法第四修正案的機制。

面對這個問題，我們採取兩項基本原則。第一，根基事實資訊經由通訊網路傳送是憲法第四修正案的重要議題。第二，憲法第四修正案必須追上科技的無情進步，否則它的保證即會枯萎跟消失。將以上原則放在心中，我們先思考憲法第四修正案是如何保護傳統形式的通訊。最高法院在 Katz v. United States, 389 U.S. 347 (1967)決定憲法第四修正案是否能適用在電話的情境上。該件事實是政府探員在外面的公共電話亭上安裝了電子竊聽裝置，藉此攔截並錄製了幾段電話對話。最高法院的決定是這是憲法第四修正案意義下的搜索，儘管電話公司本有能力監視並錄製通話內容，但最高法院的看法是通話者確信他所對話筒說的話將不會被播送到全世界。從這時起，政府若偷偷摸摸地使用電子方式攔截通話，該先例成為許多情境下政府侵犯合理隱私期待的廣泛主張。

信件也得到類似的保護。當信件是以郵件的方式存在，警方不能攔截並且檢視它的內容，除非他們基於合理根據先取得了搜索令。我們必須坦承，儘管信件被密封，一旦被交付到運輸業者手上，任何業者都有可能將隔絕信件內私人訊息與外部世界的薄薄信封袋撕開。不過換一個角度想，因信任而將信件交給中間媒介，不必然表示喪失對於信件保有隱私的期待。任何人尋求保護隱私，即使是在公眾可以觸及的地方，仍應受到憲法保障。

在電子郵件跟傳統通訊的根本相似性之下，若賦予電子郵件較小的憲法第四修正案保護是蔑視公眾意識的。電子郵件是實體信件的科技幼苗，在資訊時代扮演著不可或缺的角色。過去的十年以來，電子郵件已經變得如此普遍，有些人甚至認定電子郵件是自我表達、自我認同的必要方法跟渠道。隨之而來的是電子郵件在憲法第四修正案下受到高度保障，否則憲法第四修正案將成為私人通訊的無力保護者，這是它長久以來所致力的目標。有些通訊方式開始消逝，憲法第四修正案必須認知並保護新生崛起者。

如果我們接受電子郵件跟電話、信件的類比，很明顯地，政府探員不能在沒有憲法第四修正案的機制下強迫商業網路服務業者交出電子郵件的內容。是網路服務業者讓電子郵件成為可能，電子郵件必須經由網路服務業者的伺服器傳遞到收件者手上。因此，網路服務業者的功能等同於郵局或電信公司。如同先前討論的，警方不會為了攔截郵件對郵局掃蕩；同樣地，警方也被禁止使用話務系統對通話進行祕密錄音，除非他們有取得令狀。如果政府探員迫使網路服務業者提出用戶的電子郵件內容，則探員實際上是在進行憲法第四修正案的搜索，修正案促使探員在沒有例外情形下遵守令狀原則的要求，只有在這種情況下才是合理的。本件先前政府曾主張上述結論是不適當的，指出 NuVox 的契約保留了特定目的下存取 Warshak 電子郵件的權利。然而，如果在某些情況，我們肯認用戶的同意廣泛到足夠擊倒對於電子郵件帳戶內容的合理隱私期待，但我們質疑是不是真的會有這種情況，而且也很明顯地與本案情況不同。

作為初始討論，我們首先必須觀察到，就算第三方中介有能力存取通訊內容，也不足以抹去對於隱私的合理期待。在上述 *Katz* 先例最高法院發現在通話中對於隱私的期待是合理的，儘管電話操作員有能力

聽取通話內容。同樣地，一位魯莽的郵件處理者縱使有能力撕開一封信，也不會減損密封信件在流通的過程中仍然保持私密的假設。因此，通訊被存取的威脅或可能性，並不是對於隱私合理期待的決定性因素。另外，存取的「權利」也不是決定因素之一。如同法庭之友 Electronic Frontier Foundation 指出，在前述 *Katz* 先例被決定的年代（1967 年），電話公司在某些情況下有權利監聽通話，特別是電話公司為了對抗不適當及非法使用通話設備，以保護自己及財產，而認為有合理必要時即可聽取通話。而在本件，我們追蹤 NuVox 的使用者政策，其指出在操作過程中及有必要保護 NuVox 服務時，NuVox 得存取及使用個別用戶的資訊。因此，授權給 NuVox 的存取程度，並不會削減 Warshak 信任他的電子郵件隱私的合理性。

我們的結論發現了在出租空間應用憲法第四修正案的額外支持。舉例而言，飯店顧客在他們的房間內有合理的隱私期待，即使清潔人員例行性的進入房間更換毛巾、清潔房內設施。同樣地，房屋租客也有在其公寓內合法的隱私期待，就算維修工為了修理漏水的水龍頭而入侵公寓也一樣。結論上來說，我們已被說服，某種程度的例行性存取很難成為隱私問題的決定性因素。然而再一次地，我們也不願意作出用戶條款永遠不會廣泛到足以消滅合理隱私期待的結論。如果網路服務業者表明了稽核、檢查、監看用戶電子郵件的意圖，這就可能足夠作為沒有合理隱私期待的論點。不過本件並沒有這種聲明，網路服務業者對電子郵件的控制、特定限制條件下存取的能力，都不足以超越對於隱私的合理期待。

我們認知到我們的結論可能被以最高法院在 United States v. Miller, 425 U.S. 435 (1976)的決定抨擊。在 *Miller* 案件最高法院決議銀行存戶對於他的銀行紀錄、支票、存款憑條等內容不存有合理隱私期待。該案

的決定的背景事實是立基於銀行文件包括財務狀況及存款憑條僅包含自願傳達給銀行的訊息，以及也會暴露在經手員工例行工作流程中之上。法院特別提到，存款者承擔了揭露個人事務給他人時，他人也會將資訊傳達給政府的風險，憲法第四修正案並不禁止政府取得向第三方揭露並且由第三方提供的資訊，就算這些被揭露的資訊，是假設只能使用在限定的目的，以及信任第三方不會有背叛行為。

上述 *Miller* 案件是不同的。第一，該案只有涉及簡單的商業紀錄；相對地，本件議題是潛在著無限制、各式各樣的機密通訊。第二，該案中存款者對銀行傳達訊息以便銀行將這些訊息置入例行的工作流程中；相較之下，Warshak 透過 NuVox 的服務收受電子郵件，NuVox 不過是個中介，並不是郵件設定的收件者。因此，*Miller* 案件不能適用於本件的論述。

承上所述，我們認定，不論電子郵件是透過商業網路服務業者被儲存、傳送或收受，用戶對他們的電子郵件內容享有合理的隱私期待權利。政府在以有相當理由（Probable Casue）向法院取得搜索票以前，不能迫使一個商業網路服務業者交出用戶的電子郵件內容。因此，本件政府並沒有取得搜索票，則在得到 Warshak 電子郵件內容時，政府探員就已經違反了憲法第四修正案。更有甚者，在 SCA 所宣稱允許政府在取得此類電子郵件無須令狀的程度下，該法案是違憲的。

## 參、UNITED STATES V. SPENCER[23]

### 一、背景事實

2017 年 4 月 26 日輔助法官核發令狀給 FBI 對據信是 Spencer 住處的地方執行搜索。令狀授權的搜索範圍除了處所、Spencer 本人以外，

[23] United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588(N.D. Cal. Apr. 26, 2018).

還包含任何電腦、儲存媒體、路由器、數據機、網路設備，作為 Spencer 涉及兒童色情的證據。

FBI 執行搜所並扣押了可能含有兒童色情的十二項電子媒體物件。然而，其中幾項裝置被加密了，無法存取其中的內容。政府以 All Writs Act, 28 U.S.C. § 1651[24]尋求法院命令，迫使 Spencer 解密其中三項裝置，分別是智慧型手機、筆記型電腦、外接式硬碟。Spencer 坦承持有智慧型手機、筆記型電腦，也提供了通過螢幕鎖定的密碼（但不包含解密這兩項裝置的硬碟）。至於外接式硬碟，是跟筆記型電腦在同一張桌子上扣到。Spencer 宣稱他擁有一個硬碟，符合本件所述的扣案外接式硬碟，而且他對自己的硬碟以軟體加密，同一套軟體也有在扣案硬碟上發現。

治安法官於 2018 年 3 月 20 日同意政府上述聲請，命令 Spencer 須配合解密這三項裝置。針對這項命令，Spencer 於 4 月 16 日向法院聲請救濟。

## 二、法律議題

美國憲法第五修正案闡明刑事訴訟程序的不自證己罪原則。實務上認為，該原則只適用在迫使被告作出入己於罪的陳述。如果只是命令被告交出與犯罪相關的證據，此時並未違反不自證己罪原則；相反地，不自證己罪原則將適用在證據產生行為（act of production）本身是既「證述的（testimonial）」也「入罪的（incriminating）」。

當對證據產生行為的讓步，僅增加些許政府原本持有的資訊總量或毫無影響，且被告事實上也坦承他持有證據，則證據產生行為是既「不證述」也「不入罪」的。換句話說，此時證據產生行為傳達的資訊

[24] 28 U.S.C. § 1651
(a)The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.
(b)An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

是一個既定的結論（foregone conclusion）。既定結論的範圍是很重要的，它只適用在相關證詞是證據產生行為本質上隱含的陳述。否則的話，政府不能強迫作出自我入罪的陳述，即使這些陳述的內容屬於既定結論。舉例而言，不論是口頭或手寫，政府不能強迫 Spencer 說出密碼。但政府其實不是在尋求密碼，而是在尋求裝置的解密。Spencer 爭執檢視這些裝置的產出需要他輸入解密密碼，因此沒有落入證據產生行為原則的範圍。換句話說，Spencer 爭執既然政府不能強迫他說出裝置的密碼，就也不能強迫他用這些密碼來解密裝置。這項極其表面的爭執，也得到了一位法官的支持，認為本件就像前例 Doe v. United States, 487 U.S. 201 (1988)所論述的，不能強迫被告揭露保險箱的轉盤密碼，不論是文字上或行為上的。雖然以下比喻不盡完美，但我們可以假設儲存在加密裝置上的證據等同於存放在保險箱內被轉盤密碼保護的物品，就可以將不同意見法官的理解套用在目前的情況。

若存在一個政府不能強迫解開密碼保護裝置的規則，將會導向一個荒誕的結果。例如能否要求被告提供解密過的硬碟，將取決於被告加密硬碟時是使用指紋密碼或符號密碼。同樣的，接受保險箱的類比，一個人接到可能涉及憲法第五修正案（按：不自證己罪）的法院傳票要求他提供文件（subpoena for documents），是否要交出也會取決於這些文件究竟是放在密碼保險箱或鑰匙保險箱。但我們認為在保險箱上應該是沒有不同的，因為打開保險箱沒有要求被告產出密碼並交給政府。是否交出資料，不管是書面或數位格式，就算與憲法第五修正案有關，也不應受到被告存放資料的方式所影響。政府對裝置解密的要求，需要證據產生行為。然而，這個行動可能代表產生入罪證詞而落入憲法第五修正案的範圍，因為政府的要求，等同於表示 Spencer 有對裝置解密的能力。這樣的表示潛藏著入罪性，因為有解密的能力，Spencer 更有可能

將裝置加密，也導致 Spencer 自己會將更多極其重要的證據，存放在該裝置內。

下一個問題是既定結論規則是否適用。在普通法體系會有一些困惑，就是到底相關既定結論必須存放在政府所尋求解密的裝置內的哪裡。第十一巡迴法院曾作出決定，在既定結論規則上，政府不只需要展示被告有能力解密裝置，同時也要指出裝置內的特定檔案。該案例拒絕政府強迫被告解密裝置的請求，因為政府並未展示任何對於裝置內檔案是否存在或在何處的了解。但是本件與前述案例不同，是單只有交出被加密的裝置，無法與允許取得裝置內特定檔案或相關資料等量齊觀，因為本件政府沒有要求任何特定的檔案。因此，政府只需要展現出本件是既定結論，而且 Spencer 有能力去解密該裝置。跟經由傳票搜尋特定檔案相較，透過對硬碟的搜索令，政府可能從硬碟存取更多資料，但這些都是政府在尋求存取時所使用的法律工具。

目前為止對於適用法律框架的討論，唯一剩下的議題就是法院在評估 Spencer 知道密碼是否為既定結論時，要採用什麼標準。適當的標準應該是清楚且有說服力的證據，這帶給政府高度的舉證責任，來證明被告有能力解密裝置是一種既定結論。本件三項裝置都是在 Spencer 的住處內找到，Spencer 也坦承智慧型手機、筆記型電腦是他的，並提供了登入密碼。此外，Spencer 也承認他曾經買過一個外接式硬碟並對它加密，這些描述符合政府的搜索發現。以上顯示政府已達成其舉證責任。因此，政府可以強迫 Spencer 解密裝置。然而，即使 Spencer 解密完成，政府可能不能直接使用他解密所得的資料。如果是一個真正的既定結論，則他有能力且對裝置的解密行為，不是「證述的」，政府當然不應該將證據產生行為本身作為證據使用。

# 第五章 美國跨界案件爭議

## 第一節 數位國界[25]

在 1990 年代，許多專家、學者相信網際網路正在侵蝕政府的權限。網頁顯著的特色—立即及廣布的通訊、地理上的匿名性、去中心化的途徑—使得國內的電腦使用者可以輕易地透過電腦取得在國外的違法資訊。美國大學生可以從架設在南太平洋的伺服器下載版權歌曲，參與在安提瓜舉辦的數位二十一點賭博。沙烏地阿拉伯公民可以瀏覽架設在荷蘭的色情網站，義大利人可以從澳洲的網頁閱讀他們的禁書。國家似乎無法阻止網際網路上有關違反當地法律的行為。

網際網路的概念在 2000 年 4 月開始崩潰。當時兩個法國反種族歧視組織在法國控告美國入口網站 Yahoo!。這些團體指控 Yahoo!所屬的拍賣網站有販售納粹相關商品，而在法國可以瀏覽到這些內容，這違反了法國法律禁止納粹物品的流通。在當時比起其他網站，Yahoo!作為進入網路的入口網站有著更多的使用者。Yahoo!的富豪共同創立者 Jerry Yang，是自信但急性的人，根據網站上公司的官方歷史，他跟另一位創辦人 David Filo 將公司取名「yahoo」的原因，是他們喜歡「yahoo」的定義：魯莽、不精緻、粗野。被公司快速擴張的市占率沖昏頭，Jerry Yang 認為政府愚蠢，由其對言論的限制更是。當 Yahoo!收到來自巴黎審判法院法官 Jean-Jacques Gomez[26]的傳票，Jerry Yang 只是聳聳肩膀。反映出傳統的看法，Jerry Yang 相信巴黎的官員對於在美國的電腦沒有任何權限。

如果法國沒有任何手段可以阻止在美國的 Yahoo!，法國官方也似

[25] Jack Goldsmith and Timothy Wu (2006), DIGITAL BORDERS, at https://www.legalaffairs.org/issues/January-February-2006/feature_goldsmith_janfeb06.msp (last visited 2020/3/20).

[26] Judge Jean-Jacques Gomez of Le Tribunal de Grande Instance de Paris.

乎沒有管道可以在國內阻斷對納粹拍賣網的存取。有太多網際網路通訊管道可以跨越法國國界，而政府沒有能力去阻止及全面監管。網際網路的去中心化路徑系統能夠點對點地傳遞訊息，即使中間部分途徑被阻斷、傷害或摧毀。自由網路倡議者，同時也是 Electronic Frontier Foundation 的共同創立者 John Gilmore 宣稱，網狀結構讓審查能力有缺陷，並且可以繞過它。為了阻斷納粹網頁，法國必須切斷國境內每個網路存取點，但這看來是一項不可能的任務。

Yahoo!的抗辯是以 1990 年代版本的無國界網路為前提。在五年後，這個版本快速地被新的現實取代，新的觀念是網路可以分拆且反映國家界線。網路並沒有將世界扁平化，反而在許多方面是遵循了當地的條件。結果是，網路逐漸被法律的障壁、語言及審查機制隔離開來。加上界線的網路反應出從上到下來自政府的壓力，像是法國正在國內對他們的網路實施內國法。不過，這也反應從下到上，不同領域的個人希望網路可以符合他們的個人偏好，而形塑網路使用經驗的網站經營者及其他內容提供者則會滿足這些需求。

Gomez 法官在 2000 年 5 月初步裁定美國網站 Yahoo!違反了法國法律，他命令該公司採取全部必要措施阻止法國網友能夠在 yahoo.com 瀏覽非法的納粹拍賣訊息。Jerry Yang 不屑一顧，他表示：「我們不會改變任何在美國網站上的內容，就只是因為在法國有人要求我們這樣做。」、「以上網者的國籍要求我們過濾網站的存取是非常天真的。」Jerry Yang 的蔑視反映關於網路結構的世紀轉換假設。網路通訊位置（Internet protocol addresses，每台電腦的網路身份認證）、網域名稱（Internet domain names，例如 mcdonalds.com or cnn.com）、e-mail 信箱並不是被設計成指出網絡內電腦的地理位置。這些結構上的事實意味著大多數 1990 年代網路科技的使用者不知道他們的 e-mail 訊息跟網頁

被觀看了，更別說在哪個國家何種法律被違反了。Yahoo!宣稱他們不知道他們的使用者在何處，以及應該遵循怎麼樣的法律。更糟的是，如果法國能夠掌控在美國的 Yahoo!，則其他國家也應當有能力如此。這引起一個令人擔憂的可能性，網路公司跟使用者面臨著相互衝突的各國法律，可能會開始採行其中之一最嚴格的以免除任何的法律風險。Center for Democracy and Technology 的 Alan Davidson 預測，我們現在正面臨「逐底競爭（race to the bottom）」[27]，關於網際網路內容最嚴格限制的規則—由任何一個國家所制定，可以影響全世界的人們。

要不是一位當時在紐約 Silicon Alley 工作的法國人 Cyril Houri 看似不太可能的介入，也不會有衝突的國家間法律適用到 Yahoo!在網路上每筆交易的隱憂，使得 Yahoo!經常被推向審判的邊緣。1999 年 Houri 在返回巴黎的旅途中，他有一項發現顛覆他作為軟體工程師的職涯，更別提對於網際網路的傳統思考。Houri 在他雙親的公寓待著，某天晚餐後他翻開筆記型電腦打算收 e-mail，隨著電腦開機他注意到在紐約時習慣瀏覽的入口網站。在他螢幕上方的閃亮閃亮興高采列的橫幅廣告是美國的送花服務，伴隨一組只能在美國撥打的電號號碼：1-800-flowers。在這當下，Houri 理解到網際網路並沒有無情地指向邊界扁平化。相反地，他看到一個無國界的送花服務，一點道理也沒有。他領悟人們願意購買一個以真實國界為基礎的軟體，並且在網路上重新創造，這樣一來送花員跟其他數千電子供應商就會知道他們的顧客在哪裡。他想，一個讓美國以外的人看不到美國的廣告的技術，將是一筆大生意，取而代之的是法國廣告給法國人、德國廣告給德國人。同樣的科技將允許新聞跟娛樂網站依據他們的觀眾所在位置提供不同區塊的內容。這一切所需

[27]係指在全球化的過程中，資本為了尋找最高的報酬率而在世界各地流竄，導致政府在有關福利體系、環境標準和勞工保障的政策執行受到限制。原文以此概念類比網路世界。

的是一套可以鎖定使用者實體位置的程式。因此，Houri 創立了一間網路公司 Infosplit，致力於達成他的發想。

自從 1990 年代網路開始商業化以來，網路公司嘗試辨識他們顧客的地域身分，關於這點成功的程度各自不同。例如，網頁上無所不在的「請選擇國家」連結是一種方式。另一個是使用者在被允許進入網頁之前，要求他們透過傳真或信件提供一組區域碼或是其他地域識別資料（例如駕照）。還有一種是以確認信用卡所登錄的地址當作地域識別的證明。但是，以上這些方式有時候是不可靠的，更糟的是，他們非常耗時。「網頁的重點是簡單且快速地取得你的資訊」、「為什麼我要看網頁之前要捲動一整串國家？必然有一個方式讓網站知道我在哪裡」，地域識別公司 Digital Envoy 的創辦人 Sanjay Parekh 在跟 Houri 相似的靈機一動過程中得到的想法。

在過去的十年間，Infosplit、Digital Envoy 及其他幾間公司開始試著讓網路上的地域識別簡單、可靠及不可見。不是要求網路使用者採取步驟揭露或證明位置，相反的，他們設計一種方式依靠網際網路的根本結構辨識使用者的地理位置，雖然網際網路的設計是預設忽略地理位置。IP 位置（例如 192.168.0.55）並沒有真正地揭露電腦使用者的實體位置，不過一個精明的使用者透過在網路上發送追蹤封包（tracing packets）可以決定他們的位置。這些封包包含了一連串他們旅程中所經過的電腦資訊，某種程度上像是一輛車行駛高速公路網後在每個收費站蒐集到的收據。正如同一台車的出發地可以從檢視收費站收據判斷，電腦可以檢驗這些封包釐清最近的起始點跟所有在通訊網中曾收受封包的端點。透過記錄連上網路所有電腦的地理位置的 IP 資料庫，提供線索進行交互比對。當資料庫相互參照跟分析以後，在國家層級方面，網路使用者的位置可以精確到超過百分之九十九。

網路地理辨識服務還處於新生階段，但是他們已經開始影響電子商務。在美國，網路上的身分竊盜每年造成商家、消費者損失數十億美元。Geo-ID 可以解決這個困境，例如被竊取的信用卡號碼在網路上被使用，然而地點卻是在許多詐騙發源地的俄羅斯。如同 Houri 跟 Parekh 所預見的，Geo-ID 也可以改善網路廣告，讓廣告可以更容易配合當地條件展示。此外，Geo-ID 也加速了電子資料的傳送，讓公司可以從最近的快取（cache）網站傳遞內容，再也不用詢問消費者人在何處。最後，可能是最重要的，這些科技開始使得地域性娛樂成型。在網路上傳播娛樂的一項障礙是某些內容在其他地方被瀏覽是非法的。Geo-ID 科技可以解決這個困難，只要確保線上電影、賭博網站、軟體程式跟其他數位產品不會進入認定這些活動是違法的國家。換句話說，設計用來反應當地消費者需求的軟體，也可以幫助不同地方不同法律的遵循。

在 Gomez 法官 2000 年 5 月的初步裁定之後，Houri 聯絡原告方律師 Stephane Lilti 說，他的軟體可以識別跟掃描網際網路的內容的地理來源。Houri 隨被被邀請到巴黎向 Lilti 展示他的軟體如何運作。當原告的法律團隊看到軟體回報結果的時候，全都感到相當驚訝。因為，Yahoo!宣稱他們的伺服器受到美國憲法第一修正案（按：言論自由）的保護，但實際上竟然是架設在斯德哥爾摩的網站。Yahoo!經常將在美國本土的網站內容，放置一份鏡像（mirror）複製本到瑞典，以加速在歐洲的網站存取速度。當審判繼續在 2000 年 7 月進行時，Yahoo!的律師團隊重申，不可能辨別跟過濾來自法國的拜訪者，使他們無法瀏覽該公司美國基礎的網站。作為回應，Lilti 則解釋 Houri 的地理辨識科技，展示在法國的 Yahoo!拍賣實際上不是來自在美國的伺服器。突然間，每個網頁被世界上每個角落的每個使用者公平存取，這個假設看似錯了。如果 Yahoo!有能力從瑞典的伺服器把內容傳導給法國使用者，這意味

著 Yahoo!有能力以地理位置辨別使用者，並且，如果他們願意的話，將使用者屏除在外。之後，得到了更多額外關於地理掃描可行性的專家證詞，Gomez 法官在 2000 年 11 月作出了最後決定，認定 Yahoo!允許納粹商品銷售訊息出現在法國的網頁上，已經違反法國法律。Gomez 法官認定法國法院對 Yahoo!跟它的伺服器有審判權，因為該公司有意識地行動將被禁止的納粹拍賣頁面導向法國。Gomez 法官指出，Yahoo!對造訪他美國網站的法國使用者，以法語廣告打招呼，這表示 Yahoo!有對法國量身訂做網頁內容，某種程度上，可知它可以地理位置識別跟掃描使用者。雖然法院理解作到百分之百的屏障不可能，不過法院命令 Yahoo!作到合理的最大努力去阻擋法國使用者。

起初，Yahoo!宣稱不會遵循 Gomez 法官的決定。但公司馬上面臨一個問題：它在法國的資產，包括在法國附屬事業的收入，有被扣押的風險。在 2001 年 1 月，Yahoo!突然投降了，將所有納粹相關頁面從拍賣網站上移除，宣布在所有 Yahoo!的商業資產上，再也不允許任何擁護、榮耀仇恨或暴力的團體的相關物品刊登。這間公司的宣布是基於納粹拍賣的負面公眾形象，並不是因為法國的判決。Yahoo!表示：「我們社會整體已經拒絕了這種團體。」不過，時間點跟法國制裁的威脅，暗示了 Yahoo!其實已經屈服了。

## 第二節 刑事管轄權[28]

### 第一項 背景事實

本案促使法院決定，針對 Andrew Auernheimer 陰謀違反Computer Fraud and Abuse Act（CFAA）（18 U.S.C. § 1030），以及身分詐欺（18 U.S.C. § 1028(a)(7)）的刑事控訴，在紐澤西聯邦地方法院起訴管轄權是

[28] United States v. Auernheimer, 748 F.3d 525 (3rd Cir. 2014).

否適當。刑事案件的管轄權不只是技術性問題，它與刑事正義的公平監督跟公眾信任密切相關，尤其是在有著大量相互連結時代中的電腦犯罪。法院認定本案的管轄權不在紐澤西，因此廢棄聯邦地方法院認定有管轄權的決定，並撤銷 Auernheimer 的有罪判決。

AT&T 公司的網站對 iPad 使用者有一個安全性的瑕疵。為了簡化登入流程，如果使用者從他的 iPad 存取網站，AT&T 網站自動產生一個獨特的識別碼（ICC-ID），並將使用者導向已經填入 e-mail 地址的登入頁面。Daniel Spitler 發現，如果他讓他的電腦偽裝成 iPad，並且傳送隨機的 ICC-ID 給 AT&T 網站，他就經常的可以看到真正 iPad 使用者的電子郵件地址。Spitler 編寫了一套他稱為「account slurper」的程式自動化這個流程，蒐集大量的電子郵件地址。Spitler 將他的發現分享給 Auernheimer，他們是在網路聊天是認識但從未見過面的朋友。Auernheimer 協助 Spitler 改進這套「account slurper」程式，最終這套程式在 2010 年 6 月 5 日至 8 日蒐集到了十一萬四千個電子郵件地址。

當 Spitler 的程式持續在蒐集電子郵件地址時，Auernheimer 為了公告周知他們兩人的「偉業」，寄送電子郵件將這件事告知了幾位媒體從業人員。有些人將消息轉知 AT&T，他們隨即修補了這項漏洞。其中一位被 Auernheimer 通知的媒體人是 Ryan Tate，他是 Gawker 新聞網的記者。Tate 表達了對報導 Auernheimer 故事的興趣。為了取信 Tate，Auernheimer 分享了一串的電子郵件地址給他。接著，Tate 在 2010 年 6 月 9 日出版了一則故事描述關於 AT&T 的安全性瑕疵，標題是「蘋果電腦最大的安全漏洞：十一萬四千名 iPad 使用者被暴露」。這篇文章揭露了一些被取得電子郵件地址的姓名，不過，是以電子郵件地址跟 ICC-ID 資訊的截圖型式而被少量公開。

## 第二項 法律爭議

審判中顯示與本案有關的證據，Spitler 總是待在加州的舊金山，Auernheimer 則是在阿肯色州的法葉特維爾（Fayetteville）。而本案他們存取的伺服器，實體位置座落在德州的達拉斯、喬治亞州的亞特蘭大。儘管沒有證據顯示出 Gawker 新聞網記者在本案中的位置，但毫無爭議的，Tate 絕對不在紐澤西州。

儘管，本案欠缺與紐澤西明顯的連結性，在紐華克的大陪審團作出兩項指控 Auernheimer 的更新起訴罪名。罪名一是陰謀違反 CFAA（18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(ii)）而觸犯 18 U.S.C. § 371；罪名二是以個人資訊詐欺（通常引述為身分詐欺）而觸犯 18 U.S.C. § 1028(a)(7)。為了強化潛在的從輕罪到重罪的處罰，政府進一步指控 Auernheimer 之所以觸犯 CFAA，是為了實現紐澤西州電腦犯罪法律規範的構成要件（N.J. Stat. Ann. § 2C:20–31(a)）。

在大陪審團回以更新起訴後不久，Auernheimer 即請求駁回。除了主張幾項有關違反 CFAA 的挑戰，他爭執在紐澤西聯邦地方法院的管轄並不適當。即使，地方法院承認不論他或 Spitler 在本案發生時，人都不在紐澤西州，而且被存取的伺服器也不在紐澤西州，仍然否決了他的請求。地方法院認定陰謀違反 CFAA 的指控部分，管轄權是適當的，因為 Auernheimer 所揭露的電子郵件地址中，大約有四千五百位紐澤西居民，影響了他們及違反了紐澤西州法律。地方法院進一步指出，由於對陰謀違反 CFAA 的指控管轄權適當，所以身分詐欺部分的管轄權也是適當的，因為證明陰謀違反 CFAA 是證明身分詐欺犯罪的必要前提。

即使在本案上訴中提出了在這漸長的相互連結時代，許多複雜的、嶄新的、值得引起公眾討論的議題，不過，我們認為只需要檢視其中一個從建國時代就有的根本議題：管轄權。適當地點的殖民審判對於建國

世代是如此的重要，甚至被列為獨立宣言中的一項不平。它是如此被高度重視，美國憲法雙重保障被告的管轄權權利。憲法第三條要求，所有犯罪的應當在罪所被犯下的州審判（U.S. Const. art. III, § 2, cl. 3）；憲法第六修正案進一步指出，在所有刑事起訴中，被控訴者應享有迅捷、公開的陪審團審判，其中陪審團是由罪所被犯下的州及地區組成（U.S. Const. amend VI.）。以上的保證明文在 Federal Rules of Criminal Procedure 中，該法要求政府應當在罪名被侵犯的地區對被告提起控訴（Fed. R. Crim. P. 18）。

國會可能對特定的犯罪制定特別的管轄權要求。然而在本案，國會並沒有特別指示，因此我們必須決定本案的犯罪地。犯罪地必須從被指控犯罪的本質、行為的地點或組成的行為判斷。為了執行這項調查，一開始我們必須辨別構成該案的行為，以及區辨這些刑法上行為的執行地點。管轄權應該被精準的解構。繼續犯，例如一項陰謀起始於一個地區、完成在另一個地區，或者在一個以上地區侵犯，可以在任何一個開始、繼續、完成的地區偵查及起訴（18 U.S.C. § 3237(a)）。在陰謀控訴的背景之下，每當有共犯作出實現陰謀的舉動時，管轄權就可以被建立。政府必須以優勢證據證明管轄權。

罪名一控訴 Auernheimer 陰謀違反 CFAA( 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(ii))。在起訴書及審判中，政府認定本案行為本質上是以違反 CFAA 的方式達成觸犯紐澤西州電腦犯罪法律（N.J. Stat. Ann. § 2C:20–31(a)）。管轄權在任何 CFAA 被觸犯的地區，或任何促進該陰謀發生的地方，都是妥適的。

在 CFAA 控訴部分，條文指出，任何人故意未經授權存取電腦或超出授權，並藉此從被保護的電腦中得到資訊，應以本條文的(c)部分方式處罰（18 U.S.C. § 1030(a)(2)(C)）。為了讓被告定罪，政府必須證明

（1）故意（2）未經授權存取（或超出授權）（3）受保護的電腦（4）藉此得到資訊。法條的明文中揭露兩項必要的行為元素：未經授權存取、得到資訊。紐澤西州並不是這兩項行為元素的地點。審判中的證據顯示被存取的 AT&T 伺服器在德州的達拉斯、喬治亞州的亞特蘭大。此外，從陰謀開始、繼續、完成，Spitler 是在加州的舊金山得到資訊，而 Auernheimer 則是在阿肯色州的法葉特維爾協助他。在紐澤西州，沒有受保護的電腦被存取、沒有資料被取得。

然而，我們的分析尚未結束。因為政府不只是以一般陰謀違反 CFAA 來起訴 Auernheimer，也包括陰謀違反 CFAA 以實現州法的犯罪。紐澤西州法律認為以下情形須擔負刑事責任：若明知或故意，未經授權或超出授權，存取任何電腦或電腦系統，並明知或魯莽地揭露、引起揭露任何資料…或個人識別資訊（N.J. Stat. Ann. § 2C:20–31(a)）。該條文的必要行為元素是未經授權（或超出授權）存取，以及揭露資料或個人識別資訊。在此，沒有任何違反紐澤西州法律的必要行為元素在紐澤西州發生。如同先前討論，不論 Auernheimer 或 Spitler 都沒有存取在紐澤西州的電腦。不僅如此，沒有證據顯示，有任何一位紐澤西州居民的電子郵件地址在 Gawker 新聞網的文章中被公然揭露。所以，對於違反紐澤西法律的控訴，當然不能授予罪名一管轄權。

正如同在紐澤西州沒有任何行為該當 CFAA 的違反，也就不會有政府在更新起訴中指控的明確行為在紐澤西州發生。起訴書列出四項明確行為：編寫 account slurper 程式、操作 account slurper 程式攻擊 AT&T 伺服器、寄送電子郵件給被害人通知系統漏洞、揭露取得的電子郵件地址給 Gawker 新聞網。本案共犯從加州跟阿肯色州通力合作使用 account slurper 程式，並將程式配送到位於德州跟喬治亞州的伺服器。政府並沒有提供任何關於 Auernheimer 寄送電子郵件的被害人是紐澤

西州居民的證據，或是他洩漏給 Gawker 新聞網記者的電子郵件地址清單是位於花園之州（按：紐澤西州別稱）。

不論 Auernheimer 或者他的共犯 Spitler 都沒有在紐澤西州執行任何根基於 CFAA 必要的行為元素的違反，或有任何明確的促進陰謀行為，因此我們認為地方法院對於罪名一的管轄權認定是不適當的（按：上訴法院亦認為基於相似理由，罪名二的管轄權也是不適當的）。

## 第三節 外國法院的命令

### 第一項 GOOGLE INC. V. EQUUSTEK SOLUTIONS INC（Canada）[29]

#### 壹、背景事實

在本上訴中的議題為，一間公司在其網站非法銷售侵害另一間公司智慧財產的產品，甚至已被法庭下令禁止仍繼續，則在審判中得否命令 Google 全球性的將該公司去索引化（de-index）。

Equustek Solutions Inc.是一間位於英屬哥倫比亞的小型科技公司，他專門生產網路設備，其產品功能是讓一間製造商生產的複合產業設備可以和另一間製造商生產的複合產業設備溝通。

本件 Equustek 及被告 Datalink（包含 Morgan Jack, Datalink Technology Gateways Inc., and Datalink Technologies Gateways LLC）之間的基礎行為，是由 Equustek 於 2011 年 4 月 12 日發動。Equustek 指控 Datalink，該公司的經銷商，將他們其中一項產品重新標籤，並且當作自家產品銷售。Datalink 也取得 Equustek 的機密資訊跟營業祕密，利用這些資訊設計、生產一項競爭商品—GW1000。

嗣後法院依 Equustek 的聲請發出命令，要求 Datalink 返還文件、

[29] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34 (C.A.).

不得在網站上提到 Equustek、聲明再也不是 Equustek 的經銷商。然而，Datalink 的態度是完全放棄司法程序，並未向法院提出任何說明，同時也不遵守法院的命令。於 2012 年 7 月 26 日，法官 Punnett 發出命令凍結 Datalink 的全球資產，包括他全部的產品存貨。法官 Punnett 發現，Datalink 在全球各地成立無數的空殼公司，持續的銷售這些侵權產品，削價吸引更多顧客，並且提供額外的服務—Equustek 宣稱這些服務揭露更多他的營業祕密。

於 2012 年 9 月 26 日，Equustek 聲請法院認定 Datalink 跟其負責人 Morgan Jack 藐視法庭。並沒有任何人代表 Datalink 出現，法官 Groves 因此發出 Morgan Jack 的逮捕令，不過，至今仍未逮捕他到案。儘管法院已經命令禁止銷售存貨、使用 Equustek 的智慧財產，Datalink 仍然在地球上某個角落持續進行他的事業，在網站上向全世界的消費者販售侵權產品。由於根本不知道 Datalink 及他的供應商在何處，所以也無法要求網站託管公司將 Datalink 的頁面移除。Equustek 變通想到一個方式，於 2012 年 9 月接洽 Google，希望 Google 可以在搜尋結果移除關於 Datalink 的索引。想當然爾，Google 拒絕了。Equustek 隨即將爭議帶到法庭上，希望透過法院的命令要求 Google 依照他的意思執行。

當 Google 取得訴訟上的相關資料後，反而要求 Equustek 應該先取得禁止 Datalink 在網路上執行業務的法庭命令，接著 Google 就會遵從法庭命令移除特定的頁面。依照 Google 的內部政策，他只會自願性的將個別頁面移除索引，而不是將整個網站移除。Equustek 同意嘗試這個方法。於 2012 年 12 月 3 日，Google 與 Equustek 出現在法庭上，同時法官 Tindale 發出 Datalink 停止在任何網站上營運或執行業務的禁令。於 2012 年 12 月到 2013 年 1 月間，Google 通知 Equustek 他已經將與 Datalink 有關的 345 個特定頁面移除索引。然而，Google 並沒有將整個

Datalink 網站移除索引。

很快地，Equustek 發現單單只有針對個別頁面移除索引，而非整個網站，是一個無效的手段。因為 Datalink 只要搬移這些內容物件到同一網站新設立的頁面，就可以成功地規避法庭的命令。此外，Google 也將移除索引侷限於出現在「google.ca」的搜尋結果。Google 的搜尋引擎在全世界透過指定的網站運作。意思是，網際網路的搜尋基本上是免費的，不過 Google 透過銷售顯示在搜尋結果的廣告欄位營利，例如有著加拿大 IP 位置的網路使用者嘗試執行搜尋時，其頁面會被導向 google.ca。然而，使用者還是可以藉由 Uniform Resource Locator（URL，即在瀏覽器網址欄直接輸入地址）存取指派給不同國家的 Google 頁面。這表示，舉例來說，在溫哥華的某個人，只要簡單地輸入 URL，就可以彷彿人在國外一般地存取別的國家的 Google 搜尋引擎。也因此，即使 Datalink 的網站在 google.ca 被阻擋，潛在的加拿大消費者還是有可能在境內瀏覽到 Datalink 的網站。考量到 Datalink 的 GW1000 主要銷售市場是加拿大以外的採購者，Google 的移除索引措施並沒有達成必要的保護效果。

承上，Equustek 開始尋求命令，希望可以責成 Google 在全世界的網站搜尋結果，都不要顯示 Datalink 網站的任何一個頁面。法官 Fenlon 核發這項命令，它的執行部分提到：在命令核發日起的十四天內起，到本訴訟結束或法院進一步的命令為止，Google Inc.必須在他的網路搜尋引擎上停止索引、參照 Datalink 的網站，包括表列網站的子頁面、子目錄。法官 Fenlon 特別提到 Google 掌控全球百分之七十到七十五的網路搜尋市場，以及 Datalink 之所以能銷售仿冒產品，主要取決於消費者能透過 Google 的搜尋引擎找到 Datalink 的網站。只有讓潛在的消費者遠離 Datalink 的網站才能讓 Equustek 受到保護。否則的話，Datalink 還是

能在網路上銷售產品並持續的傷害 Equustek，這些傷害即使訴訟結束了也難以回復。

法官 Fenlon 作出結論，這些無法回復的傷害是經由 Google 的搜尋引擎實現，Equustek 沒有替代方案，只能要求 Google 將 Datalink 網站去索引化。對於 Google 而言，沒有任何的不方便。為了讓命令有效，Datalink 的網站必須在所有的 Google 搜尋結果中被屏除，而不是僅在 google.ca 上而已。法官 Fenlon 認為，在她面前的紀錄顯示，即使只是在加拿大境內，要讓命令有效，Google 必須在他的所有搜尋引擎上屏除搜尋結果；更進一步，Datalink 的主要銷售市場是其他國家，所以法庭程序若要擔保有效，只能確保法院命令使得不同司法領域下的搜尋者，無法找到 Datalink 的網站。

英屬哥倫比亞上訴法院駁回 Google 的上訴。上訴法官 Groberman 接受法官 Fenlon 的結論，法院針對 Google 有屬人管轄權（in personam），因此可以核發具有領域外效力的命令；他也同意擁有固有管轄權的法院，即使對非當事人，也可以使負擔達成合理救濟。因為對 Google 核發禁制令（injunction）是唯一實際阻止 Datalink 藐視幾項法庭命令的方法，也沒有任何可能妨礙本件命令核發而適用的國際禮讓原則或對於表達自由的顧慮，因此上訴法官 Groberman 支持原審的命令。

## 貳、法律爭議

禁制令是公正的救濟措施。公正管轄權的法院，在所有相關的條文限制之下，有無限制的權力核發命令。學者 Robert Sharpe 提到，禁制令是一個彈性且劇烈的救濟手段，不受限於任何區域的實體法，且穩定的透過法院的藐視法庭權（contempt power）實施。

英屬哥倫比亞法庭經過調查程序作出結論，認為 Google 在該省內

有廣告及搜尋的商業活動，已經足夠建立起屬人及屬地的管轄權。Google 並未挑戰該結論，他反而挑戰命令的全球觸及性。Google 主張，如果有任何的禁制令被核發，效力應該僅限於加拿大境內（或 google.ca）。

當法院有屬人管轄權，且有必要確保禁制令的有效性，可以核發禁制令責成相對人在世界上的任何行為舉止。法官 Fenlon 解釋為什麼 Equustek 請求的命令有全球效力是必要的：GW1000 的主要銷售發生在加拿大境外。因此，除了數不盡的網站更迭實際問題以外，Google 提出的解決方案，無法跟強迫 Google 從旗下全球的搜尋引擎移除 Datalink 網站搜尋結果同等有效。我因此認為 Equustek 沒有其他可茲利用的法庭外救濟。為了命令的效力，即使在加拿大境內，Google 也必須在旗下所有引擎阻擋搜尋結果。Datalink 違背了不讓 Equustek 受到無可回復的傷害的相關命令，為了確保 Google 的搜尋不會進一步擴大裂痕，法官 Fenlon 作出本件禁制令必須有全球效力的結論。

我同意。本件的問題是發生在線上及全球性的。網際網路沒有國界，它的自然屬性就是全球性。確保禁制令達成它的客觀目標，唯一的方式就是將其適用在任何 Google 營運的地方，也就是全球的。正如同法官 Fenlon 的發現，Datalink 主要銷售市場在加拿大境外。如果禁制令效力僅及於加拿大或 google.ca，如同 Google 主張他應該做的，救濟手段將會失去它本來應具有避免無可恢復損害的功能。在加拿大外的買家可以輕易地繼續從 Datalink 網站採購，而且加拿大籍買家也可以輕易地找到 Datalink 網站—即使已經從 google.ca 被去除索引。Google 可能持續地促進 Datalink 違背法院要求不得在網路上經營業務的命令。核發禁制令但現實上無法避免傷害，是不公平正義的。

防止 Datalink 在網路上執行業務造成無法回復的損害，又 Datalink

的業務若沒有 Google 協助推廣則絲毫不具商業可行性，本件的禁制令是必要的。命令的目標是 Datalink 的網站—由於 Datalink 嘗試阻撓禁制令故網站清單經常被更新—及在它們可能造成最大傷害的地方阻止呈現：Google 全球搜尋的結果。禁制令的全球效力也沒有帶給 Google 任何不便，命令並沒有要求 Google 在全球採取行動，只是要求他對自己掌控的搜尋引擎採取一些步驟。Google 已經承認他們做得到，也相對容易做到。因此，可以說命令的全球觸及性並沒有對 Google 造成任何應歸類於不便利的傷害。

接著，Google 爭論全球性的禁制令將違背國際禮讓（international comity）原則，因為理論上，在外國司法管轄權下，同樣的命令很有可能不會被取得;或者遵循該命令將導致 Google 違反當地受敬重的法律。正如同法官 Fenlon 的闡釋，Google 承認大多數的國家都會認可智慧財產權及將銷售盜版商品視為違反行為。當然，表達自由的顧慮也值得我們投以尊敬的眼光，尤其是處理另一個國家的核心價值時。在本件我並沒有看到任何會帶給 Google 重大不便的表達自由議題涉入。正如同上訴法官 Groberman 的論述：本件中沒有一個實際的主張是關於法官的命令將觸動其他國家的敏感神經。禁制令不准許侵害原告智慧財產權的被告侵權商品廣告，並沒有顯示任何會冒犯其他國家核心價值的議題。對於 Google 發出的命令是非常有限度、附屬的命令，用以確保原告的核心權利受到尊重。本件的命令是一項禁制令，而且內容可能會隨著個案有所不同。假使有任何司法權認為該命令侵害他們的核心價值，可以向法院聲請修正命令內容避免同樣的困境再次發生。

如果 Google 能提出證據，表示遵守禁制令無可避免地使他違反另一個司法權下的法律，包括干涉表達自由，英屬哥倫比亞法院總是敞開大門歡迎提出聲請作出相對應的修正。不過到目前為止，Google 還沒

有提出這樣的聲請。在欠缺證據基礎之下，以及考慮 Google 尋求修改命令的權利，就算要做到要求 Equustek 擔負依照個別國家展示命令是合法可行的責任，若斷然否決 Equustek 所需而讓救濟有效的領域外範圍，將是嚴重不公正的決定。畢竟我們是在處理網際網路案件，便利平衡測試（balance of convenience test）應當充分考慮無可避免的領域外觸及性，尤其是禁制令救濟是向 Google 這樣的主體尋求時。

這並不是像表面上那樣的移除言論而涉及表達自由價值，而是一道去索引化違背幾項法院要求網站的命令。到目前為止，我們還不認為表達自由的保障，需要透過銷售非法商品的方式增長。雖然 Google 期許自己擔任內容中性的角色，不過我還沒看見命令會對 Google 有什麼樣的干涉。禁制令沒有要求 Google 監管網路上的內容，也沒有對 Google 課以任何責任強化對侵權網站的存取。經過便利平衡測試，在禁制令中創造出對 Google 唯一的義務是將 Datalink 的網站去索引化。如同法官 Fenlon 的觀察，這道命令不過是移除個別 URL 的些許擴展，Google 也曾自願地同意執行。

關於去索引化 Datalink 的網站，Google 並沒有表達會有任何重大的不便利，或者將產生任何鉅額的花費。公平的說，他反而承認他可以，也經常做，正如同在本件中被要求的，也就是說，修改搜尋的結果。Google 經常避免搜尋結果含有兒童色情的連結、帶有仇恨性言論的網站。Google 也遵守美國的 Digital Millennium Copyright Act（Pub. L. No. 105-304, 112 Stat. 2860 (1998)），將據稱侵害著作權的搜尋結果去索引化，以及依照法院命令移除網站。

Datalink 跟他的代表人無視先前針對他們的全部法庭命令，離開英屬哥倫比亞，並繼續在加拿大外的不詳地點經營業務。Equustek 努力嘗試找出 Datalink 位置但只獲得有限的成果。Datalink 只能透過 Google

的搜尋引擎引導潛在消費者到他的網站而在市場上存活，然而代價是 Equustek 的生存。換句話說，Google 是 Datalink 就算蔑視幾項法庭命令卻仍持續傷害 Equustek 的關鍵。這非意味著 Google 必須為這些傷害負責，然而，Google 是讓這些傷害發生的決定性角色。

總體而言，在根本的訴訟結果出爐之前，禁制令是唯一有效的方式緩和 Equustek 所受的傷害，以及唯一的保護途徑。因為對於 Google 的傷害是最小的甚至不存在，本件禁制令應該被維持。

## 第二項 GOOGLE LLC V. EQUUSTEK SOLUTIONS INC（US）[30]

### 壹、背景事實

原告 Google 對 Equustek 提起本件爭訟，阻止一道加拿大法院的命令強制執行，該命令要求 Google 全球性地去除搜尋結果。現在 Google 請求一項初級禁制令，而 Equustek 沒有向法院提出摘要，所以 Google 的聲請程序應被法院受理。Google 於 2017 年 7 月 24 日向法院繫屬，尋求一個加拿大法院的命令不能在美國強制執行的宣示性判決，因此 Google 現在聲請初級禁制令的救濟。

### 貳、法律爭議

尋求初級禁制令的當事人必須舉證：（1）其主張非顯無理由；（2）若無初級禁制令可能遭受無法回復的損害；（3）公正衡平後受有利益；（4）禁制令與公共利益有關...。Google 爭論加拿大的命令在美國無法強制執行，因為它直接地與憲法第一修正案衝突，無視 Communication Decency Act 賦予互動服務業者的豁免權，以及違反了國際禮讓原則。

[30] Google Inc. v. Equustek Solutions Inc., No. 5:17-cv-04207-EJD, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

## 一、主張有理由的可能性

Communications Decency Act 的 Section 230 豁免互動電腦服務供應者由第三、方創作內容引起的責任。條文表明，互動電腦服務的供應者或使用者，不應被視為另一位資訊內容提供者所作資訊的發行人或談論者（47 U.S.C. § 230(c)(1)）。國會於 1996 年頒布 Section 230，指出在嶄新且萌芽的網際網路媒介上產生的侵權訴訟為言論自由帶來威脅。Section 230 並不是允許網路使用者不用為其發布非法資訊負責，而是，它反映出國會的政策選擇，在嚇阻傷害性的線上言論方面，若提供線上媒介服務公司的使用者有潛藏的傷害訊息，不另立途徑對公司實施侵權責任。

為了符合 Section 230 的免責條件，Google 必須證明（1）他是互動電腦服務的供應者或使用者；（2）有疑慮的訊息是由另一位資訊內容提供者所創作；（3）加拿大的法庭命令將對他施以資訊發行人或談論者的責任。在此，Google 滿足以上所有條件。首先，毫無疑問，Google 是互動電腦服務的提供者（47 U.S.C. § 230(f)(2)：互動電腦服務係指任何資訊服務、系統或軟體供應者，提供或允許多數使用者存取特定電腦伺服器）。其次，是 Datalink 而非 Google 提供本件爭議的訊息。Google 僅是爬梳第三方網站並將它們加入索引。當使用者查詢 Google 搜尋引擎，Google 呈現相關網站的連結以及簡要的內容縮圖。Google 搜尋引擎幫助使用者找到跟存取第三方的網站，但不是 Section 230 定義下的內容提供者。再者，加拿大的法庭命令將對 Google 施以 Datalink 網站資訊發行人或談論者的責任。加拿大的最高法院命令 Google 從他的全球搜尋結果將 Datalink 網站去索引化，理由是，從法院的觀點，Google 是對 Equustek 傷害持續發生的決定性角色。然而，美國的司法實務認為，不管引起訴訟的根本原因為何，當主張要求網路媒介移除第三方內容

時，就已經將網路媒介視為內容的發行人。該判決進一步說明，移除內容是發行人應該做的事，而以移除內容為基礎施以責任，必然涉及將未能移除內容的當事人視為發行人而負責。加拿大的法庭命令已將 Google 視為發行人，因為 Google 未能從他的搜尋結果移除第三方內容，卻仍要對 Google 施加責任。

Google 符合 Section 230 的所有豁免條件。因此，法院認為 Google 有可能在 Section 230 的爭論上獲得支持。

### 二、無可回復損害、公正衡平及公共利益

Google 因為加拿大法庭命令限制了 Section 230 所保護的權利。此外，公正衡平測試支持 Google，因為這道禁制令將剝奪他在美國聯邦法律下的利益。禁制令也會與公共利益有關。國會認定，如果網站因為留有使用者產出的內容而面臨侵權責任，則網路上的言論自由將會嚴重的被侵害。所以，國會頒布 Section 230 作為回應，授予線上媒介廣泛的豁免權限。（47 U.S.C. § 230(a)(3), (b)(2), (b)(3)：網際網路及其他互動電腦服務提供多元政治言論的平台、文化發展的獨特機會、智慧活動的無數管道…這是美國的政策...提倡網際網路跟其他互動電腦服務、互動媒體的持續發展，以保護現在網路網路及其他互動電腦服務自由市場的活力及競爭性，不受聯邦或州的法令所拘束）。加拿大法庭命令減損 Section 230 連結到第三方網站服務提供者的豁免權。強制網路媒介移除第三方資訊的連結，加拿大法庭命令破壞了 Section 230 的政策目標，以及威脅了全球網路的言論自由。

## 第三項 EQUUSTEK SOLUTIONS INC V. JACK

## （Canada）[31]

禁制令的決定在加拿大上訴法院、最高法院兩者都獲得支持。然而，隨後 Google 從加州法院取得命令，使得禁制令無法在美國執行。Google 現在改而聲請廢棄或變更原禁制令…。

我發現先前三個審級程序中出現的有關超領域性及司法禮讓議題，本院無法開放性地重新闡釋。在這些議題之中，加拿大最高法院已經事先定義，情事變更可以作為重新檢視的依據：如果遵守禁制令無可避免地使他違反另一個司法權下的法律，包括干涉表達自由，Google 可以在證據基礎之上聲請變更。Google 表示這應該被寬鬆的解釋，他們認為禁制令干涉言論自由，已經違反了美國的核心價值。

美國法院的決定並沒有確立禁制令要求 Google 違背美國法律。舉例來說，可能是被告 Datalink 自美國法院取得命令，要求 Google 搜尋結果連結到他們的網站的情形。但是，沒有跡象顯示，不論是遵循禁制令或任何其他理由，有任何美國法律禁止 Google 將這些網站去索引化。再說，就算沒有禁制令，Google 本來就有權力選擇要不要列出這些網站，只是禁制令限制了選擇，禁制令也頻繁地限制表面上看起來合法的行為。一位當事人在能力上被限制行使某些權利，跟當事人直接被要求違反法律，是兩件不同的事。我對法官 Abella（按：第一案承審法官）論述的解讀，認為應該是主要限制於後者的情形。

不過，即使上述解讀是錯誤的，Google 仍然沒有證明禁制令違反了美國的核心價值。我預設憲法第一修正案所保障的權利是核心價值，但是法官 Davila（按：第二案承審法官）顯然地，拒絕作出決定，確認禁制令是否違反 Google 爭論的憲法第一修正案權利。Google 爭論憲法

[31] Equustek Solutions Inc. v. Jack, 2018 BCSC 610.

第一修正案與本件有關，因為憲法第一修正案驅動了本件法律、判決兩者背後的根本政策。在我的觀點，法官 Davila 的決定不應被解讀超越他實際闡述的範圍，特別是 Google 的主張沒有被反對，以及法院不會從反對的論述中取得效益。美國法庭決定的效果，是不會有任何要求 Google 執行禁制令的行動。然而，這並不會限制本院，透過直接對有屬人管轄權的當事人，下達保護國內法律程序的整體性的命令。

儘管 Google 主要依靠加州法院的決定作為情事變更的依據，Google 也表示情況也因為一些其他措施而改變了…。Google 實施的措施進一步地讓情況不同，Google 已經修改地理位置系統，可以讓限制起源於加拿大的網路搜尋的禁制令更加有效。先前，加拿大 IP 位置的網路使用者被導向加拿大版本的搜尋引擎「Google.ca」，不過，藉由點選「go to google.com」的選項，他們可以使用提供給美國使用者的服務；使用者也可以輸入適當的 URL，藉此存取設計給其他國家的服務，例如「www.google.co.uk」即可使用英國服務。Google 現在已經把系統修改成，搜尋結果的配送取決於使用者預設位置，換言之，不論使用者如何輸入 Google 的 URL 結果都會一樣。這正表示對於所有被識別位於加拿大的使用者，除非採取特別的步驟修改電腦設定，將網站去條列化（delisting）仍然是一種有效的手段。

Google 也爭論禁制令並沒有辦法阻止被告 Datalink 在網路上繼續販售他們的產品，顯然的，他們的網站仍然存在，也可以透過 Google 以外的方式存取。我同意原告的觀點，即使禁制令無法成功地使被告 Datalink 停止營業，但不代表它是無效的、無法讓潛在的消費者更難找到他們。禁制令的有效性，已經透過被告 Datalink 不斷地設立新網頁規避封鎖證明…。本件廢棄或變更原禁制令的聲請駁回。

## 第六章 心得及建議

總結本篇報告，首先確立網路犯罪係指犯罪行為部分或全部涉及使用網際網路之犯罪，並指出網路具有持續性、可見性、擴展性、可搜尋性的特質，這些性質是探討網路犯罪時，應予一併考慮的因素。其次，以無故使用電腦、性犯罪者與社群媒體、兒童色情的網路過濾為主題，摘要美國網路犯罪相關文獻及判決，分別討論資料庫存取的權限（資料一經備份擴散，即符合上述的四項網路特質）、社群媒體的近用、網路內容的屏蔽，可知在討論網路犯罪時，理解涉及的電腦技術並予以闡釋，是不可避免且有必要性的；並在網路內容的屏蔽部分，以美國判決記載的技術分析，實際推敲我國楓林網案件偵破後，就其網站侵權內容的屏蔽方式。另外，雲端證據是在科技發展下，司法體系不得不面對的議題，因此彙整我國 hiBox 案的實務見解，即「過去已結束」的雲端證據需以扣押（附隨於搜索／非附隨於搜索）取得，再對比美國法院的觀點，分別從使用者的隱私權、政府命網路服務業者保存證據後調用、扣案電子設備內容取得三個案例的角度，拓展數位證據的法律議題。從結論上可得知，美國法院採取高標準保護隱私權，對於政府是否能無限上綱從任何裝置取得數位證據的行為，明顯採取保留態度，要求法院令狀的介入。由於網路使國家的邊界模糊化，「數位國界」的概念因應而生，2000 年代的美國網路巨擘 Yahoo!與法國法院的法律衝突，從技術探討中衍生出司法權如何跨境實現的議題，也開啟此類法律討論蓬勃發展的大門。如本文開頭所述，美國特殊的各州及聯邦法律系統分立、併行，縱使網路犯罪事實都是在美國境內發生，也會產生不同州之間的跨境審判權爭議，特別是網路犯罪中，也應對涉及的電腦伺服器所在地進行分析。最後，加拿大 Equustek Solutions Inc.要求 Google 除去網路上侵害智慧財產權產品的搜尋結果（在我國也可能發生相似的侵害智慧財

產權犯罪），這一系列兩國的判決對技術可行性、法院命令效力範圍的論述，更是國際合作的精彩教材。

在美研習上開網路犯罪的法律議題，筆者最大的收穫、也是欽佩的地方，是美國法院判決的專業度。在此所述的專業度並非指法律專業本身，而是指涉及技術議題時，法院透過法庭之友（amicus curiae）[32]的協助，不論是說明報告或者鑑定意見，取得正確的先決知識，並且將這些調查過的先決知識記載於判決中，作為判決論述的基礎材料。例如，第三章第三節的兒童色情的網路過濾議題，即詳細分析在網路世界中，技術上可能有什麼方式得以阻斷不當的網路內容，並進一步的闡述政府頒佈的法律是否有實施的可能性、對於言論自由造成過度負擔。

技術的發展日新月異，或許不是法律得以掌控的。但是，筆者認為法律需要對於技術有正確的理解，才能在法政策或是具體個案上做出正確的判斷。反應在司法實務上，由於我國欠缺法庭之友制度，每當個案涉及技術或科學議題時，若無法理解或難以理解背景技術，審理過程中若有疑難雜症，當然也不知向誰詢問或如何詢問。以筆者的工作經驗為例，常見與網路犯罪有關的技術，除了新近的區塊鏈、比特幣、挖礦機外，較為傳統的是電話詐騙。電話詐騙分工細膩，為了避免查緝，話務機房採用的技術不斷地演進，從較早期使用 Router、Gateway、Vos3000 的實體話機，到最近改採無線網路的 VoIP APP、數位式移動節費電信（Digital Mobile Trunk）等，不斷地挑戰檢警調對於技術的認知及追緝。相關法律文件上，通常僅簡略記載扣得這些物品，惟實際上怎麼設定、怎麼運作、怎麼分工卻大多不得而知。

[32] 法庭之友不是訴訟當事人的任何一方。可能是出於自願之下，或是回應訴訟雙方的當事人請求，法庭之友提出相關資訊與法律解釋的法律文書給法院，以協助訴訟進行，或讓法官更了解爭議的所在。提出這種法律文書的人，就被稱為法庭之友。

為了確認扣案物在網路犯罪中的角色，如果沒有明確方向就貿然發函詢問，此時即會陷入 garbage in, garbage out 的困境，不對的問題答的再好，還是壞答案。承此，判決適用的技術基礎錯誤，自然無法給予個案正確的法律評價。美國的司法系統在理解技術上障礙較小，因為法學院均為碩士學位，學生在大學時就讀不同領域科系，也多有工作經驗，各有所長。例如喬治城法學院 2019 年度的學生統計，美國本土公民為主的 JD 學生，平均年齡為 32 歲，即彰顯了法學院學生的多元性。又在課程設計上，如同筆者原先嘗試旁聽的 Computer Programming for Lawyers，直接在法學院導入技術課程，教導法學院學生如何撰寫電腦程式，這對於將來律師執業自己客製化程式進行判決或見解分析，或者在技術訴訟理解爭議內容都大有助益。再次強調，把問題問對，比把錯的問題答的好，更為重要。

由於我國沒有法庭之友的制度，對於其他領域專業內容的理解，例如科技、醫學、化學、工程、農業等，除了鑑定人以外，有賴於個別檢察官的專業技能及在職學習。在此建議，將來舉辦的教育訓練，不僅應拓展訓練的領域，將學習推廣至法律以外的技術類別，更重要的是，也應鼓勵同仁暫離工作崗位、多加參與、積極學習，以培養因應數位網路時代處理新興案件的應變能力。

# 第七章 卷後語

在美國進修七個月的期間，除了對於網路犯罪議題的學習外，筆者其他收穫頗豐。其一是上課風格，美國學生踴躍發言及提問令人印象深刻，在研討會形式中，甚至教授只是負責擔任引導的角色，學生總和的發言時間往往比較教授本身更長，意見有來有往，和我國以教授講課、學生聆聽為主的上課型式大不相同，讓筆者更能體會美國憲法第一修正案精神的落實；其二是判決的精彩度，如同報告本文所呈現的各篇判決，法官從不吝於表達自己意見，以貼近生活的生動比喻論述冷僻生硬的法律議題，為判決帶來親和力與生命力，使一般民眾容易理解判決背後的思維。以上的衝擊所帶給筆者的反饋，是認為檢察書類撰寫時應更具彈性，除法定用語以外不應拘泥於統一格式，論述上應盡量貼近一般民眾生活用語，除了對一般人而言易於閱讀以外，也期望透過對於司法文書的理解，提升民眾對於司法權的信任及尊重。另外就筆者在參與課堂、演講的觀察，美式教學著重於講者與聽眾的互動，甚至講者之間在別人發言時，也會互相插話發問，與我國舉辦的教育訓練，多半單方面聽講的模式大不相同，令人印象深刻。或許，往後教育訓練可以試行美國講座式教學，一位主持人、數位講者，採行類似談話性的授課，提高聽眾的參與度俾利於訓練的成效。

在此，筆者也想談論美國公民對於司法權的尊重。我國司法院於 2019 年公布「司法輿情現況調查」顯示，近四成受訪民眾相信法官會公平公正審理、判決案件，然而不信任的民眾卻達到五成六。[33]相較於美國的調查，美國民眾有六成八的比例相信美國最高法院以美國人民利益為最高優先，高達七成的人更是認為美國最高法院值得擁有適當

[33] https://news.ltn.com.tw/news/society/paper/1301734，最後瀏覽：2020/5/28。

的權力。[34]前述只是統計數據。喬治城大學法學中心位於華府市中心，其附近聯邦層級法院有美國最高法院、哥倫比亞特區地方法院、哥倫比亞特區上訴巡迴法院，哥倫比亞特區自身也設有 Superior Court（即地方法院）、Court of Appeal（即上訴法院）。

筆者曾抽空一週前往特區地方法院旁聽陪審案件，該案是盜刷換現金的詐欺案件，筆者從陪審員的選任一直到辯論終結為止均在場。陪審員必須全程參與審判，聆聽檢辯雙方攻防、證人的回答、證據的調查等，耗時甚久。而且，審判期程其實是不確定的，會持續多久仰賴審判程序的流暢程度，諸如訊問證人時間長短、證人或陪審員有無遲到，法官無法承諾審判究竟何時可以終結，這也表示陪審員告向家庭或公司告假多久，也是懸而未決。但就筆者親身觀察，從選任陪審員開始，沒有任何一位陪審員主張家庭或工作而無法參與審判（當然法官也不會准許），且審理過程中陪審員亦未顯示絲毫不耐，均專心聆聽證詞或撰寫筆記以便辯論終結後，與其他陪審員評議被告有罪無罪。

審判過程中有一段插曲。一位陪審員（A）在休庭時向法院告知，在其被選任為陪審員前中午用餐時，另一位民眾（B）曾與其攀談，聊天過程中該民眾的鄰居（C）前來打招呼，這位鄰居（C）是一位律師，與該民眾（B）談到該案法官的評價。事後陪審員（A）發現，中午跟他聊天的民眾（B）也是陪審員候選人，違背了法官命令陪審員候選人在休息時不得接觸的指示。法官裁示這段插曲不影響陪審員的資格。這段插曲使筆者對於美國公民尊重司法程序的謹慎程度印象深刻。筆者在美期間，因為友人有學齡孩童，略知美國中小學教育一二。美國公民從小受教育即認知到，擔任陪審員是國民義務，只要受通知均需全程配

[34] https://www.prnewswire.com/news-releases/most-americans-trust-the-supreme-court-but-think-it-is-too-mixed-up-in-politics-300939726.html，最後瀏覽：2020/5/28。

合，尊重司法權的行使。

此外，筆者也曾二度前往最高法院旁聽。第一次是在開庭前一個小時抵達最高法院外的排隊處，出發前已確認過當天案件並非矚目案件，沒想到還是排滿了一條長長的人龍，有些排隊的民眾看似遊客，把到最高法院旁聽當成是旅遊的一部分。由於筆者之前曾進入過大法庭，知道大法庭的容量無法容納在場的排隊人龍，當天所幸做罷擇日再來。為免鎩羽而歸，第二次清晨五點即出發前往排隊，因為當日其中一件言詞辯論案件是 June Medical Serv. v. Russo, Interim Sec., LA Dept. of Health，該案涉及女性墮胎權，引起美國社會高度矚目，可以想見將吸引大批旁聽民眾。走到了現場，天色未亮，早已有人漏夜搭帳棚等待領取號碼牌，且正反雙方的抗議團體也在最高法院外蓄勢待發。在等待入場過程中，筆者親眼目睹了一場暢所欲言、多元表達的美國式抗議，熱鬧中帶有嚴肅，歡樂中帶有議題，雙方都希望大法官能聽進他們的聲音。民眾對於司法程序參與的熱忱，都是筆者在臺灣前所未見也無法想像的。

以上的學習，因為 2019 年底起迅速蔓延的武漢肺炎疫情，戛然而止。一開始美國宣布停止中美航班，美國確診案例只發生在西岸，案例數也寥寥可數。沒想到疫情急轉直下，從 2 月底案例數暴增並在全美擴散開來，華府跟北邊的馬里蘭州、南邊維吉尼亞州開始有大量確診，甚至筆者附近的公寓也傳出確診案例。瞬間，筆者的學校信箱收到了校園關閉的公告－教室、運動中心、商店、圖書館、模擬法庭－無一倖免，課程一律改為線上教學，每週固定時間打開電腦對著螢幕聽講。

非本地學生逐漸離開校園回到自己家鄉，本來該是學期當中充滿活力的時刻，卻因為疫情的影響校園無人顯得孤寂，只有春天來臨乍開的花朵及嫩枝作伴。此時馬上面臨一個抉擇，在美國待著除了有染疫的風險外，學校無限期的關閉，何時再啟遙遙無期，研究計畫、交流活動

似乎也無法再進行下去了，不禁起了是否該提早結束訪問返回臺灣的念頭。從訂購機票到搭機返台，前後不過十天光景，擬定返台計畫，迅速的完成通知房東、聯絡學校、清空家具、行李托運，一切來的突然、也結束的突然。直到現在，還清楚記得出發搭機當天，陰雨蕭瑟，路上行人車輛不多，一路不停地開到紐約，彷如電影情節般的逃難歷程，終點是冷清又淒涼的甘迺迪機場。

回到臺灣配合中央流行疫情指揮中心指示，居家檢疫十四天。在臺灣不禁思索當機立斷的決定，到底損失了些什麼。未走完的租約、剩餘的課程、法院的旁聽、學校圖書館資源、進一步的資料蒐集、大大小小的演講跟研討會、認識教授跟其他國家友人的機會。至於得到的，是一片寧靜。在臺灣生活除了口罩、量體溫以外，生活如昔，充足的口罩供給、良好的衛生習慣，出門不用提心吊膽地主動跟別人保持距離，也不用煩惱自己廉價的醫療保險跟不熟悉的醫療體系。臺灣的這一片寧靜，加上在美國七個月的收穫，已經足夠涵蓋所餘未走完的訪問行程了吧。