# 新興科技與犯罪：
# 以美國法制之通訊隱私程序保障為論述中心

國立臺灣大學國家發展研究所法律組副教授 劉靜怡

目　次



## 摘　要

在新興網路科技的發展下，尤其是在因為雲端運算科技逐漸成為主流而促成的遠端存取架構下，人民隱私權益的保障，遭遇前所未有的挑戰，過去至今法院據以保障人民隱私權的既有法律原則，也出現了有待填補的論理漏洞，這都是我們必須面對的重要規範課題。本文從比較法的取向出發，以美國憲法及相關法制的問題，做為介紹重心，希望藉此指出網路通訊和雲端服務發展趨勢下的隱私隱憂，並說明在此一環境下，根據傳統通訊監察法令從事犯罪偵查時對於隱私保護的不足與侷限，本文認為關於規制政府通訊監察行為的界線何在此一討論的重心，應從是否構成搜索扣押的實質判準，移轉到更加關注當事人是否具有「合理隱私期待」及偵查機關的「正當化標準」兩者所隱含的程序性保障意涵，才是平衡公共安全和資訊隱私的可行處理模式。

## 壹、前言：新興科技、公共安全與資訊隱私

在這個科技不斷進步的時代裡，犯罪者利用科技提高作案成功率，以及降低遭到執法機關偵測或緝捕的風險，相對地，執法機關也嘗試善用科技從事犯罪偵查。目前的資通科技可以排除任何地域障礙，有利於從事遠端犯罪。以長期以來讓不少網路使用者備受恐懼和擔心己身安危的網路跟蹤（cyberstalking）行為為例，由於網路溝通方式的多元化，使得跟蹤者可以透過線上聊天室、個人網頁甚或社群網站平台尋找受害者並蒐集相關資訊，甚至持續發送電子郵件或惡意程式給受害者，導致受害者不堪其擾、身分遭竊，甚至在真實世界裡遭受人身攻擊。

在關於執法程序的辯論裡，往往將「安全」及「隱私」兩者視為截然二分、零和對立，此一現象的出現，一方面是出於對科技發展的普遍誤解和恐慌，另一方面則可能是因為將「秘密」（secrecy）及「自主性」（autonomy）兩者混為一談的隱私迷思所致。從某個角度來看，安全與隱私兩者的關係，並不是孰輕孰重的關係，兩者可以說是同時構成自由民主社會的雙重義務。因此，在一個由科技扮演主導角色的資訊社會裡，在科技發展策略上，我們必須採取價值敏感（value-sensitive )的策略，將可以確保個人基本權利和符合正當程序要求的科技嵌入執法程序中。雖然，科技設計所仰賴的電腦程式碼（code）並非法律，但是電腦程式碼卻可以決定法律、規範及市場等數個機制所能發揮的功能[1]。換言之，科技本身既非問題所在，也非解套之道，科技所展現的，是公共政策的決策過程中必須面對的限制和契機，科技所帶來的，是如何將科技特色和隱私考量互相結合，以建構正當執法程序的議題。換言之，犯罪偵查甚或恐怖活動的防範，不可否認地都具有某種公共利益的正當性，因此，必須建置先進的科技執法措施以便因應威脅，也是可以理解之事。然而，我們同時必須承認的是，科技對於確保個人自由及自主性的隱私價值的確深具風險，而且，在此同時，科技也無法達到絕對的安全或隱私保護目的。在此一理解下，或許才能找到真正衡平公共安全和資訊隱私兩者的執法模式。

關於執法程序中的隱私爭議，之所以成為一個充滿社會焦慮的爭議，或許和一般人對於隱私風險有不容易清楚掌握有關。究其實際，為了保護個人基本自由權利而要求政府必須對人民提供正當程序保障，其主旨應該是嘗試在「禁止不合理搜索」以及「容許合理搜索」兩者之間，取得執法平衡點。尤其是在九一一事件發生後，為了因應國際恐怖主義的威脅，執法程序的複雜性日益提高，其主要原因在於反恐戰爭事實上通常並無明確目標，而且威脅通常是在隱藏在廣大群眾之中，利用開放社會的藏匿優勢形成恐怖組織和從事恐怕活動。從保護人民基本權利的角度來看，反恐時代的執法任務，其重點不是防禦外在敵人，而是如何在避免侵害多數無辜人民的基本自由此一前提下，針對潛在的恐怖份子予以識別並偵查其不法行為。然而，不可否認的是，反恐時代裡的執法行動，往往流於妖魔化少數份子，或者有意無意地將每個人都當作嫌疑犯看待，不然便是訴諸絕對機密，而在無形中犧牲對人民的權利保護需求。

究其實際，當前的先進資訊科技，在執法機關的運用下，至少會為人民帶來以下的隱私疑慮。首先是執法行為所帶來的「寒蟬效應」（chilling effect）。此處所說的寒蟬效應，是指在先進資訊科技所發揮的監察功能下，會使原本應該受憲法保障的正當活動，在理解到政府可能監視甚或分析該活動的意識下，導致個人行為因此改變，以致於集會結社、言論表達和政治參與等憲法權利均受負面影響，而保護隱私的程序保障，其終極目的正是為了保障上述公民基本權利。其次值得注意的是「滑坡效應」（slippery slope），亦即原先是在非常時期基於維護國

[1] See generally LAWRENCE LESSIG, CODE AND OTHER LAWS IN CYBERSPACE (1999).

家安全的正當考量而採取的執法措施，可能日後會成為常態，變成使用於執法機關日常的調查行為一環，導致特殊執法程序演變成一般性執法程序，將社會推向遭受持續性監視的境地[2]，而基於國家安全此一特殊目的而來的執法程序，對於隱私權益本即較為輕忽，加上執法機關運用先進科技的情形愈益普遍，以及許多網路服務逐漸朝「雲端運算」（cloud computing）的方向發展，使得政府能取得的個人資料更為廣泛，因此，如何透過程序要求來達到保障隱私的目的，更是我們應該關切之處。

本文以下將分析的是，在新興網路科技的發展下，尤其是在因為雲端運算科技逐漸成為主流而促成的遠端存取架構下，人民隱私權的保障，究竟遭遇到怎樣的挑戰，過去至今法院據以保障人民隱私權的既有法律原則，是否出現了有待填補的論理漏洞，恐怕是我們不得不面對的重要議題。由於我國目前相關討論較少，本文以下將從比較法的取向出發，以美國憲法及相關法制的問題，做為介紹與分析的重心，希望藉此發揮他山之石的功錯效果，併此敘明。

## 貳、雲端運算服務衍生的隱私爭議

「雲端運算」的特色，是指將過去主要由使用者本身可以控制的運算功能，例如資料儲存、硬體維護、安裝運用軟體等等，透過網路的輔助，轉交給雲端服務業者從事維護運作。個人使用的常見雲端運算服務，包括直接在網路上儲存或修改相片、建立地址簿、紀錄行事曆、備份資料等等。而為企業服務的雲端運算功能，則包括處理顧客關係、儲存資料或是以遠端電腦操作應用程式等等。本文以下將說明雲端運算服務所帶來的隱私威脅和爭議，以做為後續分析的基礎。

### 一、雲端運算服務帶來的個人隱私威脅

從表面上看來，雲端運算似乎可只是個人電腦功能的延伸，但是，無論是從技術角度或者是從法律角度來看，實際上雲端運算卻可以將使用者的個人資訊所在位置，從原先的個人電腦轉到第三方伺服器上。這個過程，不但影響消費者自主控制個人資訊的能力，也更有可能將更多關於個人私密生活的資料曝光，威脅個人隱私的維護。

若是深入探究雲端運算對於個人隱私所帶來的威脅，我們不難歸納出來的是：雲端運算除了紀錄使用者個人資訊外，更會產生其他資訊，而成為服務提供者蒐集的對象，諸如消費者登入、儲存網路內容時所使用的身份、時間和所在地點。例如消費者使用 Google 文件（Google Docs）時，Google 所紀錄的資訊包括該帳號的活動、顯示或點選的資料，瀏覽器類型、IP 位址等等資訊[3]。這些資訊的揭露，都可能威脅使用者的隱私，例如 IP 位址和登錄時間，便有可能揭露使

[2] See generally Eugene Volokh, The Mechanism of the Slippery Slope, 116 HARV. L. REV. 1026 (2003).
[3] Google Docs Privacy Policy, http://google.com/google-d-s/privacy.html (visited Oct. 12, 2010).

用者的真實身份。更有甚者，有些提供雲端運算服務的公司，還會將部份服務再分包給第三方，而承包業務的第三方，或多或少可也以接觸到使用者的個人資料，例如 Amazon 的網頁寄存服務( hosting services )，讓其他公司可以使用 Amazon 所提供的伺服器去運行其應用程式或儲存商店資料，然而，在此同時，Amazon 也表示：在某些情況下，Amazon 有權揭露這些資訊。Amazon 網路服務契約條款即表明 Amazon 在管制機關相關法令規定、接獲執法機關傳票或法院命令的情況下，可以揭露上述資訊[4]，諸如此類的文字，顯示雲端運算時代裡的使用者面臨不算不嚴重的資訊隱私威脅。

## 二、雲端運算服務中的隱私保護低度規範

在隱私程序保障上佔據重要的地位的「合理隱私期待」( reasonable expectation of privacy ) 原則，本是源自於針對有形物理空間裡的隱私保護所發展出來的判斷基準，此一判斷基準是否足以使美國憲法增修條文第四條的規範射程，能夠涵蓋到口頭對話或數位世界等無形體之上，其結果當然影響網路空間或者雲端活動所衍生的隱私保護問題能否做為此一判斷基準的適用對象。

雖然目前不乏隱私保護相關法規，然而，絕大多數的法規卻是在網路通訊科技出現前的立法，不見得充分考量到網路通訊甚至雲端運算的特性，也就不免使得雲端運算資料的隱私保護處於不確定的狀態，尤其是在如何認定是否構成搜索及是否需要取得法院搜索票時，可能形成棘手的爭議。詳言之，隱私權雖然是受到憲法保障的基本權利，絕大多數的法院禁止執法機關不合理的搜索和扣押行為，以美國的法院判決為例，其將隱私權保護的範圍從住家，延伸至任何個人具有合理隱私期待的場所。在這些美國法院的判決裡，有一些可以解讀為足以針對某些類似雲端運算的現象，賦予隱私權保護。例如個人的容器，例如皮包，即使是交給他人保管，仍受隱私權保護[5]；實體儲存容器也受隱私權保護，例如保險箱或是租用的置物箱[6]；個人電腦也受隱私權保護，即使在某些狀況下該個人電腦完全是處在他人控制下，也無不同[7]；在連線網路的電腦裡所存的檔案，亦然[8]。

以各國法制的發展趨勢來看，規範監聽的通訊監察相關法規，規範之對象目前均已經包括電子通訊在內。以美國法制為例，在前述的汽車導航監聽判決中，

[4] See Amazon Web Services Customer Agreement, Jan. 20, 2010. http://aws.amazon.com/agreement/ (visited Oct. 22, 2010).

[5] See, e.g., United States v. Most, 876 F.2d 191 (D.C. Cir. 1989). See also United States v. Matlock, 415 U.S. 164 (1974).

[6] See, e.g., United States v. Spilotro, 800 F.2d 959 (9th Cir. 1985). See also United States v. Karo, 468 U.S. 705, 721 n.6 (1984).

[7] United States v. Karo, 468 U.S. 705, 721 n.6 (1984).

[8] See, e.g., United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007); United States v. Simmons, 206 F.3d 392 (4th Cir. 2000).

法院便認為 18 U.S.C. §§ 2518(4)[9]中所規定的「其他人」 (other person)，包含「提供服務給受監聽對象的服務提供者，以及透過設備或技術能力協助截聽通訊者的個人或機構組織」，[10]亦即法院認為監聽法可以當做「強制服務提供者在科技產品中新增純屬用以監聽消費者之功能」的依據。在這樣的司法立場下，消費者隱私受到保護的空間，自然極其有限。

既然我們已經從透過 Microsoft Office 處理文件的階段，轉移到幾乎日常生活的所有環節都可能需要倚賴網路──一則利用 Google 搜尋資料、在 eBay 購物、或者依賴 MySpace 和 Facebook 從事社交活動，他方面在基本運算及儲存等活動上大量倚賴雲端運算服務──的地步，那麼，面對這兩大變遷的共通點，亦即兩者皆具有建立龐大使用者資料的潛力，而這些做為 Web 2.0 和雲端運算基礎建設重要構成元素的資料，又可以轉而成為針對個人偏好和行為進行精確分析的鎖定式行銷（target marketing)，我們到底應該如何規範這些資訊所涉及的管制議題，便是不可迴避的問題。

這類規範議題，攸關個人隱私受衝擊的程度，相較於既有法律對於電信、銀行、錄影帶店等中介者就消費者個人資料使用和處理的高規範密度，但是對於構成 Web 2.0 和雲端服務時代重要環節的各種資料庫和服務提供者業者，其所適用的法律規範，則未臻明確，此一情形並非妥適。

同樣地，在許多醫療機構開始使用雲端運算服務的趨勢下，和醫療隱私有關的法律，例如美國保護個人醫療健康資訊的 Health Insurance Portability and Accountability Act（簡稱 HIPAA）[11]，在雲端運算時代裡是否仍足以保護個人醫療健康資訊隱私，即有疑義。究其實際，HIPAA 只適用於醫療院所、保險業者、健保資料的處理中心（clearing house），所以，HIPAA 是否適用雲端運算業者，也有疑慮。同理，美國保護影視錄影片租借紀錄和其他類似視聽資料的 Video Privacy Protection Act（簡稱 VPPA），也不一定能適用於雲端運算服務[12]。

雲端運算服務從某個角度來看，可以說是置物箱或個人電腦硬碟的現代版，因此，雲端運算服務的使用者，似乎也應該能期待其資料可以受到隱私保護的程序保障，免受不合理的搜索才對。然而，在傳統上，當法律管制中介者對於個人資料的使用時，例如美國的 Cable Communications Policy Act 中對於消費者隱私保護的規定，通常是要求業者在蒐集個人識別資料時，必須以書面或電子方式，

---

[9] 該規定原文為 An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.

[10] See 349 F.3d 1132.

[11] 45 C.F.R. §§ 160–64.

[12] Kurt Opsahl, Court Ruling Will Expose Viewing Habits of YouTube Consumers, July 2, 2008, http://www.eff.org/deeplinks/2008/07/court-ruling-will-expose-viewing-habits-youtube-us.(visited July 25, 2010).

取得消費者的同意，但是，若是業者基於偵測線路竊取或實施服務行為而為的資訊蒐集或處理之必要行為，則不在此限。同時，此一立法也禁止業者向第三人揭露消費者的個人識別資料，但是出於正當營業活動目的所為資揭露行為，則不在此限。[13]換言之，當消費者個人資訊被界定為「交易資訊」時，那麼業者在特定條件下可合法向第三人揭露。此一區別，正可能是雲端服務使用者隱私無法確保的重要原因之一。換言之，就雲端運算服務的資料是否受隱私保護的程序保障來說，問題癥結卻在於「企業紀錄原則」(business record doctrine)，也就是所謂的「第三人原則」(third party doctrine)。這個原則早在網路時代之前，便出現在美國聯邦最高法院的判決裡，主要內容是指當個人將其資訊交給(為其提供服務的)企業（即第三人）時，那麼，提供資料的個人對於該資料就沒有隱私之合理期待可言，所以也不適用美國聯邦憲法增修條文第四條所提供的隱私程序保障的保護[14]。換言之，法院認為：當該個人不再具有對本身資訊獨有的控制權時，也承擔了第三方可能自動將該資料轉而傳送或提交給他人的風險，因此便不能夠再合理地認為該資訊具有私密性可言[15]。根據此一原則，執法機關往往便可以主張網路活動的資料，不受憲法增修條文第四條的程序保障[16]。

在此一爭議尚未獲得妥善解決的現在，美國法院目前有兩個判決，值得一提。簡言之，這兩個判決認定：儲存在網路電子郵件信箱（webmail）的電子郵件資訊和儲存於服務提供者處的簡訊內容(text messages)，完全受到憲法增修條文第四條的保護[17]，這個判決立場，也等於意謂同樣的保護可以適用於雲端運算服務上。不過，即使如此，仍有爭議未能解決，特別是在雲端服務提供者以某種形式近用服務使用者的儲存內容（例如向使用者提供建議、掃描使用者檔案的病毒或文法錯誤、針對使用者的喜好提供廣告等等）的情形，仍有隱私隱憂。

## 參、雲端運算時代的「合理隱私期待」：判決分析

本文此一部份針對「合理隱私期待」予以分析，說明合理隱私期待標準如何建立，以及其操作現狀為何，接著，此一部份將進而說明數位世界裡的「合理隱私期待」所面對的不確定性。

---

[13] 47 USC 551(b)(2)(A).

[14] See United States v. Miller, 425 U.S. 435 (1976).

[15] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[16] See, e.g., US DOJ Computer Crime and Intellectual Property Section, Searching & Seizing Computers And Obtaining Electronic Evidence In Criminal Investigations, 1.B, Sept. 2009, available at http://www.cybercrime.gov/ssmanual/01ssma.html.

[17] Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), rev'd en banc on other grounds, 532 F.3d 521 (6th Cir. 2008) (Web email); Quon v. Arch Wireless, 529 F.3d 892 (9th Cir. 2008), cert. granted sub nom. City of Ontario v. Quon, 78 U.S.L.W. 3359 (U.S. Dec. 14, 2009) (No. 08-1332) (text messages).

## 一、合理隱私期待標準的建立及操作

在面對執法機關可能違反憲法增修條文第四條的程序保障這類爭議時，要先檢視的是執法機關的行為是否構成搜索，而構成搜索與否的判準，則是建立在「合理隱私期待」的標準。在 Katz v. U.S.此一判決中，多數法官不願意直接以「憲法保障的空間」或承認廣泛的隱私權保護的方式，來處理此一議題，而是提出「增修條文第四條保障個人，而非地方」這樣的立場。換言之，在該判決中，即使多數法官認為 FBI 在電話亭裡設置監聽器材並秘密錄下當事人的對話，是違反憲法增修條文第四條的要求，但是，該判決本身並未因此建立起明確的判斷基準，僅僅指出「無論個人身在何處，都必須具有免於不合理搜索扣押的權利」[18]。

究其實際，建立起明確的判斷基準，卻相當重要。值得注意的是，Harlan 大法官在 Katz 案中所撰寫的協同意見書裡，卻提出一項在後續判決中受到法院採納、用以判定是否構成搜索的判斷基準，亦即「合理隱私期待」此一判斷基準。「合理隱私期待」判斷基準具有兩個層次的要件，一是當事人具備其主觀（實際）的隱私期待，二是一般社會大眾也認同此一隱私期待是合理的期待。「合理隱私期待」此一判斷基準的建立，不僅可以決定是否構成搜索，也可以決定當事人是否有質疑該侵入行為的正當基礎，倘若法院認定執法機關的偵查活動不構成搜索扣押，那麼執法機關侵入行為所取得的檔案，即無證據排除法則的適用。雖然在這個判斷基準的發展過程中，的確出現某些不確定性，美國聯邦最高法院最終採納了這項判斷準則。不過，如前所述，值得注意的是，在開放空間（open fields）中的隱私期待，是否屬於合理的隱私期待，則難有定論，而且，觀諸歷年來美國聯邦最高法院處理許多因為新興科技的發展而衍生出來的隱私保護問題，也經常基於不同的理由而抽離了憲法增修條文第四條的保護。

然而，無論如何，個人是否明知自己曝露資訊於公眾眼前，卻是關鍵之一。Katz 案指出「若個人明知曝露於公眾─縱使在他家中或辦公室─眼前，即不是憲法增修條文第四條的保護對象」，根據此一邏輯，在 U.S. v. White 此一判決中，執法人員在線民同意下，監聽線民與被告之間的對話，並且將對話傳送給其他幹員時，法院認為「若法律未保護違法者所信任的同伴成為或身為警察，那麼法律亦不保護這名違法者所信任的同伴傳送或錄製對話」[19]。在 California v. Greenwood 此一判決裡，法院更進一步延伸「明知曝露」的意義內涵。在此一判決中，法院認為「被告明知他們的垃圾曝露在一般公眾的目光之下」，便難以援用憲法增修條文第四條做為保護自己隱私的依據[20]。

所謂「明知曝露」，不僅包含個人相對於朋友或一般大眾的曝露，更包含系統性地對於某些機構組織所為的曝露。因此，United States v. Miller[21]此一判決認

[18] 389 U.S. 347, 359 (1967).
[19] 401 U.S. 745 (1971).
[20] 486 U.S. 35 (1988).
[21] 425 U.S. 435 (1976).

為銀行存款人對其銀行記錄不具有合理隱私期待，因為存戶承擔「將帳戶資料揭露給銀行時，銀行可能將此資料交給政府」的風險。換言之，目前美國法院見解是認為個人對其諸如課稅紀錄、銀行與通聯紀錄等自願揭露予中介第三人的交易資料，由於個人應該早有意識到該資料已非全然私密，所以個人對此不具有合理隱私期待，而且，第三人就資料本身具有其營業利益，為利害關係人，所以警方毋須聲請搜索票即可取得第三人持有的個人資料。

而在 Smith v. Maryland 中，法院在審理執法機關安裝撥號紀錄器追蹤家用電話的撥號紀錄此一爭議，認為「所有的電話使用者皆知道他們的撥號紀錄將會被傳送給電話公司」[22]。換言之，如前所述，對於諸如此類的「交易資訊」，個人並為合理隱私期待可言。然而，即使如此，被認定為明知暴露自己資訊於大眾眼前的當事人，究竟是不是知道他們也曝露於無須搜索票即可進行搜索的風險之下呢？換言之，交易資料的數位化，會使得第三人關係更為複雜。聯邦最高法院在 Smith v. Maryland 此一判決中中所持的立場，亦即認定警方在被告住居電話安裝撥號追蹤器不構成搜索的立場，亦即因為撥號號碼是個人必須提供給電話公司以便完成通話的資料、而且個人也知悉公司需要保存此一紀錄，因此個人對此不具有合理隱私期待的見解，對於雲端運算環境下的隱私保護，更具有影響力。理由無他，無非出於遠距儲存或其他交易目的而將資料提供給雲端服務業者的情形，將會更為頻繁。同時，「交易資訊」和「內容資訊」兩者的區分，隨著雲端服務的普及化，也已經變得更加難以區分了。

## 二、數位世界中的合理隱私期待

在網路世界裡，上述「明知曝露」的判斷原則，不免出現諸多模糊空間。舉例來說，對於儲存在電腦裡的資料，「明知曝露」的意涵所指究竟為何？其判斷結果是否會受到該資料是否顯示於螢幕上、或者該資料是否能夠迅速存取等因素影響？如果是資料加密、必須輸入密碼或是當事人拋棄電腦或硬碟的情形，又將是如何？這些問題，都突顯出數位世界裡「搜索」的複雜性。學者 Orin Kerr 曾經建議可以類推憲法增修條文第四條所根據的「家即城堡」的概念，亦即一部可以用來上網的電腦，就像是我們在數位世界裡的家一般，也就是說，所謂「家即城堡」的概念，可以引伸成「硬碟即城堡」[23]，多少便可做為判斷數位世界裡的搜索是否合乎正當程序和隱私保護的基準。

然而，深究之下，即使是讓法院將此一原則適用於數位世界的搜索爭議中，依然有不少爭議可言。以 Kyllo v. United States 此一判決為例，在本案中，執法機關利用熱感應器探測被告住家所散逸的熱能分布情形，來監視被告是否有種植大麻的違法行為，法院認為熱感應設備並不是一般公眾所能使用的技術，所以推定警方利用一般民眾難以取得的先進科技設備從事監視行為，構成搜索，但是，

[22] 442 U.S. 735, 737 (1979).

[23] See generally Orin S. Kerr, Four Models of Fourth Amendment Protection, 60 STAN. L. REV. 506 (2007).

假如一般民眾也能在市面上買到諸如此類監視設備，那麼，在這種情形下，個人是否仍然具有合理隱私期待呢？倘若使用者都知道網路服務業者都會保存使用記錄及個人資料，則使用者對於儲存於網路服務提供者處的個人資料，是否還具有合理隱私期待呢？諸如此類的問題，即使根據上述判決，都不是容易回答的問題。

從比較法的觀點來看，美國國會在 1986 年通過 Electronic Communication Privacy Act [24]（簡稱 ECPA），做為處理資訊時代隱私保護問題，根據該法 Section 2703──亦即 Electronic Stored Communications Act[25]的部分──的規定，法院可以要求 ISP 業者提供儲存在外部伺服器超過 180 天以上的電子郵件與其他電子記錄，而且毋須告知當事人，便可提供上述檔案和紀錄，此一規定截至目前為止並未在聯邦最高法院遭遇到違反憲法增修條文第四條規定的挑戰。同樣值得一提的是，即使是使用者對於自己的電子郵件是否具有合理隱私期待的問題，嚴格說來也尚未獲得澄清。以近年和此議題關係最為密切的第六巡迴法院判決 Warshak v. United States[26]為例，在該案中，原本法院認為「個人對於透過 ISP 業者儲存、傳送及接收的電子郵件具有合理隱私期待」，其考量因素之一是使用者與其 ISP 業者的契約類型，因此同意發布初步禁制令（Preliminary Injunction)，禁止政府扣押個人電子郵件信箱內的內容，除非政府事先告知電子信箱使用者或顯示使用者與 ISP 業者之間無合理隱私期待，因此事實上等於認為 Section 2703(d)有違憲之虞[27]，但是，嗣後法院又以全部法官均參與（en banc）的判決方式，提出其他理由，迴避處理此一議題，所以個人的電子郵件隱私受保護程度到底如何，仍不明朗。

不過，同樣值得注意的是，美國法院最近的判決亦有認為搜索電腦的行為同樣應該受到憲法增修條文第四條之限制者。在 United States v. Crist[28]此一判決中，法院認為移除電腦裡的硬碟並重製內部數位資料影像的作法，儘管並未造成物理上的入侵現象，但也應該認定為構成搜索。法院並且指出「將整個電腦從事雜湊值分析(hash value analysis)，將會導致政府可以檢視所有檔案、網路紀錄、圖檔及好友名單」，因此其會構成個人合理隱私期待遭到侵害的結果，亦即有憲法第四增修條文的適用。

同樣值得探討的是，遠距儲存的資料，其目的並不是在於提供給大眾近用，而且，通常是以未顯示網址連結、認證、密碼或加密等機制保護，因此，除了採用雲端運算服務的企業必須權衡外包資料儲存的財務利益與資料安全成本之外，對於電子郵件這種發展已久、而且是早期雲端運算最常提供的服務類型，即使美國聯邦最高法院尚未就此發展出適用憲法增修條文第四條的判斷基準，下級

[24] Pub. L. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).
[25] 533 U.S. 27 (2001).
[26] 532 F.3d 521 (6th Cir. 2008) (en banc)(vacating in part 490 F.3d 455 (6th Cir. 2007)).
[27] 490 F. 3d. at 475.
[28] United States v. Christ, No. 1:07-cr-211, 2008 WL 4682806, at *9 (M.D. Pa. Oct. 22, 2008).

法院目前的判決趨勢及其所持理由，依然值得持續、密切地觀察其發展。

舉例來說，除了上述第六巡迴法院的判決對於電子郵件的資訊隱私保護採取比較負面的立場之外，第九巡迴法院在 2008 年的 Quon v. Arch Wireless Operating Co.[29]一案中，是採取信件、電郵及簡訊之間並無明顯區別，所以政府員工對於其簡訊內容應該享有合理隱私期待的立場。而在 United States v. D'Andrea[30]一案中，涉及的爭議是警方利用匿名告發者提供的帳號密碼，偵查一個以密碼保護其內存兒童色情圖片的網站，有無侵害隱私。該案法院雖然將該網站類比為密閉的容器，但是由於已經有私人侵入該網站，而且繫爭未具搜索票之搜索行為並未逾越上述私人搜尋的範圍，所以法院便未在該判決中再進一步探究構成虛擬密閉容器的充分措施為何[31]。從以上判決內容，更可以得出的暫時結論是：針對個人將其私人生活的眾多層面，出於儲存及存取的目的而上傳到雲端服務平台的事例，究竟憲法增修條文第四條對於警方搜索雲端服務平台資料的行為，賦予怎樣的正當性和容許程度，在司法判決所詮釋的層次來說，仍處於模糊階段。總而言之，資訊傳播科技的發展不但會改變我們的生活型態，連帶也使隱私的概念範圍隨之模糊化，當隨身攜帶筆電、黑莓機或 IPhone 成為常態，區隔工作資訊與個人資料的困難性也隨之提高。在這種情況下，不但線上與離線兩者之間的界限日趨模糊，通訊的定義也日益模糊。

以線上與離線應用的界限逐漸模糊這一點來說，傳統的離線應用程式－諸如 MS Office、Adobe、 Photoshop 等應用及其相關資料，皆存在於個別使用者的電腦硬碟裡，相對地，webmail、Google Documents, Yahoo Calendar 等線上應用及其相關資料則存在於雲端服務業者的遠端伺服器，使用者無論身在何處都可存取其所需的資訊，不需要掌握該資訊實際上儲存在何處。2008 年 9 月 Google 推出新網路瀏覽器 Chrome 時，紐約時報的 David Pogue 形容此一瀏覽器軟體「當你點選應用程式的桌面捷徑時，開啟網站不會如同以往般顯示網址列及按鈕，而是如同一桌面程式般運作，此一特色將混淆線上和離線兩者的界限」。[32]David Pogue 在該文中指出 Google 藉由此種特色，建立一個軟體運作的平台，轉移傳統上對於作業系統的重視。如前所述，不但 Chrome 及類似的 Mozilla Prism 計畫正嘗試整合線上應用及電腦本身，許多使用網路行事曆和線上文書處理的使用者，也根本並未意識到這些資料是儲存在遠端伺服器、而非個人電腦。因此，就隱私安全管制角度來說，核心議題便是使用者對於其相信儲存在個人電腦硬碟、但實際上位於遠端伺服器的資料內容，是否具有「合理隱私期待」，而此一「相信」，則是隨著科技或軟體開發者持續讓線上及離線應用兩者難以區隔，逐漸變得更加合理。

以通訊的模糊化此一特色來說，過去十年間，網際網路發生的重大變動，便

[29] Quon v. Arch Wireless Operation Co., 529 F.3d 892, 905-06 (9th Cir. 2008).
[30] United States v. D'Andrea, 497 F. Supp. 2d 117, 118 (D. Mass. 2007).
[31] Id. at 122-23.
[32] David Pogue, Serious Potential in Google's Browser, N.Y. TIMES, Sept. 3, 2008, at C1.

是朝向 Web 2.0 這種逐漸提高互動性、資料分享的網路發展，而在 Web 2.0 的網路世界裡，何謂通訊，便難以界定。例如，如果某個使用者張貼照片到 Flicker 上，而某人對該照片予以標籤，那麼，上述兩者（甚至第三人間）之間，到底有無溝通？若使用者將自己的線上日曆與他人分享並新增個人活動，這樣是否是與他人溝通？線上日曆寄電子郵件給用戶提醒將發生的事件，也算是溝通嗎？電子郵件顯然是通訊，但上述例子中，與他人溝通可能是出於偶然、附帶間接或事後補充。此種通訊模糊化的趨勢，自然也帶來了通訊隱私上的管制難題。

# 肆、雲端運算服務成為網路通訊監察工具所衍生的隱私爭議

本文此一部份說明雲端運算時代帶來的另一個隱私爭議，也就是是通訊監察行為所帶來的隱私威脅。換言之，即使多數國家的通訊監察法已經提供相當程度的隱私保護，但是，是否足以適當保護儲存在雲端運算裡的資料及其內容，卻依然不無疑問。舉例來說，執法機關是否可以在沒有搜索票或是未通知使用者的情況下，要求雲端運算服務業者提供交易紀錄，可以想見便是值得重視的爭議之一。

## 一、從個人電腦典範到雲端運算典範的犯罪偵查

從網路服務業者可能採取的經營策略來看，雲端運算時代為使用者帶來的另一個隱私威脅，就是雲端服務提供者不但在明知的情況下，疏於保護使用者的隱私，而且很可能在迫於政府部門的各種威脅利誘或者管制措施，協助政府部門侵害使用者的隱私。

換言之，近年來數位科技的進步，急速提升政府從事大規模監視的能力。電信公司及 ISP 業者的法務相關部門，往往必須隨時配合處理執法機關要求的監聽需求，或者配合提供通訊及即時發話位置等資料，早非新聞。即使在理論上執法機關的每一個執法行動，都必須是逐案審查的對象，但是，雲端服務的普及化，卻讓執法及其審查模式，受到挑戰，也是不爭的事實。在「個人電腦典範」的時代，當政府想要從十個嫌疑犯的家用電腦中尋找犯罪證據時，通常必須在警方提出相當理由的情況下，才能說服法官逐一針對個別犯罪嫌疑人簽發搜索其個人電腦的搜索票，並且必須派員到個別犯罪嫌疑人家中扣押電腦，進而取得並鑑識分析電腦內所儲存的相關檔案。但是，在「雲端運算典範」的今天，既然許多使用者已經轉而使用以雲端計算為基礎的服務，那麼，提供雲端服務的業者，便極可能轉而成為執法機關從事數位搜索扣押的關鍵所在。換言之，在雲端運算時代裡，搜索十個犯罪嫌疑人的電腦檔案，很可能會轉而變成僅須要求諸如 Google 之類的雲端服務提供者揭露某些資料即可，大幅降低執法成本。

對於傳統的電信業者來說，由於其擔心遭到協助非法監聽的指控，因此對於

執法機關所提出的監聽要求，通常會以戒慎恐懼的態度來檢驗其是否符合法定程序，而各國法制通常也會對違法提供使用者通訊資料的電信公司，課予法律責任，這便是電信公司拒絕遵循不依程式的執法要求的重要誘因。因此，當政府監視活動可以不經過電信服務業者即可進行時，那麼消費者便會被剝奪掉這層額外的隱私保障。

「合理隱私期待」原則的適用，其終極目標無非是為了保障個人免於違憲的搜索扣押。但是，如前所述，若是依照美國聯邦最高法院的「第三人原則」（third party doctrine）判決見解，「憲法增修條文第四條並未禁止政府向第三人取得當事人向第三人揭露的資訊，縱使該資訊的揭露是出於特定目的使用及第三人保密的預設，亦然」[33]。根據此一判決見解，對於個人儲存在遠端伺服器、雲端服務提供者得以分享儲存的數位資訊來說，其實便很難提供充分的隱私保護。

## 二、以正當化標準平衡安全與隱私的美國法制實務運作

更重要的是，從通訊監察的角度來看，執法機關仰賴正當化標準（justification standards）[34]的判斷，取得個人資訊並轉為犯罪證據的可能性越高，隱私風險所帶來的惡害也就越高。以美國法院實務發展為例，法院經常基於憲法或法律中所規定的正當化，標準衡量警方發動攔停、搜索扣押或者逮捕行為的合憲性或合法性，而這些正當化標準，則是可以用「該行為能找到犯罪證據的可能性」為基準，進一步區分為「相當理由」（probable cause）、「合理懷疑」（reasonable suspicion）或「關聯性」（mere relevance）三種類型，而且這三種類型皆以美國憲法增修條文第四條為基礎。

究其實際，美國憲法增修條文第四條僅明文規定取得搜索票須合乎相當理由的要件，而法院判決的發展，則是在避免個人受到國家不合理監視及干預的原則下，將其他正當化標準導入增修條文第四條中。聯邦最高法院在 1968 年的 Terry v. Ohio 判決中，訴諸「合理懷疑」原則，主張警方基於辦案經驗，不管是對可疑人車進行短暫的調查性攔停，或者是進行搜身以防該執法對象攜帶武器的行為，即使欠缺相當理由，亦屬合憲[35]。再者，在某些具有特定政府目的但非基於執法需求的情況下，例如學校安全管理需求[36]、政府機關工作場所的搜索[37]、政府公務員的藥物測試[38]等，則是經常循 Terry v. Ohio 此一判決先例，適用合理懷疑原則。在關聯性原則下，警方可以僅持大陪審團命令，便要求執法對象提出文件或證詞[39]。甚至，有時候某些蒐證行為則是被認定為不構成搜索扣押，因而毋

[33] United States v. Miller, 307 U.S. 174 (1939).
[34] See, e.g., CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21-47 (2007).
[35] See Terry v. Ohio, 392 U.S. 1, 27 (1968).
[36] See, e.g., New Jersey v. T.L.O., 469 U.S. 325, 341 (1985).
[37] See, e.g., O'Connor v. Ortega, 480 U.S. 709, 724 (1987).
[38] See, e.g., Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 666 (1989).
[39] See United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991).

須滿足任何正當化標準，例如警方可以逕自從開放場所(open fields)飛掠觀察私人土地[40]，也可以檢視私人拋棄在街道邊的垃圾[41]或是追蹤發話對象[42]，都屬於典型實例。

就線上隱私保護的領域而言，由於聯邦最高法院針對涉及第三人（例如銀行和電信業者）持有的私人記錄，是否適用憲法增修條文第四條的規定，採取否定立場[43]，所以，若是依循美國聯邦最高法院的判決立場，可能會弱化網路使用者甚或雲端運算服務使用者線上隱私受保護的程度。有鑑於此，美國國會透過立法彌補此一隱私保護的潛在落差，例如當該通訊監察行為特別具有侵入性時，國會立法即要求從事該行為須具備相當理由，方得為之，例如 the Wiretap Act 關於警方即時監聽個人電子通訊的規定，即屬之[44]，the Foreign Intelligence Surveillance Act 也要求情報人員在進行電子通訊監察時，也必須合乎相當理由的要件[45]。再者，the Stored Communications Act （簡稱 SCA）要求警方在取得儲存在第三人處的電子郵件或電子郵件內容之前，必須具備相當理由，但是，SCA[46]以及 the Pen Register and Trap and Trace Act （簡稱 Pen Register Act）[47]的部分規定，也允許警方毋須達到相當理由，只要說明該電子通訊或記錄內容與犯罪調查具有關聯性即可[48]。立法者之所以允許這類低於相當理由程度的正當化標準，其主要原因不外乎認為政府所需的上述資訊不具有高度私密性質，因此不需賦予高度保護，而採用合理懷疑或關聯性這兩個標準，已經足以避免警方以侵犯人民權益的調查手法辦案，或者，立法者認為應該調整網路通訊隱私受保護的程度，亦即如果執法者具有中等程度的懷疑時，那麼僅允許中等程度的侵入[49]。

## 三、正當化標準在規範網路犯罪偵查上所遭遇的侷限

此一立法現狀，對於隱私保護而言，可謂不利，因此，論者不乏認為應該提高正當化標準，甚至明確主張應該一律採用「相當理由」此一條件者[50]，縱使是

---

[40] See, e.g., Oliver v. United States, 466 U.S. 170, 183-84 (1984); Florida v. Riley, 488 U.S. 445, 450 (1989).

[41] See, e.g., California v. Greenwood, 486 U.S. 35, 40 (1988).

[42] See, e.g., Smith v. Maryland, 442 U.S. 735, 745 (1979). See also Pen Register and Trap and Trace Act, 18 U.S.C. §§ 3121-3127 (2006).

[43] See United States v. Miller, 425 U.S. 435 (1976). See also Smith, 442 U.S. at 736 n.1, 745.

[44] See 18 U.S.C. § 2518 (1) & (3) (2006).

[45] 50 U.S.C. § 1805(a)(3) (2006).

[46] 18 U.S.C. §§ 2701-2711 (2006).

[47] Id. §§ 3121-3127.

[48] See, e.g., Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1219 (2004).

[49] See Paul Ohm, Probably Probable Cause: The Diminishing Importance of Justification Standards, 94 MINN. L. REV. 1514, 1521-22 (2010).

[50] See, e.g., Patricia L. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 GEO. WASH. L. REV. 1375, 1436 (2004); Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 GEO. WASH. L. REV. 1557,

擁護 SCA 此一立法者，也認為該立法目前對於電子通訊內容所提供的保護過於薄弱[51]。

但是，亦有學者主張，即使將警方從事網路犯罪偵查活動的正當化標準一律提高到相當理由，實質上也無助於人民隱私權益的保護，因為，執法機關從事網路犯罪偵查時，通常不是具有相當理由，就是根本毫無依據可言，幾乎不存在適用合理懷疑或關聯性的中間折衷情形。以電子郵件信箱或 IP 位址這兩種最常見的網路證據為例，其通常附隨電子郵件和登入記錄，而且，以目前網路架構和網路技術來說，當執法機關掌握到犯罪事件中可疑的電子郵件信箱或 IP 位址時，通常可以進一步發現其他資訊，因此足以符合相當理由的要件。

詳言之，在真實世界裡，執法機關發現和蒐集證據的過程，事實上是逐步提升懷疑程度的持續過程，但是，相形之下，網路犯罪的調查過程，通常比較是跳躍而片段，執法機關取得的電子郵件信箱或 IP 位址，可能是關鍵線索，可以讓執法機關循線聯繫電信業者或網路業者，要求其提供進一步資料，並據此申請核發搜索票[52]，但是，執法機關循電子郵件信箱或 IP 位址追查的結果，也可能一無所獲，其結果鮮少介於二者。亦即在網路犯罪偵查中，很難想像執法者會遭遇「些微提升犯罪嫌疑」或「稍微縮小犯罪嫌疑範圍」的證據，通常都是取得能夠直指特定對象的證據[53]。

正因為如此，所以美國法院至今幾乎從未在網路犯罪的案件中認定執法機關不符相當理由的要件而排除執法機關所取得的證據。以 SCA 的實務為例，SCA 容許警方在未達相當理由要件的情形下，即可強制網路業者提供使用者儲存在其伺服器的部分通訊內容[54]，SCA 本身的規定雖未提供救濟管道，但是卻不難想見電子郵件內容因此遭執法機關取得的刑事被告，會主張其乃未達相當理由程度的蒐證行為，有違憲之嫌，然而，美國法院至今受理的相關案件裡，卻從未認定執法機關欠缺相當理由[55]。即使是 2004 年聯邦第九巡迴法院在 Theofel v. Farey-Jones[56]否定了聯邦司法部將 SCA 解讀為允許執法機關透過文件提交命令（subpoena）或 d-order，即可向電子郵件服務業者取得已經拆閱但儲存在其伺服器中的郵件此一見解和實務作法，但是，美國國會嗣後一連串的修法結果，卻日益弱化使用者所能期待的隱私保護。甚至，Theofel 判決根本從未真正影響到執法機關的偵查實務，因為執法機關鮮少出現未能符合相當理由的情況，此一判決出現前後唯一的差異，可能只是在文書作業的負擔增加而已。

換言之，執法機關的偵查行為是否具有正當化基礎，絕大多數的情況是屬於

---

1592 (2004). Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299 (2004).

[51] *See* Kerr, *supra* note 50, at 1242. .

[52] *See, e.g.*, United States v. Perez, 484 F.3d 735, 741-42 (5th Cir. 2007).

[53] Ohm, *supra* note 51, at 1525-28.

[54] 18 U.S.C. § 2703(b) (2006).

[55] Ohm, *supra* note 51, at 1536-38.

[56] 359 F.3d 1066 (9th Cir. 2004).

全有（合乎相當理由）和全無（缺乏任何懷疑基礎）兩種類型，基於此一現象，如何為網路犯罪偵查的正當化標準找到一個平衡治安需求與人民隱私權益的模式，應是我們面對新興科技所帶來的程序保障問題時最大的挑戰。

追根究底之下，我們不難發現，美國憲法增修條文第四條是以「相當理由」當做平衡隱私保護與安全需求的重要工具，但是，當前充斥各種網路服務中介者的通訊架構，對於憲法增修條文第四條的重心究竟何在此一問題，卻帶來頗為嚴峻的挑戰。換言之，隨著網路和智慧手機的普及，通訊網路上的中介服務將無所不在，同時，在 GPS 和 RFID 等通訊型態下分分秒秒所累積的各種資訊，則是使使用者的行蹤幾乎無所遁形[57]。在網路服務提供者運用如此完備的紀錄監視技術，詳實縝密地記錄使用者所有活動的架構下，如何建立起有效避免執法機關濫行偵查的機制，已成網路時代保護人民隱私的關鍵所在。

美國法律學者 Rubenfeld 認為美國聯邦憲法增修條文第四條的核心關切，便是「安全」（security），他特別指出隱私概念的瑕疵，在於隱私期待的操作逸脫於實際執法脈絡、取決於廣泛的社會期待，而且在數位網路逐漸擴張的趨勢下，第三人原則終將使憲法增修條文第四條成為隱私保護的空殼[58]。Rubenfeld 教授因此提出新的檢驗標準，也就是「普遍性」（generalizability）此一檢驗標準，意即政府從事監聽或拘禁的行為，也就是政府執行搜索扣押的權力，必須由法院基於特定標準或情況下核准，因此若政府搜索扣押的權力缺乏此一制衡，將導致守法民眾的安全遭到破壞，因此法院在憲法增修條文第四條下判斷政府搜索扣押合法與否時，毋寧是在判斷政府執法手段可以普遍化到甚麼程度，而不至於侵害民眾安全權利。故當政府主張的某種監視與拘禁措施，若是在日常生活中系統性、常態性且廣泛地實施，必然會侵害民眾受憲法增修條文第四條保障的權利時，這樣的措施必將摧毀民眾的安全感，並且感受到國家壓迫的令人無法容忍之處，而構成違憲[59]。政府搜索雲端服務業者管理的線上資料，在此一標準檢驗下，極可能同樣令人感到無法容忍，使民眾皆成為潛在偵查對象而侵害民眾的安全感。此一學理上的主張，即使無從完全取代現有的判斷基準，但是，或許多少可以補充現行判斷基準的不足之處。

在這個網路通訊需求導致中介服務提供者充斥的新興科技時代裡，中介服務者及其所持有的種種使用者資料，幾乎已經成了犯罪行為通訊監察系統最重要的一環，雖然不乏論者主張一般循規蹈矩、無事可隱藏的人民對於犯罪行為的通訊監察系統無須擔憂懼怕，但此一主張在隱私權學理上不具有說服力[60]。對於此一網路發展現象抱持悲觀態度者，則是認為目前通訊監察系統事實上幾乎無處不

[57] See, e.g., Jerry Kang & Dana Cuff, Pervasive Computing: Embedding the Public Sphere, 65 WASH. & LEE L. REV. 93 (2005).

[58] See generally Jed Rubenfeld, The End of Privacy, 61 STAN. L. REV. 101, 115 (2008).

[59] Id. at 131-132.

[60] See Daniel J. Solove, "I've Got Nothing To Hide" and Other Misunderstandings of Privacy, 44 SAN DIEGO L. REV. 745, 764-72 (2007).

在，在這個前所未有的全面性的通訊監察架構下，憲法中預設的「相當理由」原則所建立的界限，已經逐漸失去隱私保護作用。以 Facebook 這種社交網路為例，使用者利用 Facebook 的社交網站平台做為平常透過電話或碰面所進行社交談話的替代平台，但是，原本在現實世界中會像空氣般消失不見的談話內容，在 Facebook 上卻會被業者保存下來，執法機關只要透過 Facebook 及相關服務業者這些第三人，即可取得質量均相當可觀的資料。

美國知名的刑事訴訟法學者之一 Orin Kerr 對於美國法院從憲法增修條文第四條的規定所發展出來的第三人原則，向來多所辯護[61]，Kerr 主張第三人原則可以避免犯罪者在憲法增修條文第四條的保護下，利用第三人規避其犯罪行為，使得銀行、電信業者和網路業者等第三人成為犯罪溫床[62]。但是，Kerr 的主張，毋寧說是僅僅關注網路通訊科技如何讓犯罪行為變得更為便捷此一面向，卻忽略在第三人原則下，可以透過中介的網路服務業者所掌握的通訊技術，賦予執法機關相當強大的偵查權。雖然 Kerr 認為新興通訊技術提供了潛在犯罪者規避遁逃的新方式，因此可以正當化第三人原則這個例外情形[63]，然而，從長遠的觀點來看，在網路科技所建構起來的第三人無處不在且無時不在蒐集個人資料的數位世界裡，這無疑是將第三人原則當做規避個人隱私保護需求的執法者工具，潛藏極高的隱憂。

## 伍、結論

隨著寬頻網路與行動通訊技術演進和隨之而來的便捷互動，個人上傳或儲存資訊到網路上的雲端服務平台，已成常態，而「隨時隨地存取」也因此已經成為 Web 2.0 與雲端服務的常用語彙。儘管美國聯邦第九巡迴法院在 Quon v. Arch Wireless Operating Co.判決中認為個人對於信件內容具有合理隱私期待，卻未處理個人對於信件儲存空間(inbox)本身有無合理隱私期待可言，這樣稍嫌保守的法院立場，其實不利於因應涉及更廣泛存取活動的雲端服務環境。儘管雲端平台中儲存的個人資訊均具有私密性此一特質，在理論上或可正當化其具有合理隱私期待，但是，畢竟網際網路在許多面向上都依然被公認為具有公開媒介的特質，雖然將資訊傳送到公開空間裡，並不盡然意味著因此即無合理隱私期待可言，但在個人沒有積極採取隱匿該資訊的實際行動之前提下，該等資訊是否受隱私保護，想必會是引發爭執之處。

在 United States v. D'Andrea 一案中，法院則是將網站類比為儲存紀錄的檔案櫃，因此只要是認為以密碼保護網站者，正如同實體世界中的門鎖和防盜鈴一般，那麼該網站內容應受到隱私權保護，但做成該判決的法院卻未深論保密措施

[61] Orin S. Kerr, The Case for the Third-Party Doctrine, 107 MICH. L. REV. 561, 587-600 (2009).
[62] Id. at 576.
[63] Kerr, supra note 61, at 575-76.

必須嚴密至至何種程度，始足以受到憲法增修條文第四條的保護。以 Orin Kerr 教授的主張來說，其判斷隱私期待是否合理的取徑，是以「權利」做為基礎，亦即當該隱私期待具有可資主張的權利來禁止政府的隱私侵害行為時，始具有正當性。[64]根據此一理論立場，Katz 案所建立起來的檢驗標準，便不是依據物品保有私密的可能性，而是依據個人隔絕他人窺視的權利有無而定。換言之，加密比較類似於實體世界的不透明塑膠袋所造成的不透明狀態，然而，其他非以密碼保護的單純阻隔，例如無法透過搜尋引擎找到網站的隱匿連結本身，似乎便比較難類比至實體世界的阻隔形式，這是我們在思考雲端服務加密措施足以滿足合理隱私期待的要件時，應該注意之處。

其次，美國法院針對中介第三人角色所建立的「第三人原則」，也是我們在討論雲端服務所涉及的資訊隱私保護問題時，不得不特別留心之處。即使是面對第三人自電信服務或雲端服務等中介活動中合法取得特定交易資料，也有必要質疑「電子信件收發相對人地址等資料的取得，是否等同撥號追蹤器？」，以及密碼、未顯示網址或是雲端可存取的資料，到底是上述可以合法第三人提出之交易資料，抑或應該被認為是受保護的隱私內容。在上述第九巡迴法院 Quon v. Arch Wireless Operating Co.一案中，法院認定通訊服務提供者本身並非簡訊內容的一方，因此執法機關不得以傳票要求其提供紀錄，此一判決其實和第九巡迴法院在 United States v. Forrester[65]一案中的主張息息相關。換言之，由於電子郵件使用人應該知道電子郵件相關資訊會提供給網路服務業者作為指引路由目的使用，因此其對於信件寄信資訊和收信者地址等，均不具有合理隱私期待。Forrester 案的法院顯然是將信件收發人地址類推為 Smith v. Maryland 案中的電話撥號追蹤器，但是，這樣的類推，其最大問題在於：在 Smith 一案的法院區分撥號紀錄與通話內容的架構下，撥號追蹤器僅顯示通話兩方的號碼，無法揭露通話方的身分，然而，相對地，電子郵件卻通常可連結到特定使用者，甚至郵件帳號便常是使用者姓名，因此電子郵件收發紀錄更能精確識別通話方，在侵害程度的判斷上上，自然不該等同撥號追蹤器。

在雲端運算環境裡，交易資訊將比以往更能揭露個人身分，也更容易取得，例如網站位址此種瀏覽器必須據以進行資料交換和連線的資料，雖屬於交易資料，但這卻極可能意味著執法機關可以輕易地要求雲端服務業者提供「未顯示的網址」，甚至包括帳號密碼等認證資料，也會被納入交易資料的範疇而不保。即使美國部分法院認為第三人有限制的近用，不足以排除當事人的合理隱私期待，亦即縱然認定當事人默示同意第三人揭露的風險，該同意範圍亦應有所限制[66]。

---

[64] Orin S. Kerr, The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy ?", 33 CONN. L. REV. 507 (2001).

[65] Quon, 529 F.3d at 905 (quoting United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)).

[66] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008) (citing United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007)); See also Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), vacated, 532 F.3d 521 (6th Cir. 2008).

但是，在法院見解尚未趨於一致之前，雲端平台上的交易資料受保護程度究竟有多高，依然是需要戒慎恐懼以待的問題。

同樣地，在雲端環境裡，區分交易資料與內容資料，本是相當困難之事，例如在搜索引擎上鍵入搜尋字串，等於開啟與服務者之間的數據交換，使用者便將因此承擔雲端服務者可能揭露該資訊的風險[67]。電子郵件收發對象等交易資訊與信件內容本身有別，能夠存取信件內容的服務業者並非通訊的一方，使用者雖利用雲端平台從事文件作業，但其目的並非將內容分享予服務業者，因此服務業者並非可決定內容揭露與否的通訊一方。其次，在行事曆和相簿等明顯屬於內容資料而非交易資料的區分下，仍有部分資料，例如在雲端服務業者伺服器中架設的網站網址屬性不明，或者服務業者可以保留其網站使用者密碼或認證資料的副本，在此種架構下，如何避免任由執法機關藉由第三人深入私人空間，因此產生隱私安全過度萎縮的流弊，更是關鍵所在。

最後，科技的進步也相應地提高了執法機關追查犯罪的能力，再加上相當理由這個要件逐漸不再能稱職扮演平衡隱私保護及安全需求的角色，因此，如何找到真正的平衡點，是我們將關注重點放在「合理隱私期待」的同時，必須深入思考之處。倘若當事人具有合理隱私期待，那麼應適用相當理由的正當化標準，受憲法的隱私保護，然而，「合理隱私期待」及「相當理由」兩者恐怕都已經不足以在網路中介者難以計數的情況下，確保隱私和安全兩者的平衡，在這種情況下，若能將關注焦點轉移到美國聯邦最高法院在 Berger v. New York 一案中判定紐約州過於廣泛寬鬆的通訊監察法令無效[68]的理由上，亦即當通訊監察的範圍過於廣泛，而且未區分偵查中的犯罪類型、未限定執法機關監聽時間、鎖定的談話內容，也沒有事後通知當事人的相關規定，因此，該案法院認為有必要課予更高程度的程序保護，而 Susan Freiwald 主張網路時代的通訊監察應該符合必要性（necessity）、特定性（particularity）、有限期間（limited time）與最小侵害性（minimization）等四個要件[69]，在法院對於網路時代的合理隱私期待標準為何難以確認，而執法機關從事隱藏式、侵入性、不區別類型且持續性的廣泛通訊監察行為，已經逐漸成為執法常態的今天，本文認為關於規制政府通訊監察行為的界線何在此一討論的重心，應從是否構成搜索扣押的實質判準，移轉到更加關注當事人是否具有合理隱私期待及偵查機關的正當化標準兩者所隱含的程序性保障意涵，才是平衡公共安全和資訊隱私的可行處理模式。

[67] See, e.g., Jayni Foley, Note, Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases, 22 BERKELEY TECH. L.J. 447, 457 (2007).
[68] Berger v. New York, 388 U.S. 41, 43-44 (1967).
[69] Susan Freiwald, First Principles of Communications Privacy, 2007 STAN. TECH. L. REV. 3, 10.

# 參考文獻

Bellia, Patricia L. (2004). *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375.

Foley, Jayni (2007). *Note, Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases,* 22 BERKELEY TECH. L.J. 447.

Freiwald, Susan (2007). *First Principles of Communications Privacy*, STAN. TECH. L. REV. 3.

Kang, Jerry & Dana Cuff (2005). *Pervasive Computing: Embedding the Public Sphere*, 65 WASH. & LEE L. REV. 93.

Kerr, Orin S. (2001). *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy ?"*, 33 CONN. L. REV. 507.

Kerr, Orin S.(2004). A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. 72 GEO. WASH. L. REV. 1208.

Kerr, Orin S. (2007). *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 506.

Kerr, Orin S. (2009). *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561.

Lessig, Lawrence (1999). Code and Other Laws in Cyberspace. New York : Basic Books.

Mulligan, Deirdre K. (2004). *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557.

Ohm, Paul (2010). Probably Probable Cause: The Diminishing Importance of Justification Standards, 94 MINN. L. REV. 1514.

Pogue, David (2008). *Serious Potential in Google's Browser*, N.Y. Times, Sept. 3, 2008, at C1.

Rubenfeld, Jed (2008). *The End of Privacy*, 61 Stan. L. Rev. 101.

Slobogin, Christopher (2007). Privacy at Risk: The New Government Surveillance And The Fourth Amendment. Chicago : University of Chicago Press.

Solove, Daniel J. (2004).*Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264.

Solove, Daniel J. (2007). *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745.

Volokh, Eugene (2003). *The Mechanism of the Slippery Slope,* 116 HARV. L. REV. 1026 .