主題論文
© 臺大法學論叢 NTU Law Journal
第 52 卷特刊/Vol.52, Special Issue (11. 2023)

刑事偵查程序中加密檔案的解密

李榮耕*

<摘要>

電腦在現代生活中扮演著不可或缺的角色，大量的資訊也因而以數位的型態交換，或儲存於各式的載體中。是以，如何確保檔案的安全，確保檔案不被他人所接觸，就有其實際需求。檔案的加密技術的普遍使用，也就應運而生。不過，犯罪份子也同時使用了此一技術，隱匿犯罪事證，大大地增加偵查上的困難。在討論及分析後可以知道，可能性理論無法完整地解釋隱私的意涵，不能因為技術上難以破解，就認為人們加密後的檔案可以主張隱私權。再者，加密後的檔案無法類比為上鎖的容器，因為人們並不是看不到加密後檔案的內容，只是無法了解其意思而已。相比較之下，檔案的加密更類似於翻譯以外國語言進行的交談，使用警犬嗅聞，或是拼湊軋碎的文件。從結論上來說，我們認為人們不會僅僅因為將檔案加密而當然能夠就其內容主張合理隱私期待。在合法取得加密檔案後，檔案的解密沒有令狀程序的適用，執法官員可以逕自破解，不需要事先獲有法官的授權。

關鍵詞：隱私、加密、解密、破解、合理隱私期待、搜索、令狀原則

* 國立臺北大學法學院教授。
E-mail: ronggengli@gmail.com
・投稿日：02/01/2023；接受刊登日：06/21/2023。
・責任校對：辛珮群、黃品樺、王怡萱。
・DOI:10.6199/NTULJ.202311/SP_52.0003

♦目 次♦

壹、前言：問題的提出

電腦在現代文明社會中，在人們有計劃或無意識的情形下，既廣且深地，成為人們生活中，乃至於企業或是團體運作上不可或缺的一部分。電腦或是相關設備，隨著技術及服務的不斷推陳出新，大幅度地取代了傳統的郵信、電話、行事曆、筆記、財務管理及交通票券等功能，也因此鉅細靡遺地記錄著人們或是組織團體的各式各樣資料[1]。因為穿戴式裝置的普及（如智慧型手錶或手環等），電腦或是個人數位設備上還會儲存有人們的生理資訊，如心率、步數、睡眠及呼吸等[2]。由於電腦科技的普及，深入個人及各樣組織的種種層面，資料或是檔案的大規模、甚至是全面地數位化，如何維持資訊的私密及安全，以及檔案的不被他人所得知，自然成為了極為重要的課題。就此，檔案或是訊息的加密技術也就應運而生，讓人們能夠有效地控制可以接觸檔案內容者的範圍，使第三人無法得知其中資訊。

在過往，由於技術能力及資源的限制，大多只有國家機關基於軍事或國家安全等因素，能夠以電腦程式加密資料或是往來交換的訊息，但在電腦技術快速進步，更為普遍簡便，以及網路型態的犯罪大量發生後，企業開始大幅提高在網路上資金及訊息的交換的安全性，強化往來通訊的認證，其中包括了加密金融等資訊，避免機敏資料的外洩[3]。除此之外，加密技術也已經廣泛地應用於一般人們的生活當中。舉例來說，過去使用者在瀏覽網頁或是透過網頁寄送資訊，流程約莫會是使用者端發出瀏覽特定網頁的請求或是寄發特定資訊（如信用卡卡號、購買某項商品及地址等資料），伺服器接收到相關訊息，回傳所要求瀏覽的網頁或是回應（交易成功或是失敗等）。在使

---

[1] *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005).

[2] Garmin 網站，https://www.garmin.com.tw/products/intosports/forerunner-55-black/#specsTab （最後瀏覽日：07/28/2021）。

[3] A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 720 (1995).

用者及伺服器間，傳送及接收訊息的過程中，所使用的協定是 HTTP（超文本傳輸協定，HyperText Transfer Protocol），所有的資訊都沒有經過加密。在這過程中，有心人很輕易地就可以窺探他人間所交換的訊息。是故，技術上就發展出了加密技術或協定，讓人們可以放心地進行網際網路上的各樣活動，交換訊息，企業或是公司也因而能夠確保其內部資訊或營業上祕密事項可以安全無虞地保存或是傳送。最為人們所熟悉的，就是 HTTPS（超文本傳輸安全協定，HyperText Transfer Protocol Secure）。HTTPS 將使用者及網頁伺服器間所傳輸的訊息加密（如 SSL 或 TLC 安全協定），防止使用者的資訊被盜取，維持所交換的資訊的完整性，確保其未在過程中被修改或是讀取，提高人們使用網際網路的安全性及保護其隱私權益[4]。

不過，電腦、通訊及加密技術的進步，是把雙面刃，不只便利了一般人的需要及公司企業的營運，也使得犯罪份子可以隱密地傳遞不法活動的訊息，隱匿相關事證，逃避警察官員的查緝。在 1993 年美國世貿中心爆炸案裡，主謀 Ramzi Yousef 就加密了其筆記型電腦中的檔案，大大地增加了犯罪偵查的難度[5]。也因此，如何因應加密技術，便成了執法及法制上關鍵重要的問題[6]。從技術上來說，有幾種可能可以因應加密技術的方式[7]。其中之

---

[4] Web.dev 網站，〈在伺服器上啟用 HTTPS〉，https://developers.google.com/search/docs/advanced/security/https?hl=zh-tw （最後瀏覽日：05/31/2021）。

[5] Roberto Suro & Elizabeth Corcoran, *U.S. Law Enforcement Wants Keys to High-Tech Cover*, WASHINGTON POST (Mar. 30, 1998), https://www.washingtonpost.com/wp-srv/politics/special/encryption/stories/cr033098.htm.

[6] *See* Tom Winter, Tracy Connor & Pete Williams, *Comey: FBI Couldn't Access Hundreds of Devices Because of Encryption*, NBC NEWS (May 08, 2017, 6:17 PM), www.nbcnews.com/news/us-news/comey-fbi-couldn-t-access-hundreds-devices-because-encryption-n730646.

[7] 較常被提及的有取得金鑰、猜測金鑰、命提出金鑰、利用加密技術的漏洞、於設備使用時取得明文及於他處取得明文等方式。*See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 996-1011 (2018).每種方式都可能可以因應加密，但也都有其限制。以取得金鑰為例，其指的是，取得記錄或書寫在其他的數位檔案、文件或是物件上的密碼。一旦發現了這類的金鑰，就可以讀取檔案其中的內容。這個方式要能夠成功，取決於幾個因素。首先，金鑰必須要記錄於某個地

一是猜測密碼（guess the key）。猜測密碼指的是，透過相關的資訊，使用電腦程式或應用軟體，猜出或是試出檔案的密碼（金鑰），還原加密後的檔案，進而得知其中的內容。舉例來說，在 *United States v. Lopez* 案[8]中，警察在扣押了被告的行動電話及平板電腦後，發現其均設置有密碼保護。警察詢問被告的生日，被告也如實告知。警察成功地以被告的生日解鎖了所扣押的設備。不過，並不是所有的猜測都如此「複雜」，一份研究顯示，在四位數的密碼中，有約 15%的使用者選擇了 10 個相同的密碼，其中，最常使用的是「1234」，約佔了 4%[9]。當然，在多數的案件中，金鑰或是密碼不會這樣容易被猜測出來，而是會需要以電腦程式來計算及破解。不過，無論是以什麼樣的方式猜測密碼或是破解檔案的加密，接下來的問題是，這樣的作法是不是會侵害了相對人的隱私權益？人們是否因為加密了檔案，所以對於其中的內容享有隱私權？亦即，在加密檔案或是在電腦或個人數位裝置等設備上設定密碼後，是不是就能夠主張享有合理隱私期待？就此，如果答案是肯定的，執法機關破解檔案的加密，會是對於隱私權益的侵害，構成了刑事訴訟法（下稱「刑

方。金鑰可能是寫在嫌疑人隨身的筆記本上，也可能儲存於瀏覽器裡，讓使用者不需要反覆輸入密碼。*See, e.g.*, MANAGE PASSWORDS, GOOGLE CHROME HELP, https://support.google.com/chrome/answer/95606?co=GENIE.Platform%3DDesktop&hl=en (last visited July 22, 2019).金鑰也當然可能儲存於網路服務業者所提供的網路硬碟或電子郵件信箱中。再者，執法機關要能夠找得到且能讀取該金鑰。若是金鑰寫在筆記本或是電腦檔案裡，執法官員要能夠找得到該筆記本或檔案。另外，記載有金鑰的檔案本身也可能被加密，檢警機關必須要另外取得金鑰，才能夠予以解密。最後，從規範面來說，警察必須要以法定程序取得該金鑰。法定程序，可能是搜索票或通訊監察書。美國聯邦紐澤西地方法院在*United States v. Scarfo*案(180 F. Supp. 2d 572 (D.N.J. 2001))中便處理了以側錄按鍵輸入內容的方式取得金鑰，應適用搜索或是通訊監察的爭議。

[8] United States v. Lopez, No. 13CR2092 WQH, 2016 WL 7370030 (S.D. Cal. Dec. 20, 2016).

[9] *See* Daniel Amitay, *Most Common iPhone Passcodes*, DANIEL AMITAY BLOG (June 14, 2011, 5:30 PM), http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes.日前也有新聞傳出，一名男子在撿到提款卡後，便猜出了其密碼，並盜領帳戶內的款項。自由時報（08/12/2019），〈撿提款卡猜出密碼盜領46萬 判罰1萬關半年〉，https://news.ltn.com.tw/news/society/breakingnews/2881623（最後瀏覽日：10/30/2023）。

訴法」）上的搜索，所以原則上必須事先聲請法院核發令狀，方得為之；如果答案是否定的，警察官員則可逕自為之，無須遵行令狀程序[10]。後續的影響是，如果加密的破解屬於搜索，未經法官授權，破解檔案或是裝置上所設定的密碼，就會有證據排除規定的適用（刑訴法第 158 條之 4）。

實務上顯然也意識到了解密在個案執法上的需要，以及其中可能涉及到的法律爭議。在法務部日前所提出的科技偵查法草案[11]中規定：「檢察官、檢察事務官、司法警察官或司法警察對於行動裝置、儲存設備、電腦或其他相類之設備或其內之電磁紀錄實施搜索或扣押時，得以科技設備或技術為下列處置，對於已經合法扣押或經自願性交付之前述設備或其內之電磁紀錄，亦同：……二、破解相關帳號、密碼或保護措施。」（第 21 條第 1 項）亦即，執法官員因合法搜索扣押或經自願性同意交付，取得加密後檔案後，可以逕自破解檔案上的加密，無須適用令狀原則，不需要再另外向法院聲請令狀。條文的文字及結構很簡單，但也不免因而有著解釋及適用上的疑惑。

依前述草案條文，執法機關經合法搜索扣押或相對人的交付而取得加密後檔案，可以逕自破解，但如果透過其他的方式取得了加密檔案，是不是仍然能夠破解其上的加密？舉例來說，張三將想要購買毒品的文字檔案加密後，上傳到公開網站上，警察下載後，能不能直接予以破解？張三可不可以主張，因為檔案已經加密，所以享有合理隱私期待？警察是否必須要事先向法院聲請令狀後，才能夠破解張三加密後的訊息？於此有無適用令狀程序的原因為何？就草案條文的文字來說，似乎無法適用該規定。再者，針對加密檔案的破解，草案的立法理由僅非常簡略地提到：「至於已經合法扣押（例如合法搜索後之扣押、依據法院核發之扣押裁定而扣押）或經犯罪嫌疑人或第三人自願性交付之行動裝置、儲存設備、電腦或其他相類似之資訊設備或其內之電磁紀錄，本係合法取得之犯罪證據，自應允許偵查機關進行必要之

[10] 關於搜索不同基準的判斷及其與隱私侵害間的關係，可以參照王兆鵬（2004），〈重新定義高科技時代下的搜索〉，氏著，《新刑訴．新思維》，頁83-91，元照；李榮耕（2015），〈科技定位監控與犯罪偵查：兼論美國近年GPS追蹤法制及實務之發展〉，《臺大法學論叢》，44卷3期，頁880-889。

[11] 科技偵查法草案在2020年9月經法務部預告制定，但至今尚未經行政院會通過。

處置，亦加以明定之。」可以說是根本沒有解釋偵查機關為什麼可以破解設備或是檔案上的帳號、密碼或其他保護措施，只言明「自應允許」。其中的原因為何，實有進一步探究討論的必要。

綜上，這一篇論文所聚焦討論的，是人們對於加密後的檔案是否享有合理隱私期待，以及破解加密檔案或設備上的密碼有沒有令狀原則的適用。就此，美國在實務上已經有過許多爭議及具體個案。學者也累積了相當豐碩的研究成果。這些都是我們在分析探討相關課題時，可以參考借鏡的。以下擬先簡要地說明檔案或數位型態資料加密的概念（貳），再分別從幾個面向進行深入的分析。首先，當某項訊息或是事物有很高的機會不會被知悉時，是不是就能主張隱私權？答案若為肯定，加密技術的使用就可能受有隱私權的保護（參）。美國法院在部分案件中判定，在一個人電腦中設定密碼時，就不能以其他共用人的同意進行搜索。這是否意味著，密碼的設定或是檔案的加密就能夠主張合理隱私期待（肆）？上鎖的封閉容器是討論加密技術時，常常被提起的類比，也是支持人們就加密檔案享有隱私權的重要論據。這樣的主張是否妥適？加密檔案是否能如此比擬？（伍）。最後，這一篇論文會從政策上的角度切入，說明在此一議題，應採的立場及作法（陸），並提出整體分析探究後的結論（柒）。必須要說明的是，破解技術無法滿足執法上所有檔案或是訊息加密的需要，學理研究、實務運作及政策上，還是必須要進一步探究其他執法的方式，如命輸入密碼或跨國（境）合作等。為聚焦討論的方向，只能暫且按下，待另日為文研究。

貳、加密的概念

加密，泛指將一般人可以閱讀的文字（plaintext）按照一定規則，轉譯為無法理解的密文（ciphertext）的技術或方法[12]。除了傳統的文書外，數位型態的資料也可以透過加密技術，讓第三人無從了解其中的內容，使文件的

[12] 轉譯必須要依照一定規則，如此才能夠將密文還原為明文。

讀取權限可以控制在特定範圍的人[13]。數位型態資料的加密，一般是透過加密軟體（如 FinalCrypt[14]或是 VeryCrypt[15]）將檔案編譯或轉編為無法閱讀、沒有意義的密文。有權讀取之人通常會持有金鑰（encryption key, key，或稱密鑰），可以將密文還原為明文。加密，以往僅見於很小範圍內事務，但如今由於通訊及數位技術的普遍，已經廣泛地應用於人們生活的各個層面之中。

一、由來及過往

加密有著極為悠久的歷史，並不是近來因著電腦或通訊科技進步才產生的技術。過去因著軍事或戰爭的需要，人們就已經使用了各式各樣的加密方式傳送訊息，使敵軍或是無關的第三人，即使取得了，也全然無法了解其內容。戰國時代的兵書「六韜」中，便已經有「陰符」及「陰書」的祕密通訊方式[16]。北宋的武經總要中，則是以軍事用語密碼本、律詩及數字，溝通前後方的軍事消息[17]。明代的抗倭名將戚繼光發明了「反切碼」，被譽為最難破解的密碼，是以兩首詩作為密碼本，傳送訊息的兩方只傳遞數字，對應到詩中不同字的聲母及韻母，組合出所要傳達的訊息。在西方世界，加密同樣

---

[13] 除此之外，也有學者認為，由於加密技術所保護的客體，包括了人們之間的意思、想法、意念或是溝通，這些受保護的客體同時也是人們的「言論（speech）」，所以加密技術不只可能保護了人們的隱私，也保護了人們在憲法上所受有保護的言論自由。*See* John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution*, 2 VA. J.L. & TECH. 1, 2 (1997); Norman Andrew Crain, *Bernstein, Karn, and Junger: Constitutional Challenges to Cryptographic Regulations*, 50 ALA. L. REV. 869, 870 (1999).

[14] FINALCRYPT, http://www.finalcrypt.org/ (last visited Oct. 30, 2023).

[15] VERACRYPT, https://www.veracrypt.fr/en/Home.html (last visited Oct. 30, 2023).

[16] 中國哲學書電子化計劃，《六韜・龍韜・陰符及陰書》，https://ctext.org/liu-tao/zh（最後瀏覽日：10/30/2023）。

[17] 中國哲學書電子化計劃，《武經總要・武經總要前集・字驗》，https://ctext.org/wiki.pl?if=gb&res=817018（最後瀏覽日：10/30/2023）。

有著悠久的歷史。約西元前一世紀時，凱撒（Julius Caesar）就已經利用密文傳遞訊息給軍隊，指揮將領們在戰事中的行止[18]。

在二次世界大戰時，訊息的加密扮演了更為重要的地位。當時德軍的潛艇讓盟軍在大西洋吃足了苦頭，但在破解德國軍隊所使用的 Enigma 密碼機後，情勢逆轉，盟軍得以掌握德軍潛艇的位置及重要的軍事佈署與戰略，取得戰略上的優勢[19]。在同一個時期，美國成功地破解了日本海軍所使用的密碼，在中途島的戰役上取得了決定性的勝利，甚至是改變了整個太平洋戰爭的局面[20]。除了軍事用途之外，很早就已經有犯罪份子加密其往來的訊息，以及警察官員設法破解的情事。在 19 世紀，電報還是主要的通訊方式之一時，訊息都是透過電報員以摩斯電碼（Morse code）發送，由於電報員是將收到的摩斯電碼還原為一般人可以理解的文字，所以會知道其內容。當電報員發現訊息涉及犯罪時，會向偵查機關告發。犯罪之人為了避免犯罪計畫被執法官員發現，通常會加密其訊息[21]。警察也因而必須要破解加密後的訊息，以偵查犯罪，並在審判中得以提出，作為證據[22]。

從前述中外的歷史可以知道，訊息的加密及破解並不是一個前所未見的嶄新事物，而是有著悠久的過往的技術。然而，在電腦科技的加入後，有了不同於以往的面貌，也產生了許多新興的議題。

二、訊息的加密及解密

訊息的加密及解密，涉及到密碼學（cryptography）。密碼學指的是一種使用密碼、密文或是其他方式處理某個訊息，使得只有特定人能夠知悉或接

---

[18] Jason Kerben, *The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Genie*, 5 COMMLAW CONSPECTUS 125, 125 (1997).

[19] Thinh Nguyen, *Cryptography, Export Controls, and the First Amendment in Bernstein v. United States Department of State*, 10 HARV. J.L. & TECH. 667, 668 (1997).

[20] *Id.* at 668.

[21] *See* SIMON SINGH, THE CODE BOOK 60-79 (1999).

[22] *See, e.g.*, Allis v. United States, 155 U.S. 117, 120 (1894); Buckley v. United States, 33 F.2d 713, 716 (6th Cir. 1929).

觸到其中內容的知識或是學門[23]。密碼學涉及到兩個程序，一是加密（encryption），二是解密（decryption）。加密指的是，透過金鑰（或稱暗碼）（cipher），或是密碼（code），將可以理解或是一般人可以閱讀的訊息或文字（一般稱為「明文（plaintext）」）轉換為無法了解其意義的暗文（ciphertext）[24]。加密所使用的金鑰，可以再將暗文還原為明文，而知悉其內容[25]。舉例來說，以 01 代表 a，02 代表 b，03 代表 c，依此類推。0919121206182107 就是 iselldrug。如果不知道字母及數字間的互換關聯，0919121206182107 就只是一連串沒有意義的數字，但若是知道前述的字母及數字間替換規則，就可以知道其中真正的意思。另外，在這一個例子裡，iselldrug 就是明文，0919121206182107 則是暗文。

數位型態的訊息的加密，也類似於此。略有不同的是，在數位訊息的加密中，使用到了演算法，金鑰則是所使用的演算法中的一個變數。加密後的數位訊息的安全性，決定於所使用金鑰的複雜程度（也就是金鑰的長度）[26]，而不是所使用的演算法。亦即，真正用來將明文加密或是將密文還原為明文的是金鑰，而不是演算法[27]。是故，即使得知密文所使用的演算法，沒有金鑰，還是沒有辦法得知訊息的內容。事實上，不一樣的加密程式或軟體，可能使用了相同的演算法，但每一個加密後的檔案，幾乎都會有著不同金鑰[28]。

三、不同的數位資料加密模式

現今的加密技術已經遠比過去複雜許多，應用層面也更加地廣泛。加密，可以使用於單一裝置（如電腦、平板電腦或是智慧型電話）內的資訊，也可

---

[23] Froomkin, *supra* note 3, at 713.

[24] Laura M. Pilkington, *First and Fifth Amendment Challenges to Export Controls on Encryption: Bernstein and Karn*, 37 SANTA CLARA L. REV. 159, 168 (1996).

[25] Kerben, *supra* note 18, at 125.

[26] Pilkington, *supra* note 24, at 168. 這部分，可以參照貳、四的說明及討論。

[27] Crain, *supra* note 13, at 872.

[28] Microsoft Ignite，〈Bitlocker 概觀〉，https://docs.microsoft.com/zh-tw/windows/security/information-protection/bitlocker/bitlocker-overview（最後瀏覽日：09/30/2021）。

以是用在兩個設備間所交換的訊息（如智慧型電話間的語音通話，電子郵件或是 Line、WhatsApp 等即時通訊）。例如，在電腦上面，可以用加密軟體直接加密特定的資料夾或是檔案[29]。至於智慧型行動電話，多數會預設地將儲存在其中的內容加密，必須要輸入所設定的數字或圖形密碼、按壓指紋或透過臉部辨識，才能夠解鎖，讀取其中的資訊。在 2015 年後，使用 Android 6.0 或更新版本的作業系統的行動電話，便是以前述的方式加密電話內的資料，Apple 的 iPhone 設備也是如此。檔案加密（也就是設備上鎖）後，如果沒有輸入正確的密碼，就無法讀取儲存在其中的資料。就系統的運作程序來說，使用者所輸入的密碼或是生理特徵，是用來加（解）密金鑰，因此，使用者所輸入的密碼，是將加密後的金鑰解開，金鑰再將加密後的檔案解密[30]。也就是說，這一個模式有著兩個階段。使用者輸入的密碼（或是生理特徵）解密了金鑰，解密後的金鑰再解密設備中的加密檔案。

在前一種加密模式中，使用者必須要以輸入密碼、畫出正確的圖形、按壓指紋或是面向鏡頭等方式，以進行檔案的解密。不過，加（解）密的整個程序，也可以是在使用者完全沒有意識的情形下進行。典型的例子，是訊息的寄送及接收。人們透過行動電話、WhatsApp 或是 Line 等軟體進行通話時，電話、設備或是程式會將訊息加密，接收者必須要有金鑰，才能將訊息解密[31]。許多網站也都使用加密的技術，如 SSL 等協定，將寄送給收件人或是伺服器的訊息加密。在這一種通訊加密的協定中，常使用到「非對稱式加密（asymmetric encryption）」。在這個協定的通訊過程中，會公開一個公鑰（public key），讓傳送訊息者用來加密訊息，接收者則以私鑰（private key）來解密。亦即，公鑰是用來加密，私鑰則是用以解密。因為加密及解密使用

---

[29] *E.g.*, Yolanda Shelton, *How to Encrypt & Password Protect your Files with 7-Zip*, 7-ZIP HELP (Oct. 18, 2023), https://7ziphelp.com/password-protect-on-7zip.

[30] *See* Kerr & Schneier, *supra* note 7, at 994-95.

[31] *See How to set Letter Sealing*, LINE HELP CENTER, https://help.line.me/line/?contentId=50001520 (last visited Oct. 30, 2023); *About End-to-End Encryption*, WHATSAPP HELP CENTER, https://faq.whatsapp.com/en/general/28030015(last visited Oct. 30, 2023).

的是不同的金鑰，所以稱之為「非對稱式加密」。除了電話或是即時通訊外，網頁的瀏覽或是電子郵件，也常使用這種加密方式。在前述的加密模式中，金鑰是由設備內的程式自動產生，並進行交換，參與訊息交換者不需要自行輸入金鑰或是密碼[32]。也就是說，使用者不會察覺到整個加（解）密的過程。

四、加密的破解

加密的目的，是為了讓持有金鑰以外的人無法，或是難以在短時間內接觸檔案或是訊息的內容。不過，從技術層面來說，還是有各樣破解加密的手法[33]。其中常見者之一，便是窮舉每一個可能的密碼，測試出所使用的金鑰。這個破解方式，多稱之為暴力攻擊或是蠻力破解（the brute-force attack）。由於這一個破解方式是以各種數字、字母或是符號的組合，嘗試出正確的金鑰，也因此，加密的安全性，就會是取決於金鑰的可能組合數量。必須要輸入的字母、數字或特殊符號越多（金鑰的長度越長），金鑰的可能性就越多，就更不容易被猜測出來。金鑰的長度越長，加密後的訊息（密文）也就越是安全[34]。所使用的設備及其運算能力，會影響到破解所需要的時間，不過，最重要的關鍵還是在金鑰。

詳細地來說，目前常見的加密標準是 AES（Advanced Encryption Standard），其金鑰（密碼）長度可以是 56、64、128、168、192 或 256 位元（bit）。金鑰有不同的長度，一把 128-bit 的金鑰可以用二進位的方式表示為“01110000000000000110000100000000001110011000000000011100110000000000111011100000000011011110000000001110010000000000011001000 000000”[35]。256-bit 的金鑰則是有兩倍的長度。現在的加密

---

[32] *Email encryption in transit*, GMAIL HELP, https://support.google.com/mail/answer/6330403?hl=en (last visited Oct. 1, 2021).

[33] *See* Kerr & Schneier, *supra* note 7, at 996-1011.

[34] Pilkington, *supra* note 24, at 168.

[35] 金鑰通常不是以二進位的方式表示，而會以十六進位的編碼（hexadecimal notation）呈現。前述的金鑰，就會是：“70006100730073007700 6F0072006400”，轉換為 ASCII/Unicode，則是“password”這個英文單字。

程式，多使用 128-bit 或是 256-bit 長度的金鑰。使用大型情報機構的電腦，多可以在短時間內破解 64-bit 長度的密碼[36]，但要破解 AES-128 的加密，就算是使用高速運算的電腦，也會需要約數十億到百億年的時間[37]。即使理論或是技術上可以算得（試）出金鑰來，但是無論一個訊息或是資訊多麼重要，在那樣長時間後，都已經不再有任何的機密或是意義可言。此外，個人的數位裝置也有著各樣防止加密或密碼被破解的安全功能。例如，在 5 次錯誤輸入密碼後，必須要再等 1 分鐘，才能夠再次輸入，之後等待的時間，會隨著錯誤的輸入，越來越長。第 10 次輸入密碼仍然錯誤時，設備就會自動刪除掉儲存在其中所有資料，且無法回復[38]。類似的功能都會使得猜測金鑰的成功率越來越低。由此可知，加密可以說是保護資料安全相當有效的方式。

參、密碼的難以破解及可能性理論

以目前的電腦技術來說，加密是避免數位資料被他人知悉其內容的有效辦法。若是沒有金鑰，必須要耗費極為可觀的資源及時間，才可能破解一般常用的檔案加密技術。接下來值得探究的問題是，在這種情形下，是否可以認為人們對於加密後的檔案享有合理隱私期待，因而會有令狀原則的適用？就此，持肯定立場者所持的重要論點之一是，以現在的系統運算能力來說，即使是以超級電腦，也要耗費數千萬，甚至是億年以上的時間，才能夠將加

---

[36] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 151-54 (2nd ed. 2015). *See also* Crain, *supra* note 13, at 872.

[37] *See* Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 503 (1996); Elizabeth Lauzon, *The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues*, 48 SYRACUSE L. REV. 1307, 1318-19 (1998).

[38] *See* Jack Date, *The FBI and the iPhone: How Apple's Security Features Have Locked Investigators Out*, ABC NEWS (Feb. 17, 2016, 8:20 AM), http://abcnews.go.com/US/fbi-iphone-apples-security-features-locked-investigators/story?id=36995221 (last visited Oct. 30, 2023).

密後的檔案還原回人們可以閱讀理解的型態[39]。是故，以現在的主流技術來說，只要檔案加密了，除非持有金鑰，否則檔案內容就幾乎不可能為他人所知悉，所以檔案持有人可以主張隱私的合理期待。這樣的主張，是以可能性理論來理解合理隱私期待的意涵。

一、可能性理論意涵及概念

美國學理上多認，可能性理論，是以一個一般謹慎合理的人是否會認為某項事物或是訊息處於私密、隱匿，不被他人接觸或知悉的狀態，來決定有無美國聯邦憲法第四增修條文（下稱聯邦憲法第四增修條文）的適用[40]。從另一個角度上來說，是以某事物被他人知悉的可能性高低，來判斷一個人是不是能主張合理隱私期待。如果某事物被他人得知或是接觸的可能性非常地低，一般人都會認為該事物處於祕密狀態，就可以主張隱私權。反之，則否。

美國聯邦最高法院（下稱聯邦最高法院）曾以特定事物保持祕密的可能性來決定被告是否能主張聯邦憲法第四增修條文的權利。舉例來說，在 *California v. Ciraolo* 案（下稱 *Ciraolo* 案）[41]，被告為了避免被往來的路人發現所種植的大麻，在後院周圍設置了約 3 公尺高的圍牆。為了偵查犯罪，警察搭乘飛機，從約 300 公尺的高度飛越被告房屋的上方，並拍攝到後院中的大麻，這些照片成為了認定被告犯罪的證據之一[42]。*Ciraolo* 案經下級法院判決後，上訴至聯邦最高法院。聯邦最高法院判定，警察的行為不構成搜索，因為在民用航空器相當普遍的時代，期待自己所種植的大麻不被飛越上空飛

---

[39] 舉例來說，量子電腦的問世，甚至能夠讓加密後的檔案無法被破解。Roland Pease, *'Unbreakable' Encryption Unveiled*, BBC NEWS, (Oct. 9, 2008), http://news.bbc.co.uk/1/hi/sci/tech/7661311.stm (last visited Sep. 27, 2021).

[40] *See, e.g.*, WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(d) (4th ed. 2004); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*", 42 DUKE L.J. 727, 732-33 (1993).

[41] California v. Ciraolo, 476 U.S. 207 (1986).

[42] *Id*. at 209.

機所觀看到，是不合理的[43]。針對多數意見書，Powell 大法官表示反對，其認為由於被告後院被察看的可能性非常的低，所以保有隱私的期待[44]。在這一個案件中，雖然聯邦最高法院大法官們有著不同的立場，但是從說理的文字可以知道，多數及不同意見書都是從後院被他人觀察的可能性高低來決定被告是否能主張聯邦憲法第四增修條文的權利[45]。

在 *Bond v. United States* 案（下稱 *Bond* 案）[46]中，也可以看到聯邦最高法院運用了類似的判準。於這一個案件中，邊境警察在巴士上抓捏了被告放在頭頂行李架上的袋子，感覺其中有磚狀的物品。在經被告同意後，警察打開了該袋子，發現其中裝有甲基安非他命[47]。聯邦最高法院認為，警察的行為已經構成了搜索，因為一般巴士乘客不會預料到，在他將袋子放在頭頂行李架後，他人會為了知道其中承裝了什麼樣的物品而抓捏或擠壓[48]。亦即，由於在一般的情形，他人去揉捏被告的袋子，以探知其裝了什麼東西的可能性很低，所以被告在這一個案件中享有聯邦憲法第四增修條文所保障的隱私權。

二、不盡合理的地方

乍看之下，從是否處於被他人知悉的可能性來理解合理隱私期待，符合於一般人對隱私的想法，似乎是一個可採的解釋方向，因為祕密或是私密的直觀意涵，就是不會或是難以被他人知道、不公開，或只有相對小範圍的人

---

[43] *Id*. at 215.

[44] *Id.* at 223. (Powell, J., dissenting) ("[T]he actual risk to privacy from commercial or pleasure aircraft is virtually nonexistent. Travelers on commercial flights, as well as private planes used for business or personal reasons, normally obtain at most a fleeting, anonymous, and nondiscriminating glimpse of the landscape and buildings over which they pass.")

[45] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 510 (2007)

[46] Bond v. United States, 529 U.S. 334 (2000).

[47] *Id*. at 336-37.

[48] *Id*. at 337-39. *See* Kerr, *supra* note 45, at 509.

才知道的事項，因此就不（太）可能被他人所得知的事物，自然可以享有合理隱私期待。不過，進一步的分析後可以知道，這樣的主張可能不盡妥適。再者，回顧過去美國實務上的判決可以知道，聯邦最高法院並不都是以可能性理論判定個人得否主張合理隱私期待。

（一）可能不被知道不當然等於隱私

首先，很可能不被他人所知悉的事物或活動，不當然就屬於隱私，或是更精準地來說，不當然就應該受有隱私權的保護。這是因為，某件事物只有少數人得知，涉及到許多原因，諸如地點、人數、時間及（如果是對話）交談的方式等等，並不是只要是極不可能被他人發現的事項，就都應受有隱私權的保護。舉例來說，兩個人在深夜 2 點，在人煙罕至的荒山野嶺交易毒品，碰巧被巡邏的森林警察發現。依據前述被他人知悉的可能性的標準，就時間及地點來說，由於該交易幾乎不會被任何人所察知，所以該二人可以就其交易主張合理隱私期待，警察的行為構成了搜索，也因此必須要事先聲請令狀，才能夠在深夜的山林中巡邏。這樣的結論，恐怕難以為絕大多數人所能接受[49]。

（二）不被他人知悉的可能性要多高（低）？

到底多高的可能性才能夠主張合理隱私期待？多低就應認已經不能認為仍保持不為人知的狀態？這些問題，恐怕都很難有一個清楚的標準，在個案中很容易會是當事人爭執之所在，法院及雙方因而必須要耗費相當龐大的時間及人力，處理此一爭議，決定隱密可能性是高或低。另外，由於特定事物、資訊或是處所被他人探知的可能性不容易有明確的判準，所以很難有一個可供執法機關及後續個案依循的標準。

以電腦檔案的加密來說，需要回答的問題就會是，一個人要使用了多複雜的技術，才能夠合理相信其檔案或是文件不會被破解？128-bit？192-bit？或是 256-bit 的加密？再者，加密的破解涉及到運算能力，如果一般家用或

[49] *See* LAFAVE, *supra* note 40, at § 2.1(d).

是個人用的電腦需要數千萬或上億年才能破解，但是超級或量子電腦在很短的時間內就能夠算出金鑰來，應認其有或是沒有合理的隱私期待？亦即，能不能主張合理隱私期待，是不是要隨著電腦運算能力的增加，而有所改變？再者，與傳統類型的個案相比較，也可以知道這一個說法並不合理。聯邦最高法院從來沒有因為建築物或是容器的材質，而給予不同的隱私保護。無論是破舊不堪的茅草屋或是金碧輝煌的華廈，都能夠主張合理隱私期待。同樣地，紙袋或是上鎖的公事包也都受有隱私權的保護[50]。只要容器或是空間能夠使人無法探知其是否承裝有物品，裝載了什麼樣的物件等內部狀態，在物理上使內外有所區隔，無論容器的材質為何、是否上鎖，或是否很容易就可以破壞或撬開所使用的鎖，都不影響其所得主張的隱私權。從保護措施的強度的角度來說，加密的檔案是否也在隱私權的保護範圍之內，也應該可以得到相同的結論[51]。亦即，密碼是不是容易被破解，不應該左右檔案持（所）有人是否享有隱私權的保護。也因此，不能僅因為所使用的加密技術難以破解，就認為加密後的檔案或裝置當然可以主張存在有合理隱私期待。

（三）保護效果有限

依可能性理論，合理隱私期待指的是有保持特定事物或是訊息不為他人所知的高度可能，但如此一來，隱私權就只能在很小的範圍內，保護人們特定資訊或處所不被他人恣意探知的需要。亦即，如果只有事實上可以保持祕密，有很大的機會能夠不為他人所知悉的事項或是訊息，才能主張合理隱私期待，那麼聯邦憲法第四增修條文最後就只會保障現實上，已經難以被他人知悉的事項。執法機關很輕易就可能知道的資訊，無論其內容為何，完全不受到隱私權的保護[52]。隱私權、合理隱私期待的概念，以及令狀程序，到頭來就只是錦上添花而已，很難說能有什麼實際上保護人民的效果。

---

[50] United States v. Ross, 456 U.S. 798, 822 (1982).

[51] Kerr, *supra* note 45, at 524.

[52] Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create A "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 512 (2001).

（四）有採權利取向模式者

雖然在前述 *Ciraolo* 案及 *Bond* 案中，聯邦最高法院是以可能性理論來判斷一個人是否能主張合理隱私期待，但在其他案件中，其似乎採取了不同的審查基準。有學者在歸納整理後便認為，在部分案件中，聯邦最高法院是以權利基礎（或「權利取向」或是「權利本位」）的模式（rights-based approach）來決定是不是能主張合理隱私期待。雖然權利基礎模式也有其說理上不盡周延的地方，但從這些案件可以知道，在個案中不當然就能夠援引可能性理論，支持人們就加密後的檔案可以主張隱私權。

1. 概念及內涵

權利基礎模式指的是，一個人是否能主張合理隱私期待，決定於其是不是能夠依據聯邦憲法第四增修條文以外的規範，主張執法機關的行為違法。亦即，如果警察官員以違法（違反聯邦憲法第四增修條文以外的法規）的方式取得了關於特定人的資訊或是侵害其財產，就違反了其合理的隱私期待，警察的行為便屬於搜索，原則上，必須要事先取得令狀，方得為之。相反地，如果警察的行為合於既有的法律，相對人便不能主張合理隱私期待受有侵害，警察的資訊取得或是進入特定空間的行為就不是搜索，無須遵循令狀原則的要求[53]。

在聯邦最高法院的許多涉及搜索的判決中，都可以看到其運用了權利基礎模式的判斷基準。舉例來說，在 *Rakas v. Illinois* 案（下稱 *Rakas* 案）[54]中，被告參與了一起強盜案件，在案發後，搭乘共犯駕駛的汽車逃逸。警察攔下汽車後，從助手席底下搜出一把槍枝，並在手套箱中發現一盒子彈。主筆的 Rehnquist 大法官表示，警察對於汽車內部的檢視及搜查並未侵害被告的合理隱私期待，因為汽車並不是被告所有。多數意見書解釋道，財產權的主要功能是排除他人對於財產的侵害，絕大多數對於特定物品享有所有權、持有

---

[53] *See* Kerr, *supra* note 45, at 516.

[54] Rakas v. Illinois, 439 U.S. 128 (1978).

或是具其他財產權益者，同時可以就該物主張合理隱私期待[55]。在這一個案件中，警察所攔停及搜索的汽車是共犯所有，被告只是乘客，對於汽車或是汽車中的物品，既沒有財產權，也沒有持有的利益，所以被告不能主張警察的行為違反了其合理隱私期待[56]。另一個典型的判決是 *Florida v. Riley* 案（下稱 *Riley* 案）[57]。在這一個案件裡，警察搭乘直昇機從被告房屋約 120 公尺的上空飛過，發現了被告在其溫室內種植大麻[58]。聯邦最高法院的多數意見書判定，執法官員的行為沒有違反聯邦憲法第四增修條文，因為航空法規容許直昇機以 120 公尺的高度飛行，任何人都能夠合法地以該高度從被告房屋上飛過。警察所作的，就是一個合法行為，不是什麼法律所不容許的事情[59]。是故，被告不能主張警察侵害了其合理隱私期待，警察的行為不構成搜索，並沒有違反聯邦憲法第四增修條文的誡命。

在涉及使用傳統追蹤器的案件中，也是以類似的說理判定警察的行為合法。在 *United States v. Knotts* 案（下稱 *Knotts* 案）裡，聯邦最高法院解釋道，警察官員藉由追蹤器（beeper）掌握了被告在公開場合中的活動或是公共道路上的行蹤，不違反聯邦憲法第四增修條文。這是因為，一個人對於自己在公共道路的行跡或是開放領域（open field）上的活動，並不能主張隱私權。警察原本就可以（有權）用肉眼觀察或是監控犯罪嫌疑人，追蹤器的使用並沒有使其獲得更多的資訊。聯邦憲法第四增修條文並不禁止警察使用科技設備強化自己身體原有的感官能力[60]。是故，在這一個案件中，聯邦最高法院最後判定，追蹤器的使用並不構成搜索，被告不能主張隱私權受有侵害。

2. 與可能性理論間的不同

---

[55] *Id.* at 143 n.12.

[56] *Id.* at 129.

[57] Florida v. Riley, 488 U.S. 445 (1989).

[58] *Id.* at 448.

[59] *Id.* at 451.

[60] United States v. Knotts, 460 U.S. 276, 282 (1983).

在前述的 *Rakas* 案、*Riley* 案及 *Knotts* 案裡，無論是汽車座位底下的槍枝、汽車手套箱裡的子彈、溫室內的植物或是公開場所中的行跡，被他人發現的可能性並不高，甚至可以說是相當的低，當事人在主觀上也都知道且希望可以保持其物品不被知悉。如果是依可能性理論，前述案件中的被告應該都能夠主張隱私權利，但是聯邦最高法院最終還是判定，在這些案件中警察的行為並不構成搜索。也就是說，聯邦最高法院在這些案件中認為，一個人的隱私期待是否合理，不是取決於某一個事項不為他人知悉的機率大小，而是依其能否或有無權利採取一定方式，阻止或拒絕政府的行為[61]。從這一些判決可以知道，可能性理論並無法用以解釋或說明涉及合理隱私期待的（所有）案件。

3. 權利基礎模式及加密程式的使用

在涉及密文或是密碼的案件中，依前述的權利基礎模式，會認為一個人並不能僅因為檔案加密，就能夠主張合理隱私期待。當偵查機關合法取得密文時，密文的持（所）有人並沒有任何的權利可以反對或是阻止政府檢視密文、分析其中的規律、試圖破解，或是更進一步地將密文還原為明文[62]。同樣地，如果警察官員合法地取得了加密後的檔案（如以令狀搜索扣押電腦，或是在公開討論區中下載），個人可能確信其所使用的程式極難被破解，但由於其沒有其他法律上的權利可以拒絕偵查機關，利用電腦及相關程式破解檔案上的加密，讀取其中的內容，所以該個人不能就加密後的檔案主張合理隱私期待[63]。這就像是一個技巧高超的神偷認為自己絕對不會失風，或是網路駭客覺得自己入侵電腦的過程天衣無縫，不會被發現一樣，雖然實際上東窗事發的機率很低，但神偷或是駭客沒有任何的權利反對警察的偵查行為，所以其主觀上的想法並不是聯邦憲法第四增修條文所保護的「『合理』隱私期待」（但是若依可能性理論，結論很可能就會有所不同）。也因此，只要執法機關合法地取得加密檔案，其解密就沒有聯邦憲法第四增修條文的適

---

[61] Kerr, *supra* note 52, at 511.

[62] Kerr, *supra* note 52, at 517.

[63] Kerr, *supra* note 52, at 518-19.

用，執法機關不需要經過法院的授權或是同意，就得以電腦程式破譯該加密檔案或是文件[64]。

相對地，依可能性理論，個人似乎能夠就加密後的檔案主張合理隱私期待。然而，從過往聯邦最高法院的判決可以知道，就合理隱私期待的內涵，聯邦最高法院有著不同的判準，在個案中就曾運用權利基礎模式。是故，在個案中並不當然就可以依可能性理論，主張人們只要使用了加密技術，就可以對加密檔案主張合理隱私期待。

肆、加密檔案及他人的同意

在檔案加密及解密的討論中，第三人同意是經常被提起的議題，也是經常用來支持人們就加密後的檔案享有合理隱私期待的案件類型。詳言之，聯邦最高法院認為，一個人與他人共用空間或是電腦，但設置有自己的帳號及密碼時，可以主張合理隱私期待，所以即使獲得了共同使用者的同意，還是要事先取得法官所核發的令狀，才能夠就加密的硬碟或是檔案進行解密。乍看之下，似乎會得到一個結論，也就是當人們在電腦上設有密碼或是將檔案加密後，能夠享有隱私權，執法機關要破解密碼時，會有令狀原則的適用。不過，細究判決的理由及說理可以知道，在這一些案件中，被告之所以可以

---

[64] 必須要強調的是，權利基礎模式確實可以解釋許多聯邦最高法院的判決，但也不無可以反思的地方。在許多個案中，的確都看得到聯邦最高法院以權利基礎模式詮釋合理隱私期待的內涵。以這一個模式作為判斷基準，有其判斷及審查上明確，結果具有高度可預測性等優點。不過，此一模式是否為合適的方法，或有進一步討論的空間。詳細地來說，依權利取向模式，能不能享有隱私權的保障，取決於是否享有隱私權以外的其他權利（如財產權）。如果一個人在具體情狀中可以主張隱私權以外的權利，就有合理（法）的隱私期待（reasonable expectation of privacy or legitimate expectation of privacy） Rakas v. Illinois, 439 U.S. 128, 142 (1978) ；若無，就沒有聯邦憲法第四增修條文的適用。也就是說，被告或犯罪嫌疑人基於其他的規範，可以主張執法機關的行為違法者，就享有隱私權益。只是，如此一來，個人原本就可以向執法機關主張隱私權以外的權利，另外再承認其享有隱私權保護的實益何在？又或是，隱私權與其他的權利有什麼具體的區分？

主張隱私權益，主要的原因是，第三人同意及同意的範圍。亦即，若是一個人在電腦上設置了密碼，沒有與其他人共用自己的檔案，就沒有授予其他使用者可以同意他人檢視自己檔案的權限，也就沒有承擔了共用電腦之人向他人揭露自己電腦內資料的風險，並不是僅因為在電腦上設置了密碼，所以就當然享有隱私權益。雖然這一類案件的關鍵在第三人的同意，但由於其涉及了檔案的加密，在美國司法實務中也常是個案中的爭點，故以下分析討論之。

一、同住者同意搜索本人的電腦

United States v. Andrus 案（下稱 *Andrus* 案）[65]的事實約為，被告 Andrus 涉嫌持有猥褻幼童圖片[66]。兩位警察官員前往被告的住處敲門，電腦鑑識專家在外待命。被告不在家，應門的是被告的父親。被告的父親告訴警察，被告使用其中一個房間，並未支付租金。除此之外，警察觀察到被告房間的門是敞開的[67]。被告的父親簽署了書面，同意警察進行搜索，並帶警察進到被告的房間，且告知被告電腦的所在。電腦鑑識專家隨即進到屋內，將其設備連接上被告的電腦，搜尋其中的檔案[68]。被告的電腦設有帳號及密碼，但鑑識人員使用了特別的程式，還是可以讀取其中的檔案，因而發現電腦中存放有猥褻的幼童照片[69]。

偵查終結後，被告 Andrus 因為持有幼童猥褻圖片而被起訴。審判中，被告主張警察在其電腦中所找到的圖片沒有證據能力，應予排除。其中的理由包括了，被告的父親沒有同意警察搜索被告電腦的實際權限或表見權限[70]。聯邦地方法院及巡迴法院都判定，被告的父親對於被告的電腦有表見權

---

65 United States v. Andrus, 483 F.3d 711 (10th Cir. 2007).

66 *Id*. at 713.

67 *Id*.

68 *Id*.

69 *Id*. at 713-14.

70 *Id*. at 715. 關於表見權限，中文文獻，可以參考王兆鵬（2000），《搜索扣押與刑事被告的憲法權利》，頁153-156，自刊；以及李榮耕（2008），〈Yes, I do!：同意搜索與第三人同意搜索〉，《月旦法學雜誌》，157期，頁117-119。

限，所以警察對於電腦內檔案的搜尋查看合於同意搜索的要求，不違反聯邦憲法第四增修條文的要求[71]。

巡迴法院說明道，一個人的電腦常常存放有不願意為他人所知的資訊，所以對多數人來說，電腦是最為私密的空間[72]。是故，電腦應該等同於行李箱、手提箱或是類似的物品，享有高度的隱私保護[73]。法院肯認了被告對於其電腦享有合理隱私期待，但最後仍判定，警察所為的是合理（不違憲）的搜索。這是因為，綜合當時所有的情狀，警察可以合理地相信被告的父親有權使用該電腦，所以有權同意警察搜索電腦內的檔案。即使事後發現，被告的父親沒有實際上的權限，且被告的電腦設置有密碼，還是可認被告的父親有表見權限[74]。

在這一個案件中，法院雖然最終判定警察的搜索合於聯邦憲法第四增修條文的規定，在被告電腦裡所發現的圖片沒有證據排除規定的適用，但其中的說理，值得注意。法院認為被告享有合理隱私期待，主要的原因不是其在電腦設置有密碼，或是被告的父親不知道電腦的密碼。法院之所以認為被告就其電腦享有隱私權，是因為電腦儲存了人們各式各樣的私密資料，就如同過去口袋、手提袋或是書包等有形空間或是容器一樣。也因此，儲存在電腦中的檔案及手提箱內的物品，都受有聯邦憲法第四增修條文的保護，警察原

---

[71] United States v. Andrus, 483 F.3d 711, 715, 721-22 (10th Cir. 2007). 這一些跡象包括了由於電子郵件信箱使用的是被告父親的名字，網站上所登記的地址是被告父親的住所，被告父親告訴警察網路費用是其所支付，屋內有數人一同居住，被告的房門並未上鎖，警察能合理相信家中其他成員都可以進入，任何進到被告房間的人都可以看到電腦，且看起來像是任何人都可以使用該電腦。

[72] *Id*. at 718. United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir.2006) (en banc) (Kleinfeld, J., dissenting).

[73] *Id*. at 718-19. 法院在此強調道，在具體個案中判斷電腦是否「上鎖」與容器是否上鎖，很不一樣。這是因為，從外觀上多半可以知道容器是否已經上鎖，但除非開機及實際操作，否則幾乎無法從電腦或是數位設備上看得出來，其是否設置有密碼或是加密。也因此，在判斷執法官員是否善意地相信被告父親的表見權限時，必須要考量到電腦鑑識人員不當然從電腦的外觀上能夠知道其設置有密碼或是其中的檔案經過加密。

[74] *Id*. at 721-22.

則上必須要事先獲得同意或是令狀，才能查看儲存在其中的資訊或物品。在這一個案件中，由於警察合理地相信被告的父親有權同意查看被告所使用的電腦（表見權限），所以搜索合理，合於令狀原則的要求。亦即，被告就電腦之所以可以主張隱私權，不（只）是因為在電腦上設置有密碼，而是由於電腦與背包等有形體的容器或是空間，受有相同的保護。

二、共用電腦但設有獨立帳號密碼者同意

Trulock v. Freeh 案（下稱 *Trulock* 案）[75]裡的事實是，Trulock 與其女友同居，共用一台電腦，在詢問被告的女友後，警察知道兩人分別設定有自己的使用者帳號及密碼，彼此不相知悉，所以無法相互讀取對方的檔案。在得到了 Trulock 的女友同意後，警察查看了 Trulock 儲存在該電腦內，有密碼保護的檔案[76]。Trulock 主張警察侵害其受聯邦憲法第四增修條文所保護的權利，對警察提起了訴訟，請求損害賠償[77]。

法院判定道，Trulock 儲存在電腦中，設置有其女友不知道密碼的檔案，就像是放在兩人臥室中，上鎖的手提箱。從密碼的設置，很明確地可以知道，被告無意讓其女友接觸到檔案的內容[78]。是故，即使警察得到了被告女友的同意，也只能檢視兩個人所共用的資料，不能查看電腦中被告設有密碼的檔案[79]。但是，因為被告（執法官員）所為的搜索合於善意例外原則，所以法院最終還是判定其得以主張免責[80]。

在這一個案件判決的說理中值得注意的是，雖然法院認為，Trulock 儲存在電腦內，設置有讀取密碼的檔案，就像是臥室內上鎖的手提箱，所以享有聯邦憲法第四增修條文的隱私權[81]，但也同時承認，一個人是否能就儲存

---

[75] Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001).

[76] *Id*. at 398-99.

[77] *Id*. at 399.

[78] *Id*. at 403.

[79] *Id*. at 403.

[80] Id. at 403. 巡迴法院判定，任何一個理性（reasonable）正常的執法官員在當時的情狀下，都不會知道其行為違反了現行的規範。

[81] *Id*. at 403.

在與他人共用的電腦中，以密碼加密的檔案，主張合理隱私期待，尚未有定論，所以拒絕在本案中針對此一問題做成一個明確的判定[82]。換句話來說，由於法院意識到，關於電腦的相關法律及判決發展迅速，所以沒有直接援用過去涉及手提箱或是類似物品的判決，在這一個案件裡建立一個清楚的標準或規則。

再者，巡迴法院雖然認為，Trulock 對於其設置有密碼的檔案享有合理隱私期待，不過，從判決的說理可以知道，法院認為，雖然 Trulock 與其女友共用一台電腦，但是由於兩人設置有個別的帳號及密碼，顯示兩人皆仍保有電腦內檔案的私密，無意讓對方接觸到自己的檔案。這樣的情形，就像是兩人共用了一個房間，但仍將自己放在房間內的手提箱上鎖。所以，Trulock 的女友雖然可以同意搜索房間或是電腦中共用的檔案，但是沒有權利同意警察打開手提箱或是查看 Trulock 設置有密碼的檔案[83]。要言之，法院在這部分關於隱私的說明，主要是在解釋檔案加密及第三人同意間的關係，而不是判定使用了密碼或是加密技術，就當然能夠主張隱私權。

三、小結

從前述 2 個判決來看，電腦或是檔案是否設置有密碼，都是法院說理的重點。然而，判決中論及為什麼電腦或檔案所設置的密碼，以及其與隱私權間的關係，有深入探究的必要。

（一）密碼的設置及第三人同意

首先，*Trulock* 案的判決將檔案的密碼比擬為上鎖的容器。美國司法實務上，也確實曾有判決肯認人們對於上鎖容器可以主張聯邦憲法第四增修條

---

[82] *Id*. at 404.

[83] 類似的案件還有*United States v. Buckner*案, 473 F.3d 551 (4th Cir. 1997)。在這一個案件裡，在被告的妻子同意後，警察就被告及其妻子共用電腦進行電腦鑑識，警察因而發現被告涉及詐欺的檔案。被告主張，被告的妻子並無權同意被告設有密碼保護的檔案。法院並不接受被告的主張，並判定依照當時的情狀，被告的妻子有表見權限，警察是合理地相信被告的妻子有權同意。

文的權利。在 *United States v. Chadwick* 案（下稱 *Chadwick* 案）[84]中，被告被逮捕後一個半小時，警察官員打開了在被告車上所發現的上鎖手提箱[85]。聯邦最高法院判定，當一個人將物品放入上鎖的手提箱時，就像是把房屋的門關起來，可以認定其有合理的隱私期待[86]。不過，這不代表著在每一個案件中，都能夠逕自認為，加密後的檔案就像是 *Chadwick* 案中的上鎖手提箱。無論是前述的 *Andrus* 案或 *Trulock* 案，都必須要放在同意搜索的情境下來理解，而不是合理隱私期待的有無[87]。

在前述的案件中，尤其是 *Trulock* 案，法院似乎是將檔案的加密或是設置有密碼的電腦類比為上鎖的容器或是空間，所以將適用於實體容器或是空間的規則，應用到涉及檔案或是電腦的案件。也就是說，在共同居住於一個房屋的情形裡，警察獲得其中一個居住者的同意，就可以搜索共用的空間，但是不能進入到個別使用的房間。例如，張三及李四一起承租某住所，兩人都可以使用客廳、餐廳及廚房等共用區域，但分別使用兩個臥室。警察在獲得張三的同意後，就可以搜索客廳，但是張三的同意不及於李四的臥室，所以警察不能進入其中。同樣地，在涉及查看共用電腦的案件中，如果只獲有其中一個使用者的同意，執法官員不能檢視電腦中其他使用者加密或是設置有密碼的檔案。會有這樣的結論，是因為法院認為共用的電腦就像是一起居住的房屋，警察取得其中一位有使用權限者的同意後，可以搜尋查看其中共用的區域及檔案，但是不能夠檢閱其他使用者個別所使用的資料，就像是取得一位房客的同意，不能搜索其他人個別所使用的臥室一樣。是故，在 *Andrus* 案或 *Trulock* 案中，法院雖然認為警察的搜索違法，但並不（僅僅）是因為電腦或是檔案設置有密碼，而是因為密碼的設置顯示出一個人不欲與他人共用電腦或是其中檔案，所以共同居住或是共用電腦之人沒有同意警察官員查看設置有密碼的電腦或是檔案的權限。

---

[84] United States v. Chadwick, 433 U.S. 1 (1977).

[85] *Id*. at 3-6.

[86] *Id*. at 11.

[87] See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009).

（二）加密不當然就可以主張隱私權

從另一個角度來說，也可以知道，僅僅是將檔案加密或是設有密碼，並不當然就能夠主張合理隱私期待。舉一個稍微極端的例子來說，當檔案持有人將檔案加密或設置密碼，同時把密碼或是金鑰分享給其他使用者，其他使用者向第三人（包括警察）揭露檔案內容時，持有人並不能因為就電腦等設備設置有密碼或是將檔案加密，而能夠主張警察查看電腦內檔案的行為，構成了隱私的侵害。其中的原因在於，當檔案持有人向其他使用者透露了密碼或是金鑰後，便承擔了其可能對第三人洩露檔案內容的風險，也因而對加密後的檔案或是資料，不再能主張合理隱私期待。從這樣的例子可以知道，單純的檔案加密，不當然就因而可以享有隱私權。是否能夠主張此一權利，還是必須要納入個案中的其他情形來考量。檔案是否加密，確實重要，但應只是決定其持有人是否能主張隱私權的因素之一，並不是決定性原因或充分條件，不能認為，只要將檔案加密，就當然存在有合理隱私期待。反過來說，在一般情形下，一個人如果將某一個檔案儲存在隨身碟、行動電話或是電腦中，無論其是否加密，都能夠主張合理隱私期待（詳見下段的討論）。

（三）未設置密碼仍有隱私／電腦等個人設備中的檔案及隱私

人們對於自己存放在電腦中的檔案，無論是否加密或是設置有密碼，都可以主張隱私權，所以 *Andrus* 案或 *Trulock* 案中，電腦所設置的密碼並不是警察得否查看其中檔案的直接或決定性原因。詳細地來說，在 *Riley v. California* 案[88]裡，聯邦最高法院便判定，人們對於行動電話內的資訊享有合理隱私期待，原則上，警察必須要事先獲有令狀，才能夠查看在拘捕人身上所扣押的行動電話內的訊息[89]。值得留心的是，該案並未區分警察在被告身

[88] Riley v. California, 573 U.S. 373 (2014).

[89] *Id.* at 403. 從另一個角度來說，之所以討論與本人共用電腦之人是否有同意的實際權限或是表見權限，就是因為人們對於自己存放在電腦中的檔案，可以主張隱私權，否則就不需要討論是否獲有共用者的同意，共用者是否有同意的實際權限，或是綜合當時的所有情狀是否構成表見權限等問題。關於*Riley v. California*案判決

上所發現及扣押的行動電話是否設置有密碼，而是直接表示，查看行動電話內的資訊，有聯邦憲法第四增修條文的適用。換言之，無論行動電話或其他設備是否設置有密碼，都不會影響到人們對於這一類裝置所得主張的合理隱私期待。

即使是如 *Trulock* 案的判決，將設置有密碼的電腦比擬為上鎖的容器，也會得到相同的答案。聯邦最高法院在 *Arkansas v. Sanders* 案[90]中便明確地指出，即使是沒有上鎖的行李箱，還是受有聯邦憲法第四增修條文的保護[91]。是故，依 *Trulock* 案的類比，應認即使電腦沒有設置密碼或是其中的檔案未加密，使用者還是可以主張合理隱私期待。亦即，密碼或是加密程式的使用，並不是一個人就電腦中檔案可以享有隱私權的前提要件。由此也可以知道，*Andrus* 案及 *Trulock* 案中電腦所設置的密碼，影響的是第三人的同意是否有效，並不是單純因為被告設有密碼，所以警察的行為當然構成了搜索。

伍、上鎖容器的類比

因為在加密技術的使用上，使用了金鑰等用語，所以在理解加密檔案或是適用相關規範時，經常會使用上鎖容器的類比。認為兩者在概念上相似者認為，由於人們就後者享有隱私權，所以對於前者也可以有相同的主張。不過，加密技術的使用，是否類似於上鎖容器，而能夠適用相同的規範呢？其中不無值得思考及商榷的地方。

的分析及討論，可以參考溫祖德（2015），〈行動電話內數位資訊與附帶搜索：以美國聯邦最高法院見解之變遷為主〉，《月旦法學雜誌》，239期，頁198-220；李榮耕（2016），〈數位資料及附帶搜索：以行動電話內的資訊為例〉，《臺北大學法學論叢》，100期，頁245-322。

90 Arkansas v. Sanders, 442 U.S. 753 (1979).

91 *Id*. at 762.

一、合理隱私期待及上鎖容器

聯邦最高法院在 *Katz v. United States* 案（下稱 *Katz* 案）[92]中，判定了聯邦憲法第四增修條文保障了無實體型態的電話通訊[93]，*Riley v. California* 案[94]也肯認了人們就其儲存於行動電話內的數位資訊享有聯邦憲法上的隱私權[95]。是以，數位型態的檔案或資訊可以是聯邦憲法第四增修條文的保障的客體，應屬確論，殆無疑義。

依合理隱私期待理論，一個人採取了某些動作或作為，以確保一定空間或是訊息不為外人所知，展露出了保有該空間或訊息私密的主觀期待，而該期待為一般人認為屬合理時，就可以主張聯邦憲法第四增修條文的隱私權[96]。據此，上鎖的箱子、有密碼鎖的手提箱或是上鎖的儲物櫃，即使是置放於公共場合或位於第三人眼目可及之處，都還是應認其所（持）有人可以主張隱私權[97]。

如果檔案的加密可以類比為容器的上鎖，那麼一個人將檔案加密，就像是將物品放到容器當中，並將之上鎖。人們就上鎖的容器可以主張合理隱私期待，對加密後的檔案也享有同樣的權益。相反地，如果認為加密檔案並不像是上鎖的容器，那麼即使人們對於後者可以主張合理隱私期待，也不當然就前者享有隱私權。

---

92 Katz v. United States, 389 U.S. 347 (1967).

93 *Id*. at 353.

94 Riley v. California, 134 S.Ct. 2473 (2014).

95 *Id*. at 2494-95.

96 Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring) (1967).

97 United States v. Jacobsen, 466 U.S. 109, 120 n.17 (1984). 在這一個判決中，聯邦最高法院認為，人們對於封緘包裹享有合理隱私期待，所以原則上，執法機關必須要先取得法院所核發的令狀，才能開拆檢視。*See also* United States v. Chadwick, 433 U.S. 1, 11, 13-14 n.18 (1977). 這一個案件判定，即使是置放於公開場所，人們對於其已經上鎖的手提箱的內容物品，還是享有聯邦憲法第四增修條文所賦予的保護。United States v. Karo, 468 U.S. 705, 721 (1984). 聯邦最高法院判定，人們對儲物櫃享有合理隱私期待。

二、肯定說

主張加密後的檔案如同是上鎖容器中的物品者多認為，加密就像是一虛擬容器或是鑰鎖，加密後的檔案就像是在容器中的物品，如背包中的文件或是手提箱裡的物品[98]。傳統上，人們對於容器內的物件或是屋內的事物可以主張隱私權[99]，對加密後的檔案，也是如此。加密程式或是技術也可以比擬為是將明文置放或是封緘在數位密文所構建的牆壘之後，使他人無法觀看到其內容，或把文件或物品放在上鎖的手提箱[100]、置物櫃或是房間裡，持有金鑰的人就像是擁有鑰匙，才能夠開啟置物櫃或進入房間（讀取檔案的內容）[101]。亦即，加密程式有著與（帶）鎖的容器、信封或是儲物櫃類似的作用，都是讓本人能夠決定，誰才能夠接觸到特定訊息（文件、文書或檔案的內容或是內部所裝載的物品等），讓第三人無法（或難以）知悉其內容。兩者的差別只是，前者是以編碼或是演算法的方式使人們無法接觸到加密後檔案的內容（也就是將其「上鎖」），後者則是以金屬、木材或塑膠等材料形成阻隔[102]。將一個原本可以在電腦或是類似設備上讀取的檔案加密，就像是把一份文件放到信封袋內封緘起來，或是將物品裝載於手提箱或是置物櫃，關上門，或甚至是上鎖，可以認為在主觀上展露出了想要保有該文件或物品的隱

---

98 *See* Crain, *supra* note 13, at 870; Sean J. Edgett, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 350-51 (2003); David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2232 (2009); Timothy B. Lennon, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467, 487 (1994); Froomkin, *supra* note 3, at 871.

99 *E. g.*, United States v. Castellanos, 820 F. Supp. 80, 87 n.4 (S.D.N.Y. 1993). 這一個案件判定，人們對於上鎖房間的內部，享有合理的隱私期待。State v. Kaaheena, 575 P.2d 462, 467 (Haw. 1978). 法院在這個案件認為，窗戶在拉上窗簾後，人們對於屋內的活動可以主張合理的隱私期待。

100 United States v. Chadwick, 433 U.S. 1, 11 (1977).

101 Edgett, *supra* note 98, at 350, 365.

102 David Hricik, *Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 493 (1998).

私狀態的意向，而一般人也應該會認這一個主觀上的期待是合理的。因此，依 Harlan 大法官在 *Katz* 案所建立的合理隱私期待理論，人民對於加密後的檔案享有隱私。美國便曾有聯邦地方法院採取這樣的立場。例如，在 *United States v. D'Andrea* 案[103]中，麻薩諸塞（Massachusetts）州聯邦地方法院判定，如果認為個人可以信任鎖、保險箱或警報系統，那麼也應該可以就有帳號密碼保護的電腦及經加密或有密碼保護的檔案主張合理隱私期待[104]。

依這樣的類比，那麼未事先取得法官所核發的令狀，就以猜測密碼或暴力攻擊的獲知金鑰，就會像是無令狀，便抓捏乘客放在公車或巴士內行李架上的行李袋，或是以工具撬開鎖具，試圖得知其中可能放了什麼東西一樣[105]。由於聯邦最高法院已經判定，未經相對人的同意或是事先取得令狀，就抓捏行李袋外部，以知悉可能的內容物，會違反聯邦憲法第四增修條文，那麼類似的猜測金鑰的行為，同樣會構成了搜索，必須要依循令狀程序，方得為之[106]。從另一個角度來說，如果不認為人們對於加密的檔案可以主張合理隱私期待，會有一個突兀的結果，也就是，一個人即使將檔案加密，仍不能主張隱私權，但其只要將檔案列印出來，放進封緘的信封或是保險箱裡，就可以享有隱私權的保護。

前述立場主要是認為加密檔案類似於上鎖容器，兩者皆受有隱私權的保護。除此之外，認為兩者有其近似者也認為，從政策上的角度來說，承認加密技術的使用本身就受有隱私權的保障，可以更大程度地維護個人對於資訊或是私密事項的控制。這是因為，一個人將檔案或是訊息傳送給他人（收件人）後，就已經承擔了該他人可能將其洩露或是告知第三人的風險，所以對該訊息不再能主張合理隱私期待，所以，若執法機關從收件人處取得寄件人所寄送的訊息，寄送人不能主張隱私受有侵害[107]。如果執法機關是以違法的

---

[103] United States v. D'Andrea, 497 F. Supp.2d 117 (D. Mass. 2007).

[104] *Id.* at 121.

[105] Bond v. United States, 529 U.S. 334, 338-39 (2000).

[106] *See, e.g.*, United States v. Presler, 610 F.2d 1206, 1213-14 (4th Cir. 1979).

[107] 這一個概念，多稱之為第三人理論（the Third Party Doctrine）或是風險承擔理論（the Assumption-of-Risk Theory）。相關的介紹及討論，可以參照王兆鵬，前揭註

方式自收件人處獲得寄件人發送的通訊內容（如無令狀搜索），由於所侵害的是收件人的隱私，寄送人會因為欠缺當事人適格（standing），不能主張警察官員的行為違背法律[108]。但是，如果肯認加密後的檔案就像是把物品放入容器之內，或是將之上鎖，那麼即使寄件人將訊息寄送給了收件人，就還是可以針對檔案主張合理隱私期待，執法機關即使取得了，也不能逕自破解，閱讀其中的內容，就像是取得了一個上鎖的容器，也不當然就能夠破壞鎖具，查看其中所裝載的物品。是故，將檔案加密後，就可以主張隱私權。

三、否定說

「加密—金鑰」的文字及用語，類似於傳統的「鎖具—鑰匙」，也因此，不意外地，會有上鎖容器與加密檔案的比擬，並主張兩者有其類似之處，所以都能主張合理隱私期待。不過，有學者就此持反對的立場，認為表面上兩者都是透過一定的技術或是裝置，使得他人無法得知特定的資訊，但是其中運作的原理及本質，有很大的差異，無法相比擬。

詳細地來說，檔案的加密，只是讓未持有金鑰者無法辨識或理解檔案內的資訊，並不像是把一份文件放到（有鎖的）容器當中[109]。有形體的容器，是以物理性的屏蔽，讓容器分有內外，使人的五官（視覺、嗅覺及觸覺等）無法直接感知到容器內的狀態。也因此，一個人將物件或文件放在上鎖的容器內，可以享有隱私權益。但事實上，即使容器沒有上鎖，只要其可以完全封閉起來，使內外有所阻絕（如房間、手提箱、背包或是抽屜），就能夠主張聯邦憲法第四增修條文的權利。容器上的鎖只是讓人更能夠或是容易主張此一權利[110]。相對地，檔案的加密雖然也有「金鑰」，但其根本上的不同是，

70，頁151-153；以及李榮耕，前揭註70，頁114-115。

108 關於當事人適格，可以參照王兆鵬、張明偉、李榮耕（2022），《刑事訴訟法（上）》，頁148-152，6版，新學林。與當事人適格類似的概念為「權利領域理論」。深入的分析及討論，可以參照楊雲驊（2007），〈未告知證人拒絕證言權之法律效果：評最高法院九五年臺上字第九〇九號、九五年臺上字第二四二六號、九六年臺上字第一〇四三號判決〉，《台灣法學雜誌》，99期，頁164-172。

109 Kerr, *supra* note 52, at 520-24.

110 *See* United States v. Benson, 631 F.2d 1336, 1338-39 (8th Cir. 1980).

人們還是可以看到該檔案的內容，只是因為經過程式加密，所看到的是加密後的密文，無法了解其意義而已[111]。也就是說，加密就像是以另一種語言或是符號編寫原本文件中的內容，而不是把文件放在一個手提箱、置物櫃或是房間裡面。是故，在加密後，人們還是看得到該檔案或是資料，只是在解密之前，不了解其意義而已[112]。這就像是一個不懂中文的人，在看以中文撰寫的書報、文件或是郵信一樣，不是看不到其中的文字，而是沒有辦法了解其中的含意。由於他人還是能觀看到檔案或文件的內容（僅是以密文的型態），所以檔案的持有人不能主張合理隱私期待[113]。

四、討論與分析

由於型態上的近似，上鎖的封閉容器經常被提及，並用以主張人們對於加密後的檔案享有隱私權。不過，也有學者對這樣的看法持反對的立場。依前者，由於檔案持有人對於加密後的檔案享有合理隱私期待，所以破解加密措施，讀取檔案內容的行為會構成搜索，所以原則上，必須要事先獲有令狀，方得為之。依後者的看法，單純的加密本身並不能使檔案持有人得以主張合理隱私期待，所以執法官員可以逕自破解檔案的加密技術，無須經過法院審查授權。在分析及討論後，我們認為，後者的說法較為可採，上鎖容器及相關判決的說理並無法適用於加密檔案。

（一）癥結所在

針對加密檔案是否類似於上鎖容器中的物品，有著肯否兩種截然不同的看法。其中的關鍵點很可能是，檔案在加密後，人們究竟是否還能不能看（得）到檔案的內容？

---

[111] Kerr, *supra* note 52, at 521; Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713, 713 n.2 (2000).

[112] Kerr, *supra* note 52, at 515-19; Scott Brady, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1604 (1997).

[113] Kerr, *supra* note 52, at 515-19; Brady, *supra* note 112, at 1604.

依肯定說，加密技術可以比擬為（上鎖）容器，因此將檔案加密，就像是將傳統的文件放到上鎖的容器中，沒有鑰匙者就無法接觸到文件的內容。在這一個類比之下，傳統的容器是以物理、有實體的屏蔽（virtual wall），隔絕容器外的人的視覺，使得他人無法知悉容器中的狀態、其中裝載的物件或是文件的內容，而加密技術則是以虛擬的屏障（digital wall），讓沒有權限（沒有金鑰）的人「看不到」文件或是檔案的內容[114]。由於兩者有著類似的作用，所以加密後的檔案就像是上鎖的容器，同樣享有隱私權的保障，還原或是破解加密後的檔案，也就有令狀程序的適用[115]。亦即，持肯定說的學者主張，在加密後，人們只看得到密文，看不到明文，就像是擺放在手提箱中的物品一樣，只看得到手提箱的外部，看不到其中裝了什麼東西。由於人們對於從外部看不到的手提箱內物品可以主張隱私權，對於看不到的密文也就可以主張聯邦憲法第四增修條文的權利[116]。也因此，試圖破解加密就會像是抓捏行李袋的外部，以得知其中物品的形狀一樣，構成了對於隱私的侵害[117]。

持否定說者則認為，加密就像是將文件的內容從一個語言翻譯為另一種語言，或是轉譯為表面上沒有任何意義的字串。文件加密並不是看不到其中的內容，只是無法了解其意思，需要翻譯或是還原而已。也因此，閱讀、接觸或是試圖理解加密後的文件本身，就像是執法官員試著將外國文書翻譯為本國文字，或是翻譯幫派份子的黑話或行話一樣，並不會構成搜索，也就不需要事先向法院聲請令狀。舉例來說，檔案的加密，就像是 ISELLDRUGS0912345678 可以透過規則轉譯為 LVHOOGUXJV3245678901（字母及數字按照順序向右順移三位，末尾折回）。人們並不是看不到組合成訊息的字母及數字（加密後的 LVHOOGUXJV3245678901），只是在解密之前，不了解其意義而已。也因此，加密技術不是使他人看不到加密後檔案

---

114 Edgett, *supra* note 98, at 365.

115 Edgett, *supra* note 98, at 350.

116 *See* United States v. Chadwick, 433 U.S. 1, 11, 13-14 n.8 (1977).

117 *See Bond*, 529 U.S. at 338-39.

的內容，而只是使沒有金鑰的人無法理解所看到的密文。也因此，就像是不能反對人們猜測如何將 LVHOOGUXJV3245678901 還原為 ISELLDRUGS0912345678，或是將外國文字翻譯為本國文字一樣，人們不能反對執法人員破解加密後的檔案。

從前面的討論可以知道，之所以會有肯否兩種截然不同的立場，主要是因為對於「觀看」或是「觀看到」的理解不同。依肯定者的看法，在加密後，人們已經無法理解檔案的內容，就像看不到一樣，所以持有人對於加密檔案享有合理的隱私期待；否定者則主張，人們還是看得到加密後的檔案的內容，只是看不懂而已，也正因為他人還是看得到，所以檔案持有人不能主張隱私權。持肯定者的「觀看」，偏向於是「理解」或「瞭解」文字、符號或圖案的意義；否定者的「觀看」，則是單純的「看到」或是視覺上有所感受。

（二）加密技術不能類比為上鎖容器

從結論上來說，否定說比較符合加密技術的原理及運作方式，較為可採。必須要肯認的是，隱私權益的理論及規範，需要隨著科技或是電腦技術的發展而有所調整。司法院釋字第 689 號解釋理由書中指出：「尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。」Alito 大法官在 *United States v. Jones* 案[118]的協同意見書中便指出，科技能夠改變人們對於隱私的期待及觀感，也因此，法院的判決必須要有所改變及因應[119]。Sotomayor 大法官在同一個案件中，也表達同樣的看法，認為法院必須要因為科技，重新考量聯邦憲法第四增修條文中的諸多原則[120]。不過，基於下述幾點理由，我們還是認為，加密技術不能類比為上鎖的

---

[118] United States v. Jones, 132 S. Ct. 945 (2012).

[119] *Id*. at 962 (Alito, J., concurring).

[120] *Id*. at 957 (Sotomayor, J., concurring). 聯邦第四巡迴法院在*Trulock v. Freeh*案中也判定，即使獲得電腦的共同權限人的同意，警察還是不能讀取本人設定有密碼的檔案。亦即，即使與他人共用電腦，本人只要就檔案設定了共用人所不知道的密碼，就還是享有合理隱私期待，執法官員必須要另外取得令狀或是得到本人的同意，才能夠讀取其中的內容。這樣的判決，等於是改變了過往對於共同權限或是

容器，檔案的持有人不能只是因為使用了加密技術，就可以主張合理隱私期待。

1. 看不懂等於看不到？

肯定說的優點在於，讓人們在電腦技術發達的現代，受有範圍更大更強的隱私保護，但是其說理及在個案的適用上，勢必會有其爭議。依肯定說，人們無法理解加密後檔案的內容，就像是看不到一樣，所以可以主張合理隱私期待。但問題是，如果觀看、看得到指的是能夠「了解」所看到的文字或符號的意涵，那接下來的問題是，對於文字或符號要認識到什麼樣的程度，才能算是「了解」[121]？再者，要用什麼樣的標準判斷是否「了解」或「不了解」所看到的訊息的內容？要以執法官員為準？還是一般人？舉例來說，檢警官員在逮捕毒犯後，在其身上發現一本可能與毒品交易有關的小冊子。在檢視後發現，該冊子是以警察完全不懂的緬甸文書寫而成。此時，是否可以說警察已經看到了其內容？如果警察粗識緬甸文字呢？如果是用法文、日文、英文或是江湖黑話，答案是否會有所不同？依肯定說，答案似乎會是，只要警察不了解冊子裡的文字或符號的意思，即使看到了其中的內容，冊子的所有人就還是可以主張合理隱私期待，但警察要多不了解冊子裡文字的意思，才能認為等同於看不到？再者，如果看不懂就等於是看不到，那麼前述案例中冊子的所有人就可以主張隱私權，如此一來，警察請求熟識緬甸文的人幫忙翻譯，或是詢問黑話的意思，就會侵害了冊子所有人的隱私，構成了刑訴法意義中的搜索，因而應有令狀原則的適用。這樣的結論，恐怕難以為一般人所接受。

2. 封閉容器（即使沒有上鎖）就可以主張合理隱私期待

主張加密後檔案受有隱私權的保護，很重要的理由之一，是其類似於上鎖的容器。亦即，容器上的鎖具像是加密技術，鑰匙就像是可以將密文還原為明文的金鑰，由於人們對於上鎖的容器享有合理隱私期待，所以加密後的

風險承擔理論的看法。Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

[121] Kerr, *supra* note 52, at 523.

檔案也會在隱私權的保障範圍之內[122]。乍看之下，上鎖容器與加密技術（檔案）類似，人們對於兩者可以主張相同的權利，但事實上，這樣的說法與過往封閉容器相關的判決不盡相符。

詳細地來說，美國實務上向來認為，只要是封閉容器，無論有沒有上鎖，人們就享有合理隱私期待。舉例來說，在 *New York v. Belton* 案（下稱 *Belton* 案）[123]中，聯邦最高法院判定，警察在攔查違規車輛，聞到大麻燃燒的氣味，發現印有「超級金（Supergold）」（通常指稱的就是大麻）的信封袋，合法逮捕車上的 4 名乘客後，可以打開該信封袋及檢查在車內夾克，查看其中的內容物[124]。但是，聯邦最高法院同時也指出，在一般的情形下，人們對於手提袋、背包、公事包、口袋或是皮夾等容器，享有合理隱私期待，也因而有令狀原則的適用[125]。

從 *Belton* 案的判決可以知道，將加密檔案比擬為上鎖容器的問題在於，無論上鎖與否，人們對於封閉容器及其內所裝載的物品或文件，都享有隱私權。亦即，如果認為加密後的檔案就像是上鎖後的容器，所以受有隱私權的保障，其似乎是暗示，人們對於未上鎖的容器，是不享有合理隱私期待的，但這顯然與過往學說及實務上的看法相左[126]。再者，即使是認為，加密技術

---

122 也有學者提出類似的看法，認為使用加密技術交換的訊息，就像是在房屋等處所加裝門鎖或警報系統，所以可以主張聯邦憲法上的隱私權。Francis A. Gilligan & Edward J. Imwinkelried, *Cyberspace: The Newest Challenge for Traditional Legal Doctrine*, 24 RUTGERS COMPUTER & TECH. L.J. 305, 334-35 (1998).

123 New York v. Belton, 453 U.S. 454 (1981).

124 *Id*. at 460-61.

125 *See id*. at 460-61. 亦即，在本案中，警察之所以可以無令狀地搜索汽車內部的空間，打開信封袋及夾克，是因為合法地逮捕了Belton等人。

126 主張加密後的訊息就像是上鎖或是裝置有警報系統的房屋的說法，也有著類似問題。如果加密後的檔案就像是上鎖後的房屋，似乎是暗示著，沒有上鎖的房屋就沒有合理隱私期待。此外，房屋等處所，無論上鎖與否，無論是否安裝有警報，居住者都可以主張合理隱私期待，而實務上已經判定，無論是否經過加密，通訊都受有隱私權的保護。*See, e.g.*, Scott v. United States, 436 U.S. 128 (1978); United States v. Kahn, 415 U.S. 143 (1974); United States v. Giordano, 416 U.S. 505 (1974). 司法院釋字第631號解釋也明確肯認，人們對於透過電話所進行的通訊享有憲法所保障的祕密通訊自由（通訊隱私）。

在效果或是作用上，就「像是」實體的鎖具，把原本可以看得到的檔案「鎖」起來，讓沒有鑰匙（解密的金鑰）的人無法接觸其內容，但就資訊及電腦的整個運作程序來說，並沒有一個封閉容器，或是類似於封閉容器的階段。亦即，有形體的容器是：「容器→放入物品→容器上鎖→沒有鑰匙的人無法接觸容器內物品」但相對地，加密技術的使用是：「檔案→加密程式→加密後的檔案→沒有金鑰的人無法接觸到檔案的內容」前者中的「容器上鎖」，在後者中並沒有相對應的概念。是故，上鎖的容器不盡能與加密程式相提並論。

3. 肯定說於適用上的困難

肯定說除了會有前述理論上的疑義之外，在具體個案中，也會因為其與傳統鎖具有著本質上的差異，在判斷警察官員是否故（惡）意以違法的方式取得數位檔案時，可能會有判斷上的困難。美國實務上，有法院指出，在電腦上或就檔案所設置的密碼並不像是鎖，因為手提箱或是行李箱等容器上的鎖，從表面就可以看到，知道相對人不欲讓他人知道容器內的狀態，但電腦或是檔案上所設置的密碼並不是如此。從電腦等設備的外表，單以肉眼觀察，並沒有辦法知道其是否有密碼保護[127]。這個差異影響所及的是，在進行電腦鑑識時，如果使用程式沒有特別設定，偵查官員可能完全不會知道鑑識的電腦或是類似的設備（如智慧型行動電話）設置有密碼。如果所使用的鑑識程式破解或是繞過了密碼的保護措施，在電腦等裝置內進行搜索，取得了可為證據的資料，是不是能夠就認為屬於執法官員故（惡）意以不法的方式取得證據，不無疑義。

（三）更近似於檔案加密的案件

基於前述的因素，加密檔案並不能類比為上鎖的封閉容器。從加密技術及加密檔案的本質來看，其更類似於外國語言的翻譯、警犬的嗅聞及軋碎的紙本文件。法院在這一類案件中的判決及說理，更能夠用以說明執法機關得否破解加密後的檔案，以及其是否應依令狀原則為之。

---

[127] *Andrus*, 483 F.3d at 718-19 (10th Cir. 2007).

1. 外國語言的翻譯

美國實務上曾有案件認為，人們即使刻意使用在場之人所不了解的語言交談，對於談話的內容，仍然不得主張合理隱私期待。以 *United States v. Longoria* 案（下稱 *Longoria* 案）[128]為例，被告 Longoria 涉嫌走私毒品。包括被告在內的毒販在外人面前，會刻意地以西班牙語交談。美國聯邦調查局（Federal Bureau of Investigation, FBI）的線民錄下了某次毒販間以西班牙語進行，關於販毒計畫的對話[129]。後來，該對話被翻譯為英文，並且成為了起訴被告販賣毒品等犯罪事實的重要證據[130]。在審判中，被告主張他對於談話享有合理隱私期待，因為他選擇以在場人不瞭解的西班牙語交談，無意使他人知悉對話的內容[131]。是故，被告主張，由於其對於與他人以西班牙語進行的對談享有隱私權，而依聯邦通訊監察法，執法官員在監察這一類通訊前，原則上必須先獲有法官所核發的令狀，但在本案中，法官並未審查授權線民的監錄，所以其行為違法，所取得的對話內容無證據能力[132]。後案件上訴至美國聯邦第十巡迴法院。審理後，法院並沒有接受被告這樣的主張[133]。

巡迴法院指出，被告對於其所進行，能夠被他人清楚地聽到的對話，不能主張聯邦憲法所保障的隱私權。在本案中，被告明確地知道當時有其他人在場，談話會被他人聽到，但還是自願在該他人面前談論犯罪的計畫，所以不能期待在場的他人不會將所聽到的對話內容告訴其他人[134]。再者，雖然被告刻意以在場的人（包括線民在內）所不懂的西班牙語進行交談，但並不能因此就主張享有合理隱私期待。這是因為，當一個人選擇在他人面前進行談話時，就已經承擔了會被聽到且會被知悉該談話內容的風險，本案中的被告

---

[128] United States v. Longoria, 177 F.3d 1179 (10th Cir. 1999).
[129] *Id.* at 1181.
[130] *Id.* at 1181-83.
[131] *Id.* at 1182-83.
[132] *Id.* at 1182.
[133] *Id.*
[134] *Id.* at 1183.

雖然是以西班牙語進行談話，並且希望在場的人（包括線民在內）不瞭解其內容，但是被告此一主觀上的期待，在客觀上並不是合理的[135]。

依 *Longoria* 案的判決，將檔案加密後，只有握有金鑰或密碼的人，才能夠將檔案解密，得知其中訊息的內容，就像是以西班牙語進行的對話，也只有懂得西班牙語的人才能夠知悉其中的內容一樣。亦即，以西班牙語談話就像是使用金鑰將檔案加密一樣，是將談話內容以西班牙語予以編碼，使其只能夠為一定範圍內（懂得西班牙語）的人所瞭解。但是，在他人面前交談，就已經承擔了被他人所知悉談話內容的風險，不能因為只是選擇了其他人所不了解的語言交談，就享有合理隱私期待。這就像是，警察在公眾場合偶然地聽到幫派份子以黑話對談時，也可以側聽，並不會因而侵害了其隱私權。儘管犯罪嫌疑人使用了江湖行話，自信旁人聽不懂，但是由於其不能主張合理隱私期待（因為是在公開場所），所以警察不需要向法院聲請令狀，就可以解譯所聽到對話內容，或是詢問其他了解黑話的人[136]。同樣地，不能只是因為將檔案加密，使他人無從知悉其內容，就能夠針對檔案的內容主張隱私權[137]。是故，破解加密後的檔案，沒有令狀原則的適用[138]。

再者，加密後的檔案之所以不能類比為上鎖容器中的物品是因為，沒有金鑰並不是無法開啟加密後的檔案。人們還是能夠用加密前所對應的應用程

---

[135] *Id*. at 1183-84.

[136] Kerr, *supra* note 52, at 515-19; Brady, *supra* note 112, at 1604.

[137] *See* Kerr, *supra* note 52, at 513-17.

[138] 無論是什麼樣的類比，都是拿兩個以上不相同事物，以對應或是相類似的地方，幫助我們從比較熟悉者，了解比較陌生者。例如，「母親像月亮一樣」，是以月光的柔和怡人，描述媽媽們的慈祥及對兒女的無微不至，並不是說，母親就是月球這個天體，有陰晴圓缺，只有在晚上才看得到。也就是說，無論是什麼樣的類比，都會有其極限，到了某個地步，就無法再繼續下去。舉例來說，就某個加密檔案，只有相當少數的人會有其金鑰，但是有上億的人口會講西班牙語。再者，金鑰中只要有一個字元有誤，就無法將密文還原為明文，但是使用外國語言交談，即使帶有口音，或是用詞或文法上有些許錯誤，很可能還是不會影響參與對話人相互間的理解。雖然如此，就將訊息轉換為一定範圍的人才能夠了解或是接觸到其內容的作用來說，使用外國語言確實是可以用來說明為什麼人們對於加密檔案不當然就能夠主張合理隱私期待。*See* Edgett, *supra* note 98 at 356-57; Couillard, *supra* note 98, at 2235.

式（如文書處理軟體等）或是其他軟體開啟加密後的檔案，只是開啟後所能看到的訊息對於未持有金鑰者，沒有任何意義可言而已。加密檔案就像是將一個訊息從一個語言翻譯為另一個語言。人們不能反對執法機關翻查字典、使用翻譯軟體、詢問熟悉特定語言的人或是猜測訊息中的內容[139]。從這一個角度來說，如果還是要將加密檔案比擬為容器中的物件，加密程式或是加密後的檔案不是上鎖的容器，而是一個神奇的盒子，物品在放入後，還是可以拿出來，只是物品在取出後會改變其型態、外觀或成分，無法再辨識出所放入的到底是什麼東西。也因此，只要加密檔案的取得合於聯邦憲法第四增修條文的要求，如在公開網站上下載了加密檔案，或是緊急搜索了特定人的行動電話或是電腦後發現加密檔案，不需要事先向法官聲請令狀，就可以予以解密，將檔案還原為明文[140]。

2. 警犬的嗅聞

在過往的案件，聯邦最高法院認為，警察使用警犬嗅聞人們在公開場合中的行李或背包，不構成搜索。根據相同的理由，在涉及破解加密後檔案的案件中，也可以得到相同的結論。

(1) 相關案件及聯邦最高法院的說理

聯邦最高法院曾經判定，由於毒品是違禁品，人們並不能就其主張任何的權利（包括隱私權），所以警察官員檢驗郵件包裹破損處的白色粉末，如果只是確認其是不是毒品，不會揭露或知悉關於該粉末的其他資訊（例如，如果不是毒品的話，是糖粉、麵粉、太白粉或是其他物質等）者，不構成隱私的侵害[141]。在 *United States v. Place* 案[142]中，聯邦最高法院同樣認為，警察官員使用警犬嗅聞行李，只會知道非常有限的資訊，也就是行李中是否裝

---

139 Kerr, *supra* note 52, at 515-19; Brady, *supra* note 112, at 1604.

140 Kerr, *supra* note 52, at 505.

141 United States v. Jacobsen, 466 U.S. 109, 122-23 (1984).

142 United States v. Place, 462 U.S. 696 (1983).

載有毒品，所以不會構成聯邦憲法第四增修條文意義下的搜索，沒有令狀原則的適用[143]。

除了前述原因外，還有另一個理由可以解釋為什麼警犬嗅聞不構成搜索：警犬僅探知了暴露在公共場域中的訊息，而不是私密空間內的狀態。亦即，警犬之所以可以反應行李內有沒有毒品，不是直接探知到其內部，而是因為行李內部物品的氣味飄散到了外部，被警犬所嗅聞到。由於人們對於暴露在公共空間的資訊，並不能夠主張合理隱私期待[144]，而警犬接收到的是擴散到行李外部的空間的氣味分子，不是行李內部的狀態[145]，所以行李的持有人不能主張隱私權被侵害，警察使用警犬嗅聞行李也因而無須事先向法官聲請令狀。

(2) 破解加密檔案類似於警犬的嗅聞

在這一個類型的案件中，人們並不是無法接收到逸散到行李外的氣味，而是因為氣味分子的濃度較低，即使吸入了帶有毒品氣味的空氣，也不會有所感知。也就是說，人們不是聞不到，只是不知道自己聞到了些什麼物質的味道而已。人們沒有辦法感知空氣中是否有毒品的氣味，但透過經過訓練，嗅覺更為靈敏的警犬，就可以知道從包袋內飄散到外部的氣味，是不是含有毒品的氣味分子。人們不是看不到加密後的檔案，只是看不懂其中的涵義。同樣地，人不是吸不到含有毒品氣味的空氣，只是不知道呼吸到的空氣中有著毒品的味道。就後者而言，持有毒品之人不能阻止，或是沒有權利反對警察官員使用犬狗嗅聞飄散在公開場域中的氣味，相同地，將檔案加密的人也不能反對執法機關使用破解技術，知悉檔案的內容。這是因為，對於加密資料及容器外氣味，人們都不是無法接觸到，只是無法理解、判斷或感知所接觸到的是什麼。也因此，無論是使用警犬嗅聞行李及破解技術的使用，都沒有侵害相對人的隱私權益，也因而沒有令狀原則的適用。

---

143 *Id.* at 707.

144 *See* United States v. Knotts, 460 U.S. 276, 282-83 (1983).

145 *See Id.* at 285.

3. 軋碎的文件

人們對於攪碎或是軋碎後的文件不能主張合理隱私期待。這可以說明為何不能只是因為使用了加密技術，就能夠主張隱私權。

(1) 法院的判決及說理

在 *United States v. Scott* 案[146]中，被告 Scott 涉嫌謊報退稅資料，為了蒐集相關證據，國稅局（the Internal Revenue Service，下稱 IRS）的官員拾取了被告置放在其屋外，等待清潔業者收取的垃圾袋。垃圾袋中有碎紙機處理過，約 0.04 公分寬的紙條。將紙條拼湊還原後，官員用以向法院聲請搜索票，獲准。被告主張，其對於切碎後的紙條享有合理隱私期待，受有聯邦憲法第四增修條文的保護，官員未依令狀程序取得紙條的行為違憲[147]。聯邦地方法院同意被告的主張，認為判定依據切碎的紙條所為的搜索欠缺相當理由，IRS 官員所為的搜索違法，所取得證據沒有證據能力[148]。案件上訴至聯邦第一巡迴法院。巡迴法院審理後，撤銷聯邦地方法院的裁定，改認法院所核發的搜索票合法，IRS 執行搜索扣押所得的證據無須排除。

聯邦第一巡迴法院解釋道，本案涉及到的是置放在公共場合的垃圾，當一個人將垃圾放在路邊，留待他人處理，就不再能夠就其主張合理隱私期待[149]。即使被告以碎紙機將文件軋碎，其仍然是丟棄在公共場所的垃圾，不會因為經過碎紙機的處理，就能夠主張更高或更多的隱私權利保護，因此警察可以拾取這一些軋碎後的紙條，作為聲請令狀或是認定其犯罪之用[150]。更為關鍵重要的是，法院最後判定，被告不能僅僅因為在丟棄前將紙張軋碎，就可以主張聯邦憲法第四增修條文的權利，也因此，警察可以拼湊組合在垃圾中撿拾到的撕碎或軋碎的文件[151]。

---

[146] United States v. Scott, 975 F.2d 927 (1st Cir. 1992).
[147] *Id.* at 928.
[148] *Id.*
[149] *Id*. at 929-30.
[150] *Id.*
[151] *Id.* at 930.

(2) 加密後檔案可以類比為軋碎的文件

碎紙機及加密技術有其極為類似的地方，所以關於前者的判決能夠用以說明後者與隱私權間的關係。在文件被軋碎之前，人們可以閱讀得到其上的記載，同樣地，在加密之前，也可以接觸得到檔案的內容。在碎紙機處理過後，雖然看得到切碎的紙片，但已經可以說無法理解其中的內容，在使用加密程式後，也不能再認識檔案中的資訊。由於個人不能只是因為將文件軋碎或是撕碎，就可以主張合理隱私期待[152]，而將檔案加密就像是把文件軋碎，都是透過某個程序或是加工，使得他人無法或難以接觸到某項資訊的內容，所以單純地使用程式加密檔案，也不能因而就能受有隱私權的保障[153]。據此，執法官員不需要令狀，就可以將軋碎的紙片拼湊回為文件，也可以利用程式或軟體，破解加密後的檔案，將之還原為人們能夠理解的資料型態[154]。

4. 小結

從前述的幾個案件可以知道，加密檔案很難與上鎖的容器類比。從加密技術的性質及運作的原理來看，加密檔案更加近似於以外國語言進行的交談、裝載在行李中的毒品、或是軋碎後的文件。這三者共同之處是，雖然已經處置或處理，人們無法了解訊息的內容或袋中的情狀，但還是可以接觸得到本人不欲為他人所知悉的訊息，所以不能主張合理隱私期待。也因此，警察可以透過翻譯、警犬或拼湊，了解訊息的內容，無須向法院聲請令狀[155]。

---

[152] *See* California v. Greenwood, 486 U.S. 35, 39-41 (1988).

[153] Kerr, *supra* note 52, at 513-15.

[154] 不可諱言地，碎紙機及加密技術還是有著不盡相同的地方。舉例來說，人們將文件碎成紙片及檔案加密的目的不同。前者是希望透過碎紙機的處理，使他人（甚至是包括自己）難以再查看文件的內容；但在後者，將檔案加密的目的是為了將可以接觸到檔案者限制在一定的範圍之內（持有金鑰者），而不是讓任何人都無法再看到檔案內的資訊。也因此，加密的檔案會有相對應的金鑰，但碎紙機不會有還原機制。此外，在軋碎後的紙張上，或多或少還是可以看到一些文字或是符號，但檔案在加密後，是完全無法接觸到其中的任何資訊。不過，兩者雖然有著這些不一樣的地方，但是就將原本人們可以知悉的訊息轉變為無法理解的作用來說，加密技術及碎紙機還是可以幫助我們理解其與隱私權益間的關係。

[155] 從結論上來看，*Scott*案及*Longoria*案這兩個案件判定，與前述的權利基礎模式（參、

加密檔案類似於前述 3 種情形。人們還是看得到加密後檔案的內容，只是因為加密技術使用，無法理解其中意義，所以檔案持有人不能僅因為使用了加密技術，對檔案就能夠主張隱私權。是以，在合法取得檔案後，執法官員不需要事先獲有令狀，就可以破解其上的加密或所設置的密碼。

陸、政策上的論據

或許會有論者主張，在人們大量使用電腦，各樣的資料都已經數位化的時代，過往的理論或是判決所建立的法則，不能繼續援用，必須要有所修正或是限縮，以周延的保護人們的隱私權益。例如，聯邦最高法院在 *Riley v. California* 案[156]，便判定警察不能依附帶搜索的規範，查看在被拘捕人身上所發現及扣押的行動電話。其中的原因之一就是，行動電話不是人們隨身攜帶的香煙盒、名片夾或皮包等物件所能夠類比[157]。在 *Carpenter v. United States* 案[158]中，聯邦最高法院也拒絕在基地台位置資訊的調取，直接適用第三人法則。認為加密檔案的破解沒有令狀程序的適用，對於人們的隱私保護不周，會有不當侵害人們隱私等權益的問題。這樣的看法，著重於人們私密訊息的保障，值得肯定。不過，細究之下可以知道，這可能是不必要的疑慮。

詳細地來說，從技術及政策層面來說，即使容許執法官員不需要令狀就可以破解加密技術，也不會就犧牲了人們的隱私權益或是破壞令狀程序。這是因為，與向法院聲請令狀相比較，破解密碼本身是更為複雜，更耗費執法機關的資源、成本及人力的手段。破解密碼需要耗費極大量的電腦系統資源（運算能力），以 128-bit 的金鑰來說，即使是使用超級電腦，也必須要耗

二、（四））的隱私權判斷基準相一致。詳細地來說，依照權利取向的概念，在這3個案件中，由於Soctt沒有權利可以阻止國稅局的官員撿拾其丟棄的軋碎文件，並將之拼湊還原，Longoria沒有權利可以反對執法官員將錄下的對話翻譯為英文，所以這幾位被告都無法主張聯邦憲法第四增修條文的權利。

156 Riley v. California, 573 U.S. 373 (2014).

157 *Id.* at 393.

158 Carpenter v. United States, 138 S. Ct. 2206 (2018).

費億萬年的時間，才有辦法破解[159]。但相對地，電腦使用者很輕易地就可使用比 128-bit 更強或是更長的密碼（金鑰）來保護自己的資料、文件、檔案或是往來的通訊。相較於破解加密檔案，必須要有特別的電腦設備，需要極長的時間，相較之下，令狀的聲請程序簡便許多，偵查官員也較為熟悉。這一個現實上的因素，會促使偵查機關只會在確實存在有相當理由的案件中，才會試圖破解加密後的資料，而不是動輒破解偵查中所發現的所有加密檔案，私密資訊也因此不會被他人所得知。由於加密技術能夠給予使用者極強且有效的實質及技術上的保護，能夠避免未持有金鑰的第三人接觸到檔案的內容，所以破解加密檔案本身不適用令狀原則的結論，並不會有造成不當侵害人們隱私權益的疑慮。事實上，在日常生活中，真正能夠有效保護人們隱私，使他人（包括國家機關在內）無法得知其不欲為外人所知的事項者，常常是技術本身，而不是法律或是憲法的規範[160]。

第二個無需過慮隱私保護的原因是，執法機關還是必須要以合於令狀程序，或是合法的方式取得加密檔案[161]。亦即，即使檢警官員毋須事先向法官聲請令狀，就可以破解加密檔案，警察還是必須要以合法的方式（如事先獲有令狀），取得加密檔案（密文），才能夠破解密碼。認為人們對於加密技

---

159 *See* Bonin, *supra* note 37 at 503; Lauzon, *supra* note 37, at 1318-19.

160 *See* United States v. Jones, 565 U.S. 400, 429 (Alito, J., concurring) (2012). 不過，科技在很多時候，都是中性的，可以用以保護人們的私密資訊，也可以被用來刺探他人的祕密。現在如銅牆鐵壁般的加密技術，隨著電腦科技的一日千里，可能會變成不堪一擊。舉例來說，日趨成熟的量子電腦有著驚人的運算能力，可以在8個小時內便破解1,028-bit的金鑰。*See How Quantum Computer Could Break 2,048-bit RSA Encryption in 8 Hours*, COMMUNICATIONS OF THE ACM (June 5, 2019), https://cacm.acm.org/news/237303-how-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/fulltext (last visited Oct. 13, 2021). *See also* Stephen Shankland, *Quantum computers could crack today's encrypted messages. That's a problem*, CENT (May 24, 2021), https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem (last visited Oct. 13, 2021). 余至浩（08/12/2020），〈【臺灣資安大會直擊】為對抗量子電腦攻擊手法，後量子加密PQC演算法有望變成未來全球加密與數位簽章新標準〉，iThome，https://www.ithome.com.tw/news/139334（最後瀏覽日：10/30/2023）。

161 Kerr, *supra* note 52, at 531-32.

術的使用本身，不能主張合理隱私期待，並不代表偵查機關就因而可以違法取得任何的加密檔案，完全無須遵循令狀原則的要求。舉例來說，警察違法搜索嫌疑人的身體，在其身上發現及扣押隨身碟，其中儲存有加密的檔案，破解後所取得的明文，還是違反了令狀原則，會有證據排除法則的適用。相對地，如果警察是在公開的討論區上取得任何人都可以下載的加密檔案，或在本人同意後，取得加密的檔案，才可以破解檔案的加密，讀取還原後的訊息（明文）。是以，認為破解加密檔案本身不需要事先取得令狀，並不等於執法機關就可以完全不受令狀程序的控制，依前述的結論，人民的隱私權益還是受到了完整且必要的保護。

柒、結 論

訊息的加密有著悠久的歷史，但在今日，不僅有著非常不同的樣貌，也更為廣泛地為人們所使用。歸納整理先前的討論可以知道，隱私並不是訊息或是事物不被他人知悉的高度可能，也因此，不能因為檔案在加密後，很難被破解，他人幾乎不可能了解到其中的內容，就認當然可以主張合理隱私期待。在有共同使用人的案件類型中，電腦所設置的密碼所顯示的是一個人不欲與他人共用電腦或是其中檔案，所以共同居住或是共用電腦之人沒有同意警察官員查看設置有密碼的電腦或是檔案的權限。亦即，單純的檔案加密，只是決定其持有人是否能主張隱私權的因素之一，並不是充分條件，不能認為，只要將檔案加密，就當然享有隱私權。上鎖的封閉容器經常被用以類比加密檔案，但在分析後可以知道，兩者在本質上有其不同，因為加密後的檔案並不是看不到其中的內容，而是無法了解訊息的意思，但容器中的事物是因為物理的屏蔽，完全阻隔了人們的視線。相較之下，加密檔案應更類似於使用外國語言交談、行李中的毒品或是軋碎的文件，也因此，加密檔案的破解就像是翻譯外國語言、警犬的嗅聞及拼湊軋碎的文件，不構成隱私的侵害，沒有令狀程序的適用。另外，從政策的角度來說，加密技術本身提供了使用者非常實質有效的保護，取得加密檔案本身還是必須要合於令狀程序（如合

法扣押電腦或是行動電話，或是合法通訊監察取得即時通訊的內容），所以認為加密檔案的破解不構成搜索，不需要事先獲有法官同意，並不會有隱私權利保障不足的疑慮。

隨著電腦科技的進步及普及，在執法上勢必會碰到加密檔案及其破解上的問題及需要。日前法務部所提出的科技偵查法草案便就此有相對應的規定。大抵來說，我們贊同草案的立場。亦即，只要是檢警機關可以合法地針對儲存裝置（如隨身碟）、數位設備（如行動電話或電腦）或檔案為搜索扣押，就可以破解其上所設置的加密，只是何以執法官員可以逕自破解密碼或其他保護措施，並沒有清楚的說明，也就留有說理上的闕漏。這一篇論文試著從幾個不同的角度解析及回答此一問題，提出論理的基礎及依據，於日後法制在形成或建置時，供作立法者參考，也對於相關的研究成果累積，聊盡棉薄。

參考文獻

一、中文部分

王兆鵬（2000），《搜索扣押與刑事被告的憲法權利》，自刊。

--------（2004），《新刑訴・新思維》，元照。

王兆鵬、張明偉、李榮耕（2022），《刑事訴訟法（上）》，6 版，新學林。

中國哲學書電子化計劃，《六韜·龍韜·陰符及陰書》，載於：https://ctext.org/liu-tao/zh。

-------- 《武經總要・武經總要前集・字驗》，載於：https://ctext.org/wiki.pl?if=gb&res=817018。

李榮耕（2008），〈Yes, I do!：同意搜索與第三人同意搜索〉，《月旦法學雜誌》，157 期，頁 102-125。

--------（2015），〈科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展〉，《臺大法學論叢》，44 卷 3 期，頁 871-969。https://doi.org/10.6199/NTULJ.2015.44.03.04

--------（2016），〈數位資料及附帶搜索：以行動電話內的資訊為例〉，《臺北大學法學論叢》，100 期，頁 245-322。

楊雲驊（2007），〈未告知證人拒絕證言權之法律效果：評最高法院九五年臺上字第九〇九號、九五年臺上字第二四二六號、九六年臺上字第一〇四三號判決〉，《台灣法學雜誌》，99 期，頁 157-176。

溫祖德（2015），〈行動電話內數位資訊與附帶搜索：以美國聯邦最高法院見解之變遷為主〉，《月旦法學雜誌》，239 期，頁 198-220。

二、英文部分

Amitay, D. (2011, June 14). *Most Common iPhone Passcodes.* Daniel Amitay Blog. http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes.

Bonin, A. C. (1996). Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation. *University of Chicago Legal Forum, 1996*, 495-517.

Brady, S. (1997). Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication. *Harvard Law Review*, *110*(7), 1591-1608. https://doi.org/10.2307/1342181

Couillard, D. A. (2009). Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing. *Minnesota Law Review*, *93*, 2205-2239.

Crain, N. A. (1999). Bernstein, Karn, and Junger: Constitutional Challenges to Cryptographic Regulations. *Alabama Law Review*, *50*(3), 869-909.

Edgett, S. J. (2003). Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy. *Pepperdine Law Review*, *30*(2), 339-366.

Fraser, J. A. III (1997). The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution. *Virginia Journal of Law & Technology*, *2*, 1-45.

Froomkin, A. M. (1995). The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution, *The University of Pennsylvania Law Review*, *143*(3), 709-897. https://doi.org/10.2307/3312529

Gilligan, F. A., & Imwinkelried, E. J. (1998). Cyberspace: The Newest Challenge for Traditional Legal Doctrine. *Rutgers Computer & Technology Law Journal*, *24*, 305-343.

Hricik, D. (1998). Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail. *Georgetown Journal of Legal Ethics*, *11*, 459-508.

Kerben, J. (1997). The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Genie, *CommLaw Conspectus*, *5*, 125-152.

Kerr, O. S., & Schneier, B. (2018). Encryption Workarounds. *Georgetown Law Journal*, *106*, 989-1019. https://dx.doi.org/10.2139/ssrn.2938033

Kerr, O. S. (2001). The Fourth Amendment in Cyberspace: Can Encryption Create A "Reasonable Expectation of Privacy?". *Connecticut Law Review*, *33*, 503-533.

-------- (2005). Searches and Seizures in a Digital World. *Harvard Law Review*, *119*, 531-585.

-------- (2007). Four Models of Fourth Amendment Protection. *Stanford Law Review*, *60*(2), 503-552.

-------- (2009). The Case for the Third-Party Doctrine. *Michigan Law Review*, *107*(4), 561-602.

LaFave, W. R. (2004). *Search and Seizure: A Treatise on the Fourth Amendment* (4th ed.). Thomson West.

Lauzon, E. (1998). The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues. *Syracuse Law Review*, *48*, 1307-1364.

Lennon, T. B. (1994). The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?. *Albany Law Review*, *58*, 467-508.

Nguyen, T. (1997). Cryptography, Export Controls, and the First Amendment in Bernstein v. United States Department of State. *Harvard Journal of Law & Technology*, *10*(3), 667-682.

Pilkington, L. M. (1996). First and Fifth Amendment Challenges to Export Controls on Encryption: Bernstein and Karn. *Santa Clara Law Review*, *37*(1), 159-211.

Post, R. (2000). Encryption Source Code and the First Amendment. *Berkeley Technology Law Journal*, *15*(2), 713-723. https://doi.org/10.2139/ssrn.238191

Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119183471

Shankland, S. (2021, May 24). *Quantum computers could crack today's encrypted messages. That's a problem*. Cent. https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem

Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Fourth Estate & Doubleday.

Slobogin, C., & Schumacher, J. E. (1993). Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society". *Duke Law Journal*, *42*(4), 727-775. https://doi.org/10.2307/1372714

Suro, R., & Corcoran, E. (1998, March 30). U.S. Law Enforcement Wants Keys to High-Tech Cover. *Washington Post.*https://www.washingtonpost.com/wp-srv/politics/special/encryption/stories/cr033098.htm

The Decryption of Encrypted Files in Criminal Procedure

Rong-Geng Li[*]

Abstract

Computers have become an integral and essential part of our daily lives. A huge amount of digital data is exchanged among devices and stored in various storage types. With this increased reliance on technology comes the growing concern for data security and privacy. In this digital age, where personal and sensitive information is constantly being transmitted and stored, it becomes imperative to protect this data from unauthorized access. One way to achieve this is through the use of encryption technology. Encryption is the process of converting plain text into a code to prevent unauthorized access. This technology is widely used to secure data, but unfortunately, it can also be exploited by criminals to hide illegal activities and information. This makes it even more challenging for law enforcement agencies to carry out criminal investigations. While encryption provides a certain level of security, it does not automatically grant individuals privacy rights. In fact, the use of probability theory is not a suitable explanation for privacy. Encrypted files should not be equated with locked containers such as rooms or suitcases. The contents of encrypted files may be visible, but their meaning may not be understandable. Decrypting encrypted files is similar to interpreting a conversation in a foreign language or searching bags with sniffer dogs. Moreover, encrypting files does not provide absolute privacy protection. Law enforcement agencies are allowed to decrypt encrypted files that have been legally obtained, without obtaining a warrant in advance. In conclusion, while encryption technology is an effective tool for securing data, it does not provide complete privacy protection. It is important for individuals to be aware of the limitations and to adopt a multi-layered approach to data security and privacy.

[*] Professor of Law, National Taipei University.
E-mail: ronggengli@gmail.com

This may include using encryption technology, implementing strong passwords, and regularly updating software to stay ahead of potential security threats.

Keywords: privacy, encryption, decryption, crack, reasonable expectation of privacy, search, warrant requirement