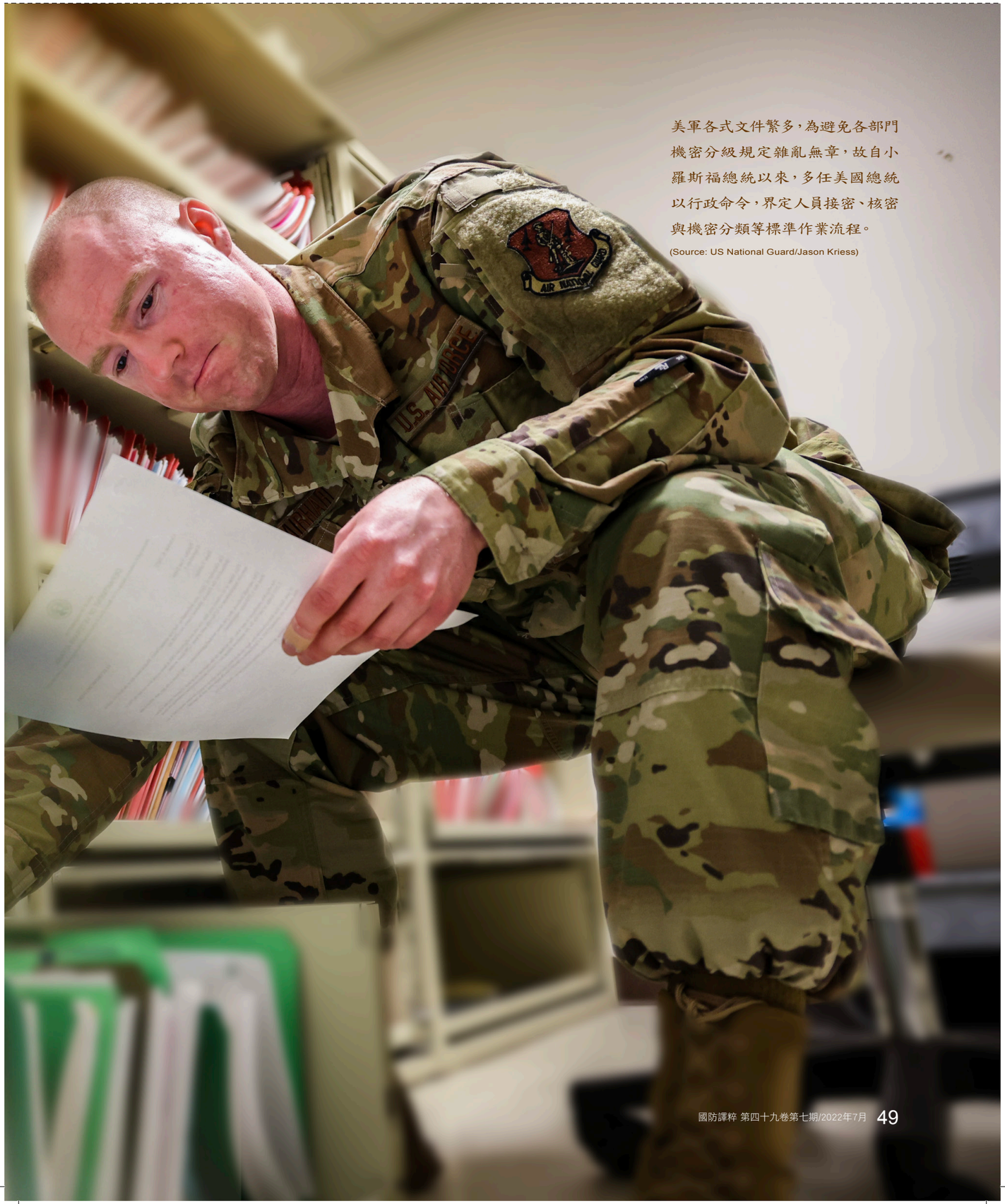
作者/Oona A. Hathaway　譯者/黃文啟　審者/馬浩翔

保密作為與國家安全

Keeping the Wrong Secrets: How Washington Misses the Real Security Threat

取材/2022年1-2月美國外交事務雙月刊(*Foreign Affairs*, January-February/2022)

美國花費鉅資與龐大人力將許多資料列爲機密，但事實上卻保密過度，結果反而使美國政府面對爲數過於龐大的機密資料，而陷入無法識別眞正安全威脅的危機。



美軍各式文件繁多，為避免各部門機密分級規定雜亂無章，故自小羅斯福總統以來，多任美國總統以行政命令，界定人員接密、核密與機密分類等標準作業流程。

(Source: US National Guard/Jason Kriess)

美國保有許多祕密。2017年，也就是在資料完整的最後一年，大約有400萬通過安全查核的美國人，將約5,000萬份文件列為機密，而美國納稅人須為此支付約180億美元的稅金。

筆者也曾在某段短暫期間是那400萬人之一。從2014年到2015年，在我替美國國防部法務長工作時，該項職務賦予我「絕對機密」等級的安全查核資格。在接任此職務前，我認為自己所會接觸到的所有機密文件，一定是只有那些經過嚴謹背景查核，並且被評比為能寄予信任者才能接觸的重要國家安全機密。但筆者後來卻相常驚訝地發現，在閱覽多數機密文件後，其中內容事實上與網路上可取得的資料並無太大不同。當然有某些例外：例如筆者比世界上其他人早幾小時甚或幾天知道某些事件，還有由特定情報管道所提供的資訊。但絕大多數作者所看過的機密資料，讓人驚訝的是其資料本身沒有什麼讓人驚訝之處。

美國在作機密等級分級時，其理念係基於政府所能取得某些重要資訊，是民間百姓或組織無法取得，或至少無法容易取得者。然而，漸漸地，美國政府情報管道相較私人情報管道已喪失優勢。在包含地理位置追蹤裝置、物聯網和商用衛星等新監視與監控科技協助下，民間目前可獲得的資訊，往往比政府所取得的資訊更好——有時甚至好上許多。

與此同時，這些科技也衍生出一個截然不同的新威脅：亦即可供外來勢力加以利用的眾多個人資料，其中有許多資訊更可快速取得。每一筆新資訊，就其本身而言，看似不太重要，但將其組合起來，這些片段可以讓外在敵人對於多數美國人生活擁有前所未有的深入瞭解。

但美國至今卻仍未開始針對保護資訊調整現有制度，仍將重點放在保護過多根本不具真正重要性的機密，視政府資訊如稀世珍寶，反而讓隱私資料幾乎完全未受保護。此種過度強調保護機密，卻犧牲個人隱私的作法，並非僅只是缺乏效率的問題。其損及美國民主制度，也對美國國家安全造成日益嚴重的危害。

間諜傳染病

美國政府並非向來如此保密到家。事實上，在20世紀更迭之際，其甚至連正式全國性機密保護制度都沒有。一直到日本在1905年日俄戰爭中擊敗俄羅斯，震撼所有西方國家，並且顯示亞洲已經出現一個有能力挑戰歐洲強權的新區域性強國，情況才有所改變。日本過去向來禁止百姓移民，但到1886年時卻決定取消這項限制，正值其軍事力量躍昇之際。到1908年，已經有大約15萬日本移民進入美國。

隨著新移民數量不斷增加，美國各報開始報導某些消息，如《亞特蘭大憲法報》(*The Atlanta Constitution*)在1911年就曾報導有關「日本間諜在菲律賓群島、夏威夷和美國本土各地活動頻繁，忙著繪製火砲、雷區和其他防衛武器兵要位置圖」。《信使日報》(*The Courier-Journal*)則詳細報導一篇日本在洛杉磯、波特蘭及普吉特海灣(Puget Sound)周邊港口進行縝密間諜行動的專文，包含謠傳「日本陸軍省的探員，以居住在當地的鐵路部門勞工或僕役家庭作為掩護，守在太平洋岸的各座大型鐵路橋附近」。這些故事都相當

引人入勝——但很可能絕大多數都是空穴來風，就如同廣為人知的故事，稱日裔糖果店主人實際上是繪製地圖的人、日本漁民實際上是在量測港口水深，還有日裔理髮師從那些毫無戒心的顧客蒐集軍事機密。

美國國會議員對這些消息深感戒懼而決定採取行動。《國防祕密法》(*The Defense Secrets Act*)遂於1911年通過，成為第一部將間諜行為入罪的美國法律。其內容要求「任何人……在未獲正當授權下，持有、取得或製造、或企圖持有、取得或製造任何其無權擁有之任何國防相關文件、繪圖、照片、攝影底片、計畫、模型或消息」得予以罰款或拘禁。

在歐洲爆發戰爭後，時任美國總統威爾遜(Woodrow Wilson)親臨國會，要求國會加強制裁煽動民眾及洩露資訊等相關行為的法令。他的種族排外主義觀點展露無遺，威爾遜宣稱，「部分美國公民，我很遺憾地必須說，出生在其他國家的旗幟之下，但卻仍為我國寬大的歸化法律所歡迎，而得以享有美國完全的自由和機會」，但他們卻「想方設法刺探所有美國政府的機密往來資訊，去幫助那些與我國背道而馳的利益」。這項演說的產物，就是1917年《間諜法》(*Espionage Act of 1917*)——一部至今(除少數條文修訂)仍構成禁止未經授權揭露美國國家安全資訊行為的主要法律基礎。這部法律涵蓋範圍極其廣泛，將所有揭露足以「用於傷害美國」的「國防相關資訊」都列為犯罪行為。

現在還有規定也將揭露國家安全機密列為犯罪行為。但什麼才是祕密呢？歷史學家認為，同樣也是在1917年頒布的《美國遠征軍第64號通用命令》(*American Expeditionary Forces' General Order No. 64*)是美國政府首次嘗試建立正式機密分級制度，以適用具國家安全價值的政府資訊。在爾後幾年間，美陸軍和海軍建立自己的機密資訊規定，衍生出各軍種部門間雜亂的機密分級規定。後來在1940年，小羅斯福總統(Franklin Roosevelt)以一紙行政命令取代這一系列各行其是的機密分級規定，要求凡在未經許可下記錄「某些有關軍事或海軍設施重要資訊」的行為均屬非法。這類規定適用於飛機、武器以及其他軍事裝備，還有書籍、手冊與其他被列屬「極機密」、「機密」或「限閱」的類似文件。

自此之後，有多任美國總統曾頒布行政命令，界定哪些資訊列屬機密、如何賦予機密，以及誰可接觸機密。最近一份全般性行政命令，是由歐巴馬總統於2009年頒布，內容律定三個機密等級——絕對機密、極機密及機密——還有多項各種規定，規範各機密等級意義為何。依據此項行政命令，機密文件以兩種方式產製：指定擁有「最初核密權限」的1,867位官員，皆得決定某項文件應予以核密，或約400萬左右經授權可接觸機密資料的人員，所產製一份使用原已核密資訊的新文件亦屬之——即所謂衍生核密。2017年，超過4,900萬份由美國政府產製的文件都屬於衍生核密類型。

保密復保密

幾乎所有曾經審視過美國機密保護制度的人，都會認為這套制度造成諸多過度保密行

為。曾經在布希政府時代擔任過「資訊安全督察室」(Information Security Oversight Office)主任的李歐納(J. William Leonard)就曾說過，超過一半以上符合機密核定標準的資訊「真的不該列屬機密」。其他人則認為此比例應該還更高。擔任過中央情報局局長的前美國國家安全局局長海登(Michael Hayden)就曾抱怨，他曾收過被列為極機密等級的「耶誕快樂」電子郵件。

造成此種過度保密現象的原因之一，就是負責核定機密的人，幾乎都被鼓勵採取偏向謹慎小心的作法──保密等級寧高勿低。當筆者在五角大廈任職時，假如自己錯將某份文件或電子郵件賦予過高的機密等級，很可能不會受到任何處份。如筆者所知，共事過的同僚從未有人因為將某份文件賦予過高機密等級而遭懲處。然而，若將某項文件賦予太低機密等級，就有可能造成嚴重專業後果──更別提可能威脅到美國國家安全。換言之，「保密到底」就是最簡單且最安全的行動方案。

保密行為還會衍生出更多保密行為，因為所有文件的核密方式必須以其內含最高機密等級的內容為核定基準。舉例來說，如果有一份十頁的備忘錄，

2019年5月，美國司法部以違反《間諜法》、獲取及公開機密文件之罪名，起訴維基解密創辦人亞桑傑，對言論自由產生寒蟬效應。(Source: Reuters/達志)

其中雖然只有一句話列屬絕對機密，這份備忘錄就必須整份被歸類為絕對機密(除非其採取「區隔標識」[Portion Marked]，意即每一個部分——例如包含標題、每段落、各要點及所有表格等——都分別賦予不同機密等級標記)。此種要求助長了無止境擴大衍生的保密措施，讓美國原本就龐雜的過度保密問題變得雪上加霜。

隱性傷害

過度保密讓民主制度付出不容小覷之代價。其中最顯著者：國家在讓敵人無法獲取其機密時，同時必須把百姓矇在鼓裡。大規模政府保密作為會損害民主制衡，因為讓大眾——且通常就是國會議員——幾乎完全難以瞭解行政部門在做什麼。

美國政府過去在進行祕密行動時，往往有驚世駭俗之舉。中央情報局的祕密處所，在小布希政府任內曾對那些涉嫌參與恐怖團體的受拘禁者肆意凌虐，如此行為完全經不起大眾監督——所以才會私下祕密運作多年。保密作為也在某些更不顯著之處破壞美國民主制度。當政府保護某些祕密時，那些祕密會造成——且有時必須捏造——謊言。當謊言曝光後，大眾對政府的信任就會大打折扣——如同2013年國家安全局約聘人員史諾登(Edward Snowdon)，揭發該局有龐大監控計畫存在，意圖截取數以百萬計美國人的電子郵件、即時訊息和行動電話資料後，就對政府威信造成重大打擊。這次曝光事件重創百姓對美國情報機關的信任，使其更難執行情蒐工作——恰與當初美國政府保密作為所望達到之目的背道而馳。

機密對於言論自由也會造成寒蟬效應。2019年5月，美國司法部以17項違反《間諜法》，獲取及公開機密文件的罪名起訴吹哨組織「維基解密」(WikiLeaks)創辦人亞桑傑(Julian Assange)。這是美國政府首度針對單一公開揭露行為提起如此多項訴訟，因而在媒體界引起恐懼，憂心美國政府可能會開始引用《間諜法》起訴新聞從業人員。如同《紐約時報》在當時的報導指出，亞桑傑被起訴的罪行恰好就是該報作為：其亦獲得與維基解密所公開之相同文件，同樣也未獲政府授權，且已公開其中部分內容，只不過《紐約時報》沒有透露告密者的姓名。

不僅是吹哨者和新聞工作者必須擔憂；離職政府官員也可能被指控違反機密保護法令。即便已經離職，公職人員如果洩露任公職期間所知悉的機密資訊，不僅可能面臨刑事訴訟，同時還會被要求必須將自己的著作(以及公開談話草稿)交付「公開前審查」。川普總統任內的美國國家安全顧問波頓(John Bolton)，就成了侵犯公開前審查流程的意外代表人物，因為他所撰寫的一本書似乎就因為政治考量而被迫延後出版。波頓絕非唯一例子。數百萬名離職政府公務員，包含筆者在內，都受到類似法規所約束。然而，受到這套制度真正傷害的並非離職政府公務員，而是公眾論述的品質，因為瞭解美國國家安全體系的離職政府公務員，經常會覺得保持完全緘默比較簡單。

過度保密行為也讓真正重要的機密難以確維。美國最高法

美陸軍預備軍官訓練團學生以手機錄下克萊門森大學老虎隊進入林肯紀念體育場(Memorial Stadium)的英姿，但有時這種表面上看似無害的資訊公開後，可能會成為國家安全的漏洞。(Source: DVIDS/Ken Scar)

院大法官史都華(Potter Stewart)在1971年下令公開俗稱「五角大廈文件」的美國國防部對美國在越南扮演角色機密歷史報告時，在其同意見解中就說，「當一切事物皆保密，就沒有何事為機密，而這套制度也就成為憤世嫉俗者或不在乎者忽視之對象，且亦將為意圖自我保護或自我吹捧之人所操弄」。過度保密作為也會讓保護美國大眾免於各種國家安全威脅的工作變得更形困難——例如，限制原本可以作為決策參考或發掘新危險因子的資訊共享行為。「911事件委員會」就發現，911恐怖攻擊事件之所以沒能在事先偵知這項陰謀即將進行的其中原因之一，就是過度保密作為：各政府機關與大眾未能分享資訊，才讓攻擊者有機可趁。該委員會主席基恩(Thomas Kean)曾表示，「公開透明會讓我們過得更好。在保護我們自己對抗恐怖主義時，最佳盟友就是知情的大眾」。

處處皆耳目

但或許保護過多機密所付出的最鉅代價，會是這種行為讓美國完全看不到某個成形中，甚或可能更具危險性的威脅：新的追蹤和監控科技讓即便是最機敏的資訊都愈來愈難隱藏。以運動應用程式Strava為例，這種軟體讓運動員可以記錄自己的跑步或自行車運動還有其他各種活動狀態，並且能將資訊與朋友分享。2017年，這種看似無

害的應用程式變成國家安全夢魘，因為某位澳大利亞學生，竟然利用美國Strava使用者資料，將似乎是阿富汗前進作戰基地和敘利亞軍事巡邏等活動畫面貼上網路。其他人則很快繪製出一處法國駐尼日軍事基地、一處義大利基地及另一個未曾公開的美國中央情報局駐吉布地據點的地圖。不久後，大家明顯發現Strava的資料不但可以用來揭露此類軍事設施的內部結構，同時只要配合某些推特文，甚至能辨識和追蹤特定個人。

數以百計的類似應用程式，每天都在追蹤不知情美國人的位置，並且由有心人士綜整資訊後加以販售。其中一家名為X-Mode的公司，在蒐集、綜整和轉售定位資料方面作得非常精細，甚至能追蹤個人裝置移動狀況，並且判斷其硬體組合項目。X-Mode公司透過其自家應用軟體蒐集此類資訊，但也付錢向使用該公司軟體開發工具及其位置追蹤程式碼的應用程式開發者收購資料。據2019年某則新聞報導內容，平均每個月X-Mode公司可以取得全球高達6,000萬人次的定位資訊。2020年底時，蘋果公司和谷歌公司雖然禁止X-Mode公司從使用這兩間公司作業系統的行動裝置來蒐集定位資訊，但類似追蹤科技仍然是隨處可見。

X-Mode是最有名的定位追蹤資料綜整者，但其絕非是唯一一家利用公開可獲資訊追蹤人們隱私生活的公司。開設於紐約市的「明視人工智慧」(Clearview AI)公司就設計出一套史無前例的臉部識別應用程式軟體，讓使用者可以上傳某些照片，然後利用從臉書、Venmo、YouTube及其他數百萬網站所擷取的300多萬張影像資料庫中比對，辨識照片中人員的身分。美國聯邦及各州執法機關就發現，這種APP軟體要比聯邦調查局用在追緝犯罪嫌犯的資料庫功能更強大。2019年，美國印第安那州警察局將一則從路人行動電話攝影畫面所擷取的影像上傳到「明視」軟體進行比對，20分鐘內就偵破某個案件。這名被辨識出犯罪嫌疑者，既沒有駕駛執照，在任何政府資料庫中也無資料，但某個人(並非嫌犯本人)將其影像畫面貼上社群媒體，還加註了此人的姓名，該名嫌犯很快就被逮捕並遭起訴。

物聯網的崛起(網路裝置)意味著蒐羅大眾日常生活之相關資訊比過去更多，其中包含諸如亞馬遜Alexa等語言指令助理所產生的大量語言資料。在2017年的報告中，美國國家情報總監柯茨(Dan Coats)將物聯網造成的網路安全弱點列為國家安全重大威脅。但這份報告僅狹隘地將重點放在精密網路工具會對汽車及醫療裝置等消費產品所造成之實質危險，而並未提到這些工具對於資訊安全所構成的威脅。2020年底時，美國國會通過《物聯網網路安全精進法》(*Internet of Things Cybersecurity Improvement Act*)，律定互相鏈結裝置的各項最低安全條件。但這項法律僅適用於販售予聯邦政府部門的裝置。平民百姓只能自求多福。而各種裝置幾乎完全不是公司蒐集個人資訊的唯一管道。臉書設計的第三方置入功能，諸如「按讚」和「留言」鍵與追蹤像素等，讓該公司的廣告夥伴可以附加其自家非臉書網頁及應用軟體。這些置入功能，除了替臉書上的夥伴蒐集資料，也讓臉書公司得以監控用戶的網路活動，無論其是否登入網站。

一個世紀前促使《間諜法》立法的間諜，大多數已由這種全面涵蓋的追蹤與監控科技所取代。假如某個應用程式就可以揭露駐防阿富汗前進作戰基地中美軍官兵的位置和身分，其同樣能揭露在維吉尼亞州朗里中央情報局總部工作的情報官員位置和身分，甚至是美國國防部長及其家屬。別再妄想派遣喬裝幹員，無論他們如何小心避免自己的身分在網路上曝光，這些人的朋友貼在臉書和Instagram網站上的照片，還有無孔不入的監視器錄影畫面等資料綜整者，與客戶能輕易取得的資料，就讓掩飾其真實身分與聯絡人幾乎不可能，更別提這些人的家屬及朋友身分與行蹤。

美國政府之所以忍住不發出警訊，部分原因在於其情報機關本身也在利用這類弱點。例如，2017年在維基解密公開的文件中，揭露中央情報局曾利用三星連網電視的弱點，利用其作為祕密監聽裝置。美國政府雖然默不作聲，然而民間產業早已達到，有時甚至超過當局蒐集資訊的能力。在衝突地區運作之非政府組織現在已能利用群眾外包方式蒐集衝突相關資訊，其精確度往往堪比美國情報機關所蒐集之資訊，甚至更高。與此同時，民間衛星公司提供精密衛星影像的訂閱管道，實際上已能涵蓋地球上任何一處。簡言之，政府當局已經不再擁有所有重要資訊的獨占權力。

馬賽克理論

在國家安全社群中，有一個名為「馬賽克理論」(Mosaic Theory)的概念，認為彼此迥異、表面上無關緊要的片段資訊，在與其他多個片段資訊結合後，就能成為重要情資。此理論正是為何大多數有權限接觸機密資訊的人，都會被告知其無法判斷何種資訊應核予機密的其中一項原因。一份看似毫無意義的文件，在結合其他資訊後，可能會讓敵人獲得馬賽克中的某個重要片段。

過去，情報分析人員會將各種片段資訊拼湊起來完成馬賽克。身為領域中的專業人士，好的分析員最後會知道什麼時候表面上無關痛癢的片段資訊可能在特定背景下相當重要。大數據發展，加上人工智慧，有望顛覆此類傳統作法。為瞭解其原因，想想零售業巨人達吉特（Target)百貨公司在約十年前的一項突破。和多數公司一樣，達吉特百貨將客戶身分識別號碼綁定其專用店卡和客戶信用卡、姓名及電子郵件帳號。在某位顧客完成購買後，會蒐集並綜整該項資訊。2012年，某位達吉特百貨的統計人員想出其可運用該項資訊，加上曾完成嬰兒登記的女性購買資訊，判斷哪些顧客可能有孕在身。例如，懷孕的女性顧客會開始購買無香精乳液，並且更有可能購買鈣、鎂、鋅等營養補充品。運用此類資訊，達吉特百貨當年得以設計出「懷孕預測分數」，計算出女性可能在其懷孕期間贈送女性可能需要之產品優惠券。此項科技直到某位憤怒的顧客提出客訴，抱怨該公司送一份明顯針對懷孕女性的郵寄廣告給其千金，這才引起大眾注意。後來，這名顧客致電道歉：「結果是我家發生一些其實我不太清楚的事。小女8月要當媽媽了。在此致歉」。

那只是某家公司在十年前利用簡單統計分析，來監控特定購買行為而已。現在試想，如果敵人能結合該類資訊與來自各種不同資料庫的類似資訊，並且運用現代人工智慧偵測樣態，會做出

什麼事。

此事很可能已經發生。中共疑似蒐集數以百萬計的美國人個資。前美國國家反情報暨安全中心(The U.S. National Counterintelligence and Security Center)主任艾凡尼那(William Evanina)在2021年初就曾提出警告，中共已經竊取八成美國人的個資，採取手段包含入侵健保公司及連上網路的智慧家用裝置。2021年4月，聯邦調查人員推斷，中共駭客可能已經從「領英」(LinkedIn)等社群媒體網站中竊取資訊，以幫助其判斷哪些電子郵件帳號為系統管理者擁有，接著他們就可以運用該資訊對微軟公司的電子郵件軟體進行網路攻擊。換言之，中共似乎已經利用非法從公開網站上獲取並竊得之資料，建立龐大的美國百姓隱私資訊資料庫。

2014年3月，中共駭客駭入存有所有聯邦公職人員個人資訊的美國人事管理署(The U.S. Office of Personnel Management)電腦網路，並且取得數十萬曾申請絕對機密安全查核資格人員檔案——包含筆者在內。雖然這些檔案非屬機密，但卻含有相當高價值的國家安全資訊：亦即通過絕對機密安全查核資訊的政府公務員身分，以及其家屬聯絡方式、海外旅遊與國際聯絡人、社會安全保險號碼，還有親朋好友的聯絡資訊。結合美國人民個人資訊的資料庫，此種資訊很可能讓中共得以判斷在擁有絕對機密接觸權限的聯邦政府公務員中，哪些人背負龐大信用卡債務、有誰在婚後使用約會應用程式、誰又有小孩在海外就學，或哪些人會在辦公室加班到很晚(可能正在執行某項重要行動)。簡言之，當美國政府浪費大量精力保護機密資訊時，其中有許多根本無足輕重，卻反而讓外人輕易取得那些具有更高國家安全價值的資訊。

表面上無關緊要、大相逕庭的片段資訊，結合其他資訊後，透過情蒐人員專業視角分析，可能成為極重要的機密情資，此即為「馬賽克理論」所隱含之概念。(Source: US Navy/Charlotte C. Oliver)

停止過度保密

現行美國國家安全體系設計來保護20世紀的機密，在建立這套制度時，最重要的國家安全資訊都掌握在政府手中。因此，設計出一套專門用來防止間諜獲得該類資訊，並且避免內部人員洩密的制度確有其理。然而時至今日，民間資訊已經超越政府。美國需要一套

能因應此種新現實條件的國家安全資訊處理作法，必須澈底改革這套不斷製造有如巨型高塔，大半為無用機密資訊的龐大國家安全制度，同時減少可輕易取得的私人資訊量。

在追求第一個目的時，美國首先應是訂定所有機密資訊十年自動解密的規則。目前，雖然所有超過25年以上的機密紀錄都應該自動解密，但此項規則卻有諸多例外，而導致多件資料超過半世紀卻仍被列為機密。例如，有關甘乃迪總統遇刺事件的2,800項機密紀錄，一直到了2017年才解密，即便在當時，川普政府仍將某些檔案持續保密。

十年解密期限應該只能有兩個例外：依據《原子能法》(Atomic Energy Act)列為「限閱資料」的資訊，以及辨別仍在世情報機關線民身分的資訊。有關解密任何其他資訊是否可能損及國家安全的決策，則應交由離職政府官員、史學家、新聞工作者以及民權倡議者所組成的獨立審查委員會加以認定。政府機關在面對其認定可能造成傷害之資訊自動解密情況時，可向該委員會申請延長保密期限──基本上，就是強迫該機關提出正當理由說明為何不遵守這項規則。藉由將解密列為基本要求，此規則將促使美國政府給予該項審查程序充足資源，並容許其能適時進行。

美國政府亦應掌握人工智慧和機器學習的能力，來發掘保密過度的案件。找出那些經常較同儕將密等資訊核定過高的公務員，告知其較其他人更常將文件核定為機密，並鼓勵他們應更審慎評估加密與否之必要性。人工智慧最終可能也將會在公務員草擬文件或電子郵件時建議機密等級，並且在完成時質疑有誤的核密決定，同時審查存檔文件的機密等級。

終結龐雜的過度保密作為，可以讓官員有更多時間以創意方式思考，解決龐大個人資料可快速獲得而形成之新威脅。華府當局剛開始可以仿傚北京當局的作法，因為中共雖然是實施侵入性監控的國家，但最近卻通過全世界最嚴格的資料隱私法──其主要目的很可能不是為了保護民眾隱私，而是防止百姓資料遭到外來敵人所蒐集與利用。這部法律適用中共內部，以及海外所有處理百姓或內部個別資料的組織與個人，管制相關資料，並且允許中國大陸百姓在資訊遭竊、濫用或扭曲時提出訴訟。藉由此種方式，該部法律將可遏止在中國大陸經營的企業，蒐集並且取得可能對外國情報部門具重要性的個人資料。換言之，中共正在對想要利用其百姓個人資料的外來強權關上大門，而美國卻在同時門戶洞開。

與此同時，美國的隱私權卻得依靠東拼西湊的聯邦與州法律，這些法律都僅針對問題一小部分，而未能涵蓋全般。多年來，公民自由團體呼籲聯邦政府應該保護個人隱私資訊，但這些呼籲多半沒有得到回應。然至今日，可以愈加清楚發現有必要保護美國人民隱私，不只是在保護公民自由，更是在保衛國家。

美國國會首先應將目前僅適用於政府擁有或使用裝置的安全要求，擴及所有網路連結裝置上。在裝置中有特定項目構成嚴重危險：亦即監控人體的裝置。這些裝置包括穿戴在身

上的體能追蹤器，同時也包含那些植入或插入身體的裝置：諸如心律調節器、心律去顫器，以及具內建感測器記錄藥品服用情形的「數位藥丸」等。為降低這些裝置在遭到駭客攻擊的不堪一擊，聯邦主管機關必須要求製造商改善其安全流程。

美國政府應提供消費者更新、更好的工具，來控制某些公司蒐集資料。華盛頓州民主黨眾議員戴貝尼(Suzan DelBene)於2021年3月提出的《資訊透明暨個人資料管制法》(*The Information Transparency and Personal Data Control Act*)，要求「加入」與「退出」同意及「以英語簡要告知其隱私權益」。這些措施當然都是針對現況的精進作為。但研究顯示，消費者通常不會閱讀公告內容，因此即便有明確個人加入與退出要求，可能都無法限制對不知情的消費者進行資料蒐集。這項研議中的法案也限制州法律的保護程度不得逾越聯邦法律，意味其實際上可能反而在某些部分降低保護措施。國會可以採取的更佳選項，應該是通過仿傚近期由加州為典範所執行之聯邦法律，加州要求企業必須尊重個人全然拒絕資料蒐集的選擇。此舉是讓控制權回到消費者身上的重要作法。

最後，美國國會應該成立獨立聯邦機關，負責監督及執行資料保護規定。美國是極少數未設立資料保護專責機關的民主國家之一。相反地，美國依賴「聯邦貿易委員會」(Federal Trade Commission)負責民眾相互對等義務。紐約州民主黨參議員陸天娜(Kirsten Gillibrand)於2021年6月提出的2021年《資料保護法》(*Data Protection Act*)，研擬成立一個「主管高風險資料作法及蒐集、處理與分享個人資料」之機關──特別是針對資料綜整者。成立此種機關也可以讓聯邦政府發展資料隱私議題專業能力，並且更快速且有效處理各種全新挑戰與威脅。

拒之於外

發明家凱特林(Charles Kettering)曾經說過，「當你把實驗室大門鎖上，你拒之於外的部分必然多過保留在內」。20世紀初，當現行保密制度開始成形時，值得保護的資訊大多存放在聯邦機關內，因此關上大門還有道理。然而時至今日，凱特林的說法比過去更貼切。民間可以取得比政府更多，並且在許多案例中是更佳的資訊，因此鎖上大門只是隔絕聯邦機關，但卻未能保護到多少值得確保的資訊。

在21世紀處理國家安全資訊真正所須採取之作法應更重視隱私。然而美國在這個人工智慧與機械學習對國家安全構成日益嚴重威脅的世界中，卻在保護尋常公民資訊方面幾無所作為。美國耗費百億鉅資保護機密資訊，但其中泰半早已能從公開管道中快速取得。卻幾乎從未幫助對美國公民，包含位居要津的公職人員，防止其隱私生活遭到側錄、追蹤與揭露。因為此種作法，美國正將國家安全馬賽克的片段資訊四處散落，而讓敵人加以蒐集與拼湊。

作者簡介

Oona A. Hathaway現任耶魯大學法學院國際法教授。