國家安全與人權──史諾頓事件的省思*

施正鋒

東華大學民族發展暨社會工作學系教授

> For me, in terms of personal satisfaction, the mission's already accomplished . As soon as the journalists were able to work, everything that I had been trying to do was validated. Because, remember, I didn't want to change society. I wanted to give society a change to determine it should change itself.
>
> All I wanted was for the public to be able to have a say in how they are governed. That is a milestone we left a long time ago. Right now, all we are looking are stretch goals.
>
> Edward Snowden（Gellman, 2013）

前言

英國《衛報》（*Guardian*）、以及美國《華盛頓郵報》（*Washington Post*）在 2013 年[1]中揭露美國國家安全局（National Security Agency）秘密蒐集通訊元資料[2]的程式 PRISM，主要的功能是在儲存境外非美國人[3]的網際通信資料。這些報導是依據 NSA 外包公司 Booz Allen Hamilton 僱員史諾頓（Edward Snowden）所洩漏的檔案，駭人聽聞，尤其是連德國總理梅克爾（Angela Merkel）、以及巴西總統羅塞夫（Dilma Rousseff）都遭竊聽。根據史諾頓的說法，原本 NSA 及其他情報單位是爲了軍事作戰、及國家安全而進行海外情報的蒐集，然而，他發現 NSA 竟然以國家安全爲由，想盡辦法蒐集所有人的通訊資料，有系統地進行攔截、篩選、儲存、測度、以及分析，已經超越法律所允許的範圍；由於擔心這些

---

* 發表於中華安全科技與管理學會舉辦「雲端技術與安全管理研討會」，中壢，中央大學太空及遙測研究中心 2014/6/16-17。

[1] 其實，《紐約時報》（*New York Times*）早在 2005 年底就有揭露，小布希（George W. Bush）總統在 2002 年以秘密行政命令，要求 NSA 未經法院授權、非法監控國人的電話、及電子郵件（Sinha, 2013: 3）。

[2] 英文是 metadata（或是 non-content），又稱爲「資訊的資訊」（information on information）、或是「通訊資料」（communications data），包含通信的對象、內容、以及時間，也就是所謂的「電話數據紀錄」（call data record/call detail record, CDR）（Wikipedia, 2014a; Newell, 2014: 6, 8）。

[3] 在這裡，所謂的「美國人」，我們沿用 Margulies（2014: 2137）的寬鬆用字 U.S. person，包含美國公民、以及具有永久居留權者。

資料被濫用，他決定讓大眾來決定是非曲直，而非政府的雇員就可以作決定（Landau, 2013: 66）。

消息傳來，輿論譁然，NSA 局長 Keith Alexander 將軍承認史諾頓已經給美國造成無法修補的損害，參議院情報委員會主席 Dianne Feinstein 甚至於認爲史諾頓之舉是叛國的行爲[4]。一般而言，洩密給媒體很少被視爲犯罪行爲，不過，美國政府已經以間諜罪通緝史諾頓；前美國副總統高爾（Al Gore）看法不同，認爲 NSA 的監控行爲已經違法違憲，特別是美國憲法第四修正案的規定。先前，情報局長 James Clapper 才在參議院作證實信誓旦旦表示，NSA 並未刻意蒐集無數美國人的資料[5]，因此，當檔案揭露以後，參議員 Rand Paul 指控局長公然跟大眾說謊、以國家安全名義違法，而史諾頓才是說出真相（Landau, 2013: 67）。

在過去，監聽採用人工方式、相當費時又費力；然而，由於電訊科學的進步，特別是由對比到數位，政府監聽的技術超乎一般人的想像，隨之而來的就是政治、以及道德上的爭議。早期通訊方式是靜止的，元資料看起來沒有必要保護，加上這些是由電話公司所保有，不像實質內容需要憲法保障，因此，政府可以恣意取得，不需提供相當的理由（probable cause）；然而，當行動電話出現以後，法律對於隱私的保障就顯現左支右絀。尤其是在九一一事件（2001）爆發後，聯邦調查局可以使用「國家安全令」（national security order）要求調閱通訊紀錄，不必經過法院核准（Landau, 2013: 68）。

照說，監聽的人員應該是依據權限決定可以獲得多少資料也就是說，並非所有雇員都可以知道任何資訊、爲所欲爲；然而，根據史諾頓的說法，只要找得到電子郵件地址，任何分析師都可以隨時監控世界上任何人的所有資訊，包括聯邦法官、甚至於總統[6]，橫行無阻（Bamford, 2013）。依據史諾頓洩漏 NSA 督察長

[4] 其實，NSA 的高級官員 William Binney 早在 2001 年，因爲目睹政府違法蒐集國人的情資，憤而辭職抗議；局長 Alexander 當然矢口否認，宣稱 NSA 只是一個蒐集外國情報的單位（Bamford, 2013）。

[5] James Clapper 後來被抓包，竟然大言不慚地說，先前並未說謊，而是使用「比較不假」（least untruthful）的方式回話（Bamford, 2013）。

[6] 根據媒體報導，擔任參議員的歐巴馬在 2004 年也是竊聽的對象（Bowden, 2013: 14）。

在 2009 年所撰寫的內部報告，差不多世界上三分之一的國際電話必須在美國中轉，也就是經過一些「咽喉點」（choke point），因此，美國剛好是國際電話交換轉接的通衢；此外，幾乎全球所有的網際網路的通訊都經過美國，只有不到1%跳過美國，這種主場優勢讓 NSA 有上下其手的絕佳良機，不需要申請任何搜索票（Bamford, 2013）。

最駭人聽聞的是「上游設施」（UPSTREAM）、以及「稜鏡計畫」（PRISM[7]）：首先是 NSA 在通訊公司架設秘密機房，使用前者直接從承載網際網路的光纖來攔截、過濾、及複製通訊內容，可以取得 80%的資料[8]；接著透過九家美國雲端供應商的伺服器[9]，包括微軟、雅虎、谷歌、臉書、網路聊天（Palatalk）、YouTube、Skype、美國線上（AOL）、以及蘋果公司，運用後者蒐集即時通訊、或是既存的資料，以確保滴水不漏；接著再運用搜尋程式加進行資料探勘（data mining）般的分析檢索萃取，譬如 X-KEYCORE（維基百科，2014b; Bamford, 2013; Bowden, 2013: 16）。

正如英國小說家歐威爾（George Orwell, 1949）在《一九八四》（*Nineteen Eighty-Four*）所描述「老大哥正在看你」（Big Brother Is Watching You）的作法，我們在過去所看到的是極權政權對於所有老百姓、或是威權政權對於異議份子的控制，也就是政治偵防。我們現在卻發現，成熟民主國家所進行的大規模監聽，已經不是針對特定的對象，也就是已經犯罪、或是即將犯罪的嫌疑犯，譬如恐怖份子、或是黑社會，而是對所有的通信使用者作地毯式的搜索，只要使用網際網路就是監聽的對象不管是電子郵件、瀏覽網頁、雲端運算、或是社交網絡，通通

[7] 這是 Planning Tool for Resource Integration, Synchronization, and Management 的簡寫。英國的政府通訊總部（Government Communications Headquarters, GCHQ）也有類似的 TEMPORA，據說被植入英國西南海域的 200 條左右光纖纜線（Bigo, et al., 2013: 13）。我們由附錄 1 的全球海底電纜分佈圖可以看出，這是通往美洲的大衢，密度相當高。

[8] 基本上，這是使用「分光鏡」（beam splitter）的原理，以稜鏡的方式複製通訊資料，分流到 NSA 的機房。根據史諾頓所洩漏的 NSA 在 2009 年機密報告，NSA 跟美國三大電話公司有秘密合作協議，可以取得 81%進出美國的電話紀錄，雖然沒有指明，外人可以對號入座大概是 AT&T（39%）、Verizon（28%）、以及 Sprint（14%）（維基百科，2014b; Bamford, 2013; Klein, 2006）。

[9] 表面上說是「公私伙伴關係」（public-private-partnership, PPP），其實是半強迫性質（Bigo, et al., 2013: 3）。

成爲嫌疑犯。目前，NSA 每天監控世界 20 億的電子郵件、電話、以及其他通訊方式（Sinha, 2013: 2）。

那麼，政府的國家安全措施是否會危害我們的民主自由？情治單位的作爲是否受到有效的監督、以達到起碼的課責？根據憲政主義（constitutionalism）的基本精神，「爲了保障人民的權利必須限制政府的權力」。當然，並非所有的權利是絕對的，譬如說，如果政府爲了國家安全，有時後必須侵犯人民的隱私，這時候，公民作爲資訊的擁有者、以及政府做爲安全的捍衛者，兩者之間要如何取得平衡？

早先，大家的關注是國家如何限制、或是防止人民使用新的通訊科技，也就是「自由表達意見的權利」（right to freedom of opinion and freedom）現在，當科技的進步允許政府可以輕易對人民的通訊加以取得、儲存、彙整、檢索、以及傳遞，焦點則在如何改善各國的通訊法規，強化對於行政部門監聽的司法授權、或是立法監督，亦即包括個人的「隱私權」（right to privacy）的關懷（Human Rights Council, 2011; 2013）。接下來，我們先將從人權的隱憂著手，接著分別從美國、歐盟、以及國際人權公約，考察通訊隱私權的保護機制，再作簡單的結論。

人權的隱憂

隱私權的基本理念，是假設每個人對於自己的公共呈現、以及私人生活不同；也就是說，每個人應有自己的私人領域，可以自主發展、與人互動、以及享有自由，不受國家干預、也不受其他不請自來的干擾（Redmond, 2014: 738; Human Rights Council, 2013: 6-7; PoKempner, 2014: 2），也就是 Warren 與 Brandeis（1890）所謂「保護私生活不被打擾」（to protect the privacy if private life）的權利。

我們可以把政府情治或是國安單位所從事的電信監聽，大致上解析爲目的（why）、對象（who）、以及方式（how）。如果不提威權、或是集權國家的社會控制，民主國家在傳統上所關注的是犯罪的防範、或是處罰；然而，目前在

國家安全、或是反恐的大目標下，爲了要達到滴水不漏，反而模糊原本的用意。同樣地，不管是監聽的對象（包括外國人）、還是方式，原本是要將罪犯繩之以法、或是嚇阻符合側寫的嫌疑犯，現在卻是不需要事先申請搜索證，不僅是監聽一些特定團體，甚至於沒有特定對象、大小通吃，簡直是拿大砲打小鳥（圖 1）。

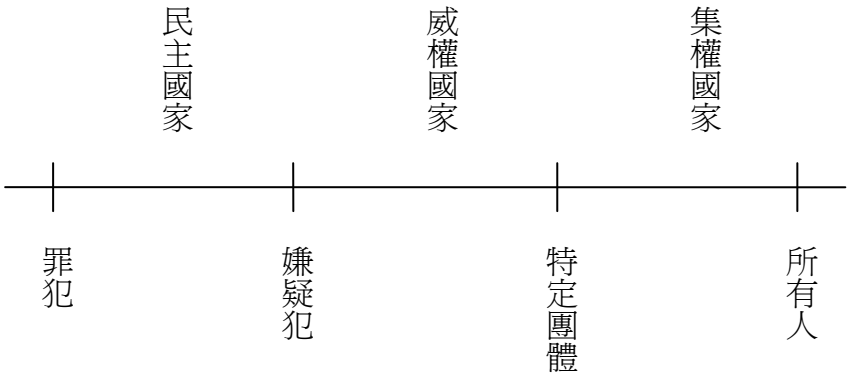


圖 1：政體與監控對象

就監聽的對象而言，警察國家與民主國家的差別在於：前者緊盯著異議份子，而後者則只注意嫌疑犯。即使是在冷戰時期，美國的內部監控至少是針對民權運動者、共產黨（1950 年代）、以及反戰份子（1960-70 年代），而採用的非法手段頂多是線人、拆信、竊聽、或是闖空門；然而，現在的電子監控卻是針對所有人，彷彿集權政府的作法（Bigo, et al.: 2013: 6）。不禁令人擔心，國家是否有能力保障人民的隱私權？現有的人權保障機制是否充分？甚至於民主體制是否遭到侵蝕？

基本上，西方民主國家有起碼的共識，也就是不應該從事大規模監聽，而且應該接受某種形式的監督，不管是司法、還是立法。因此在 1990 年代，歐洲國家發生幾件便衣警察滲透政黨的醜聞，涉案者無不因爲侵犯人權黯然下台：譬如西班牙成立反恐組織 GAL（Groupos Antiterroristas de Liberación）以對抗巴斯克游擊組織 ETA，內政部長在 1996 年被判有罪下獄；法國情報局 Renseignements Généraux 因爲涉及非法竊聽、甚至於暗殺行動，差一點被解散；在 2013 年，盧森堡總理因爲涉及非法竊聽政敵，公開宣佈要去職（Bigo, et al., 2013: 7）。

然而，經過九一一事件，一切改觀，對於情治單位監控的監督有實質上的困難：最主要的裡由是這些行動往往跨國的，彼此交換情報、相互掩護，單一國家的法規無從約束；再來是所謂的「機密」說詞，一旦相關檔案被列爲機密，調查工作就受阻了；接著，有時後很難區分國家利益與特定政治團體利益，監督者爲免投鼠忌器；最後，由於監控竊聽程式是全球性的，對象是境外的他國公民，不要說受害者渾然不自覺、連他們的政府很可能也被埋在鼓裡，因此，這已經不是隱私權的保護而已，而是自己國家存在是否還有意義的問題。當然，由科技日新月異，有時外行人分不出到底這是可以接受的特定嫌疑對象監控、還是通盤的老百姓資料探勘，外部監督者徒呼奈何（Bigo, et al., 2013: 7-8）。

情治單位爲了規避監督，通常有兩種策略：首先，他們會堅稱監控行動完全按照規定行事、而其他國家的伙伴也一定事先會獲得知會，此外，彼此的反恐合作會儘量不要作大、監視的網際網路協定位址限於特定個人，而且所獲得的資料只是用來查證嫌疑，因此，絕對不是在進行大規模的資料探勘。接著，即使不是在進行反恐監控任務者，他們會宣稱從事光纖安全保護的工作，有權定義國家安全與隱私權的界線，也知道國際規約、國際協定、或是國內法的分際，因此可以免於受罰；也些人甚至於主張，即使是民主國家也有可能面對內部的敵人，因此不得不逾越法律，這時候，唯有總統、或是總理應該知道他們的行動，這是行規，連司法都不應該過問（Bigo, et al., 2013: 8-9）。

相對之下，人權組織、以及媒體工作者無法接受國家安全至上的藉口：首先，他們認爲民主就是法治，沒有人可以超越，因此主張司法單位應該積極介入；此外，如果有必要進行監控，也必須遵循比例原則，不能接受空白授權，否則，人民在網際的自由很可能會被侵犯，宛如「在監控國度夢遊」一般；他們也不滿意美國挾科技的優勢進行光纖戰爭，包括對於友邦政治領導人的竊聽，形同對於主權國家的侵略行爲，罔顧彼此之間的互信；最後，即使沒有反恐的考量、或是人權的顧慮，也有可能涉及商業間諜的行爲，終究還是會危及國家利益（Bigo, et al., 2013: 10-11）。

西方民主國家對於情治單位的監聽，通常有幾種搜索票的核發、及監督的機制：瑞典是由情報法庭（UNDOM）、及情報行動督察（SIUN）主管，英國是分別由行政單位、及國會的情報安全委員會（ISC）負責，法國則另外成立獨立的機構（CNCIS），美國是由聯邦特別法庭、以及國會的委員會處理，他們的共同缺點是獨立性不足；再來是法制不足，也就是立法永遠趕不上監控科技的進步，因此被譏爲情治單位的行爲不是違法（illegal）、而是根本無法可管（a-legal）；不過，最大的問題是西方國家彼此之間的情資交換，以規避本國的相關法規，特別是管制較寬鬆的英國向美國兜售情報（Bigo, et al., 2013: 17:Bamford, 2013）。

美國的保障

基本上，美國並沒有通盤的隱私保護機制，而是透過憲法、判例、以及法規拼拼湊湊而成（Redmond, 2014:741-42; Richards, 2013: 1942）。在殖民時期，英國政府時常以搜捕狀進入私人財產進行無限制搜查，民怨甚深，終於導致美國的獨立，『美國憲法第四修正案』（*Fourth Amendment to the United States Constitution, 1792*）就是針對官方恣意搜捕所作的規範：

> 人民的人身、住宅、文件和財產不受無理搜查和扣押的權利，不得侵犯。除依照合理根據，以宣誓或代誓宣言保證，並具體說明搜查地點和扣押的人或物，不得發出搜查和扣押狀。
>
> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

不過，一直要到聯邦最高法院作出 *Griswold v. Connecticut*（1965）判例，隱私權才獲得確認。

NSA 的前身「密碼局」（Cipher Bureau，又稱 Back Chamber）是在一次世界戰後成立的，基本上是一個支援軍事作戰、以及外交政策的情報單位；當時的

局長 Herbert O. Yardley 對電報公司西聯匯款（Western Union）的老闆曉以大義，秘密取得每天進出電報的管道，展開百年的政府竊聽行動（Redmond, 2014: 751-52; Bamford, 2013）。在 1947-73 年之間，政府把數以百萬計的電報移交 NSA，老百姓完全蒙在鼓裡，而電報公司的高層被保證不會吃官司，因爲這是爲了國家的最高利益；在 1960 年代初期，NSA 開始監控那些到過古巴的人，理由是擔心他們會對總統、或是其他政要不利；接著，又把監控對象擴及民權、及反戰人士，理由是爲了防範騷動；到了尼克森總統時代，NSA 的監視名單已經高達三十萬人[10]（Sinha, 2013: 8）。

爲了管制政府對於私人有線電話、以及電子通訊的監聽，『綜合犯罪防制及街坊安全法第三篇／有線監聽法』（*Title III of the Omnibus Crime Control and Safe Streets Act, 1968*）是最早出現的相關法律。在尼克森總統水門事件（1972）東窗事發後，參議院展開調查，才揭露美國政府在過去四十多年的監控氾濫，不限於敵人，連記者、國會議員幕僚、最高法院法官、行政官員、反對黨、以及和平示威的老百姓，都是監聽的對象（Church Committee, 1975-76）。尤其是當政府以國家安全爲由展開不當的監控，幾乎沒有任何監督的機制，因此有『國外情報監控法』（*Foreign Intelligence Surveillance Act, 1978*）來加以規範，保障『美國憲法第四修正案』所宣示的隱私權，保護的對象是美國公民、及永久拘留者；此後，政府如果打算監聽國人本身、或是與外國嫌犯的通訊，必須先向新進設於法務部的秘密法庭「國外情報監控法庭」（Foreign Intelligence Surveillance Court, FISC）取得搜索票，而「國外情報監控複審法庭」（Foreign Intelligence Surveillance Court of Review, FISCR）則負責前者拒絕監聽申請的再審[11]（Landau, 2013: 67: Sinha, 2013: 13-16; Henderson, 2003）。

接下來則是『電子通訊隱私法』（*Electronic Communications Privacy Act,*

[10] 美國總共有 16 個情治單位（Bowdem 2013: 24。）聯邦調查局（FBI）、以及中央情報局（CIA）也有各自的非法監控，包括黑人民權運動領導者金恩牧師等政治異議份子（Martin Luther King, Jr.）（Sinha, 2013: 8-9）。

[11] 事實上， FISC 在成立的開頭二十多年從未拒絕過任何監聽申請案；在 1978-2001 年間，總共核准 13,102 件監聽申請案，只有兩件經過修正後才通過（Newell, 2014: 19: Sinha, 2013: 14）。

1986），進一步針對「監視記錄器」（pen register）、以及「追蹤裝置」（trap and trace）的規範，禁止在沒有搜索票之下紀錄跟傳遞即時通訊的通話、路由、定位、以及訊號等資訊（維基百科，2013）。

FISA 經過多年來的巨幅修訂，已經違背當年保障隱私權的立法初衷，包括免除民事責任，特別是在九一一事件（2001）後，小布希總統以反恐爲由大幅授與 NSA 的權力，便宜行事放寬政府的監聽限制[12]，不需要搜索狀就可以違法進行國際監聽，並以『愛國者法』（*PARIOT Act, 2001*）來就地合法[13]（Landau, 2013: 68；Bamford, 2013; Sinha, 2013: 16-22; Henderson, 2003）。在 2008 年，數位人權組織 Electronic Frontier Foundation（EFF）向第四巡迴法庭提告，指控 AT&T 跟 NSA 勾結電訊監控、侵犯隱私權；國會乾脆通過『國外情報監控修正法[14]』（*FISA Amendments Act, 2008*，又簡寫爲 FAA），不止弱化原有的保障規定、延長無搜索狀竊聽期限，還回溯性免訴近五十個監聽案件，無法進行有效司法制衡（Newell, 2014: 21; Sinha, 2013: 28; Redmond, 2014: 748--51）。

在 *Clapper v. Amnesty International USA*（2013）[15]，一些人權組織及 NGO 控告『國外情報監控修正法』（2008）所賦予政府的海外監控權違憲；聯邦最高法院加以駁回，認爲只有政府知道哪些通訊已經被攔截，做爲第三者的原告並沒有辦法證明監聽給任何人損害；不過，史諾頓稍後揭露，FISC 先前要求 Verizon 電話公司把所有的資料交給 NSA。隨後，EFF 根據史諾頓所提供的秘密檔案提告（*Jewel v. NSA, 2013*），再度控訴 NSA 等幾個聯邦機構沒有搜索票就從事監控，還是落敗；類似的案子還有、*CCR v. Obama*（2013）及 *New York Times Co. v. U.S. Dept. of Justice*（2013），大體可以看出法官對於 NSA 的監控沒有特定對象的作法，顯然是視若無睹（Newell, 2014: 20-23）。

---

[12] 原本，在 FISA 之下，政府可以先斬後奏，不經核准就進行 24 小時的緊急監控，後來逐漸放鬆，由 72 到 168 小時；至於戰爭期間，還可以長達 15 天（Sinha, 2013: 15）。

[13] 在 2002 年，七名 FISC 法官一致反對情報單位與檢方合作使用外國監聽所得資訊，不過半年後，FISCR 將判決加以推翻（Newell, 2014: 19-20）。

[14] 其中有一個過渡時期的『保護美國法』（*Protect American Act, 2007*）（Bowden, 2013: 21）。

[15] 早期的判例有 *Olmstead v. United States*（1928）、*Katz v. United States*（1967）、以及 *United States v. U.S. District Court*（1972），見 Redmond（2014: 744-46）。

歐盟的保障

『歐洲人權公約』（*European Convention on Human Rights, 1950*）第 8 條規定：

> 一、人人有權使他的私人和家庭生活，他的家庭和通信受到尊重。
>
> 二、公共機關不得干預上述權利的行使，但是依照法律的干預以及在民主社會中為了國家安全，公共安全或國家的經濟福利的利益，為了防止混亂或犯罪、為了保護健康或道德、或為了保護他人的權利與自由，有必要進行干預者，不在此限。
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

『歐盟基本權利憲章』（*EU Charter Fundamental Rights, 2009*）除了在第 7 條規範個人與家庭生活：「人人均有權要求尊重其私人與家庭生活、住居及通信」（Everyone has the right to respect for his or her private and family life, home and communications.），更在第 8 條特別針對個人資訊之保護加以規範：

> 一、人人均有權享有個人資訊之保護。
>
> 二、此等資訊應僅得於特定明確目的，且於資訊所有人同意或其他法律規定之正當依據下，公平地被處理。人人均有權瞭解其個人資訊，並有權要求銷毀其個人資訊。
>
> 三、應由獨立之主管機關監督這些原則之確實遵守。
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

另外，歐洲議會也通過『資料保護指令』（*Data Protection Directive, 1995*）、以及『通訊指令』（*Communications Directive, 1997*）。不像美國的相關法律，『歐洲人權公約』、以及『歐盟基本權利憲章』保障所有的人，而非簽署國、或是歐盟國家的公民而已。接下來，我們將檢視「歐洲人權法院」（European Court of Human Rights, ECtHR）相關情治監控及隱私權的判例。

歐洲人權法院有關隱私權判例的爭辯，主要在於各國政府是否可以根據法律進行監聽，用來追求的民主社會的目標[16]。在 *Weber and Saravia v. Germany*（2006）一案，德國情報局（German Federal Intelligence Service）除了進行電訊監控，還把個人資料轉交其他單位使用；法官的判決是德國現有的法律足夠保障人民防止政府濫權，此外，就民主社會而言，對於通訊秘密的干預是確保國家安全、以及防範罪犯所必須。當然，爲了避免濫權及恣意，法官盧列起碼的保護準繩，用來檢視政府的作爲是否妥當，包括目的、對象、期限、程序、傳遞、以及銷毀（Bigo, et al., 2013: 21-22; Newell, 2014: 113-14）。

接著在 *Liberty v. UK*（2008），法院認爲英國法律不清楚、不足防範情治單位濫權，不論是監控的範圍、或方式，政府的裁量權太大，因此判定違反『歐洲人權公約』第 8 條。法官除了指出監控行爲必須有法律基礎，特別要求法律必須符合「可預見度」（foreseeability），也就是精確而可以合理預期監控可能造成人民權利的損害；法官承認，有關於情資檢視、使用、儲存、傳遞、及銷毀的規定，或許會影響蒐集的效能、甚至於造成洩密的危險，不過，如果德國當局認爲國內相關法規的詳細要求都是安全的，那麼，英國應該也可以依樣畫葫蘆（Bigo, et al., 2013: 21-22; Newell, 2014: 14-16）。

再來是 *Kennedy v. UK*（2010），歐洲人權法院進一步檢視英國情治單位的電訊攔截，看是否合乎民主社會的法治要求。法院承認，『歐洲人權公約』的簽署國對於法律程序的必要性有一些裁量權，然而，還是必須接受監督；同時，如

[16] 早先的判例 *Klass and Others v. Germany*（1978）、及 *Malone v. the United Kingdom*（1984），見 Newell（2014: 9-13）。

果必要的界線不被逾越，那麼，監督的程序必須儘量合乎民主社會的價值；此外，由於監控行動很容易因爲濫權而給個人跟社會集體造成傷害，因此，對於情治單位的監督最好交給司法機構。法院重申監控的三個要求，立法規範、合乎法治、以及可預見度，並特別強調如何有效防範濫用（Bigo, et al., 2013: 22-23）。

最後是 *Nada v. Switzerland*（2012），法院針對『聯合國安全理事會第 1267 號決議』（1999），也就是安理會制裁委員會（Sanction Committee）凍結賓拉登（Osama bin Laden）、蓋達組織（al-Qaeda）、以及塔利班（TaliBam）的作爲，是否違反『歐洲人權公約』。法官認爲，只要符合迫切的社會需要、合乎比例原則、理由充分，那麼，人權的侵犯可以視爲民主社會所必須；至於所謂比例原則、以及必要性，法官提醒政府必須考慮是否還有其他損害較小的途徑；最後，法官強調，究竟侵犯人權的措施是否必要，必須由歐洲人權法院判斷是否合乎『歐洲人權公約』（Bigo, et al., 2013: 23-24）。

國際公約的保障

根據『世界人權宣言』（*Universal Declaration of Human Right, 1948*）第 12 條，隱私權是基本人權：

> 任何人的私生活、家庭、住宅和通信不得任意干涉，他的榮譽和名譽不得加以攻擊。人人有權享受法律保護，以免受這種干涉或攻擊。
>
> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

同樣地，『公民及政治權利國際公約』（*International Covenant on Civil and Political Rights, 1966*）第 17 條也把隱私權當作基本的公民權；第 1 款作負面的陳述，第 2 款作正面的陳述[17]：

[17] Sinha（2013: 51）引用 Fernando Volio 的看法，當 ICCPR 的條款使用負面陳述，表示這是基本的權利。相較起來，『歐洲人權公約』第 8 條第 2 款規定文字比較明確，不過，卻條列了一些排除情況，很難說哪一個的保障比較周延；另外，ICCPR 的用字是「不得干涉」，『歐洲人權公約』

> 一、任何人的私生活、家庭、住宅或通信不得加以任意或非法干涉，他的榮譽和名譽不得加以非法攻擊。
>
> 二、人人有權享受法律保護，以免受這種干涉或攻擊。
>
> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

由於參議院已經在 1992 年批准 ICCPR， 照道理，美國應該有義務遵守該國際條約所保障的基本人權，包括隱私權，然而，由於美國對於部分條文有諸多保留[18]，迄今不願意簽訂相關的『公民及政治權利國際公約任擇議定書』（*Optional Protocol to the International Covenant on Civil and Political Rights, 1966*），因此，美國人無法像聯合國人權事務委員會（Human Rights Committee）提告；同時，由於美國認爲該公約並不算是自動履行條約（self-executing treaty），意思是說不必經過立法就可以生效的條約，因此，目前不可以在美國法庭引用（Peters, 2013; Redmond, 2014: 740）。

接下來是 NSA 對於境外非美國人的監聽，是否適用 ICCPR 的規範。美國的基本立場是憲法並不保障境外非國人的隱私權[19]，也就是反對 ICCPR 的境外適用性（extraterritoriality）；不過，這樣的看法是跟國際法界、以及學術界的解釋大相逕庭（Margulies, 2014: 2137-38）。根據該公約第 2 條的門檻條件：

> 一、本公约每一缔约國承担尊重和保證在其領土内和受其管轄的一切個人享有本公约所承認的權利，不分種族、膚色、性别、語言、宗教、政治或其他見解、國籍或社會出身、财產、出生或其他身分等任何區别。
>
> 1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

卻使用「尊重」，也有不同的詮釋（Sinha, 2013: 51-52）。

[18] 通稱爲「RUDs」，也就是 reservation、understandings、以及 declarations（Sinha, 2013: 50）。

[19] 有關於聯邦最高法院的判例，見 *United States v. Verdugo-Urquidez*（1990）（Margulies, 2014: 2137; Milanovic, 2014: 9）。

關鍵是「在其領土內」（within its territory）跟「受其管轄」（subject to its jurisdiction）這兩個條件如何詮釋[20]。如果依據圖 2 來看，應該是只要符合「在其領土內」、或是「受其管轄」其中條件（也就是聯集），就應該接受該國保護，而非要兩個條件都符合（也就是交集）。美國迄今主張政府保護隱私權的對象是自己的公民、以及境內具有居留權的人士，將權利與公民結合在一起，至於境外的（extra-territorial）電訊監控則不受約束，因此堅持現有的作爲並不違法，與人權推動者、或是學術界的看法不同（Sinha, 2013; Milanovic, 2014; Privacy International, Access, et al., 2014）。

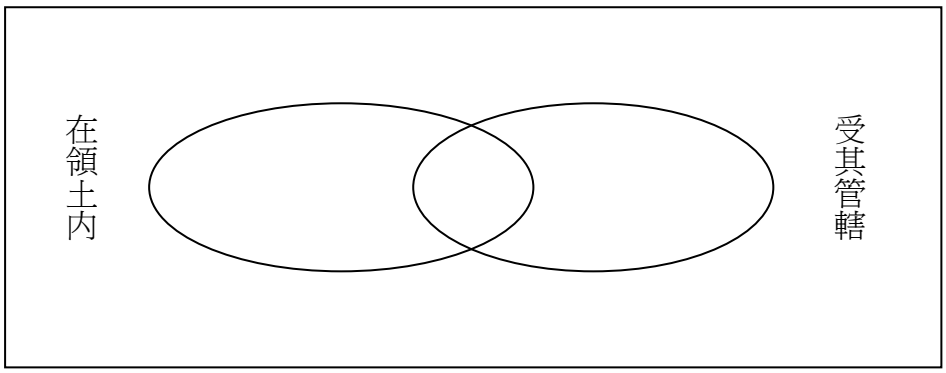


圖 2：ICCPR 的保護對象

「在其領土內」的認定比較明確，至於所謂的「受其管轄」，在國際法上是指「有效控制」（effective control），具體而言，包括對人、以及對領土的「實質控制」（physical control）；不過，在網絡通行的時代，監聽的技術已經構成超越空間的「虛擬控制」（virtual control），也就是「遙控」（remote control）[21]，當然符合 ICCPR 對於「通信」（correspondence）的保護（Peters, 2013; Margulies, 2014: 2166）。更何況，聯合國人權事務委員會針對 ICCPR 第 17 條所作的『第 16 號一般性意見』（*ICCPR General Comment No. 16, 1988*）也明確表示：

不管是電子還是其他形式的監聽，對於電話、電報、或是其他通訊方式

[20] 請比較 Milanovic（2014: 7）從情報單位（agency）、國籍（nationality）、以及地點（location）三個面向來分析。

[21] 根據媒體報導，NSA 利用藏在軟式程式裡頭的「後門」，可以破解各種加密系統；另外，即使電腦不跟網際網路連線，NSA 透過電腦廠商，也能夠植入的無線發射器加以控制；更不用說，美國有能力接近深海電纜、以及影響電訊的業者（Margulies, 2014: 2151）。

的攔截，竊聽、以及對話的錄音，都應該禁止

Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.

接下來就是「不得加以任意或非法干涉」（arbitrary or unlawful interference）的解釋，也就是說，隱私權並非無限上綱的，而是可以合理的加以限制（justifiable interference）（Sinha, 2013: 57-58）。那麼，除了 ICCPR 的上述原則性規範，一般的判準有三：程序必須經過立法[22]、目的必須有正當性、以及手段必須符合比例原則；那麼，反恐應該是一個合理的目標，至於大規模的進行電訊監控，明顯違反比例原則（Peters, 2013）。

比較有模糊地帶的是電訊監控的合法性，特別是當政府之間有協定、或是密約的情況。我們知道，美國透過「五眼」（Five Eyes）情報合作聯盟[23]，也就是澳洲、加拿大、紐西蘭、以及英國，蒐集及分享網際網路監控情報[24]，相互監督對方的公民，狼狽爲奸，以迴避自身國會的監督；目前，合作的對象擴及丹麥、法國、荷蘭、挪威（稱爲「九眼」Nine Eyes）、德國、比利時、義大利、西班牙、及瑞典（稱爲「十四眼」Fourteen Eyes），另外，新加坡、日本、韓國也是合作對象（Wikipedia, 2014b）。這些一直要到 NSA 的檔案在 2010 年解密，外面才比較知道全貌（Newell, 2014: 18-19）。

以德國爲例，戰後跟美國簽訂了不少協定，特別是針對境內的北大西洋公約組織的駐軍；問題是，這些協定可以超越憲法、以及相關法律所保護的隱私權嗎？

---

[22] 根據聯合國人權事務委員會針對 ICCPR 第 17 條所作的『第 16 號一般性意見』：
The term “unlawful” means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.

[23] 最早是由美國跟英國在 1943 年正式展開有關信號情報（SIGINT）分享的 *BRUSA Agreement*，次年再透過 *United Kingdom-United States of America Agreement*（UKUSA），擴充爲五國，合作內容由通信情報系統（COMINT）擴及電子情報系統和（ELINT）（Wikipedia, 2014b; 2014c）。有關這些國家現有的監督機制，見 Bigo 等（2013）、以及 Privacy International（2014）

[24] 主要透過 ECHELON 程式，當然，美國還有多種惡名昭彰的工具，包括 CAPPS（Computer-Assited Passenger Pre-Screening System）、PNR（Personal Name Records）、NIMD（Novel Intelligence from Massive Data）、ARDA（Advanced Research and Development Activity）、以及 MATRIX（Multistate Anti-Terrorism Information Exchange）（Bigo, et al., 2013: 8; Bedan, 2007）。

Peters（2013）指出，根據「馬太原則」（Matthews Principle[25]），『歐洲人權公約』的簽署國不可以藉口跟其他國家有協定，就可以罔顧對內的人權保障，譬如說盟國對於本國百姓的電訊監控；然而，權利是屬於人民的，政府不能跟其他國家讓渡。德國憲政法庭在 2004 年作出判例，行政跟司法部門必須考量國際條約，然而，不意味可以不顧憲法的規範；也就是說，法官在裁決時必須想辦法調和憲法、法律、以及國際法，然而，如果真正有困難時，當然是憲法優先（Peters, 2013）。

面對聯合國的保護性觀點、及美國的限制性詮釋，Margulies（2014: 2137-38, 2143-48, 2153-57）提出法律「互補性」（complementarity）的概念，認爲 ICCPR 對於隱私權保護的適用未必是零或一，主張折衷的方式，也就是針對第 2 條的要求「尊重」（respect）、但未必要「保證」（ensure），以便讓各國有比較大的彈性空間。換句話說，他建議讓聯合國人權事務委員會贏得面子、讓美國保有理子；只不過，他所提出來得一些改革方案，譬如讓一些獨立人士參與 FISC 審查、以及成立部會級的單位（pp. 2165-66），看來只是不傷大雅。

結語

在史諾頓事件後，美國總統歐巴馬總統長篇大論（Obama, 2014）宣示一番，了無新意；他隨後作出『第 28 號政策指令』（*Presidential Policy Directive/PDD-28, 2014*），宣示對於「所有人」（all persons）的隱私權尊重，聽起來是空谷足音，而且對 ICCPR 隻字不提：

> In addition, our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

我們同時也可以看到，歐巴馬總統所任命的 FISA 評估小組（President's Review Group on Intelligence and Communications Technologies, 2013）一方面強調隱私權

[25] 我們查不到相關的名詞，猜想是歐洲人權法院所作出來的判例 *Matthews v United Kingdom*（1989）。

是所有人的基本權利（pp. 155-56）：

> Perhaps most important, however, is the simple and fundamental issue of respect for personal privacy and human dignity – wherever people may reside. The right of privacy has been recognized as a basic human right that all nations should respect. Both Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights proclaim that "No one shall be subjected to arbitrary or unlawful interference with his privacy. . . ." Although that declaration provides little guidance about what is meant by "arbitrary or unlawful interference," the aspiration is clear. The United States should be a leader in championing the protection by all nations of fundamental human rights, including the right of privacy, which is central to human dignity.

也建議必須改善對於外國人監聽的方式（Chap. 4），然而，另一方面卻又對於 FISA 內外有別的機制表示贊同（p. 154），表示美國對於本身的優勢不會讓步：

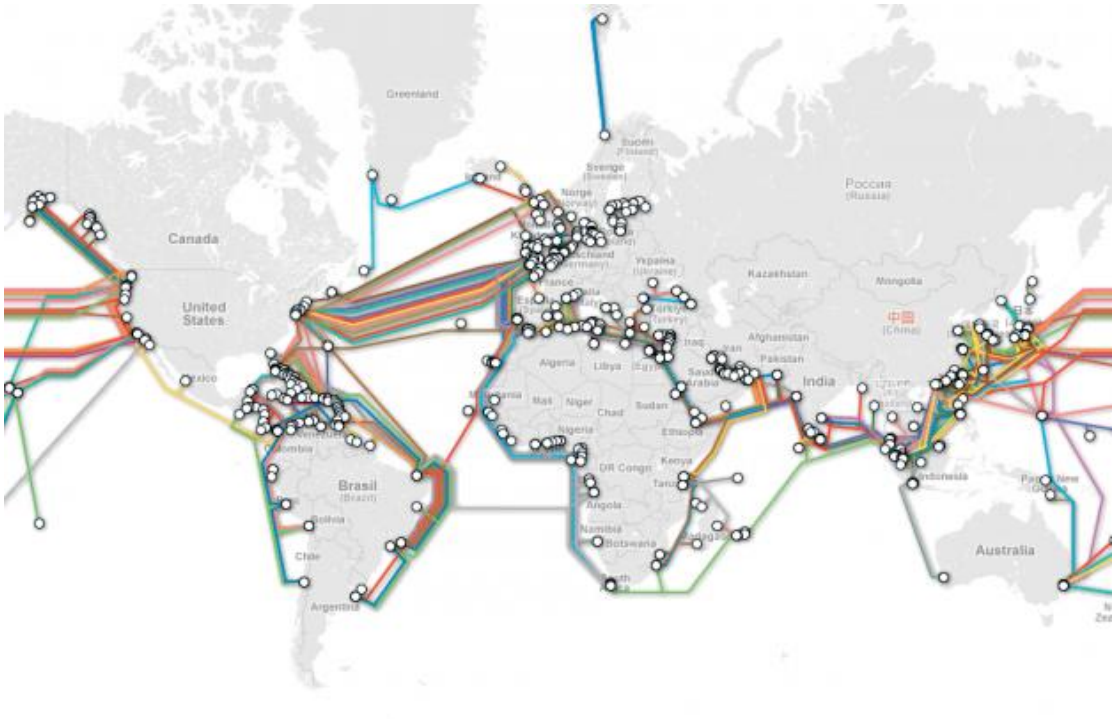
> Against that background, FISA's especially strict limitations on government surveillance of United States persons reflects not only a respect for individual privacy, but also—and fundamentally—a deep concern about potential government abuse within our own political system. The special protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact special restrictions on government surveillance of those persons who participate directly in its own system of self-governance.

也因如此，即使德國總理、以及及巴西總統一怒之下，在聯合國大會成功推動決議『數位時代的隱私權』（United Nations General Assembly, 2014），折衝的結果，用字淺詞看起來也是不痛不癢。

美國以公民的資格決定是否有隱私權，因此，外國人、或是境外人士不在保護的範圍，這樣的立論源自在於我們耳熟能詳的共和主義（republicanism）、或社會契約論（social contract）。然而，人權的理念立基於天賦不容剝奪的基本尊嚴，不是因爲你剛好出生在某個國家取得公民權（Milanovic, 2014: 21。由於國際規約並未能明確約束電子監控、及充分保障數位隱私權[26]，因此，除了強化現有的獨立監督機制（深化），再來就是推動國際隱私權權規約了（廣化），這是學術界的初步共識（Redmond, 2014; Milanovic, 2014; Mihr, 2013）。

[26] 即使是聯合國人權事務委員會『第 16 號一般性意見』（1988），還是稍嫌陽春。

附錄 1：全球海底電纜分佈圖



來源：Flowingdata（2011）。

國際規約、憲法、法規、判例

『美國憲法第四修正案』，1792（http://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9C%8B%E6%86%B2%E6%B3%95%E7%AC%AC%E5%9B%9B%E4%BF%AE%E6%AD%A3%E6%A1%88）（2014/6/4）。

『世界人權宣言』，1948（http://www.un.org/zh/documents/udhr/）（2014/6/4）。

『歐洲人權公約』，1950（http://www.cahr.org.tw/lawdan_detail.php?nid=105）（2014/6/4）。

『公民及政治權利國際公約』，1966（http://www.un.org/chinese/hr/issue/ccpr.htm）（2014/6/4）。

『歐盟基本權利憲章』，2009（http://www.hrp.scu.edu.tw/library/literature/entry.jsp?id=1236571265852-bdbe8a11-3085-4049-8168-2129a906421b）（2014/6/6）。

Fourth Amendment to the United States Constitution, 1792

Olmstead v. United States, 1928

Radio Communication Act, 1936

BRUSA Agreement, 1943

United Kingdom-United States of America Agreement, 1944

Universal Declaration of Human Right, 1948

European Convention on Human Rights, 1950

Griswold v. Connecticut, 1965

International Covenant on Civil and Political Rights, 1966

Optional Protocol to the International Covenant on Civil and Political Rights, 1966

Katz v. United States, 1967

Title III of the Omnibus Crime Control and Safe Streets Act, 1968

United States v. U.S. District Court, 1972

Foreign Intelligence Surveillance Act, 1978

Klass and Others v. Germany, 1978

Malone v. the United Kingdom, 1984

Electronic Communications Privacy Act, 1986

ICCPR General Comment No. 16, 1988

Matthews v United Kingdom, 1989

United States v. Verdugo-Urquidez, 1990

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (*Data Protection Directive, 1995*)

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal data and the Protection of Privacy in the Telecommunications Sector (*Communications Directive, 1997*)

PARIOT Act, 2001 (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*)

Weber and Saravia v. Germany, 2006

Protect America Act, 2007

FISA Amendments Act, 2008

EU Charter Fundamental Rights, 2009

Nada v. Switzerland, 2012

Jewel v. NSA, 2013

CCR v. Obama, 2013

New York Times Co. v. U.S. Dept. of Justice, 2013

Presidential Policy Directive/PDD-28, 2014

參考文獻

Bamford, James. 2013. "They Know Much More Than You Think." *New York Review of Books*, August 15 (http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/) (2014/6/9)

Bedan, Matt. 2007. "Echelon's Effect: The Obsolescence of the U.S. Foreign Intelligence Legal Regime." *Federal Communications Law Journal*, Vol. 59, No. 2, pp. 425-444. (http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1477&context=fclj) (2014/6/9)

Bigo, Didier, Sergio Carren, Nicholas Hernanz, Julien Jeandesboz, Joanna Parki, Francesco Ragazzi, and Amandine Scherrer. 2013. "Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law." (file:///C:/Documents%20and%20Settings/Ohio/My%20Documents/Downloads/No%2062%20Surveillance%20of%20Personal%20Data%20by%20EU%20MSs%20(1).pdf) (2014/6/9)

Bowden, Caspar. 2013. "The US National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and Their Impact on EU Citizens' Fundamental Rights." (http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf) (2014/6/9)

Church Committee. 1975-76. *Church Committee Reports* (http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm) (2014/6/7)

Flowing Data. 2011. "Submarine Cable System Connecting the World." (http://flowingdata.com/2011/10/03/submarine-cable-system-connecting-the-world/) (2014/6/5)

Gellman, Barton. 2013. "Edward Snowden: 'I Already Won'." *Washington Post*, December 24 (http://www.pulitzer.org/files/2014/public-service/washpost/20washpostnsa2014.pdf) (2014/6/9)

Henderson, Nathan C. 2003. "*The Patriot Act's Impact* on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications." *Duke Law Journal*, Vol. 52, pp. 179-209.

Human Rights Council. 2011. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom, Frank La Rue." May 16, A/HRC/17/27 (http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf) (2014/6/9).

Human Rights Council. 2013. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom, Frank La Rue." April 17, A/HRC/23/40 (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/

133/03/PDF/G1313303.pdf?OpenElement) (2014/6/9).

Klein, Mark. 2006. "Wiretap Whistle-Blower's Account." (http://archive.wired.com/science/discoveries/news/2006/04/70621) (2014/6/7)

Landau, Susan. 2013. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *Spotlight*, July-August, pp. 66-75.

Margulies, Peter. 2014. "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism." *Fordham Law Review*, Vol. 82, pp. 2137-67.

Mihr, Anja. 2013. "Public Privacy Human Rights in Cyberspace." (http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1$5D.pdf) (2014/6/9)

Milanovic, Marko. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485) (2014/6/9)

Newell, Bryce Clayton. 2014. "The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe." (http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Newell.pdf) (2014/6/9)

Obama, Barack H. 2014. "Remarks by the President on Review of Signals Intelligence." January 17 (http://www.whitehouse.gov/the-press-office/2014 /01/17/remarks-president-review-signals-intelligence) (2014/6/8)

Orwell, George. 1949. *Nineteen Eighty-Four* (http://www.iblist.com/book57.htm) (2014/6/9)

Peters, Anne. 2013. "Surveillance without Borders" The Unlawfulness of the NSA Panopticon, Part II." EJIL: Talks! November 4 (http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/) (2014/6/9)

PoKempner, Dinah. 2014. "The Right Whose Time Has Come (Again)" Privacy in the Age of Surveillance." (http://www.hrw.org/sites/default/files/related_material/privacy_Endnotes.pdf) (2014/6/9)

President's Review Group on Intelligence and Communications Technologies. 2013. Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf) (2014/6/8)

Privacy International, Access, Electronic Frontier Foundation, Article 19, Association for Progressive Communications, Human Rights Watch, and World Wide Web Foundation. 2014. "OHCHR Consultation in Connection with General Assembly Resolution 68/167 'The Right to Privacy in the Digital Age'." (http://www.hrw.org/sites/default/files/related_material/OHCHR%20joint%20NGO%

20submission%20final%2031.03.14.pdf) (2014/6/9)

Redmond, Valerie. 2014. "I Spy with My So Little Eye: A Comparative of Surveillance Law in the United States and New Zealand." *Fordham International Law Journal*, Vol. 37, pp. 733-75.

Richards, Neil M. 2013. "The Dangers of Surveillance." *Harvard Law Review*, Vol. 126, pp. 1934-65.

Sinha, G. Alex. 2013. "NSA Surveillance since 9/11 and the Human Right to Privacy." (http://www.aaron-zimmerman.com/wp-content/uploads/2014/01/Privacy-Supplement-1-Sinha.pdf) (2014/6/9)

United Nations, General Assembly. 2014. "Resolution adopted by the General Assembly on 18 December 2013: The Right to Privacy in the Digital Age." A/RES/68/167 (http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167) (2014/6/8)

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." Harvard Law Review, Vol. 4, No. 5 (http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm) (2014/6/9)

Wikipedia. 2014a. "Call Detail Record." (http://en.wikipedia.org/wiki/Call_detail_record) (2014/6/9)

Wikipedia. 2014b. "Five Eyes." (http://en.wikipedia.org/wiki/Five_Eyes) (2014/6/9)

Wikipedia. 2014c. "Global surveillance." (http://en.wikipedia.org/wiki/Global_surveillance) (2014/6/9)

維基百科，2013。《電子通訊隱私法》（http://zh.wikipedia.org/wiki/电子通信隐私法）（2014/6/9）。

維基百科，2014a。《641A 室》（http://zh.wikipedia.org/wiki/641A_室）（2014/6/9）。

維基百科，2014b。《稜鏡計畫》（http://zh.wikipedia.org/wiki/稜鏡計畫）（2014/6/9）。