A Hogan Lovells White Paper

A Sober Look at National Security Access to Data in the Cloud

Analyzing the Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions

by

Winston Maxwell, Paris, France
Christopher Wolf, Washington, DC

May 22, 2013

Updated July 23, 2014 to add sections on Brazil, Italy, and Spain; add new French law; and add new EU case law

Introduction

In our 2012 White Paper, *A Global Reality: Governmental Access to Data in the Cloud*, we debunked the oft-repeated misconception that the 2001 USA PATRIOT Act ("Patriot Act") gives the United States government greater powers of access to data stored with a third-party Cloud computing service than governments elsewhere.[1] This misconception has been perpetuated by critics, including in advertisements by non-U.S. Cloud service providers, to support the notion that the best way to "protect" one's Cloud data from troublesome government access is to use Cloud service providers present only in "safe" jurisdictions – as typically stated, those located outside of the U.S.

Most recently, these critics have focused their attention on another law, Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), enacted under the FISA Amendments Act of 2008 ("FAA") and codified at 50 U.S.C. § 1881a ("Section 1881a").[2] FISA provides a formalized structure for U.S. law enforcement agencies to obtain information about persons suspected of international terrorism or espionage against the United States. Enacted in 1978 after the Watergate scandal in reaction to President Nixon's unsupervised use of wiretaps for purportedly national security purposes,[3] FISA actually **added** privacy protections in the form of judicial review and legislative oversight of the ability of the President and law enforcement agencies to conduct national security surveillance. Specifically, such surveillance is subject to review by courts presided over by federal judges, with appeals possible to the U.S. Supreme Court. The law enforcement agencies tasked with complying with FISA are required to provide regular compliance reports to the Congressional committees with responsibility over national security.

As with the Patriot Act, Section 1881a has been invoked by some in Europe as a kind of shorthand to express the belief that the United States has greater access to data in the Cloud than governments elsewhere, and that the U.S. government is the principal threat to the privacy of European citizens. Criticisms typically are based on a bare reading of Section 1881a and the FAA without any context surrounding its operation, and are used to level highly speculative accusations. For example, some raise the specter of the United States using Section 1881a to conduct purely political surveillance of individual Europeans.[4] The Chairperson of the French data protection regulator recently implied that the U.S. government might be accessing European data in the course of law enforcement investigations to facilitate economic espionage.[5]

In parallel to this policy debate, Europe-based Cloud providers use the FAA and Section 1881a as commercial arguments to convince Europe-based customers not to use their U.S. competitors.[6] Curiously, the protagonists in this

[1] Our survey of the laws of ten countries with strong legal protections on civil rights and due process revealed that each country vests authority in the government to require a Cloud service provider to disclose customer data and in most instances enables the government to access data physically stored outside the country's borders. Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud* (2012) [hereinafter Maxwell & Wolf, *A Global Reality*], *available at* http://hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique.

[2] In December 2012, Congress voted to reauthorize the FAA, which had been scheduled to sunset at the end of 2012, through the end of 2017.

[3] Congressional Research Service, *Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization* at 3 (2011), *available at* http://fas.org/sgp/crs/intel/R40980.pdf.

[4] European Parliament, Directorate-General for Internal Policies, *Fighting cyber crime and protecting privacy in the cloud*, PE 462.509 (2012), *available at* http://europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050.

[5] Marc Cherki, *Alerte au risque d'espionnage dans le cloud computing*, LE FIGARO, June 24, 2012, http://lefigaro.fr/societes/2012/06/24/20005-20120624ARTFIG00125-alerte-au-risque-d-espionnage-dans-le-cloud-computing.php.

[6] *See, e.g.*, TeamDrive Blog, *The US law enables the US government to snoop on Europeans' data held with US cloud*

debate rarely mention government access in other non-European countries that host large global data centers, including those whose data protection laws are recognized as "adequate" by EU authorities,[7] and they rarely mention the national security legislation in other countries, including virtually all EU Member States, which give police and intelligence agencies far-reaching access to data in the Cloud in cases justified by national security, **frequently without court authorization**.

Ultimately, governments need some degree of access to data stored in the Cloud to conduct investigations relating to national security and terrorism. But privacy and confidentiality also are important concerns. This White Paper does not enter into the ongoing debate about the appropriate balance between the protection of privacy and government access to data for law enforcement and national security purposes. Rather, it undertakes to dispel some of the common, unfounded criticisms of Section 1881a, and to compare the nature and extent of governmental access to data in the Cloud for terrorism and counterintelligence purposes in many jurisdictions around the world.

The Operation of Section 1881a

In general, FISA governs the surveillance of and the collection of evidence about persons suspected of being part of a terrorist organization or acting as spies for foreign governments. Such requests are subject to prior authorization by the Foreign Intelligence Surveillance Court ("FISC"), a court comprised of a rotating panel of existing, independent, lifetime-appointed federal judges to evaluate whether requests for surveillance meet the standards of FISA and the FAA. Decisions of the FISC are appealable to the Foreign Intelligence Surveillance Court of Review ("Court of Review"), also a panel of existing federal judges, whose decisions in turn are appealable to the U.S. Supreme Court.

Prior to the enactment of Section 1881a, and temporary legislation that preceded the FAA called the Protect America Act,[8] FISA provided procedures for the U.S. government to apply to the FISC for a warrant that would permit it to acquire foreign intelligence information through a variety of methods. Section 1881a supplemented these pre-existing FISA procedures by creating an additional framework and procedural requirements for foreign intelligence collection.

Section 1881a does not give the U.S. government *carte blanche* to seize whatever information it wants from Cloud service providers. As the Supreme Court recently acknowledged, surveillance under Section 1881a is subject to statutory conditions, judicial authorization, and Congressional supervision.[9] These safeguards are similar to those imposed under the European Convention on Human Rights and Fundamental Freedoms, and applied by most European countries. To make use of Section 1881a, the Attorney General and the Director of National Intelligence must jointly and under oath submit a certification to the FISC attesting, among other things, that a significant purpose of the surveillance is to obtain foreign intelligence information. Absent emergency circumstances, this certification must be submitted and approved by the FISC **prior to** conducting the surveillance. Once the FISC approves this certification, the government is permitted to direct a service provider to conduct the authorized surveillance for a one-year period.

Providers that are subject to such directives can immediately challenge the lawfulness of the directive before the FISC, and can appeal such decisions to the Court of Review and petition the Supreme Court. In addition, the government is required to declare in advance whenever it wishes to use any information collected through Section 1881a in a judicial or administrative proceeding, and if so, any affected person or entity can challenge the lawfulness of the acquisition before the government introduces it as evidence.

The discussion that follows addresses the main limitations on the government's surveillance authority under Section 1881a – the requirement that the surveillance be to obtain "foreign intelligence information," judicial oversight, and legislative oversight – as well as the fact that despite its critics, Section 1881a provides comparable transparency and due process to the legislation in other democratic countries engaged in foreign intelligence gathering.

I. The Scope of "Foreign Intelligence Information"

As mentioned above, some have suggested that Section 1881a authorizes purely political surveillance of individuals and economic espionage. These suggestions are vastly overstated. Rather, Section 1881a largely restricts surveillance to the specific areas of national defense, national security, and the conduct of foreign affairs, with

providers without needing to obtain a warrant (Feb. 27, 2013), http://blog.teamdrive.com/2013_02_01_archive.html ("European companies that want to avoid being snooped on by the US government can trust TeamDrive.").

[7] The European Commission has the power to determine, on the basis of Article 25(6) of directive 95/46/EC, whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. This determination allows the free cross-border flow of personal data to the third country.

[8] The Protect America Act, enacted in August 2007, was a temporary law that sunset six months later in February 2008, and later was replaced by the FAA in July 2008.

[9] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013).

specific emphasis given to international terrorism, sabotage, the proliferation of weapons of mass destruction, and other grave hostile acts. This is a narrow scope – for example, Section 1881a cannot be used to investigate ordinary crimes, or even domestic terrorism.[10] Unlike the French statute on national security interceptions, Section 1881a does not extend to organized crime or to protection of national economic interests.

The overstatement of the scope of Section 1881a seems to be driven by a lack of context. The law only permits the targeting of persons where a significant purpose is to acquire "foreign intelligence information." [11] When acquired from a non-U.S. person, "foreign intelligence information" is defined as:

(1) information that relates to . . . the ability of the United States to protect against—
   (A) actual or potential attacks or other grave hostile acts of a foreign power or an agent of a foreign power;
   (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
   (C) clandestine intelligence activities by an intelligence service or network of a foreign power by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to . . . —
   (A) the national defense or the security of the United States; or
   (B) the conduct of the foreign affairs of the United States.[12]

By definition, the purposes contained in subsection (1) are measures designed to protect against acts of terrorists and other third parties seeking to harm the United States, and the purposes contained in subsection (2) are designed to enable the gathering of intelligence pertinent to national defense, security, or foreign affairs. As discussed later in this White Paper, this is authority reserved and exercised by other major sovereign powers, not just the United States.

Moreover, these categories of information all have one thing in common: they **must be ascribed to a "foreign power or foreign territory."** This means that private business records, academic research, and political opinions do not constitute "foreign intelligence information." Even with respect to the inclusion of information concerning "the conduct of the foreign affairs of the United States" under subsection (2), Congress **expressly signaled its intent to exempt the private political views of non-U.S. citizens** from the scope of what could be collected.[13] Instead, the term "foreign intelligence information" most likely encompasses information necessary to conduct diplomacy and engage in international relations.[14]

Regarding what organizations might be affected, the term "foreign power" as defined by the statute primarily incorporates foreign terrorist organizations, foreign governments, and instrumentalities of both.[15] Much has been made about the inclusion of "foreign-based political organization[s]" within the definition of "foreign power."[16] Importantly, however, this term **does not** encompass any organization that can be said to have a political opinion. Instead, Congress indicated that it must be interpreted in line with the other types of enumerated "foreign powers" to encompass political parties that act as "mere instrumentalities of" government and other organizations with actual political power in a foreign country.[17]

These limitations on "foreign intelligence information" and the types of organizations covered by the law should provide comfort to private businesses, academics, universities, and private citizens located outside of the U.S. that Section 1881a cannot be used to target the data that they store in the Cloud.

[10] *Cf. In re Sealed Case*, 310 F.3d 717, 735-36 (F.I.S.C.R. 2002) (exempting searches for evidence of "ordinary crimes" from the definition of "foreign intelligence information"). This includes offenses with an international character, such as smuggling, international money laundering, and bank fraud aimed at international financial institutions. 1 David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions § 8:31 (2d ed. 2012) [hereinafter Kris & Wilson].

[11] 50 U.S.C. § 1881a(a). This requirement is reinforced by the Attorney General's internal Acquisition Guidelines, which provide that "a non-U.S. person may not be targeted unless a significant purpose of the targeting is to acquire foreign intelligence information that the person possesses, is reasonably expected to receive, and/or is likely to communicate." U.S. Department of Justice & U.S. Office of the Director of National Intelligence, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2008 – May 31, 2009* at 7 (Dec. 2009), *available at* http://aclu.org/files/pdfs/natsec/faafoia20101129/FAAODNI0001.pdf.

[12] 50 U.S.C. § 1801(e).

[13] *See* H.R. Rep. No. 1283, Pt. I., 95th Cong. 2d Sess., 1978 U.S.C.C.A.N. 4048, at 50 (June 8, 1978) ("The information must pertain to a foreign power or foreign territory; and thus it cannot simply be information about a citizen of a foreign country . . . unless the information would contribute to meeting intelligence requirements with respect to a foreign power or territory."). Because these definitions remain from FISA as originally enacted in 1978, the legislative history from 1978 is applicable when evaluating these provisions today.

[14] Kris & Wilson § 8:33.

[15] 50 U.S.C. § 1801(a).

[16] 50 U.S.C. § 1801(a)(5).

[17] *See* S. Rep. No. 604, 95th Cong., 1st Sess., 1978 U.S.C.C.A.N. 3904 (Nov. 15, 1977); Kris & Wilson § 8:8.

II. Judicial Oversight of the Use of Section 1881a

As described above, an important limitation on the government's use of Section 1881a (and FISA as a whole) is the requirement, unlike that in many other countries, to certify surveillance requests under oath to the FISC for its review and approval.[18] This certification must be submitted **prior to** conducting the surveillance, unless exigent circumstances dictate that delay may result in the loss of intelligence, in which case the certification must be submitted "as soon as practicable" but in no event more than seven days later.[19]

If the FISC denies the certification, the government must correct any deficiency in its request within thirty days; otherwise it must not begin (or must cease any existing) collection.[20] If the FISC approves the certification, the government then may issue a directive to the electronic communications service provider specified in its request to comply with the FISC's order.[21] The provider at that point can appeal the FISC's order to provide the requested surveillance at three levels; first to a separate FISC judge, then to the Court of Review, and finally to the U.S. Supreme Court.[22] This way, no information is collected by the government without the involvement of the provider, which can challenge the legality of the request.

At each step of the process, the FISC and Court of Review are required to provide a written statement of its reasons for the record: when the FISC approves a government request, when the separate FISC judge decides the appeal, and when the Court of Review decides the subsequent appeal.[23] These written decisions are classified in the interest of national security, but can be published upon an order by a presiding judge *sua sponte* or on motion by a party (subject to redaction of sensitive national security information by law enforcement).[24]

Once in possession of information collected under Section 1881a, the government is prohibited from using or disclosing the information except for lawful purposes.[25] If the government intends to use or disclose information obtained or derived from a Section 1881a acquisition in a judicial or administrative proceeding against a person or business, it must provide notice of its intent to do so to both the person or business and the court that presides over the proceeding.[26] At that point, the aggrieved person or business can challenge the legality of the data collection, and if successful, the court is required to suppress the evidence consistent with evidentiary rules applicable in U.S. courts.[27]

The FISC is composed of eleven federal trial judges, and the Court of Review is composed of three federal appellate or trial judges, all publicly appointed to seven-year terms by the Chief Justice of the Supreme Court.[28] In their separate capacity as regular federal judges, each FISC or Court of Review judge has a lifetime appointment and exercises his or her judgment independent from the executive branch.

These judges do not serve as a mere formality – they provide meaningful checks that result in denials, modifications, and withdrawals of requests for government orders under FISA.[29] For example, the FISC has issued publicly rules of procedure that, among other things, require the government in submissions involving an issue not previously presented to the court – including, but not limited to, a novel issue of technology or law – to inform the court in writing of the nature and significance of the issue.[30]

As one commentator put it:

> The FISC is not at all the rubber stamp it has been periodically purported to be. The judges, after all, are sitting federal court judges, and any prosecutor or defense attorney will tell you that federal district court judges do not hesitate to demand information, accuracy and explanation when needed. FISC judges do not abandon their judicial sensibilities and responsibilities when they sit on the FISC. They bring all of their attention, consideration, and exacting requirements to their meaningful role on the court.[31]

---

[18] 50 U.S.C. § 1881a(g).
[19] 50 U.S.C. § 1881a(g)(1).
[20] 50 U.S.C. § 1881a(i)(3)(B).
[21] 50 U.S.C. § 1881a(h)(1).
[22] 50 U.S.C. §§ 1881a(h)(4), (6).
[23] 50 U.S.C. §§ 1881a(h)(4)(D), (h)(4)(E), (h)(5)(C), (h)(6)(A), (i)(3)(C), (i)(4)(A).
[24] U.S. Foreign Intelligence Surveillance Court Rule of Procedure 62, *available at* http://uscourts.gov/uscourts/rules/FISC2010.pdf; *see also In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (F.I.S.C.R. 2008) (published opinion of FISA Court of Review under similar judicial review provisions in temporary Protect America Act).
[25] 50 U.S.C. §§ 1806(a), 1881e.
[26] 50 U.S.C. §§ 1806(c), (d); 1881e.
[27] 50 U.S.C. §§ 1806(e) - (g); 1881e.
[28] 50 U.S.C. §§ 1803(a)(1), (b), (d); *see* Federation of American Scientists, *The Foreign Intelligence Surveillance Court, 2013 Membership*, http://fas.org/irp/agency/doj/fisa/court2013.html.
[29] *See* Kris & Wilson § 5:4.
[30] U.S. Foreign Intelligence Surveillance Court Rule of Procedure 11, *available at* http://uscourts.gov/uscourts/rules/FISC2010.pdf.
[31] Benjamin Wittes, *Carrie Cordero on FISA Court Lessons for a "Drone Court"* (Feb. 18, 2013), http://lawfareblog.com/2013/02/carrie-cordero-on-fisa-court-lessons-for-a-drone-court; *see also* Speech by Judge Royce Lamberth, *Remarks on the Role of the Judiciary in the War on Terrorism* (Apr. 13, 2002), *available at* http://pbs.org/wgbh/pages/frontline/shows/sleeper/tools/lamberth.html; Interview with James Baker, Frontline: Spying on the Home Front (March 2, 2007), *available at*

III. Legislative Oversight of the Use of Section 1881a

Because FISA was originally enacted due to concerns about executive branch overreaching in the name of national security, Congress has imposed numerous and substantial reporting and oversight requirements on the executive branch to determine how it exercises its authority under FISA and Section 1881a. This includes the requirement for the Attorney General, on a biannual basis, to report to the Congressional intelligence and judiciary committees on the implementation of Section 1881a, including:

- any certifications filed under Section 1881a;
- for each determination made by the Attorney General and the Director of National Intelligence to authorize surveillance on an exigent basis prior to submitting a certification, the reasons for exercising that authority;
- any directives issued by law enforcement to service providers under Section 1881a, and any actions taken by service providers or law enforcement to challenge or enforce those directives;
- a description of significant legal interpretations of Section 1881a by the FISC and Court of Review along with copies of any such interpretations;
- certain internal implementation details pertaining to Section 1881a, including any procedures implemented and compliance reviews by law enforcement; and
- a description of any incidents of noncompliance with internal procedures or court orders by members of the intelligence community and service providers.[32]

In recently describing the government's compliance with these reporting obligations, Senator Dianne Feinstein (D–Calif.) reported:

> For the past four years, the Senate Select Committee on Intelligence has conducted robust oversight of the Executive Branch's use of the surveillance authorities added to the Foreign Intelligence Surveillance Act (FISA) by the FISA Amendments Act of 2008 (FAA). . . . Collectively, the assessments, reports, and other information obtained by the Committee demonstrate that the government implements the FAA surveillance authorities in a responsible manner with relatively few incidents of non-compliance. Where such incidents have arisen, they have been the inadvertent result of human error or technical defect and have been promptly reported and remedied. Through four years of oversight, the Committee has not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law. Moreover, having reviewed opinions by the FISA Court, the Committee has also seen the seriousness with which the Court takes its responsibility to carefully consider Executive Branch applications for the exercise of FAA surveillance authorities.[33]

In addition, under FISA generally, the responsible law enforcement agencies must inform the Congressional intelligence and judiciary committees of the number criminal cases in which information obtained through FISA has been authorized for use at trial.[34]

IV. A Comparison of Procedures in National Security and Foreign Intelligence Investigations in Other Countries

Despite the newfound focus of European critics on the 2008 statute, **Section 1881a imposes at least as much, if not more, due process and oversight on foreign intelligence surveillance than other countries afford in similar circumstances**. In other words, the extensive judicial procedures it requires and the robust legislative oversight exceeds what would typically be expected of a country conducting foreign intelligence surveillance.

Many other developed countries have laws similar to those of the United States governing counterterrorism or foreign intelligence investigations.[35] They have one set of procedures for traditional law enforcement access to data, and a second set of procedures for national security and foreign intelligence gathering. The latter are more secret, and many are not subject to review by judicial courts. By contrast, the United States has published its rules and procedures for these types of investigations, judicial review, and legislative oversight under FISA, and the criticism we see today of Section 1881a (as opposed to the dearth of criticism of European procedures) could very well be the result of that transparency and awareness.

In this section, we provide information about these procedures in Australia, Brazil, Canada, France, Germany, Italy, Spain, and the United Kingdom, each of which provide similar (if not greater) access to law enforcement as in the United States. Compared to these countries, the United States is much more transparent about its procedures and requires more due process protections in investigations involving national security, terrorism, and foreign intelligence.

http://pbs.org/wgbh/pages/frontline/homefront/interviews/baker.html.

[32] 50 U.S.C. § 1881f(a), (b).

[33] S. Rep. No. 174, 112th Cong. 2d Sess. at 7 (June 7, 2012), *available at* https://fas.org/irp/congress/2012_rpt/faa-extend.pdf.

[34] 50 U.S.C. § 1871(a)(3) .

[35] *See generally* Maxwell & Wolf, *A Global Reality*; INT'L DATA PRIVACY L., Vol. 2, No. 4 (2012) (issue on "Systematic Government Access to Private-Sector Data").

A. *Australia*

Australian law provides a number of exemptions from standard legal procedures for the intelligence and defense agencies. First and foremost, these agencies are either partially or completely exempt from Australian data protection law.[36]

The *Crimes Act 1914* authorizes Australian law enforcement to request electronic documents from a Cloud service provider "on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offence."[37] This request can be made with no prior court approval; in contrast, typical investigatory procedures requesting access to Cloud data require prior authorization by a judge.[38]

The *Australian Security Intelligence Organisation (ASIO) Act 1979* grants computer access powers to ASIO, Australia's domestic security organization, if a government Minister – not a judge – is "satisfied there are reasonable grounds for believing that access by the Organisation to data held in a particular computer (the target computer) will substantially assist the collection of intelligence in accordance with the Act in respect of a matter (the security matter) that is important in relation to security."[39] The law does not, however, require precise identification of the "security matter" in the warrant. Moreover, in addition to copying data relevant to a security matter, ASIO is authorized to add, delete, or alter other data on the target computer if necessary.[40]

Regarding telecommunications carriers, a term which includes some Cloud service providers, the *Telecommunications Act 1997* requires carriers to establish systems to enable the interception of communications and to provide assistance to the government as "reasonably necessary" for the enforcement of laws related to the safeguarding of national security.[41] An ASIO officer may authorize the disclosure of "specified information or specified documents" maintained by the carrier if the officer "is satisfied that the disclosure would be in connection with the performance by [ASIO] of its functions,"[42] again with no judicial authorization. ASIO also can authorize disclosure of data from telecommunications carriers prospectively,[43] which may permit it to collect information such as specific web browsing activities or the location of computing devices on an ongoing basis.[44] Covered carriers also are permitted to voluntarily disclose information to ASIO,[45] whereas U.S. law prohibits Cloud service providers from disclosing customer data to the government without legal process.[46]

Given ASIO's broad powers to issue computer access warrants, obtain telecommunications data in storage and on a prospective basis, and voluntarily obtain data from telecommunications carriers, one commentator concluded that "the powers granted to ASIO could be used for systematic, direct, and unmediated access to private-sector data."[47]

B. *Brazil*

The Brazilian Intelligence Agency ("ABIN") does not have formal investigative or surveillance authority. Rather, it is a central agency that coordinates the intelligence activities of various government institutions such as the Central Bank, the Federal Police, the Revenue Service, and the Ministries of Defense, Foreign Relations, Justice, Environment, and Finance.[48]

Despite this lack of surveillance authority, ABIN's twenty-year history has been marked by surveillance scandals. For example, in 2000, ABIN's director stepped down for surveillance activities, including surveillance of Greenpeace, the human rights group Americas Watch, the Monsanto company, and the Unification Church.[49] And in 2008, the President suspended the agency's leaders for authorizing an allegedly illegal wiretap of a Supreme Court Justice and Senator.[50]

Moreover, recent legislation has expanded the exchange of information between ABIN and other governmental bodies and, according to one commentator, "created

---

[36] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108, at 1166 (May 2008) (citing *Privacy Act 1988* §§ 7(1), (2)), *available at* http://alrc.gov.au/publications/report-108.
[37] *Crimes Act 1914* § 3ZQN.
[38] *See* Dan Jerker B. Svantesson, *Systematic government access to private-sector data in Australia*, 2 INT'L DATA PRIVACY L. 268, 270 (2012).
[39] *Australian Security Intelligence Organisation (ASIO) Act 1979* § 25A(2).
[40] *Id.* § 25A(4)(a), (b).
[41] *See* Svantesson, 2 INT'L DATA PRIVACY L. at 271 (citing *Telecommunications Act 1997* § 313).
[42] *Telecommunications (Interception and Access) Act 1979* § 175.
[43] *Id.* § 176.
[44] *See* Svantesson, 2 INT'L DATA PRIVACY L. at 271.
[45] *Telecommunications (Interception and Access) Act 1979* § 174(1).
[46] *See* Maxwell & Wolf, *A Global Reality*, at 3.
[47] Svantesson, 2 INT'L DATA PRIVACY L. at 271.
[48] *See* Bruno Magrani, *Systematic government access to private-sector data in Brazil*, 4 INT'L DATA PRIVACY L. 30, 35 (2014).
[49] *Spy Agency in Brazil Is Accused of Abuse*, N.Y. TIMES, Dec. 14, 2000, *available at* http://nytimes.com/2000/12/14/world/14BRAZ.html.
[50] *Spying on Justice*, THE ECONOMIST, Sept. 4, 2008, *available at* http://economist.com/node/12060388; *Lula suspends Brazil spy chiefs*, BBC NEWS, Sept. 2, 2008, *available at* http://news.bbc.co.uk/2/hi/americas/7593265.stm.

unprecedented integration of the Police and the ABIN's databases."[51] And in 2010, a major Brazilian newspaper exposed that the Brazilian Communications Agency was building a system to allow it to have direct access to the customer usage metadata from telecommunications carriers.[52] While the Agency has given assurances that the system will not be used for surveillance,[53] the potential scope of data collection is massive, and it not too far afield to think that ABIN or other law enforcement authorities may look to expand their spheres of influence by asserting a need to access that rich set of data for law enforcement purposes.

C. Canada

Canada's primary national security intelligence-gathering agencies, the Communications Security Establishment of Canada ("CSEC") and the Canadian Security Intelligence Service ("CSIS"), are subject to fewer limitations than Canada's general law enforcement agencies when collecting information from Cloud service providers.[54]

The Minister of National Defense may authorize CSEC to intercept private communications if certain criteria are satisfied, such as where interception is necessary to CSEC's foreign intelligence mandate, which includes the collection of information "essential to either international affairs, defence or security." Thus, the agency is not required to obtain prior judicial approval to intercept communications relating to foreign intelligence – as U.S. intelligence agents are under the FAA – and the ministerial authorizations that it obtains for such purposes last longer than authorizations to intercept communications under the Canadian Criminal Code and never need to be disclosed to those whose communications were intercepted.[55]

In addition, CSIS, which collects intelligence from Canada and abroad, is subject to its own warrant provisions under the CSIS Act. These provisions provide for judicial authorization for searches relating to the threats to national security or operations to gather intelligence relating to the capability, intentions, or activities of foreign actors – a similar scope as under FISA. Such authorizations may last up to sixty days and never require notification of the target after a search has been completed, although the activities of CSIS are reviewed by the Security Intelligence Review Committee.[56]

[51] Magrani, 4 INT'L DATA PRIVACY L. at 35.
[52] *Id.* at 33.
[53] *Id.*
[54] *See* Jane Bailey, *Systematic government access to private-sector data in Canada*, 2 INT'L DATA PRIVACY L. 207, 207 (2012).
[55] *Id.* at 213.
[56] *Id.*

D. France[57]

France enacted a law in 1991 to provide an institutional framework for interceptions of communications conducted for national security reasons. Previously, various forms of interceptions were conducted under general national security powers of the President, without any institutional safeguards. The 1991 law was enacted because the European Court of Human Rights required that invasions of privacy be provided for in a specific law.[58]

The law applies to the French government's real-time interceptions of private communications for reasons relating to national security, protection of France's economic and scientific assets, prevention of terrorism or organized crime, and related reasons.[59] The communications can be via phone or Internet. The law applies to the targeted interception of communications and not to broad, untargeted, and random monitoring of radio traffic for "defense of national interests," which can be performed by government authorities without authorization.[60] However, once broad surveillance measures reveal a potential threat, a targeted interception can only be implemented after an authorization is given by the Prime Minister's office under the 1991 law.[61] The law also permits government agents to obtain from telecommunications operators any "information or documents that are necessary for the implementation or use of the interceptions authorized by law."[62]

No courts are involved in interceptions under the 1991 law, which are kept secret. The requests for interception are presented to the Prime Minister's office, which grants the authorization.[63] Afterwards, the authorizations are presented to a special security commission that can

[57] For more detailed information on the French regime, see generally Winston Maxwell, *Systematic government access to private-sector data in France*, 4 INT'L DATA PRIVACY L. 4 (2014).
[58] *Kruslin v. France*, European Court of Human Rights, case n° 11801/85, April 24, 1990.
[59] Article L 241-2, Internal Security Code.
[60] Article L 241-3 of the Internal Security Code provides that the procedures of the 1991 law do not apply to the French government's general surveillance of airwaves for national security reasons. However, the reasoning could also be applied to general untargeted surveillance of Internet traffic. The reason why the 1991 law does not apply to general surveillance of the airwaves is that such surveillance does not target any particular individual or communication. Consequently there is no "interception" of a "communication."
[61] National Commission for Review of Security Interceptions (*Commission Nationale de contrôle des interceptions de sécurité – CNCIS*), 20th Annual Report 2011-2012, at 43 [hereinafter CNCIS 20th Annual Report].
[62] Art. L 244-2, Internal Security Code.
[63] The Prime Minister's office also can order encryption service providers to provide encryption keys to permit the decryption of encrypted communications. Article L 244-1, Internal Security Code.

evaluate the justification for the warrant and inform the Prime Minister of any concerns. The Commission is comprised of three persons: one named by the French President upon recommendation by the French *Conseil d'Etat* and the *Cour de Cassation*, one member of the National Assembly, and one member of the Senate. The Commission provides an annual report to the French Parliament.

The 1991 law is comparable to FISA in that it provides the government with broad authority to acquire data from Cloud service providers for national security reasons. Unlike FISA, however, the French law does not involve a court in the process; instead, it only involves an independent committee that only can recommend modifications to the Prime Minister. In addition, France's 1991 law is broader than FISA in that it permits interceptions to protect France's "economic and scientific potential," a justification that is lacking in FISA.

French law also requires telecom providers and "hosting providers" (a definition that would generally include Cloud providers) that provide services in France to collect and retain for one year information relating to the identity of persons storing data in the Cloud, including their email address, payment information, information relating to their password, and log information for each connection during which they access, create, or delete data.[64] French telecommunications operators also are required to retain for one year identification data and traffic logs showing each connection made by their subscribers, as well as geolocation data for mobile phones,[65] which is not required under U.S. law. These data can be accessed by government officials without a court order where necessary for national security investigations.[66] In 2011, government authorities made 34,081 requests for traffic and/or identification data for reasons relating to preventing terrorism.[67]

France's rules on data retention are based on EU Directive 2006/24/EC, which obligates EU member states to enact legislation to ensure that traffic data are retained by service providers for law enforcement purposes. On April 8, 2014 the Court of Justice of the European Union ("CJEU") annulled Directive 2006/24/EC on the ground that the indiscriminate storing of traffic data for potential law enforcement use creates a disproportionate intrusion into individuals' privacy rights, and therefore violates the European Charter of Fundamental Rights.

In light of the CJEU's decision, France's data retention rules probably are unconstitutional, and will have to be amended.

[64] Decree 2011-219 of February 25, 2011.
[65] Article R 10-13, Post and Electronic Communications Code.
[66] Articles L246-1 through L246-5, Internal Security Code.
[67] CNCIS 20th Annual Report, at 66.

In addition to the provision described above, France enacted a December 18, 2013 law that allows French intelligence agencies to collect metadata (and in particular location data) in real time from telecommunications operators without a court order. The real-time data collection must be authorized by an individual designated by the Prime Minister. The reasons justifying this real-time data collection include terrorism, national security, and "defense of France's economic and scientific potential."[68]

E. Germany

German intelligence agencies, such as the *Bundesnachrichtendienst* ("BND"), are allowed to monitor letters, telecommunications, and conversations through "individual investigation," with targeted collection of personal data to investigate serious criminal threats to the state.[69] They also are permitted to conduct "strategic surveillance" to investigate specific dangers including risk of armed attacks or drug trafficking, or to proactively gather relevant information about other countries that are important to the foreign and national security policy of Germany.[70] These searches extend to electronic communications made via the Internet.[71] A prior court order is not required to conduct strategic surveillance; instead, the responsible Federal Ministry or Federal State Authority orders the measures. If German intelligence agencies request data from certain Cloud service providers that are regulated as telecommunications carriers, the Cloud service providers are prohibited from disclosing to its customers or other parties that they provided information to the government.

The Federal Office of Criminal Investigation, the *Bundeskriminalamt* ("BKA"), has broad authority in investigations that concern national security or terrorism. For example, the BKA is permitted to use a computer virus, the so-called *Bundestrojaner* (or "Federal Trojan"), to search IT systems, monitor ongoing communications, and collect communication traffic data without the knowledge of data subjects or service providers.[72] While the BKA must obtain a court order to use the Federal Trojan, systems on which it is deployed – which may include Cloud service providers – are not aware of its deployment, as compared to the FAA through which Cloud service providers receive notice of and are given an opportunity to contest acquisition orders handed down by the FISC.

[68] Article 20, Law n° 2013-1168 of December 18, 2013.
[69] *See* Paul M. Schwartz, *Systematic government access to private-sector data in Germany*, 2 INT'L DATA PRIVACY L. 289, 291 (2012) (citing 100 BVerfGE 313, 316 (1999) (*G-10*)).
[70] *See id.*
[71] *Id.*
[72] John Leyden, *German states defend use of 'Federal Trojan'*, THE REGISTER, Oct. 12, 2011, *available at* http://theregister.co.uk/2011/10/12/bundestrojaner.

Two bodies oversee the activities of Germany's intelligence agencies. The first is a Parliamentary Control Panel, to which the intelligence agencies must report about their activities and provide files and other documents. In this manner, the Panel occupies a similar role to U.S. Congressional oversight.[73] The Panel, in turn, appoints a non-judicial body called the G-10 Committee, which supervises the processing of personal data and decides the "permissibility and necessity" of surveillance conducted by the intelligence agencies.[74]

F. Italy

Under Law n. 124 of 2007, which reformed the intelligence community in Italy, the External Security and Intelligence Agency ("AISE") and Internal Security and Intelligence Agency ("AISI") are responsible for gathering and processing all information necessary to defend external and internal security. Those agencies have the authority to collect information in order to "protect the independence, integrity and security of the Republic . . . against threats originating abroad," as well as to "defend the internal security of the Republic and its underlying democratic institutions as established by the Constitution . . . from every threat, subversive activity and form of criminal or terrorist attack" and to preserve "Italy's political, military, economic, scientific, industrial interests."[75] Intelligence activities are directly monitored by the Prime Minister and by a special Parliament Committee named COPASIR, whose function is to ensure that the AISE and AISI operate in compliance with the Constitution and the law.[76]

Unlike in normal criminal investigations, Law n. 124 of 2007 allows the intelligence agencies to collect all information necessary without a court order and does not specify the extent to which or means by which the agencies can request and collect such information. Moreover, electronic communication service providers are required to provide information requested by the agencies and to give the agencies access to their databases for cybersecurity purposes, on the basis of specific confidential agreements entered into between the agencies and the providers.[77]

Italian law allows for preventive electronic interception with the authorization of the Public Prosecutor of the Rome Court of Appeals.[78] Additionally, telecommunication providers are required to retain electronic communications traffic data for twelve months as from the date of the communication for crime prevention purposes,[79] although like France, Italy probably will have to reform its rules on data retention to reflect the April 8, 2014 CJEU decision annulling Directive 2006/24/EC.

While providers cannot retain the contents of communications, other information, such as log information, email addresses, and duration of communications are collected and retained by covered entities. Also, the competent authorities might well be able to acquire data from a Cloud service provider through a reasoned order issued by the Public Prosecutor, such as can be issued to any company. Moreover, in the light of the powers provided for by Law n. 124 of 2007, this data can be accessed by intelligence agencies where necessary to comply with the agencies' duties.

Overall, Italian law provides the security and intelligence agencies with broad powers of investigation, including the authority to acquire data from Cloud service providers for national security reasons. Unlike FISA, Italian national security surveillance law does not require prior approval by a neutral judge and has a broader scope of application because, as described above, collection is authorized when it is aimed to protect not only national security, but Italy's economic, scientific, and industrial interests as well.

G. Spain

Pursuant to Spanish Act 25/2007, electronic communications service providers in Spain must: (i) retain the data generated or processed within the context of their activities, except for the contents of communications; and (ii) disclose such data to those "authorized agents" who have been granted permission by a relevant court to access to the data for the purpose of investigating a serious offense.[80] "Authorized agents" include authorized police authorities within the context of an investigation of a serious offense, the National Intelligence Centre ("CNI") for national security purposes, and certain personnel of the Spanish Customs Surveillance Service.

In light of the CJEU's April 8, 2014 decision, however, the Spanish rules enacted based on Directive 2006/24/EC probably will have to be modified.

---

[73] Schwartz, 2 INT'L DATA PRIVACY L. at 297.
[74] *Id.* at 298.
[75] Arts. 6, 7 of Law n. 124 of 2007
[76] Art. 30 of Law n. 124 of 2007.
[77] Prime Minister Decree of January 24, 2013 in Italian Official Journal of March 19 , 2013, n. 66.
[78] By "preventive interceptions," Italian law refers to the monitoring of telephonic communications aimed at preventing and blocking serious crimes (e.g., organized crime and international terrorism). Such activities can be performed not only by the Italian Intelligence, but also by other subjects indicated in the Law (i.e. the Minister of the Intern, Police authorities), and data collected in this manner cannot be used as evidence in criminal proceedings. Law n. 133 of 2012.
[79] Art. 132 of Legislative Decree n. 196 of 2003.
[80] Spanish Act 25/2007, 18 October. "Authorized agents" include certain police bodies, the National Intelligence Centre, and certain personnel of the Spanish Customs Surveillance Service.

The law as currently enacted requires the providers to retain communications data for a period of twelve months from the date of the communication has taken place. Additionally, the government can extend the retention term for specific types of data for one additional year or reduce the term by six months, bearing in mind the costs of the data storage and its value in relation to the investigation of serious crimes. The Act 25/2007 applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered users.

According to Article 7 of Act 25/2007, the disclosure of data to "authorized agents" must only take place under a judicial order which should establish the term for the execution of the order. If the order does not indicate any period, the transmission must be made within twenty-four hours after the working day, following the one in which the operator received the order.

Article 33 of Act 32/2003 provides for rules regarding the interception of communications by authorized agents. As a general rule, interceptions must be ordered by a competent judicial authority.[81] Finally, a proposed amendment to the law would allow courts to authorize the installation of spy software (i.e., Trojan viruses) for certain investigatory purposes. However, it is not certain whether this measure ultimately will be adopted.

H. United Kingdom

In the United Kingdom, the Regulation of Investigatory Powers Act 2000 ("RIPA") allows a Secretary of State to authorize the interception of communications for one of the following purposes: (1) in the interests of national security; (2) for the purpose of preventing or detecting serious crime; (3) for the purpose of safeguarding the economic well-being of the United Kingdom; or (4) in response to a request under an international mutual legal assistance agreement.[82]

Interception warrants relating to foreign intelligence are generally issued by the Foreign Secretary. Although a warrant issued under these provisions must be "proportionate" to the intended purpose, intercepted information is expressly excluded from legal proceedings to prevent interception methods from being revealed. Thus, the courts play no role in the authorization or review of these interceptions, as they do in the United States. Moreover, while there is an Investigatory Powers Tribunal that hears complaints under RIPA, composed of nine senior members of the legal profession, the absence of a requirement to provide after-the-fact notification to those who have been placed under surveillance suggests that many who might have cause to bring claims to the Tribunal will not in practice do so.[83] Further, in situations involving national security under RIPA, it is easier to modify interception warrants and the time period for which warrants can be obtained is increased from three to six months.[84]

In addition to providing for the interception of communications, RIPA also establishes mechanisms through which law enforcement entities may require the disclosure of "communications data" (i.e., traffic, usage and subscriber data) from public and private telecommunications operators in the interest of national security or for a number of other enumerated purposes.[85] Cloud computing service providers are likely to meet the definition of "telecommunications operator" under these provisions of RIPA.[86] A party receiving a disclosure request must comply or risk being subject to civil enforcement proceedings.[87]

UK government entities also may access private-sector data through voluntary agreements with operators of databases and other companies. Sections 28-29 of the Data Protection Act 1998 expressly authorize such arrangements for national security, law enforcement, and certain other purposes. Additionally, Section 19 of the Counter-Terrorism Act 2008 broadly authorizes entities to disclose information "to any of the intelligence services for the purposes of the exercise by that service of any of its functions," thus removing any obligation of confidence or other restriction on disclosure to intelligence agencies.[88]

Under the Intelligence Services Act 1994 ("ISA"), the relevant Secretary of State has broad powers to issue warrants for the Security Service (MI5), the Intelligence Service (MI6) or the UK's Government Communications

[81] Art. 33 of Act 32/2003, of 3 November, on Telecommunications; Chapter II of Royal Decree 424/2005, of 15 April, Regulation on the Conditions for Electronic Communications Services (providing for the rules regarding the interception of communications by authorized agents); Art. 579 of the Criminal Procedure Law, the Organic Law 2/2002, of 6 May (regulating the judicial control of the National Intelligence Center and any other Organic Law).
[82] RIPA § 5(3).

[83] *See* Ian Brown, *Systematic government access to private-sector data in the United Kingdom*, 2 INT'L DATA PRIVACY L. 230, 235 (2012).
[84] RIPA §§ 10(6), 16(3A).
[85] RIPA § 22.
[86] Section 25 of RIPA defines "telecommunications operator" as "a person who provides a telecommunications service." Section 2(1) defines "telecommunications service" as "any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy."
[87] *See* RIPA §§ 22(6), (8).
[88] Brown, 2 INT'L DATA PRIVACY L. at 235.

Headquarters (GCHQ) to enter into property and seize any documents as may be required.[89]

Conclusion

In summary, the U.S. has developed over three decades a relatively complex set of rules under FISA, most recently modified by the FAA and Section 1881a, defining the circumstances under which authorities can obtain electronic information in the context of national security. The provisions are much more detailed than those in most other countries. The provisions originally were enacted to put an end to unsupervised wiretaps such as those that came to light in the Watergate scandal. As they have evolved today, these measures are more extensive and protective of privacy than exist in most countries.

There has been confusion based on the reports of casual commentators who have sounded the alarm about Section 1881a. This confusion can be attributed to the following three reasons.

First, as noted above, the FISA provisions are long and complex. A casual reader can mistakenly conclude that the foreign intelligence measures targeting non-Americans are indiscriminate and conducted without court supervision, which is incorrect. Instead, the government must certify before the FISC that the surveillance is to obtain "foreign intelligence information," a term closely tied to the hostile acts and official activities of foreign countries and terrorist organizations. Incongruously, some commentators compare FISA measures to normal criminal investigations in Europe. That is comparing apples to oranges. Because countries generally provide greater and more visibly protective due process protections in standard criminal proceedings than when conducting foreign intelligence surveillance, it is misleading to compare standard criminal investigative procedures in Europe with American foreign intelligence procedures under FISA.

Second, decisions relating to national security surveillance are classified in the U.S. as they are in France and in other European countries. Only certain qualified U.S. judges and members of Congress have access to the actual decisions. While it is not possible to access this classified data that could disprove Europeans' suspicions, there are plenty of published, unclassified procedures and protections incorporated into the U.S. intelligence-gathering process that provide important checks on U.S. law enforcement. Moreover, there has been a recent effort by civil liberties groups and members of Congress in the U.S. to declassify FISC opinions, which has resulted in the intelligence community's publication of additional FISC opinions in the past year.[90]

Lastly, the debate seems to start from the unsubstantiated premise that the U.S. law enforcement agencies are likely to violate their own laws, or are more likely to do so than their counterparts in other countries. The U.S., Australia, Brazil, Canada, France, Germany, Italy, Spain, the UK, and many other countries are known for their effective counterterrorism capabilities.[91] It would be naïve to think that these countries' intelligence agencies do not utilize information collected from Cloud service providers in their investigations, and as allies do not work with each other to achieve mutual national security. However, these relationships are formalized and prominent under U.S. law, unlike in some other countries, and other evidence suggests that the protections under the FAA and Section 1881a are greater than in other countries.

[89] *See* ISA s.5.

[90] *See* Shawn Turner, Dir. of Pub. Affairs, Office of the Dir. of Nat'l Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)* (Aug. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa.

[91] *See, e.g.*, Steven Erlanger, *Fighting Terrorism, French-Style*, N.Y. TIMES, March 30, 2012, http://nytimes.com/2012/04/01/sunday-review/the-french-way-of-fighting-homegrown-terrorism.html.