United States Compliance with Article 15 of the Budapest Convention on Cybercrime in its Collection of Foreign Intelligence Information and Use in Criminal Investigations

Discussion paper

Prepared by

Joseph J. Schwerha IV, M.S., J.D.

for the

Octopus Conference

Council of Europe, Strasbourg, France, 4-6 December 2013

www.coe.int/octopus2013

Version 20 November 2013

Contents

INTRODUCTION

Earlier this year, Edward Snowden revealed what he believed to be improper national intelligence gathering techniques that were being utilized by the United States National Security Agency. Reminiscent of George Orwell's 1984, Mr. Snowden's revelations illustrated how secret court orders permitted the capturing of data from perhaps almost every telephone call in the United States. This sparked an international debate on the extent civilized societies want our government to be able to capture and/or monitor communications. Numerous articles have been written about what types of communications may be used in criminal investigations. However, not many have been produced to question whether or not basic civil rights have been preserved under the collection of evidence pursuant to powers provided by United States law on national security. This article initiates a discussion about whether our current national security foreign intelligence gathering paradigm is consistent with the United States' obligations under the Council of Europe's Cybercrime Convention.

This article has five primary parts. Part I summarizes the current state of affairs under the U.S. law for compliance with Article 15 of the Budapest Convention. This is, essentially, a summary of part of an earlier work this author drafted for the Economic Crime Program of the Council of Europe. Part II reviews the events that gave rise to the present controversy, summarizing the history of Mr. Snowden and what he revealed. Part III reviews the legal authority for collection of information relevant to national security. Part IV describes the circumstances under which law enforcement officers may obtain and use information that was first gathered in under national security law. Part V analyzes whether the techniques and circumstances under which said information is obtained comports with the United States' obligations under Article 15 of the Budapest Convention.

PART I: PROTECTIONS MANDATED BY ARTICLE 15

On January 1, 2007, the Council of Europe's Convention on Cybercrime (hereinafter referred to as the "Convention"), went into full effect.[1] Upon ratification of the Convention, the United States arguably already had many of the provisions within its legal system since signing it in November of 2001. While the United States does provide for conditions and safeguards as called for by Article 15, one must really look beyond pure criminal procedure to see how these conditions and safeguards are implemented in practice.[2]

Section 2 of the Convention is made up of Articles fourteen through twenty one.[3] Consequently, the topics covered in those articles are self-evident from the titles themselves:

> "Article 14 – Scope of procedural provisions";

[1] This paper is dedicated to my father. While he was a skilled and well-known physician and scholar, he always told me that the people who succeed in life are not necessarily the most talented, but the most determined. I will never forget that.

[2] For instance, the *Health Insurance Portability and Accountability Act* **(***HIPAA***)** of 1996 (P.L.104-191), requires that a person consent before the data holder could give it to the police voluntarily and before a court order was put into place.

[3] *See* COE Convention on Cybercrime.

"Article 15 – Conditions and safeguards";
"Article 16 – Expedited preservation of stored computer data";
"Article 17 – Expedited preservation and partial disclosure of traffic data";
"Article 18 – Production order";
"Article 19 – Search and seizure of stored computer data";
"Article 20 – Real-time collection of traffic data"; and
"Article 21 – Interception of content data".[4]

This article is particularly concerned with the United States perspective on the conditions and safeguards set forth in Article 15 in light of recently revealed tactics for information collection relevant to national security.

Article 15 is a subsection of Section 2 of the Convention. It is comprised of three paragraphs, each one addressing a different aspect of how the governmental powers provided by the Convention shall be limited by "conditions and safeguards provided under its domestic law, which shall provide for the adequate protection of human rights and liberties."[5] The entire article is set forth as follows:

> "Article 15 – Conditions and safeguards
> Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
> Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
> To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.[6]"

Paragraph one primarily mandates "conditions and safeguards" that are sufficient to ensure the "adequate protection of human rights and liberties." Further, paragraph one states that any such conditions or safeguards "shall incorporate the principal of proportionality".[7] The clause is inclusive but not limiting, in that it defines those human rights and liberties as including two specific instruments: 1. The 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, and 2. The 1966 United Nations International Covenant on Civil and Political Rights[8], as well other "applicable international human rights instruments".[9] While Article 15 does not define the human rights and liberties provided by such documents, the Preamble to the Convention mentions that those documents "reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the

[4] *Id.*
[5] *See* Art. 15 (1) of the COE Convention on Cybercrime.
[6] *Id.*
[7] *Id.*
[8] The protections set forth by these two instruments will be discussed later herein.
[9] *Id.*

freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning respect for privacy."[10]

Paragraph two attempts to identify various forms of "conditions and safeguards" that the Convention deems mandatory.[11] It states that said conditions and safeguards "shall"[12], include at least three things: 1. "judicial or other independent supervision", 2. "grounds justifying application", and 3. that such "power or procedure" shall be limited in "scope" and "duration".[13] It should be noted, however, that said limitations must also be "appropriate in view of the nature of the procedure or power concerned".[14]

Paragraph three concerns itself with a very particular issue: how the powers and procedures provided for in section 2 will impact the "responsibilities and legitimate interests of third parties".[15] Such concern must only be present, however, when it is "consistent with the public interest", and which further goes on to define "public interest"[16] as specifically including "the sound administration of justice."[17]

The protections for civil liberties in the United States derives from a combination of protections set forth in the United States Constitution, State Constitutions, Federal Statutes, State Statutes and relevant case law. While it is beyond the scope of this article to discuss every protection, the author attempts to discuss the particular statutory and case law citations when most appropriate.[18] In an earlier article, this author analyzed whether the U.S. provided for Article 15 Safeguards in criminal prosecutions. However, current events have caused curiosity about whether the acquisition of evidence under the procedures allowed under U.S. National Security defense also arguably comply with Article 15

[10] *See* Preamble to Council of Europe Convention on Cybercrime (signed 23 Nov. 2001) ETS 185.
[11] Council of Europe Convention on Cybercrime (signed 23 Nov. 2001) ETS 185, Article 15(2).
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *See* Council of Europe Convention on Cybercrime (signed 23 Nov. 2001) ETS 185.
, Article 15(3).
[16] *Id.*
[17] *Id.*
[18] It should be noted that scores of authors have written thousands of pages on United States criminal procedure and constitutional protection of civil liberties. The scope of this article is merely to illustrate the most evident implementation of the safeguards and conditions called for in Article 15 of the Convention.

PART II: REVELATIONS ABOUT NATIONAL SECURITY TECHNIQUES

In May of 2013, Edward Snowden left his job as a subcontractor for the National Security Agency and revealed details about several sensitive intelligence gathering programs which have been utilized both within the United States and at least one other country. The details were so profoundly worrisome to the international community, that Mr. Snowden immediately became international news, and the world asked questions of both the United States and their own governments about what techniques are appropriate in modern society.

Who is Edward Snowden?

Edward Snowden is an American former technical contractor for the United States National Security Agency and a former employee of the Central Intelligence Agency who leaked details of several top-secret United States and British government mass surveillance programs to the press. Born on June 21, 1983 in North Carolina[19], Snowden did not finish high school, instead opting to obtain his GED.[20] In 2004, Snowden enlisted in the United States Army as a special forces recruit, but had to halt training when he broke both of his legs in a training accident.[21] From there, Snowden became a security guard for the NSA[22] before joining the CIA to work on IT security.[23] A self-proclaimed "computer wizard," Snowden was stationed in Switzerland in 2007 by the CIA to maintain computer network security before leaving the agency in 2009.[24] He then began work as a private contractor for the NSA at a U.S. military base in Japan., where he had access to classified contracts and remained on the payroll until early 2013[25] before beginning work as a consultant. At the time of his departure from the United States in May 2013, Snowden had been in that position for less than three months.[26] Intelligence officials claim that Snowden was simply a system administrator, while Snowden himself described his job title as "infrastructure analyst," a position that would include looking for ways to penetrate the communications traffic around the world.[27] Later, Snowden would claim he took the job specifically so that he could gather information on the NSA that he could later leak to the press.[28]

---

[19] Ruth, Susan (June 12, 2013). *"Snowden's loose lips on NSA: A millennial generation thing?"*. *The Washington Post*. Retrieved July 26, 2013.
[20] Greenwald, Glenn; MacAskill, Ewen; Poitras, Laura (June 9, 2013). *"Edward Snowden: the whistleblower behind the NSA surveillance revelations." The Guardian*. Retrieved July 26, 2013.
[21] Gaskell, Stephanie (June 10, 2013). *"Records show Army discharged Edward Snowden after 5 months"*. *Politico*. Retrieved July 26, 2013.
[22] Leger, Donna Leinwand (June 10, 2013) "*Who is NSA whistleblower Edward Snowden?*" *USA Today*. Retrieved July 26, 2013.
[23] "*Edward Snowden: Ex-CIA worker comes forward as leaker, says he was protecting 'basic liberties'*" (June 10, 2013). Chicago Tribune. Retrieved July 26, 2013.
[24] Memmott, Mark (June 10, 2013). *"Who Is Edward Snowden, The Self-Styled NSA Leaker?"* NPR. (Retrieved July 26, 2013)
[25] Drew, Christopher; Shane, Scott (July 4, 2013). *"Resume Shows Snowden Honed Hacking Skills" The New York Times*. Retrieved July 26, 2013.
[26] Bacon, John. *"Contractor fires Snowden from $122,000 per-year job." USA Today*. Retrieved July 26, 2013.
[27] Shane, Scott; Sanger, David E. (June 30, 2013). *"Job Title Key to Inner Access Held by Snowden"*. *The New York Times*. Retrieved July 26, 2013.
[28] Lam, Lana (June 24, 2013). "*EXCLUSIVE: Snowden sought Booz Allen job to gather evidence on NSA surveillance." South China Morning Post* (Hong Kong). Retrieved July 26, 2013.

Snowden reached out to three journalists to leak the information he had gathered on the NSA: Laura Poitras, a member of the Freedom of the Press Foundation and a documentary filmmaker whom Snowden chose to contact in January 2013[29]*;* Glenn Greenwald, another member of the Freedom of the Press Foundation and a reporter for *The Guardian* who claimed to have been in contact with Snowden since February 2013[30]; and Barton Gellman, a writer for *The Washington Post* who said his first direct contact with Snowden was in May of 2013.[31] Snowden communicated via encrypted e-mails, and allegedly related to the journalists that he recognized that there would be punishment for his actions and that they, too, were in extreme danger until the information was published. In May 2013, Snowden took temporary leave from his position at the NSA center in Hawaii under the pretext of seeking treatment for his epilepsy. Snowden traveled to Hong Kong, where he remained until the first articles detailing the leaked information were published on June 6, 2013.[32] In those articles, Snowden divulged the existence and top secret protocols of several NSA surveillance programs, most notably PRISM[33] and Boundless Informant[34]. He also revealed details of Tempora,[35]a British black-ops surveillance program run by the NSA's British partner, GCHQ. At his request, *The Guardian* revealed their source as Snowden on June 9, 2013. Snowden has said that he chose to go public with the information to protect civil liberties, and chose to forego anonymity because he knows he has done nothing wrong.[36] "I don't want to live in a society that does these sort of things…I do not want to live in a world where everything I do and say is recorded," says Snowden.

Since the leaks have been published, Snowden has sought political asylum in 26 different countries.[37] On June 23, 2013, Snowden left Hong Kong and traveled to Moscow, as Hong Kong authorities were considering granting the United States' request for Snowden's extradition.[38] With his United States passport revoked, Snowden has been stuck in transit in a Moscow airport

---

[29] Carmon, Irin (June 10, 2013*). "How we broke the NSA story"*. *Salon*. Retrieved July 26, 2013.

[30] Weinger, Mackenzie (June 10, 2013). *"Barton Gellman, Glenn Greenwald feud over NSA leaker"*. Politico. Retrieved July 26, 2013.

[31] Gellman, Barton (June 10, 2013*). "Code name 'Verax': Snowden, in exchanges with Post reporter, made clear he knew risks"*. *The Washington Post*. Retrieved July 26, 2013.

[32] Yang, Jia Lynn (June 10, 2013). *"Edward Snowden faces strong extradition treaty if he remains in Hong Kong"*. *The Washington Post*. Retrieved July 26, 2013.

[33] PRISM is an NSA surveillance program operating under FISA which allows the intelligence community in the U.S. to tap directly into the servers of nine U.S. internet providers to extract and monitor communications between foreign nationals. The program has received must criticism for its tendency to "incidentally" collect American communications as well.

[34] Boundless Informant is a program used by the NSA to count and categorize the data it collects from its intelligence programs (metadata)—it focuses on categorization and volume, as opposed to content. "Boundless Informant: NSA explainer – full document text" (June 8, 2013). http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text. Retrieved July 28, 2013.

[35] Gellman, Barton; Poitras, Laura (June 6, 2013). *"U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program". The Washington Post*. Retrieved July 28, 2013.

[36] *"NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'"* (video) (June 9, 2013). *The Guardian*. Retrieved July 26, 2013.

[37] *"Edward Snowden seeks asylum in 20 nations, but gets no immediate takers"* (July 20, 2013). CBS News. Associated Press. Retrieved July 4, 2013.

[38] Barrett, Devlin; Chen, Te-Ping (June 24, 2013). *"Snowden on the Run"*. *The Wall Street Journal*. Retrieve July 26, 2013.

for over a month with no travel papers.[39] Since his arrival in Moscow, the United States has tried, unsuccessfully, to convince Russian leaders to return Snowden to the United States for prosecution. It has become known that Snowden has applied for asylum in Russia and has agreed to their terms, one of which was his pledge to not further harm U.S. interests.[40] On July 26, 2013, the Russian President's spokesman reiterated Russia's position that they did not intend to "hand anyone over."

What Activities of U.S. Intelligence did he reveal?

PRISM is a mass electronic surveillance data-mining program that is run by the National Security Agency (NSA).[41] The program, which commenced in 2007 in the wake of the Bush administration's Protect America Act[42], is designed to collect and analyze foreign communications in an effort to further the United States' antiterrorism efforts. PRISM, while court approved, does not necessitate individual warrants. Instead, the program functions under broader authorization from federal judges[43] who supervise the use of the Foreign Intelligence Surveillance Act (FISA).[44] Although the court-approved program focuses on foreign communications traffic, such communications often stream through U.S. servers—even when sent from one foreign country to another. Therefore, the program allows the NSA and the U.S. intelligence community to tap directly into the servers of nine U.S. Internet providers (Microsoft, Yahoo, Google, Facebook, YouTube, Skype, AOL, Apple, and PalTalk) to extract audio and video chats, photographs, e-mails, documents, and connection logs.

Slides detailing the program's practices and objectives were leaked to the *Washington Post* on June 6, 2013 by Edward Snowden, an NSA contractor. According to a slide that specifies the program's process, when an NSA analyst "tasks" the PRISM system for information about a new surveillance target, the request is automatically passed to a supervisor who reviews the "selectors," or search terms, that were used by the analyst. The supervisor must approve the analyst's "reasonable belief" (defined as 51 percent confidence), that the stated target is a foreign national who is outside of the United States at the time of collection.[45] For stored communications, but not for live surveillance, the FBI consults its own database to ensure the selectors do not match any known Americans. After communications information is gathered, the data is processed by specialized systems that handle voice, video, and "digital network information" (which includes the locations and unique device signatures of targets). Each target is assigned a case notation, and (depending on the provider) the NSA may receive

---

[39] *"Russia and US security services 'in talks' over Snowden"* (July 26, 2013). BBC. Retrieved July 29, 2013.

[40] "Fugitive Edward Snowden applies for asylum in Russia" (July 16, 2013) BBC.

[41] Gellman, Barton; Poitras, Laura (June 6, 2013). *"US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program"*. *The Washington Post*. Retrieved July 27, 2013.

[42] The Protect America Act of 2007 is a controversial amendment to the Foreign Intelligence Surveillance Act (FISA) that removed the warrant requirement for government surveillance of foreign intelligence targets that are "reasonably believed" to be outside of the United States.

[43] FISA created the Foreign Intelligence Surveillance Court (FISC). It is comprised of eleven federal judges appointed by the Chief Justice of the United States, who oversee requests for surveillance warrants.

[44] FISA (1978) prescribes procedures for physical and electronic surveillance, as well as the collection of foreign intelligence information between foreign powers.

[45] *NSA slides explain the PRISM data-collection program*, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Retrieved July 27, 2013.

live notifications when a target logs on or sends communications. Voice and text chats may also be monitored as they happen. According to the slides leaked by Snowden, as of April 5, 2013, there were 117,675 active surveillance targets in PRISM's counterterrorism database.

Criticism of PRISM has been swift and unforgiving, claiming that the program is unconstitutional and a flagrant abuse of privacy.[46] Critics of the program[47] have been quick to identify the tendency of the federal government (namely, the intelligence community) to overstep its bounds in the name of national security.[48] Opponents of PRISM also cite the fact that in the program's quest to obtain its targets' communications, many other Internet users (and among them, many Americans) have their communications collected "incidentally." This raises civil rights issues, specifically ones pertaining to the Fourth Amendment. Critics argue that the Supreme Court has long since held that where a person has a reasonable expectation of privacy, search and seizure may occur only once the government has obtained a warrant, supported by probable cause and issued by a judge, specifying the placed to be searched and items to be seized. Those who condemn PRISM do so under the belief that Americans reasonably expect that their movements, communications, and decisions will not be recorded and analyzed by the government and therefore collection of such intelligence requires a warrant—which PRISM does not. Several class action law suits are pending in the courts, including a $20 billion dollar suit filed by former Justice Department prosecutor Larry Klayman, which names President Obama, Attorney General Eric Holder, the heads of the NSA, and many participating companies who have collaborated with PRISM as defendants.[49]

PRISM is a National Security Agency (NSA) program recently uncovered that aims to collect and monitor the communications of foreign nationals by directly tapping into U.S. Internet servers. Similarly, Boundless Informant is a data analysis and visualization system used by the NSA to give its managers summaries of the organization's worldwide data collection activities. [50] Unlike PRISM, however, the purpose of Boundless Informant is to count and categorize the communications that are recorded by the United States' intelligence community, rather than focusing on their content. While data mining projects such as these have existed for decades, recent amendments to FISA[51] have made it easier for intelligence agencies to survey and collect data without obtaining individual warrants.[52]

---

[46] Granick, Jennifer Stisa; Sprigman, Christopher Jon (June 27, 2013). "*The Criminal NSA*". *The New York Times*. Retrieved July 28, 2013.

[47] Donohue, Laura (June 21, 2013). "NSA *surveillance may be legal — but it's unconstitutional*". *The Washington Post*. Retrieved July 28, 2013

[48] Lawrence, Jill (June 7, 2013). "*Why PRISM is Different and Scarier Than Other NSA Spying*". *The National Journal*. Retrieved July 28, 2013.

[49] Nelson, Steven (June 12, 2013). "*PRISM Class-Action Lawsuit Filed: $20B, Injunction Sought Against 'Complicit' Companies and Officials*". *U.S. News*. Retreived July 28, 2013.

[50] Greenwald, Glenn; MacAskil, Ewen (June 11, 2013). "*Boundless Informant: the NSA's secret tool to track global surveillance data*". *The Guardian*. Retrieve July 27, 2013.

[51] FISA stands for the Foreign Intelligence Surveillance Act. This Act prescribes procedures for physical and electronic surveillance, as well as the collection of foreign intelligence information between foreign powers.

[52] The Protect America Act of 2007 is a controversial amendment FISA that removed the warrant requirement for government surveillance of foreign intelligence targets that are "reasonably believed" to be outside of the United States. Additionally, the FISA Amendments Act of 2008 immunized private companies that cooperated with U.S. intelligence agencies.

The existence of Boundless Informant was leaked to *The Guardian* on June 8, 2013 by Edward Snowden, an NSA contractor. Along with slides, the information leaked included a three-page document answering NSA officials' frequently asked questions regarding the program.[53] The document describes the program's purpose as providing the ability to dynamically describe collection capabilities through the use of metadata[54] and to graphically display the information in a map view, bar chart, or simple table. The program allows a user to a select a country and review the volume of data that has been collected on that country, as well as specific details of the data. Boundless Informant, according to the slides, is designed to answer analyst questions such as, "What type of coverage do we have on country X?" An interactive global map leaked by Snowden assigned each nation a color code based on how extensively it is subjected to NSA surveillance (green being the least, red being the most). The map showed that Iran was the most surveyed, with more than 14 billion reports in March 2013 alone, classifying it as a red country. During that time period, three billion reports were generated in the United States, classifying it as a yellow country on the map. All of this information would suggest that the purpose of Boundless Informant is pattern recognition and social network identification, as opposed to directly eavesdropping on communications.[55]

Criticisms of Boundless Informant find their bases in the Fourth Amendment of the Constitution, much like those of PRISM.[56] One of the most weighted criticisms of PRISM is its tendency to "incidentally" collect the communications of Americans.[57] The controversy as it pertains to Boundless Informant is whether it is a violation of Americans' civil rights to track that "incidentally" collected data. While United States laws restrict wiretapping and eavesdropping on the actual content of the communications of American citizens, there is little protection over the digital data created by communications when they are made.[58] While this data was less of a concern in the past, it does raise some constitutional concerns in the present.[58] The information associated with communications today is often equally, if not more, significant that the content of the communication itself. Advances in technology have made it possible to gain extensive knowledge about a person merely by integrating metadata, without ever reviewing the content of the communication itself. Therefore, the fact that the NSA can freely track this type of information via Boundless Informant raises some troubling privacy issues for opponents of the program, prompting new proposed legislation to regulate NSA surveillance.[59]

---

[53] "Boundless Informant: NSA explainer—full document text". http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text (June 8, 2013). Retrieved July 26, 2013.

[54] Metadata focuses on the counting and categorization of data, rather than the content of the data itself.

[55] Garber, Megan (June 9, 2013). *"Meet 'Boundless Informant,' the NSA's Secret Tool for Tracking Global Surveillance Data." The Atlantic*. Retrieved July 28, 2013.

[56] The Fourth Amendment prohibits unreasonable searches and seizures and requires a warrant to be judicially sanctioned and supported by probable cause. PRISM's critics believe the "incidental" collection of American communications in the program's quest to obtain foreign intelligence constitutes a violation of this civil right.

[57] Donohue, Laura (June 21, 2013). "*NSA surveillance may be legal — but it's unconstitutional*". *The Washington Post*. Retrieved July 28, 2013

[58] Risen,James; Lichtblau, Eric (June 8, 2013). "*How the U.S. Uses Technology to Mine More Data More Quickly" The New York Times*. Retrieved July 29, 2013.

[59] "Sen. Paul to Introduce Fourth Amendment Restoration Act of 2013" (June 6, 2013). http://www.paul.senate.gov/?p=press_release&id=838.

PART III: GATHERING OF FOREIGN INTELLIGENCE INFORMATION

Collecting information for national security purposes has several facets. This section details some of the legal authority available within the United States' legal system, as well as some of the current methods for acquiring said information.

The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978, 18 U.S.C. §§ 1801 et seq., is the preeminent United States law regarding collection of "foreign intelligence information"[60] that is communicated or sent by "foreign powers"[61] or "agents of foreign powers"[62]. Information

[60] Under 18 U.S.C. § 1801(e), foreign intelligence information means:
"(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
(A) actual or potential attack 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 or by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States."

[61] Under 18 U.S.C. § 1801(a), foreign power is defined as follows:
"(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign-based political organization, not substantially composed of United States persons;
(6) an entity that is directed and controlled by a foreign government or governments; or
(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction."

[62] Under 18 U.S.C. § 1801(b), an agent of a foreign power is defined as follows:
"(1) any person other than a United States person, who—
(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
(C) engages in international terrorism or activities in preparation therefore;
(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or
(2) any person who—
(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

obtained is set forth in a statutory framework to obtain such information via wiretapping, physical searches, pen registers, trap and trace devices, or other access to things such as business records.[6364] The FISA contains limits on how these powers can be applied to "U.S. Persons".

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C)."

[63] *See* Liu, Edward C. *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services (April 8, 2013).

[64] Legislative attorney Edward C. Liu has a good discuss of the powers granted by the Electronic Communications Privacy Act as opposed to FISA:

"ECPA provides three sets of general prohibitions accompanied by judicially supervised exceptions to facilitate law enforcement investigations. The prohibitions address (1) the interception of wire, oral, or electronic communications (wiretapping); (2) access to the content of stored electronic communications and to communications transaction records; and (3) the use of trap and trace devices and pen registers (essentially in-and-out secret "caller id" devices).

In some circumstances, the use of surveillance activities for foreign intelligence purposes might fall within the scope of the activities prohibited by ECPA. There are two exceptions to ECPA's general prohibitions that address this situation.

First, if the activity in question falls within the definition of electronic surveillance under FISA, then it may be conducted if the government complies with FISA's procedures. For example, the interception of a domestic telephone call is the type of activity that would generally be prohibited by ECPA. It would also qualify as electronic surveillance under FISA. Therefore, if the government obtained a court order from the FISC authorizing the interception of that call, it would be a lawful surveillance activity notwithstanding the general prohibition against wiretapping found in ECPA.

Second, if the activity in question is not electronic surveillance, as that term is defined in FISA, but involves the acquisition of foreign intelligence information from international or foreign communications, then it is not subject to ECPA. For example, the interception of an international telephone call would not be considered electronic surveillance for purposes of FISA if the target were the person on the non-domestic end of the conversation and the acquisition would not occur on United States soil. So long as the purpose of that acquisition was to acquire foreign intelligence information, then it would not be subject to the general prohibitions in ECPA.

Although both exceptions result in the non-application of ECPA, they differ in one important aspect that is particularly relevant to understanding the changes wrought by Title VII of FISA. Both ECPA and FISA provide that the two statutes constitute the exclusive means of conducting electronic surveillance, as defined in FISA. As a result, using the procedures under FISA is compulsory for those activities that qualify as electronic surveillance but cannot be accomplished by, and are exempt from, ECPA. In contrast, prior to the FISA Amendments Act, FISA's procedures were generally never needed for wiretapping activities that did not qualify as electronic surveillance, and which were also exempt from ECPA because they involved international or foreign communications. However, as discussed below, the recently added § 704 of FISA does make FISA's procedures compulsory when the target of such surveillance is a United States person. Those activities that remain beyond the scope of either ECPA or FISA are governed by Executive Order 12333 and the Fourth Amendment, discussed in the next two sections."

See Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services, at 2-3 (April 8, 2013)

While more specifically defined in 18 U.S.C. § 1801, it refers to U.S. citizens, lawfully admitted permanent resident aliens and corporations incorporated within the United States.[65] It contains several sections that not only detail the procedure for applying for authorization for a warrant to seek certain foreign intelligence information; but, it also designates safeguards for violations thereof. The effectiveness of those safeguards largely have been called into question due to the secrecy of the FISA Court, and the fact that no one, as far as can be determined, has ever been sanctioned under those subsections. Said procedures will, nonetheless, be discussed below.

The FISA was introduced as a bill on May 18, 1977 by Senator Ted Kennedy, and was signed into law in 1978 by then President Carter. The FISA was the result of U.S. Senate Committee investigations into President Richard Nixon's use of Federal employees to spy on political groups. The leaders of the investigation were Senators Sam Irvin and Franck Church, which is why the Committees were sometimes referred to as the Church Committee. This committee, which was formally the United States Senate Committee to Study Governmental Operations with Respect to Intelligence Activities, ultimately became the U.S. Senate Select Committee on Intelligence. In 1975 and 1976 the Church Committee published fourteen different reports regarding the intelligence agencies, their transgressions, as well as suggested reforms. These activities were well documented.

The Patriot Act Changes to the FISA

The USA PATRIOT ACT of 2001 was signed into law on October 26, 2001 by then President George W. Bush. It was comprised of several acts bills that had not passed previously, cumulatively amending the Foreign Intelligence Surveillance Act of 1978, the Electronic Communications Privacy Act of 1986, as well as others. Consideration was short, as the Country reeled from being attacked. While the Patriot Act contained several controversial provisions, the most enduringly controversial ones were in Title II.

In Title II, entitled Enhanced Surveillance Procedures, surveillance procedures were amended. It allowed the Government to collect information from both U.S. citizens and non-U.S. citizens. It then changed the FISA by making the gathering of foreign intelligence information the primary purpose of that Statute to making it need only be a significant purpose.[66] This was done to remove the previous wall between foreign intelligence gathering and criminal investigations, since prior to the Amendment, in order to use the powers set forth under FISA, the government had to show that the "primary purpose" was only to gather foreign intelligence information.

Title II also expanded criminal law enforcement powers by allowing: roving wiretaps, wiretapping of "protected computers" by consent, sneak and peak warrants, greater powers for obtaining information from Internet Service Providers via subpoena. Because these were

[65] Under 18 U.S.C. § 1801(i), the FISA defines United States person as:
"a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section."

[66] USA PATRIOT ACT (U.S. H.R. 312, Public Law 107-56), Title II, Sec. 218.

controversial, however, the numerous sections were automatically set to expire on December 31, 2005, unless reauthorized.[67]

Title V contained another controversial provision. Under that section, National Security Letters were now able to be approved by the Special Agent in Charge of the FBI field office, whereas they used to have been approved by the Deputy Assistant Director of the FBI.[68]

Protect America Act of 2007

In 2005, The New York Times issued a report the U.S. Federal Government had been monitoring international phone calls and emails without having obtained any kind of warrant.[69] Several parties have alleged that this was a sea-change in domestic surveillance since the NSA traditionally had only performed surveillance outside the borders of the United States. President George W. Bush admitted that after the attacks of September 11, 2001, he had authorized the NSA to execute a Terrorist Surveillance Program, which allowed them conduct warrantless wiretaps of communications into and out of the United States if, essentially, linked to terrorist organizations.[70] The Bush administration had asserted, however, that the Authorization for Use of Military Force[71], passed by Congress on September 14, 2001, along with the President's inherent authority under Article II of the United States Constitution superseded the warrant requirements of the FISA. This seemingly continued until January of 2007.[72] Due to uncertainty in that position, on July 28, 2007, then President Bush announced he had submitted a bill to amend the FISA. It was passed by Congress on August 3, 2007.

The Bill altered the FISA in several ways. First and foremost, it redefined "electronic surveillance" so that such term would not be "construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."[73] It also changed the warrant and notification requirements. It eliminated the need for a warrant, instead substituting several areas of internal controls. It did require notification to the FISA court if any warrantless surveillance had been conducted with 72 of said surveillance. The amendments made clear that a person on a phone in the United States; but, who was talking with someone from outside the US could be wiretapped, so long that the person within the US was not a target of the investigation. It did install reporting requirements to Congress, though they were quite minimal. They had to report to Congress which had to include: 1. Incidents of corporation non-cooperation, 2.

[67] Sections 201, 202, 203(b), 204, 206, 207, 209, 212, 214, 215, 217, 218, 220, 223, 225.
[68] USA PATRIOT ACT (U.S. H.R. 3162, Public Law 107-56)
[69] *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services (April 8, 2013), citing, James Risen and Eric Lichtblau, Bush Lets US Spy on Callers Without Courts, N.Y. Times, December 16, 2005, at 1.
[70] *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services, at 4 (April 8, 2013).
[71] Pub. L. 107-40
[72] *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services, at 5 (April 8, 2013), citing, S.Rept. 110-209, at 4. See also Letter from Attorney General Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (January 17, 2007).
[73] *See* 50 U.S.C. § 1801.

Incidents of non-cooperation, 3. The number of certifications and directives, and 4. Reports of procedural failures. These powers were temporary and expired on February 16, 2008.[74]

FISA Amendments Act of 2008

On July 10, 2008, George Bush signed the FISA Amendments Act into law[75]. It performed several functions. First, added new sections to the FISA almost identical to the old FISA, in the form of a new Title VII which was very similar to the provision of the Protect America Act of 2007, it having expired earlier in 2008. Under the FAA, the "Attorney General and the DNI may authorize jointly, for up to one year, the 'targeting of persons reasonably believed to located outside the United States to acquire foreign intelligence information.'"[76] These procedures affected both U.S. Persons and non-U.S. persons, specifically adding:

> "• a new procedure for targeting non-U.S. persons abroad without individualized court orders;[77]
> • a new requirement to obtain an individualized court order when targeting U.S. persons abroad;[78] and
> • new procedures that can be used to obtain court orders authorizing the targeting of U.S. persons abroad for electronic surveillance, the acquisition of stored communications, and other means of acquiring foreign intelligence information."[79]

These procedures are, of course, are contained in one of a few Federal laws that allow for the use of electronic surveillance.

Extensions of Amendments in 2011

On May 26, 2011, President Obama extended three amendments to FISA through June 1, 2015. Those Amendments were originally passed as part of the USA PATRIOT Act[80], in the wake of the attacks of September 11, 2001. Recognizing that at least three of the powers granted thereby were controversial, the United States Congress established sunset provisions. These powers include:

> "• Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act (IRTPA), also known as the "lone wolf" provision, which simplifies the evidentiary showing needed to obtain a FISA court order to target non-U.S. persons who engage in international terrorism or activities in preparation therefor, specifically by authorizing such orders in the absence of a proven link between a targeted individual and a foreign power;
> • Section 206 of the USA PATRIOT Act, which permits multipoint, or "roving,"

---

[74] *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, p. 2, Congressional Research Services at 5 (April 8, 2013).
[75] FISA Amendments Act of 2008, Pub. L. No. 110-261, §403, 122 Stat. 2463, 2473 (2008)
[76] Blum, Stepanie Cooper, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 Pubic Interest Law Journal 269, 297.
[77] Citing 50 U.S.C. § 1881a.
[78] Citing 50 U.S.C. § 1881c(a)(2).
[79] Citing 50 U.S.C. § 1881b, 1881c. *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, p. 2, Congressional Research Services (April 8, 2013).
[80] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56 (2001).

> wiretaps (i.e., wiretaps which may follow a target even when he or she changes phones) by adding flexibility to the manner in which the subject of a FISA court order is specified; and
> • Section 215 of the USA PATRIOT Act, which broadens the types of records and other tangible things that can be made accessible to the government under FISA."[81]

Because of the sunset provisions, those parts of the USA PATRIOT Act had to be re-approved annually.

Renewal of FISA Amendments Act

On December 30, 2012, President Obama signed into law H.R. 5949, otherwise known as The Foreign Intelligence Surveillance Act Amendments Reauthorization Act of 2012. This extended Title VII of FISA until December 31, 2017. Title VII of FISA was added by the FISA Amendment Act of 2008. It created a new procedure for targeting non-U.S. Persons, as well as U.S. Persons reasonably believed to be outside of the United States.[82] This was immediately challenged by several lawsuits.

In February of 2013, however, the United States Supreme Court passed judgment on the constitutionality of the The Foreign Intelligence Surveillance Act Amendments Reauthorization Act of 2012. In Clapper v. Amesty International, The U.S. Supreme Court dismissed the suit on the basis that none of the plaintiffs had suffered enough definite injury to have standing to challenge Title VII.[83]

Summary of current abilities to collect foreign intelligence information

Executive Order 12333

One of the other two ways to legally authorize electronic surveillance is under Executive Order 12333. This Executive Order, states in section 2.5 thereof, as amended, that the Attorney General has the power to approve the use of any technique for intelligence purposes against a U.S. person abroad, or anywhere within the United States.[84] However, if a warrant would otherwise be required, the Attorney General must make the additional determination that the technique being utilized is so directed against either a foreign power or an agent thereof.[85] This authority must comply with FISA; but, also goes beyond the powers granted to the Attorney General by FISA.[86]

FISA authorizations

[81] Liu, Edward C., *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, CRS Report R40138 (June 16, 2011)
[82] *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services (April 8, 2013).
[83] *See Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013).
[84] *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services at 3 (April 8, 2013).
[85] *Id.*
[86] *Id.*

Different sections of Title 50 deal with different aspects of collection of data. Subchapter I covers Electronic Surveillance, generally, and is composed of Sections 1801-1812. The FISA provides a procedure for the President of the United States to order electronic surveillance without a court order under certain limited circumstances.[87] Therein, such procedure is legal if the Attorney General certifies in writing and under oath to that the electronic surveillance meets the following three criteria:

> "(A) the electronic surveillance is solely directed at—
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801 (a)(1), (2), or (3) of this title; or
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801 (a)(1), (2), or (3) of this title;
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
> (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801 (h) of this title"

The minimization procedures[88] are defined in Section 1801(h), and contain four provisions. The first is that the Attorney General shall adopt such procedures "reasonably designed" to minimize the "acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning nonconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[89] The second requirement prohibits dissemination of the identity of any nonconsenting United States person "unless such person's identity is necessary to understand foreign intelligence information or assess its importance."[90] Third, it must include procedures that permit the "retention and dissemination" of "evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[91] The fourth requirement for minimization procedures require that "no contents of any communication to which a United

[87] *See* 18 U.S.C. § 1801(a)(1)

[88] The term minimization procedures are defined under 18 U.S.C. §180(h) 1-4 as follows:
"(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person."

[89] See 18 U.S.C. §1801(h)(1).

[90] See 18 U.S.C. §1801(h)(2).

[91] See 18 U.S.C. §1801(h)(3).

States person is a party" may be "disclosed, disseminated, or used for any purpose or retained for longer than 72 hours" unless a court order under section 1805 is obtained, or if the Attorney General has decided that "the information indicates a threat of death or serious bodily harm to any person."

Subchapter II governs physical searches and is made up of Sections 1821-1829. Subchapter III deals with Pen Registers and Trap and Trace Devices for Foreign Intelligence purposes (Sections 1841-1846). Subchapter IV deals with Access to Certain Business Records for Foreign Intelligence Purposes (Sections 1861-1863). Subchapter V specifies the reporting requirements and only contains Section 1871. Subchapter VI covers additional procedures regarding persons outside of the United States (Section 1881). Lastly, Subchapter VII provides protections for those persons assisting the Government (Section 1885).

Section 1881a provides for electronic surveillance of persons outside of the United States: "[t]he Attorney General and Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[92] Subsection b, however, then immediately lays out the limitations, in that the actions authorized under subsection (a):

> "(1)may not intentionally target any person known at the time of acquisition to be located in the United States;
> (2)may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
> (3)may not intentionally target a United States person reasonably believed to be located outside the United States;
> (4)may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
> (5)shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."[93]

There is a required predicate to the joint authorization of the Attorney General and Director of National Intelligence. Such authorization must be based upon either the existence of a court order approving of a joint certification submitted by the AG and DNI, or a determination by the two officials that exigent circumstances exist".[94]

Any such acquisition must be accomplished in accordance with both the targeting and the minimization procedures heretofore established by the Attorney General and the Director of National Intelligence. It also requires submission of a certification.[95] And just in case anyone would possibly believe that someone might still need a warrant, subparagraph explicitly dispels that notion: "[n]othing in subchapter I shall be construed to require an application for a court

[92] 50 U.S.C. § 1881a(a).
[93] 50 U.S.C. §1881a(b).
[94] *See* Liu, Edward C., *Reauthorization of the FISA Amendments Act*, CRS Report R42725, Congressional Research Services at 6 (April 8, 2013).
[95] See 18 U.S.C. § 1881a(c).

order under such subchapter for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States."[96]

Pursuant to this subchapter, the Attorney General and the Director may directly order electronic communication service providers to:

> (A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and
> (B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.
> Of course, the providers get something for this cooperation. They get compensated at the prevailing rate: "for providing information, facilities, or assistance".[97] They also get a complete release from being sued by anyone for providing such assistance.[98]

Even though a judge does not oversee the issuance of the directive, there are procedures for challenging such. An ECS receiving such a directive may file a petition to modify or set aside such directive. That petition, however, is filed directly with the FISC. The original directive stands unless the presiding judge of the FISC determines that the directive at issue doesn't meet the requirements of this section "or is otherwise unlawful." Certainly, the Judge can also ask for a plenary review of the whole court, as well. Either the Government or the ECS subject to the directive could then file a petition with the Foreign Intelligence Surveillance Court of Review (FISCR) for a review of such decision rendered under subsections 4 or 5. The FISCR then must provide a written "statement for the record of the reasons for such determination."[99] If the ECS doesn't comply, however, the "the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition."[100] The presiding judge must assign a Judge to the petition within 24 hours and then that judge must issue an order with regard thereto within thirty days.[101] Subsection (i) provides for review of certifications and procedures, having very similar mechanism to those described above for directives.[102]

The whole process remains secret in the eyes of the general public. Under 50 U.S.C. § 1881a(k), the FISC shall maintain records of these proceedings. However, "[a]ll petitions under this section shall be filed under seal."[103] Nevertheless, the "Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued."[104]

---

[96] See 18 U.S.C. § 1881a(c)(4).
[97] See 18 U.S.C. § 1881a(h)(2).
[98] See 18 U.S.C. § 1881a(h)(3).
[99] See 18 U.S.C. § 1881a(h)(4)(D).
[100] See 18 U.S.C. § 1881a(h)(5).
[101] See 18 U.S.C. § 1881a(h)(5).
[102] See 18 U.S.C. § 1881a(i).
[103] See 18 U.S.C. § 1881a(k).
[104] See 18 U.S.C. § 1881a(k)(3).

There is a review procedure for assessment of the Program. Not less than every 6 months, the Attorney General and Director of National Intelligence "shall assess compliance with the targeting and minimization procedures" and shall submit same to:

> "(A) the Foreign Intelligence Surveillance Court; and
> (B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—
> (i) the congressional intelligence committees; and
> (ii) the Committees on the Judiciary of the House of Representatives and the Senate."[105]

These reports then go to the Attorney General, Director of National Intelligence and the Congressional committees referred to above as part of the semi-annual review procedure. Indeed, there is even further review mandated. There must be an annual review conducted by the head of each element of the intelligence community conducting electronic surveillance under this section. The review shall provide:

> "(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;
> (ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;
> (iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and
> (iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment."

Those heads must then use said procedures to determine if the adequacy of the aforesaid minimization procedures and how they were used.[106] In turn, those reviews must be provided to the FISC, the Attorney General and the Congressional Committees referred to above.[107]

National Security Letters

Another controversial provision in information collection under the guise of protecting national security is what has been come to known as national security letters. Section 2709 of title 18 of the U.S. Code is entitled "Counterintelligence access to telephone toll and transactional information".[108] Under this section, a special agent in charge of a field office, if designated by the Director of the Federal Bureau of Investigation, may issue a confidential demand for information relevant to international terrorism or "clandestine intelligence activities".[109] The letter may not request the content of communications. Rather, it can include the "subscriber information and toll billing records information, or electronic communication

[105] 18 U.S.C. § 1881a(l).
[106] *See* 18 U.S.C. § 1881a(l)(3).
[107] *See* 18 U.S.C. § 1881a(l)(3).
[108] 18 U.S.C. § 2709.
[109] 18 U.S.C. § 2709(b).

transactional records" in its possession.[110] The recipient must not disclose the existence of said letter to anyone except those necessary to comply with the request, or their legal counsel, as long as the requesting party makes elementary allegations regarding how disclosure could hurt one of several things, such as an investigation. While limited by statute to being issued solely by the FBI, it has been reported that the CIA and the Department of Defense have been issuing similar letters under unknown authority.[111]

PART IV: SITUATIONS WHEN INFORMATION MAY BE SHARED FOR CRIMINAL INVESTIGATIONS

It has long been a fundamental principle of U.S. law that information collected under the powers to keep the United States secure is completely separated from the information collected to protect the safety of America through enforcement of our criminal laws. There are numerous safeguards in place to protect civil liberties in the prosecution of criminal acts.[112] The purpose of this section is to discuss whether those safeguards may be avoided by collecting evidence via the powers of national security law.

There is a long history of the legal precedent used to collect information under national security law. However, for purposes of this article, we are only going to retreat about 13 years. On September 11, 2001, the U.S. intelligence community failed to prevent attacks committed by terrorists in New York, Washington, D.C., and Pennsylvania by the hi-jacking of airplanes and wrecking them into targets. This was viewed as a large failure of the U. S. intelligence system and caused a major report to be produced to determine what, if anything, could have been done differently to prevent it. The result was the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.[113] That committee made the finding:

> "Within the Intelligence Community, agencies did not adequately share relevant counterterrorism information, prior to September 11. This breakdown in communications was the result of a number of factors, including differences in the agencies' missions, legal authorities and cultures. Information was not sufficiently shared, not only between different Intelligence Community agencies, but also within individual agencies, and between the intelligence and law enforcement agencies."[114]

This supported the changes that were made in the USA Patriot Act, which were a major change to prior policy of keeping those efforts "walled off from one another through a complex arrangement of constitutional principles, statutes, policies and practices."[115] Prior to the USA

[110] 18 U.S.C. § 2709 (a).
[111] Lichtblau and Mazzetti, *Military Expands Intelligence Role in U.S.*, Washington Post (January 14, 2007)
[112] *See* Schwerha, Kaspersen, and Dragicevic, *Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime*, Cybercrime@IPA, EU/COE Joint Project on Regional Cooperation Against Cybercrime, 29 March 2012.
[113] U.S. Congress, 107th Congress, Senate, Select Committee on Intelligence, and House of Representatives, Permanent Select Committee on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attack of September 11, 2001, Report, S.Rept. 107-351, H.Rept. 107-792, December 2002, p. 33.
[114] Id. at p. xvii.
[115] Best, Richard A. Jr., Sharing Law Enforcement and Intelligence Information: The Congressional Role, CRS Report for Congress, Congressional Research Service, RL33873 (Feb. 13, 2007). Traditionally, intelligence agencies concentrate on efforts outside of U.S. territory, including the National Security Agency, the Central

Patriot Act, there had been several efforts to regulate this type of information sharing.[116] On October 26, 2001, the Patriot Act was made law, significantly changing the information sharing landscape.

In this regard, the Patriot act made several changes. A discussion of all of the changes is beyond the scope of this paper. However, some of the most significant changes for the purposes of this paper were:

> 1. It changed the requirement that FISA surveillance had to have a primary purpose of collecting foreign intelligence information to the new requirement that the collection of such information only had to be "a significant purpose" of collecting foreign intelligence information. Afterwards, FISA authority could be used to collect information where criminal investigation was the primary purpose.[117]
>
> 2. Section 504 explicitly now allowed federal officers conducting electronic surveillance and physical searches under FISA to consult with law enforcement officers at the Federal, state and local levels under certain circumstances relating to attacks, sabotage, international terrorism or attempts to collect intelligence by foreign powers.[118]

Likewise, the Patriot Act was followed by the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act 2004, which also created new procedures for sharing intelligence information about international terrorism. The latter also created the Information Sharing Environment (ISE), which was later supplemented by an implementation plan issued by the Administration.[119]

At this point, it would be fair to point out a few different salient points. A lot of the efforts with regard to information sharing was aimed at getting law enforcement officers to share information with intelligence officers, not the other way around. Naturally, these efforts wouldn't have much of an impact on Article 15 Safeguards. Also, the efforts to share information expanded exponentially, making exceptionally hard to decipher any type of bright line rule as to when information obtained under powers meant to be used to protect national security can be used to obtain information that ultimately would be shared with criminal law enforcement officers. In 2011, the Federal Bureau of Investigation issued the FBI Information Sharing Report[120], summarizing its effort to coordinate information sharing and the "Report highlights the efforts undertaken by FBI to ensure law enforcement remains relevant to this process in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties." Therein, the Report summarizes efforts as part of its joint national security and law enforcement missions. The depth of the effort makes it difficult to determine when and under what circumstances information is shared. What is easily apparent, is that there are significant efforts. Even a cursory review reveals that they need to coordinate: state and local fusion centers, national joint terrorism task forces, nationwide suspicious activity reporting

---

Intelligence Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, the Department of Homeland Security, the Bureau of Intelligence and Research of the State Department, as well as intelligence components of the military.

[116] See Sharing Law Enforcement and Intelligence Information, infra. at pp. 6-10.

[117] *Id.* p. 11.

[118] *Id.* at pp. 11-13.

[119] *Id.* at 14.

[120] *FBI Information Sharing Report*, presented by FBI Chief Information Sharing Officer (2011).

initiative, biometrics, private sector shareholders, as well as international partners and many others.[121] Likewise, at late as 2012, the Obama Administration issued the National Strategy for Information Sharing and Safeguarding, wherein it outlines its strategy to "strike the proper balance between sharing information with those who need it to keep our country safe and safeguarding it from those who would do us harm."[122] While this is helpful in that it lists protection of civil liberties among the objectives, it provides little guidance in how those are protected, in particular.

At this point in time, it is not clear what exact safeguards are in place. There is obviously great concern that such information, such as NSA electronic surveillance under FISA authority, might be prohibited from use in criminal investigations. However, there does not appear to be any publicly available resources that clearly demonstrate when the products of such surveillance may NOT be used in criminal investigations. What can be discerned is that national security must at least be a significant purpose in the original intent for conducting same. From there, however, it is much less clear what can be done with that information. Indeed, there appears that there may be the condoning of such efforts, based upon recent reports.[123]

Perhaps the most illuminating information concerning whether and under what conditions personnel from the NSA may share information with other law enforcement authorities collected under their authority with other law enforcement authorities is that set forth in the declassified orders from the FISA Court.[124]

In one order, the FISA Court approves a certification based upon the following findings:

1. "there are procedures in place … that are reasonably designed to … ensure that the acquisition … "is limited to targeting persons reasonably believed to be located outside the United States";
2. Said procedures "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States';
3. There are "minimization procedures"[125] in place that meet the requirements of subsections 101(h) and 301(4) of the FISA;

[121] *Id.* at p. i.
[122] *National Strategy for Information Sharing and Safeguarding*, Office of President of the United States (December 2012).
[123] Reuters, Exclusive: U.*S. Directs Agents to Cover Up Program Used to Investigate Americans*, August 6, 2013, available August 7, 2013 at http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.
[124] Title VII, Section 702 of the FISA is for targeting people other than U.S. Persons and is codified at 50 U.S.C. §1861.
[125] Section 101(h) provides as follows:
"(h) "Minimization procedures", with respect to electronic surveillance, means—
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

4. Guidelines have been adopted in accordance with section 702(f)[126] to ensure compliance with the limits imposed by 702(b)[127] of the FISA and that an application for a court order is filed as required;
5. That those procedures are consistent with the Fourth Amendment to the U.S. Constitution[128];
6. That "a significant purpose of the acquisition is to obtain foreign intelligence information"[129];
7. That acquisition is to be obtained directly from or with the assistance of an electronic communication provider; and
8. The acquisition otherwise complies with 50 U.S.C. 1881(b).

Attached to said certification were Exhibits A and B, among others. Exhibit A was the "procedures used by the National Security Agency for Targeting Non-United States Persons reasonably to be located outside the United States to acquire foreign intelligence information pursuant to section 702 of the foreign intelligence surveillance act of 1978, as amended." This document contains the variety of processes and guides that NSA personnel would use to determine that they are targeting a legal subject, which, due to its detail, is beyond the subject of this paper.

Said document also specifies what they do if they find out they were incorrect in determining a particular target was appropriate. In that case, the NSA would take the following steps:

> "Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures."[130]

---

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person."
See 50 U.S.C. §1801(h).

[126] Section 702 refers to part of the Foreign Intelligence Surveillance Act Amendments of 2008, which is codified at 50 U.S.C. §1881a.

[127] These are the limitations on targeting certain persons outside the U.S. and not U.S. persons. Here they are in detail:
"(b) Limitations
An acquisition authorized under subsection (a)—
(1) may not intentionally target any person known at the time of acquisition to be located in the United States;
(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
(3) may not intentionally target a United States person reasonably believed to be located outside the United States;
(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."
See 50 U.S.C. 1881(b).

[128] This is of significant debate since obtaining any of the information contemplated for a criminal investigation would necessarily require entirely different processes if done in a routine criminal investigation.

[129] See Order of August 10, 2010 of the Foreign Intelligence Surveillance Court, Docket Number 702(i)—10-02.

[130] See Order of August 10, 2010 of the Foreign Intelligence Surveillance Court, Docket Number 702(i)—10-02, p. 8.

Plus, then they would report same to the required channels within 5 business days.[131]

It is evident, however, that the protections set forth above only apply to U.S. persons and to anyone else, if they are located within the geographical boundaries of the United States, which includes "all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands".[132] Naturally, U.S. persons includes those aliens that are admitted for permanent residency within the U.S. This would not include visitors who are not admitted to take up permanent residency.

Exhibit B to said certification is titled "Minimization procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information pursuant to Section 702 of the foreign intelligence surveillance act of 1978, as amended". This applies to the "acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be outside the United States in accordance"[133].

This exhibit is particularly instructive as to how and under what circumstances information inadvertently may be used for criminal investigations. Exhibit B uses the term inadvertent to include both accidental and that which was obtained outside of the established authorizations (i.e. illegally obtained). While I appreciate the assumption that NSA agents would not intentionally violate the law, including both subsections within the definition of "inadvertent" has implications from a civil rights perspective that deserves further investigation. Section 3 (b) of Exhibit B indicates, NSA "personnel" will determine in their own judgment whether information must be destroyed, if said information does not contain foreign intelligence information, or does not contain "evidence of a crime which may be disseminated under these procedures." That paragraph goes on to state that those communications may not be kept more than five (5) years and includes "electronic communications acquired because of NSA's ability to filter communications."[134] It does not specify what may not be included, however.

Should collection include attorney client communication of a person then under criminal indictment in the United States, then that communication will be segregated so as not be used "in any criminal prosecution" but it would be allowed to be used in further NSA investigations. Any dissemination thereof must be reviewed by the NSA Office of General Counsel prior to said dissemination.[135] The Exhibit does not dictate any restriction on use of attorney-client communications for those merely under investigation.[136]

---

[131] *See* Order of August 10, 2010 of the Foreign Intelligence Surveillance Court, Docket Number 702(i)—10-02, p. 9.

[132] *See* 8 U.S.C. §1101(j).

[133] *See* Order of August 10, 2010 of the Foreign Intelligence Surveillance Court, Docket Number 702(i)—10-02, Exhibit B to Certification.

[134] *See* Order of August 10, 2010 of the Foreign Intelligence Surveillance Court, Docket Number 702(i)—10-02, Exhibit B to the Certification, p. 3.

[135] *See* Order of August 10, 2010 of the Foreign Intelligence Surveillance Court, Docket Number 702(i)—10-02, Exhibit B to the Certification, pp. 4-5.

[136] This in and of itself presents issues. Why restrict only to those under indictment? Does someone being investigated deserve less protection? I think many would argue no.

Section 5 of Exhibit B details the treatment of "domestic communications." Generally, if a communication is identified as such, it will be promptly destroyed. But, if the Director of the NSA makes one of several determinations, then such communication need not be destroyed. The most relevant subsection is number 2, which details as follows:

> "[t]he communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such communications may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes."

Thus, dissemination of domestic communications may be shared with law enforcement if said dissemination complies with the four requirements set forth above. Notably, those limitations do not set forth general "hurdles" which must be met in order to share such information. Rather, the sharing can be done if said communication is "reasonably believed" to contain evidence of a crime.

Each of the restrictions presents different issues.[137] Section 1806(b) provides no information may be provided to law enforcement unless accompanied by a statement indicating that such information may not be used in a criminal proceeding without advance authorization of the Attorney General. Section 1825 (c) provides the same disclosure, only for that subchapter.

The executive order is more involved. Executive Order 12333, as amended, is entitled "United States Intelligence Activities." Therein, the President makes several directives with regard to information sharing. As an overarching principle, it states that "[a]ll departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance."[138] Therein, many standards are established for the collection and dissemination of terrorism information, including establishment of an entire Information Sharing Environment among several agencies.[139]

Certain paragraphs are worth further exploration. In paragraph 2.5, the President delegates the "power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if

[137] The restriction of Section 1806(b) deals with when a physical search "involves" the residence of a United States person, and when the Attorney General determines that there is no duty to maintain the secrecy of the search. Under that circumstance, the Attorney General shall notify the subject of the search and identify if any such property was "seized, altered, or reproduced during such search." As the acquisition of a communication would seemingly not be a physical search of a residence, it is uncertain as to how this would be applied in practice. However, one could surmise that it could apply where a physical search was done to collect a communication; but, that is just speculation.

[138] *See* Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 132 (2003), 13355 (2004) and 13470 (2008).

[139] The structure and extent of this information sharing environment is quite involved and, therefore, is beyond of the scope of this paper.

undertaken for law enforcement purposes." However, such directive is limited to situations where the Attorney General has probable cause to believe that "the technique is directed against a foreign power or an agent of a foreign power", and if such technique involves electronic surveillance, then the Attorney General must comply with the FISA.[140] Further, paragraph 2.6 authorizes any element of the intelligence community[141] to assist law enforcement and other civil authorities, though said section does not specify when any sort of information could be shared.

Section 6 of Exhibit B deals with foreign communications of or concerning United States Persons. The collection of said information is limited by 50 U.S.C. § 1881a. However, the dissemination of said information may occur with the Federal Bureau of Investigation or the Central Intelligence Agency if the identity of the United States person is deleted and generic symbol is substituted. Otherwise, the dissemination can be made "to a recipient requiring the identity of such person for the performance of official duties", and, for the purpose of this paper, "is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed", subject to the same restrictions as for domestic communications.[142] It is also noteworthy that Section 7 specifically states that foreign communications "of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy."[143] Further, section 6(c) seems to indicate that the Central Intelligence Agency and the Federal Bureau of Investigation can identify targets directly to the NSA and the NSA may provide "unminimized" information to the CIA and FBI, who would, in turn, process them under their own minimization procedures. Lastly, section 8 delineates sharing with foreign governments. It specifically states that information obtained

[140] *See* Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 132 (2003), 13355 (2004) and 13470 (2008), paragraph 2.5.

[141] The intelligence community includes:
"(1) The Office of the Director of National Intelligence;
(2) The Central Intelligence Agency;
(3) The National Security Agency;
(4) The Defense Intelligence Agency;
(5) The National Geospatial-Intelligence Agency;
(6) The National Reconnaissance Office;
(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;
(9) The intelligence elements of the Federal Bureau of Investigation;
(10) The Office of National Security Intelligence of the Drug Enforcement Administration;
(11) The Office of Intelligence and Counterintelligence of the Department of Energy;
(12) The Bureau of Intelligence and Research of the Department of State;
(13) The Office of Intelligence and Analysis of the Department of the Treasury;
(14) The Office of Intelligence and Analysis of the Department of Homeland Security;
(15) The intelligence and counterintelligence elements of the Coast Guard; and
(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community." [141] *See* Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 132 (2003), 13355 (2004) and 13470 (2008), paragraph 3.5(h).

[142] *See* Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 132 (2003), 13355 (2004) and 13470 (2008), section 6(b), pp. 6-7.

[143] *See* Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 132 (2003), 13355 (2004) and 13470 (2008), section 7, p. 8.

under 50 U.S.C. § 1881a may be done if done in a manner consistent with subsections 6(b) and 7. Section 7 applies to foreign communications of or concerning non-United States person and provides merely states that they can be shared in any form as long as applicable with law. And we already discussed section 6(b), which allows for dissemination if evidence of a crime.

PART V: IS THE U.S. LIVING UP TO ITS PROMISES UNDER ARTICLE 15?

This author had previously participated in drafting a discussion paper, part of which covered how the civil rights protections as integrated in criminal prosecutions within the United States matched to the conditions and safeguards as mandated under Article 15.[144] Now, the question becomes whether the United States' use of its investigative powers under its national security laws is being executed in such a way as to violate the Article 15 prescriptions.

Since the Cybercrime Convention deals with criminal prosecutions, and not really terrorism investigations directly, it is assumed that conditions and safeguards would most only be violated if the both: 1. Information collected under national security law is actually used in criminal prosecutions in some way; and 2. The manner in which such information is collected is done in such way as to violate Article 15.

Is the information collected under national security law used in criminal prosecutions?

It is clear that at least some information collected is used in criminal prosecutions, though the extent of such use is uncertain. In an interview with the Washington Post on November 5, 2013, United States Attorney General Eric Holder confirmed that the United States Department of Justice has used evidence gathered in the warrantless surveillance program in criminal prosecutions. Indeed, he indicated that the Department of Justice was doing a review of all such cases and will be notifying defendants of same "where appropriate".[145] Further, as detailed elsewhere herein, there are other strong indications that the law permits such use, including those found in Executive Order 12333 and the minimization procedures used by the Department of Justice. Indeed, there does not appear to be any clear standards whatsoever that prohibit use of such information in criminal investigations. Thus, it is reasonable to conclude that such information is used in at least some criminal prosecutions.

Is information collected under national security law in such a way as to violate Article 15?

While it is evident that information collected under national security law powers is and can be used in criminal investigations, the manner, standards for and extent of such use is uncertain due the secrecy surrounding use of national security law and the sheer size of the entities collecting such information.

[144] Schwerha, Kaspersen, and Dragicevic, *Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime*, Cybercrime@IPA, EU/COE Joint Project on Regional Cooperation Against Cybercrime, 29 March 2012.

[145] Horwitz, Sari, *Justice is reviewing criminal cases that surveillance evidence gathered under FISA*, Washington Post, November 5, 2013.

The use of national security powers is secret

Whether it's the warrantless surveillance utilized under section 702 of the FISA, or distribution of National Security Letters, the actions taken are executed under the veils of secrecy. Unlike criminal prosecutions, the process and results of which are almost entirely open to the public, national security protection is entirely secretive. There are, obviously, good reasons for not publicly disclosing efforts taken in the name of national security. However, when such actions are questioned, it makes such questioning extremely difficult because the very use of those powers is secret. And while there have been some secret documents that have recently been made publicly available, the secrecy of the use of national security powers in evidence collection makes studying same almost impossible.

The size and scope of the U.S. Intelligence community makes it difficult to study

Under Executive Order 12333, the top-level branches of the U.S. intelligence community are listed as the following:

> (1) The Central Intelligence Agency (CIA);
>
> (2) The National Security Agency (NSA);
>
> (3) The Defense Intelligence Agency (DIA);
>
> (4) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
>
> (5) The Bureau of Intelligence and Research of the Department of State;
>
> (6) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and
>
> (7) The staff elements of the Director of Central Intelligence.[146]

Studying those large agencies, especially given their secretive nature is extremely difficult. However, if you combine that with the sheer scope of their operations, monitoring what they are doing would be equally difficult. According to a multi-faceted study by the newspaper named the Washington Post, they found:

> -1271 different governmental organizations and 1931 private companies work on counterterrorism, homeland security and intelligence at about 10,000 locations throughout the United States.
> -about 854,000 people have top secret clearance.
> -since 2001, over 33 different building complexes around Washington D.C. had been built, or were then under construction for top-secret intelligence work.
> -over 50,000 intelligence reports are created each based on foreign and domestic spying.[147]

Indeed, even people within that community have indicated that it is so large that studying same would be extremely difficult. General John R. Vines was reported to have told the Washington Post: "I'm not aware of any agency with the authority, responsibility or a process in place to coordinate all these interagency and commercial activities", later adding "[t]he complexity of

[146] *See* Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 132 (2003), 13355 (2004) and 13470 (2008).
[147] *See* Washington Post Study entitled "Top Secret America", 2011, http://projects.washingtonpost.com/top-secret-america/.

this system defies description."[148] Thus, it is not only hard to determine in theory the circumstances under which they would share information, but it would be beyond difficult for an outside observer to determine what is shared in actuality.

It is thereby apparent that it is beyond the capabilities of this author to determine whether, in fact, the United States may have violated the conditions and safeguards under Article 15. Nevertheless, an analysis of available evidence strongly indicates that the United States has engaged in activities that arguably need to be eliminated to assure compliance with the conditions and safeguards prescribed by Article 15.

As we previously determined, Article 15 provides for several conditions and safeguards, a review of which was done previously and does not need to be repeated here.[149] That being said, there are several areas which demonstrate the proposition that the United States may not be complying with all of those conditions and safeguards because of their activities under national security laws:

1. The standard, if any, for dissemination of evidence to criminal law enforcement authorities is unclear

Recently unclassified documents reveal that the United States intelligence community is both vast and detailed. Under the minimization procedures made available, it appears that there may be several legal standards that would dictate whether and under what circumstance evidence of a crime that was originally obtained under the legal authority provided by national security law could be later disseminated to criminal law enforcement officers.

This creates a problem of duality of standards because national security evidence could be collected and then provided to criminal law enforcement authorities without restriction. For example, examination of Judge Claire V. Eagan's opinion of the Foreign Intelligence Surveillance Court makes clear that the standards are lower under 50 U.S.C. § 1861 than under 18 U.S.C. 2703(d), which contains the equivalent criminal investigative standard.[150] If the standards are lower, and that evidence may be shared with criminal investigators, then one may certainly argue that the conditions and safeguards required by Article 15 may be being by-passed.

2. Information acquired through national security law may still be disseminated to criminal investigators without regard as to whether the disseminated information was obtained properly

In normal criminal prosecutions, evidence that is not legally obtained may not be used in that criminal prosecution due the exclusionary rule. This is a basic civil rights protection which provides incentives for law enforcement to follow the appropriate rules during criminal

[148] *Id.* at Priest and Arkin, *"A hidden world, growing beyond control".*
[149] *See* Schwerha, Kaspersen, and Dragicevic, *Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime*, Cybercrime@IPA, EU/COE Joint Project on Regional Cooperation Against Cybercrime, 29 March 2012.
[150] See *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from (redacted)*, Docket Number: BR13-1-9, Amended Memorandum Opinion, United States Foreign Intelligence Surveillance Court, Washington, D.D., pp. 12-16.

investigations. For example under 18 U.S.C. § 2511 et seq., it is illegal to intercept a wire, oral or electronic communication. If law enforcement wanted to conduct a wiretap as part of an investigation, then they would have to meet the applicable standards and receive an order from a Judge. However, under national security law, government employees may intercept a wire communication of someone as long as they meet some basic requirements, including that they are not targeting a United States person and as longs as not all of the recipients to a communication are within the United States.[151]

On August 19, 2010, Judge John D. Bates issued an order based upon a certification filed by the Director of National Intelligence and the Attorney General. The Certification made as part of the application, contained as an exhibit, the detailed minimization procedures to be utilized in national security investigations. Those procedures indicate when information may be shared with those investigating crimes. Said procedures allow for the sharing of the captured communication even if said information was collected outside of allowable methods. Theoretically, I would imagine the justification is that the investigator was not trying to investigate the crime; but, just came across evidence of the crime and could share it. However, that provides a very inconsistent standard. Normally, if evidence is obtained under circumstances not allowed, then it would be excluded. However, because evidence was happened across during a national security investigation, it may be able to be legally used in a criminal prosecution. Many could argue that this provides a problematic situation, robbing those under investigation of fundamental civil rights protections.

3. There is less protection for certain foreign nationals than those of U.S. citizens or those that qualify as United States Persons

U.S. collection of foreign intelligence information has been criticized as not protecting civil liberties of foreign citizens.[152] However, the purpose of the FISA and other associated powers really are not and were not meant for that.[153] This is especially true for data collected and stored in the cloud. For data stored therein, there are threats to civil liberties from the Patriot Act and the FISA, as amended by the FAA.[154] In particular, U.S. governmental access under the FISA was not ever designed to protect the civil liberties of European and other foreign citizens unless they found themselves physically with the United States. Even a cursory review of the FAA supports that premise. One article has summarized the concerns as follows:

> "The significance of Title 50 USC §1881a for Europeans and other non---U.S. persons located abroad can best be understood by looking at a combination of three elements. The first is the constitutional protection of U.S. persons and the lack of such protection for non---U.S. persons located outside the United States (discussed in more detail section 2.1.2). Second and related, one has to look at the background to the FISA, namely the wish to introduce a system of oversight over the acquisition of intelligence information, in view of its possible impact on the fundamental rights of U.S. persons. And third, it is important to understand that the FAA 2008 amendments to the FISA were a codification and legalization of the illegal and

[151] 50 U.S.C. § 1881a (b)(1) and (4).
[152] Van Hoboken, Arnbak and Van Eijk, *Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad* (June 9, 2013)(available at SSRN: http://ssrn.com/abstract=2276103).
[153] *Id.* at p. 7.
[154] *Id.* at pp. 4-7.

> warrantless wiretapping program of the electronic communications of U.S. citizens by the Bush administration."[155]

The purpose of these laws was to codify the manners in which collection of foreign intelligence information is collected so as to not infringe upon the rights of U.S. citizens and other U.S. persons, as described in those respective laws.

Further, this situation is exacerbated because foreign nationals within the United States will not ever know for sure whether they qualify as a "United States Person." Under the FISA and other national security laws, it is clear that United States persons get more civil rights protections than those that don't qualify as United States persons. This in and of itself may provide a problem, given the apparent lack of uniform standards in sharing of evidence with criminal investigators. However, it also presents a problem because you may not know if you qualify as a United States person. This provides an uncertainty in the amount of civil rights protections one may possess and thereby, could present an issue as to whether such situation complies with Article 15.

Under Article 15, the procedural powers to be adopted are to be "subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties..." If one believes that human rights and liberties applies to humans of all nationalities, then one may argue that the differing protections for provided for United States Persons versus non-United States Persons does not comply with Article 15. While this article is not a general review of civil liberty protections as threatened by the collection of foreign intelligence for national security purposes, this matter deserves more study in so much that at least some of the data collected under these provisions seems to find its way to law enforcement authorities.

4. Unrestricted sharing of foreign intelligence with foreign governments could lead to rampant civil rights violations by freely exchanging information in a bilateral fashion

Intelligence agencies conceivably could circumvent protections by cooperating directly with other country's intelligence agencies. While restrictions may be dependent upon whether someone has a particular relationship to the United States (i.e. citizen, U.S. person, alien with significant ties, etc.), that regime does not necessarily account for information sharing internationally between agencies. Under section 8 of Exhibit B to the 2009 Certification of the Attorney General and Director of National Intelligence, as explained in Part IV *infra*, it appears that information obtained through electronic surveillance of a foreign national while outside of the United States could be shared with criminal law enforcement authorities merely if the NSA believes that said communication contained evidence of a crime.

If other countries have similar laws, then intelligence services in both countries could give the foreign intelligence service access to domestic communication portals and bypass their own country's civil rights protections by simply having the other country's officials doing the same within their own country. Indeed, it has been reported that this information sharing has

[155] *Id.* at p. 6.

been done in other countries and the amount is uncertain.[156] Some authors describe a 2009 report issued by the Dutch Review Committee on the Intelligence and Security Services, summarizing:

> "[t]he report interestingly observes that day-to-day data sharing between agencies is mediated by the principle of 'quid pro quo': what you give is what you get. The reasoning is, that by giving away intelligence to foreign intelligence agencies, and getting some in return, intelligence agencies serve national security interests. There is a clear interest for intelligence agencies to increase their own levels of access to information in the private sector and to have as broad a possible legal powers. Interestingly, these practices are described in market terms, while privacy, confidentiality and information security interests of public and private actors are not at all mentioned. As such, the exchange between governmental agencies in different countries seems to introduce a dynamic of its own: it is perceived as a means to establish a superior information position over other agencies."[157]

The authors go on to speculate that that the individual agencies seeking information could freely exchange information with other countries that have little or no civil rights protections, thereby possibly causing "a race to the bottom in terms of information security and data confidentiality interests."[158] At the very least, this situation provides an unnecessary threat to civil rights in both countries.[159]

5. There is no evidence of proportionality in certain cases

As can be detailed above, it can be argued that there are no proportionality provisions under much of the national security legal authority described herein. For instance, there appears to be no analysis of individualized threat level in order to justify surveillance of a foreign citizen outside the United States under 50 U.S.C. § 1881a. Similarly, there is no such analysis as part of 18 U.S.C. § 2709 for issuance of a national security letter. Also, it does not appear to be a requirement for national security agencies to assess whether they can obtain this information in a less invasive fashion. Consequently, one may logically assert that there is no direct proportionality provision.

CONCLUSION

Ultimately, one also may argue that to conclude whether or not the United States complies with Article 15 would necessarily entail a comparison to other countries and what they believe constitutes compliance. Despite the differences between U.S. law and that of other countries, please remember that vast generalizations about appropriateness of protections must be couched in terms of relativity. It is noteworthy that other countries, including European ones, may have similar abilities. On May 23, 2012, the firm of Hogans Lovells released a white paper entitled: A Global Reality: Governmental Access to Data in the Cloud" wherein they performed

---

[156] *See* Van Hoboiken, Arnbak, and Van Eijk, *Obscured by Clouds or How to Address Governmental Access to Cloud Data From Abroad*, draft paper submitted at Privacy Law Scholars Conference, 6-7 June, Berkley, CA.
[157] *Id.* at 17.
[158] *Id.* at 18.
[159] Van Hoboken, Arnbak and Van Eijk, *Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad* (June 9, 2013)(available at SSRN: http://ssrn.com/abstract=2276103).

a comparative analysis of governmental access to data stored in the cloud in ten different countries, concluding that: "civil rights and privacy protections related to governmental access to data in the Cloud are not significantly stronger or weaker in any one jurisdiction, and that any perceived locational advantage of stored Cloud data can be rendered irrelevant by MLATs."[160] Their conclusions were based upon reviewing the United States, Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain and the United Kingdom.[161]

Due to the disclosures of Edward Snowden and declassification of documents from the United States Foreign Intelligence Surveillance Court, it now is apparent that information that otherwise would not be obtainable under general criminal procedure may be first captured under United States national security law and then be shared with law enforcement authorities. It is also clear that the legal authority provided to those United States personnel seeking to acquire foreign intelligence information is different than that which must be met by those doing criminal investigations. If those standards are indeed different, and information may be shared from performing national security investigations with those doing criminal investigations, then it is worth exploring whether the adequate civil rights protections provided for in the Convention are being met.

As reviewed previously, Article 15 Conditions and Safeguards probably are being met in the United States, if one just looks at the civil liberty protections provided generally for purely criminal investigations.[162] However, evaluating whether the Article 15 safeguards are being met in national security investigations is a more difficult endeavor. Both the methods and the resulting data are secret. Even the judicial oversight is secret. Moreover, the apparatus conducting intelligence operations is enormous. This article contains an initial review, and concludes with five areas of concern. Further investigation is now necessary to determine the scope and depth of this potential gap in compliance with the conditions and safeguards required under Article 15 of the Convention.

[160] Hogan Lovells, *A Global Reality: Governmental Access to Data in the Cloud*, Washington, D.C., May 23, 2102. http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf,

[161] *Id.*

[162] Even assessing conditions and safeguards under criminal procedure can sometimes be challenging since some procedures executed under that that authority can be equally elusive. *See* Scott Shane and Colin Moynihan, *Drug Agents Use Vast Phone Trove Eclipsing N.S.A.'s*, The New York Times, September 1, 2013.