UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30 | Issue 2 Article 1

2013

Prism and The European Union's Data Protection Directive, 30 J. Marshall J. Info. Tech. & Privacy L. 227 (2013)

Liane Colonna

ARTICLES

PRISM AND THE EUROPEAN UNION'S DATA PROTECTION DIRECTIVE

LIANE COLONNA*

I. INTRODUCTION

On June 6, 2013, two major news sources reported that United States national intelligence services had developed a sweeping surveillance system targeted at non-American persons located outside of the United States called PRISM.[1] Two days later, the U.S. Director of National Intelligence issued a fact sheet stating that PRISM "is not an undisclosed collection or data mining program," but rather "an internal government computer system" used to facilitate the collection of foreign intelligence information "under court supervision, as authorized" by law.[2] Although a complete understanding of the internal workings of PRISM is not publically available, the main idea behind the program is to allow the U.S. government to request personal data from nine major technology companies such as Google, Yahoo, and Facebook.[3] The U.S. government has been emphatic that it is only allowed to access this

* Liane Colonna is a doctoral candidate at the Swedish Law and Informatics Research Institute located at Stockholm University. The topic of her dissertation concerns privacy and data mining.

1. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845d970ccb04497_story.html; *see also* Glenn Greenwald & Ewan MacCaskill, *NSA Prism Program Taps into User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

2. *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, DIRECTOR OF NATIONAL INTELLIGENCE 1, 1 (June 8, 2013), http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf.

3. *See generally* T.C. Sottek & Josh Kopstein, *Everything You Need to Know about PRISM: A Cheat Sheet for the NSA's Unprecedented Surveillance Programs*, VERGE (July 17, 2013), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

data when it is authorized under U.S. law.[4]

From a European perspective, a fundamental problem raised by programs like PRISM is that there is a tremendous amount of personal data about Europeans located on U.S. servers or traveling across U.S. networks, which, is not necessarily protected under European law. When the U.S. government gains access to this data and processes the data, the U.S. government is able to engage in "extra-territorial surveillance from domestic soil."[5] This reality creates a visceral anxiety on behalf of Europeans because U.S. privacy and data protection standards are perceived to be markedly lower than European standards.[6] This means that even if the U.S. government's accessing and processing of this data is in accordance with U.S. law, European data can still be compromised, albeit from a normative human right's perspective. Furthermore, even if the privacy and data protection standards are considered tantamount, it is still true that U.S. surveillance law does not afford Europeans the same level of protection as Americans. A central question becomes: how can Europeans safeguard their personal data where the U.S. government can regularly and lawfully gain access to huge amounts of this data and then process it with dynamic techniques?

While there may be many solutions to this problem such as political solutions (refusal to enter into the EU-U.S. free trade area), economic solutions (trade sanctions), technical solutions ("FISA Proof Clouds"), the focus of this Article is on the use of the EU Data Protection Directive and the forthcoming EU Data Protection Regulation as mechanisms to ensure that personal data about Europeans is safeguarded from the ostensible threats posed by programs like PRISM. More specifically, this Article will explore whether the Data Protection Directive and/or forthcoming Regulation can be applied in such a way that would nullify or modify the way the U.S. government is able to obtain and process personal data about European residents which is collected from large, U.S. based technology firms. In other words, the goal is to explore whether the European Union can demand private U.S. companies, operating on sovereign U.S. territory, to adhere to EU data protection law when complying with security requests from the U.S. government.

---

4. *Id.*

5. Katitza Rodriguez & Tamir Israel, *Using Domestic Networks to Spy on the World: Spies Without Borders*, ELECTRONIC FRONTIER FOUND (June 13, 2013), https://www.eff.org/deeplinks/2013/06/spies-without-borders-i-using-domestic-networks-spyworld.

6. *See* Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention* 108, 2 INT'L DATA PRIVACY. L. 68, 70 (2012) ("The USA's (data protection) standards are fundamentally lower than Europe's.").

The structure of this Article is as set forth. First, the PRISM program will be briefly explained from both a technical and a legal perspective in order to understand why the program offends core EU data protection principles. Next, the EU Data Protection Directive and the forthcoming Regulation will be examined as potential tools to safeguard European personal data from the perceived threats posed by programs like PRISM. Here, the focus is placed on examining the rules regarding transfers of personal data to third countries such as those contained in Chapter IV of the current Directive. The viability of EU claims will be addressed in turn with a specific focus on whether the international community will recognize potential EU reactions to PRISM as legitimate and whether the European Union will be able to enforce any such claims.

II. PRELIMINARY ASSUMPTIONS AND CLARIFICATIONS

At the very outset, it is important to make clear that this Article will use Facebook, a social networking service provider, as a paradigmatic example. The scale of the problem of how to control large technology companies that are established in the U.S. and collect a substantial amount of data about EU residents is made obvious when one considers Facebook.

Facebook has both a European headquarters and a subsidiary company established in Ireland.[7] Its main place of establishment, however, is in California.[8] Until recently, Facebook has declared that all of its user data is stored in the United States on servers owned or managed by Facebook.[9] That said, Facebook has recently launched a server farm in Sweden where user data may also be stored.[10]

The way that Facebook has organized its business raises a series of questions, which serve as the focus of this Article. Can Facebook be required to comply with EU law when operating on U.S. territory? If so, what rules must Facebook comply with in the context of programs like PRISM? Can Facebook be required to obey both U.S. and EU law at the same time? What happens when there is a conflict of laws?

---

7. *Facebook Response to European Commission Communication on Personal Data Protection in the European Union* 1 (May 22, 2011), http://ec.europa.eu/justice/news/ consulting_public/0006/contributions/not_registered/facebook_en.pdf.

8. *Key Facts*, FACEBOOK, https://newsroom.fb.com/Key-Facts (last visited Mar. 15, 2014) (explaining that Facebook's headquarters is located at 1601 Willow Road, Menlo Park, California, 94025).

9. *Facebook Response to European Commission, supra* note 7 ("Facebook user data is stored in the United States on servers owned or managed by Facebook.").

10. *Welcome to Sweden, Facebook! Social Network Launches First Massive Server Farm outside U.S. at the Edge of Arctic Circle*, DAILY MAIL (June 12, 2013), http://www.dailymail.co.uk/news/article-2340608/Welcome-Sweden-Facebook-Social-network-launches-massive-server-farm-outside-U-S-edge-Arctic-Circle.html.

III. PRISM

This section will explore PRISM from both a technical and a legal perspective. The goal is to better understand some of the concerns raised by programs such as PRISM from a European perspective in order to understand why PRISM represents an affront to basic European data protection principles. In short, PRISM will act as a lens to define, contrast, and question EU extraterritorial actions in the realm of data protection.

A. TECHNICAL

1. Collection: Building the Haystack

IBM estimates that humanity creates 2.5 quintillion bytes of data every day (1 followed by 18 zeroes), with ninety percent of the world's data created in the last two years alone.[11] This data comes from everywhere and includes transactional records, photos, videos, word-processing files, Skype chats, emails, and so on.[12] Wired Magazine has recently noted that humans write the equivalent of 520 million books every day on social media and email.[13] Because much of this data is in digital form, it cannot only be easily stored for long periods of time, but it can also be shared, compared, reorganized, combined and duplicated at very fast speeds and with relatively little cost.[14]

Underlying PRISM is the idea that there are great possibilities in the huge amounts of data that is being collected, particularly with respect to uncovering national security threats. Pappalardo explains:

> The concept behind the [National Security Agency's] data-mining operation is that this digital information can be analyzed to establish connections between people, and these links can generate investigative leads. But in order to examine data, it has to be collected—from

---

11. Joe Pappalardo, *NSA Data Mining: How It Works*, POPULAR MECHANICS (Sept. 11, 2013, 6:30 AM), http://www.popularmechanics.com/technology/military/news/nsa-data-mining-how-it-works-15910146; *see also* Marcia Conner, *Data on Big Data,* MARCIA CONNER (July 18, 2012), http://marciaconner.com/blog/data-on-big-data/.

12. Pappalardo, *supra* note 11.

13. Clive Thompson, *Why Even the Worst Bloggers Are Making Us Smarter,* WIRED (Sept. 17, 2013), http://www.wired.com/opinion/2013/09/how-successful-networks-nurture-good-ideas/.

14. Christopher Kuner, Fred H. Cate, Christopher Millard, & Dan Jerker B. Svantesson, Editorial, *The Challenge of "Big Data" for Data Protection*, 2 INT'L DATA PRIVACY L. 47, 47 (2012).

> everyone. As the data-mining saying goes: To find a needle in a haystack, you first need to build a haystack.[15]

The precise manner in which the PRISM "haystack" is built is not clear. Reports suggest that PRISM facilitates the U.S. National Security Agency's (NSA) access to data in the servers of nine information technology companies: Google, Microsoft, Facebook, Yahoo, Skype, Apple, Paltalk, Youtube, and AOL.[16] Initially, it was declared that these Internet companies provided back-door access to their networks, allowing the NSA to search their networks unilaterally.[17] More recent reports suggest, however, that the NSA has only been provided with limited access to the data such as through an intermediate portal.[18] Sottek and Kopstein explain:

> At its most innocuous, PRISM appears to be a database capable of interacting directly with the networks of participating Internet companies through a series of portals whose specific features and capacities are negotiated and developed with each participating company . . . It is possible, but not confirmed, that some of the portals in question also facilitate qualitatively different levels of data acquisition.[19]

The specific kinds of data that are collected through PRISM include emails, chats, videos, photos, cloud-stored files, VoIP calls, and more.[20] Much of this data is in unstructured forms—it does not reside in any fixed dimensions/fields.[21] It can be textual (e.g. generated in a Word document) or non-textual (e.g. generated in a video).[22] This form of data, which is exploding at a rapid pace and fueling the so-called "big data" surge, generally requires extensive processing to extract and structure the information contained in it.[23] It is also significant that

---

15. Pappalardo, *supra* note 11.

16. Didier Bigo, et al., *Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU*, JUST & HOME AFFS., CEPS POL'Y BRIEFS 3 (June 18, 2013), *available at* http://www.ceps.eu/book/open-season-data-fishing-web-challenges-us-prism-programme-eu.

17. Rodriguez & Israel, *supra* note 5 ("Initially suspected to provide *back-door* access to the networks of a number of Internet companies, giving the NSA direct access to search service providers networks unilaterally, more recent reports paint a picture of a more narrowly curtailed, but still potentially troubling interface.").

18. Sottek & Kopstein, *supra* note 3.

19. Rodriguez & Israel, *supra* note 5.

20. *See, e.g.*, Ashkan Soltani, *PRISM: Solving for X,* ASHKAN SOLTANI (June 14, 2013), http://ashkansoltani.org/2013/06/14/prism-solving-for-x/.

21. Bin Zhou, *Keyword Search on Large-Scale Structured, Semi-Structured, and Unstructured Data*, *in* HANDBOOK OF DATA INTENSIVE COMPUTING 733-51 (Borko Furht & Armando Escalante eds., 2011).

22. *Id.*

23. MEHMED KANTARDZIC, DATA MINING: CONCEPTS, MODELS, METHODS, AND ALGORITHMS 23 (2d ed. 2011); *see also* Tengjiao Wang, *Preface to the 2nd International Workshop on Unstructured Data Management (USDM 2011)*, 6612 WEB TECHS. &

this data is often embedded with metadata—data about data.[24] Biersdorfer explains:

> Metadata, a term created by the fusion of an ancient Greek prefix with a Latin word, has come to mean "information about information" when used in technology and database contexts. The Greek meta means behind, hidden or after, and refers to something in the background or not obviously visible, yet still present. Data, the Latin term, is factual information used for calculating, reasoning or measuring.[25]

Examples of metadata include the date and time of a phone call or the location from which an individual last accessed his email. While this data generally does not contain personal or content-specific details, it reveals transactional information about the user, the device, and activities taking place such as email logs, geolocation data (IP addresses), and web search histories.[26] When paired with dynamic data processing techniques, metadata is thought to be more valuable than the raw data itself because it reveals a tremendous amount about a person's life and habits.[27] Babeanu explains, "metadata is often used to manage digital assets but can itself be a digital asset."[28]

APPLICATIONS LECTURE NOTES COMPUTER SCI. 398, 398 (2011). "The management of unstructured data has been recognized as one of the most attracting problems in the information technology industry." *Id.* "Over eighty percent of world data today is unstructured with self-contained content items." *Id.* "Since most techniques and researches that have proved so successful performing on structured data do not work well when it comes to unstructured data, how to effectively handle and utilize unstructured data becomes a critical issue to these data-centric applications." *Id.*

24. Kuner, Cate, Millard, & Svantesson, *supra* note 14 (explaining that metadata is "data about when and where and how the underlying information was generated").

25. J.D. Biersdorfer, *Weeding out Windows Fonts*, N.Y. TIMES (Feb. 16, 2006), http://www.nytimes.com/2006/02/16/technology/circuits/16askk.html?pagewanted=print&_r=0.

26. Sottek & Kopstein, *supra* note 3.

27. Mathew J. Schwartz, *What Prism Knows: 8 Metadata Facts*, INFO. WK. (June 19, 2013, 11:53 AM), http://www.informationweek.com/security/risk-management/what-prism-knows-8-metadata-facts/d/d-id/1110429?. An excerpt from the article, *Government Surveillance: Little Peepers Everywhere*, explains how metadata can be used:

> Metadata (the records of who people call and e-mail, and when, as distinct from the content of conversations) can now be amassed on a vast scale, and run through powerful software that can use it to create a fairly complete portrait of a person's life and habits—often far more complete than just a few recorded conversations.

Government Surveillance: Little Peepers Everywhere, ECONOMIST (July 21, 2012), http://www.economist.com/node/21559331.

28. Delia Babeanu, Alexandru Adrian Gavrila, & Valerica Mares, *Strategic Outlines: Between Value and Digital Assets Management*, 11 ANNALES UNIVERSITATIS APULENSIS SERIES OECONOMICA 318, 319 (2009).

2. Analysis: Finding the Needle (Targeting and Tasking?)

There is no doubt that the NSA has access to a colossal digital haystack. Ostensibly, much of this data involves uninteresting, innocent communications and much of it concerns U.S. citizens, which, for reasons explained below, it must not examine. As such, in order for an NSA analyst to find the rare and interesting classes of data—"the needles"—he must build a "smaller haystack." According to the leaked internal NSA documents apparently used to train intelligence operatives on the capabilities of the program, the U.S. intelligence operatives are able to build this smaller haystack by sifting through the huge amounts of data that they have access to through the application of a process of targeting and tasking.[29]

With respect to "targeting," it appears that an NSA analyst must type one or more "selectors" in order to retrieve information. Gellman and Lindeman explain:

> Selectors may refer to people (by name, e-mail address, phone number or some other digital signature), organizations or subjects such as the sale of specialized parts for uranium enrichment. Along with the selectors, the analyst must fill out an electronic form that specifies the foreign-intelligence purpose of the search and the basis for the analyst's "reasonable belief" that the search will not return results for U.S. citizens, permanent residents or anyone else who is located in the United States.[30]

The actual search request, known as a "tasking," is then sent out, possibly to multiple sources.[31] For example, a tasking for Google is routed to equipment installed at the company.[32] A tasking may return an array of data ranging from e-mails, attachments, address books, and video chats to metadata identifying the locations of a target.[33]

After the tasking is completed and the requisite information is obtained from the Internet companies, the data is passed to the NSA, which analyzes it. The leaked slides indicate that "[a]fter communications information is acquired," the data is "processed and analyzed by specialized systems that handle voice, text, video, and 'digital network information' that includes the locations and unique device signatures of targets." While there are few details about the precise kinds of data

---

29. Ian Black, *NSA Spying Scandal: What We Have Learned*, GUARDIAN (June 10, 2013, 2:48 PM), http://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned.

30. Barton Gellman & Todd Lindeman, *Inner Workings of a Top-Secret Spy Program*, WASH. POST (June 29, 2013), http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/.

31. Sottek & Kopstein, *supra* note 3.

32. *Id.*

33. *Id.*

processing techniques used to understand the collected material, the leaked slides provide names and a brief description of a couple of the processing systems used by the NSA to explain or clarify the data it collects. For example, "PRINTURA" is described as a tool "which automates the traffic flow."[34]

Ultimately, the results are automatically provided to the analyst who made the original tasking. The Washington Post reports that "[t]he time elapsed from tasking to response is thought to range from minutes to hours."[35] Ostensibly, the human analyst will interpret the patterns revealed by the data analysis, such as connections between people, in such a way that will generate investigative leads.[36]

Testifying before the House Intelligence Committee, the Federal Bureau of Investigation (FBI) deputy director Sean Joyce explained that through PRISM, the NSA was able to stifle a plot to bomb the New York Stock Exchange (NYSE).[37] Joyce said that the NSA was monitoring "a known extremist in Yemen," and "this individual was in contact with an individual in the United States named Khalid Ouazzani."[38] According to Joyce, Quazzani, along with other unnamed individuals, was involved in "nascent plotting to bomb the NYSE."[39] Joyce explained, "Ouazzani had been providing information and support to this plot."[40] Fortunately, "the FBI disrupted and arrested these individuals."[41]

Based on this testimony, it appears that these kinds of processing techniques may likely involve some kind of content filtering and traffic analysis in order to uncover terrorist connections. Essentially, "content filtering is used to search for the occurrence of particular words or language combinations that may be indicative of particular communications (or persons) of interest such as 'nuclear weapon' or 'osama bin laden.'"[42] The actual search algorithms are, of course, much more complex and sophisticated.[43] Posner explains traffic analysis as "examining message length, frequency, and time of communication and other non-content information that may reveal suspicious patterns."[44]

---

34. *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

35. Gellman & Lindeman, *supra* note 30.

36. Pappalardo, *supra* note 11.

37. James O'Toole, *Gov't Claims Spying Programs Stopped Plot to Bomb New York Stock Exchange*, CNN MONEY (June 18, 2013), http://money.cnn.com/2013/06/18/news/economy/stock-exchange-plot/.

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

42. Kim A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH. 128, 151 (2007).

43. *Id.*

44. Richard A. Posner, *Privacy Surveillance, and Law*, 75 U. CHI. L. REV. 245, 253

Traffic analysis is attractive because it cannot be foiled by encryption, and together with social network theory, it can help identify organizations, groups, and the key people involved.[45]

B. LEGAL

1. American Perspective

(a) FISA, the Patriot Act, and the Targeting of Non-U.S. Citizens

In 1978, the U.S. Congress passed the Foreign Intelligence Surveillance Act (FISA).[46] The law was passed in response to, first, Justice Powell's "invitation" in the *Keith* case to regulate domestic security surveillance.[47] In addition, the law was a reaction to the Church Committee Report, which documented nearly fifty years of systematic executive abuses such as warrantless wiretapping of political opponents and opening mail of U.S. citizens.[48]

While FISA was a compromise designed to protect American citizens against the tyranny of unchecked government power, it also allowed the U.S. government to conduct surveillance for foreign intelligence purposes in order to safeguard the nation.[49] FISA provides a statutory framework for the government to engage in electronic surveillance in order to obtain "foreign intelligence information."[50] While the term "foreign intelligence information" is a term of art, it generally indicates information about international terrorism,

---

(2008).

45. Kim A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, 7 N.Y.U. REV. L. & SECURITY, SUPL. BULL. ON L. & SEC (2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=889120.

46. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*; *see generally* ELIZABETH B. BAZAN, CONG. RESEARCH SERV., RL30465, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND RECENT JUDICIAL DECISIONS (2005).

47. *See United States v. U.S. Dist. Court for E. Dist. of Mich.*, 407 U.S. 297, 322 (1972) ("Given [the] potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.").

48. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, S. REP. NO. 94-755, at 5 (1976).

49. Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists:" The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 486 (2006) ("FISA was a compromise forged in the fires of controversy created by Watergate, COINTELPRO, and the fifty-year litany of abuses meticulously documented in the Church Committee Report.").

50. *See* Stephanie Cooper Blum, *"Use It and Lose It:" An Exploration of Unused Counterterrorism Laws and Implications for Future Counterterrorism Policies*, 16 LEWIS & CLARK L. REV. 677, 702 (2012).

espionage, and sabotage.[51]

FISA establishes a special court (the "FISA Court") to review applications requesting electronic surveillance.[52] All cases brought before the FISA Court are heard *ex parte*, meaning that the government is the only party present at its proceedings.[53] Appeals from the FISA Court go to the Foreign Intelligence Surveillance Court of Review.[54]

For purposes of a discussion about PRISM, the general acquisition and interception power, included in Section 702, is the most important feature of FISA to understand. Section 702 (50 U.S.C. § 1881a) refers to part of the Foreign Intelligence Surveillance Act (FISA) Amendments of 2008. It provides that "the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to one 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."[55] It is explicit that the targeting can only be of foreign nationals outside of the United States. More specifically, Section 702 sets forth five key limitations:

> [The NSA] (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.[56]

---

51. 50 U.S.C. § 1801(e) (2006 & Supp. 2009). "Foreign Intelligence Information" is defined as:

> Information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against [an] actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism . . . by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to the national defense or the security of the United States; or the conduct of the foreign affairs of the United States.

Id.; *see generally* Blum, *supra* note 50.

52. 50 U.S.C. § 1803(a) (1994).

53. 50 U.S.C. §§ 1801-05 (2006).

54. *Id.*

55. 50 U.S.C. § 1881a(a) (2008).

56. *Id.* at § 1881a(b)(1-5).

In order to authorize the targeting, the Attorney General and Director of National Intelligence must obtain an order from the FISA Court or certify, "intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order."[57] When requesting an order, the Attorney General and Director of National Intelligence must certify to the FISA Court, among other things, that the targeting is limited to persons reasonably believed to be located outside the United States and that "a significant purpose of the acquisition is to obtain foreign intelligence information."[58]

At this point, it is important to mention that there is no requirement to specify which facilities, telephone lines, e-mail addresses, places, or property will be targeted.[59] Under Section 702, "the targeting might be directed at a terrorist organization, a set of telephone numbers or e-mail addresses, or perhaps at an entire [Internet Service Provider] or area code."[60] In fact, the statute is explicit that "a certification . . . is not required to identify the specific facilities, places, premises, or property at which an acquisition . . . will be directed or conducted."[61] It is also important to mention that there is no requirement that the government has any reasonable belief that the targets of surveillance have a connection to criminal or terrorist activities. This is how the U.S. intelligence community is lawfully able to issue broad orders to U.S. based Internet Service Providers (ISPs) and electronic communication service providers to turn over all communications that are reasonably believed to involve a non-American who is outside the country.[62]

After receiving a FISA Court order or determining that there are emergency circumstances, the Attorney General and Director of National Intelligence can direct a provider to "immediately provide the Government with all information, facilities, or assistance necessary to

---

57. *Id.* at § 1881c(2).

58. 50 U.S.C. § 1881g(2)(A)(5) (2006).

59. *Id.* at § 1881g(4) ("A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted."); *see also* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1646 (2010) ("Unlike traditional FISA applications, the government is not required to identify the facilities, telephone lines, e-mail addresses, places, or property where the programmatic surveillance will be directed.").

60. Banks, *supra* note 59.

61. § 1881g(4).

62. Ryan Singel, *Dems Agree to Expand Domestic Spying, Grant Telecoms Amnesty*, WIRED (June 19, 2008, 12:09 PM), http://www.wired.com/threatlevel/2008/06/dems-agree-to-e/ (indicating that under the proposal, "the intelligence community will be able to issue broad orders to U.S. ISPs, phone companies and online communications services like Hotmail and Skype to turn over all communications that are reasonably believed to involve a non-American who is outside the country").

accomplish the acquisition in a manner that will protect the secrecy of the acquisition."[63] If a provider complies with the mandate, then it is released from liability to its users for providing the information and is reimbursed for the cost of providing it.[64] If, however, a provider rejects the mandate or fails to comply with it in some way, "the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the [FISA Court], which shall have jurisdiction to review such petition."[65] Failure to obey an order issued by the FISA Court may be punished by the court as contempt of court.[66]

Rather than reject the mandate outright, the provider also has the option to "file a petition to modify or set aside such directive with the [FISA Court], which shall have jurisdiction to review such petition."[67] The provider can appeal the FISA Court's denial to the Foreign Intelligence Surveillance Court of Review. If the Court of Review rejects the appeal, the provider may then appeal the decision to the U.S. Supreme Court by a writ of certiorari for review under seal.[68]

2. European Perspective

(a) FISA is Targeted at Non-U.S. Citizens

Section 702 facilitates the acquisition of foreign intelligence information concerning non-U.S. citizens located outside the United States by permitting the U.S. government to collect information from electronic communication service providers under court supervision. As such, European residents who use U.S. based Internet services fall squarely within the ambit of this provision.[69] To the extent that there are limitations on the surveillance powers authorized under Section 702, these limitations are primarily designed to limit the exposure of U.S. persons. Director of National Intelligence, James Clapper, has stated that surveillance programs like PRISM, authorized under Section 702, involve "extensive procedures . . . to ensure that *only non-U.S. persons outside the U.S.* are targeted, and that minimize the acquisition, retention and

63. 50 U.S.C. § 1881 h(1)(A) (2008).

64. *Id.* at § 1881 h(3).

65. *Id.* at § 1881 h(5).

66. *Id.*

67. *Id.* at § 1881 h(6).

68. *Id.*

69. *See* Eva Galperin, *International Customers: It's Time to Call on US Internet Companies to Demand Accountability and Transparency*, ELECTRONIC FRONTIER FOUND (June 10, 2013), https://www.eff.org/deeplinks/2013/06/international-customers-its-time-call-us-internet-companies-demand-accountability.

dissemination of incidentally acquired information about U.S. persons."[70]

There are, however, a few safeguards set forth in Section 702 that limit the scope of programs like PRISM, even from the perspective of a foreigner. First, there is the obligation that the surveillance is employed only for foreign intelligence purposes. The PRISM Fact Sheet reads:

> The Government cannot target anyone under the court-approved procedures for Section 702 collection unless there is an appropriate, and documented, foreign intelligence purpose for the acquisition (such as for the prevention of terrorism, hostile cyber activities, or nuclear proliferation) and the foreign target is reasonably believed to be outside the United States. We cannot target even foreign persons overseas without a valid foreign intelligence purpose.[71]

Second, surveillance is subject to judicial review, albeit by a highly secretive court, the Foreign Intelligence Surveillance Court of Review. It is also subject to oversight by the Congress and the executive branch of the U.S. government.[72] Finally, if information about foreigners inside the United States is captured then "those details must be removed from all records and cannot be shared with any other entity in the government unless it is necessary to understand and interpret related foreign intelligence or to protect lives from criminal threats."[73]

(b) No Fourth Amendment Protections?

Europeans contend that they should be afforded greater protection from surveillance programs like PRISM under U.S. law. One central argument is that if the EU affords privacy and data protection rights and remedies to any third-country national, then the U.S. should also

---

70. Patrick Goodenough, *Clapper Insists Internet Data Mining Deliberately Targets Only "Non-US Persons,"* CNS NEWS (June 7, 2013), http://cnsnews.com/news/article/clapper-insists-internet-data-mining-deliberately-targets-only-non-us-persons.

71. Press Release, Office of the Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (June 8, 2013), http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf.

72. 50 U.S.C. § 1881 *et seq.* (2008). The Director of National Intelligence's Press Release, dated June 8, 2013, states:

> The law specifically requires a variety of reports about Section 702 to the Congress . . . In addition, the Congressional Intelligence and Judiciary Committees are regularly briefed on the operation of Section 702 . . . The Executive Branch, including through its independent Inspectors General, carries out extensive oversight of the use of Section 702 authority.

Press Release, *supra* note 71.

73. *See* Kurt Eichenwald, *PRISM Isn't Data Mining and Other Falsehoods in the N.S.A. "Scandal,"* VANITY FAIR (June 14, 2013), http://www.vanityfair.com/online/eichenwald/2013/06/prism-isnt-data-mining-NSAscandal; *see also* 50 U.S.C. § 1801(h) (2008) (defining "minimization procedures" for the Foreign Intelligence Surveillance Act).

protect "non-American citizens or residents" as data subjects.[74] The idea is that since the EU treats privacy and data protection as fundamental human rights afforded to all individuals then the U.S. should also do so. This normative argument, however, represents a misconception about U.S. constitutional law.

The Fourth Amendment of the U.S. Constitution treats communications privacy as between an individual and the government as a fundamental right.[75] *United States v. Verdugo-Urquidez* is a landmark case with respect to understanding the relationship between the Fourth Amendment and non-U.S. citizens. Here, the Supreme Court held that non-U.S. citizens living outside of the U.S. and searched by the American government are not entitled to the protections of the U.S. Constitution.[76] The Supreme Court reasoned that aliens should enjoy certain constitutional protections only when they have come "within the territory of the United States and developed substantial connections with the country" such that they have become a part of the national community that makes up "the People of the United States" as stated in the Constitution.[77] In other words, the Court seems to have adopted a social compact theory of the right, which can be juxtaposed to the natural rights theory applied in the EU.

Because EU residents generally have no connection with or physical presence in the U.S., they have no protection under the Fourth Amendment. One commentator sums up the EU perspective as, "if you are a U.S. citizen, you have the Fourth Amendment. But if you're not, you have no protection."[78] However, there is an alternative perspective that, ". . . even U.S. citizens do not enjoy the full protection of the Constitution outside the U.S. minus one exception in the foreign intelligence area, where the U.S. government does not need a court order to conduct electronic surveillance outside the U.S. even when targeting U.S. citizens."[79]

---

74. Bigo, et al., *supra* note 16, at 8.

75. *See* Leslie Harris, *Government Surveillance Viewed though a Global PRISM*, CENTER FOR DEMOCRACY & TECHNOLOGY (July 18, 2013), https://www.cdt.org/blogs/leslie-harris/1807government-surveillance-viewed-though-global-prism.

76. United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990); *see also* Martinez-Aguero v. Gonzalez, 459 F.3d 618, 622 (5th Cir. 2006).

77. *Martinez-Aguero*, 459 F.3d at 622 (citing *Verdugo-Urquidez*, 494 U.S. at 266-67).

78. Carol Matlack, *U.K. Foreign Secretary Hague commenting on Prism in London Privacy Europeans Ask if Prism Has Been Spying on Them, Too*, BUSINESSWEEK (June 11, 2013), http://www.businessweek.com/articles/2013-06-11/europeans-ask-if-prism-has-been-spying-on-them-too.

79. Harris, *supra* note 75.

(c) Privacy and Data Protection Concerns

Broadly, PRISM raises privacy and data protection concerns pertaining to the procedures for examining, using, and storing data from the surveillance. Concerns also include questions about the retention and the deletion of the data, the inclusion of security measures, as well as transparency mechanisms and rights to access of stored data.[80] Although this Article is not an in-depth analysis of the privacy and data protection concerns raised by PRISM, it will discuss them, albeit briefly, to better understand why Europeans feel that PRISM represents an affront to their data protection and privacy principles.

First, the lack of transparency associated with the kind of data mining that takes place in the context of PRISM creates the potential for abuse or misuse by government bureaucrats.[81] Zarsky explains how the relevant officials might be improperly balancing rights and interests as a result of being led by their own bigotry, or being over-influenced by private interests.[82] Section 702 affords the U.S. government a breadth of powers that are interpreted secretly and insulated from any adversarial challenge.[83] Second, there is a concern that a slippery slope may result when powerful data mining tools are used for increasingly pettier needs until finally society is smothered under a veil of constant surveillance.[84] Here, the ultimate fear is the creation of an oppressive, "big brother" government that regulates all aspects of individual existence, including the regulation of individual and private thoughts. Furthermore, if the government becomes aware of everything about an individual, then it will be much easier for the government to attain that individual's obedience.

Third, there is the chilling effect that information access and data sharing by the U.S. government might have on innocent behavior.[85] Here, the primary concern is that individuals will act differently if they know that the government might observe their conduct. Ultimately, individual autonomy will be compromised. For example, an individual's ability to express himself/herself, protest ideas that he/she finds repugnant, or associate with whom he/she chooses may be affected by encouraging "conformity with a perceived norm, discouraging political dissent, or otherwise altering participation in political life."[86]

---

80. Rolf H. Weber, *Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives*, 3 INT'L DATA PRIVACY L. 117-30 (2013).

81. Taipale, *supra* note 42.

82. Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1533 (2013).

83. Rodriguez & Israel, *supra* note 5.

84. Taipale, *supra* note 42.

85. *Id.*

86. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 35 (2004).

Finally, Solove discusses how large-scale government surveillance programs can create a loss of control over personal data with real world consequences.[87] The classic example here is the individual who finds his/her name stuck on a no-fly list and does not understand why this has happened.[88] He/she finds himself/herself frustrated and powerless because of this bureaucratic decision that has been made based on his/her personal data but he/she has not been a part of the decision-making process.[89]

IV. PRISM AND THE EU DATA PROTECTION DIRECTIVE

This section will examine whether the EU Data Protection Directive and the proposed Regulation can be applied to safeguard European personal data from the perceived threats posed by programs like PRISM. In other words, the goal is to see whether the EU can bind companies that provide services to European residents to its data protection principles, such as transparency and information requirements, when they operate on U.S. sovereign territory. The focus is placed on an examination of the rules regarding transfers of personal data from the EU to third countries, which have been designed to protect the high level of data protection that is afforded by the Directive from being undermined when data flows beyond the territorial borders of the Union.

First, the EU-U.S. Safe Harbor Agreement, a voluntary program designed to facilitate transfers of data between the EU and the U.S., will be examined. Then, assuming the EU Data Protection Directive applies to the type of large technology firms involved in PRISM, Chapter IV of the current Directive, "Transfers of Personal Data to Third Countries," will be analyzed. Finally, the so-called "Anti-FISA Amendments" (generally forbidding any company bound by the forthcoming Regulation from handing the personal data of EU citizens over to non-EU governments unless the disclosure is done in accordance with EU law),which have been proposed to be included in the forthcoming Regulation, will be explored.

---

87. DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 188-98 (2011).

88. *See generally id.*

89. *Id.; see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1194 (2002) (stating, "the current collection and use of personal information are used to make decisions affecting an individual's life, yet individuals often have no way to participate and no notice about what is happening").

A. ADEQUACY AND THE SAFE HARBOR PROGRAM

Currently, when the EU Data Protection Directive applies, a controller may only transfer data outside the EU pursuant to the rules set forth in Articles Twenty-Five and Twenty-Six of the Directive.[90] That is, either the recipient of the data offers an adequate level of protection, or it falls under one of the exceptions to the rule such as the use of model contractual clauses or binding corporate rules.[91] The purpose of the adequacy requirement is simple in that "if controllers in a Member State transferred data to a third country that failed to protect personal data, then the Member State's protection of personal data would be effectively lost once the Member State transferred the data to the third country."[92] Specifically, Article Twenty-Five, Section One states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.[93]

In determining whether the recipient is adequate, a data controller can rely on a Union finding of adequacy made by the European Commission.[94] To date, the European Commission has only made adequacy findings with regard to eleven countries.[95] Despite the fact that the U.S. has not been deemed to afford an adequate level of data protection, transfers of data to the U.S. are still possible through an agreement reached between the U.S. Department of Commerce and the European Commission referred to as the U.S.-EU Safe Harbor Program.[96]

---

90. Council Directive 95/46/EC, On the Protection of Individuals with Re-gard to the Processing of Personal Data and on the Free Movement of Such Data, art. 25, 1995 O.J. (L 281).

91. *Id.* at art. 25-26.

92. Patrick J. Murray, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INT'L L.J. 932, 964-65 (1998).

93. *See* Council Directive 95/46/EC, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

94. *Id.*

95. *See Adequacy Findings*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/ data-protection/document/international-transfers/adequacy/ index_en.htm (last visited Feb. 9, 2014) (providing an up-to-date list of commission decisions on the adequacy of the protection of personal data in countries). To date the European Commission has only made adequacy findings with regard to eleven non-EEA countries: Switzerland, Canada, Argentina, Guernsey, the Isle of Man, Andorra, Jersey, Israel, the Faroe Islands, New Zealand and Uruguay. *Id.*

96. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_ main_018476.asp (last updated Dec. 18, 2013).

The U.S. Commerce Department administers the U.S.-EU Safe Harbor Program and permits companies to accept personal data transferred from the EU without any conflicts arising under the Data Protection Directive.[97] Under the Safe Harbor Program, U.S. companies can either self-certify their agreement to abide by the Safe Harbor framework, which includes seven privacy principles similar to those found in the Data Protection Directive (e.g. notice, choice, access, and enforcement), through the safe harbor website, or send a letter to the U.S. Department of Commerce announcing their intention to comply with the safe harbor principles.[98] After certification, an organization participating in the program is not required to obtain prior approval of data transfers as the approval will either be waived or automatically granted.[99]

Importantly, the Safe Harbor Program permits signatories to the agreement to deviate from its principles "to the extent necessary to meet national security . . . requirements."[100] Here, the questions become: (i) whose national security requirements permit deviation from the Agreement (i.e. the U.S., the EU, or both); and (ii) whether the national security requirements demanded of technology companies pursuant to, *inter alia*, Section 702 fall within the ambit of this exception. Indeed, the Article Twenty-Nine Working Party, an independent European working party that deals with issues relating to the protection of privacy and personal data, has "doubts whether the seemingly large-scale and structural surveillance of personal data that has now emerged (in light of PRISM) can still be considered an exception strictly limited to the extent necessary."[101]

If there is an alleged breach of the principles set forth in the Safe Harbor Agreement, then there are several different courses of action. First, the U.S. Federal Trade Commission can bring an enforcement action against the entity that has allegedly failed to comply with the agreement.[102] Second, an affected individual can bring a direct action in

---

97. *Id.*

98. Caspar Bowden & Judith Rauhofer, *Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud* (Edinburgh Sch. of L., Research Paper No. 2013/28, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2283175.

99. *See U.S.-EU Safe Harbor Overview*, *supra* note 96.

100. *Safe Harbor Privacy Principles*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 30, 2009) ("Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements.").

101. *PRISM and Data Protection for EU Citizens*, THE SOCIETY FOR COMPUTERS AND LAW (Aug. 16, 2013), http://www.scl.org/site.aspx?i=ne32989.

102. *See Safe Harbor Enforcement Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018481.asp (last updated Jan. 30, 2009).

U.S. courts pursuant to U.S. law.[103] Finally, it is possible for an EU Member State, who believes that the principles of the Safe Harbor Agreement are in breach, to suspend data flows to the U.S. This rule is set forth in Article Three, Section 1(b) of the Commission Decision on the Safe Harbor principles that ". . . gives to the competent authorities in Member States the possibility to suspend data flows in cases where there is a substantial likelihood that the Principles are being violated and where the continuing transfer would create an imminent risk of grave harm to data subjects."[104]

A major problem with an EU response to PRISM based on the U.S. Safe Harbor Program is that the types of entities that are involved with PRISM are those that are already, or will soon become, subject to EU data protection law. This opinion is based on the broad interpretation of Article Four of the Data Protection Directive that has been set forth by the Article Twenty-Nine Working Party,[105] the recent opinion by the Advocate General in the *Google Spain* case,[106] and Article 3 of the forthcoming Regulation which extends the scope of EU data protection law to controllers, established anywhere in the world, who process personal data of EU residents in order to offer them goods or services or to monitor their behavior.[107] While an in-depth discussion of the applicable law provisions set forth in the Directive and Proposed Regulation is outside the purview of this Article, the point is to understand that the types of transnational entities involved in PRISM are those that almost certainly must comply with the EU Data Protection Directive based on their, albeit tenuous, connections to the EU, such as the fact that they have establishments in the EU or use equipment in the EU.

---

103. Bowden & Rauhofer, *supra* note 98.

104. *PRISM and Data Protection for EU Citizens*, *supra* note 101.

105. Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, (Dec. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

106. *Advocate General's Opinion*, Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, 2013 E.C.R, *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077en.pdf. The Opinion of the Advocate General Niilo Jääskinen concluded that the personal data processed at Google Spain SL was in the "context of the activities" of that establishment because it bridges two (interrelated) limbs of the business. *Id.* This is a rather broad interpretation of Article 4 because Google Spain was only processing data for marketing purposes and did not have any role in or control over the particular data processing at issue in the case, namely data processing associated with the search engine operations. *See* Case C-131/12, Google Spain SL Google, Inc. v. Agencia Española de Protección de Datos, 2013 E.C.R.

107. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, EUROPEAN COMMISSION (Jan. 25, 2012), *available at* http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65776/20130508ATT65776EN.pdf.

The Article 29 Working Party's comments in its Opinion about the level of protection provided by the Safe Harbor Program clearly show that the Safe Harbor Agreement is not the equivalent of a get-out-of-jail-free card. The comments make clear that the Program does not affect the application of Article 4 of the Directive by explaining that the principles of the Safe Harbor Program are not intended to substitute the national provisions implementing the Directive in situations where those national provisions apply.[108] Because U.S. companies cannot self-certify to the Safe Harbor Agreement and have avoided all liability under the Directive, why not hold them accountable under the Directive rather than the Safe Harbor Agreement, particularly when recourse under the Program is implemented by the Federal Trade Commission or U.S. courts applying U.S. law?

B. ADEQUACY, DATA TRANSFERS, AND THE "IMPORTANT GROUND OF PUBLIC INTEREST EXCEPTION"

As noted above, controllers subject to EU law may only transfer EU personal data, when either the recipient of the data offers an adequate level of protection, or the data falls under one of the exceptions to the rule, regardless of where in the world the controller is processing EU data. By assessing the standards utilized in the receiving state or authority, the adequacy requirement seeks to ensure that the data protection values enshrined within EU legal texts are not rendered meaningless after the data is transferred abroad.[109] In other words, the adequacy requirement is designed to ensure that there are no lacunae or loopholes found in the high level of protection of personal data provided by the Directive.[110]

At this point, it is important to elaborate upon the concept of a data "transfer," which is undefined in the Directive, and the kinds of data transfers that are involved in the context of programs like PRISM. First, there is the transfer of EU personal data to the United States. On one hand, it seems, in many situations, that users upload their data

---

108. *Opinion 4/2000 on the Level of Protection Provided by the "Safe Harbor Principles,"* DATA PROTECTION WORKING PARTY (May 16 2000), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf; *see also* Aleksandra Kuczerawy, *Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS*, *in* PRIVACY AND IDENTITY MANAGEMENT FOR LIFE IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 75, 79 (vol. 320 2010) ("This means that the Principles of Safe Harbor were not intended to substitute the national provisions implementing the Directive in situations where those national provisions apply.").

109. Els De Busser & Gert Vermeulen, *Towards a Coherent EU Policy on Outgoing Data Transfers for Use in Criminal Matters? The Adequacy Requirement and the Framework Decision on Data Protection in Criminal Matters. A Transatlantic Exercise in Adequacy. EU and International Crime Control*, (GOFS Research Paper Series, 2010).

110. Article 29 Data Protection Working Party, *supra* note 105.

directly to U.S. webpages without any intermediary in Europe. The access of the website by an EU resident that results in a company processing the data in the U.S. should arguably not be considered a transfer. If a data transfer were found to exist in this instance, then the restrictions of Article 25 would apply at any time that information is loaded onto and made accessible via the Internet. This application would make EU law applicable to the entire Internet.[111] On the other hand, it is also possible that an EU subsidiary sends personal data about EU residents to a U.S. parent company. This would more obviously be considered an "export" of personal data because there is an active transmission of data from the EU to the U.S.[112] The problem is, of course, that reliable information about the precise way that technology firms like Facebook collect personal data about EU residents and the role that EU establishments have in processing this data is very difficult to obtain.[113]

In any event, there is a clear transfer of EU personal data from U.S. servers owned by technology firms like Facebook to the U.S. government. If the technology firm is obligated to comply with the Directive under Article 4, then arguably, the firm can only transfer the data to the U.S. government if it can ensure an adequate level of protection. In light of the discussion at the outset of this Article, it is doubtful that the U.S. government offers an adequate level of data protection in the context of PRISM.

In response to EU claims that they are in breach of data transfer rules when they transfer data to the U.S. government, however, a technology company such as Facebook could claim that it is permitted to transfer data pursuant to the "important ground of public interest exception." Specifically, Article 26(1)(d) states:

> By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that . . . the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence (sic) of legal claims.[114]

---

111. *See* C-101/01, Criminal Proceedings against Bodil Lindqvist, 2003 (ECJ), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62001J0101:EN:HTML.

112. Cécile de Terwangne & Sophie Louveaux, *Data Protection and Online Networks*, 13 COMP. L. & SECURITY REV. 234, 234 (1997).

113. Kuczerawy, *supra* note 108.

114. Council Directive 95/46/EC, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 26(1)(d), 1995 O.J. (L 281).

This could include, for instance, "data transfer between competition authorities, tax and customs administrations, or it could be for the prevention and investigation, detection and prosecution of criminal offences."[115] In the context of PRISM, the companies could assert that they are required to meet national security requirements. However, this explanation might not be accepted because, just as with deviations from the Safe Harbor Agreement, it is not EU national security requirements but rather U.S. national security requirements that are at issue. Furthermore, the seemingly large-scale and structural surveillance of personal data that has emerged in light of PRISM may not be considered a narrowly tailored exception.

At any rate, Article 26(1)(d) seems to provide fairly good support for U.S. companies' actions. This fact has not gone unnoticed by EU politicians. Consequently, several Amendments—the so called "Anti-FISA Amendments"—have been proposed to close this perceived legal loophole.

C. THE ANTI-FISA AMENDMENTS

Several amendments to the Regulation have been proposed to address access requests by public authorities in third countries to personal data about EU residents.[116] Generally, these so-called "Anti-FISA Amendments" only permit the disclosure of EU personal data in response to a legal obligation or public interest duty that specifically emanates from EU law.[117] Such clauses would prohibit any entity subject to the EU Data Protection Directive from disclosing the personal data of EU citizens to non-EU public bodies unless it is in accordance with the Mutual Legal Assistance Treaties (MLATs), an international agreement between the requesting country and the EU or an EU member state. Additionally, such disclosure would only be permitted after an EU Data Protection Authority (DPA) verifies that the transfer complies with the

---

115. *Debates*, EUROPEAN PARLIAMENT, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+CRE+20120215+ITEM-019+DOC+XML+V0//EN (last updated Feb. 15, 2012).

116. *European Parliamentarians Seek Reinsertion of Onerous "Anti-FISA" Article 42 into Proposed EU Data Protection Legislation*, SIDLEY AUSTIN LLP (July 2, 2013), http://www.sidley.com/files/News/103dad94-9337-434e-8d7c-4eaf0d21ae42/Presentation/NewsAttachment/62be53ed-a865-4b19-97a64f25e3485e91/7.2.2013%20Privacy%20Update.Pdf; *see also* Jan Philipp Albrecht, *New Article 43(a) on Transfers Not Authorized by Union Law* (Comm. on Civil Liberties, Justice & Home Affairs 2012), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

117. Eduardo Ustaran, *How PRISM will affect the EU Data Protection Regulation*, FIELD FISHER WATERHOUSE PRIVACY & INFO. LAW BLOG (June 10, 2013), http://privacylawblog.ffw.com/2013/how-prism-will-affect-the-eu-data-protectionregulation.

Regulation.[118] Notice to data subjects about the transfer would also be required.[119]

The Working Party supports such provisions and has explained that the Regulation must include a provision mandating the obligatory use of MLATs in case of disclosures not authorized by Union or Member States law.[120] The Working Party contends that without such a provision, the "important grounds of public interests" exception set forth in Article 44(1)(d), and based on the existing provision set forth in Article 26 of the Directive, will allow for wide transfers of personal data for a large and unlimited category of "important grounds of public interests."[121] The Working Party further underlines "that in cases where a MLAT is in place, the competent authority under the MLAT (or comparable international agreement) shall be the authority dealing with the request and should, where necessary, consult the DPA."[122] European academics have also commented:

> The general data protection Regulation should include a provision stipulating the legal requirements applicable where a judgment of a court or tribunal (or any decision by an administrative authority) from a third country requires a data controller/processor to transfer personal data of EU citizens and residents. These should be only recognised [*sic*] and enforceable if there exist a mutual assistance treaty or international agreement in force between the requesting country and the EU, and after the verification by relevant EU data protection authorities.[123]

These Amendments raise many legal issues. First, under the provision of Article 2 of the proposed EU General Data Protection Regulation that states, "[the] Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security,"[124] it appears that the EU is acting outside the scope of its authority.

---

118. *See European Parliamentarians Seek Reinsertion of Onerous "Anti-FISA" Article 42*, *supra* note 116; Albrecht, *supra* note 116.

119. *See European Parliamentarians Seek Reinsertion of Onerous "Anti-FISA" Article 42*, *supra* note 116; Albrecht, *supra* note 116.

120. *See European Parliamentarians Seek Reinsertion of Onerous "Anti-FISA" Article 42*, *supra* note 116; Albrecht, *supra* note 116.

121. *Opinion 01/2012 on the Data Protection Reform Proposals 2012 Article 29,* DATA PROTECTION WORKING PARTY (Mar. 23, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191 _en. pdf.

122. *Id.*

123. *Amendment 259, Article 43a*, EUROPEAN PARLIAMENT, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+COMPARL+PE-501.927+04+DOC+PDF+V0//EN&language=EN (last visited Feb. 9, 2014); *see also* Bigo, et al., *supra* note 16.

124. *The Proposal for a Regulation of the European Parliament*, *supra* note 107.

Second, any requirement to notify a EU DPA would contradict the requirements of secrecy as set forth in FISA , placing companies between a rock and a hard place because, under U.S. law, it is a serious offense, possibly even treason, to reveal any details of the data transfers from the technology companies to the U.S. government.[125] Third, the language of some of these provisions is sweeping: any "judgment of a court or tribunal [or] decision of an administrative authority of a third country requiring a controller or processor to disclose personal data," could include not only FISA court orders, but "also routine discovery orders, warrants, subpoenas, administrative orders, SEC and other oversight requests, or other ordinary forms of legal requests for information that are quotidian to global businesses."[126]

Furthermore, such an expansionist approach to data protection arguably runs contrary to the notion of state sovereignty. There is a clear impingement upon U.S. state sovereignty as States are generally free to prescribe the forms of surveillance and investigation they wish in relation to people, places, and things on its sovereign territory.[127] By trying to impose its norms upon the United States in such a dramatic fashion, the EU is effectively dressing up data protection law as imperialism in disguise.[128]

It is also worth mentioning that even if the EU enacts these provisions, there is very little guarantee that they can be enforced. As the saying goes: the English Parliament is free to outlaw smoking on the streets of Paris, but there are practical limits to such an action.[129] While these controllers may have assets or establishments in the EU, which would help to force some compliance with the law, it is unlikely the EU will know about the requests because the ISPs are required to remain silent about them. Tene states, "(u)nenforceable legislation brings the law into disrepute."[130] Likewise, Bygrave warned in 1990 about

---

125. 50 U.S.C. § 1881 h(5)(D) (2008) ("Failure to obey an order . . . may be punished by the Court as contempt of court."); *see* 18 U.S.C. § 2381 (defining "treason"); *see also* Sophie Curtis, *Yahoo CEO: Revealing NSA Secrets Would Be "Treason*," THE TELEGRAPH (Sept. 12, 2013), http://www.telegraph.co.uk/technology/news/10304597/Yahoo-CEO-revealing-NSA-secrets-would-be-treason.html.

126. *European Parliamentarians Seek Reinsertion of Onerous "Anti-FISA" Article 42*, *supra* note 116.

127. Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SECURITY L. & POL'Y, 179, 198 (2011).

128. Note, *Constructing the State Extraterritorially, Jurisdictional Discourse, the National Interest, and Transnational Norms*, 103 HARV. L. REV. 1273, 1301 (1990).

129. PETER W. HOGG, CONSTITUTIONAL LAW OF CANADA 301 (student ed. 2003); *see also* IVOR JENNINGS, THE LAW AND THE CONSTITUTION 170-71 (5th ed. 1959); *see also* B.C. Elec. Ry. v. The King, A.C. 527, 541-42 (1946).

130. Omer Tene & Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, FUTURE OF PRIVACY (Jan. 22, 2013), http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf.

"a situation in which rules are expressed so generally and non-discriminatingly that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced."[131]

Finally, the Anti-FISA Amendments could undermine the emerging concept of interoperability.[132] This concept "recognizes that although global privacy frameworks will continue to diverge due to cultural and historical reasons, transborder data flows can be maintained and individual rights protected."[133] If the EU enacts legislation like the Anti-FISA Amendments then transnational companies will be faced with a direct conflict in privacy laws at a time when interoperability is key.

V. CONCLUSION

With so much personal data about EU residents held on U.S. servers, PRISM creates a difficult problem from the perspective of Europeans who are deeply concerned about the way that the U.S. government is able to collect and process this information. This is especially true because of the perceived lack of privacy and data protection standards exhibited on behalf of the U.S. government and the fact that EU residents are afforded just a few of the same safeguards that Americans are afforded. Binding companies that provide Internet services to EU residents to EU data protection principles is one means to meet the challenge represented by PRISM.

However, the problem with an aggressive response to PRISM based on the imposition of stronger EU Data Protection rules is three-fold. First, it is unlikely that the EU will be able to enforce its claims, which could undermine the law and bring the law to disdain. Second, it is not clear whether international law allows for broad extraterritorial claims on behalf of the EU because such claims conflict with the United States' sovereign right to collect data about Europeans through electronic surveillance techniques applied within its borders. Third, it is likely that the result of the EU's claims, especially if the Anti-FISA Amendments are adopted, will be to cause transnational entities to choose between conflicting regulatory frameworks. This is regretful at a time where promoting interoperability in the realm of data protection is critical.

---

131. *Id.*; *see also* Lee Bygrave, *Determining Applicable Law pursuant to European Data Protection Legislation*, 16 COMPUTER LAW & SEC. REPORT 252 (2000).

132. Tene & Wolf, *supra* note 130.

133. *Id.*; *see also Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; *see also* Paula Bruening, *Interoperability: Analysing the Current Trends and Developments*, 100 DATA PROTECTION L. & POL'Y 12 (May 2012).