American University Business Law Review

Volume 3 | Issue 2 Article 5

2013

The NSA'S Prism Program And The New EU Privacy Regulation: Why U.S. Companies With A Presence In The EU Could Be In Trouble

Juhi Tariq
American University Washington College of Law

NOTE

THE NSA'S PRISM PROGRAM AND THE NEW EU PRIVACY REGULATION: WHY U.S. COMPANIES WITH A PRESENCE IN THE EU COULD BE IN TROUBLE

JUHI TARIQ*

Recent revelations about a clandestine data surveillance program operated by the NSA, Planning Tool for Resource Integration, Synchronization, and Management ("PRISM"), and a stringent proposed European Union ("EU") data protection regulation, will place U.S. companies with a business presence in EU member states in a problematic juxtaposition. The EU Proposed General Data Protection Regulation stipulates that a company can be fined up to two percent of its global revenue for misuse of users' data and requires the consent of data subjects prior to access. U.S. company participation in the PRISM program, which conducts clandestine data-mining on a widespread scale, would directly violate several stipulations of the Proposed Regulation. U.S. companies with a business presence in the EU, caught in this juxtaposition, can push for governmental transparency to attenuate the economic repercussions, either through lobbying efforts or support for a security arrangement or treaty between the U.S. and EU.

"Consequently, since we are dealing with a situation in which the one who must tell the truth, whose function is to tell the truth, the one whom one consults to tell the truth, is the one who cannot tell the truth, since

---

* I want to give many thanks to the members of the American University Business Law Review for all of their hard work editing my piece, especially to my Note and Comment Editor Heba Tellawi for all of her time and effort during the writing process. I would also like to express heartfelt gratitude to my supportive parents who have earnestly provided encouragement throughout every step of this process. Finally, I would like to thank the legal department at Towers Watson for their support, particularly Paul Meyer for his invaluable expertise without which this note would not be possible.

the truth would be a confession concerning himself, how will the truth make its way, how will truth-telling be established and at the same time establish the possibility of a political structure within which one will be able to tell the truth in parrēsia? Well, it has to be through men."[1]

Introduction 372
I. The Proposed Regulation 373
II. The PRISM Problem 374
A. Key Aspects of the Proposed Regulation that are Incompatible with U.S. Government Surveillance 375
III. U.S. Companies Will Undermine the EU Proposed Regulation Through Compliance with the PRISM program 376
A. The EU Response to the Revelation of the PRISM Program 376
B. PRISM's Negative Economic Repercussions So Far and Further Predictions 377
C. Recent Cases Demonstrate a Desire in EU Member States to Enforce Data Protection Standards against U.S. Companies 380
IV. What can companies do to alleviate liability? 382
A. U.S. Companies Should Lobby for Favorable Data Protection Legislation in Both the U.S. and EU to Decrease Their Potential Liability and Increased Compliance Loads Under the Proposed Regulation 383
B. Companies Should Support an Agreement Modeled After the Passenger Names Record Agreement 386
Conclusion 388

INTRODUCTION

On June 6, 2013, Edward Snowden, a former U.S. government contractor, publicly divulged a clandestine electronic surveillance program operated by the United States' National Security Agency ("NSA") called the "Planning Tool for Resource Integration, Synchronization, and Management" ("PRISM").[2] The documents detailed the program and identified several technology companies, such as Facebook, YouTube, Google, and Microsoft that participate in PRISM and allow the government

1. MICHEL FOUCAULT, THE GOVERNMENT OF SELF AND OTHERS: LECTURES AT THE COLLÈGE DE FRANCE, 1982–1983 89 (Arnold I. I. Davidson ed., Graham Burchell trans., 2011).

2. *See* Timothy B. Lee, *Here's Everything We Know about PRISM to Date*, WASH. POST (June 12, 2013, 3:43 PM), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ (demonstrating the lack of information the public has had of the intricacies of PRISM).

to gain access to user information.[3] U.S.-based companies operating in the European Union ("EU"), caught in the balance between security and privacy, could be liable for violating the stringent EU Proposed General Data Protection Regulation ("Proposed Regulation") if they continue to comply with the U.S. government's PRISM program.[4] A solution lies in the form of either political pressure by U.S. companies for U.S. government transparency, an adequate security arrangement, or a U.S.–EU treaty that would protect U.S. companies operating in the EU.

I. THE PROPOSED REGULATION

The EU Proposed Regulation, widely regarded as one of the most complex regulations considered by the EU, aims to both harmonize practices across a diverse region and to modernize the existing 1995 Data Protection Directive.[5] The Proposed Regulation marks an important policy shift from directives to regulations[6] because the latter establishes enforceable standards, becomes part of a national legal system, overrides contrary national laws, and has legal effect independent of national law.[7] The key changes include a "right to be forgotten,"[8] a consent requirement,[9] a single set of EU data protection rules across the EU,[10] a single national data protection authority ("DPA"),[11] jurisdictional reach outside of EU-established companies,[12] and overall increased responsibility and

3. *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

4. Because the data is transmitted electronically from a company's servers to the U.S. government without judicial scrutiny of FISA information requests, and the U.S. government does not need "probable cause" to request information on a non-U.S. citizen, companies would be violating key provisions of the EU Proposed Regulation that stipulate certain requirements for the processing of personal data.

5. *See generally* Craig Timberg, *U.S. Firms, Officials Resisting Europe's Push for Stronger Digital Privacy Rules*, WASH. POST (Jan. 24, 2013), http://articles.washingtonpost.com/2013-01-24/business/36525323_1_privacy-advocates-data-protection-commissions-data-bill.

6. Directives must be enacted by EU member states to become enforceable, whereas regulations issued by the European Commission do not require individual member state enactment and have immediate force of law within the EU.

7. *See* Paul M. Schwartz, Note, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures* 126 HARV. L. REV. 1966, 1992–93 (2013) (arguing modifications to the Proposed Regulation that would ease EU-U.S. collaboration on data protection matters).

8. *See id.* at 1994.

9. *See id.*

10. *See id.* at 1997–98.

11. *See id.* at 1999–2001.

12. *See id.*

accountability for companies processing personal data.[13] Articles 16 and 216 of the Treaty on the Functioning of the European Union permit the EU to implement rules that regulate the processing of personal data by EU institutions, bodies, offices, agencies, and member states when "the activities fall within the scope of EU law."[14] On March 2013, the European Commission's Legal Affairs Committee formally approved main aspects of the Proposed Regulation, demonstrating the strong likelihood that it will be adopted.[15]

II. THE PRISM PROBLEM

Governed by Section 702 of the U.S. Foreign Intelligence Surveillance Act ("FISA"),[16] the PRISM Program facilitates data collection directly from the servers of large technology companies such as Microsoft, Yahoo, Google, and Facebook.[17] A 41-slide PowerPoint presentation used to train intelligence operatives was leaked to several news sources and confirms the possibility that communications made entirely within the U.S. could be collected without warrants.[18] Prior to the PRISM revelation, a top-secret court order compelling Verizon to turn over telephone records of millions of U.S. customers was leaked to news sources.[19] A distinguishing factor of PRISM collection is that it can include the content of communications and not just metadata, unlike the Verizon court order.[20] Companies have

---

13. *See id.* at 2002.

14. *See* Consolidated Version of the Treaty on the Functioning of the European Union of 30 March 2010, arts. 16, 216, 2010 O.J. (C 83/47) 9, *available at* http://europa.eu/pol/pdf/qc3209190enc_002.pdf.

15. *See* Press Release, European Comm'n, EU Data Protection: European Parliament's Legal Affairs Committee Backs Uniform Data Protection Rules (Mar. 19, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-233_en.htm. *But see* Cedric Burton, Christopher Kuner, & Anna Pateraki, *The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report*, BLOOMBERG BNA 2 (Jan. 21, 2013), *available at* http://www.wsgr.com/publications/PDFSearch/proposed-EU-0113.pdf (discussing agreement among EU member states for the goals of the Proposed Regulation but further noting that cumbersome legislative and negotiation processes in the EU may postpone development, setting forth the Albrecht Report as an example of suggested modifications that may delay final adoption).

16. 50 U.S.C. § 1881(a) (2012).

17. *See* Lee, *supra* note 2 (demonstrating the lack of information the public has had of the intricacies of PRISM).

18. *See Verizon Forced to Hand Over Telephone Data—Full Court Ruling*, THE GUARDIAN (June 5, 2013, 7:04 PM), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order; *see also* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

19. *See* Lee, *supra* note 2.

20. *See* Greenwald & MacAskill, *supra* note 18.

denied involvement, claiming that data is shared only after company lawyers have reviewed FISA requests.[21] The U.S. government used the Patriot Act[22] to justify obtaining records of every phone call on Verizon's network, demonstrating its willingness to adopt broad legal interpretations for its requests.[23]

A. Key Aspects of the Proposed Regulation that are Incompatible with U.S. Government Surveillance

The following provisions requiring a transparent processing of data would conflict with the broad access PRISM grants the U.S. government to the servers of the U.S. companies involved. Article 5 of the Proposed Regulation requires that the processing of personal data be "adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed."[24] Additionally, a temporal limitation on data processing manifests itself in the newfound "right to be forgotten."[25] The Proposed Regulation also gives the data subject the right to ascertain the "means of the processing of personal data, ask for the erasure of personal data relating to them, and abstention from further dissemination of such data" when certain conditions are met.[26] Under this provision, EU citizens would be able to ask that their data be deleted if they no longer want the data to be processed.[27] In an effort to encourage respect for individual privacy, the Proposed Regulation increases the size of monetary

---

21. *See* Lee, *supra* note 2 (noting that section 702 allows the NSA to obtain private communications of U.S. citizens as part of a request that officially targets a foreigner, and orders can range from inquiries about specific people to a broad sweep for intelligence, including logs of certain search terms). *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2011) (codified at 18 U.S.C. 1 (2012)).

22. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001.

23. Lee, *supra* note 2.

24. *See Commission 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 (General Data Protection Regulation)*, art. 5(c), COM (2012) 11 final (Jan. 25, 2012).

25. *Id.* art. 17(1)(a)–(d).

26. *Id.* (including the following conditions: the data is no longer necessary in relation to the purposes for which they were collected or otherwise processed, consent for the processing has been withdrawn, the authorized storage period has expired and, the concerned individual has objected to the processing of the information).

27. *Id.* (noting further that there must be no legitimate reasons for keeping the data).

sanctions for violations of these standards, permitting fines amounting to two percent of a company's global revenue.[28]

III. U.S. COMPANIES WILL UNDERMINE THE EU PROPOSED REGULATION THROUGH COMPLIANCE WITH THE PRISM PROGRAM

U.S. companies are accused of not only failing to adhere to the principles of EU data protection laws despite continuing to receive personal data from the EU, but also aiding the mass surveillance of EU citizens by granting the U.S. government access to their servers.[29] The widespread acknowledgement of the diminished capability these companies have to protect the data of EU citizens demonstrates the strong likelihood that continued compliance with the PRISM program jeopardizes the very purpose of the Proposed Regulation. U.S. companies operating in the EU are likely to be held in breach of EU law, and without more action, will face negative economic repercussions due to a loss of transatlantic trust.[30] Moreover, provisions that would punish breaching companies with hefty fines have been deemed a "necessity" and "irreversible" by the European Parliament, indicating that the heightened emphasis on stringent EU data protection reform is unlikely to abate.[31]

A. The EU Response to the Revelation of the PRISM Program

The European Commission voiced concern about PRISM as early as June 11th, 2013, a week after the PRISM documents were leaked.[32] The

---

28. *Id.* art. 79(2) (reiterating that the sanctions are meant to be "effective, proportionate, and dissuasive" and that a multifactor test to calculate administrative fines takes into account the nature, gravity, duration, and the intentional or negligent character of the breach; the degree of responsibility of the natural or legal person; the technical and organizational measures and procedures implemented; and the degree of cooperation with the supervisory authority).

29. *See* Claude Moraes, *The U.S. NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs* 11 (Comm. on Civil Liberties, Justice and Home Affairs, Eur. Parl., Draft Report 2013/2188(INI), 2014) [hereinafter *Draft Report*], *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN (pointing to the Federal Trade Commission's acknowledgement that the Safe-Harbor Agreement protecting U.S. companies needs to be reviewed).

30. *See id.* at 12, 24.

31. Allison Grande, *EU Parliament Backs Privacy Reform, Bashes NSA Spying*, LAW 360 (Mar. 12, 2014, 9:28 PM), http://www.law360.com/articles/517796/eu-parliament-backs-privacy-reform-bashes-nsa-spying-.

32. *See European Commission: European Union Position on PRISM,* YOUTUBE (June 11, 2013), http://www.youtube.com/watch?v=YMaSkMLVEgw; *see also* Andreas Geiger, *EU Will Ramp Up Data Protection in Wake of Snowden*, THE HILL (Aug. 14, 2013, 7:00 PM), http://thehill.com/blogs/congress-blog/foreign-

statement highlighted differences between U.S. and EU approaches to data protection, specifically that the U.S. only grants U.S. citizens privacy protections in the U.S. while EU citizens are not guaranteed constitutional safeguards or sufficient oversight of data collection, ensuring that it is within legal bounds.[33] The authoritative statement from the European Commission emphasized that the PRISM program must be limited to individual cases and based on concrete suspicions if it is for law enforcement purposes.[34] Specifically, data protection reform would need to address territorial scope to ensure non-EU companies would be subject to EU data protection law while operating in Europe.[35]

B. PRISM's Negative Economic Repercussions So Far and Further Predictions

The U.S. cloud-computing industry is likely to lose substantial amounts of revenue and become less competitive in the global cloud-computing market.[36] Companies storing electronic data with U.S. cloud-computing firms will suffer because of a loss of EU trust in the U.S. government, and may also lose revenue as a result of their use of U.S. cloud-computing firms.[37] Moreover, some European cloud providers have noted an increase in business after the PRISM scandal.[38] Switzerland's Artmotion

---

policy/317061-eu-will-ramp-up-data-protection-in-wake-of-snowden-.

33. *See European Commission: European Union Position on PRISM*, *supra* note 32.

34. *See id.*

35. *See id* (addressing the need for a territorial scope provision within EU data protection law that would require U.S. companies to apply EU law to any processing of EU citizens' personal data when operating in the EU).

36. *See* Juha Saarinen, *US Cloud-Computing Industry Faces US$35 Billion PRISM Fallout*, IT NEWS (Aug. 6, 2013, 8:00 AM), http://www.itnews.com.au/News/352419,us-cloud-computing-industry-faces-us35-billion-prism-fallout.aspx?goback=.gde_1243587_member_263605405. *But see* Charles Babcock, *NSA's Prism Could Cost Cloud Companies $45 Billion*, INFO. WEEK CLOUD (Aug. 14, 2013, 7:47 PM), http://www.informationweek.com/cloud-computing/infrastructure/nsas-prism-could-cost-us-cloud-companies/240159980 (making a bleaker prediction of a $45 billion loss, because the Information Technology and Information Institute's (ITIF) projected loss does not consider firms already planning on leaving U.S. providers regardless of the NSA surveillance program, and cloud users in the U.S. that may circumvent the U.S. cloud providing firms and may offshore some of their business to meet international demands).

37. *See* Babcock, *supra* note 36 (describing ITIF's findings that of the 207 non-U.S. respondents surveyed, 56% claimed that they were less likely to use U.S.-based cloud providers because of PRISM, and 10% even cancelled projects with U.S. based cloud providers).

38. *See Germans Look for Encrypted Emails in Wake of NSA Revelations*, UPI (Aug. 29, 2013, 11:12 AM), http://www.upi.com/Top_News/World-News/2013/08/29/Germans-look-for-encrypted-emails-in-wake-of-NSA-revelations/UPI-3402137

experienced a significant revenue increase of 45% the same month the details of the PRISM program were leaked by Snowden.[39] Although some conclude that data stored in the U.S. is still more protected than data stored in European countries, more information about PRISM is necessary to fully understand its economic repercussions for cloud-computing.[40]

If FISA requests are incompatible with the Proposed Regulation and companies are obliged to comply with them, U.S. companies will be subject to legal and financial penalties under EU law.[41] For example, Skype was under investigation by the DPA in Luxembourg for alleged contribution to the PRISM program.[42] Because the NSA only gains direct access to data after FISA orders are reviewed by a company's lawyers, and because the requests are not search warrants under the Fourth Amendment and do not require probable cause for authorization, it is likely that the EU will ask for more FISA transparency.[43] Furthermore, the NSA has defended FISA requests by emphasizing that the orders only target non-US citizens, making it more likely that the EU will be concerned about the

---

7789143/ (detailing the statements of the Managing director of Cloudsafe, indicating that the volume of traffic and customers of his company has increased by 20 percent); *see also* Elizabeth Dwoskin & Frances Robinson, *NSA Internet Spying Sparks Race to Create Offshore Havens for Data Privacy,* WALL ST. J. (Sept. 27, 2013, 12:15 PM), http://online.wsj.com/article/SB10001424052702303983904579096082938662594.html (reporting that several European countries are attempting to be the 'Cayman Islands' of privacy and on European leaders that are calling for a domestic 'Euro Cloud,' also noting that some have called such goals impractical due to the inherent widespread nature of the internet).

39. *See* Elizabeth MacDonald, *NSA Leaks Slam Cloud Computing Industry,* FOX BUS. (Aug. 9, 2013), http://www.foxbusiness.com/government/2013/08/09/nsa-leaks-slam-cloud-computing-industry/.

40. *See* Lee, *supra* note 2 (failing to note whether FISA requests, which have not been reviewed by the Supreme Court, can be considered legitimate court orders, given the unequal bargaining power between U.S. companies and the U.S. government).

41. *See* John Nugent, *Silicone Valley Could Become Collateral Damage in NSA Leaks*, FORBES (July 31, 2013, 12:42 PM), http://www.forbes.com/sites/riskmap/2013/07/31/silicon-valley-could-become-collateral-damage-in-nsa-leaks.

42. Ryan Gallahger, *Skype under Investigation in Luxembourg over Link to NSA*, THE GUARDIAN (Oct. 11, 2013, 6:30 AM), http://www.theguardian.com/technology/2013/oct/11/skype-ten-microsoft-nsa (detailing the revelations of Skype's involvement with the NSA which allegedly dates back to February 2011, and how Microsoft, which owns Skype, has been embroiled in legal disputes with the U.S. government to reveal the number of U.S. information requests it receives).

43. *See* Lee, *supra* note 2; *see also* Ian Brown, *Will NSA Revelations Lead to the Balkanisation of the Internet?*, THE GUARDIAN (Nov. 2, 2013, 2:05 PM), http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet (describing reports that EU member states are calling for greater U.N. participation in internet privacy after the PRISM revelations; Germany specifically has called for the U.N. Human Rights Council to create an optional protocol in the International Covenant on Civil and Political Rights regarding internet privacy).

flexibility afforded to U.S. government surveillance when it does not target a U.S. citizen.[44]

Data privacy compliance costs for U.S. companies with a presence in Europe will increase because of the expected rigorous enforcement of the Proposed Regulation.[45] Article 26 of the Proposed Regulation would build on Article 17(2) of Directive 95/46/EC[46] and increase the obligations of the data processors chosen by data controllers. Overall, increasing concerns about cloud security will push EU policy makers to prioritize security guarantees over open markets, further complicating EU compliance for U.S. companies.[47] The Proposed Regulation's stringent set of data privacy rules are not cost-effective for businesses that will, as a result, grapple with an increased and unfavorable compliance load.[48]

Jan-Phillip Albrecht, the European Parliament's chief negotiator on the Proposed Regulation, has indicated a desire to ensure that the data of EU citizens stays on servers in the EU and transfers of data are limited to certain places.[49] In September of 2013, the European Parliament began conducting an inquiry into the NSA's PRISM program.[50] The Civil Liberties, Justice and Home Affairs ("LIBE") Committee released its report evaluating U.S. surveillance on January 8th, 2014, strongly condemning the

---

44. *See* Behnam Dayanim, *Julie Brill, the Safe Harbor and the NSA: Unintended Consequences?*, LEXOLOGY, (August 26, 2013), http://www.lexology.com/library/detail.aspx?g=936b4385-d7c3-46a4-b46b-4e4061254767 (concluding that the Safe Harbor is likely to be upheld due to the economic stronghold between the U.S. and EU, but that U.S. dominance in the communications sector will suffer instead).

45. *See* Frances Robinson, *U.S. Surveillance Programs Spur Efforts to Tighten Data Protection Rules*, WALL ST. J. (Aug. 8, 2013, 5:23 PM), http://online.wsj.com/article/SB10001424127887324522504579000702411343532.html.

46. *E.g.*, Council Directive 95/46, art. 17(2), 1995 O.J. (L 281) 31-50 (EC), *available at* http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46 ("The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.").

47. *See* David Meyer, *European PRISM Anger Gains Momentum with Fresh Cloud Warnings and Data Threats*, GIGAOM (July 4, 2013, 7:18 AM), http://gigaom.com/2013/07/04/european-prism-anger-gains-momentum-with-fresh-cloud-warnings-and-data-threats/.

48. *See* Kevin J. O'Brien, *Firms Brace for New European Data Privacy Law*, N.Y. TIMES (May 13, 2013), http://www.nytimes.com/2013/05/14/technology/firms-brace-for-new-european-data-privacy-law.html?_r=0.

49. *See id.*

50. Allison Grande, *EU Parliament Members Bash NSA Spying, Push Cos. to Talk*, LAW 360 (Sept. 6, 2013, 5:06 PM), http://www.law360.com.proxy.wcl.american.edu/articles/470674/eu-parliament-members-bash-nsa-spying-push-cos-to-talk.

PRISM program which, according to its findings, amounts to "political and economic espionage."[51]

C. *Recent Cases Demonstrate a Desire in EU Member States to Enforce Data Protection Standards against U.S. Companies*

Five recent cases in France and Germany involving Twitter, Facebook, and Apple demonstrate that EU member states enforce their individual data protection laws against U.S.-based companies. The Civil Court of Paris held that Twitter is not subject to French data protection law but remains obligated under the French Code of Civil Procedure to reveal the identity of its users in France posting racist tweets.[52] Because Twitter has not cooperated with the order, the Union of French Jewish Students that filed the claim is taking further legal action.[53]

Germany's state data protection regulators also issued an opinion arguing that Facebook's policy requiring users to register accounts under their real name violates Germany's data protection law, which allows anonymous use of social media.[54] However, since the relevant data is processed in Ireland, which does not have an identical data protection law, a German administrative court ruled that Facebook is not subject to German law.[55] Facebook was less successful in a 2012 case involving a regional German court that ruled that its "Friend Finder" method of soliciting new users via other users' email addresses, and its practice of forcing users to give access to their online material is illegal.[56] Facebook

---

51. *See Draft Report*, *supra* note 29, at 18, 20, 21 (detailing the investigation procedure and recommendations of the Committee which include: suspension of the Safe-Harbor agreement, redress for EU citizens in case of data transfers, and EU IT independence from the U.S.).

52. Cecile Martin, *Navigating the Patchwork: When is European Data Privacy Law Applicable to US Companies?*, PROSKAUER PRIVACY L. BLOG (Apr. 17, 2013), http://privacylaw.proskauer.com/2013/04/articles/online-privacy/navigating-the-patchwork-when-is-european-data-privacy-law-applicable-to-us-companies/ ("Article 145 of the French Code of Civil Procedure does not include . . . geographical limitations and allows parties . . . to seek evidence before a case has been formally instituted.").

53. *See Verwaltungsgericht gibt Eilanträgen von Facebook statt*, LANDESREGIERUNG SCHLESWIG-HOLSTEIN (Feb. 15, 2013), http://www.schleswig-holstein.de/OVG/DE/Service/Presse/Pressemitteilungen/15022013VG_facebook_anonym.html; *see also* Martin, *supra* note 47.

54. *See* Martin, *supra* note 52.

55. German data protection regulators have subsequently filed an appeal.

56. *See* Pressemitteilung [Press Release], Landgericht Berlin [Berlin District Court], Facebook unterliegt der Verbraucherzentrale in Wettbewerbsprozess [Facebook is Subject to the Consumer in the Competitive Process] (Mar. 6, 2012), *available at* http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20120306.1545.367067.html; Shayndi Race & Friedrich Gieger, *Facebook Loses Privacy Case in German Court Over Email*, WALL ST. J. (Mar. 6, 2012, 6:44 PM), http://online.wsj.com/news

was already amending its Friend Finder policy in 2011 after the Irish Data Protection Commission reported that Facebook needed to amend its policies regarding user privacy.[57] Further regulating data privacy, in May 2013, a court in Berlin voided eight contract clauses regarding data usage in Apple's contracts with German customers.[58] Apple requested "global consent" for the data of its customers, but the court denied the request, reasoning that Apple should be more transparent regarding details of how users' data are utilized.[59]

The controversy in Europe regarding Google's "Street View" helps distinguish the approaches among EU member states to data protection.[60] Member states use a national or regional DPA, which may either directly fine violators of data protection standards or submit a report to a prosecutor to bring the matter to a court of law.[61] Germany's regional Hamburg-based DPA previously enforced its data privacy standards against Google.[62] Between 2008 and 2010, Google Street View camera cars allegedly recorded and stored information, including emails, photos, and private passwords illegally from unsecure Wi-Fi networks.[63] Although the data was collected accidentally and criminal prosecution against Google was subsequently deemed unnecessary, German data regulators fined Google

---

/articles/SB10001424052970203458604577265764008504218.article/SB10001424052970203458604577265764008504218.html.

57. *See* Race & Gieger, *supra* note 56.

58. *See* Landgericht Berlin [Berlin District Court] Apr. 30, 2013 (Ger.), *available at* http://www.vzbv.de/cps/rde/xbcr/vzbv/Urteil_des_LG_Berlin_zur_Datenschutzrichtlinie_von_Apple.pdf; *see also* Karen H. Bromberg, *Berlin Court Rules that Apple's Privacy Policy Violates German Data Protection Laws*, COHEN & GRESSER LLP 1 (May 2013), *available at* http://www.cohengresser.com/assets/publications/Berlin_Court_Rules_that_Apples_Privacy_Policy_Violates_German_Data_Protection_Laws.pdf.

59. *See* Bromberg, *supra* note 58, at 1.

60. The existing privacy directive provides a framework that requires EU member states to enact legislation to implement the directive into its country's laws and has been described as setting the floor for EU member state legislation and, in some cases, may also set the ceiling, leading to great divergence among member states' interpretation and application of the directive.

61. *See* Andrea Ward & Paul Van den Bulck, *Differing Approaches to Data Protection/Privacy Enforcement and Fines, Through the Lens of Google Street View*, IAPP: INT'L ASS'N OF PRIVACY PROFESSIONALS (June 1, 2013), https://www.privacyassociation.org/publications/2013_06_01_differing_approaches_to_data_protection_privacy_enforcement_and.

62. It is worth noting that Article 35 of the Proposed Regulation, which requires the appointment of a data protection officer in companies employing at least 250 persons, is based on German data protection law.

63. *See* Ian Steadman, *Google Fined by German Regulator over Street View Privacy Breach*, WIRED (Apr. 22, 2013), http://www.wired.co.uk/news/archive/2013-04/22/google-germany-fine.

€145,000, the maximum under German law, even pushing to increase the fine.[64] Given that the personal information was deleted and never used by Google employees, and Google still incurred a fine, the actions of the German data regulators indicates the perception of unauthorized usage and storage of data in Germany.[65]

The decision by the DPA in Hamburg regarding Google Street View's unauthorized data storage was preceded by similar actions in the member states of France and Belgium. While France's national DPA did not find Google's actions to be in "bad faith," which would have resulted in a publication of the judicial decision in the media, it did fine Google €100,000, the highest fine given by the French DPA at the time.[66] In Belgium, Google avoided going to a criminal court and agreed to a €150,000 settlement with the Belgian national DPA.[67] Possibly because of political pressure resulting from EU member states taking action, the UK Information Commissioner's Office eventually required Google to agree to both improving its methods of collecting and protecting data and allowing the Office to audit Google.[68] Meanwhile, Google still faced penalties in the U.S.: 39 U.S. states' attorneys general required Google to agree to an "Assurance of Voluntary Compliance."[69]

IV. WHAT CAN COMPANIES DO TO ALLEVIATE LIABILITY?

Companies involved in the PRISM program should take immediate steps to demonstrate a desire to protect the data of EU citizens despite continued allegations of mass surveillance. Support for a security arrangement that guarantees information will be proportionate and necessary for law enforcement purposes, or a push for U.S. governmental transparency with

---

64. *See* Press Release, Hamburg Comm'r for Data Prot. and Freedom of Info., Fine Imposed Upon Google (Apr. 22, 2013), *available at* http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease_2013-04-22_Google-Wifi-Scanning.pdf; *see also* Ian Steadman, *Google Fined by German Regulator over Street View Privacy Breach*, WIRED (Apr. 22, 2013), http://www.wired.co.uk/news/archive/2013-04/22/google-germany-fine.

65. *See* Ian Steadman, *supra* note 63.

66. *See generally* Letter from Christopher Graham, U.K. Info. Comm'r, to Peter Fleischer, Global Privacy Counsel, Google Fr. (Nov. 3, 2010), *available at* http://www.ico.org.uk/~/media/documents/library/Corporate/Notices/google_inc_gsv_letter_03112010.ashx; *see also* Ward & Bulck, *supra* note 61.

67. *See* Ward & Bulck, *supra* note 61.

68. *See id.*

69. *See Rhode Island v. Google, Assurance of Voluntary Compliance*, *available at* http://www.riag.ri.gov/documents/AVC-RIAG-Google.pdf; *see also* Ward & Bulck, *supra* note 61 (noting the requirement and agreement for companies to pay $7 million in fines to the states that had been subjected to the unauthorized data storage and to, *inter alia*, train its workforce about privacy protection).

FISA requests would help diminish the negative perception that U.S. companies are facing due to PRISM involvement.

A. U.S. Companies Should Lobby for Favorable Data Protection Legislation in Both the U.S. and EU to Decrease Their Potential Liability and Increased Compliance Loads Under the Proposed Regulation

U.S. companies can continue to lobby for legislation both in the EU and U.S., as many have done in the past, to eschew potential compliance costs under the Proposed Regulation. Google and Facebook successfully spent $5.03 million and $650,000 respectively to lobby the U.S. Congress in the first quarter of 2012, much of which went to legislation on data privacy issues.[70] Recently, President Obama announced support for key reforms to the FISA program, including a more adversarial court system in which privacy advocates would be able to voice their concerns in the FISA court.[71] Another proposal is to limit the scope of Section 215 of the Patriot Act, because it allows the U.S. government to maintain a national system of telephone metadata and has been criticized for a lack of judicial oversight.[72] The technology industry has been actively lobbying the White House for the adoption of policies that promote more transparency, privacy, and international free flow of information.[73] Specifically, the companies call for support for a bill sponsored by Senators Patrick Leahy and Mike Lee that would bring the Electronic Communications Privacy Act of 1986[74] up to date since it has had no significant revisions since its implementation.[75] Companies could also support a bill authored by U.S. Representative Rush D. Holt, who is sponsoring the "Surveillance State Repeal Act."[76] This Act would, *inter alia*, repeal the Patriot Act, significantly revise the FISA

---

70. *See* Leena Rao, *Google, Facebook Spent Record Amounts on D.C. Lobbying in Q1 2012*, TECH CRUNCH (Apr. 22, 2012), http://techcrunch.com/2012/04/22/google-facebook-spent-record-amounts-on-d-c-lobbying-in-q1-2012/.

71. *See* Daniel Klaidman, *Obama Says He'll Reform the NSA. Happy Now?*, THE DAILY BEAST (Aug. 9, 2013), http://www.thedailybeast.com/articles/2013/08/09/obama-says-he-ll-reform-the-nsa-happy-now.html.

72. *See id*; *see also* 50 U.S.C. § 1881(a) (2012).

73. *See* Andrew Ramonas, *Tech Groups Want Transparency in NSA Surveillance*, CORP. COUNS. (Aug. 21, 2013, 1:19 PM), http://www.corpcounsel.com/id=1202616426454/Tech-Groups-Want-Transparency-in-NSA-Surveillance?slreturn=20140210171452.

74. Electronic Communications Privacy Act, S. 607, 113th Cong. (2013).

75. *See id.*

76. *See* Scott Shane & Nicole Perlroth, *Legislation Seeks to Bar N.S.A Tactic in Encryption*, N.Y. TIMES (Sept. 6, 2013), http://www.nytimes.com/2013/09/07/us/politics/legislation-seeks-to-bar-nsa-tactic-in-encryption.html?pagewanted=all.

Amendments Act of 2008, and prohibit the federal government from requiring manufacturers of electronic devices or software to build a mechanism allowing the U.S. Government to bypass the encryption or privacy technology of such device or software.[77]

U.S. companies also put their efforts in lobbying the EU to reform its data protection laws to create a marketplace more favorable for U.S companies. Amazon's suggestions to reduce the responsibilities of non-EU cloud providers were incorporated into proposed amendments to the Proposed Regulation.[78] The European Parliament, however, recently voted to reintroduce a clause that was previously dropped due to U.S. lobbying efforts.[79] That clause would regulate transfer of data from Europe to the U.S., and the addition of the clause suggests that the EU may not be receptive to making concessions for its data protection laws.[80]

One notable attempt by a U.S. company to push for greater government transparency is Yahoo's order requesting the U.S. government to justify the legality of the PRISM program. After the documents leaked confirming the existence of PRISM, Yahoo's lawyers asked the FISA Court to declassify and publish decisions detailing the constitutionality of the PRISM program.[81] The court, siding with Yahoo, ordered the Obama Administration to declassify and publish a court decision justifying the PRISM program,[82] Companies including Microsoft, Google and Facebook, have also asked for U.S. government permission to publicly identify the number of national security related requests that each company receives, in an effort to contribute to the ongoing public debate surrounding user privacy.[83] An 85-page ruling recently released by the Obama

77. *See* Surveillance State Repeal Act, H.R. 2818, 113th Cong. (2013).

78. *See Forum Shopping for IT Companies*, http://www.europe-v-facebook.org/IMCO_pub_en_ON.pdf (last visited Sept. 4, 2013) (noting that suggestions include limiting the Proposed Regulation to setting uniform data protection aspects across member states, preserving future opportunities for collaborative policy-making, and limiting the power of the Commission).

79. Ian Traynor, *MEPs Tighten up Draft Data Privacy Rules After Snowden Revelations*, THE GUARDIAN (Oct. 22, 2013, 7:04 AM), http://www.theguardian.com /world/2013/oct/22/meps-data-privacy-rules-snowden-nsa-gchq.

80. *See id.*

81. *See* Spencer Ackerman, *Justice Department to Declassify Key Yahoo Surveillance Orders*, THE GUARDIAN (July 30, 2013, 10:34 AM), http://www.theguardian.com/world/2013/jul/30/justice-department-declassify-yahoo-surveillance-orders.

82. *See id.* (arguing that the Justice Department's review may declassify particular documents).

83. *See* Charles Arthur & Dominic Rushe, *NSA Scandal: Microsoft and Twitter Join Calls to Disclose Data Requests*, THE GUARDIAN (June 12, 2013, 5:50 PM), http://www.theguardian.com/world/2013/jun/12/microsoft-twitter-rivals-nsa-requests.

Administration could shed light on the nature of future decisions that may be released.[84] The opinion, authored by Judge John D. Bates, a former chief judge on the FISA court, focuses on a NSA program that searches the content of Internet communications of U.S. citizens without a warrant if it targets noncitizens outside of the U.S. [85] Bates expressed skepticism as to the scope of the government's surveillance, deeming the government's behavior a "substantial misrepresentation."[86] Bates additionally noted that the NSA had consistently violated a 2009 ruling regarding the standard of queries of metadata, and had done so consistently, causing the NSA to have never "functioned effectively."[87] Skeptics of the release note that the opinion is demonstrative of the limits of the FISA court.[88]

There is also evidence that the Department of Commerce is lobbying the EU as the latter plans to reform data privacy. The Department of Commerce has been explicitly concerned about the requirement the EU may impose on companies to report to the appropriate DPAs within 24 hours of data breaches, as well as the right to be forgotten.[89] The rule is problematic because many firms lack the appropriate technologies to recognize such data breaches in a timely manner.[90] Firms may also report inaccurate cases of breaches to the authorities because of fear of missing the 24-hour notification requirement and consequently being subject to a fine.[91]

---

84. *See Judge's Opinion on N.S.A. Program*, N.Y. TIMES (Aug. 21, 2013), http://www.nytimes.com/interactive/2013/08/22/us/22nsa-opinion-document.html (providing scanned images of the court documents).

85. *See id.*

86. *See id.*

87. *See id.*

88. *See* Charlie Savage & Scott Shane, *Secret Court Rebuked N.S.A. on Surveillance*, N.Y. TIMES (Aug. 21, 2013), http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?pagewanted=all&_r=0 (expressing skepticism because the scrutiny is limited to what the NSA actually reveals to the court which has no independent ability to investigate the representations).

89. *See* Shelton Abramson, *TechWeek Europe: US Department of Commerce Involved in Lobbying to Change EU Data Protection Regulation*, INSIDE PRIVACY (Oct. 15, 2012), http://www.insideprivacy.com/united-states/techweek-europe-us-department-of-commerce-involved-in-lobbying-to-change-eu-data-protection-regulati/ (providing a broad overview of the Department of Commerce's lobbying efforts, and also noting that its specific proposals are unclear).

90. *See EU Businesses Prep for Regulations Requiring 24-Hour Data Breach Notification*, INFOSECURITY (Aug. 22, 2013), http://www.infosecurity-magazine.com/view/34102/eu-businesses-prep-for-regulations-requiring-24hour-data-breach-notification/ (discussing that processing network data inefficiently can lead to breaches).

91. *See id.* (noting that problems may arise for firms where data is inefficiently processed).

B. Companies Should Support an Agreement Modeled After the Passenger Names Record Agreement

Another possible solution would be to implement an agreement similar to the U.S. and EU agreement regarding the use and transfer of passenger name records to the Department of Homeland Security ("DHS").[92] The agreement requires European airlines to give the DHS data about trans-Atlantic travelers prior to departure. The information includes each passenger's name, address, reservation dates, number of bags, payment details, seat number, travel itinerary and, in some instances, racial or ethnic origin, religion, and health.[93] The agreement came to fruition as a result of both parties wanting to combat transnational crime and terrorism, while maintaining transatlantic travel and tourism, which accounts for $72.2 billion in trade each year.[94] Stipulations provide for the depersonalization of such information, which is the "masking out" of key information including names, contact information, general remarks, and collected Advance Passenger Information System data, after six months, after which the remaining data will be kept on an active database for five years and in a dormant database for another ten years.[95] Any data in the dormant database may be "repersonalised" for only a period of five years.[96] Data under the Passenger Name Records Agreement ("PNR") can be "repersonalised" only if it is "in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk."[97]

Similarities can be drawn between the current PRISM problem and the enactment of the PNR. The Obama administration has defended the PRISM program, reiterating that it has led to the prevention of numerous terrorist attacks.[98] As an example, should the NSA wish to gain access to

---

92. *See generally* Agreement Between the United States of American and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, U.S.-EU, Nov. 8, 2012, 2012 O.J. (L 215) [hereinafter PNR agreement], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:215:0005:0014:EN:PDF.

93. *See id.* Annex, at 10. (detailing the types of PNR data).

94. *See* Claire Davenport, *EU Agrees to Share Airline Passenger Data with U.S*, REUTERS (Apr. 19, 2012), http://www.reuters.com/article/2012/04/19/oukwd-uk-eu-usa-flights-idAFBRE83I0TG20120419.

95. *See* PNR agreement, *supra* note 92, at 4.

96. *See id.* at 4.

97. *See id.* at 4 (explaining that after the dormant period, the data must be "rendered fully anonymised" and cannot be "repersonalised" under any circumstance, and any individual, regardless of citizenship, can access his or her Passenger Name Record under the Freedom of Information Act).

98. *See* Sumi Somaskanda, *NSA Spying Rankles Privacy-Loving Germans*, THE ATLANTIC (July 25, 2013, 10:00 AM), http://www.theatlantic.com/international/archive/2013/07/nsa-spying-rankles-privacy-loving-germans/278090/.

the information of a phone call, it could request such information immediately, under the condition that the information be depersonalized after the call has transpired, while the remaining information on the call will be put on a dormant database after five years (only to be "repersonalised" in limited cases pertaining to global or national security) and fully deleted in another ten years.[99] Furthermore, the agreement would prove abundantly helpful for U.S. companies, like the PNR proved for European Airlines, because it would mitigate the difficult choice between complying with U.S. or EU law.[100] Finally, if U.S. companies publicly advocate for such an agreement, it would help demonstrate a commitment to abide by EU data protection standards, which could in turn afford them some leverage in lobbying efforts to amend the Proposed Regulation.

Unfortunately, the prospects for a PNR-like agreement may be waning given recent political developments. On July 4th, 2013, the European Parliament, in light of the U.S. surveillance programs, overwhelmingly adopted a resolution (483 supporting, 98 opposing, 65 abstaining) in support for ending, should the European Commission find it necessary, any sort of data sharing, including the PNR agreement.[101] Many of the critics of the PNR agreement believe that the agreement has not been useful in preventing terrorism.[102] For the EU's Home Affairs Commissioner Cecilia Malmström, a new PNR agreement would better secure EU citizens' right to privacy than the prior PNR agreement in 2007.[103] Specific improvements suggested to the 2007 PNR agreement include the clarification that EU citizens have a right to access their PNR information in a U.S. database, to ascertain how their information is processed, and to correct any inaccurate data.[104] The new PNR agreement would prohibit

---

99. *See* PNR agreement, *supra* note 92, art. 8, at 4.

100. *See id.* (suggesting that the plausibility of such an agreement in the data privacy context will depend on whether it limits the scope of U.S. government surveillance to specific and concrete claims, requires explicit EU approval before any surveillance is conducted, and requires disclosure of surveillance details).

101. *See* Zack Whittaker, *EU Votes to Support Suspending U.S. Data Sharing Agreements, Including Passenger Flight Data*, ZDNET (July 4, 2013), http://www.zdnet.com/eu-votes-to-support-suspending-u-s-data-sharing-agreements-including-passenger-flight-data-7000017677/ (reporting on a European Parliament resolution supporting the termination of the U.S.-EU PNR agreement, a significant shift from an April 2013 approval of an updated PNR agreement).

102. *See id.*

103. *See European Parliament Approves the Controversial EU/US PNR agreement*, INFOSECURITY (Apr. 20, 2013), http://www.infosecurity-magazine.com/view/25284/european-parliament-approves-the-controversial-euus-pnr-agreement/ (providing general background information on the PNR agreements and the rationale behind its passage).

104. *See id.*

government profiling for decisions that will affect passengers, which is especially significant since a vote earlier in the year in the LIBE rejected the modified PNR agreement, amidst concerns that the modified agreement does not respect the fundamental rights of Europeans.[105]

CONCLUSION

Under the Proposed Regulation, U.S. companies could face sanctions reaching two percent of their global revenue for failure to comply, and even a cursory look at the Proposed Regulation indicates that participation in the PRISM program would clearly violate its stipulations. U.S. companies likely to receive FISA requests need to continue demanding transparency from the U.S. government and demonstrating a desire to ensure compliance with EU data protection standards. Such demands can materialize in the form of lobbying efforts for favorable data protection legislation; a push for maintaining the existing Safe Harbor Agreement, which has protected U.S. companies in the past;[106] or support for an agreement similar to the PNR between the U.S. and EU. Continuing to monitor the EU reaction to PRISM and subsequent U.S.-EU talks will help U.S. companies gauge what necessary efforts they must make to avoid violating EU data protection laws. Given the EU response thus far, it is likely that an intensive review of the Safe Harbor Agreement and amendments to the Proposed Regulation will address limitations on the extent to which U.S. government surveillance is permissible.[107] The U.S. government response

---

105. *See Latest PNR agreement for the EU Thrown out by European Parliament*, SHOEMAN.EU (Mar. 24, 2013), http://www.shoeman.eu/latest-pnr-agreement-for-the-eu-thrown-out-by-european-parliament/ (explaining the reasons behind a lack of support for the latest draft of the PNR agreement: a failure to adhere to the terms of the agreement, and extension of the scope of U.S. data mining). *But see Moraes: EP Is Looking Not Only into NSA Allegations but Also at EU's Own Backyard*, EUR. PARLIAMENT (June 11, 2013), http://www.europarl.europa.eu/news/en/news-room/content/20131106STO23912/html/Moraes-EP-looks-not-only-into-NSA-allegations-but-also-at-EU's-own-backyard (describing an interview with Moraes, head of the LIBE committee, who contends that although commercial trust has been damaged, he expects that there will be an agreement reached between the U.S. and EU).

106. Although a renewal of the Safe Harbor Agreement would be ideal, revelations regarding PRISM have jeopardized the existing agreement. EU Commissioner Vivian Reding has repeatedly emphasized that the Safe Harbor "may not be so safe after all" even though it has been an adequate method for U.S. companies to self-certify conformance to EU data protection standards because the U.S. lacks a data protection law. Additionally, various MEPs have called for review of the Safe Harbor and characterize it as a loophole for U.S. companies, making it unlikely that it will be maintained in the same fashion in the future.

107. *Moraes: EP Is Looking Not Only into NSA Allegations but Also at EU's Own Backyard*, *supra* note 105 (describing a report released in 2014 by the European Parliament which attaches a new legal remedy for EU citizens when their data is used,

to the situation has included suggestions that the EU is not immune from conducting clandestine surveillance in their own region.[108] Companies should, at the same time, take precautions to ensure maximum data protection security, possibly in the form of internal policies or employee training to demonstrate that data protection, at least internally, is a high priority.

---

also increasing potential liability for U.S. companies).

108. Karen Kornbluh, *Could the Revelations Regarding the NSA PRISM Program Hinder U.S. Relations Around the World?*, COUNCIL ON FOREIGN REL. (Oct. 7, 2013), http://www.cfr.org/defense-and-security/could-revelations-regarding-nsa-prism-program-hinder-us-relations-around-world/p31566 (concluding that trade discussions between the EU and U.S. still seem to be going forward but implications remain for U.S.–EU data management, also referring to a comment made by President Obama regarding a seemingly hypocritical criticism in the EU because the EU allegedly engages in surveillance tactics similar to PRISM).