THE KENAN INSTITUTE FOR ETHICS at DUKE UNIVERSITY

Teaching Caselettes

NSA, PRIVACY, SAFE HARBOR

Alexandra Zrenner

In June 2014, an Austrian privacy activist issued a complaint to the Irish Data Protection Commission (DPC). He argued that the NSA program PRISM, which collected the online data of foreign targets from various communication platforms, violated his privacy rights as a European citizen. The Irish DPC referred the complaint to the highest court in the European Union, the Court of Justice. The Court invalidated the Safe Harbor arrangement in light of the revelations of the NSA's data collection with PRISM. This case study will examine the origins of the Safe Harbor agreement, the NSA's PRISM program, and subsequent invalidation of the agreement.

This case study was completed under the direction of Dr. Amber Díaz Pearson, The Kenan Institute for Ethics.

Introduction

In October 2015, the European Union Court of Justice invalidated a fifteen-year-old trade arrangement between the European Union and the United States. This arrangement, known as "Safe Harbor" had allowed tech companies based in the United States to transfer data associated with European consumers to the United States so the company can serve the consumer. The Safe Harbor arrangement established a set of principles that would ensure United States companies would protect European consumers' data. The Safe Harbor arrangement set a minimum standard of privacy protections accepted by the European Union and allowed the United States Federal Trade Commission to oversee the enforcement of the arrangement in the States.

In June 2014, a young Austrian privacy activist, Max Schrems issued a complaint to the Irish Data Protection Commission (DPC). Schrems argued that the NSA program PRISM, which collected the online data of foreign targets from various communication platforms, violated his privacy rights as a European citizen. The Irish DPC referred the complaint to the highest court in the European Union, the Court of Justice. The Court invalidated the Safe Harbor arrangement in light of the revelations of the NSA's data collection with PRISM. With Safe Harbor no longer in effect, United States companies that serve European consumers now must meet the higher standard of privacy mandated by European laws. As the companies' business models rely heavily on data, the Court's decision has serious economic consequences for the US firms operating in European markets.
In February 2016, the United States and European Union created a new agreement, the E.U.- U.S. Privacy Shield, to protect the privacy of European Union citizens as their data is transferred to American companies. The E.U.-U.S. Privacy Shield created a higher standard of privacy protections (compared to the Safe Harbor standards) United States companies had to comply with for their European Union consumers.

This case study will examine the origins of the Safe Harbor agreement, the NSA's PRISM program, and subsequent invalidation of the agreement.

Origins of Safe Harbor

With the rise of the Internet and online-services like Google and Amazon in the 1990s, online and traditional business began to use consumers' personal data in providing goods and services. The European Union responded in 1995 with the Data Protection Directive, which provided a singe privacy framework for member states.[1] Unlike the European Union's DPD, the United States has no central law regarding information privacy.[2] Given the difference in data privacy laws, there were concerns that the European Union's new privacy protections could disrupt the economic trade that relies on personal data.

To address the different privacy standards, the European Union and United States negotiated an arrangement (though not a formal treaty), which created a set of principles and a framework for United States companies to follow to join and remain in the U.S.-E.U. Safe Harbor program. As a member of the program, the company is considered to adequately comply with the DPD. To satisfy Safe Harbor's requirements, the company must either join a self-regulatory privacy program or develop its own program, both of which must adhere to the Safe Harbor principles. These principles required an organization provide an individual information and choice regarding the uses of that individual's data. Moreover, an organization must only use data for relevant purposes and there must be enforcement mechanisms to ensure the companies comply with the Safe Harbor principles.[3]

NSA

In June 2013, the conversation surrounding individuals' personal data abruptly changed. *The Guardian* and *The Washington Post* published articles revealing the existence of the NSA's massive data collection program, PRISM. The NSA can access an individual's data directly from tech company servers, specifically Microsoft, Yahoo, Google, PalTalk, AOL, Skype, YouTube, and Apple, all of which publicly denied that the NSA had such access.[4]

Technology companies that provide a service online require some data to perform that task, whether personal information about an individual's preferences, IP addresses, or previous messages exchanged between individuals.[5] That information is stored on company servers. PRISM allows the NSA, and the FBI in some instances, access to that information through the company servers.

The Foreign Intelligence Surveillance Amendment (FISA) created the PRISM program and a court to oversee the program. The Foreign Intelligence Court (FISC) would issue warrants for the NSA to collect information.[6]

---

[1] European Union, European Parliament. (1995, October 24). *Directive 95/46/EC*. Retrieved May 17, 2016, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[2] Ku, R. (2014-2015). Data Privacy as Civil Right: The EU Gets It. *Kentucky Law Journal* 103(3), 391-404.

[3] U.S.-EU Safe Harbor Overview. (2013, December 18). Retrieved May 17, 2016, from https://build.export.gov/main/safeharbor/eu/eg_main_018476

[4] Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. Retrieved May 17, 2016, from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[5] For more information about what data a technology company collects, see Kenan's Google caselette Clipp, C. (2011). Don't Look Now, You're Being Googled. Retrieved May 17, 2016, from http://kenan.ethics.duke.edu/wp-content/uploads/2012/08/GoogleData_Case20151.pdf

[6] FISC created by FISA.

However, the court's actions were classified which prevented public accountability, and the *Washington Post* and *Guardian* discovered the program's processes were not standardized or predictable.

The NSA would request a warrant from the FISC to collect information on "targets," foreign nationals who were overseas. "Targets" would only exclude United States citizens, or citizens of close ally countries: Britain, Australia, Canada and New Zealand.[7] If the NSA discovers a "target" is a US citizen, the data is discarded.[8]

These warrants vaguely defined who constituted a target and allowed the NSA to collect information of individuals who were distantly connected to a target. The NSA can collect data of anyone within three degrees of an online connection to a target. If a target has 200 Facebook friends, there are over 32 thousand second degree friends and over 5 million third degree friends.[9] Therefore, the NSA could access up to 5 million other individuals in connection to one target, this data was considered incidental to a target.[10]

Moreover, internal documents of NSA communications indicate that there was a "lower threshold for foreignness 'standard of proof'" needed to satisfy the FISC. NSA analysts did not have to work hard to prove that a person whose data was collected was foreign. In some circumstances, analysts could presume that chat list friends of a known foreign national are also foreign.[11]

With this incidental data, the NSA would minimize identifying data of American, British, Canadian, Australian, and New Zealander citizens. Minimizing data is equivalent to the NSA analysts masking the data to protect the individual's privacy. Even if the NSA did mask an account, there was still unmasked information that could be traced back to the account with commercial level-access to information.[12] Incidental data of any other foreign citizen was not required to be minimized.

---

[7] Gellman, B., Tate, J., & Soltani, A. (2014, July 5). In NSA-intercepted data, those not targeted far outnumber the foreigners who are. Retrieved May 17, 2016, from https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

[8] Gellman, B. (2014, July 11). How 160,000 intercepted communications led to our latest NSA story. Retrieved May 17, 2016, from https://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html

[9] MacAskill, E., Dance, G., Cage, F., Chen, G., & Popovich, N. (2013, November 01). NSA files decoded: Edward Snowden's surveillance revelations explained. Retrieved May 17, 2016, from http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[10] Gellman, B. (2014, July 11). How 160,000 intercepted communications led to our latest NSA story. Retrieved May 17, 2016, from https://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html

[11] Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. Retrieved May 17, 2016, from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[12] Gellman, B. (2014, July 11). How 160,000 intercepted communications led to our latest NSA story. Retrieved May 17, 2016, from https://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html

The revelation of PRISM was shocking to European Union citizens. The NSA had access to foreigners' data since the majority of popular tech companies are based in the United States; since Safe Harbor permitted the transfer of EU data to the US, the NSA could access that data from US technology company servers. The NSA could also target EU citizens without a warrant (unless the individual was currently in the United States), and was not required to minimize the incidental data of non-British EU citizens. Moreover, a European could not sue the NSA in an American court, and did not have direct and obvious pathways for legal redress. The level of protection for EU citizens, and foreigners generally, was practically non-existent.[13]

Safe Harbor Decision

A year after the public discovery of PRISM, Max Schrems, the Austrian privacy advocate brought a complaint to the Irish Data Protection Commission.[14] The Austrian lawyer argued that the export of his personal data to the United States under Safe Harbor violated his fundamental rights as a European Union citizen.[15] The NSA could access any European Union citizen's data transferred to the United States, and this is a violation of the privacy protections required under Safe Harbor.

The Irish judge hearing the complaint referred the central questions of the complaint to the European Union's Court of Justice: given the claim that the laws and practices of the United States fail to adequately protect a EU citizen's data, does the Safe Harbor agreement still adhere to Articles 7, 8 and 47, (articles protecting an individual's privacy and private data) of the Charter of Fundamental Rights given?[16]

Originally, the Irish judge found, "that 'national security, public interest, or law enforcement requirements' have primacy over the Safe Harbor principles."[17] The judge indicated that a United States company should prioritize national security requirements, i.e. PRISM, above the Safe Harbor principles.

The European Union Court of Justice found that the data transfer program was, "beyond what was strictly necessary and proportionate to the protection of national security."[18] Moreover, the Court of Justice found that the EU data subjects had no legal means to address any violations of their personal data. The Court of Justice concluded that the Safe Harbor agreement is invalid.

---

[13] Even the established minimization process did not appear to be consistently employed; the *Washington Post* could strongly link nearly a thousand emails to American citizens from the leaked documents. Gellman, B. (2014, July 11). How 160,000 intercepted communications led to our latest NSA story. Retrieved May 17, 2016, from https://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html

[14] Under the EU Data Protection Directive of 1995, EU member states were required to create a supervisory authority to monitor the data protection within the state. European Union, European Parliament. (1995, October 24). *Directive 95/46/EC*. Retrieved May 17, 2016, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[15] Farrell, H., & Newman, A. (2015, October 6). This privacy activist has just won an enormous victory against U.S. surveillance. Here's how. Retrieved May 17, 2016, from https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/10/06/this-privacy-activist-has-just-won-an-enormous-victory-against-u-s-surveillance-heres-how/

[16] Maximillian Schrems v Data Protection Commissione, Curia (European Union Court of Justice October 6, 2015).

[17] Ibid.

[18] Ibid. 90.

Just as the news of PRISM had implications for the European Union, the invalidation of Safe Harbor has implications for the United States. The decision created, "great uncertainty for (the) businesses" that used the Safe Harbor framework for data transfers.[19] Transatlantic data transfers are more costly and burdensome, and potentially impossible, for companies with the invalidation of the Safe Harbor.[20]

The United States government was disappointed by the invalidation. The Secretary of Commerce, Penny Pritzker, stated that the invalidation created "significant uncertainty" for both U.S. and E.U. consumers and companies. Prtizker noted that the U.S. has worked with the E.U. to strengthen the Safe Harbor framework and privacy protections. Pritzker also said the US was prepared to create a new framework with the EU.[21]

Despite the Secretary's statement, companies remained concerned because the ruling is so broad that, "that any mechanism used to transfer data from Europe could be under threat."[22] The companies were no longer sure whether their practices were legal or not and whether they could face potential costly lawsuits. The companies could potentially stop transatlantic data transfers, losing a significant portion of their consumers and thus profits. Alternatively, the company could build data storage systems specifically located in Europe and for European customers, which would greatly increase the company's cost of operations and thus decrease profits. Almost any action, including inaction, in response to the Safe Harbor, could potentially and probably decrease the company's profits.

The invalidation of Safe Harbor created even more concerns for smaller tech companies. The large established tech companies, like Google and Facebook, could afford to create storage systems abroad or afford the legal costs of potential action taken against them in Europe. The smaller start-ups could not afford to create new systems or legal costs, or lose the access to European consumers.

Both the United States Chamber of Commerce and European business association, BusinessEurope, urged American and European leaders to negotiate a new agreement immediately following Court of Justice's decision.[23]

The new agreement is called the E.U. – U.S. Privacy Shield, which creates more opportunities for E.U. citizens to seek legal redress and stronger connections between U.S. and E.U. agencies.[24] As it currently stands, the E.U. – U.S. Privacy Shield gives E.U. citizens multiple avenues to gain legal redress whether through the company or the U.S. Federal Trade Commission or the E.U. Data Protection Authorities. The Privacy Shield also calls for an

---

[19] Dockery, S. (2015, December 1). U.S. Chamber of Commerce Sounds Alarm Over Safe Harbor. Retrieved May 17, 2016, from http://blogs.wsj.com/riskandcompliance/2015/12/01/u-s-chamber-of-commerce-sounds-alarm-over-safe-harbor/

[20] Ibid.

[21] *The Advisory Council to Google on the Right to be Forgotten* (Madrid). (2014, September 9). Retrieved May 17, 2016, from Google website: https://docs.google.com/document/d/1tFES5cz_n5gtq8WDbNiVxqVk-3NYxhJZsfZ42tbyjjA/pub

[22] Scott, M. (2015, October 06). Data Transfer Pact Between U.S. and Europe Is Ruled Invalid. Retrieved May 17, 2016, from http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html

[23] Dockery, S. (2015, December 1). U.S. Chamber of Commerce Sounds Alarm Over Safe Harbor. Retrieved May 17, 2016, from http://blogs.wsj.com/riskandcompliance/2015/12/01/u-s-chamber-of-commerce-sounds-alarm-over-safe-harbor/

[24] U.S. Department of Commerce. (2016, February 2). *EU-U.S. Privacy Shield* [Press release]. Retrieved May 17, 2016, from https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield

ombudsperson, who will follow up on an individual's complaints, within the U.S. Department of State and isindependent from national security services.[25] The European Commission's press release stated that the new agreement, "restore(s) trust in transatlantic data flows since the 2013 surveillance revelations."

[25] European Commission. (2016, February 29). *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield* [Press release]. Retrieved May 17, 2016, from http://europa.eu/rapid/press-release_IP-16-433_en.htm