The NSA, Snowden and the Tension between the US and Its European Allies

Abstract

In June 2013, Edward Snowden, an NSA contractor for Dell and Booz Allen Hamilton, leaked thousands of documents revealing many global surveillance programs run by the NSA. Snowden downloaded more than 1.7 million intelligence files from US agencies. This was the largest number of secrets ever to be stolen in the history of the United States. However, Snowden only shared between 50,000 and 200,000 documents with reporters. Although this number makes up only a small fracture of the documents that were captured, the contents of the documents were enough to create worldwide awareness of how privacy of individuals and even diplomats and politicians could be invaded in the name of protection against terrorism. The leaked documents contained important information about covert global surveillance systems and databases run by the NSA and the United Kingdom's Government Communication Headquarters(GCHQ) such as PRISM, XKeyScore and Tempora. The real controversial aspect of these leakages was that the NSA was collecting data and information on foreign state officials, and billions of telephone records a day of mobile users all around the world. US officials condemned Snowden's actions, claiming that he endangered the security of Americans by revealing state secrets. However, the fact that he was brave enough to share how the NSA spies on foreign countries, world leaders and the general population made him a hero in the eyes of many.
As a result of countless stories based on Snowden's leaked documents, it became evident that the NSA has spied on many prominent foreign governments and their leaders. The German newsweekly Der Spiegel disclosed that the NSA targeted at least 122 world leaders. Specific targets of the intelligence agency over the years included German chancellor Angela Merkel, the French Foreign Ministry, and the leaders at the 2010 G8 and G20 summits in Toronto. The NSA utilized its corporate partnerships with major US companies such as AT&T, Microsoft, Google and Verizon in order to intercept the communications of the targeted foreign governments and leaders. Since the NSA surveillance scandal erupted, the tension between the US and EU countries has been on the rise. Although there have been negotiations between EU ambassadors and the US on global surveillance programs and data privacy, the issue continues to damage US foreign relations.²

1. Introduction

In my paper, I will first focus on the technical aspects of surveillance programs, and analyze surveillance programs and techniques that the NSA uses in order to spy on Internet users. I will present two of the most controversial NSA surveillance programs that were introduced by Snowden: PRISM, and XKeyScore. The disclosures of these two programs compel us to analyze the legality of practices carried out by intelligence services. Thus I will focus on the policy aspects of NSA surveillance in order to better understand how the surveillance scandal affects the relationship between the US and EU. I will thus analyze the compatibility of surveillance and EU law. Finally, I will describe the tensions between the US and its European allies, mainly Germany and France, and the efforts in order to protect European data privacy and rebuild trust between the US and Europeans.

2. PRISM
PRISM is a program which allows the NSA to capture e-mail and other private communications from Internet companies. It allows the streamlined, electronic capture of communications to, from, and between Americans. Section 1881a of the FISA Amendments Act of 2008 gave the president the extensive authority to conduct electronic surveillance without warrant and justifies the legitimacy of PRISM. Under the program, if the attorney general and the director of national intelligence confirm that the aim of the monitoring is to collect foreign intelligence about any non-American individual or entity that is not in the United States, the Foreign Intelligence Surveillance court can order Internet companies to provide access to the international communications of Americans. This court does not take any initiative in order to minimize the intrusion. Hence, the government can issue top-secret rulings to giants such as Microsoft and Google to turn over e-mails, calls, video and voice chats, social networking information, and voice over IP calls such as Skype records. The Washington Post reported that PRISM’s confidence in a target’s foreignness is measured at 51%, which means that there is a 49% chance that the communications intercepted are protected communications of Americans. The 4th Amendment states that the government has to demonstrate probable cause before carrying out invasive surveillance. The Constitution thus does not approve of the government’s seizing of revealing data on the communications of millions of innocent Americans. This means that the NSA has intentionally captured information illegally, despite the support of the FISA Amendments Act.³

The PRISM program costs around 20 million dollars per year. The program collects a wide range of data from 9 large Internet companies. These companies are Microsoft, Google, Yahoo, Facebook, PalTalk, Youtube, Skype, AOL, and Apple. Although the content of the data received by the NSA varies depending on the providing company, the surveillance agency
generally receives e-mail, chat (video or voice), videos, photos, stored data, VoIP, file transfers, video conferencing, video conferencing, and notifications of target activity such as logins, and online social networking details. The first company to join the program was Microsoft and the last company to join it was Apple. Microsoft joined PRISM on September 11th 2007, and Apple joined the program in October 2012. All of the remaining 7 companies joined the PRISM in less than 5 years.

Below is a slide which explains how the tasking process works for the PRISM system when an NSA analyst seeks to add a new target. The supervisor automatically receives the request of the analyst and examines the search terms, or “selectors”, in order to confirm that there is reasonable belief (51% confidence) that the specific foreign national target is in fact overseas.
Notice that the FBI consults its own databases via ECSU to confirm that the selectors do not match known Americans for stored communications. The FBI is able to use government equipment on a private company that participates to the PRISM program such as Google, without further review to the NSA.  

After the information is collected, it is processed by extensive systems that can handle text, voice, video and digital network information. Below is a slide that shows this dataflow.

As we can see, the FBI’s interception unit passes the information to one or more customers at the NSA, CIA or FBI. After the information is passed, PRINTAURA automates the traffic flow, and SCISSORS and Protocol Exploitation sort the data types. After the sorting, NUCLEON analyzes voice content, PINWALE analyzes video content, MAINWAY analyzes call records, and
MARINA analyzes Internet records. FALLOUT and CONVEYANCE are the final layers to filter out the necessary information and reduce the intake of information.  

PRISM is also able to conduct real-time surveillance by assigning each target a case notation. Below is a slide which shows an example of a case notation that PRISM uses in order to analyze real-time information of a specific target.

![PRISM Case Notations](image)

As we can see, the PRISM provider of this target is Yahoo specified by “P2”. The following “E” means that the target either logged on or sent an e-mail, and the NSA can receive a live notification of this action. The following characters specify the fixed trigraph, the year the search term was endorsed by the supervisor (2012 in this example), and a serial number.  

---

7.  
8.  

---
According to another slide, there were 117,675 targets in PRISM’s counterterrorism database on April 5th 2013 at 12.22 PM GMT. However, the slide does not indicate how many innocent Americans were affected by intrusion of the NSA as it was conducting surveillance of specific targets. Notice that there is a 49% chance per target that the target under surveillance is not a foreign national who is overseas at the time of collection.9

The PRISM program is very effective in collecting much of the world’s communications through certain Internet companies, because much of the communication in the world flows through the US. The US is generally on the cheapest path when a target phone calls or e-mails someone else. Currently, the communications path of packets is determined by not the physical proximity of the sender and receiver, but the price of the path. This means that the US is more likely to be a part of the path between a sender and a receiver. A research conducted by Telegcography Research in 2011 confirms this fact. The research found that the bandwidth capacity between certain regions were the following:

- US & Canada and Latin America & Caribbean: 2,946 Gbps
- US & Canada and Asia & Pacific: 2,721 Gbps
- US & Canada and Europe: 4,972 Gbps
- US & Canada and Africa: 11 Gbps
- Europe and Latin America & Caribbean: 5 Gbps
- Europe and Africa: 343 Gbps
- Europe and Asia & Pacific: 1,345 Gbps
- Africa and Asia & Pacific: 40 Gbps
Notice that 86% of the international bandwidth capacity includes the US and Canada. This result verifies that the US is highly likely to be on the path of packets sent between any sender and receiver.\textsuperscript{10}

3. XKeyScore

XKeyScore, or XKS, is a top secret NSA program which allows analysts to search through very large databases which contain e-mails, online chats, and browsing histories of millions of people all around the world. When he leaked the documents and training documents indicating the existence of XKS in 2013, Edward Snowden claimed that analysts who use the system do not need authorization when they look through individuals’ recorded communications. In a video interview conducted by the Guardian, Snowden stated that he could wiretap anyone as long as he had a personal e-mail, even the president of the United States, using XKS. The training documents leaked state that XKS was the widest-reaching system for extracting intelligence from the web as of 2008. The materials demonstrate that analysts need only a broad justification for their search as they fill in a simple on-screen form. These search requests are not reviewed by a court nor any NSA supervisor before processing. The training materials also claim that XKS, the system with the widest reaching intelligence obtained from networks by the NSA, is also referred as Digital Network Intelligence (DNI) by the agency. The program has supposedly access to nearly everything a user has done while browsing the internet, including the information about the websites visited, searches and the content of e-mails. XKS can also allow analysts to extract the metadata of the users. Like PRISM, XKS allows real-time interception of user activity on the Internet.\textsuperscript{11}

XKS consists of 700 servers that are located at 150 different sites all around the world. These servers are running on Linux, and constantly scanning and intelligence from the Internet
that were accumulated by NSA’s gathering tools. Notice that the tools that the NSA uses for data accumulation are separate from XKS. Below is a training material that was leaked which shows how the NSA gets the data into the XKS servers.

There are 3 sources that are used by the XKS server when the user queries data. F6, or the Special Collection Service, is responsible for placing eavesdropping equipment in important communications hubs. FORNSAT, or the foreign satellite collection, intercepts and collects data from the links of foreign satellites. Finally SSO, or the Special Source Operations division, is responsible for collecting data from all other sources, such as fiber-optic cables.¹²
Below XKS training material illustrates the ability of the analyst to query the XKS databases that are constantly collecting information at any time.

Analysts can query by name, phone number, keywords, IP addresses, even the language in which the internet activity happened or the type of the browser. The slides warn the analysts, claiming that querying the full database could be a difficult and slow process. They are thus advised to use the metadata which are also part of the databases in order to have a narrower search. The plug-ins can express various fields of information, including “every e-mail address seen in a session..."
XKS can search within bodies of e-mails, webpages, and documents including the “To, From, CC, BCC lines” and ‘Contact Us’ pages on various websites. The analyst can enter the e-mail address of the individual into a simple online search form, a simple justification for the search, and the time period for which the e-mails are requested in order to complete the query of the database. Below is a slide that is an illustration of a sample query in order to find a target in Africa.

The analyst can then select a specific e-mail that was returned after the query that he or she wants to look at by using the reading software of the NSA. Below is an illustration that demonstrates a sample e-mail which was opened using the NSA software.
One training document which was created in 2010 clarifies that analysts can commence surveillance on any individual by clicking a few simple pull-down menus that were created to provide both targeting and legal justifications that the analyst can choose from. Once the options on the pull-down menu are selected, the analyst can begin the surveillance on the individual without further approval. Below is a leaked material documenting a sample pull-down menu.
As I stated above, XKS allows analysts to monitor other types of online activities including social media activities. The analyst uses DNI Presenter, which is a tool that was designed to read the content of Facebook chats and messages. After the results are returned by the query, the analyst can monitor activity on Facebook by entering the user name and date range in a search screen, as can be seen below.
Furthermore, analysts can search for browsing activities including targets’ search terms and or viewed websites. Below is a slide which demonstrates a query using the search term “Musharraf” and BBC as the website viewed.
XKS also allows analysts to extract the IP addresses of all the individuals that visit a specified website. Below is a query searching for everyone in Sweden who visited al-hisbah.com.

1. If you know the particular website the target visits. For this example, I’m looking for everyone in Sweden that visits a particular extremist web forum.
An NSA report in 2007 estimated that there were 850 billion call events and around 150 billion internet records stored in the NSA databases. The report also claimed that between 1 and 2 billion entries were added to the database daily. William Binney, a former NSA mathematician, stated that the number of transactions assembled of calls and e-mails was in the order of 20 trillion transactions total. In 2010, Washington Post reported that the NSA was intercepting 1.7 billion e-mails and calls, proving that the rate of collection hadn’t slowed down since 2007. XKS is collecting so much data that it can only be stored for a limited period of time. Regular content stays in the system between 3 and 5 days before being replaced with more recent information. Unlike regular content, metadata can be stored up to 30 days. In order to solve this problem, the NSA is utilizing a multi-tiered system, which allows the storage of more interesting and important content for longer periods of time. For example Pinwale can store its material for up to 5 years. Below is a training material which shows the different tiers of the system.¹⁷
4. The compatibility of surveillance programs with EU law

In the US, an individual’s data belongs to the service or company that assembled the data. However, EU Charter and the Treaty state that the individual is the sole owner of his or her data. Hence, under European law, certain surveillance activities of the NSA can constitute data theft and illegal access to private property. Although the ratification of the EU-US Mutual Legal Assistance Agreement allows for collaboration in counter-terrorism activities, there is evidence which suggests that the collaborating surveillance agencies have ignored the lawful search mechanisms in favor of covert actions that go beyond counter-terrorism concerns. The fact that the NSA and other agencies are collecting massive amounts of user data for strategic surveillance may put democracy at risk. I will first analyze how surveillance affects the democratic rule of law. Then, I will question whose interests these surveillance agencies protect if they compromise their own citizens’ liberties.19

4.1 Surveillance against democratic rule of law

Democratic rule of law declares that the legal system of a state has to be democratic and there must be mechanisms of accountability. Under this principle, there has to be an independent judiciary that oversees the inner workings of the system. Today, there are serious debates about whether EU surveillance activities are compatible with the standards of democratic rule of law. These standards are essential for the constitutions of EU member countries and fundamental rights of any citizen of a democratic state. EU constitutional systems believe in judicial supervision and control of government surveillance activities. They do not accept programs such as PRISM as part of the democratic understanding of national security. These constitutional
traditions provide protection against abuse of power and care deeply about the principle of the separation of powers. Hence, they do not favor the idea of an all-powerful surveillance system at the core of national security practices. 20

The main standards for the lawfulness of government surveillance can be found in Article 8 of ECHR (European Convention of Human Rights). In its exemplary judgment of the case of Weber and Saravia v. Germany 2006, the Strasbourg Court dismissed the accusations of applicants under Article 8 ECHR that the German Federal Intelligence Service abused its powers by strategic monitoring and use of personal data obtained. The Weber case became the main set of criteria for determining whether government surveillance activities and interference of communications is compatible with democratic rule of law. Minimum safeguards of surveillance included a definition of categories that would allow the state to monitor people’s telephones, a limit on the duration of these monitoring activities, the procedure that must be followed for storing the acquired data, sharing data with other parties, and cases in which the data must be erased from records. Following these guidelines, the European Court of Human Rights found UK’s communications interception to be in violation of Article 8 in the case Liberty v UK. 21

The main target of the democratic rule of law and Article 8 of ECHR is to define boundaries of intelligence actions and “to protect the individual against arbitrary interference by the public authorities”. This interference must be in accordance with the law. As a result of these principles, in the case if El-Masri v Macedonia, the Strasbourg Court stated that even though allegations of terrorist offences create special problems for nations, this does not mean that the authorities can arrest suspects or detain them in police custody without the effective control and supervision of the domestic courts. This means that the democratic rule of law is against
detaining a suspect without supervision of a state court even if surveillance agencies believe that the suspect is connected to terrorist offenses.  

Another important document that oversees surveillance activities is the EU Charter of Fundamental Rights. The EU Charter has had the same legal importance as the Treaties since its entry into force of the Lisbon Treaty. According to this document, the national authorities within EU can apply national standards of law as long as the unity and effectiveness of European law is not undermined. The EU Charter is becoming a constituent of “the national constitutional traditions” of European nations. As Viviene Reding, the vice president of the European Commission stated, the Charter supports the view that states should not have the right to conduct unlimited secret surveillance. The Charter states that an individual should have the right of data protection irrespective of his or her nationality. The document thus believes that Europeans or non-Europeans can go to Court if they believe that their right of privacy is being infringed; and the mere fact that a decision affects the security of a state does not make EU law inapplicable. In the case ZZ v. Secretary of the State of Home Department C-300/11, of 4 June 2013, based on the EU Charter, the Court concluded that the freezing of assets of ZZ, a dual French and Algerian citizen, was in breach of the individual’s fundamental rights and was to be annulled.

4.2 Surveillance compromises citizens’ liberties

The surveillance activities of the US endanger the EU principle of sincere cooperation, because they put at risk the realization of important EU objectives, such as a common foreign and security policy between states. Even when surveillance targets a particular state, the nature of these activities affect the security of the Union as a whole. Surveillance also endangers the use of legally established channels between EU and the US. European Parliament LIBE Committee
stated in June 2013 that “if you don’t go through the MLA and directly to companies asking data of EU citizens, that is a violation of international law”.  

Large-scale NSA surveillance programs deprive EU citizens of their ownership of private data. However, another important aspect of these programs is that nationals of some EU member states are affected disproportionately compared to the nationals of the UK, the closest ally of the US. Privacy International argued that the Tempora Program (a surveillance program of the British GCHQ that was supported by the NSA) discriminates against non-UK nationals and EU citizens while collecting users’ personal data. Privacy International stated that:

“The Tempora operation has a disparate adverse impact on EU citizens who are not nationals of the UK. This is because a certification under section 8(4) of RIPA 2000 can only be granted in respect of the interception of external communications, which are more likely to be made by non-UK citizens. Union citizens who are not UK citizens are far more likely to have their communications intercepted, searched and retained.”

The Strasbourg Court also reported in 2013 that the disparities between foreign and domestic information collecting programs lead to a lack of legal protection when personal data and information is shared between states. We can thus conclude that NSA programs such as PRISM and XKeyScore, which make a clear distinction between foreign and domestic interception, create a hole in protection and accountability in the EU.

4.3 Conclusions

The collaboration between European intelligence agencies and the NSA has been kept secret and is illegitimate according to certain agreements in place. The surveillance activities of these agencies have also created spying suspicions against European companies in favor of US
ones. The secret collaboration of British agencies and the NSA also violates the solidarity principle between EU members in favor of another alliance, as the British are sharing with the NSA data of other European citizens without the awareness of their own state. 28

NSA surveillance programs PRISM and XKS are warrantless and may imply forms of data mining. They are not only programs to detect terrorist threats. The involvement of predictive analytics and data mining while conducting large-scale surveillance raises questions whether there is an asymmetry of sovereignties in diplomatic alliances and whether these measures are putting democracy at risk. An important legal issue that has to be addressed is to prevent the use of predictive analytics and data mining while conducting surveillance. 29

The most important challenge moving forward is to reconsider US-EU relationships in the field of surveillance. The US dominates the diplomacy of surveillance, which disturbs the cohesion of the EU in the field. The US surveillance agencies have established three different layers of cooperation since cold war:

- The Five Eyes Network, which was created in 1946, includes the US, the UK, Canada, Australia and New Zealand. This is a multilateral agreement for cooperation in signals intelligence. Under this agreement, the US shares parts of its collected information with the member states.

- A number of EU countries with whom the US participates in ad hoc collaboration but also against whom conducts offensive espionage. These countries include France, Germany, Italy, Belgium and Switzerland. Note that at certain times, the espionage activities cause serious tensions between the nations. In 2009, France and the US accused each other of illicit economic espionage.

- Other countries all around the world the US considers simply as targets.
These layers demonstrate that EU institutions can never become strong partners of the US agencies in the field of surveillance. EU states also have different attitudes towards collaborating with agencies such as the NSA. Certain EU member states’ national laws do not allow collaboration between their intelligence services and the US in terms of information sharing. Hence, large-scale surveillance activities present asymmetries at the international level. 

5. The tension between the US and its European allies after the surveillance scandal

5.1 Germany-US relations

After revelations about the NSA’s controversial international spying operations, the relationships between the US and its EU member allies have debilitated. In this section, I will present how Germany and France, two of the most prominent European countries, reacted to the surveillance scandal after Snowden revealed top secret NSA documents in 2013.

According to SPIEGEL research, the NSA tapped German chancellor Angela Merkel’s cellphone for more than a decade, and used the American embassy in Berlin as a listening station. The research revealed that the NSA is able to store most of the cellphone communication in the German government quarter. The leaked documents unveil that the NSA was able to tap into Merkel’s cellphone that she used to lead her party, the center-right Christian Democratic Union (CDU), and carry out most of the government business. After these revelations in 2013, German Foreign Minister Guido Westerwelle summoned the US ambassador of Germany, John Emerson, to discuss the matters of surveillance at the Foreign Ministry. Note that Germany reserves this type of gesture when it is displeased with the actions of rogue states, not the US. The NSA scandal also caused the CDU to question the trans-Atlantic free trade agreement. The authorities stated that unless the US government didn’t clarify the situation and take the
necessary steps to eliminate the surveillance of government officials, the talks over the agreement would be put on hold.\textsuperscript{31}

But how exactly did the NSA manage to infiltrate the German government quarters? A top secret NSA document from 2010 indicates that the most active NSA unit in the country was called the “Special Collection Service” (SCS). This unit was operational mainly in Berlin and Frankfurt. Both of the German bases of SCS was equipped with the most advanced surveillance tools and highly skilled active personnel. Although wiretapping from embassies is unauthorized in Germany, this was exactly the task of the SCS. Snowden’s leaked documents indicate that it was this elite NSA unit that targeted the cellphone of German Chancellor Angela Merkel. One particular document that appears to come from the NSA database contains the cellphone number of Merkel that she uses to communicate with CDU members and ministers mostly over text messages. The number of Merkel appears as the “Selector Value” and the “Subscriber” is identified as “GE Chancellor Merkel” in the document. Another leaked document claims that the NSA first tapped into Merkel’s phone in 2002, when she was only party chair of the CDU. However, according to the “National Intelligence Priorities Framework” of US intelligence agencies, it appears that Chancellor Merkel should not have been monitored. This means that Merkel could have been targeted by the NSA without the US president’s knowledge.\textsuperscript{32}

After the revelations about the surveillance activities of the US, Christoph Heusgen, Merkel’s foreign policy adviser, made an initial call to Obama to inform him that Merkel intended to make some serious complaints. He also stated that she planned to go public with these complaints. On October 23 2013, Merkel spoke with Obama from her secure landline in English. Obama stated that he had not known of the illicit surveillance of her and other German diplomats, and conveyed his regrets and apologized. On the same day, the German
administration went public with the matter. Merkel’s spokesman Steffen Seibert described the spying of the chancellor’s cellphone as a “grave breach of trust”, a phrase of highest intensity among diplomats of ally countries. The chancellor’s office also started considering a possible failure of the trans-Atlantic free trade agreement between the two nations. Bavarian Economy Minister Ilse Aigner stated that: “We should put the negotiations for a free trade agreement with the US on ice until the accusations against the NSA have been clarified”. Merkel’s intelligence coordinator Gunter Heiss demanded that the Americans should agree to sign a contract excluding mutual surveillance. Although Germans were eager to make a non-spying pact with the US, Americans were not inclined to seriously engage with the idea.33

5.2 France-US relations

A top secret NSA document from 2010 unveiled that the agency was notably interested in the computer network of French diplomats. The document claims that the NSA managed to tap into a number of government web addresses, including “diplomatie.gouv.fr”. A list from September 2010 indicates that French diplomatic offices in Washington and at the UN in New York were also among the NSA’s targets with codenames “Wabash” and “Blackfoot” respectively. The agencies’ technicians installed bugs in both targets. A priority list of the NSA showed that the agency was particularly interested in French foreign policy objectives, weapons trade, and economic stability. After the revelations, the French President Francois Hollande threatened the US of suspending the process for the trans-Atlantic free trade agreement until the US ensured the French that they would halt their spying activities. Hollande stated that there could not be negotiations nor transactions between the two countries until the US gave these guarantees.34
On top of these reactions, the French Foreign Ministry summoned the American ambassador Charles H. Rivkin on October 21 2013. The French were disturbed after they found out that the NSA had recorded over 70 million digital communications in France in a single month from December 10 2012 to January 8 2013. The French officials described the spying activities as “totally unacceptable” and demanded that they cease.\textsuperscript{35}

\textbf{5.3 Efforts to protect European data privacy}

On October 21 2013, a European Parliament committee approved new data protection rules which would increase online privacy and prohibit most data transfers to the authorities of other countries. The goal of this new set of rules is to create a stronger data protection law for the 500 million EU citizens by replacing an outdated collection of national rules. The new legislation aimed at enabling users to ask companies to erase their personal data, limiting user profiling, necessitating companies to describe the use of personal data to customers, and requiring all companies to seek prior consent. The legislation also introduced stiff fines for violations, up to 5\% of a company’s annual turnover.\textsuperscript{36}

Another proposal to protect EU members from the US spying activities was introduced by Germany and France on February 16 2014. The two prominent EU member countries proposed the creation of “safe communication networks” in the EU. Merkel stated that: “We will speak to France about this and about all things regarding what kind of European providers we have who can offer security for our citizens: So that we don’t even have to go with our emails and other information over the Atlantic, but that we can set up safe communication networks within Europe.”. In order to achieve this goal, German communications provider Deutsche Telekom had been doing research on an “Internetz”. The company’s view is that by using European-made software and hardware, European citizens’ data are not exposed to US
surveillance systems. Its main goal is to create a new network that covers 26 countries in the Schengen zone, the passport-free travel area, which keeps the UK out.37

6. Conclusion

The NSA, the most prominent intelligence agency in the US, conducts many global surveillance programs. In my paper, I first analyzed two of the most important surveillance programs of the agency, PRISM and XKeyScore. PRISM is a program which allows the NSA to capture e-mail and other private communications from Internet companies. It allows the streamlined, electronic capture of communications to, from, and between Internet users. XKeyScore is a top secret NSA program which allows analysts to search through very large databases that contain e-mails, online chats, and browsing histories of millions of people all around the world. After the technical analysis of these two important NSA programs, I looked at the European policy issues caused by US surveillance. EU Charter and the Treaty state that the individual is the sole owner of his or her data. Hence, certain surveillance activities of the NSA constitute data theft and illegal access to private property under European law. NSA surveillance compromises European citizens’ liberties. After analyzing the technical and policy aspects of NSA surveillance, I examined the debilitating relationships between the US and its EU member allies, particularly Germany and France. Finally, I investigated the efforts of EU to protect its data privacy. To combat NSA surveillance, in 2013, a European Parliament committee approved new data protection rules which would increase online privacy and prohibit most data transfers to the authorities of other countries. Another proposal to protect EU members from US spying activities was introduced by Germany and France on February 16 2014. The two EU member countries proposed the creation of “safe communication networks” in the EU to ensure data privacy.
37 "Germany and France to Hold Talks on Protecting EU Data from NSA." Germany and France to Hold Talks on Protecting EU Data from NSA. Web. 1 Apr. 2015. <https://euobserver.com/justice/123158>.