THE NSA AND EDWARD SNOWDEN: SURVEILLANCE IN THE 21ST CENTURY

Joseph Verble
Saint Xavier University
3700 W. 103rd St.
Chicago IL, 60655
verble@sxu.edu

ABSTRACT
This paper examines the case and background of Edward Snowden, the history and purpose of the National Security Agency (NSA), legality and American public opinion and its aftermath.

Categories and Subject Descriptors
Social and Professional Topics – Professional Topics – Computing profession – Codes of ethics; Social and Professional Topics – Computing/technology policy – Surveillance--Government surveillance

General Terms
Security, Human Factors, Legal Aspects.

Keywords
Edward Snowden, NSA, Security, Intelligence, Government.

1. INTRODUCTION
In May 2013, Edward Snowden stole approximately 1.7 million documents of secret data from the NSA and delivered them to a slew of news agencies in order to expose many secret programs conducted against its own citizens, foreign leaders and various targets abroad. Many of these files detail domestic spying programs held by the NSA that collects data from average American citizens through various online sources. This incident has been reported worldwide, with new reports and details making headlines every other day.

Since the story was first reported to *The Guardian*, a famed British newspaper, Snowden has been held up in Hong Kong, only to have his passport revoked and eventually relocating to Russia, who granted him a one-year asylum and later extended his stay. Presently, the US Government struggles to handle how properly to handle the situation with Edward Snowden and the NSA. Several Congressmen offered varying opinions on the fates of both Snowden and the intelligence agencies. On January 17th, 20014, President Barack Obama gave a speech detailing the need for NSA reforms while touting the necessity of the program. Changes are in the air as details spew forth about what has been taking place behind closed doors at the NSA.

This report has been made to analyze both Edward Snowden's motives, the future of the NSA and its programs. Both parties deserve a fair amount of scrutiny. It would be a mistake to make this a black-and-white, good-versus-evil discussion; there are things that both parties have done that the public likes and dislikes. It is the NSA using the Internet to spy on U.S. citizens? Will Edward Snowden ever return to the US? Are NSA tactics legal? How did Snowden get away with this? Did Snowden leak these documents to our rival governments in Russia and China?

2. THE HISTORY AND PURPOSE OF THE NSA
The roots of the National Security Agency have existed since World War I as a code and cipher decryption unit. It wasn't until October 1952 when the Armed Forces Security Agency was replaced by the new NSA. The NSA became the management system for the many cryptology agencies throughout the military and researchers into new computer technology and communications infrastructure. The beginning of the NSA was not without problems, as they often butted heads with the Department of Defense (DoD) and the CIA. After World War II, the U.S. Military and Intelligence Agencies were being downsized, but after the start of the Korean War, they reserved course and built up and expanded rapidly. This expansion led to the NSA becoming the intelligence centerpiece that would guide U.S. troops in several international incidents and major conflicts.

The NSA is one of the largest government organizations in staff and in funding. Though the official numbers on staff size are classified, the estimates on it are nearly 40,000 employees and an annual budget about $11 billion ($10.8 billion as of 2013). The U.S. intelligence community employs nearly 107, 000 people, including the CIA and the National Reconnaissance Office.

The NSA has run into a series of missteps over the years earning both public and government scrutiny. One of the first examples led to the Church Committee meetings in the mid 1970's, analyzing the misuse of data by the NSA and the subsequent passing of Foreign Intelligence Surveillance Act. In the early 2000's, the horrifically expensive and monumental disaster known as the Trailblazer Project, an information gathering program, was canceled and cost taxpayers over $1.2 billion. The most controversial of its problems stemmed from their post-9/11 warrantless wiretapping programs and recently its numerous domestic spying programs.

The NSA first had major domestic spying issues highlighted during the Church Committee meetings in 1975 when then Senator Frank Church (D-Idaho) headed the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. The Committee discovered many issues such as plans to assassinate several foreign leaders, including Fidel Castro during the Bay of Pigs invasion in 1962, The Committee also found a program called HTLINGUAL in which the FBI and CIA was obtaining, opening and photographing nearly 220,000 pieces of mail. The program was implemented to gain foreign intelligence, but was also used on domestic targets like the anti-Vietnam War protesters and civil rights activists of the era, including Martin Luther King Jr.

Many new polices were implemented short of dismantling the CIA and NSA, but both agencies were spared. The important piece of legislation was the Foreign Intelligence Surveillance Act of 1978 (FISA). The purpose of FISA was to limit the amount of domestic spying in the US. FISA was amended in 2008 to include electronic surveillance, and in its current form prohibits targeting US citizens, targeting foreign citizens in order to get to a US citizen and communication coming from abroad to US citizens. Those same amendments also allow for "telecom companies blanket immunity from prosecution for participating in domestic surveillance" (McAllister). Strict foreign targets can still be spied on under these rules. After the terrorist attacks of September 11th, 2001, the NSA was granted more powers in order to combat terrorism. The Bush Administration covertly authorized the NSA to spy on American citizens and others without warrants from the FISA court. The Administration ended

the unwarranted surveillance program in early 2007 and returned to prior regulations requiring warrants.

The Obama Administration "continues to deploy many of the national security tools he inherited from his predecessor." (Baker) In 2012, Congress extended many of the provisions in the FISA Amendments Act of 2012, notably, it "specifically authorizes intelligence agencies to monitor the phone, email, and other communications of US citizens for up to a week without obtaining a warrant, provided one of the parties to the communications is outside the US" (McAllister). The Obama White House argued that this extension,

> …allows the Intelligence Community to collect vital foreign intelligence information about international terrorists and other important targets overseas, while providing protection for the civil liberties and privacy of Americans. Intelligence collection under Title VII [of the FISA Amendments of 2008] has produced and continues to produce significant information that is vital to defend the Nation against international terrorism and other threats.
>
> (Executive Office of the President).

Today, the NSA remains an ever-expanding government agency, supported by administrations on either side of the aisle. Even while scrutinized in the public's eye or in the world of politics, the size and scope of the NSA and their programs has not taken a significant hit. With the rapid growth of technology and its reach around the globe, it doesn't seem like the NSA will slow down any time soon.

3. THE CASE OF EDWARD SNOWDEN

> "I have no intention of hiding who I am because I know I have done nothing wrong,"
>
> --Edward Snowden in an interview with Glenn Greenwald, 2013

Sunday, June 9th 2013: *The Guardian*, the famed British newspaper revealed the source of the biggest US intelligence leak in history. The source was Edward Snowden, a 29-year-old employee of defense contractor Booz Allen Hamilton, hired by the National Security Agency (NSA). The week prior, *the Guardian* released the first few details of the NSA leaks. Starting on June 5th, *The Guardian* revealed a document indicating that the US government made Verizon turn over millions of phone records. On June 6th, they published a story about the NSA's secret program, PRISM. This program supposedly allowed direct access to data from companies such as Apple, Google, Facebook and more. These high -profile companies denied that the NSA set up back doors to their systems. The next day, *The Guardian* revealed in addendum to the PRISM story that the Government Communication Headquarters (GCHQ), the UK equivalent to the NSA, had access to the PRISM program and thus access to data from these tech giants as well.

Edward Joseph Snowden was born June 21st, 1983 in Elizabeth City, North Carolina. He never completed high school, but received his GED. He joined the Army at age 20 and was discharged after breaking both of his legs. His first job was as a security guard at an NSA facility located at the University of Maryland; he then was hired by Central Intelligence Agency (CIA) working in IT security. At age 24, he was stationed in Geneva, Switzerland working with the CIA for three years until taking a job as a private contractor working for Dell, and Booz Allen Hamilton, an American management- consulting firm that specializes in technology and security. Snowden was located in Hawaii, working at the NSA's Kunia Regional SIGINT (Signals Intelligence) Operations center. This is where Snowden stole the documents, before he took off to Hong Kong in late May 2013.

Snowden claimed that his time with the CIA "really disillusioned me about how my government functions and what its impact is in the world" (Poitras, Greenwald and MacAskill). He is afraid that the NSA "[is] intent on making every conversation and every form of behavior in the world known to them"(Poitras, Greenwald and MacAskill). Not seeking personal attention, Snowden exclaims "I really want the focus to be on these documents and the debate which I hope this will trigger among citizens around the globe about what kind of world we want to live in." Adding, "My sole motive is to inform the public as to that which is done in their name and that which is done against them" (Poitras, Greenwald and MacAskill).

Snowden managed to pull of this theft with some deception of fellow employees. According to an internal memo released by the NSA on February 10th, 2014,

> *n 18 June 2013, the NSA civilian admitted to FBI Special Agents that he allowed Mr. Snowden to use his (the NSA civilian's) Public Key Infrastructure (PKI) certificate to gain access to classified information on NSANet; access that he knew had been denied to Mr. Snowden. Further, at Mr. Snowden's request, the civilian entered his PKI password at Mr. Snowden's computer terminal. Unbeknownst to the civilian, Mr. Snowden was able to capture the password, allowing him even greater access to classified information. The civilian was not aware that Mr. Snowden intended to unlawfully disclose classified information. However, by sharing his PKI certificate, he failed to comply with security obligations.* (Bauman)

How Snowden managed to download numerous files quickly became an important question to investigators that determined that he used web crawler software to catalog and organize all the information. *The New York Times* reports "A web crawler, also called a spider, automatically moves from website to website, following links embedded in each document, and can be programmed to copy everything in its path" (Sanger and Schmitt). The documents were then stored on a simple USB flash drive, which are mostly banned inside the NSA.

After extracting the files, Snowden left from Hawaii to come to Hong Kong, staying at the Mira Hotel. From there, he contacted Glenn Greenwald of The Guardian, simply saying, "I am a senior member of the intelligence community." while sending a sample of documents to prove of his position (Harding). Greenwald and American journalist Laura Poitras flew to Hong Kong to meet Snowden face-to-face. Snowden proceeded to hand over countless classified documents, resulting in the biggest leak in the history of the United States.

After the reports by The Guardian were released, the US government was quick to defend the NSA and its practices. President Obama defended the NSA's programs, claiming that "lives have been saved" and also that phone and Internet surveillance conducted by the NSA is "narrow" (Bruce). Meanwhile, numerous politicians and pundits have come out to either praise or denounce the efforts from both the NSA and Edward Snowden.

Snowden decided to leave Hong Kong after "he learned he could spend years in prison without access to a computer during the process to determine his asylum in Hong Kong or extradition to the U.S." (Kelley). After his decision to leave, he mulled several different possible spots to relocate. Snowden ended up in Russia, which further infuriated his detractors. Russia granted Snowden asylum for one year and as of late January 2014, Russian officials "opened the door to Snowden staying there indefinitely" (Volz).

Snowden has occasionally made online appearances and interviews, such as the SXSW conference on March 10th, speaking about internet freedom and other topics. This has made him a sort of celebrity and a much sought after figure. The young man from Elizabeth City, North Carolina has turned into a hotly debated topic: is he a hero, or a traitor? Should he be granted amnesty or spend the rest of his life in prison? It might take months, years or decades before we see the real impact of this story, and his fate.

4. CHARGES AGAINST SNOWDEN AND THE LEGALITY OF THE NSA'S TACTICS

The US District Court for the Eastern District of Virginia filed the charges against Edward Snowden on June 14th 2013. The district has "a long track record of prosecuting cases with national security implications" (Finn and Horwitz). The United States officially charged Edward Snowden with Theft of Government Property (18 U.S.C 641), Unauthorized Communication of National Defense Information (18 U.S.C. 793(d)), and Willful Communication of Classified Communications Intelligence Information to an Unauthorized Person (18 U.S.C. 798 (a)(3)) (U.S. vs. Edward J. Snowden). According to *the Washington Post*, "[t]he Obama administration has shown a particular propensity to go after leakers and has launched more investigations than any previous administration. This White House is responsible for bringing six of the nine total indictments ever brought under the 1917 Espionage Act. Snowden will be the seventh individual when he is formally indicted" (Finn and Horwitz).

The program PRISM is deemed perfectly legal according the federal government and they also claim it adheres to the standards set by FISA. If the retrieval of data happens to be incidental and unintentional, then it is technically legal.

Prior to the 2008 FISA amendments, the NSA or other intelligence agency needed to request permission from the Foreign Intelligence Surveillance Court (FISC) to conduct such spying. FISC rarely denies any requests and has only denied two requests out of nearly 9,000 from 2008 to 2013. It may not seem like the toughest oversight, but in adhering to the court system, airtight cases need to be made in order to pursue any action.

The Fourth Amendment clearly states,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

If anything, lawmakers need to rework FISA and NSA protocol to adhere to the Constitution and protect US citizens from this overreach of power.

After 9/11, many security measures were put into place in order to protect citizens, but at the same time, increase power of government agencies. The Department of Homeland Security (DHS) was formed as a national security organization as well as the Transportation Security Administration (TSA) which began major overhauls to airport security. With the terror attacks still fresh, some didn't mind the overbearing security measures in place, saying that it kept people safe, despite being an inconvenience to travelers. The mindset was people had to sacrifice a little freedom for the sake of safety and if you weren't guilty of anything, then you have nothing to hide. Due to the murky laws, loopholes and executive orders, these agencies can easily skate by with limited oversight. With the rapid growth of technology and the ripe environment of the post-9/11 landscape, the NSA and intelligence community could only get bigger and bigger.

5. THE PUBLIC EYE: AMERICAN'S PERCEPTIONS ON SNOWDEN, THE NSA AND DOMESTIC SPYING

Shortly after the Snowden leak was reported June 5, 2013, numerous polls were conducted to tap into the public's perceptions. Rasmussen Reports found that the majority of American voters opposed the federal government secretly collecting phone records. Fifty-nine percent opposed, while 26 percent approved and 15 percent were undecided about the data collection (Rasmussen Reports).

A Gallup poll released around the same time showed similar results as the Rasmussen poll. Fifty-three percent of American adults disapproved of the federal governments collecting phone data while 37 percent approved and ten percent registered no opinion. Gallup also asked a question during the same poll to find how concerned Americans were about the possible violation of their right to privacy. Thirty-five percent were very concerned, 22 percent somewhat concerned, 21 percent not too concerned and 21 percent were not concerned at all and lastly, one percent had no opinion (Newport).

The most telling information is a statement by Gallup that "[s]ixty-four percent of Americans are following news about this issue very or somewhat closely, which is slightly above average for all news stories tested by Gallup over the past two decades" (Newport).

The Pew Research Center's poll differed from Rasmussen and Gallup in which 56% of Americans said that "the National Security Agency's (NSA) program tracking the telephone records of millions of Americans is an acceptable way for the government to investigate terrorism" (Pew Research Center).

Forty-one percent of Americans disapproved of the NSA's tactics, while two percent had no opinion. A disappointing find by Pew was the lack of young adults following these stories. Only 12 percent of young adults from 18 to 29 years of age had been following the news stories involving the NSA and domestic spying very closely. More disappointing in all three aforementioned polls is the partisan shift when it comes to different administrations.

In the Pew Research poll conducted in January 2006 during the second term of the Bush Administration, those who identify as Republicans were highly in favor of the work conducted by the NSA (75 percent) and inversely Democrats highly disapproved (61 percent). Fast forward to June 2013 in the second term of the Obama Administration, Republicans slightly disapproved of the NSA programs 52 percent; while Democrats found the NSA's work highly acceptable at 64 percent. The trend is that the opinions of Americans are too often shaped by the political party that holds the White House.

In both the Bush and Obama Administrations, the NSA has been infringing upon the privacy of Americans, and yet with the Edward Snowden case, public opinion is still a toss-up. Since

NSA spying is not tangible like identity theft or other cyber-crimes, Americans will still be on the fence about this issue. Politically, NSA spying does not seem to be a major campaign issue for the upcoming 2014 midterm elections. Unless the issue of spying is tied to national security matters, namely the Russia-Ukraine conflict, it may be no more important heading into the 2016 Presidential elections.

More recently, Reason.com conducted a poll at the end of March 2014, asking a myriad of questions about politics and other topics. One such question asked *which of the following do you trust the most with your personal information?* The IRS came in first with 35 percent and the NSA second with 18 percent, which is more than Google at ten percent and Facebook at five percent, which are used by the public daily. However, the next question asked *who do you think is most likely to violate your*

privacy? The NSA came in first at 36 percent (Reason.com).

Pew Research Center/USA Today poll about the fate of Edward Snowden nearly two weeks after the leak story broke. According to the poll, 49 percent of adults believed the leaks served the public interests, where 44 percent believed it harms, yet 54 percent believed that a criminal case should be pursued against Snowden and 38 percent disagreed.

Rasmussen Reports conducted a survey released April 2nd 2014, that stated that twenty-four percent of "voters now supports amnesty for NSA leaker Edward Snowden in exchange for the information he still possesses" (Rasmussen Reports).

It appears that Americans currently have conflicting opinions towards the NSA and domestic spying. After the Snowden incident, the national conversation has started to take place. Until the American public has concrete proof that NSA spying affects them, look for attitudes to remain mixed.

6. THE AFTERMATH

Since the incident was first reported in June of 2013, numerous stories, hearings, rumors and questions have appeared in the news featuring Snowden, the NSA and its programs and the government's policies toward spying and data collection.

On January 17th, 2014, President Barack Obama gave a speech on the NSA and its future. President Obama defended the NSA program, while pointing out that certain reforms were needed. In the same token, he also discredits the notion that this stems from the leaks caused by Edward Snowden.

In March 2014, President Obama called for an end to the NSA's collection of American's phone records, but not other types of data, such as text messages and e-mails. It is possible that future NSA reforms proposed by the Obama Administration will require telecom companies to hold on to more data. According to Reuters, "if the Obama administration pushes through with a proposal to require carriers - instead of the NSA - to collect and store phone metadata, which includes dialed numbers and call lengths but not the content of conversations. Under the administration's proposal, the phone companies would be required to turn over the data to the NSA in response to a court-approved government request" (Selyukh and Hosenball).

On March 11, 2014, Sen. Dianne Feinstein (D-CA), the Chairman of the Senate Intelligence Committee, accused the CIA of hacking into and stealing documents from the computers of those on the committee. Several members of Congress expressed their anger at these allegations brought by Sen. Feinstein. Unfortunately, their outage dwarfs that of most American citizens when it comes to being spied on, and also points out the double standard held by Congress. They can spy on you, but you cannot spy on them.

7. CONCLUSION

The case of Edward Snowden and the NSA is a very deep, nuanced and complex issue. On the surface, some view Snowden as a whistleblower against the machine, or a traitor who betrayed his country. The reality is that Edward Snowden is an intelligent and crafty man, who struggled to deal with the reality of a bloated and flawed government agency. Snowden's methods, however, can be viewed as questionable. He whole-heartedly believes his intentions are good, but the consequences will both harm and help the people and country he loves. The odds are that he will never touch American soil ever again. He has made a big sacrifice in his young life that will be viewed as either valiant or fool-hearted. The perception of Edward Snowden is bound to change over the course of time. What may seem like a victory for those in the United States who are adamant about maintaining their privacy may ultimately turn their back on him when it comes to the safety of our troops and citizens abroad.

There are a few things to be suspicious about when it comes to Edward Snowden. If we are to have our doubts about the overreaching and intrusive federal government, then we ought to equally have doubts about the methods and intentions of Mr. Snowden as well. Snowden didn't just innocently stumble upon a treasure trove of documents detailing surveillance programs. Average citizens would be severely punished for employing the measures he took to obtain these documents. After stealing these documents, he fled to Hong Kong, controlled by the United States' biggest rival China, and then relocated to Russia; the US's other big rival. What would really sour the opinion of the American public is if Snowden leaked info to the Chinese or Russians. In an interview with *The New York Times* in October, 2013 Snowden claimed he took no documents to Russia because "it wouldn't serve the public interest," and that all documents were distributed to journalists in Hong Kong. As *The Guardian* reported,"[Snowden] purposely chose… to give the documents to journalists whose judgment he trusted about what should be public and what should remain concealed" (Poitras, Greenwald and MacAskill).

There is always a potential for bias and misreporting when it comes to the media. Snowden could have tried other avenues and talked to high-ranking officials. The inspector general of the NSA, George Ellard, said that "[Snowden] could have come to me" (Samuelsohn). Ellard claimed that if Snowden was unhappy with an internal investigation that he could have spoken to the House and Senate intelligence committees. Snowden refutes the idea that in-house investigations worked in the NSA.

The public opinion on the NSA is very mixed and it might take more Snowden-like incidents for a further shift in opinion. If it is proven that Russia or China has obtained documents from Snowden himself, then American's opinion on him may dramatically sour. The NSA and other agencies are not perfect. One senior NSA official interviewed in a Washington Post article about an NSA audit from May of 2012 plainly stated, "[w]e're a human-run agency operating in a complex environment with a number of different regulatory regimes, so at times we find ourselves on the wrong side of the line" (Gellman). Every intelligence agency wants to avoid trouble internally as well as externally.

Though the NSA will carry this stigma of this incident in the public eye for some time, they will have to demonstrate transparency as well as explain the intentions and necessity of these programs. Unfortunately, they will get little help from the press explaining to the American public what exactly these programs do and their limitations. The NSA will not simply

disappear; they must become leaner and more efficient and work for the American people within the framework of the Constitution, particularly the Fourth Amendment.

If US citizens are concerned and wish to make personal and online privacy an important issue, then they will have to make it a prime issue on the local, state and federal levels.

People also need to be cautious about what details they share on the internet through social media, transactions and communication. Privacy does not exist when people share every detail about themselves in every facet of life. As much info as the NSA collects so do websites and other businesses. Information is collected in smart phones, laptops and tablets as well as apps and websites for e-mail, online shopping and banking. These businesses, devices and services may collect more data on individuals than the NSA ever will.

8. ACKNOWLEDGMENTS

Special thanks to Dr. Donald Fricker, Dr. James Aman, Erin Laske, Molly Caldera and Prof Florence Appel.

9. REFERENCES

[1] Ackerman, S., Borger, J. 2014. Obama: US must "win back the trust of ordinary citizens" over data. *The Guardian*. <http://www.theguardian.com/world/2014/mar/25/obama-us-nsa-data-collection-trust>.

[2] Ackerman, S.2014. Snowden welcomes Obama's plans for NSA reform as a "turning point." *The Guardian.*<http://www.theguardian.com/world/2014/mar/25/edward-snowden-welcomes-obama-nsa-reforms>.

[3] Agence, F.P. 2014. Encryption business booms as privacy, security concerns rise. *InterAksyon.com.* <http://www.interaksyon.com/business/83721/encryption-business-booms-as-privacy-security-concerns-rise>.

[4] Associated Press. 2014. Edward Snowden's digital maneuvers still stumping U.S. government. CBS News. <http://www.cbsnews.com/news/edward-snowdens-digital-maneuvers-still-stumping-us-government/>.

[5] Baker, P. 2013 Even as Wars Fade, Obama Maintains Bush's Data Mining *New York Times* <http://www.nytimes.com/2013/06/07/us/obamas-strong-embrace-of-divisive-security-tools.html>

[6] Bauman, E. L. 2014. Congressional Notification-Resignation of NSA Employee. msnbcmedia.msn.com. *accessed 12 March 2014.* <http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/nsa-snowden.pdf>.

[7] Benac, N. 2014 Obama recasts chase for Snowden as unexceptional. *My Way. Accessed 28 February 2014.* <http://apnews.myway.com/article/20130628/DA76JNVG1.html>.

[8] Berman, M., et al. 2014.Obama: NSA Reforms Should Give Americans 'Greater Confidence'. *National Journal*. *Accessed 28 February 2014* <http://www.nationaljournal.com/white-house/obama-nsa-reforms-should-give-americans-greater-confidence-20140117>.

[9] "Bill of Rights." n.d. Archives.gov. *accessed 11 April 2014* <http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html>.

[10] Borger, J. 2013. NSA files: why the Guardian in London destroyed hard drives of leaked files. *The Guardian*. *Accessed 1 April 2014.* <http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london>.

[11] Bruce, M. 2013. NSA Dragnet 'Saved Lives,' Obama Says. ABC.com. *Accessed 14 April 2014.* <http://abcnews.go.com/Politics/obama-nsa-dragnet-saved-lives/story?id=19434444>.

[12] Bush, George W. 2008. Executive Order 13470. Executive Order. Washington, D.C.: The White House.

[13] Cesca, B. 2013. Greenwald Stands By His NSA Reporting in Spite of Growing Questions. *The Daily Banter*. *Accessed 1 April 2014*.<http://thedailybanter.com/2013/06/greenwald-sticks-with-his-story-in-spite-of-growing-questions/>.

[14] Christopher, T. 2013. Fulsome Prism Blues: The Guardian Offers 2nd-Worst Clarification Ever On NSA Story. *Mediaite*. *Accessed 1 April 2014.* <http://www.mediaite.com/online/fulsome-prism-blues-the-guardian-offers-2nd-worst-clarification-ever-on-nsa-story/>.

[15] Dilanian, K. 2013. Officials: Edward Snowden took NSA secrets on thumb drive. *Los Angeles Times.com. Accessed14 April 2014.*<http://articles.latimes.com/2013/jun/13/news/la-pn-snowden-nsa-secrets-thumb-drive-20130613>.

[16] Donohue, L.K. 2013. NSA surveillance may be legal — but it's unconstitutional. *Washington Post*. *Accessed 11 April 2014* <http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html>.

[17] Ellsberg, D. 2013. *The Guardian. Accessed 25 January 2014* <http://www.theguardian.com/commentisfree/2013/jun/10/edward-snowden-united-stasi-america>.

[18] Executive Office of the President. 2012. Statement of Administration-H.R. 5949.10 September 2012. White House.gov. *Accessed 13 April 2014.* <http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr5949r_20120910.pdf>.

[19] Finn, P., Horwitz, S. 2013. U.S. charges Snowden with espionage. *Washington Post. Accessed 28 February 2014* <http://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_print.html>.

[20] Foust, J. 2013. NSA Rule Violations Matter, but Aren't Severe. *Joshua Foust*. *Accessed 1 April 2014* <http://joshuafoust.com/nsa-rule-violations-matter-but-arent-severe/>.

[21] Gellman, B. 2013. NSA broke privacy rules thousands of times per year, audit finds. *Washington Post. Accessed 1 April 2014* <http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html>.

[22] Gertz, B. 2013. Breach, U.S. officials: China, Russia gained access to Snowden's secrets. *The Washington Free Beacon*. *Accessed 28 February 2014* <http://freebeacon.com/breach/>.

[23] Gidda, M. 2013. Edward Snowden and the NSA files – timeline. *The Guardian. Accessed 30 Match 2014*

<http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>.

[24] Gorman, S. 2006. Little-known contractor has close ties with staff of NSA. *The Baltimore Sun*¸ *Accessed 27 April 2014* <http://articles.baltimoresun.com/2006-01-29/news/0601290158_1_saic-information-technology-intelligence-experts>.

[25] —. 2008. NSA's Domestic Spying Grows. *The Wall Street Journal. Accessed 28 February 2014* <https://web.archive.org/web/20090124141023/http:/online.wsj.com/public/article_print/SB120511973377523845.html>.

[26] Greenwald, G. 2013. Members of Congress denied access to basic information about NSA. *The Guardian*. *Accessed 28 February 2014* <http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access>.

[27] —. 2013. NSA collecting phone records of millions of Verizon customers daily. *The Guardian. Accessed 1 April 2014.* <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

[28] Grier, P. 2014. Does Edward Snowden deserve mercy? *The Christian Science Monitor. Accessed* 28 February 2014 <http://www.csmonitor.com/USA/DC-Decoder/Decoder-Buzz/2014/0124/Does-Edward-Snowden-deserve-mercy>.

[29] Griggs, B. Gross, D. 2014. Edward Snowden speaks at SXSW, calls for public oversight of U.S. spy programs. *CNN. Accessed 7 April 2014* <http://www.cnn.com/2014/03/10/tech/web/edward-snowden-sxsw/index.html?iid=article_sidebar>.

[30] Hampson, R. 2013. Is Snowden a traitor or a public servant? *USA Today. Accessed 28 February 2014* <http://www.usatoday.com/story/news/nation/2013/06/10/snowden-leaks-nsa-privacy-terrorist/2408803/>.

[31] Harding, L. 2014. *The Snowden Files*. New York: Vintage Books.

[32] Hattem, J. 2014. Bar Association protests NSA spying. *The Hill. Accessed 28 February 2014* <http://thehill.com/blogs/hillicon-valley/technology/199075-lawyers-protest-nsa-snooping>.

[33] Horowitz, S. 2013. *Washington Post. Accessed 2014 January 25* <http://www.washingtonpost.com/world/national-security/nsa-collection-of-phone-data-is-lawful-federal-judge-rules/2013/12/27/4b99d96a-6f19-11e3-a523-fe73f0ff6b8d_story.html?hpid=z3>.

[34] Hosenball, M., Stobel, W. 2013. Exclusive: Snowden persuaded other NSA workers to give up passwords - sources. *Reuters. Accessed 28 February 2014* <http://www.reuters.com/article/2013/11/08/net-us-usa-security-snowden-idUSBRE9A703020131108>.

[35] Hosenball, M. 2013. Feds hunted for Snowden in days before NSA programs went public. *Reuters. Accessed 28 February 2014* .<http://www.reuters.com/article/2013/06/12/us-usa-security-snowden-hunt-idUSBRE95B1A220130612>.

[36] Ingersoll, G. 2013. Meet The Anti-Glenn Greenwald, Who Has A Totally Different Take On The NSA Leaks. *Business Insider. Accessed 1 April 2014* <http://www.businessinsider.com/joshua-foust-on-the-nsa-leaks-2013-10>.

[37] Isikoff, M. 2014. Exclusive: Snowden Swiped Password From NSA Coworker. *NBC News*¸ *Accessed 28 February 2014* <http://www.nbcnews.com/news/investigations/exclusive-snowden-swiped-password-nsa-coworker-n29006>.

[38] Kelley, M. 2013. Edward Snowden Fled Hong Kong After Learning His Computer Could Be Taken Away. *Business Insider. Accessed 1 April 2014.* <http://www.businessinsider.com/why-edward-snowden-fled-hong-kong-2013-6>.

[39] Labott, E., Castillo, M. 2014. Edward Snowden won't be pressured to end asylum, Russia says. *CNN. Accessed 7 April 2014*. <http://www.cnn.com/2014/01/24/world/europe/russia-snowden/>.

[40] MacAskill, E., Borger, J., & Greenwald, G. 2013. The National Security Agency: surveillance giant with eyes on America. *The Guardian*¸ *Accessed 11 April 2014* <http://www.theguardian.com/world/2013/jun/06/national-security-agency-surveillance>.

[41] McAllister, N. 2012. Senate votes to continue FISA domestic spying through 2017. *The Register*. *Accessed 13 April 2014* <http://www.theregister.co.uk/2012/12/29/senate_fisa_extension_vote/>.

[42] Newport, F. 2013. Americans Disapprove of Government Surveillance Programs. *Gallup. Accessed 28 February 2014* <http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx>.

[43] Oliphant, J. 2013. Somewhere in Russia, Edward Snowden Is Smiling. *National Journal. Accessed 28 February 2014* <http://www.nationaljournal.com/whitehouse/somewhere-in-russia-edward-snowden-is-smiling-20130809>.

[44] Pew Research Center. 2013. Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic. *Pew Research. Accessed 28 February 2014*. <http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/>.

[45] —. 2013. Public Split over Impact of NSA Leak, But Most Want Snowden Prosecuted. *Pew Research Center*. <http://www.people-press.org/2013/06/17/public-split-over-impact-of-nsa-leak-but-most-want-snowden-prosecuted/>.

[46] Picket, K. 2014. Issa Rips CIA Over Feinstein Spying Allegations: 'Treason'. *breitbart.com*. <http://www.breitbart.com/Big-Government/2014/03/12/Issa-Rips-CIA-Over-Feinstein-Spying-Allegations-Treason>.

[47] Poitras, L., Greenwald, G. & MacAskill, E. 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian.* <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

[48] Pomfret, J. 2013. Snowden extradition battle in Hong Kong could go on for years. *Reuters.* <http://www.reuters.com/article/2013/06/22/us-usa-security-snowden-hongkong-idUSBRE95L02X20130622>.

[49] Rasmussen Reports. 2014. 24% Support Amnesty for Edward Snowden. Rasmussen Reports.com. <http://www.rasmussenreports.com/public_content/politics/general_politics/march_2014/24_support_amnesty_for_edward_snowden>.

[50] —. 2013. 59% Oppose Government's Secret Collecting of Phone Records. *Rasmussen Reports.* <http://www.rasmussenreports.com/public_content/politics/general_politics/june_2013/59_oppose_government_s_secret_collecting_of_phone_records>.

[51] __. 2014. Reason-Rupe Public Opinion Survey. *Reason.* <http://reason.com/assets/db/13964619214696.pdf>.

[52] Risen, J. 2013. Snowden Says He Took No Secret Files to Russia. *The New York Times.* <http://www.nytimes.com/2013/10/18/world/snowden-says-he-took-no-secret-files-to-russia.html?pagewanted=all&_r=0>.

[53] Rosenbush, S. 2014. Post Snowden, Some Internet Usage Is Contracting, Study Finds. *Wall Street Journal.* <http://blogs.wsj.com/cio/2014/04/03/post-snowden-some-internet-usage-is-contracting-study-finds/>.

[54] __. 2013. Snowden: There's no chance Russia, China have NSA docs. *rt.com.* <http://rt.com/news/snowden-russia-china-documents-332/>.

[55] Samuelsohn, D. 2014. NSA watchdog: Snowden should have come to me. *Politico.* <http://www.politico.com/story/2014/02/nsa-inspector-general-edward-snowden-103949.html>.

[56] Sanchez, R. 2013. *The Telegraph*. <http://www.telegraph.co.uk/news/worldnews/barackobama/10228529/Barack-Obama-cancels-meeting-with-Vladimir-Putin-over-Edward-Snowden.html>.

[57] Sanger, D. E. &Schmitt, E.2014. Snowden Used Low-Cost Tool to Best N.S.A. *The New York Times*.<http://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?_r=2>.

[58] Sasso, B. 2014. NSA Wants to Expand Phone Database—Because of Privacy Suits. *National Journal.* <http://www.nationaljournal.com/tech/nsa-wants-to-expand-phone-database-because-of-privacy-suits-20140226>.

[59] Selyukh, Alina and Mark Hosenball. "Obama's NSA overhaul may require phone carriers to store more data." 3 April 2014. Reuters.com. 14 April 2014 <http://www.reuters.com/article/2014/04/03/us-usa-security-obama-idUSBREA3228O20140403>.

[60] Snowden, E. 2013. Edward Snowden Interview: The NSA and Its Willing Helpers Jacob Appelbaum and Laura Poitras. *Der Spiegel.* <http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006-2.html>

[61] Statista. 2014. Public opinion of Americans on whether the NSA's secret data collection without a suspicion of wrongdoing is acceptable. *Statista.* <http://www.statista.com/statistics/260140/opinion-of-americans-on-whether-the-nsas-secret-data-collection-is-acceptable/>.

[62] __. 2013. US files criminal charges against NSA whistleblower Edward Snowden. *The Guardian.* <http://www.theguardian.com/world/2013/jun/22/us-charging-edward-snowden-with-espionage>.

[63] __. 2014. First interview while in Russia: Snowden talks to German NDR – reports. *Voice of Russia.* <http://voiceofrussia.com/news/2014_01_26/First-interview-while-in-Russia-Snowden-talks-to-German-NDR-reports-8339/>.

[64] U.S. vs. Edward J. Snowden. No. 1:13 CR 265 (CMH). Eastern District of Virginia. Alexandria: 14 June 2013.

[65] Voice of Russia. *Voice of Russia.* 25 January 2014. <http://voiceofrussia.com/news/2014_01_26/First-interview-while-in-Russia-Snowden-talks-to-German-NDR-reports-8339/>.

[66] Volz, D. 2014. Russia to Snowden: Stay as Long as You Like. *National Journal.* <http://www.nationaljournal.com/technology/russia-to-snowden-stay-as-long-as-you-like-20140124>.

[67] Walker, H. 2013. *Former NSA Chief: The Agency Has 'Very Good Idea' Which Secrets Snowden Swiped.* <http://talkingpointsmemo.com/dc/former-nsa-chief-the-agency-has-very-good-idea-which-secrets-snowden-swiped?ref=fpb>.

[68] Waterman, S. 2013. NSA leaker Ed Snowden used banned thumb-drive, exceeded access. *Washington Times.* <http://www.washingtontimes.com/news/2013/jun/14/nsa-leaker-ed-snowden-used-banned-thumb-drive-exce/>.

[69] __, 2014. "Edward Snowden." *Wikipedia.* <http://en.wikipedia.org/wiki/Edward_snowden>.

[70] —. 2014. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. *Wikipedia*. <http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008>.

[71] —. 2014. National Security Agency. *Wikipedia.* <http://en.wikipedia.org/wiki/Nsa>.

[72] Wolde, H.T. 2014 Phones for outsmarting snoopers get pitched to mass market. *Yahoo! News.* <http://news.yahoo.com/mobile-privacy-sells-post-snowden-world-134136822--finance.html;_ylt=AwrBEiJknQtTwxwAU9_QtDMD>.

[73] Wood, L.T. 2014. How Could the Obama Admin Allow Snowden to Acquire Classified Information?. *Breitbart.* <http://www.breitbart.com/Big-Peace/2014/02/14/How-Obama-Administration-Allowed-Snowden-to-Acquire-the-Information>.