Erik A. Buschardt

CSSS 5210 – Cybersecurity Law and Policy

Webster University - Spring I 2016

Major Topic: #2:

Electronic surveillance and the NSA with regards to continuing international threats

Minor Topic: Within the scope of terrorism and so-called nation states such as ISIS/ISIL

Respectfully Submitted 26 March 2016

Extended to latest 18 April 2016

INTRODUCTION - Past cases and causes: Cold War, 9/11, Bush Era, Pre-Snowden

During the suspicions of the Cold War, the United States and Russia engaged in a series of covert activities that eventually revealed a paralyzing tension in diplomatic relations due to the potential release and firing of nuclear arms into each other's territory. Such mutually assured destruction was a primary reason, but far from the only reason, for the eventual stalemate and collapse of that war, [BBC ON THIS DAY 1989].

These historic events bring to mind the fact that eavesdropping and wiretapping is nothing new, and that history often repeats itself. For decades, using whatever means technically, legally, or covertly illegal possible, our government has been protecting national interests and investigating persons of interest using the latest in sophisticated and classified technologies.

Because cyber attacks can occur remotely, instantaneously, and with great destruction, it remains imperative that our government remain at the forefront of technological intelligence and knowledge. Any other country that does the same, and has developed covertly or openly any cyber weapon in preparation for a mutually destructive battle, can be considered a threat if not aligned with national interests and bound by treaties, or any other diplomatic assurances of preservation.

Fast forward to the events surrounding the attack and destruction of the World Trade Center buildings 1 and 2 on September 11, 2001 (9/11), as well as the damage suffered to the Pentagon in Arlington, Virginia. As a result of that landmark event, the American public has bore witness to the creation and implementation of one of the world's strictest set of policies with regards to the monitoring of internal and external terrorist threats during the presidency of George W. Bush from 2001 to 2009. Several wide-sweeping regulations designed to combat the threats posed to our nation since the events of 9/11 were introduced during this time, which are described and discussed herein.

This paper serves to highlight and provide a basis for catalyst discussions on the choice to provide and enforce electronic surveillance, and the role that the National Security Agency (NSA) plays in such provisions, statutes and legal enforcements. More specifically, this paper provides a logical framework from which to draw premises, draw conclusions, and provide a backdrop on NSA activities performed covertly as well as those activities revealed publicly.

II. The Current Status - Obama's activities and 2011 Bin Laden raid

Since the events surrounding and leading up to 9/11, the legal basis for the capture and elimination of a high-value terrorist was secretly generated by a small team of lawyers representing various intelligence and military departments within the federal government.

Issues to resolve for this team included (a) where to take this terrorist once captured, (b) the level of international cooperation and involvement of the foreign state with regards to the precise location of the final operation (within Pakistan), (c) the protections and authorizations afforded to the Executive Office of the President (EOP) with regards to the pursuit of persons of interest immediately following the attacks of 9/11 as authorized by the 107th United States Congress, (d) the legalities and protections afforded to civilian persons unaffiliated with the raid compound, but who nonetheless inhabit the surrounding community, and (e) conditions needed for a lawful burial at sea with respect to Muslim religious tradition and Saudi Arabian consent, the home country of Bin Ladin, [Savage, C].

Following the successful and infamous covert raid conducted on-site in Pakistani territory, any further questions as to the legality of the operation ceased to gain traction [Bellinger, J.B]. In May of 2011, a raid was conducted by the United States Navy SEALs of the U.S. Naval Special Warfare Development Group (also known as DEVGRU or SEAL Team Six) in Abbottabad, Pakistan. Part of the mission was to recover classified materials (later declassified in part) that would prove useful for studying the evolution of daily operations within Al-Qaeda, as well as to give western intelligence forces a preview of the development of another fast-rising jihadist movement within Iraq and Syria, derived from the Al-Qaeda terrorist movement.

In the meantime, a “library-sized” treasure trove of computer hardware, disks, external drives, and hardcopies were recovered prior to the departure of these Special Forces from Abbottabad, revealing several operational insights, as follows:

1. Because of Bin Laden's experiences from within the CIA (per Operation Cyclone, 1979-1989), he had an obsession with computer (cyber-) security, even going so far as to strictly maintain a dedicated and trusted offline courier rather than to establish any trace of a network connection for fear of immediate online detection by the Americans.
2. A tendency towards top-down micromanagement of the entire operation. Osama was in control and wanted to keep it that way, lest the organization he led fell apart on his watch.
3. A call to keep the focus of the attacks towards the west and not towards more localized regional conflicts in Somalia, Iraq, or Syria, as these conflicts would drain resources and focus away from the initial primary target.
4. A fascination with traditional broadcast media including Al-Jazeera, a Qatar-based satellite network channel, in order to spread propaganda with regards to the then-recent Arab Spring popular liberation movements against oppressive and dictatorial regimes, as well as anniversaries of 9/11.

5. An exploration into possible uses of social media in order to take advantage of the unrest generated by the populist movements described above [Burke, J].

This evidence recovered form the basis of understanding for the next generation of terrorism as our government seems to understand it, with particular emphasis placed on recruitment of American citizens via social media outreach efforts as evidenced by the 2011 raid. Time and time again, we see national security and the combat of international terrorism used as a justification against technical barriers and the implementation of safeguards such as passcodes, data encryption and biometrics in order to ensure the security of data and privacy for the individual user.

Origins of ISIS/ISIL

The Islamic State of Iraq and Syria (ISIS), also known as Islamic State of Iraq and the Levant (ISIL), is a group of Muslim extremists aligned with the interests of Al-Qaeda in Iraq following the 2003 invasion of coalition forces. Their following grew with the onset of the Syrian Civil War of 2011, and has modernized into a formidably harsh and brutal opposition following the continuing presence of western allies operating in the Middle East.

Part of their mastery in growth and sustainment is a result of their high fluency in web-based and social media operations, recruitment, and the exploitation of sentiments expressed against democratic and western values. Their mission and values include a complete and unquestionable dominance of territory and public perception, in the mindsets of islamic fundamentalism [Wood, G].

To the extent that they have defined themselves as a nation state, that may certainly be the case. Merriam Webster defines a nation state as "a form of political organization in which a group of people who share the same history, traditions, or language live in a particular area under one government", and in particular context, "a form of political organization under which a relatively homogeneous people inhabits a sovereign state; especially : a state containing one as opposed to several nationalities" ["Islamic State…"].

Mentioning the definition of a nation state as sponsors of terrorism means that they have widespread homogeneous support and have legitimized themselves as a collection of militarized persons seeking a unified goal as described herein. By seeking attention, they have gained support and sympathy to their extremist causes.

The Fight Against ISIS and legal precedence

Activities of beheadings and the destruction of significant historical, ancient and cultural artifacts, while maintaining an extremist view of muslim theocracy, have defined the radical culture and extremist nature of this group, one of the world's most nefarious terrorist groups in modern times ["Islamic State…"]. In addition, the hacktivist group Anonymous has recently staged a battlefront with ISIS, saying they will shut down any social media account related to the promotion and distribution of pro-ISIS activities. Facebook spokesman Andrew Souvall has denounced the terrorist group's online recruiting efforts, saying "There is no place for terrorists on Facebook." Meanwhile, Twitter spoke of the number of pro-ISIS accounts as being wildly misrepresented.

Regarding hacktivism activity, It remains to be seen if Anonymous's and Ghost Security's (GhostSec's) efforts will pay off in thwarting the physical attacks of ISIS and any similar terrorist network. Legally, new territory is being charted with respects to jurisdiction, matters of enforcement, moral guidelines, parties involved, and international cooperation to defeat this threat to western national security [Rogers, K].

Other Activities - Encryption and Backdoor Policies

Of recent media interest was a particular feud involving encryption policy between two main parties: the United States Federal Bureau of Investigation (FBI) and Apple Inc.,

(Apple). As a result of a mass shooting in San Bernadino, California on December 2, 2015, an iPhone 5C smartphone was recovered as evidence from a black Lexus sedan, reportedly used by one of the two attackers involved in the shooting.

At stake was the data inside this phone, which was formerly protected with extremely powerful encryption by the manufacturer (Apple). The FBI believed that such valuable information is stored on this iPhone that they mandated Apple via a series of court orders (citing the All Writs Act of 1789, of all precedents) to develop software that would enable federal authorities to unlock and decrypt at will any suspected phone in any subsequent investigation going forward, as a matter of national interest and protecting the homeland.

As a result of this struggle, the FBI has since reached out to Cellebrite, an Israeli tech company that specializes in the decryption of mobile devices, and related unlocking capabilities thereto [Wieczner, J]. The details of the successful hack, including whether or not the hack involved a hardware vulnerability, a software vulnerability, or a combination of the two, have not and will not be disclosed for fear of exposing further technical vulnerabilities with regards to mobile devices currently on the market, placing Apple at an economic and marketing disadvantage, as its products are now not as secure as customers would expect. Subsequently, any company that handles decryption for

mobile devices such as Cellebrite, now faces possible legal action with respect to the Digital Millennium Copyright Act of 1998 from mobile manufacturers such as Apple, Samsung, and Google.

Apple's main argument for their noncompliance with the FBI's series of court orders was the lack of precedent for this national security interest, as well as the fear of abuse by subsequent and similar investigations going forward, whereby any government can force manipulations of digitally encrypted product in the name of national security and terrorism. Indeed, the FBI has immediately stated that upon the successful resolution of this hack, a legal precedent has now been set whereby the government can require private manufacturers to comply with decryption orders in the name of national security. As security expert Richard Clarke notes, it was never about technical expertise, but about setting a legal standard for which all mobile manufactures must now comply [McCarthy, K].

Microsoft and the Department of Justice

Related to the Apple case lies Microsoft, a chief rival. In an ironic twist of fate where the Department of Justice sued Microsoft Corporation (United States v. Microsoft Corporation 253 F.3d 34, 2001) over concerns of market monopolization, the latter is now suing the former over the receipt of thousands of federal inquiries and demands of

customer information; specifically the suit claims that Microsoft would not be allowed to advise their customers when the government has accessed customer information. As professor Neil Richards vividly points out, these type of cases will test the validity and utility of an important legal theorem known as “third party doctrine” whereby users will no longer have any reasonable expectation of privacy once they submit any data to a remote server in the “cloud”, or Internet itself.

The legal precedent set by Cellebrite’s willingness to violate Apple’s security protocols in the interest of national security, and the formal sponsorship of the FBI to employ the services of a foreign third party to do so, establishes a dangerous uncharted territory with respect to eavesdropping and encryption standards. In effect, such litigation significantly undermines and diminishes the ability to market safely encrypted devices and secure products to consumers.

While not directly associated with the NSA in relation to wiretapping and eavesdropping activities, this discussion points to a larger 1984-style Big Brother issue, with 4th Amendment search & seizure demands placed upon private corporations and private citizens, complete with the public rebellion and outcry therefrom. This author is choosing to involve that debate within the scope of this paper due to the large potential of consequences involved [Cook, T].

The Intel Reform and Terrorism Prevention Act

The Intel Reform and Terrorism Prevention Act (IRTPA) of 2004 was a formal codification by Congress, (50 U.S.C. ch. 15 § 401 et seq.), mirroring Executive Order actions taken by President Bush in August of 2004 [White House, The] with the stated intentions of sharing intelligence by federal departments, as well as a continued promotion of shared resources, combatting a longstanding stigma of compartmentalization of valuable intel operating from within these respective departments.

Prior to 9/11, there existed certain non-overlapping areas of expertise and specialty with regards to each federal department's role in combatting terrorism. For example, the FBI was designed to investigate domestic criminal matters, the DOD was designed chiefly for foreign warfare and defense from foreign threats, the CIA was designed as a central depository for intelligence collections, whereas the NSA was designed as an advisory channel at the president's immediate disposal, operating out of the White House Situation Room (along with other folks from the Department of Homeland Security, created in 2002).

Because of the severity of 9/11 and the anticipation of cybersecurity threats since that time, overlapping duties and concerns from each department were consolidated via IRTPA, including eavesdropping and wiretapping activities. This law is designed to solidify efforts so that the intelligence communities may more closely coordinate activities of national security in a unified and more efficient fashion.

The PATRIOT Act

The USA FREEDOM Act was a response to civil violations as performed by Mr. Snowden with regards to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act, 115 Stat. 272 (2001), and subsequently exposed via the media to the worldwide public. Originally designed as a blanket approach to combat the causes of 9/11 via the Global War on Terror (or "GWoT"), the PATRIOT Act and its subsequent Sunsets Extension Act of 2011 went largely unchecked in terms of magnitude and scope of combating this global war. As a result of Section 215 of the PATRIOT Act, phone companies will be allowed to obtain and retain the metadata, while the NSA will be permitted to gather information regarding certain individuals with explicit permission from a federal court [DeRosa, M.].

USA FREEDOM Act

Another piece of the puzzle, in order to ensure the full compliance, valid lawfulness, and morality of governmental activities with respect to wiretapping, eavesdropping, and forced backdoor decryption implementations, involves the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring (USA FREEDOM) Act, enacted on June 2, 2015.

This law was not passed in direct reaction to 9/11, but rather due to the actions performed by Edward Snowden in 2013. It was a successor to the PATRIOT act described above, and was meant as a "balanced" modification of wiretapping and eavesdropping efforts, with specific regard to telephony and cellular metadata. Due to Mr. Snowden's exposure, this act was passed to limit widespread 'dragnet-style' collection, whereby massive quantities of user data was scooped up first, then sorted for utility after the fact.

FISA (United States v Isa, GRF v O'Neil)

With regards to the Foreign Intelligence Surveillance Act of 1978 ("FISA" Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36), certain technical issues affected the outcomes of at least two cases discussed here: that of United States v. Isa, and Global Relief Foundation, Inc. v. O'Neil. In the former case, FISA specifically authorized the retention of information relevant for pursuit of a criminal matter outside the scope of foreign

intelligence, which remains FISA's general intent [Solive, D. J. et al, pg. 171-2]. In the latter case, a warrantless search was conducted on an emergency pretense.

The search revealed sensitive information that led to a potential harm of the national security [Solive, D. J. et al, pages 168-9]. Both cases demonstrate the practical uses of FISA outside its normal and practical boundaries, as well as its documented flexibility as established by these now-precedent cases.

Surveillance - Clapper v Amnesty Intl USA

The prediction of negative outcomes cannot be anticipated by suspicion or fear, nor was it allowed to warrant activities of surveillance, ruled SCOTUS on April 1, 2013 [Solove, 195-202], [Clapper v. Amnesty Intl (2012)]. In this case sensitive communications with foreign persons of interest were hampered by surveillance activities, authorized by FISA, on the sole basis of their foreign origin, possession of foreign intelligence, and premature suspicion of future injury. The case was dismissed because of a lack of Article III standing, defined as injuries that are "concrete, particularized, and actual and imminent…" as per *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139 (2010).

The Role of Edward Snowden

INTRODUCTION

Edward Snowden was employed as a civilian contractor for Booz Allen Hamilton, working on behalf of the National Security Agency (NSA), and was responsible for leaking a treasure trove of classified information to the world press in 2013. Specifically, his actions against his former employer, with regards to covert intelligence activities, eavesdropping, and wiretapping, were deemed illegal and immoral from the viewpoint of the federal government.

PROGRAMS EXPOSED

Programs exposed include the PRISM electronic data mining program, a program to uncover private networks called "Black Pearl", as well as various covert Signal Intelligence (SIGINT) programs, designed primarily to intercept, decrypt, and interpret wired and wireless electrical and fiber optic transmissions from public worldwide networks. In addition, the NSA's CO-TRAVELLER ANALYTICS surveillance program acquired and interpreted information regarding user contacts and social relationships via the collection of HTTP cookies, user app data, and text messages both sent and received from any user mobile device [How the NSA].

MOTIVATIONS

Unsatisfied with the lack of response by authorities when submitting his original complaints of abuse by the intelligence system and in particular those actions of the NSA,

Mr. Snowden claimed to have first taken steps through internal channels to expose wrongdoings and suggest alternative measures to these actions and intentions to the acquisition of data mining operations, but was repeatedly and systematically denied in his efforts.

NOBLE INTENTIONS?

He claims to have won his objective by setting in motion the investigative curiosity that feeds the international media interest, formal inquiry process, and public justification. Indeed, he stated that "I acted on my belief that the NSA's mass surveillance programs would not withstand a constitutional challenge, and that the American public deserved a chance to see these issues determined by open courts ... today, a secret program authorized by a secret court was, when exposed to the light of day, found to violate Americans' rights. It is the first of many." [Savage, Charlie (2013)]

RELEVANCE TO CYBERSECURITY AND LAW

Legal ramifications with regards to Mr. Snowden's actions are numerous and range from high treason to issues of public domain, classification schemes used, jurisdiction and citizenship, not to mention the basis of legal issues that stem as a result of the covert actions of the NSA.

OUTCOMES

Partly because of his actions, the USA FREEDOM Act of 2015 was passed with overwhelming congressional majorities in both the House and Senate. His actions still resonate with us today, due to the far-reaching implications of the programs involved, which struck a fundamental cord with the relationship of trust between citizens and their government [Andrews, Burrough, Ellison (2014)].

INTERNATIONAL LAW AS ENFORCED BY THE UNITED NATIONS

Finally, several complications of international law as enforced by the United Nations exist, as the Security Council continues to address international threats within current treaties, practices, and diplomatic expectations. Of particular interest is the role that terrorist groups such as ISIS play in international diplomacy efforts among western nations as a unifying threat. Politicians have needed to jump through an increasing number of hurdles, bipartisan actions, and diplomatic efforts within their respective countries in order to justify the counter offensive efforts needed to restore national order following each successive and massively destructive terrorist attack.

While Article 51 of the United Nations Charter explicitly and strictly prohibits the use of militaristic force applied within the territory of another independent sovereign state, a number of questions are raised. For example, if the target country is unable or unwilling

to dedicate resources in order to effectively combat any terrorist threat from within their borders, what risk does that pose upon their neighbors and the worldwide community? If any terrorist group does not explicitly target any host nation from which they launch operations against any other sovereign nation, is that host nation responsible for harboring said terrorists after an attack is carried out? And finally, what role does the target nation play in retaliation for these efforts per the Charter, the Geneva Conventions, as well as any other internationally agreed upon treaties in force?

Several factors come into play, including humanitarian intervention, consent, the right to a collective self-defense, cultural respect to questions of conflict resolution, war, economic sanctions, or threats related thereto by rogue nations or terrorist groups. Whatever the outcome, it remains to be seen how the balance of international power will play out when combatting threats as large as ISIS [Hanley & Downes (2014)].

CHINA

In keeping with the theme with international threats and state sponsorship of terrorists, hackers, and other types of cyber criminals, China has long played a role in anti-western nationalist sentiments with regards to national security, corporate trade secrets, and a disregard for most forms of democratic economic profit, insomuch as they can grab themselves more than a fair share. Eavesdropping, wiretapping, and other forms of

corporate and state-sponsored espionage have been a longstanding byproduct of the current government administration led by President Xi JinPing of the People's Republic of China's Communist party.

With known threats and countermeasures deployed across both nations, China plays a major role in both our economic health and our worldwide infrastructure as both superpowers seek to maintain an advantage and advance the interests of their peoples. However, in pursuing this balance of power, both the American public and the Chinese public must be careful to not be tempted with a false sense of security when choosing a candidate with a militaristic background, or even those candidates who trump themselves as the best choice in order to protect national interests. Personality will only get a candidate so far - political skill and a sound mastery of diplomacy, compromise, and humility will determine a long lasting legacy [Parkins 45].

FUTURE TRENDS AND CONCLUSIONS

There will always remain a need and a strengthened effort for a population to remain collectively self-defensive, that is, having a means to preserve itself under any circumstance. Throughout the era of terrorism witnessed from 2001 up until the present day, electronic surveillance techniques have served a convenient role in the government's role of the protection of its citizens.

Western societies are not asking for such eavesdropping to stop entirely, but to cease its invasions of privacy perceived throughout this time by our governments, both covertly and overtly. It is unfortunate that it took either an act of treason or an act of patriotic duty (depending on your viewpoint) in 2013 to expose a devastatingly obtuse quantity of evidence of wiretapping, data mining, civil violations, moral breaches and international incidents in order to rectify a balance of power overreached since the 1960's, throughout the modern era, highlighted most luminously with 9/11, and through these past 15 years since.

Indeed, that is the point. A balance of power has always been required since the beginning of any government. Trust must be earned, and when that trust is violated, trust must be earned again. Through our judiciary, we have established many precedents and case law examples to study, dissect and study in great detail. Through our executives,

enforcement of constitutional liberties must be upheld, even when terrorism and technology collide. And finally through our legislative bodies, that the creation of statutes follow sound moral codes of conduct.

As noted in this paper throughout, ultimately a fight against terrorism is endless and futile without full support of the populace, lest it turn itself into a 1984-style dystopia. Major cities throughout the world including London and Tokyo have implemented automated camera systems into their law enforcement agendas, and because the population is educated enough to trust an intelligent government, such systems persist peacefully without major conflict or headline.

It is when the populace is not educated in the true intent of Big Brother activities, or any of the three branches violated that sacred trust, that headlines are splashed region wide and worldwide, and the balance falls out of whack again. Such are the ebb and flows of this dynamic pattern.

Keeping our government in check is the voter's responsibility, and a civic advocate's act. Hacktivists such as Anonymous and GhostSec flourish when a divisive threat is in focus, target, and range of their cyberweaponry, both automated, and manned. Societies benefit, for the whiter the hacker's hat, the better.

Finally, a quote from “The Philosophy of Witchcraft” by Ian Ferguson in 1924 adds a final perspective and outlook to this field of study: *“The habit of eavesdropping and spying, so characteristic of Puritanism, became a natural safeguard, for if a man was not at his neighbor's keyhole it is probable that his neighbors would be at his.”*

REFERENCES:

BBC ON THIS DAY 1989: Malta summit ends Cold War. (2008, December 03). Retrieved March 13, 2016, from http://news.bbc.co.uk/onthisday/hi/dates/stories/december/3/newsid_4119000/4119950.stm

Bellinger, J. B., III. (2011, May 02). Bin Laden Killing: The Legal Basis. Retrieved March 13, 2016, from http://www.cfr.org/terrorist-leaders/bin-laden-killing-legal-basis/p24866

Burke, J. (2015, May 21). Bin Laden's declassified documents reveal a family-oriented conspiracist. Retrieved March 18, 2016, from http://www.theguardian.com/world/2015/may/21/osama-bin-laden-declassified-documents-us-intelligence-al-qaida

Cellebrite. (2016). *Unlock Apple Devices Running IOS 8.x With No Risk Of Device Wipe Or Hardware Intervention* [Press release]. Retrieved from http://www.cellebrite.com/Pages/cellebrite-solution-for-locked-apple-devices-running-ios-8x

Cook, T. (2016, February 16). A Message to Our Customers [open letter]. Apple, Corp. Retrieved from http://www.apple.com/customer-letter/

Daimond, Jeremy. "NSA surveillance bill passes after weeks-long showdown". CNN. Retrieved 3 March 2016, from http://www.cnn.com/2015/06/02/politics/senate-usa-freedom-act-vote-patriot-act-nsa/

DeRosa, M. Patriot Debates [Web log post]. Retrieved from https://apps.americanbar.org/natsecurity/patriotdebates/sections-214-and-215

Greene, Jay & Barrett, Devlin (April 14, 2016). "Microsoft Sues Justice Department Over Secret Customer Data Searches". *The Wall Street Journal*. Retrieved March 21, 2016.

Hanley, C. & Downes, J. (2014, November). ISIS: The Complications of International Law [Web log post]. Retrieved from http://the-ballot-box.blogspot.com/2014/11/isis-complications-of-international-law.html

“How the NSA is tracking people right now.” (2015, December 28). Retrieved March 18, 2016, from

https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-tracking-people-right-now/634/

"Islamic State in Iraq and the Levant (ISIL)". Encyclopædia Britannica. Retrieved 24 March 2016, from http://global.britannica.com/topic/Islamic-State-in-Iraq-and-the-Levant

James R. Clapper, Jr., Director of National Intelligence, et al., Petitioners v. Amnesty International USA, et al., 2d Cir. (2012)

McCarthy, K. (2016, March 14). Former US anti-terror chief tears into FBI over iPhone unlocking case. Retrieved March 18, 2016, from http://www.theregister.co.uk/2016/03/14/former_counterterrorism_chief_tears_into_fbi/

Nation-State. (2016). In Merriam-Webster's dictionary (11th ed.). Springfield, MA: Merriam-Webster.

Parkins, D. (2016, April). Beware the cult of Xi. *The Economist, Volume 419* (Issue# 8983), pp.43-pp.46.

Rogers, K. (2015, November 25). "Anonymous Hackers Fight ISIS but Reactions Are Mixed." *The New York Times.* Retrieved March 13, 2016, from http://www.nytimes.com/2015/11/26/world/europe/anonymous-hackers-fight-isis-but-reactions-are-mixed.html

Savage, C. (2015, October 28). How 4 Federal Lawyers Paved the Way to Kill Osama bin Laden. Retrieved March 18, 2016, from http://www.nytimes.com/2015/10/29/us/politics/obama-legal-authorization-osama-bin-laden-raid.html

Savage, Charlie (December 16, 2013). "Federal Judge Rules Against N.S.A. Phone Data Program". *The New York Times*. Retrieved March 21, 2016.

Solove, D. J., & Schwartz, P. M. (n.d.). *Privacy, law enforcement and national security.*

Suzanna Andrews, Bryan Burrough & Sarah Ellison (May 2014), "The Snowden Saga: A Shadowland of Secrets and Light" *Vanity Fair*

The White House, Office of the Press Secretary. (2004). *Executive Order: Strengthened Management of the Intelligence Community* [Press release]. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-6.html

Vint, J. (n.d.). The European View of Privacy. Retrieved March 13, 2016, from http://www.navigant.com/insights/hot-topics/technology-solutions-experts-corner/the-european-view-of-privacy/#sthash.dXYTlViB.dpuf

Wieczner, J. (2016, March 29). This Stock Is Soaring Because the FBI Cracked the San Bernardino Shooter's iPhone. *Forbes Magazine*.

Wood, G. (2015, March). What ISIS Really Wants. Retrieved March 18, 2016, from http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/