University of Nebraska at Kearney

Security, Privacy, and Convenience in a Connected World

An independent study

Chase Miles

University of Nebraska at Kearney, Senior

OCTOBER 2016

Introduction

The year is 2016 and technology is infused into our daily lives. Technological devices sit in our pockets that have more computing power than the NASA computers which landed us on the moon. Calculators exist with more processing power than the space shuttle's on-board computer in 1991. We live in an interconnected world where smartphones track our GPS location, browsing habits, travel habits, and our shopping tendencies. Everything we do is recorded and analyzed - saved to the cloud and synchronized across all of our devices. Cyber-security has become increasingly more important as we become more and more reliant on technology - how we deal with security and making sure it is well-balanced with privacy concerns is something that must be considered sooner, rather than later.

This presents a problem. With so much personal data stored and shared across the Internet, issues with privacy and security become more and more prevalent. People have a large number of online accounts, many times with inadequate passwords that are shared across all of their logins. Data about users is shared with advertisers, or in some cases, shared with government agencies - creating potential privacy concerns.

With the rise of interconnectivity and the "always-online" way of life, society has opened itself up to exploitation in new ways. Identity theft, hacked accounts, personal photos or information stolen and posted online - the list goes on.

Privacy in an ultra-connected Society

The emergent "internet of things" has permeated our society. Devices of all shapes and sizes now connect to the Internet and synchronize data and information across accounts. Refrigerators know when and what you eat, thermostats track when you're home, browsers track your online habits, phones track where you go, and the list goes on. These devices may even tie into a singular account, creating a veritable treasure trove of data about you - data which could be collected by an organization to do with as they see fit.

Our world is connected. We have traded privacy for convenience. Take Google as an example: Google, or its parent company Alphabet, owns an Internet browser, mobile phone OS, an Internet Service Provider, a popular email platform, a social media site, a smart-thermostat which tracks when you're home, an advertisement company, a shopping platform, and even a robotics company. When combined into a single "Google account," many of these various services can combine their data and provide a frighteningly thorough picture of who you are and what your habits may be.

Social Media, the Anti-Privacy

The very nature of a social media website goes against the idea of privacy. Using a social media site is by design a willful reduction in your own privacy. Sharing photos, status updates, and biographical details are common on social media. In addition, many people will share these historically private things with people they barely know. Some sites call these "friends" but in many cases, some of those "friends" are just someone they passed in the halls in high school or happened to sit next to in home room. Worse still, some people set their profiles to "public," showing off their personal details to the whole world.

Facebook is perhaps the most well-known and most popular social media platform in the Western world. According to Statista.com, Facebook had over 1.7 billion monthly *active* users in the second quarter of 2016. It had reached 1 billion back in 2012 and is showing no signs of stopping. People post their lives on Facebook. People share hundreds of photos and status updates about their personal lives to all of their friends on Facebook.

These detailed and in-depth looks into an individual's personal life is often viewable to hundreds of "friends" on Facebook. According to some research conducted by John M. Grohol on psychcentral.com, one in four "friends" could not be named from memory. The same study reminds us just how loose the word "friend" has become. Roughly 25 to 30% of people on a person's "friends" list do not meet the traditional definition of friendship. That is a shockingly high number of "friends" who clearly aren't

known very well, yet have been entrusted with a very large amount of personal information.

What problems can arise from this sharing of information? Well, those who have no compunction with becoming friends with their boss and co-workers may find that calling in sick and then posting pictures of themselves at the local amusement park doesn't really work out for their long term career goals.

In one incident reported by the Washington Post, a daycare worker was fired for posting a status on Facebook saying that she hates 'being around a lot of kids.' After the end of her first day, she made a post on Facebook that resulted in her getting fired and told not to bother coming in the next day. In another incident, a person posted on Twitter with a negative comment about starting a new job. The boss saw the post and immediately responded telling the person not to bother showing up for their first day.

Social media is a tool. As with most things, moderation is necessary. There are plenty of stories about child predators showing up at soccer games, people getting fired for selfies in a bar, and stalkers tracking down their persons of interest. Much of the issue with social media is that people are all too willing to share plenty of information about themselves with anyone who will listen. The 'privacy filters' we historically used in regular conversation just don't seem to be translated into good-practice on social media profiles.

Privacy vs. the Government

In the aftermath of the September 11th attacks, security became much more tight in the United States. One of the mandates passed down by President George W. Bush's administration is known as the PATRIOT Act. This act granted, among other things, broad surveillance powers to intelligence agencies in the United States.

One of the major sources of public consternation stems from the fact that the NSA used some of these powers to initiate a broad phone-tapping program of thousands of US citizens. The irony of this is that while people are more than willing to post everything about their personal lives for the world to see on Facebook, they protest

and squirm the moment the NSA is revealed to have been listening in on their conversations at home.

Despite the fact that the PATRIOT Act was occasionally considered a Republican legacy, in February 2010, President Barack Obama, a Democrat, signed a legislative law that would temporarily extend three controversial provisions of the PATRIOT Act that had been set to expire:

- Court-approved wiretaps that allowed surveillance of multiple phones
- Court-approved seizure of property and documents in anti-terrorism operations
- Allowance for surveillance on a so-called “lone-wolf,” which is a non-US citizen engaged in terrorism that may or may not be part of a recognized terrorist group

Another extension of the bill was made the following year by the House of Representatives by the FISA Sunsets Extension Act of 2011. Two years later, abuses of the Act were brought to light due to a massive leak of classified documents. This revealed the NSA’s PRISM program. The abuse was widely renounced and created a public outcry at the apparent misuse of the Act. Representative Sensenbrenner of Wisconsin (R) released a statement following the leaks:

> As the author of the Patriot Act, I am extremely troubled by the FBI’s interpretation of this legislation. While I believe the Patriot Act appropriately balanced national security concerns and civil rights, I have always worried about potential abuses. The Bureau’s broad application for phone records was made under the so-called business records provision of the Act. I do not believe the broadly drafted FISA order is consistent with the requirements of the Patriot Act. Seizing phone records of millions of innocent people is excessive and un-American.

As is clear, the American government has been facing increasing struggles to balance security, especially against terrorism, with the concerns of privacy. On the one hand, September 11th shocked the US into a hyper-awareness that revealed the looming, credible threats of terrorism. This spawned legislation like the PATRIOT Act which granted broad powers in the name of security. Coupled with the staggering growth of the Internet and inter-connectivity during the same time, a definitive risk to

privacy was being realized. Thankfully, some of these privacy concerns have been taken more seriously in the more recent years but the balancing act continues.

Security and privacy constantly exist in a delicate balance. Sacrifices are made to privacy in the name of increased security while compromises to security are made in the interests of privacy. If the scales tip too far in one direction, it creates a potential problem: Too much emphasis on security can lead to a dystopic future such as those set out in books like *The Giver* by Lois Lowry or George Orwell's *1984*. Too much emphasis on privacy may lead to escalating terrorist attacks resulting from the sacrifices made to security. This balancing act has been going on for centuries in one form or another. During the formative years of the United States, Benjamin Franklin famously said, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

With the rise of the Internet and mobile devices which are "always online," there is an unprecedented amount of interconnectivity between people of all walks of life. This connectivity is often viewed as an excellent source of intelligence for government agencies like the American FBI or the NSA who seek to use the information ostensibly for national security.

In a recent case, the FBI demanded that Apple create a backdoor in their iPhone devices to allow access to encrypted and locked iPhones. They made the request as they were wanting to gain access to an iPhone belonging to a suspected terrorist in the San Bernardino, CA shootings. Apple refused to cooperate with the FBI's request. The FBI made this request because of an ongoing investigation into an American couple which had shot up an office in California. This created an uproar amongst those who did not believe the government should have the ability to freely decrypt anyone's phone. Reportedly, the FBI managed to find their own way of getting into iPhones after Apple refused to give them a back door.

Probes to find out what they did were made by Apple, but in an ironic twist, this time it was the FBI's turn to refuse. There has been some consternation amongst the public as who who exactly the FBI hired to break into the phone. USA Today and three

other news companies sued the FBI, pressing for a release of the identity of the anonymous source which cracked the phone and how much the government paid this source. The suit states that there is “no lawful basis” for the FBI to withhold this information from the public. The FBI Director James Comey did state back in April 2016 that the price had been over $1 million. He also stated that the exploit only “works on a narrow slice of phones,” and that it would be unlikely to be effective or useful on anything other than an iPhone 5C with iOS 9 installed, which was the specific type of the phone used by one of the San Bernardino shooters.

This is hardly the only instance of government agencies stepping on aspects of privacy in the name of security. Internet Service Providers (ISPs) and cellphone carriers have frequently been served with warrants to hand over records and logs pertaining to the private data of thousands of citizens.

Society must find ways to incorporate new challenges to privacy and security. Governments must be kept in check, lest they sacrifice too many individual freedoms or privacy, while individuals must not neuter their governments and effectively open the door to the destruction of their way of life. Technology must be factored into modern discussions on the subject, and politicians or individuals must maintain a basic understanding of the Internet and the ever-growing connectivity we face.

Security in the Modern Age

With more and more reliance being put on online databases and data storage, there is an increasing demand for cybersecurity. Credit cards, addresses, and even healthcare records are stored on networked databases which can be vulnerable to attack. Over the last 6 years there have been several high profile breaches with wide impacts.

In what has colloquially become known as *the Fappening* on social media, a high profile breach of several celebrity iCloud accounts resulted in hundreds of private cell-phone photos being leaked to the Internet. Included among these photos are many which show their subject either nude or partially nude. Several celebrities reacted to

the hacks. Jennifer Lawrence of *The Hunger Games* fame called this hack a “sex crime” and attempted to take legal action against sites or individuals which propagated photos. Seth Rogen, while not one of the victims, did scold the offenders by saying “Posting pics hacked from someone’s cell phone is really no different than selling stolen merchandise.”

In another well-known breach, Target’s point of sale (PoS) system was breached. Millions of stored credit card records were stolen. This occurred because the system accessed by a contractor to work on their PoS system was not properly segregated from the database. Wendy’s franchises across the nation also suffered a similar breach of their own PoS software just this year.

During the 2008 election year, Republican Vice-President hopeful Sarah Palin suffered a breach of her personal Yahoo email account. The attack was perpetrated by David Kernell - a 23-year old former University of Tennessee student and son of a senior Democratic politician. This so-called “hack” wasn’t even a real hack and only took 45 minutes. It was a basic social engineering attack. Access was gained by using the “forgot your password” function and looking up the answers to the security questions with information readily available on sites like Wikipedia. Questions involved seemingly personal but hardly private information, especially for a person running for office: when she met her husband, her birthdate, and home zip code, which were all very easily obtained with a few searches on the Internet. Kernell ended up being sentenced to a minimum security prison for 1 year at the start of 2011 despite the judge’s recommendations that he serve the time in a halfway house. This attack is a great reminder to us that security is not something to be left in the back of the mind.

As a society, we definitely should punish hackers and cyber-criminals but we must also take steps to learn from these blunders. It is the responsibility of individuals and organizations to take adequate measures to protect accounts and information systems from the bad guys. For a business, a large breach of data could result in fines or even a class-action lawsuit. For an individual, it can result in identity theft, breach of privacy, or stolen accounts.

In 2014, Sony Pictures Entertainment was hacked by a group calling itself the "Guardians of Peace"*,* according to a report released by Gabi Siboni and David Siman-Tov. This hack is one of the largest in recent history. Included in this hack were hundreds of confidential emails, detailed personal information about its employees, copies of unreleased films, and other information. Much of this information is still available on the Internet if you care to look for it.

About a month after the hack, the hacker group demanded that Sony cancel its upcoming film *The Interview*, a comedy about a plot to assassinate the 'glorious' North Korean leader Kim Jong-un, threatening to launch terrorist attacks on locations that showed the film. Many theaters, including Regal Entertainment, AMC Entertainment, Cinemark, and Carmike Cinemas even refused to show the film due to fears of terrorist attacks. In response to the drama, and according to the New York times, Sony opted to cancel the theatrical premiere and released the film for sale or rent digitally via online streaming services such as Google Play, YouTube, and Amazon Video.

Why is this hack different than the others? After investigation by US intelligence officials, it was determined that the hack was sponsored by North Korea. There was a "long forensic trail" for the Sony hacks, according to security researchers. One such part of the trail had the signal being bounced off of proxy servers mostly located within North Korea. The malware used on Sony shared several similarities with malware used in attacks on South Korean banks and broadcasters the previous year.

In an INSS report submitted by Siboni and Siman-Tov, titled *Cyberspace Extortion: North Korea vs. the United States*, the purpose of the attack "...was to deter Sony Pictures from releasing [*The Interview]..."* because it portrayed the nation's leader as a "mockery." The North Korean regime has a history of totalitarian practices and anti-free speech policies. They may have viewed the release of a movie mocking their leader as something that could not be tolerated lest it fall into the hands of their citizens.

In a study by Verizon, reported on by cnet.com, the number of cyber-espionage attacks worldwide has risen 15% between 2011 and 2013. The costs of these kinds of attacks is not insignificant either. The annual cost of a successful cyberattack increased to $20.8 million in the financial sector, $14.5 million in the tech industry, and $12.7 million in the communications field.

It is believed that most attacks targeting United States-based organizations come from China and France - though there are plenty of attacks occurring domestically as well. According to Kurt Stammberger, a senior vice president of Internet research firm Norse, state-sponsored hacking is “undeniably on the rise.” US President Obama warned that these types of attacks are expected to grow in regularity and severity. “They’re going to be costly, they’re going to be serious,” he said in a 2014 news conference.

Security analysts warn that, in the future, terrorist groups may be able to do what North Korea did to Sony in as few as three years. The truly devastating attacks wouldn’t come from attacks on corporations but from cyberterrorism attacks targeted at a country’s infrastructure. Power grids, city traffic instruments, and emergency services could be vulnerable to cyber-attacks. Our world is embracing interconnectivity at an exponential pace with our basic infrastructure and services becoming internetworked, some with woefully inadequate security. Networking these systems and leaving them with Internet access leaves them exposed to attacks launched by cyber terrorists and hostile government agencies. What happens if someone brings down the power grid for New York City? What if our traffic lights suddenly malfunctioned? What if water-pipes were shut down? Securing these systems from attack is imperative as it can disrupt daily life and even security if coordinated with more conventional attacks.

Future wars may not be fought on the battlefield, but in cyberspace. In 2015, according to CNN, Russians allegedly hacked the White House. They hacked into the State Department and gained access to sensitive information in the White House computer system. The affected data was not classified, but the information was still considered sensitive.

Security at Home vs. Convenience

The problem with security doesn't just affect major corporations and governments. Individuals must remember that their own accounts must be appropriately secured. So many people do not take their own account security seriously. In a report released by SplashData, three of the most commonly used passwords in 2015 include "123456," "qwerty," or "password." They said that "123456" was the most common password for the fifth year in a row. Other common passwords included "football," "monkey," and "starwars." These passwords are so simple that they would take no time at all to crack - hacking software often tries these most common codes first. This data is obtained from breaches across the Western world, including the hack of the Ashley Madison dating site from last year.

Passwords like these would take mere minutes to hack using a technique known as brute-forcing. Brute-force attacks involve entering every possible combination until achieving a successful result. When used in conjunction with a dictionary attack, passwords with simple words and numbers can be hacked in no time.

Something else that many people do not take into account is that their email should be the most secure account of all; even more so than bank accounts. The reason email accounts should have the most security is precisely because they provide the 'keys to the kingdom,' so to speak. If someone wants to get into any of your accounts, many times all they need is access to your email account - hitting "forgot password" on most sites will send the reset link to the email address belonging to that account, which gives the attacker the ability to reset the password and log in.

Compounding the problem is that people use the same username and password across several sites. If one site gets hacked, then *all* sites using that username and password may be compromised. This is obviously done out of convenience - it's easier to remember one set of credentials and use it everywhere. For most users, convenience and laziness beat out security.

A better password practice involves using a long pass-phrase containing multiple words, numbers, and symbols. It is also recommended that a different password be used for each account to prevent a cascade of breached accounts. There are programs in existence such as LastPass or Roboform which let users maintain an encrypted database containing all of their login credentials to make this a little more convenient - though it should be noted that a breached database would expose all of the saved logins anyway. Using a password manager may alleviate some of the concerns about security while also making security just a little more convenient.

Passwords are just one problem facing home users with information security. A problem that some folks have is leaving their routers unsecured. I've caught several of my own friends and family using the default administration passwords for their routers and one person even had fully unsecured wifi "because [she] doesn't like typing [her] password in."

Unsecured Wifi

Unsecured wifi is vulnerable to several types of attacks, including something called a man-in-the-middle attack. This attack involves an attacker connected to the same network setting their device up as a "relay." They get all of your device's traffic to go through their device and forward it onto the router and back. This allows them to snoop on any and all of your activities without anyone even knowing the signal is being intercepted. This is just one type of attack in a criminal's toolkit. Things like this are why routers must be properly secured with a WPA or WPA2 key and the admin password must be changed as well, but not to the same password as the Wifi login!

According to an article run by cnet.com, a community of individuals on Wigle.net frequently go wardriving (driving around looking for unsecured wifi connections) and found that almost 28 percent of cataloged networks were completely unsecured. With just an antenna and the right software, a hacker can park outside a building and capture a large amount of private data including passwords, emails, form data, and any other unsecured information transmitted across that network.

A person could also launch targeted attacks on devices located on an unsecured network - for example, they may gain access to the files located on the computer, or even upload an executable program to the computer's hard drive which can perform any number of tasks such as stealing data, leaving a backdoor, or corrupting data on the device. Even data which is secured using common encryption protocols like SSL(Secure Sockets Layer) or TLS(Transport Layer Security) may be hijacked and broken into.

Any traffic that goes through your network connection is considered your responsibility. If a person, such as a neighbor, were to connect to a household's unsecured network and perform illegal activities like watching child porn or engaging in online piracy, the network's owner can be held accountable for those crimes as the traffic would be traced back to them, rather than the neighbor who committed the crimes.

Wardriving Research

I decided to perform my own independent research on the city of Kearney, NE by engaging in a wardriving run using the Wigle application on my Android phone. I mounted my smartphone to my windshield, activated the scanner, and proceeded to drive around the city of Kearney for about an hour and a half. I managed to obtain a list of 6088 total wifi networks.

The surprising part is that approximately 11% of those networks were *unsecured* wifi networks. Of the 6088 networks, a total of 626 of them were counted as unsecured, which means they did not use any form of encryption, not even the outdated and obsolete WEP standard. Though some of these unsecured networks do include public wifi hotspots, most of my wardriving was centered around various suburban neighborhoods. A number of the unsecured SSIDs included common consumer naming schemes like "linksys," "Sandrock Family Network," and "Basement."

The fact that so many individuals operate their networks completely unsecured from outside intrusion in a world where everyone has a wifi-capable device in their pocket is astounding. I also decided to make a run on some of the UNK campus dorms.

I ended up finding that a number of students opted to run their own wifi network. A few of them were unsecured. I opted to ask a couple of students sharing a dorm room with unsecured wifi why they did not secure the network; They wished to remain anonymous so no identifying data was collected. Their response was that they did it because it was just ‘easier’ not having to enter a password and they didn’t mind if others used their wifi connection.

Convenience usually does not go hand in hand with security - but sacrificing too much security for the sake of convenience is a potentially grievous mistake in our ultra-connected and high-tech information age society. As evidenced by the students who stated they ran unsecured wifi because it was easier, convenience is definitely a driving factor for some people who just don’t care about security. Coupled with the ridiculousness of the most common passwords found in past hacks being things like “password,” it’s easy to see just how many people sacrifice their data security on the altar of convenience.

Summary and Conclusion

Technology is advancing at rates unimaginable to technologists of just 20 years ago. As technology improves, so does the rate at which it improves. Security, privacy, and convenience live in this constant triad of balance which is always fluctuating. The key to ensuring our future is utopian rather than dystopian is to make sure that the balancing act remains relatively centric.

Data collection is performed by companies, governments, and private organizations. Everyday household items such as refrigerators, thermostats, doorbells, and even vehicles are becoming part of the Internet of Things. Just about everything we do is ‘on the grid.’ As we connect our daily lives to the Internet and post about our day to Facebook and Twitter, we open up things that were once considered private. Privacy is becoming more difficult to maintain in the modernized interconnected world we are creating for ourselves.

While the increase in data collection and interconnectivity threaten our privacy, it can also both enhance and simultaneously hinder our security. Security comes at the expense of privacy but as mentioned before, sacrificing your liberties and privacy on the altar of security is a grave mistake and will swing the triadic balance too far towards security - leaving us with a “big brother” situation that is definitely unappealing.

Connectivity by its very nature will reduce privacy. However, as mentioned, its effects on privacy are both detrimental and helpful at the same time. Interconnectivity lets governments monitor their citizens to ‘enhance security’ by looking for terrorists. At the same time, interconnectivity can leave systems vulnerable to attack from external threats. Infrastructure can be easily disrupted by the actions of a skilled hacker if it isn’t walled off from the outside world. A power grid that is digitally controlled with computer systems linked to the Internet can be vulnerable to someone remotely hacking in and shutting it down. A communications network could be hacked into and remotely monitored and disrupted. A nation that relies heavily on cell networks could suffer immensely if that network was attacked. During the 9/11 attacks, cellular connections in the New York City area were congested so badly that calls simply failed entirely - and that was just from an overload in usage, not from an attack. An attack could theoretically achieve the same results by effectively flooding towers with traffic, bringing them down.

Something that security and privacy are *both* at odds with would be convenience. Convenience is one of the driving factors behind the development of the aforementioned interconnectivity. The development of cars which auto connect to our cellphones via Bluetooth, thermostats that can be controlled via the Internet without getting up from the couch, or accounts that synchronize our photos and documents in the cloud across multiple devices are all examples of convenience driven technologies. These same technologies produce the kind of interconnectivity that can damper individual privacy and security.

People don’t just give up their privacy, they also sacrifice their own security willingly for their lives to be more convenient. By using the same short relatively

insecure passwords, individuals make their lives much more convenient; the flip side of this is that it also makes it much easier for the bad guys to get into their accounts. There are counters to this, however, such as password managers.

Ultimately, we must remain aware of advancing technology, keep an eye on the world, and keep the triadic balance intact. Society should never sacrifice too much security for the sake of convenience or privacy lest it result in a successful terrorism event. Privacy should also never be abandoned for the sake of security and convenience, or else a “big brother” state similar to the Soviet Union may arise. Convenience should not become the primary focus of society as it would leave both our privacy and security at risk. On the flip side, ceasing the advancement of society by ignoring anything that is considered ‘convenient’ would create a stagnant state which would be surpassed by other nations - reducing the security and privacy of the stagnant nation.

Works Cited

"Author of Patriot Act: FBI's FISA Order Is Abuse of Patriot Act." *Congressman Jim Sensenbrenner*. N.p., 06 June 2013. Web. 25 Oct. 2016.

"Cover Exclusive: Jennifer Lawrence Calls Photo Hacking a “Sex Crime”." *Vanity Fair*. N.p., Nov. 2014. Web. 25 Oct. 2016.

"Facebook Users Worldwide 2016 | Statista." *Statista*. N.p., July 2016. Web. 25 Oct. 2016. <http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>.

Grohol, John M., Psy.D. "How Well Do You Know Your Facebook Friends? | World of Psychology." *World of Psychology*. PsychCentral, 15 Mar. 2016. Web. 25 Oct. 2016. <http://psychcentral.com/blog/archives/2016/03/15/how-well-do-you-know-your-facebook-friends/>.

Heath, Brad. "USA TODAY, Others Sue FBI for Info on Phone Hack of San Bernardino Shooter." *USA Today*. Gannett, 16 Sept. 2016. Web. 25 Oct. 2016.

Holley, Peter. "Day-care Employee Fired for Facebook Post Saying She Hates ‘being around a Lot of Kids’." *Washington Post*. The Washington Post, 4 May 2015. Web. 25 Oct. 2016.

Mills, Elinor. "The Unvarnished Truth about Unsecured Wi-Fi." *CNET*. N.p., 01 Nov. 2010. Web. 25 Oct. 2016.

Purewal, Sarah Jacobsson. "Palin E-Mail Hacker Imprisoned Against Judge's Recommendation." *PCWorld*. N.p., 14 Jan. 2011. Web. 25 Oct. 2016.

Rainie, Lee, and Shiva Maniam. "Americans Feel the Tensions between Privacy and Security Concerns." *Pew Research Center RSS*. N.p., 19 Feb. 2016. Web. 25 Oct. 2016.

Sanger, David E., and Nicole Perlroth. "U.S. Said to Find North Korea Ordered Cyberattack on Sony." *New York Times*. N.p., 17 Dec. 2014. Web. 25 Oct. 2016.

Sherr, Ian, and Seth Rosenblatt. "Sony and the Rise of State-sponsored Hacking." *CNET*. N.p., 20 Dec. 2014. Web. 25 Oct. 2016.

Siboni, Gabi, and David Siman-Tov. "INSS Insight No. 646, Cyberspace Extortion: North Korea versus the United States." *Institute for National Security Studies* (n.d.): n. pag. 23 Dec. 2014. Web. 25 Oct. 2016.

Stephey, M.J. "Sarah Palin's E-Mail Hacked." *Time*. Time Inc., 17 Sept. 2008. Web. 25 Oct. 2016.

"Text - H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001." *Congress.gov*. Rep. Sensenbrenner, F. James, Jr, 10 Oct. 2001. Web. 25 Oct. 2016.

Titcomb, James. "Do You Have One of the Most Common Passwords? They’re Ridiculously Easy to Guess." *The Telegraph*. Telegraph Media Group, 23 Mar. 2016. Web. 25 Oct. 2016.