The Internet is an Open Book

Vanessa E. Ulloa

California State University, Monterey Bay

The Internet is an Open Book

The Internet is one of the most important inventions of the 20th century because it allows communication across a vast network of computers regardless of geographic location. On March 12th, 1989 Tim Berners-Lee distributed a proposal to "improve information flows [with] 'a 'web' of notes with links between them" (Berners-Lee, 2014). Tim Berners-Lee is credited with the invention of the World Wide Web while employed as an engineer at CERN, a physics laboratory. Berners-Lee's intent was to create a better network of communication for all. The "www" you often see in a web address for a website, stands for World Wide Web. However, since the 1960's there have been many attempts to create the infrastructure to support hypertext browsing, editing, electronic mail and Doug Engelbart even invented the mouse for this purpose (Connolly, 2000). The World Wide Web was released as free for all to use and since then it has expanded to support multiple browsers, such as Google Chrome and Mozilla Firefox, and support Social Media as the number of users continues to grow even a quarter of a century after the World Wide Web's invention.

Increased communication and outreach was a result of this new invention as a user from the United States could send an email to a colleague in the United Kingdom quickly and therefore that produces increased effectivity on an international level. However, the Internet's purpose has changed significantly over time, Bill Clinton even stated "[w]hen I took office, only high energy physicists had ever heard of what is called the World Wide Web... Now even my cat has its own page" (Internet Growth Statistics, n.d.). The number of Internet users as grown from 16 million in 1995 to an estimated 2,937 million users in March of 2014 (Internet Growth Statistics, n.d.). That is an increase from .4 % of the world's population to about 41%. However, this vast network also provides a new venue for new types of crime called cyber or computer

crimes. At risk is the privacy of the Internet User's data and personal information and overtime personal data such as banking information and social security numbers have become targets for cyber and computer crimes. However, there is a fine line between a computer crime and actions by an Internet User that allows personal data to be accessed. The line falls in-between, for example, hacking a banking database to access personal information, or oversharing on the user's part via a social media website or a lack of knowledge about the "at-risk" nature of the Internet itself and this brings up the issue of Internet Privacy and who is responsible for ensuring that personal data from Internet users is not stolen or accessed by other users or companies that are not supposed to have access to it. The issue of Internet Privacy has called Internet users to evaluate what is happening to their own and all user data on the Internet and asks the question: How can private user data be kept private?

The zeitgeist, or "general intellectual, moral, and cultural climate of an era" (zeitgeist, n.d.) Is changing. The social norms relating to the Internet and user data and activities has changed because of the increase of Social Media presence and because of events that have revealed government surveillance using the internet and other telecommunications. Many companies with online websites use targeted advertising to focus their ads on the internet user, the Government uses Internet surveillance to battle terrorism and cyber-crimes, but the average Internet user wants control on how their online information is collected and used. A Consumer Reports Survey revealed that "93 percent of Americans think internet companies should always ask for permission before using personal information" (Poll: Americans strongly oppose publicacy & expect online privacy — Part XV Privacy-Publicacy Series, n.d.). The Internet user expects their data to be private, especially with most mediums using personal data now using an electronic format. This includes online banking, online medical records, and online retail. Aside

from targeted ads and the data that users wish to be private, users also worry about data and content that is supposed to be seen and their 1st amendment rights. When the founding fathers authored the Bill of Rights and the Constitution in the 18th century, the Bill of Rights and amendments were put into place and practice according to the customs and technology of the time. In the 1997 court case *Reno vs. ACLU*, "the Supreme Court found Internet communication similar to newspaper publishing, which historically enjoyed broad First Amendment protection" (Lipschultz, 2014). The Supreme Court ruled this verdict because the Court determined that "websites functioned as publishers" (Lipschultz, 2014). However, the question arises of whether the 1st amendment, which traditionally protects free speech in America, applies to Social Media such as a Facebook post or a Tweet on Twitter.

There have been many reported cases of people getting arrested or questioned because of threatening Social Media posts, for example two travelers planning to travel and visit the United States had their passports detained at Los Angeles International airport and were questioned by Homeland Security. One traveler "tweeted another friend asking for some preparation before he was going to 'go and destroy America'" (Demas, 2013). The travelers were subsequently sent back to their home country after spending the night in a jail. According to CNN "[o]ne expert told CNN that anything posted online is material the government can use as evidence to arrest and charge a person" (Russell, 2013). Internet users who post on Social Media sites such as Facebook or Twitter do have the option to delete their content from their page, this ensures that other users on that website do not see that content anymore and users expect it to be deleted forever. However, "[t]he government can subpoena deleted content from social media companies, as a judge did from Twitter for a case involving an Occupy New York protester in July 2012" (Russell, 2013). The issue now goes from 1st amendment rights to 4th amendment

rights. The 4th amendment is 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" (Fourth Amendment - U.S. Constitution, n.d.). Traditionally for Law Enforcement to search a person's home or vehicle, for example, a warrant was required. Warrants are issued by judges and require probably cause in order to be executed. Law Enforcement can typically get a subpoena, instead of a warrant, when it comes to retrieving online records from databases often maintained by companies, telecommunication services and social media sites. The process of issuing a subpoena does not require probably cause or a judge, simply a signature of an Attorney who represents the course, such as a District Attorney. Subpoenas maybe issued for "[c]omputer files and downloaded material" (What Is a Subpoena, n.d.). Internet users wish their data to be private and the content that they upload to be protected as well, the 1st and 4th amendments fall under the realm of the civil liberties granted to citizens of the United States. A Civil Liberty is defined as "the right of the people to do or say things that are not illegal without being stopped or interrupted by the government" (civil liberty, n.d.).

The Internet is not only for internet users to communicate and connect with one another. Companies use the Internet to host their retail websites or host their company website for the purpose of providing information and services to a wider audience. Many of these companies use Targeted Internet Advertising that use clickstream data, cookies, search data, purchase data and profile data to create customized ads for the Internet user. Many internet users consider this as an invasion of their privacy because of the methods used to target the advertisements to users. Clickstream "refers to a record of Web pages you've visited" (Prumphrey, 2012). This data is then stored into a file called a cookie. An internet cookie is a "file that may be added to your computer when you visit a Web site and that containers information about you (such as an

identification code or a record of the Web pages you have visited)" (cookies, n.d.). Other methods include using search data which is retrieved from Search Engines such as Google or Yahoo, purchase data such as the history of purchased items on Amazon and profile data such as the content you place on your Facebook profile. However, online advertising relies on the content a user searches for or the websites that they have visited, the user essentially remains anonymous. Furthermore, "[o]nline advertisers adhere to industry codes of conduct from self-regulation groups, such as the Network Advertising Initiative and the Digital Advertising Alliance, and the governing laws of the land. They do not know who you are" (AdExchanger, 2013).

The Government of the United States also has an interest in the Internet and the activities upon it. In the Post-9/11 world there is an increased interest in preventing terrorism both domestically and foreign. The Federal Communications Commission, or the FCC, is responsible for "interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories" (What We Do, n.d.). However, the National Security Agency, or the NSA, has become more and more involved in monitoring communications by Americans every day. In the aftermath of September 11, 2001, Congress pass The Patriot Act with the goal of "arming law enforcement with new tools to detect and prevent terrorism" (The USA PATRIOT Act: Preserving Life and Liberty, n.d.). This act broadened Law Enforcement's and the Government's ability to engage in surveillance activities against suspected terrorist. This includes roving surveillance, which is "a court order allowing surveillance on a particular person allows officers to use any means available to intercept that person's communications, regardless of where the person goes" (Grabianowski, 2007). This statement can be interpreted as access to GPS location, Social Media content, Cellular Device

records and other forms of non-electronic and electronic communication. The Government and Law Enforcement agencies have an interest in preventing crimes and terrorist activities to keep the United States safe, the Patriot act and its subsequence amendments are designed to give the agencies the tools to do so. The growth of technology for communication including the growth of the internet and the number of users necessitates that Law Enforcement have tools to access communications on those mediums. Another important addition to criminal law from the Patriot act is that computer hacking in the form of cyberterrorism has increased penalties under the Computer Fraud and Abuse act. Cyberterrorism, according to the Center for Strategic and International Studies (CSIS) "has defined it as 'the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population.'" (Tafoya, 2011). But, while Computer hackers use the internet for criminal and illegal means, the Government uses the Internet in their surveillance efforts to battle terrorism and prevent crime. Law Enforcement will reach out to companies such as Google or Facebook for user data and content. Many Government forms of electronic surveillance have been revealed in the past decade as a result of the Patriot act or subsequence Surveillance acts under the jurisdiction of the NSA.

Computer hackers will often use their skillset and knowledge of the internet to gain access to private and confidential systems. What makes the acting of "hacking" illegal is that the access is unauthorized and private user data can be affected. By definition, "[c]omputer hackers are unauthorized users who break into computer systems in order to steal, change or destroy information, often by installing dangerous malware without your knowledge or consent" (Computer Hackers and Predators, n.d.). And malware is defined as "software designed to interfere with a computer's normal functioning" (malware, n.d.). While not all computer hackers

are cyberterrorists, a computer hacker's crimes are considered cyber or computer crimes. Cybercrimes include identity theft, transaction fraud, advance fee fraud, hacking, and piracy. In their 2013 Norton Report Symantec, a Computer Security company, the "global price tag of consumer cybercrime is S$113 Billion annually" (Paganini, 2013). The Norton report is based on "self-reported experiences of more than 13,000 adults across 24 countries" (Paganini, 2013). And according to the Norton Report Consumer Cybercrime costs Americans 38 billion dollars annually. Computer hackers use different techniques to obtain private user data, for example a weak password can be bypassed or if you are storing passwords for multiple accounts on your computer or smartphone. Using public-Wi-Fi provides an easy connection to the device that is connected to that Wi-Fi service. Lastly, Social Networks can be used to obtain personal data such as birthdates and addresses. (Huddleston, 2013).

Internet users struggle to keep their data private not only from Computer hackers and cybercrimes but also from Government surveillance programs. The debate over how safe private user data is, has not only produced many questions but it has also produced many answers and possible solutions. In response to Government electronic surveillance, the Government uses the argument "if you've got nothing to hide, then you've got nothing to fear" (Abdo, 2013). This argument suggests that if an Internet user is not doing anything illegal, then the user should not have to worry about watched electronically. However, this argument does not answer the question: who should be allowed to have your private data? Search Engines such as Google and Social Media sites such as Facebook retain all user data for some time in a database. This information can be mishandled by the companies or requested by the Government on a specific Internet user. However, what about deleted information? An Internet User may remove information for their social media profile such as content or a phone number, but that

information is still retained within the company's database and still available from that database. All that is needed to access Internet user data in this fashion is a subpoena, which has less restrictions than a traditional warrant (Section 215 of the Foreign Intelligence Sureveillance Act, n.d.). However, despite these facts if an Internet user is not participating in online illegal activity then there should be no concern over the content that the user uploads to the Internet or what websites the user visits. Daniel J. Solove examines the "I've got nothing to hide" argument in the San Diego Law Review where points out that "[t]he nothing to hide argument is one of the primary arguments made when balancing privacy against security" (Solove, 2007). The NSA uses electronic surveillance to monitor electronic activity and communications of people to search for possible crimes. While this preventative measure is good in major crime prevention, if content is taken out of context is that a form of internet censorship? Many advocates of Internet Privacy cite the 1st amendment and free speech as their right and civil liberty. But, what most Internet may not understand is that the 1st amendment may protect Free Speech, but it does not protect against the consequences of such. Supreme Court Justice Oliver Wendell Holmes wrote in his opinion of the 1919 case Schenck v. United States that "[t]he most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic" (Schenck v. United States, n.d.).

Another amendment that is often cited is the 4th amendment, this amendment protects against illegal search and seizure. The 4th amendment is the reason that Law Enforcement is compelled to seek a warrant from a judge and present their reasoning along with probable cause before searching a suspect's property such as their home or vehicle. However, how does this apply to user Internet data? Naturally, the inference can be drawn that public posts such as Tweets and Facebook posts, protected by the 1st amendment, are now public information and can

be used by Law Enforcement. However, even private and deleted posts on Social Networking sites are still kept and server-side copies are kept of everything. Facebook, for example, has "tens of thousands of servers holding [user] data, which as soon as it is uploaded, belongs to [Facebook] to do as and what they wish with it" (Whittaker, 2010). The question arises, is this information protected under the 4th amendment? Most Internet users are not aware of this common practice on Social Network sites and this information, past and present still exists and can be retrieved under electronic surveillance programs. Government surveillance is one way the Government is being proactive in preventing crime and terrorism. Users are generally unaffected by their data being viewed and nothing illegal being found, and the NSA claims that "the government's sweeping surveillance programs have foiled some 50 terrorist plots worldwide" (Dozier, 2013). The information on these terrorist plots have not been made public, however the assumption can be made that many lives were saved domestically and internationally.

Opponents of Government surveillance have pointed out that there are not many rules, regulations or laws to ensure that the Government continues its electronic surveillance while at the same time respecting the civil rights of Americans. The surveillance programs use a process called Data Mining, which is "the process of discovering interesting and useful patterns in relationships in large volumes of data" (Clifton, n.d.). Using this technique the NSA can process a lot of information and search for key-terms, phrases or names when acting in crime prevention. Advocates for surveillance compare the privacy argument to that of when the telephone was being used by organized crime to conduct illicit activities many years ago and how it cost a "bit of our privacy to be able to track the Mafia with wiretaps" (Gallington, 2013). The United States differs from other countries and governments where "the communications infrastructures are mostly government owned or operated" (Gallington, 2013), much like the Post Office. Naturally,

this allows for Government surveillance in a Government controlled area, whereas in the United States the telecommunications industries and communication infrastructures are not Government owned and operated. In the Summer of 2013, a former NSA contractor named Edward Snowden brought to light Government surveillance actions and programs such as PRISM, a program that "directly access[es] the servers of U.S tech giants like Google, Facebook, Microsoft and Apple, among others" (Franceschi-Bicchierai, 2014). Among the many revelations there were published from many secret NSA documents were that a "[s]ecret court orders allow NSA to sweep up Americans' phone records" (Franceschi-Bicchierai, 2014), specifically that Verizon had passed along the phone records of its customers, and presumably so had other telecommunication companies in the United States. Snowden also claimed that the NSA was undermining internet security by "forcing companies to install backdoors, hacking into servers and computers, or promoting the use weaker algorithms" (Franceschi-Bicchierai, 2014), this could possibly weaken the security of the Internet for users and leave a vulnerability open to computer hackers or cyber criminals. The information that was made public by Snowden was important because the question was asked: What are the limits to Government surveillance? However, beneficial the NSA programs are at preventing crime and terrorism, should an American's civil liberties be the cost. Recently, the director of the Federal Bureau of Investigation (FBI) James Comey asked for "more permissive government surveillance policies, claiming new encryption technologies are poised to leave law enforcement agencies 'in the dark' as they try to hunt down terrorists and child molesters" (Prupis, 2014). Comey claimed that access to personal data should be granted to the Government and Law Enforcement so that they could pursue justice within acceptable means. Comey also pointed out that advanced encryption was the equivalent of "[a] safe that can't be cracked", and that the cost of such measures would mean the police would not be able to

use “cell phone data to track down and later convict a variety of criminals—from drug kingpins to abusive parents” (Franceschi-Bicchierai, 2014). This still brings up the question: is over-sight free Government surveillance worth the cost of American civil liberties?

The Government is receiving a lot of scrutiny after Edward Snowden’s whistleblowing on the NSA and the United States Government. This scrutiny may or may not be justified, but what about the accountability of the Internet user? Many websites, including Social Media and Networking sites, ask an Internet user for a birthday prior to registration. This is in accordance with the Children’s Online Privacy Protection Act of 1998. This act places “parents in control over what information is collected from their young children online” (Complying with COPPA: Frequently Asked Questions, n.d.). The act holds businesses and websites accountable for underage users and collecting their personal information. However, the internet is a large place and the increasing presence of Social Media has not only increased the Internet usage world-wide, but the number of underage Internet users has also increased. ABC News reported that “7.5 million [Facebook] users in the U.S. are under the age of 13” (Heussner, 2011). This number was inferred from the number of parents aware of their underage child on Facebook, this does not include the users who join without their parent’s knowledge or consent. Many Internet user groups, whether they are underage or not, are over-sharing on the internet. Social Media sites make it easy for a user to share their information whether it be a birthday, picture, a vacation or any content they wish to upload.

Many opponents of Government surveillance want their privacy protected online and hold the Government accountable for protecting their civil liberties, however how accountable is the Internet user in what he or she might post on Facebook or say online? There are many consequences to oversharing online, for example The New York Times reported in that 3 men

had “burglarized more than 18 homes in the Nashua area of New Hampshire simply by checking status updates on Facebook and then pillaging the houses of victims who announced on the social network that they were not home” (Bilton, 2010). This is a real consequence to oversharing on your Social Media website, such as Facebook. However, Facebook does have some controls in place, for example a user can choose who can see their information such as workplace or birthday, and choose to enable different privacy options for their profile. Other possible results of oversharing on the Internet could be cyber-bullying or cyber-stalking, especially if you do not enable any privacy settings on the applicable website. The accountability lies with both parties—the Internet user and the Government. The Internet user can be careful of the content uploaded and shared on the Internet, and the Government is obligated to protect the civil liberties afforded to citizens in reference to their Internet data.

My personal stance on the issue of Internet Privacy, prior to writing this paper, was that if I am not doing anything wrong or illegal I should not be worried about the electronic surveillance programs and the data I post on the Internet. However, after examining both sides of the issue and conducting my research I would say that my stance has changed. I do believe that Government surveillance may be necessary for the purposes of national defense and security but I do believe that there should be limits, laws and regulations in place so that the 1st and 4th amendment rights are still protected. In light of that, the average Internet user should be accountable about how and where they are putting data on the Internet. Many sites have privacy policies and Terms & Conditions, however if “every Internet user, were they to read every privacy policy on every website they visit would spend 25 days out of the year just reading privacy policies” (Madrigal, 2012). That equates to about 76 work days if you read privacy policies for 8 hours a day. So, with these extensive Terms and Conditions and privacy policies

that often exceed 2500 words, how is the average Internet user supposed to become educated on a particular site's privacy practices or know how their data will be used on a website instead of assuming that the data will be kept safe? A solution would be to help make privacy policies and site's terms and conditions easier to the average Internet user to understand and make a better and well-informed decision about the web sites that they choose to visit. This helps the Internet user become accountable in what they are sharing, especially on popular Social Media sites such a Facebook. I believe that many Internet users using Facebook today habitually overshare, I made this assumption because I am a Facebook user myself and can view the posts that my Facebook friends make or even the posts that I have previously made over time. The Netflix documentary *Terms and Conditions May Apply*, documents how many companies that have online websites use Internet user data because it is stated in the Terms and Conditions that most users do not read and agree to. Cullen Hoback, the director of the documentary, also explores the Government connection in this situation and instances where a Facebook quote or a Tweet was responded to by SWAT because of the content taken out of context.

My main questions when thinking about Internet Privacy were does the end justify the means? Does thwarting possible terrorist attacks and groups, the end, justify the methods the Government is using to scrutinize all electronic communications? And does the security of the many outweigh the rights of the few? The assumptions I have made on this issue are based on my personal experiences on the Internet, on Social Media websites, reading articles about the NSA, reading articles about Edward Snowden and learning about how the Government uses data from Social Media sites for surveillance purposes. I am not an expert in the matter of the Internet, the NSA nor do I understand a lot of the legal language in the Terms and Conditions.

A solution to this issue would be to allow users to truly opt out of sharing. That means that if a Facebook user removes their cell-phone number from their profile page, that data is truly deleted from Facebook server-side. Most Internet users are not aware that information on a website is not truly deleted when that button is clicked. The assumption is made because it no longer appears on the particular website. In addition, most internet and communication information can be retrieved with a subpoena which does not require the probable cause that a warrant and is a much easier process to obtain. For example, a warrant is required to wiretap a phone call, but only a subpoena is required "to monitor the numbers for incoming and outgoing calls in real time, as well as the duration of the calls" (Meyer, 2014). Many cell phone companies also will respond to a request for a cell-phones location, typically charging to start and continue tracking the device. The justification is that Law Enforcement does "not need a search warrant to obtain your personal documents if you have already shared them with somebody else" (Zwerdling, 2013). This logic not only applies to telecommunication companies, but also bank and credit card companies, because the assumption is that the customer has shared their purchase information with the bank or credit card company by using the debit or credit card versus cash. The U.S. Department of Health, Education and Welfare established The Code of Fair Information Practices in 1973. The code states 5 principles:

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. (The Code of Fair Information Practices, n.d.). These principles can be used as guidelines for future surveillance law and laws relating to how companies treat user data on the Internet. It is possible to create and modify existing surveillance laws and also to create laws for companies that store user data online. However, additional steps can be taken by Internet users to protect their data on the Internet, one way would be to limit what data is being uploaded to Social Media and what interactions are taking place. Additionally, future and current Internet users should be educated on how data is treated on the Internet and essentially be aware of the risks of the Interest whether it be a cybercrime or the knowledge that the Government is conducting electronic surveillance. It is possible to take steps forward to modify existing policies and to educate Internet users, though the result will not be immediate.

However, assumptions are made based on the information that is available at the time. It is a certainty that the Government will continue the electronic surveillance programs in place with the NSA and FBI, but the concession must be made that the average Internet user and American citizen does not really know the true occurrences within these agencies. Without the full knowledge, changing existing policies could have the adverse effect of encouraging more cybercrime and computer hackers breaking into company and government databases. So, the compromise must be reached in the future and having better educated Internet users on the issues of the internet and privacy can help achieve a better compromise for all parties involved.

The Government and NSA is currently operating on the logic that "if you have nothing to hide, you have nothing fear" (Abdo, 2013). and that the price for national security and liberty are the loopholes in the civil liberties granted by the 1st and 4th amendment. There should be limits to Government surveillance and oversight to ensure that justice is met but also that rights are not violated and that accountability is established. However, Internet users are ultimately responsible for the data that they put on the Internet and the content that they wish to share, so the accountability is also shared with them. In time the true impact of Edward Snowden's revelations on Internet privacy and possible changes to Government policy will be revealed and questions will be answered regarding how Internet users and companies evaluate what is done with personal user data and how can it be kept private.

References

Abdo, A. (2013, September 13). *Surveillance: You may have 'nothing to hide'-but you still have something to fear*. Retrieved from MSNBC: http://www.msnbc.com/msnbc/surveillance-you-may-have-nothing-hide

AdExchanger. (2013, October 9). *Targeted Online Advertisements: A Threat To Personal Identity And Security?* Retrieved from AdExchanger: http://www.adexchanger.com/data-driven-thinking/targeted-online-advertisements-a-threat-to-personal-identity-and-security/

Berners-Lee, S. T. (2014, March 11). *On the 25th anniversary of the web, let's keep it free and open*. Retrieved from Google Official Blog: http://googleblog.blogspot.com/2014/03/on-25th-anniversary-of-web-lets-keep-it.html

Bilton, N. (2010, September 12). *Burglars Said to Have Picked Houses Based on Facebook Updates*. Retrieved from The New York Times: http://bits.blogs.nytimes.com/2010/09/12/burglars-picked-houses-based-on-facebook-updates/?_php=true&_type=blogs&_r=0

civil liberty. (n.d.). Retrieved from Merriam-Webster: http://www.merriam-webster.com/dictionary/civil%20liberty

Clifton, C. (n.d.). *Data Mining*. Retrieved from Encyclopedia Britannica: http://www.britannica.com/EBchecked/topic/1056150/data-mining

Complying with COPPA: Frequently Asked Questions. (n.d.). Retrieved from Bureau of Consumer Protection: http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions

Computer Hackers and Predators. (n.d.). Retrieved from Webroot: http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-hackers

Connolly, D. (2000). *A Little History of the World Wide Web*. Retrieved from W3: http://www.w3.org/History.html

cookies. (n.d.). Retrieved from Merriam-Webster: http://www.merriam-webster.com/dictionary/cookies

Demas, N. (2013, July 17). *8 Social Media Users Arrested For What They Said Online*. Retrieved from Policy Mic: http://mic.com/articles/54961/8-social-media-users-arrested-for-what-they-said-online

Dozier, K. (2013, June 18). *NSA: Surveillance Programs Foiled Some 50 Terrorist Plots Worldwide*. Retrieved from Huffington Post: http://www.huffingtonpost.com/2013/06/18/nsa-surveillance_n_3460106.html

Fourth Amendment - U.S. Constitution. (n.d.). Retrieved from Find Law: http://constitution.findlaw.com/amendment4.html

Franceschi-Bicchierai, L. (2014, June 5). *The 10 Biggest Revelations From Edward Snowden's Leaks*. Retrieved from Mashable: http://mashable.com/2014/06/05/edward-snowden-revelations/

Gallington, D. J. (2013, September 18). *The Case for Internet Surveillance*. Retrieved from US News: http://www.usnews.com/opinion/blogs/world-report/2013/09/18/internet-surveillance-is-a-necessary-part-of-national-security

Grabianowski, E. (2007, July 06). *How the Patriot Act Works*. Retrieved from HowStuffWorks: http://people.howstuffworks.com/patriot-act.htm

Heussner, K. M. (2011, May 10). *Undersage Facebook Members: 7.5 Million Users Under Age 13*. Retrieved from ABC News: http://abcnews.go.com/Technology/underage-facebook-members-75-million-users-age-13/story?id=13565619

Huddleston, C. (2013, September 10). *6 Ways You Invite Hackers to Steal Your Personal Information*. Retrieved from Kiplinger: http://www.kiplinger.com/article/credit/T048-C011-S001-6-ways-you-invite-hackers-to-steal-your-personal-i.html

Internet Growth Statistics. (n.d.). Retrieved from Internet World Stats: http://www.internetworldstats.com/emarketing.htm

Lipschultz, J. H. (2014, March 17). *Social media and the First Amendment*. Retrieved from Huffington Post: http://www.huffingtonpost.com/jeremy-harris-lipschultz/social-media-and-the-first-amendment_b_4976694.html

Madrigal, A. C. (2012, March 1). *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*. Retrieved from The Atlantic: http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

malware. (n.d.). Retrieved from Merriam-Webster: http://www.merriam-webster.com/dictionary/malware

Meyer, T. (2014, June 27). *No Warrant, No Problem: How the Government Can Get Your Digital Data*. Retrieved from Pro Publica: http://www.propublica.org/special/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data

Paganini, P. (2013, October 9). *2013 Norton Report, the impact of cybercrime according to Symantec*. Retrieved from Security Affairs: http://securityaffairs.co/wordpress/18475/cyber-crime/2013-norton-report.html

Poll: Americans strongly oppose publicacy & expect online privacy — Part XV Privacy-Publicacy Series. (n.d.). Retrieved from NetCompetition.org: http://www.netcompetition.org/congress/poll-americans-strongly-oppose-publicacy-expect-online-privacy-part-xv-privacy-publicacy-series

Prumphrey, C. (2012, September 2012). *How do advertisers show me custom ads?* . Retrieved from HowStuffWorks: http://computer.howstuffworks.com/advertiser-custom-ads1.htm

Prupis, N. (2014, October 17). *FBI Director: Government Surveillance 'Enhances Liberty'*. Retrieved from Common Dreams: http://www.commondreams.org/news/2014/10/17/fbi-director-government-surveillance-enhances-liberty

Russell, L. (2013, April 24). *When oversharing online can get you arrested*. Retrieved from CNN Tech: http://www.cnn.com/2013/04/18/tech/social-media/online-oversharing-arrests/

Schenck v. United States. (n.d.). Retrieved from Cornell University Law School: http://www.law.cornell.edu/supremecourt/text/249/47

Section 215 of the Foreign Intelligence Sureveillance Act. (n.d.). Retrieved from IC on the Record: http://icontherecord.tumblr.com/topics/section-215

Solove, D. J. (2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Deigo Law Review, Vol. 44*, 745-771.

Tafoya, W. L. (2011, November). *Cyber Terror*. Retrieved from FBI.gov: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

The Code of Fair Information Practices. (n.d.). Retrieved from Electronic Privacy Information Center: http://epic.org/privacy/consumer/code_fair_info.html

The USA PATRIOT Act: Preserving Life and Liberty. (n.d.). Retrieved from Preserving Life and Liberty, Justice.gov: http://www.justice.gov/archive/ll/highlights.htm

What Is a Subpoena. (n.d.). Retrieved from Find Law: http://litigation.findlaw.com/going-to-court/what-is-a-subpoena.html

What We Do. (n.d.). Retrieved from Federal Communcations Commission: http://www.fcc.gov/what-we-do

Whittaker, Z. (2010, April 28). *Facebook does not erase user-deleted content*. Retrieved from ZDNet: http://www.zdnet.com/blog/igeneration/facebook-does-not-erase-user-deleted-content/4808

zeitgeist. (n.d.). Retrieved from Merriam-Webster Online Dictionary: http://www.merriam-webster.com/dictionary/zeitgeist

Zwerdling, D. (2013, October 2+). *Your Digital Trail: Does The Fourth Amendment Protect Us?* . Retrieved from NPR: http://www.npr.org/blogs/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us