Reverend Jerry L Cason Jr.

Dr. Phil Lunsford

ICTN4040

April 17th 2017

Privacy Concerns in Modern America

The fourth amendment to the constitution promised the right to privacy for every American citizen. Protections were put in place to help ensure these rights wouldn't be violated. For instance, the United States government needs probable cause and a warrant to search things like our homes and person. When it comes to the Internet and technology, these types of protections don't seem to exist. For years the government has been fighting hard to strip the privacy of American citizens online. The legality of these programs has appeared to be of no concern to the government which has been caught time and again attempting to hide these tactics from the American populace.

Before discussing the legality of these privacy invasions it is important to mention several of the laws that pertain to privacy online. One of which is the Electronic Communications and Privacy Act or the ECPA which was passed in 1986. Many proponents interested in reforming the ECPA state that the law doesn't do nearly enough to protect the electronic files of American citizens. The ECPA allows the government access to online communications such as data stored in a public cloud providers databases, emails, even messages sent through various communication platforms after 180 days with only a subpoena. In the words of Robert Holleyman, former president of the Business Software Alliance, "A paper letter sitting in your home or office drawer has a significantly higher level of constitutional protection compared to an email right now," clearly a cause for alarm for those interested in online privacy (Butler).

The Foreign Intelligence Surveillance Act or FISA is another important piece of legislation that received an amendment in 2008. This amendment granted United States companies immunity from being sued by their customers when the company was complying to a surveillance request made by the government. This protection existed regardless of the legality of the request made by the government. This enabled the United States government to make requests for records of the customers of these companies without the companies having to worry about repercussions. The government stated this was done in an effort to improve national security. While the success of laws like this in terms of protecting citizens could be debated, this legislation had the effect of encouraging these companies to cooperate with government information requests (MacKinnon).

It would be difficult to discuss privacy laws in the United States of America without mentioning what many privacy advocates feel to be the most egregious, The Patriot Act. This legislation passed after the terrorist attacks that the country suffered on September 11th, 2001. The goal was to improve national security by making it easier for the government to intercept and analyze communications in an effort to stop future attacks and protect the American public. It enabled the Federal Bureau of Investigation to obtain numerous records without a court order. These records included financial and credit records as well as telecommunication records. While the government is required to properly document the wiretapping of phone lines, no such protection existed for Internet based communications. It wasn’t until 2009 when Nick Merrill, with help from the American Civil Liberties Union, managed to challenge a provision of the Patriot Act concerning these gag orders that enabled companies to inform their customers about some aspects of information requests. The Electronic Frontier Foundation published a report in 2011 which stated that between the years of 2001 and 2008 the FBI may have used this provision to violate the rights of American citizens nearly 40,000 times (MacKinnon).

With the government passing laws to legalize surveillance and attempting to stop companies from informing their customers of information requests, it may come as no surprise that there were numerous programs created in secrecy to monitor American citizens online. Without the help of whistle-blowers willing to speak out about these programs the American public may never have learned what was being done with their online data. These men and women had knowledge of what was being done, and in some cases helped with the setup of these programs. Many of them struggled with the moral dilemma of invading their countryman's privacy as well as the legality of these programs. These issues led some to speak out and notify the public of the surveillance tactics being used by the United States government and governments around the world.

One such man was William Binney a former Defense Department foreign signals intelligence agency employee. William Binney worked with the Defense Department for 32 years before resigning. His resignation came after he felt that the NSA was purposefully violating the constitutional rights of American citizens. Binney stated that he helped to supervise the creation of an NSA program named “Thin Thread”. His sworn declaration of facts claimed that this program was designed to discover international connections between people using their Internet communications. He stated that originally, as some of the data obtained belonged to American citizens, this domestic data was encrypted to protect their privacy until a warrant was obtained. After the attacks on September 11th, 2001, the encryption of that data was no longer a priority and data was being collected and analyzed by the Thin Thread program for both foreign and domestic communications. This new policy to remove the privacy protections for domestic data was called the President’s Surveillance Program or PSP (Kelley).

Thomas Drake, a senior executive at the National Security Agency from 2001 to 2008 confirmed much of what was said by William Binney. He stated the government had implemented technology at key points in Americas network infrastructure to analyze information using the Thin Thread program developed by William Binney. Responses on the program according to Drake were rarely done in a form that could be recorded or saved so as to retain no records. According to Drake he was instructed to install equipment usually used to monitor foreign communications in a way that allowed for the domestic surveillance of American citizens. Drake stated numerous times he’d tried to bring up the legality of these programs but that those in charge seemed not to care about the legality of their work (FRONTLINE).

In 2006 Mark Klein, an AT&T technician turned whistle-blower, helped to explain just how deep these surveillance programs were embedded into America's network infrastructure. According to Klein the United States government was enlisting the help of companies such as AT&T and other large communications companies to spy on American citizens. Klein stated that part of his duties while working at AT&T were to connect key Internet circuits that enabled communication online to a splitter located in a room at an AT&T office in San Francisco. He stated that there were rooms like this installed in numerous other American cities around the country. These circuits allowed the government to siphon data from American citizens and store it before sending the data to its destination. Much of these statements were denied. It wasn't until June 2013 that leaked documents vindicated Mark Klein and led credence to his statements (Kravets).

In February of 2014 Power Point slides were leaked from American and British intelligence agencies. The slides revealed that the two countries were using capabilities found in popular mobile apps as well as tools built into mobile handsets to surveil the populace. The leaked information showed that the US and UK were attempting to develop programs that allowed them to intercept mobile data as it actively streamed through the Internet from mobile devices. The data collected included phone call logs, emails, web surfing activity and more. The metadata being collected allowed these agencies to determine various characteristics of people such as their location, gender, age and much more (Levine).

The United States government frequently states that these surveillance programs are designed to improve national security and keep American citizens safe. The efficiency of these bulk information collection programs in achieving those goals has been called into question by several studies. A report by the New American Foundation discovered that "Of the 225 individuals charged as al-Qaeda affiliated or inspired for acts, or potential acts, of terrorism since 9/11 only a small fraction of those cases stemmed from information made possible by NSA surveillance," (Queally). The findings stated that the problem with these programs was not the amount of information obtained. Instead the New American Foundation found that it was necessary to find better ways to analyze the information being obtained (Queally).

Governments aren't the only ones attempting to gather as much data as possible from Internet users. There is a sizable business dedicated to analyzing user traffic and using this information to create comprehensive profiles on these users. Companies such as Facebook collect a myriad of data about their users in an effort to offer targeted advertisements and content relevant to an individual users tastes. Nearly everything done on Facebook is monitored and collected. Users aren't even required to be on Facebook for information to be collected. Just being logged into a Facebook account and visiting a website with Facebook connectivity features can send that information right back to Facebook's servers. Facebook then offers these information profiles to other companies so that they can create targeted advertisements for groups of people (Kim). Choosing not to own a Facebook account or at the very least remembering to logout of it before navigating somewhere else is one way to keep your information from Facebook. Another important step is to go through the privacy settings offered for Facebook accounts and select what you do or do not wish to be shared and who it should be visible too.

Collecting user data for the purposes of targeted advertisements has shown itself to be extremely fruitful. From September 2015 to September 2016 Google's ad business represented an astounding $76.1 billion in revenue (Chafkin). With money like this flowing in from user data collection other companies have been clamoring for a piece. On April 3rd 2017, President Donald Trump signed into law a piece of legislature that repealed some hard-fought Federal Communications Commission privacy guidelines. The rules that were repealed would have required Internet service providers to get consent from their users before offering up various information to companies interested in user data ("Trump"). Privacy advocates claim that the removal of these protections will now allow ISP's to sell their customers online information to companies in bulk. There are also worries that this legislation will only strengthen the capabilities of blanket government surveillance in America (Pressman).

With these revelations it becomes important for the average citizen to understand how they can protect their privacy while online. Luckily as the surveillance tactics have improved so too have the tactics used by privacy advocates to protect themselves in an increasingly virtual world. Unfortunately even when correctly using many of these tools to combat surveillance, withstanding the direct attempts of any nation-state to monitor communications can be extremely difficult if not impossible. The controversy surrounding The Onion Router, abbreviated as TOR, is an excellent example of government efforts to combat and find flaws in commonly used privacy tools.

Originally developed by the Naval Research Laboratory, TOR was designed with the protection of U.S. Naval communications in mind (“Who Uses Tor?”). At its core TOR is a network of relay servers run by volunteers that enables people to bounce their communication securely through encrypted virtual tunnels around the world. The goal is to anonymize network traffic and avoid traffic analysis in a way that makes finding the originator of the data difficult. TOR is used by privacy advocates, journalists around the world and those looking to circumvent government surveillance programs. It has even been used to allow whistle-blowers to dump information and contact journalists with sensitive information privately ("Tor: Overview"). The relative success of TOR has come much to the dismay of governments around the world interested in surveilling their citizens.

To combat TOR the United States government began looking for ways to de-anonymize the software’s users. In 2013 Edward Snowden, a former NSA employee, leaked numerous top-secret documents from the NSA. Some of these documents revealed how the NSA had been attempting to compromise the abilities of the TOR network. Much of the ideas to compromise the TOR network were deemed impractical with the resources the NSA had. Though they had managed to demonstrate proof-of-concept attacks, these attacks frequently required access to the relay servers used to transmit data over TOR. As the NSA found they would be unable to control enough servers for this tactic, they instead turned their attention to other tools frequently used in conjunction with TOR. By exploiting a vulnerability in Firefox, a browser packaged with the Tor Browser Bundle that directs traffic over the TOR network by default, the NSA found some success. The NSA found the vulnerability allowed them to install software to the users computer without the user's knowledge. The malicious software being run allowed them to monitor the victims file system and keystrokes as well as their web browsing habits (Gingerich).

Encryption is another vital tool used to combat unwanted surveillance. We use encryption to protect our information online when doing things like signing into a website, purchasing an item, or performing some online banking. When visiting websites we typically utilize the Hypertext Transfer Protocol Secure, abbreviated as HTTPS, to protect our communications. HTTPS helps prevent an unwanted third-party from tampering with or viewing the communication between a web host and it's users. This helps combat man-in-the-middle attacks among other attacks as well as encrypts the data sent between the two communicators. In the context of this paper, HTTPS is useful because visiting an HTTP version of a website can leak information about a users browser activity and offer more data to entities looking to create a user profile of a particular user. HTTPS uses separate protocols known as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to help ensure the integrity of information (Basques).

While encryption is vital to protecting information sent and received online it is just as useful in securing offline information stored on computers and phones. There are numerous algorithms to help encrypt data, including DES, 3DES, RSA, and the more modern AES. In a study done by Gurpreet Singh and Supriya, several popular encryption standards were analyzed including RSA, DES, 3DES, and AES. The study determined that symmetric algorithms such as AES were speedier than asymmetric algorithms like RSA. In the research and literature survey that they performed, AES was determined to be the best algorithm in terms of "speed, time, throughput and avalanche effect," (Singh). The avalanche effect referred to is equal to the number of flipped bits in ciphered text divided by the number of bits in ciphered text. AES is also the encryption standard recommended by NIST to replace the older DES standard. Choosing the right encryption algorithm to protect sensitive data can require research as some algorithms perform tasks better than others (Singh). Usually choosing a strong encryption standard like AES with a key-length appropriate to the sensitivity of the data can be enough to thwart those looking to crack through the encryption and view the plaintext data.

Using a Virtual Private Network or VPN can be another way to anonymize and protect private data online. VPNs have many uses but the biggest use to mention here is the ability of individuals to use them to secure and encrypt their data online. This can be especially helpful in situations when a trusted network isn't available and users have to connect to public networks. Usually these connections are handled via VPN clients. The VPN clients usually require users to provide credentials to an account that the user is paying for. After logging in trusted keys are exchanged between the users device and a VPNs server. If both the user device and the VPN server determine the keys are authentic and there hasn't been any tampering, the user will be allowed to transmit their data over the VPNs encrypted network. Not all VPNs are made equal, it's important to find one that uses strong encryption protocols. When taking user privacy into account it also becomes necessary to research what information the VPN collects on its users and the laws of the country where the VPN servers are located (Henry).

Securing devices with a firewall and anti-virus software is another important step to keeping data safe. Malware can be used to identify a device and monitor the activity performed on it. It is also important to limit exposure to social media and control the amount of information you chose to release (Branson). A good rule of thumb is to operate under the assumption that everything posted online will be visible to anyone who wants to view it. While not necessarily true it can help get users into the mindset of avoiding the pitfalls of over-sharing online. Another way to protect your data is to choose strong passwords containing letters, numbers, and special characters that wouldn't be easily guessed or found in a dictionary. Randomizing passwords can be easy with password managing software such as KeePass which allows users to store all their passwords into an encrypted password bank.

Without a change in mindset regarding privacy issues by the United States government the privacy of American citizens online will continue to be in danger. The government will be free to continue these blanket surveillance programs and attempts to undermine privacy tools. Washington desperately needs to update the laws already in place for the 21st century and abide by these legislation's. This includes updating laws concerning the bulk collection and selling of user data by companies such as Facebook. Until such a time, it’s clear that the battle between those who wish to protect themselves from surveillance online, and those who wish to surveil them, will continue to rage on-wards.

Works Cited

Basques, Kayce. "Why HTTPS Matters." *Google*. Google, n.d. Web. 13 Apr. 2017. https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https.

Branson, James. "7 Powerful Ways to Maintain Your Privacy and Integrity Online." *Collective Evolution*. N.p., 13 June 2013. Web. 14 Apr. 2017. http://www.collective-evolution.com/2013/06/13/7-powerful-ways-to-maintain-your-privacy-and-integrity-online/.

Butler, Brandon. "4 Internet privacy laws you should know about." *Network World*. Network World, 12 Mar. 2013. Web. 17 Mar. 2017. http://www.networkworld.com/article/2164315/lan-wan/4-internet-privacy-laws-you-should-know-about.html.

Chafkin, Max, and Mark Bergen. "Google Makes So Much Money, It Never Had to Worry About Financial Discipline." *Bloomberg*. Bloomberg, 08 Dec. 2016. Web. 3 Apr. 2017. https://www.bloomberg.com/news/features/2016-12-08/google-makes-so-much-money-it-never-had-to-worry-about-financial-discipline.

Henry, Alan. "Why You Should Be Using a VPN (and How to Choose One)." *Lifehacker*. Lifehacker.com, 05 Sept. 2012. Web. 12 Apr. 2017. http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs.

Gingerich, David. "The Effectiveness of the Tor Anonymity Network." *Lewis University*. Lewis University, 30 Nov. 2014. Web. 11 Apr. 2017. http://www.cs.lewisu.edu/mathcs/msisprojects/papers/Tor_DavidGingerich.pdf. *

Kelley, Michael B. "NSA Whistleblower Says The Feds Are Gathering Data On Nearly Every US Citizen." *Business Insider*. Business Insider, 17 July 2012. Web. 20 Mar. 2017. http://www.businessinsider.com/nsa-whistleblower-says-the-government-is-gathering-data-on-every-us-citizen-2012-7.

Kim, Larry. "You Won't Believe All the Personal Data Facebook Has Collected on You." *Inc.com*. Inc., 12 Sept. 2016. Web. 1 Apr. 2017. https://www.inc.com/larry-kim/you-wont-believe-all-the-personal-data-facebook-has-collected-on-you.html.

Kravets, David. "NSA Leak Vindicates AT&T Whistleblower." *Wired*. Conde Nast, 27 June 2013. Web. 1 Apr. 2017. https://www.wired.com/2013/06/nsa-whistleblower-klein/.

Levine, Yasha. "Surveillance Valley Has Put a Billion Bugs in a Billion Pockets." *Alternet*. N.p., 12 Feb. 2014. Web. 25 Mar. 2017. http://www.alternet.org/news-amp-politics/surveillance-valley-has-put-billion-bugs-billion-pockets.

MacKinnon, Rebecca. "We're losing control of our digital privacy." *CNN*. Cable News Network, 29 Jan. 2012. Web. 19 Mar. 2017. http://www.cnn.com/2012/01/26/opinion/mackinnon-sopa-government-surveillance/.

Pressman, Aaron. "Privacy Groups Sound Alarm on Repeal of Internet Privacy Protection." *Privacy Protection Groups Blast Repeal of FCC Internet Rules | Fortune.com*. Fortune, 29 Mar. 2017. Web. 10 Apr. 2017. http://fortune.com/2017/03/29/privacy-advocates-decry-repeal-internet-privacy/.

Queally, Jon. "Bulk Spying Is Not Effective Terrorism Prevention Tactic: Report." *Common Dreams*. N.p., 13 Jan. 2014. Web. 17 Apr. 2017. https://www.commondreams.org/news/2014/01/13/bulk-spying-not-effective-terrorism-prevention-tactic-report.

Singh, Gurpreet, and Supriyah. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." *International Journal of Computer Applications* 67.19 (2013): n. pag. Semantic Scholar, Apr. 2013. Web. 13 Apr. 2017. https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf. *

"The FRONTLINE Interview: Thomas Drake – United States of Secrets." *PBS*. Public Broadcasting Service, n.d. Web. 20 Mar. 2017. http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-drake/.

"Tor: Overview" *Tor*. Tor Project, n.d. Web. 13 Apr. 2017. https://www.torproject.org/about/overview.html.en.

"Trump signs repeal of US broadband privacy rules." *CNBC*. NBC Universal, 03 Apr. 2017. Web. 10 Apr. 2017. http://www.cnbc.com/2017/04/03/trump-signs-repeal-of-us-broadband-privacy-rules.html.

"Who Uses Tor?" *Tor*. Tor Project, n.d. Web. 13 Apr. 2017. https://www.torproject.org/about/torusers.html.en.