Who's Watching You?

The Trade off Between Privacy and National Security

Rowan Bittner

"In a time of turbulence and change, it is more true than ever that knowledge is power."

- John F. Kennedy in 1963.

Knowledge is power. A common saying prevalent throughout the years, that can be applied to almost any setting including the one of privacy and national security. There has always been a tradeoff between National Security and the privacy of the people. If a state is to provide more security over its people, against instate actors, there must be an increase of monitoring on its population. Ever since the Internet became easily accessible it has been used as a form to easily and instantly communicate with people across the country. No longer were you limited to people in your general area, or waiting for your letter to be sent. Email, text, and social media had taken over the means of communication. This in turn gave the government an incentive to justify the tracking and spying of everything done by a user on the internet. This begs the question of how much data is the government collecting on us? Have we hit a point of diminishing returns where their amount of data collection just isn't worth it?

An Increase in Surveillance

Security leaks had been prevalent throughout history and so the National Security Agency (NSA) was founded in 1952 in an effort to combat this while at the same time to find Communist sympathizers inside the United States. This originally started with in person spying and tapping phone lines, as the internet was not available. Throughout the 20th century there were numerous security breaches that have caused the NSA to change the way they do internal

moderation, however arguably the most influential events are those of terrorist attacks more specifically the attack on the World Trade Center on September 11th, 2001.

The events that took place on and after September 11th would go on to change how national security, and in turn your privacy, was handled forever. Not only did we see an increase of in person security (airport security, bag checks, car scans), we also saw an increase in digital security. Immediately after the attacks then President, George W. Bush provided twenty billion dollars on security and intelligence[1]. This funding went into traditional security and the relatively new cyber security. In 2002, the NSA launched its program called ‘ data mining ‘ with the purpose of investigating electronic transaction data by collecting personal information of users who recently purchased items that might be used to make weapons. In the same year President Bush authorized the NSA to listen in to phone calls and read emails of American’s without the need of a warrant. It took three years for the public to find out about this as in 2005 it was exposed and two years later, under the pressure of the press and the people, President Bush ended the warrantless program in 2007[2]. To add on to the list of actions made, the Department of Homeland Security (DHS) was signed into action on October 8th, 2001 with Executive Order 13228. The DHS is a somewhat broader version of the NSA, investigating potential attacks both foreign and domestic. This addition of a new intelligence agency meant that a large increase of domestic surveillance was imminent. The National Cybersecurity and Communications Integration Center (NCCIC), a branch of the DHS, that is responsible for

---

[1]Taylor, 2013 “The Evolution of Airline Security Since 9/11”

[2]Heilgenstein & O'Brien, 2018 “A Brief History of the NSA: From 1917 to 2014”

working directly with private sector companies by collecting information on the users[1]. This department is still at full operation, collecting information on us, to this day. Executive Orders 13224 and 13231 signed into action soon after the attacks also affected and diminished the privacy of the American people, by allowing government agencies to collect information on those for the "protection of the private sector" and the "interest of national security". These include access to the new CCTV security cameras that were being pressured for business to install, putting everyone under constant surveillance. There has always been suspicion of someone watching our every move, and this was confirmed to be our own government, in 2013 by Edward Snowden.

Exposed

Edward Snowden, better known as just Snowden, is an American veteran, worked for the CIA and NSA, and most of all an infamous whistleblower. He is now forced to take refuge from the United States government in Russia, as he is considered a traitor by US officials. Snowden is most famous for leaking thousands of documents in 2013 exposing the US government for spying on its citizens by means of common household technology, including telephones, social media, and webcams. While working in the government programs, Snowden was granted top secret access to confidential documents. Among these documents he discovered that the government was actively invading the privacy of millions of civilians. This was being done without consent or knowledge of those being watched, or even the knowledge of our

---

[1]Bush, 2001 "Critical Infrastructure Protection in the Information Age"

representatives[1]. After much consideration and preemptively fleeing to China, Snowden leaked the documents and his information to multiple different reporters. He has yet to return to the United States, even eight years later.

One of the largest programs that Snowden was able to leak was about a program entitled PRISM. PRISM went much further than the metadata that was collected by other programs that have been previously revealed by other whistleblowers. Metadata is general information, for instance general location and if you were in contact with someone and for how long. However, PRISM data collection went much further than this, collecting specific content of what you were sending, to whom you were sending that to, and allowed direct access to internet giant's servers including Google, Facebook, Microsoft, and Apple[2]. These companies are strong- armed into complying with the NSA, some reports even saying that these company data centers were broken into by the NSA[3]. Some companies did try to contest these actions bringing them to court, however the courts that heard these hearings were secret government run, used for cases that required confidentiality, and that rarely sided against the government.

The government knew exactly what it was doing by trying to come after these technology companies. An article from ProPublica in 2013 revealed that the NSA had a specific program, titled Bullrun, to intentionally mislead private companies in efforts to diminish encryption standards. The NSA pushed for either very easily broken encryption or for backdoors to be implemented. These backdoors would be used for the government to be able to easily access any information that a company had on its user. The term backdoor is used because it is meant as an easy entry to information while not being obvious to the average user, the flaw here

---

[1, 3]Snowden, 2014 "Here's How We Take Back the Internet"

[2]Ray, 2021 "Edward Snowden"

is that if there is a way for someone to unlock that backdoor there is a way for anyone to unlock it[1]. This means that not only our government would have easy access to information, it also allows someone with enough time and the skill set access, whether this be an individual or another state actor. Recently we have seen large tech companies fight against the use of their user's information. In 2016 the FBI attempted to gain access to private information on an Apple iPhone. Apple and later the Judge denied them the information based on the grounds that it was an unconstitutional invasion of[2]. We have seen these and continue to see these attempts by government agencies to invade the privacy of people, whether it is asking directly for it or trying to force large companies, like Apple, to provide passwords to people under investigation.

Instead of attempting to force companies to include vulnerable backdoors that have the possibility of easily being breached, the law of a certain level of encryption should be put in place. Data breaches are no stranger to large companies, and luckily most companies have independently taken steps to secure its user's data. However there are no such laws forcing companies to keep private information private. One of the most recent notorious data breaches that happened to a private company was Yahoo! in 2013 and 2014. The internet giant revealed in 2016 that back in 2013 and 2014, it's users were victims of a massive data breach affecting upwards of one billion users[3]. These are currently the largest known security failures of a company's computer network. Numerous sensitive information was now in the hands of complete strangers, including names, telephone numbers, dates of birth, passwords, and

---

[1]Larson, 2013 " The NSA's Secret Campaign to Crack, Undermine Internet Security"

[2]The Guardian, 2016 " Apple Case: Judge Rejects FBI Request For Access to Drug Dealer's iPhone"

[3]Goel & Perlroth, 2016 " Yahoo Say s1 Billion User Accounts Were Hacked"

security answers. This all happened because Yahoo failed to keep up to date with its security measures. If there were laws requiring large companies with billions of users to keep user information under some standard level of security and encryption, that information most likely would have never been leaked.

While the ethicacy of the NSA is up to the individual, after Congress granted border powers in 2008 there were still clear privacy rules and regulations that were broken. NSA officials had been witnessed lying in front of Congress on what information is collected, what they have access to, and what data they can provide. In 2013 it was revealed that the NSA has had at least 2,776 'incidents' in respect to surveillance of Americans or foreign targets in the United States in one year alone[1]. A majority of these errors resulted in the 'unintended' interception of thousands of emails and telephone calls. The largest one being when it accidentally monitored the telephone calls of everyone in DC because the area code for Egypt was misread. It was also reported that NSA officials were told to not report these errors in surveillance and to remove details in favor of more general terms[2]. Even going as far as hiding a collection method from the Foreign Intelligence Surveillance Court, that would later rule it unconstitutional after its findings. Even though it has been found by two independent White House panels, that these programs have never stopped a single terrorist attack that was imminent to the United States[3].

The NSA, FBI, DHS, Law Enforcement and every other government agency would advocate the use of this level of surveillance to protect you and to protect our national security. It

---

[1]Gellman, 2013 "NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds"

[2,3]Snowden, 2014 " Here's How We Take Back the Internet"

is no secret that information is power, so for an entity to gain power it must gain information. Terrorism has been the catalyst for most major privacy and security changes. We saw this with the events after 9/11 with the numerous executive orders passed. We also saw this after the Boston Marathon Bombing with bills like H.Res. 164 that allowed sharing of information on cyber security threats and "other purposes." The FBI had come to Congress multiple times before these terrorist acts but were turned down. It wasn't until these agencies took advantage of a rightfully emotional country to secretly enact and justify these unnecessary surveillance methods[1].

Even the devices that we purchase ourselves are acting as ways to collect personal information. Popular virtual assistants, like Amazon's Alexa or Apple's Siri, use voice recognition and recording on a daily basis. Multiple data leaks and allegations have risen over the years calling out companies that have collected and stored user's personal information and selling it off to the highest bidder. Amazon admitted in 2019 to Senator Christopher Coons, that it "maintains Alexa recordings indefinitely (unless a user manually comes in and deletes them)."[2] This means that at any point a third party, including the government, is able to go to Amazon and retrieve personal recordings that happen in your private space without your explicit consent.

As society advances further and further into the technological age we see a necessity to continually update our privacy standards. Over the very recent history we have seen a massive trickle down effect in technology. Resources that would have cost millions just twenty years ago are now widely available and at a fraction of the cost. The case *United States v. Jones* explored in

---

[1]Snowden, 2014 "Here's How We Take Back the Internet"

[2]McCue, 2019 "Amazon Alexa Accused Again of Spying: Here is Another Solution"

an essay by Yale students Kevin Bankston and Ashkan Soltani, referred to just this in the case of the constitutional rights of police tracking a suspect by attaching a GPS to their vehicle. Prior to this case there was no reasonable expectation to privacy for your general location, however this was overturned in this case with the use of GPS instead of radio based devices[1]. The thought, referred to as the Bankston-Soltani Principle, tells us that our privacy is violated every time a new technology becomes cheaper and widely used by the government because there are no current laws or regulations against it. It is up to the people to actively protect their data and fight against invasive forms of surveillance. There are multiple means that the average user can help prevent the government, or any other party, from tracking their information. It is recommended that companies and the public start utilizing private encrypted services that hides and secures any user data.

The Deep Dark Web

Encrypted services come in many different varieties. From the widely used Virtual Private Networks (VPN) that are used to fool websites that you are in a location that you are not, or most commonly used to watch shows that are only on Candaian Netflix while you are in the United States. VPNs are a great way to prevent websites, internet providers, and other entities from using tracking systems, called cookies. Cookies are used by companies to track what websites you have visited, what you looked at, and even how long. That is why if you recently searched for ‘phone cases' on Amazon you will most likely be shown ads for Phone Cases while

---

[1]Bankston & Soltani, 2014 “ Tiny Constables and the Cost of Surveillance”

on other websites. From these cookies alone a website is able to tell almost anything about a user, their shopping habits, relationships, possibly even their ethnicity, gender, and sexual orientation. While a VPN can protect you and your information, there are things that it cannot protect you from. This is where the Deep Web comes into play.

The Deep Web is a special form of the internet. While any computer can easily access the World Wide Web and search to their heart's desire, the Deep Web requires a specialized and encrypted browser service, for example Tor and I2P. The Deep Web, or the idea or a secret peer-to-peer means of communication over the internet, is as old as the idea of the web itself. However the Deep Web, as we commonly refer to it today, didn't become widely available until Freenet, a privacy and anti-censorship centric browser, was released in March of 2000[1]. While the Deep Web might sound like an intimidating back alley of the internet filled with illegal goods and services, it's actually far from the truth. The vast majority of the Deep Web is filled with any private link, where it can be test pages for company websites, personal blogs, or even just private social media accounts. While it is true illegal activities do occur on the Deep Web, they actually occur on a deeper separate part called the Dark Web that is just a fraction of the Deep Web[2].

The Dark Web is a place where activities considered illegal or immoral take place. Whether it's the sale of illegal narcotics, bets, hiding funds, or sexually explicit services or material it can be found on the Dark Web. The site known as 'The Silk Road' was the most well known services for illegal drugs, and gave the Deep Dark Web its infamous reputation. With the rise of services being offered on the deep web a form of private, untraceable payment was in need. Bitcoin was created in 2008 as a response.

---

[1]Butler, 2018 " Dark Web History: Where Did It Come From?"

[2]Sebastian, 2015 "Deep Web & Dark Web as Fast as Possible"

Unlike every ‘genuine’ currency, Bitcoin is a completely digital medium that is not backed by gold or any tangible object. This makes the value of Bitcoin completely reliant on the confidence of the currency in the public’s eye, almost like a stock traded in the public market. Over the years the price fluctuates greatly, but as it became more popular the price shot up. Sitting at just ten thousand dollars per bitcoin in 2017 now a single bitcoin is worth fifty thousand dollars in 2021. The attractiveness of Bitcoin to the Deep and Dark web is that the currency is virtually untraceable. When making a purchase with bitcoin it works just like any other purchase is made on the internet, except with Bitcoin the process is led through what is called a ‘BlockChain’. This process encrypts all the information between the buyer and seller, making it impossible to trace by anyone, including government agencies[1]. While it’s true Bitcoin started off as a way to pay for illegal goods, it is now used by the general public for perfectly legitimate and legal means. You might be able to find smaller hotels, flights, and stores alike accepting Bitcoin as a form of payment. The Future of Bitcoin is uncertain, but with the crypto currency gaining such widespread recognition it’s possible to become a widely accepted form of payment.

Will You Protect Your Privacy?

Ultimately going through these recent years, we can see that the average American citizen is having their private life invaded via online interactions. The NSA and other government agencies collect and abuse information unknowingly taken from its victims, going as

---

[1]Sebastion, 2018 “How Does Bitcoin Work?”

far as to break their own rules set in place. Most Private Companies have gone to length to protect your privacy, but to no avail. Some private companies work directly with the government to collect and share your information. The only way to truly protect your privacy is by yourself. Only use services from trusted services that encrypt their user data. Use services like Tor to utilize the Deep Web.

> *"...democracy may die behind closed doors, but we as individuals are born behind those same closed doors, and we don't have to give up our privacy to have good government. We don't have to give up our liberty to have security."*
> *-Edward Snowden, 2014*

This is all of course if you are concerned about your privacy. If you are concerned that your personal information is being sold. If you are worried about strangers tracking your habits online. If you are concerned about living in an Orwellian future of being monitored 24/7. How much privacy are you comfortable with giving up in exchange for the mere feeling of security?

Bibliography

Bankston, K., & Soltani, A. (2014, January 9). Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones. The Yale Law Journal - Home. https://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

Bush, G. (2001, October 18). Critical Infrastructure Protection in the Information Age. Federal Register. https://www.federalregister.gov/documents/2001/10/18/01-26509/critical-infrastructure-protection-in-the-information-age.

Butler , S. (2018, December 23). Dark Web History: Where Did It Come From? TechNadu. https://www.technadu.com/dark-web-history/52017/.

Gellman, B. (2013, August 15). NSA broke privacy rules thousands of times per year, audit finds. The Washington Post. https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

Goel, V., & Perlroth, N. (2016, December 14). Yahoo Says 1 Billion User Accounts Were Hacked. The New York Times. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

The Guardian. (2016, February 29). Apple case: judge rejects FBI request for access to drug dealer's iPhone. The Guardian. https://www.theguardian.com/technology/2016/feb/29/apple-fbi-case-drug-dealer-iphone-jun-feng-san-bernardino.

Heiligenstein, M. X., Editors, P., & O'Brien, G. (2018, October 3). A Brief History of the NSA: From 1917 to 2014. The Saturday Evening Post. https://www.saturdayeveningpost.com/2014/04/a-brief-history-of-the-nsa/#:~:text=A%20Brief%20History%20of%20the%20NSA%3A%20From%201917,a%20long%20history%20of%20surveillance%2C%20scandal%2C%20and%20scrutiny.

Jones, S. (2019, September 19). Author Post: 9/11 Changed the Security Industry Forever. Forbes. https://www.forbes.com/sites/forbesbooksauthors/2019/09/19/911-changed-the-security-industry-forever/?sh=1a9295a16d9a.

Larson, J. (2013, September 5). Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security. ProPublica.

https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

McCue, T. J. (2019, July 30). Amazon Alexa Accused Again Of Spying: Here Is Another Solution. Forbes. https://www.forbes.com/sites/tjmccue/2019/07/30/amazon-alexa-accused-again-of-spying-here-is-another-solution/?sh=47da5cde65f3.

Ray, M. (2021, March 26). Edward Snowden. Encyclopædia Britannica. https://www.britannica.com/biography/Edward-Snowden.

Sebastian, L. (2015, August 12). Deep Web & Dark Web as Fast As Possible. YouTube. https://www.youtube.com/watch?v=nKrODPtVinw.

Sebastian, L. (2018, January 30). How Does Bitcoin Work? YouTube. https://www.youtube.com/watch?v=L-Qhv8kLESY.

Snowden, E. (2014, March). Here's how we take back the Internet. TED. https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet#t-175409.

Taylor, A., & Steedman, S. (2013, August 28). The Evolution of Airline Security Since 9/11. International Foundation for Protection Officers. https://www.ifpo.org/resource-links/articles-and-reports/protection-of-specific-environments/the-evolution-of-airline-security-since-911/.