An Analysis of American Mass Surveillance
in the post-9/11 Era – Governmental & Corporate

Ben Meshanko
Purdue University Department of Computer Science
CS390GIS: Great Issues in Computing
Prof. Eugene Spafford
October 14th, 2020

It is no secret that vast swathes of user metadata are collected by Federal Government agencies under the guise of national security and counterterrorism. Shortly after 9/11, the Patriot Act, which gave incredibly enhanced powers to the government agencies to gather intelligence to protect against potential terrorists (ACLU), was signed. I believe that this dramatic shift in our national security approach severely compromised the privacy of nearly all telecommunications worldwide. The surveillance capabilities of not just the NSA, FBI and CIA, but also telecommunications and other internet corporations are incredibly impressive and leave those concerned for privacy worrisome for the future. If privacy and national security are not successfully balanced, how will the era of AI and quantum computing, which have the capability to severely harm both, affect people with secure information saved on cloud-based databases? Many will recommend immediately Congressional action, but I propose that advocating for cultural change is a superior approach than any temporary band-aid Congress can provide. Furthermore, the information that Edward Snowden uncovered is far too potent to not act on – how can we trust Congress to act in our favor when radical governmental action was a spark for surveillance and data collection? Keeping the post-9/11 surveillance state in place is a sin that every administration since Bush has committed, and only when there is enough public pressure on the Federal Government and massive conglomerates will it change. Unsurprisingly, nothing has changed, and perhaps the practices of surveillance and data collection are being accelerated by the vast growth in social media platforms and the Internet of Things. The American public is generally concerned but functionally apathetic to and unknowledgeable about computing-related privacy issues. In this case study, I will go through the surveillance state, the corporate cooperation, what we can do, and how we can protect our country without compromising the privacy of the Internet.

To begin, it is useful to mention how intertwined the progression of computing has been to this state surveillance. There is incredibly sophisticated and complex infrastructure dedicated to collecting and storing consumer data. On June 7th, 2013, much of this infrastructure, called the NSA Prism program, was exposed to the public by The Guardian. Prism gives the National Security Agency the ability to access a wide array of data of Apple, Google, Facebook and Microsoft users (Greenwald & MacAskill, 2013). Computing-based corporations that generate

immense amounts of user data and cooperating with the Federal government in surveillance campaigns provides reason to be gravely concerned for your privacy. As computing grows in importance in our everyday lives, perhaps less and less of our information will be sheltered and algorithms and AI employed by the National Security Agency will be analyzing our data to determine our potential threat level. Hopefully, society can avoid this Orwellian future. Regardless, the Prism program allows the NSA "direct access to the companies' servers" with "consent unnecessary" (Greenwald & MacAskill, 2013). Details on how the NSA is collecting user data are unknown and classified, but it is safe to assume that there is some backdoor in these companies' software that allows the NSA access to their databases. Currently, the Prism program has been officially halted, but the overwhelming majority of the National Security Agency has remained intact. The Patriot Act is expired as of today, but the Foreign Intelligence Surveillance Act Amendments, which were also responsible with giving the NSA tremendous powers to act extra-judiciously, were renewed in 2017[1]. There is still incredible political pressure from leadership of both parties to pass legislation that supports surveillance. Out of the 2017 House/Senate leadership, Ryan, Pelosi, McConnell and Schumer all voted to renew the FISA amendments (S. 139). These four powerful individuals exhibit tremendous influence on the remaining 531 Senators and Representatives from both parties to follow suit. The political science is there to support surveillance – all else that is needed is computer science.

While computing and politics are at the forefront, it is important to note that there is certainly a human aspect to the uncovering of this surveillance. Edward Snowden, age 29 at the time, with a long career ahead of him, sacrificed his lifestyle as a Systems Engineer for the CIA and NSA so that the public could know the practices of these agencies that he believed were wrong. He is the embodiment of a geek. He explains in his 2019 book *Permanent Record* how techies and geeks alike will "[inherit] the earth" (Snowden, 2019). He goes on to write about how he spent most of high school "on the computer" and goes into the technical details of copying NSA records onto an SD card (Snowden, 2019). There are tens of thousands of Federal Government employees, young men and women who have an aptitude for computing employed doing what Snowden revealed today. Snowden is not a criminal and not a Russian or

[1] https://www.congress.gov/bill/115th-congress/senate-bill/139

Chinese spy. He is a computer scientist, disillusioned at what the National Security Agency was doing to the American public, and he did something about it. He acted on his principles and sacrificed his freedom to do so. Without computer scientists who are willing to sacrifice their careers to uphold their values and ethics, society will go down a dark road where computers, data and numbers are the basis of power, and traditional ethics and morals will be abandoned in the pursuit of power.

I believe that Edward Snowden revealed unethical and perhaps unconstitutional action by the Federal Government. After 9/11 and the Anthrax attacks of 2001, it was obvious that America was going to respond in some way to prevent future terrorist attacks from occurring. However, the bloated, inefficient mess of a militarized cybersecurity state that was created is a disgrace to the ideals of liberty and justice that America was founded upon. The First and Fourth Amendments are not suspended in times of national emergency, and many believe that the Patriot Act is unconstitutional legislature. One entity who believes this is the American Civil Liberties Union, an organization that fights for: "the individual rights and liberties guaranteed to all people by the Constitution and laws of the United States" ("FAQs", n.d). Regarding national surveillance, the ACLU believes "Section 215 of the Patriot Act violates the Constitution in several ways" ("Surveillance under the USA/Patriot Act," n.d). They go on to list the ways in which it violates the First and Fourth Amendments. The expansion of records searches violates the First Amendment because recipients of search orders are prohibited from telling others (free speech) and by "effectively authorizing the FBI to launch investigations of American citizens in part for exercising their freedom of speech" (ACLU, n.d). Similarly, the Fourth Amendment is violated by authorizing searches without probable cause and failing to provide notice, before or after, to persons who are searched (ACLU, n.d). There has been heavy debate on whether or not the Patriot Act is Constitutional. Nonetheless, rushing a comprehensive national security bill with tremendous pressure and urgency is a good idea for a temporary fix. However, emergency powers tend to not go away. Despite being intended to be temporary, the Patriot Act lasted another 14 years. Today, the surveillance infrastructure has already been built, and billions of people's privacy have been infringed upon.

The remnants of the complex surveillance network that was built to provide tools to combat terrorism still exist today. The majority of cyber traffic today exists on platforms created by companies that were complicit in Patriot Act data collection (Apple, Facebook, Google and Microsoft). There have been controversies recently involving these companies' practice of collecting user data and selling it to advertisers. One of the most notable of which is the Cambridge Analytica scandal that plagued Facebook surrounding the 2016 election. It was found that Cambridge Analytica was providing a platform for Russian disinformation to spread on Facebook, which many have said was one of the deciding factors in an election that was decided by a few thousand votes in 4-5 swing states. But the concerning thing is that certain groups of people where targeted based on their demographics and psychographics and were bombarded with Russian propaganda on Facebook. Christopher Wylie played whistleblower to how a company headed by Trump adviser Steve Bannon was using personal information taken from individual Facebook accounts to "build a system that could profile individual US voters, in order to target them with personalised political advertisements" (Cadwalladr & Graham-Harrison, 2018). Wylie revealed evidence about data misuse of over 50 million Facebook profiles, the largest ever data-breach in its history. Russian influence aside, the massive amount of data harvested helped the Trump campaign "identify possible swing voters and craft messages more like to resonate" (Cadwalladr & Graham-Harrison, 2018). Perhaps more ominous, Facebook maintains that the data was not a breach, but GSR and Cambridge Analytica obtained this data legitimately. Either way, user data is being collected and is for sale to the highest bidder. Data collection mechanisms that were original used solely for national security are now being monetized and have the ability to dramatically shift public opinion through targeted advertisements.

Perhaps an even larger culprit of modern data collection is Google. Security.org rates them as the worst offender when it comes to data. Vigderman and Turner write: "Personally, I think of it more like a way of life, a tool that has an impact on nearly all of my daily decisions, like which subway I should take to get to work the fastest, what's the best place to get my boots repaired, or even what a random woman I went to college with is doing at this very second" (2022). Google collects almost every piece of information that you have, aside from

incredibly secure data like your address or SSN – they are the all-encompassing data giant that has the potential to control your life decisions algorithmically. Forbes contributor Nicole Martin wrote about the massive amounts of data that Google is collecting on an individual who has not restricted the platform with aggressive privacy settings: "[She] downloaded [her] data and it was 2GB which equals roughly 1.5 million word documents" (2019). A quick Google search can tell you how many users Google has – somewhere in the ballpark of 1 billion. I also had to Google the unit necessary to express the total amount of user data Google controls, assuming they have 2GB on each of their billion users. The answer: $2 * 10^{18}$ bytes – 2 exabytes. That is the amount of data that can be stored on 2 million 1 TB hard drives. It's worth a reminder that Google was also complicit in the NSA's PRISM program as they continued to accelerate in their data collection efforts. As Google continues to create more services, they are collecting more and more data on consumers, having some worried about both the handling of this data and the scope of the algorithms trained by that data.

A Pew Research report on the attitudes of Americans towards the collection and use of their data was released in November 2019, finding that the majority of Americans are concerned about their privacy online (Auxier & Rainie). The results of the survey are astonishing, Americans are significantly more concerned for their privacy than they were just 4 years prior, when a similar survey was conducted. About 6 in 10 Americans believe that it is not possible to go about daily life without being tracked by companies or the government, and about 1 in 20 Americans believe that they understand what is being done with the data that is collected on them (Auxier & Rainie, 2019). 81% believe the risks outweigh the benefits when it comes to corporate data collection, compared to 66% for governmental data collection. Two thirds believe risks outweigh the benefits for governmental data collection, but just under half of Americans believe that it is acceptable for the government to "collect data about all Americans in order to assess potential terrorist threats" (Auxier & Rainie, 2019). I believe that this attitude comes from a general misunderstanding of the infrastructure that is required for mass data collection and surveillance. If the government is capable of collecting information about "all Americans" for the purpose of combatting terrorism, they are capable of collecting information about all Americans for any purpose. When you construct a complex surveillance

network, it doesn't disappear the second the terroristic threat is eliminated. Companies like Google and Facebook inherited the PRISM program, and for the past decade have monetized data collection to the scale of trillions of dollars. When the Pew Research Center conducted a similar survey in 2014, they found that Americans who were more informed about government surveillance where about 40% more likely to say they believe internet companies should not save user information (Madden & Rainie, 2015). The more educated people are on the topics of data collection and surveillance, the more they oppose it. 75% of Americans support increased regulations on what corporations are able to do with user data, but 36% have more than "very little" understanding of the current privacy laws (Auxier & Rainie, 2019). A lot of ground can be made up on educating Americans about privacy, and perhaps that is the routing to pursuing action – a cultural revolution where we fight back against corporate data collection and forfeit some of the benefits that big data gives society.

When considering a strategy that can fight back against the practices of governmental and corporate data surveillance, there are two main ways to channel activism – cultural or political. Both require an educated populace that has turned on the idea that their data is being weaponized against them. Purdue University is doing an incredible job at this – Computer Science majors are required to take a "Great Issues" course that teaches about problems in society in which computing is applicable. Adding a "Computing Issues" course this semester shows their commitment to educating the next generation of techies about the power and dangers of computing without consideration of ethics. Purdue is also increasing their requirements on Civics education for all graduates starting with the class of 2025[2]. This is a good start, but the average Purdue student is far more educated on the issues of cyber privacy and civics than the average American. Perhaps we have to start earlier. School boards have been successful in changing the education curriculum in recent years, most notably in opposition to Critical Race Theory. Perhaps its time to use some of that energy to educating high school students about privacy in the world of computing and what they can do to stay protected. It's important to note that this is far more than a civil liberties issue – mass data collection leaves user information far more vulnerable to hackers and other cyber threats. Only

[2] https://www.purdue.edu/provost/about/provostInitiatives/civics/faq.html

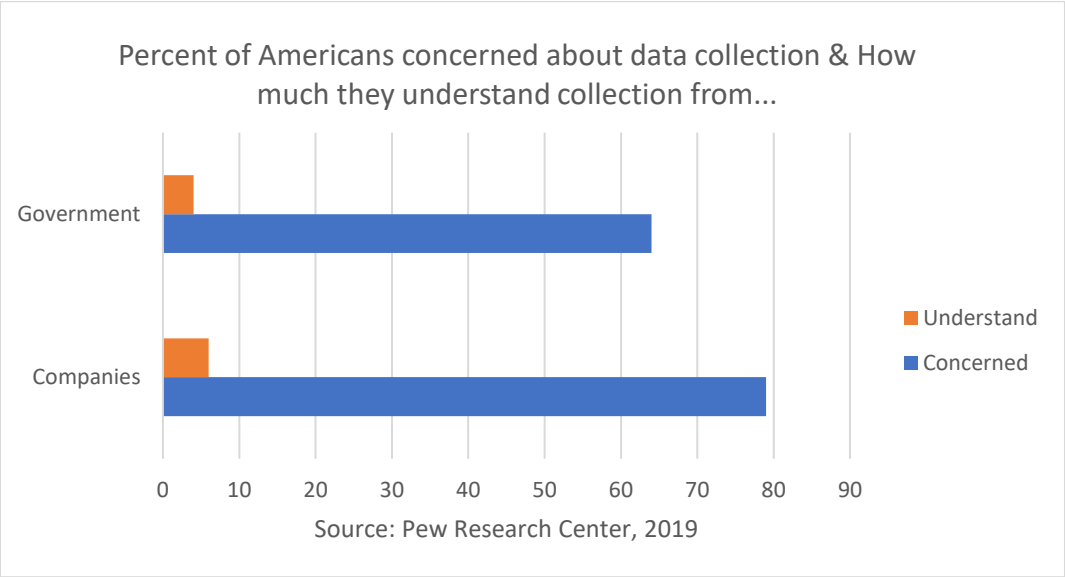
when the public is sufficiently educated and passionate about privacy and cybersecurity in their daily lives can mass cultural or political changes occur. I believe that cultural change is more potent – politics cannot keep up with the rapidly changing environment that is cyberspace. An educated populace creates a market for Signal and DuckDuckGo and does work to replace notably egregious platforms such Facebook Messenger and Google. The window before AI has a significant enough role in our lives for the average person to be completely reliant is closing. The futurists reading this may think that I am suggesting that we go backwards on computing in order to create a world that is safe for people. They are correct – data science has gone too far. I believe that society is innovating incredibly fast in Data Science because of the profit incentive, but it would be best if we innovate in the physical world first. For example, if humans cannot solve climate change without hyper-intelligent AI, why should AI keep us around if our greatest accomplishment was creating a machine that surpasses our intelligence?

As mentioned before, issues of privacy will only be exacerbated as computing power increases each year. Even if the National Security Agency does not access user data anymore, the amount of people who are able to is growing rapidly. Consider the NotPetya cyberattack. The costliest cyberattack in history severely impacted government agencies in Ukraine, but also crippled the Danish shipping giant Maersk (Greenberg, 2018). If the Russian-military-sponsored hackers had attacked a US Tech company in the same way and obtained personal information about millions, the consequences would be geopolitically profound. In the near future, when hackers could be aided by quantum computers or a particularly competent AI, cyberattacks may become the norm. Thus, it is imperative to do something about it today – limit the information you put out on the Internet, advocate for an end to governmental surveillance and educate others about the risks of navigating the Internet. Harishankar Singh wrote an ominous piece for IBM about the importance of data for AI. Data is the fuel that is driving the progression of AI (Singh, 2021). But that data is being collected without the majority of the population being aware that their data is being used to fuel AI and algorithms that compromise the majority of the features of the platforms that they most often use. We have to be willing to sacrifice some of these features like incredibly accurate restaurant recommendations, targeted ads for products that you would like, or “suggested friends” that connect you to an old

colleague in order to maintain our data privacy and security. Snowden's message may have fallen upon deaf ears, but as computing becomes increasingly intertwined with reality, something needs to be done to swing the pendulum in favor of privacy and liberty.

As humanity progresses technologically, there is reason to be increasingly worried about the privacy and security of data that you generate online. The United States government kicked off Internet surveillance by creating a vast, complex mechanism to collect user data to combat terrorism in the post-9/11 era. Big Tech inherited this network, and user data is collected and sold to the degree of trillions of dollars annually. It is ultimately up to individuals to protect their own user data from these networks of surveillance and data collection. Educating the public on how their data is collected and how they can browse the Internet safely goes a long way – most people do not know how much of their sensitive personal information is stored in massive databases. Only with a public educated on issues in cyberspace can we fight back against the misuse of data by governments and corporations that leaves the Internet a more dangerous place.

Many Americans are Concerned about the practice of user data collection from the government and from companies but very few understand it (Auxier & Rainie, 2019).



Works Cited

ACLU. (n.d.). *FAQs*. https://www.aclu.org/faqs

ACLU. (n.d.). *SURVEILLANCE UNDER THE USA/PATRIOT ACT*. https://www.aclu.org/other/surveillance-under-usapatriot-act

Auxier, B., & Rainie, L. (2019, November 19). *Key takeaways on Americans' views about privacy, surveillance and data-sharing*. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Electronic Frontier Foundation. (n.d.). *NSA Spying*. https://www.eff.org/nsa-spying

Greenburg, A. (2018, Aug 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenwald, G., & MacAskill, E. (2013, June 7). *NSA Prism program taps in to user data of Apple, Google and others*. The Guardian. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). *Edward Snowden: the whistleblower behind the NSA surveillance revelations*. The Guardian. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Madden, M., & Rainie, L. (2015, May 20). *Americans' Attitudes About Privacy, Security and Surveillance*. Pew Research Center. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Martin, N. (2019, May 11). *How Much Does Google Really Know About You? A lot.* Forbes. https://www.forbes.com/sites/nicolemartin1/2019/03/11/how-much-does-google-really-know-about-you-a-lot/?sh=452081c57f5d

S.139 - 115th Congress (2017-2018): FISA Amendments Reauthorization Act of 2017. (2018, January 19). https://www.congress.gov/bill/115th-congress/senate-bill/139

Savage, C. (2018, May 4). *N.S.A. Triples Collection of Data From U.S. Phone Companies*. https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html

Singh, H. (2021, May 14). *Data Is The New Fuel, AI is The Accelerator*. IBM Digital Transformation Blog. https://www.ibm.com/blogs/digital-transformation/in-en/blog/data-is-the-new-fuel-ai-is-the-accelerator/

Snowden, E. (2019). *Permanent Record*. Metropolitan Books.

Somaiva, R. (2014, April 14). *Pulitzer Prizes Awarded for Coverage of N.S.A. Secrets and Boston Bombing*. New York Times. https://www.nytimes.com/2014/04/15/business/media/coverage-of-snowden-and-boston-attack-win-pulitzer-prizes.html

U.S. Department of Justice. (2005, April). *USA Patriot Act: Sunsets Report*. https://www.justice.gov/archive/olp/pdf/sunsets_report_final.pdf

Vigderman, A., & Turner, G. (2022, October 10). *The Data Big Tech Companies Have On You*. Security.org. https://www.security.org/resources/data-tech-companies-have/