Introduction

Hello, everyone! My name is Sebastian Rodriguez and I'm a second year undergraduate student at the University of Toronto. Today I'd like to teach you how mass surveillance works in the United States.

Before we begin, I feel it's important to say that, although I'm studying in Canada, I'm from the United States so I conducted my research with a US lens. Now, just because this presentation focuses on the US that doesn't mean that this isn't important on a global scale – as we all know, things that happen in the US tend to affect and influence people across the globe.

I remember when Edward Snowden's leaks first came to light in 2013. I was only 12 at the time, but I grew up completely immersed in technology. I already had a Facebook account, an email, and I got my first smart phone when I was 9-years-old. I was so young that I didn't really understand what Snowden's leaks meant to *me* at the time, but I got the "big idea" – the government has the capability to and a history of violating our online privacy.

As I grew older, public privacy concerns grew exponentially. It seemed like every year there was another data breach, or people had personal information leaked, but the question of the government having access to our data seemed like a forgotten memory. Occasionally we'd hear about some new scary surveillance program or Edward Snowden would appear in an interview, but the "hype," so to speak, certainly died down. A relatively older version of myself wanted a better understanding of how mass surveillance worked. I looked around online and found websites and databases citing very specific, very detailed answers that were almost impossible for me to understand. There was so much information and it was so overwhelming that I just gave up.

This year I had the opportunity to take my first Digital Humanities class. I learned not only about how technology can be used as a medium for important topics like this, but how technology has a real social influence. Thanks to COVID, I had a lot of free time on my hands so I decided to revisit my earlier question and attempt to uncover how mass surveillance works, but also share what I learned with others in a way that's easy to understand.

And that is what led me to create *The United States of Surveillance*, an open-access, open-source website that summarizes all of the complex laws, programs, and court cases that support mass surveillance in the United States. The website, which you can all access by going to masssurveillance.net, mimics a layout that's often used for developer documentation – because, well, I'm a computer science major and that was what I was most comfortable with.

The website is broken down into three sections that reflect the role each branch of the US government has in monitoring our data. There's quite a bit of information on this website, so I'll attempt to break down each page as briefly as possible.

Understanding the Law

Before we start talking about what the US government does, it's important to understand how all of this is even legal.

The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act, or FISA, is the basic legal framework that supports mass surveillance. It's important to recognize the very specific language used in this law: programs may not *intentionally* collect data on US citizens or people in the US. This loophole is so important because eventually it became easier for agencies like the NSA to just collect as much data as possible when targeting a specific person – because it's faster and easier.

The next thing FISA did was create the Foreign Intelligence Surveillance Court. Now, the FISA court generally operates like any other court. There is a judge, and the government must make an argument outlining why they need a specific program or why they need a warrant for information. The key differences are that individuals are typically not represented or even notified of a case, and the court's records are classified due to national security. These records can be declassified, which is how the public can learn about what the government's doing, but the ability to declassify a document rests with the Director of National Intelligence. That means that the FISA court, since it is a federal court, can set legal precedents that change how the law works in the United States – and don't worry, I'll explain this in detail later.

The Patriot Act

The next law, which is probably what everyone thinks about when they hear the term mass surveillance, is the Patriot Act. While the Patriot Act is important, its value comes from changing FISA. The Patriot Act basically says that the FBI can access information collected under FISA if it relates to an FBI investigation. The Patriot Act also comes with a clause that gives the government the ability to prosecute whistleblowers who try to expose when the government asks for information. The Patriot Act basically opens the door for the government to use FISA, which was originally intended as a foreign surveillance tool, domestically.

The Third-Party Doctrine

The Third-Party Doctrine is crucial in understanding why surveillance programs don't automatically violate the Fourth Amendment, which is the US's protection from unlawful searches and seizures, typically covering all personal property including data. The Third-Party

Doctrine states that if people voluntarily give information to a third-party, say Facebook or Google, the original owner of that data loses protection and the government does not need a warrant to access that information. The third-party doctrine is not a law, so it can be overturned by a court at any time, and recently the Supreme Court repealed part of the precedent when it ruled that the government needs a warrant to access cell phone location data. The Third-Party Doctrine is important because it bypasses the need for a warrant whenever information is collected directly from a company and not an individual, which, thanks to things like social media, internet service providers, and cell phone companies, is all the government really needs.

The Unitary Executive Theory

The Unitary Executive Theory is a term *almost* synonymous with executive power, however, it affords the President with a certain level of extra privileges. Executive privilege provides an alternate, yet conjoined, set of rules for surveillance. Executive Order 12333 is a perfect example of the power a President yields with executive authority. The order expands upon the language of FISA and states that information collected through foreign surveillance can be used domestically if it includes evidence that a person violated US laws. This pairs perfectly with, and is even mentioned in, the Patriot Act, allowing the FBI to legally use any surveillance data if it holds incriminating evidence.

Another example of the theory is from a memo written by John Yoo, a former Deputy Assistant Attorney General under George W. Bush who became infamous for the administration's torture memos. The memo stated that the President can deploy the military domestically and use military-grade surveillance technology that is more powerful than typical law enforcement agencies have. The memo can be used by any future administration to justify both military deployment and domestic surveillance, going directly against the Posse Comitatus Act that says the military cannot be deployed domestically.

Using executive power to authorize surveillance is a dangerous tool the government possesses. It does not require court approval, unlike FISA programs, and its usage can vary widely depending on the person in power.

Summary

So far we understand that FISA permits the government to collect data on foreigners, with the exception of incidental information collected on US citizens. This loophole turned into a practice of mass information gathering that has a strong potential of domestic data collection. The Patriot Act makes this information available to the FBI, and an executive order allowed the government to use this foreign intelligence if it contains evidence that someone broke a domestic law. And the third-party doctrine nullifies the need for a warrant by stating the information someone gives to a third-party is not protected by the Fourth Amendment.

Surveillance Programs

With a basic understanding of the law, we can now dive into the actual surveillance programs. Keep in mind that most of the programs we'll talk about were leaked in 2013 and may have changed or grown over the years. While we don't know how these programs exist today, we can follow a simple trend: these programs often come with broad mandates to collect mass sums of information, only to use a small fraction of that information for fighting terrorism.

NSA XKeyScore

XKeyScore is a database that records internet activity, including emails, online chats, and browsing history. The database is updated in real-time with data on nearly everything a user does on the internet. This program takes advantage of the third-party doctrine – because a lot of the information on the internet is given to a third party, we forfeit our legal rights to the data. According to the guardian, the database helped, in some way, capture 300 terrorists by 2008. We don't know the time period that applies to this statistic, but this is obviously a powerful and valuable tool for the NSA.

NSA PRISM

Prism is a program that provides the NSA with a "back-door" into the servers of major technology companies, like Google, Apple, and Microsoft. Slides from a NSA presentation boasted access to emails, videos, photos, and even voice over IP – which, if you don't know, is what things like FaceTime, Skype, and WhatsApp use. I should note that a journalist reached out to both Apple and Google for a comment on this program, and both companies denied it. Although that isn't surprising considering the Patriot Act's silencing order.

NSA MYSTIC

Mystic is a program that collects both metadata and recorded contents of calls. When information about the program was released in 2013, the program was only used in a handful of countries – Mexico, Kenya, and the Bahamas – and was primarily used to fight drug trafficking. The program provided the NSA with the ability to record every phone conversation in a country over a span of 30 days. Although we only know that the program was only implemented in three countries, this capability and framework can be used to target virtually any country.

NSA FASCIA

Fascia is a program that collects metadata, including location records, of people around the world. In 2013, Edward Snowden said that around 5 billion records were collected every day in

the case that the NSA needed 1% of that data. Fascia is the program President Obama referred to when he said that the NSA was only looking at metadata and not recording the contents of calls, even though we know that the NSA has that capability.

FAMS Quiet Skies

Quiet Skies is a program operated by the US Air Marshals. Although it doesn't deal with digital surveillance, it is an example of how other agencies can utilize surveillance law. Quiet Skies monitors travelers who may not be under investigation or even on a watch list. Marshals within the program even said that their job was to watch travelers who didn't appear to pose a threat. The surveillance included documenting when someone on a domestic flight used their computer, changed their clothes, or even fell asleep during the flight.

The Five Eyes Network

This is where things get a bit interesting for those of you outside the United States. The US has an agreement with the United Kingdom, Canada, Australia, and New Zealand that allows the countries to share surveillance information. Together, they form the largest surveillance network in the world and have the ability to circumvent their respective domestic laws. Don't take my word for it, the European Parliament said that their program provided people with no legal protections because it isn't illegal for any of these countries to spy on people outside of their country. This basically means that if any of your information was collected by the US, and if you live in the UK, Canada, Australia, or New Zealand, your government has access to those records.

Court Cases

Now that we understand both surveillance laws and programs run by the government, let's talk a little bit more about the role of the courts. The FISA court plays a vital role in this whole process: they authorize mandates for surveillance programs, which have to be renewed every so often, and they also provide a form of oversight to make sure programs don't violate any laws. Because of the robust legal framework that supports surveillance, it isn't always easy to fix ethical problems with these programs, and sometimes the government outright defies the court's orders. The FISA court sometimes overlooks significant issues, and even worse changed Constitutional law without public knowledge for a period of time.

FISA Court Opinion 2011

In 2011, the FISA court ruled that the NSA had been collecting data on US citizens that wasn't related to the mandate of their program. The court referred to a program where the NSA directly accessed fiber-optic cable lines, which is basically the cable that connects the internet together, indicating a new method of data collection. The court also stated that the NSA was running this

program before they received approval, and that this was the *third* time in less than three years that the government misrepresented information about their programs. The opinion stated that the Court's mandate was, and I quote, "so frequently and systematically violated that it can be fairly said that this has never functioned effectively." This starts to show a pattern of the government defying the court's orders and starting new programs without approval.

FISA Court Opinion 2015

In 2015, the court attempted to be impartial by appointing a third party to review the process where information from surveillance programs are parsed and used by other agencies. The person they appointed found that information shared by the NSA and used by the FBI served no foreign intelligence purpose. The court said that this was lawful and that the information could be used if it contained evidence of a crime. This clearly shows that information collected under foreign surveillance programs can and has been used domestically.

In this opinion, the FISA court furthered an important exception to the Fourth Amendment. The court ruled that a warrant is not required to collect foreign intelligence, even when a US citizen is the target of the surveillance. Presumably this means that if a US citizen is traveling internationally, the government doesn't need a warrant to collect their data. But it can also be applied to the broad mandates that the NSA has when collecting information: collect as much information as possible. This was also the first time that the court referred to a US citizen as a foreign intelligence target, opening the door for programs to specifically obtain information on US citizens.

Because this court ruling was initially classified, there was a period of time where this broadened exemption to the Fourth Amendment was both legal and unknown by the public. This shows the court's ability to create a secret set of laws, fundamentally changing an interpretation of the Constitution and applying it to US citizens without their knowledge.

FISA Court Opinion 2016

In 2016, the FISA court attempted to clamp down on some of the NSA's broad information gathering. The court found that the NSA was using US person identifiers, so something like an email address or phone number, to specifically target US citizens. It took the government over five months to identify all of the areas where the NSA was targeting US citizens, indicating a rampant abuse of the programs and a vast collection of data on US citizens.

FISA Court Opinion 2018

2018 was another important year for the FISA court. It found that the FBI repeatedly violated the Fourth Amendment while analyzing information from the NSA's surveillance programs. To give you an idea of how many times the FBI may have violated the Fourth Amendment, the FBI ran

3.1 million database searches in 2017, compared to the CIA and NSA's combined 7,500 searches. To make things worse, the court found that a "large number" of the FBI's searches were not likely to provide evidence of a crime or a relation to foreign intelligence. Many of these searches were accidental, due to lack of training, or done by FBI agents for, and I quote, "improper personal uses." So, lets say, and this is just an example, the database could have been used by an FBI agent to spy on an ex or to research someone their child was dating. It's impossible to know the specifics because the FBI wasn't recording what their searches were for, which was something the court required when they granted the FBI access to the database.

Another example of the FBI's misuse of the data is if they suspect someone at a company intends to commit a crime. They would search for information on *all* of the company's employees to find the one person who they *suspect* is going to commit a crime.

United States v. Moalin

But not all hope is lost! In 2020, a panel of judges said that the government *may* have violated the Fourth Amendment when it collected telephone metadata on millions of Americans. It doesn't outright say that the government's practices are illegal, but it is a step towards recognizing illegal surveillance.

Conclusion

We covered a lot of material in a relatively short amount of time, but it's important that the public learns about how the government maintains their mass surveillance programs. As we've learned, there's no one law or one program that defines the practice. It's woven into law after law, program after program, and only small progress has been made to limit the government's surveillance abilities. But we also learned that even if every surveillance law and program were repealed right now, the government can still collect information if, say, Canada ran similar programs and collected data on US citizens.

So, what can we do? The reason why I tried to frame this site in a developer mindset is because it's up to developers and tech companies to secure our information. For those of you who don't know, there's something called end-to-end encryption that prevents anyone except the sender and receiver of a message from reading the contents of that message. That means that even if the government collects the encrypted version of a message, which could be an email, text message, or a record of you accessing a website, they won't be able to access it without a key that's only stored on the devices of the person sending or receiving the message. A lot of companies are already using this encryption now so it's significantly harder for the government to obtain information.

We must recognize not only the government's ability to collect information but also the potential for hackers and malicious actors, building a future where all of our data is secure and can only be accessed by the people it was intended for.

Thank you for listening! If you have any questions, feel free to reach out to me during the Twitter discussion!