

sned – An End-to-End Encrypted File Transfer Service
(Technical Paper)

**Government Surveillance in the United States: The Motivations and Impacts of
Government Spying**
(STS Paper)


A Thesis Prospectus Submitted to the
Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering


Hamza Mir
Fall, 2020

Technical Project Team Members
Hamza Mir

On my honor as a University Student, I have neither given nor received
unauthorized aid on this assignment as defined by the Honor Guidelines
for Thesis-Related Assignments

Signature  Date 5/10/2021
Hamza Mir

Approved _____ Date _____
David Wu, Department of Computer Science

Approved  Date 5/4/2021
Hannah Rogers, Department of Engineering and Society

Government Surveillance in the United States: The Motivations and Impacts of Government Spying

Introduction

Following the September 11 terrorist attacks, concerns over terrorism, as well as counterterrorism efforts, were at an all-time high. One such counterterrorism effort was the USA PATRIOT Act, which eased restrictions on the government's ability to collect information on citizens' activities and communications ("Domestic Surveillance Overview", 2015). This legislation is one of many examples of government surveillance methods to achieve a particular end, often to combat crime or terrorism. The rise of the internet and information technology has encouraged governments to pursue new techniques to address these issues. The US government in particular strives to attain an "information advantage" over potential adversaries in light of new information technology (Clift, 2003).

As new surveillance methods are deployed in the name of security, distrust towards governments, and concerns regarding privacy arise. In 2013, Edward Snowden leaked highly classified information from the National Security Agency (NSA) regarding surveillance programs carried out by the United States, which he deemed unethical (Rusbridger & MacAskill, 2014). The Snowden leaks encouraged a discussion regarding surveillance in the United States and created apprehension of many United States citizens towards the government with regards to digital surveillance. A critical question in this field is: how can counterterrorism and crime-fighting efforts be balanced with the privacy of its citizens?

There are two proposed projects in this portfolio – an STS research project and a technical project. In the proposed research project outlined here, the methods and motivations behind government surveillance will be assessed – both inside and outside the United States. Different actors pertinent to surveillance will be analyzed, as well as their connections between

each other. The technical project aims to address individuals' concerns over surveillance by offering a tool for individuals to share data with a high level of privacy.

Technical

In today's era of the Internet, computer networking enables parties to communicate data to one another. In order to ensure that communications between two parties are kept private, encryption is used. The study of encryption, and more broadly cryptography, predates the Internet by thousands of years. The Ancient Greeks were known to have constructed a tool, the scytale, to encrypt and decrypt messages on the battlefield (Kelly, 1998). In modern computer encryption, a well-established way of sending an encoded message is known as asymmetric encryption. This encryption scheme involves both parties creating a pair of keys, known as a public key and private key. These two keys are related in that, if a plaintext (i.e. unaltered) message is encrypted by the public key, that encrypted message can be decrypted back to plaintext via an operation with the private key. A user's public key is made available "publicly," without much concern to who can see it. Those wishing to communicate with this user encrypt their message with that public key and send it to them. Upon receiving the message, the user can use the private key to decrypt it. Malicious third parties snooping on the encrypted message will be unable to read that encrypted message without the private key. A critical requirement of this scheme is that one should not be able to derive the private key using the public key. The owner of the key-pair must also never share their private key, lest their messages are read by outside parties.

More often than not, in the practice of computer networking, messages sent between two parties, known as clients, must go through a third party, known as a server. When one client sends a message designated for the other, they actually send it to the server and encrypt it such

that only the server can decrypt it. After that, the server forwards the message along to the other client. This sequence means that the server is able to read the message of the sending client, which is common to standard encryption. In what is known as end-to-end encryption (E2EE), the server is unable to decipher what either client sends to it, allowing for a greater degree of privacy, keeping messages secret when the server is hacked or when a government with jurisdiction over the server demands to view its contents. One popular service providing E2EE messaging is WhatsApp, which serves two billion users worldwide (Porter, 2020).

While E2EE messaging services are widely used, there is a distinct absence in popularity of E2EE file sharing. This lack of popularity is surprising, given how critical of a function of the internet file sharing is, and noting giants in this space such as Google Drive and Dropbox. The goal of this independent project is to create a scalable, end-to-end encrypted file transfer service, named “sned.” The project will consist of two components – the client and the server. The client will either encrypt and request to send files, or request to receive and decrypt files that are stored in the server. The server will handle client requests to store encrypted files, facilitate the transfer of files between users, and act as a lookup for mapping usernames to public keys. The server will also run on multiple instances and leverage load balancing – a process used to distribute traffic across computing resources.

STS Topic

The relationship between security and privacy has always been a fragile one, especially in the context of government surveillance. Among the most notable United States legislation for giving increased power to intelligence agencies and expanding surveillance is the Foreign Intelligence Surveillance Act (FISA), which established a framework for the use of electronic surveillance and also established the Foreign Intelligence Surveillance Court (FISC) for

overseeing surveillance activities (“The Foreign Intelligence Surveillance Act”, 2007). Another early initiative was Executive Order 12311 – issued by President Reagan – which permits collection and retention of data which indicates involvement of persons in unlawful activities (“Executive Order 12333”, n.d.). The September 11 terrorist attacks had a significant impact on the government’s use of surveillance. Al Qaeda, the terrorist organization responsible for the attack, made considerable use of the Internet to organize it. They used the Internet to “collect information such as flight times; to communicate reliably and in real time among themselves and with terrorist cells; and to share information and coordinate their attacks” (“Terror on the Internet”, n.d.). Mass surveillance measures exploded in response to the event, notably with the introduction of the USA PATRIOT Act, also known as “the Patriot Act.” The Bush administration made clear that this legislation was intended to combat terrorism in light of recent events. Shortly after signing the bill, Bush stated “We’re dealing with terrorists who operate by highly sophisticated methods and technologies, some of which were not even available when our existing laws were written. The bill before me takes account of the new realities and dangers posed by modern terrorists. It will help law enforcement to identify, to dismantle, to disrupt and to punish terrorists before they strike” (“Text: Bush Signs Anti-Terrorism Legislation”, 2001). The Patriot Act extended FISA considerably, redefined “terrorism” to include domestic terrorism, and also “expanded wiretap powers, gave the government power to demand electronic communications, and made it easier to obtain a federal search warrant in cases of suspected terrorism” (Delaney, 2020). In 2008, Bush signed the FISA Amendments Act (FAA) of 2008, giving the NSA “almost unchecked power to monitor Americans’ international phone calls, text messages, and emails” (“NSA Surveillance”, n.d.). The existence of the Patriot Act and the FAA are clear indications of substantial mass surveillance taking place within the United States.

The threat of terrorism was sufficient motivation to pass the Patriot Act and subsequent surveillance legislation and keep them in place. However, in 2013, former NSA contractor Edward Snowden began leaking a series of documents that called into question the legitimacy and ethics of government surveillance in the United States. Among the most notable surveillance initiatives exposed were FISC orders for telecommunication companies to produce “telephony metadata” for communications inside and outside the United States, as well as PRISM – a broad Internet data collection program (Kim, 2018). Large-scale surveillance shows no sign of slowing down. In 2018, the NSA collected 534 million records of phone calls and text messages – three times more than what was collected in 2016 (Savage, 2018). Many United States citizens contend that data privacy is an issue that merits great concern. Sixty-three percent of Americans believe that it is not possible to avoid having their data collected by the government in their day-to-day life, with sixty-six percent believing that the potential risks of this data collection outweigh the benefits (Auxier et al., 2019). The Snowden leaks influenced public opinion on surveillance. Following the leaks, the share of Americans “who disapproved of the government’s collection of telephone and internet data as part of anti-terrorism efforts increased from 47% in the days after the initial disclosure to 53%” (Geiger, 2018). An analysis of United States surveillance programs using Actor-Network Theory (ANT) will yield valuable insights into the methods and motivations behind government surveillance and their effects on citizens, foreigners, criminals, terrorists, and more. ANT is a methodology developed by Bruno Latour, Michel Callon, and John Law that assesses technological impacts on society (and vice-versa) as a set of interconnected, shifting networks, made up of decision-making agents called “actors” that react to one another (Cressman, 2009). A common criticism of ANT is that actors chosen for analysis are chosen arbitrarily and subject to the biases of the author. However, the mechanisms

and targets of government surveillance can be made clear through research, enabling a more objective construction of an actor-network. More specifically, an analysis of the political climate before and after policies regarding government surveillance were passed may indicate the motivations for these policies and the parties that were impacted. Notable actors in the actor-network for this project are likely to include legislating bodies, executive government agencies like the NSA and CIA, terrorist organizations, and individual citizens who are subjected to surveillance.

Methodologies

Research Question: What motivates the United States government to take action with respect to government surveillance, and what approaches does it use to surveil its targets?

To answer this research question, the project will use the Wicked Problem Framing and Policy Analysis methodologies. The Wicked Problem Framing technique observes the actions taken to solve a problem and analyses the hidden consequences of those actions (Seager, Selinger, & Wiek, 2012). With this technique, the project will discuss foreign and domestic terrorism and crime as a motivation for surveillance, and also connect the US initiatives of surveillance to fight crime and terrorism with the issues of data privacy of American citizens. Policy of analysis of legislation which gives power to or revokes power from the US government to conduct surveillance will be conducted. Relevant documents include FISA, Executive Order 12311, the Patriot Act, and the FAA. The project will also explore unclassified and leaked government surveillance programs such as PRISM. These documents will be assessed chronologically, in order to better assess how the reasons behind surveillance evolved over time.

Conclusion

The technical project outlined in this proposal describes an end-to-end encrypted web service allowing for two parties to securely transfer files with strong guarantees of privacy. This project will consist of two components. The first component is the client, which encrypts and decrypts data that is sent to or received from the server. The second component is the server, which maintains a mapping between human-readable usernames and public keys, and facilitates the secure transfer of files between clients.

The STS research paper will provide an analysis of the programs and methodologies used by the United States government to surveil its citizens and other targets, as well as the ordinances and legislation which grant or deny the government to conduct such surveillance. The reasons and motivations behind the surveillance and legislation concerning it will also be assessed. The research project and technical project aim to address issues of data privacy and offer insight on how the need for security and the right to privacy might be balanced in the modern world.

References

- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. *Pew Research Center*.
<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- Clift, A. D. (2003). Intelligence in the Internet Era. *Studies in Intelligence*, 47(3), 73-79.
- Cressman, D. (2009). A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation. *ACT Lab/Centre for Policy Research on Science & Technology*.
- Delaney, K. (2020). The USA Patriot Act and Privacy: A New Frontier of Mass Surveillance. *GPSolo*, 37(5), 34–37.
- Domestic Surveillance Overview. (2015). *Congressional Digest*, 94(10), 2–32.
- Executive Order 12333 – United States Intelligence Activities. (n.d.). *Department of Defense Senior Intelligence Oversight Official*.
<https://dodsioo.defense.gov/Library/EO-12333/>
- Geiger, A.W. (2018, June 4). How Americans have viewed government surveillance and privacy since Snowden leaks. *Pew Research Center*.
<https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/>
- Kelly, T. (1998). "The Myth of the Skytale". *Cryptologia*, 22, 244-260.

Kim, H. (2018). The Resilient Foundation of Democracy: The Legal Deconstruction of the Washington Posts's Condemnation of Edward Snowden. *Indiana Law Journal*, 93(2), 533–548.

NSA Surveillance. (n.d.). *American Civil Liberties Union*.

<https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance>

Porter, J. (2020, February 12). WhatsApp now has 2 billion users. *The Verge*.

<https://www.theverge.com/2020/2/12/21134652/whatsapp-2-billion-monthly-active-users-encryption-facebook>

Rusbridger, A., & MacAskill, E. (2014, July 19). I, spy: Edward Snowden in exile. *The Guardian*.

<https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill>

Savage, C. (2018, May 4). N.S.A. Triples Collection of Data From U.S. Phone Companies. *The New York Times*.

<https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html>

Seager, T., Selinger, E., & Wiek, A. (2012). Sustainable Engineering Science for Resolving Wicked Problems. *Journal of Agricultural and Environmental Ethics*, 25(4), 467–484. <https://doi.org/10.1007/s10806-011-9342-2>

Terror on the Internet: Questions and Answers. (n.d.). *United States Institute of Peace*.

<https://www.usip.org/publications/terror-internet-questions-and-answers>

Text: Bush Signs Anti-Terrorism Legislation. (2001, October 25). *The Washington Post*.

https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bush_text_102601.html

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions. (2007). *EveryCRSReport*.

https://www.everycrsreport.com/reports/RL30465.html#_Toc216168113