The NSA, Mass Surveillance, and the Fourth Amendment

The Fourth Amendment marked the repudiation by the United States of general search warrants, known as writs of assistance in colonial America. The Fourth Amendment affirms, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized” (US Const. amend. IV). Above all, the Fourth Amendment protects the privacy interests of U.S. citizens and their freedom from arbitrary searches. Justice Harlan in his concurring opinion in Katz v. U.S. provides a two-pronged test for determining whether the Fourth Amendment applies in a given situation, which has become the de facto standard today. In order to receive Fourth Amendment protection, a person must have a subjective expectation of privacy, and society has to deem that expectation reasonable (Katz v. United States). The emphasis on society – not Congress, law enforcement, the president, or judges – is important. With 62% of Americans opposed to the government reading any domestic email without a warrant and 71% of Americans opposed to the government listening to any domestic phone call without a warrant, there seems to be incongruity between government opinion and popular opinion in light of the recent NSA leaks (Dance).

On June 5, 2013, The Guardian published the first document, a court order that required Verizon to share telephone records for millions of Verizon customers with the NSA, of the NSA leaks by Edward Snowden, a former employee of the NSA contractor Booz Allen Hamilton. Since the initial NSA leak was released to the public, further leaks have slowly been published by various news outlets. These leaks have revealed controversial NSA projects such as XKeyscore, PRISM, MUSCULAR, and Tempora; encryption backdoors engineered by the NSA; data collection on foreign diplomats and leaders; phone tracking; video game infiltration; and research toward quantum computing. It is estimated that 1.7 million NSA documents were obtained by Edward Snowden, which would mean that only approximately 1% of the documents have been released to the public (Strobel). Glenn Greenwald of The Guardian has warned that the most egregious infractions by the NSA still have not been published.

The combination of the rapid growth of internet and smart phone usage and the fear of terrorism in the post-9/11 era have provided the foundation for the government to implement a mass surveillance system. Two major components of this mass surveillance system are the bulk collection of phone records and the monitoring of communications. The Foreign Intelligence Surveillance Act of 1978 clarified that the scope of the NSA was limited to foreign intelligence and implemented stricter requirements for the NSA to be able to gather data on Americans. Specifically, it required the NSA to obtain a warrant from the FISA court in order to monitor a person residing in the United States. However, the 2008 FISA Amendments Act
relaxed this restriction by allowing communications to be monitored without a warrant if at least one person in a communication resides outside of the United States. The bulk collection of phone records appeals to a different law, the Patriot Act through sections 214-216. These sections amend FISA to allow the NSA to collect the metadata associated with certain forms of communication if that metadata could aid in an espionage or terrorism investigation. While certain provisions within the Patriot Act have been deemed unconstitutional, sections 214-216 remain in effect.

Technology and innovation make it increasingly easy and seamless to collect data on a massive scale in secret. Edward Snowden’s leaks on the NSA show that the U.S. government has already started to cross the threshold of what U.S. citizens deem acceptable in terms of data collection. It is important to determine which elements of mass surveillance, if any, can be reconciled with the Fourth Amendment.

For CPSC 490 I plan to research controversial NSA programs through the primary documents of the Edward Snowden leaks and through the secondary sources accompanying the leaks to the public. The objective of this research will be two-fold. First, I plan to succinctly summarize what we can reasonably infer that the NSA is doing through their controversial programs, as well as identify interesting areas where the leaked documents are insufficient to draw conclusions. Second, I plan to dissect the particular processes of data collection – such as intercepting data traversing fiber-optic cables or exploiting encryption backdoors – and give a precise, technical description of what the NSA is doing. After this preliminary research, I plan to draw upon precedents set through Fourth Amendment legal cases to determine which exposed NSA projects are inconsistent with the Fourth Amendment. Finally, I plan to conclude with policy recommendations of laws and regulations to constrain the government’s collection and use of mass data to ways congruous with the Fourth Amendment, while allowing the government the flexibility and dynamism to provide security against terrorism and legitimate threats.

My principal deliverable will be a final paper that focuses on the four components delineated above: a summary of what the NSA is doing, a technical description of how the NSA conducts mass surveillance, an examination of the constitutionality of the NSA’s projects, and policy recommendations to clarify the Fourth Amendment in an age of technology and big data. Ancillary to this final paper will be smaller deliverables – an outline of each week’s readings along with a higher level synthesis after the outline in the framework of the four components above.

The syllabus for my CPSC 490 will be as follows:

I. Week 2 (1/20 – 1/26): Verizon metadata collection

II. Week 3 (1/27 – 2/2): XKeyscore, the NSA’s monitoring of browsing histories, emails, and chats

c. https://www.eff.org/document/20131211-svt-xkeyscore-sweden-meeting
e. https://www.eff.org/document/20131211-svt-xkeyscore-slide-swedish-example


III. Week 4 (2/3 – 2/9): PRISM

d. https://www.eff.org/document/2013-07-10-wapo-upstream
e. https://www.eff.org/document/20130823-guard-prism-payments
g. https://www.eff.org/document/prism-april-2013
i. http://www.theguardian.com/world/2013/jun/08/nsa-surveillance-prism-obama-live#block-51b36893e4b0cc6424372292


IV. Week 5 (2/10 – 2/16): NSA encryption backdoors and the NSA sharing data with the DEA/IRS

b. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security


V. Week 6 (2/17 – 2/23): MUSCULAR, intercepting data from fiber-optic cables among Google and Yahoo data centers

VI. Week 7 (2/24 – 3/2): Research toward developing a quantum computer

VII. Week 8 (3/3 – 3/9): Tracking phones, infiltrating video games, and religious targeting

VIII. Week 9 (3/24 – 3/30): Video spying, phone tapping, and the black budget
    c. https://www.eff.org/document/20130911-guardian-israel-sharing

g.  http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

IX.  Week 10 (3/31 – 4/6): Reserved for new developments

X.  Week 11 (4/7 – 4/13): Final paper: summary of what the NSA is doing and the technology that the NSA is using

XI.  Week 12 (4/14 – 4/20): Final paper: constitutionality of NSA projects

Works Cited


*U.S. Constitution.* Amend. IV.