Government Surveillance of American Citizens

Christel Lefort
November 25, 2012
Since the attacks of September 11, National Security has been a priority for the US government. Much effort, time and money has been spent in the interest of National Security. Many organizations and departments of the government are involved in national security measures and many committees have been formed. To add to this, many laws and acts have been put into place to allow the government to use electronic and technological surveillance in order to stay on top of what the terrorists are up to. This paper is not a political paper but some political background, including laws, is necessary to give perspective. The intent of this paper is to talk about the types of technology that are in use and the legal framework that supports this.

Throughout our history the government has performed surveillance of its citizens in one form or another. The method of surveillance made use of the technology of the time. Technological advances have made data mining and surveillance easier. It is very simple to capture electronic communications and to spy on people. This has been an area of contention for quite a while. Many groups and private citizens feel this is an invasion of privacy and a violation of the Fourth Amendment, which states “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”. (Constitution of the United States) One can argue that the Fourth Amendment wording applies to only physical items. However, our forefathers had no way of knowing what technology would bring. Even so, it can be applied to electronic communications as well.

Prior to September 11th, government surveillance was something we did not often hear about. Indeed, prior to Watergate, the infamous wiretapping incident by Nixon, government surveillance was not something most people considered, nor did our government. Watergate brought government surveillance to light. After Watergate, Congress did a study on the government’s intelligence gathering practices. The Foreign Intelligence Surveillance Act, FISA was the result of this study. It was introduced in 1977 and signed into law in 1978. The intent of this act was to set procedures for government surveillance of foreign powers/governments and agents of foreign powers, spies, terrorist groups to protect against
attacks and terrorist activity. This surveillance can include American citizens if they are suspected of espionage or of violating U.S. law.

The FISA Court was set up as a required component of this legislation. The purpose of the court is to review the warrant requests and either approve or deny them. The contents of the warrant requests are secret. The FISA court will only report how many warrants are requested, how many are approved and how many are denied. The contents or reasons for the warrants are not disclosed. Since the attacks of 9/11 the number of warrant requests and approvals has increased significantly. In 1979, 199 FISA applications were presented. All were approved. In 2011, 1745 applications were presented and approved. Very few warrant requests are denied. Over the last ten years only 11 applications have been denied. (Foreign Intelligence Surveillance Act Court Orders 1979-2011, 2012)

FISA does make provisions for warrantless surveillance. The President can request warrantless surveillance through the Attorney General. Approval is granted for one year and the President has to show that the intelligence sought is from a foreign power and that the information obtained is from a US individual is not likely. The warrantless surveillance only applies to foreign powers. FISA does not make provisions for surveillance of agents of foreign powers/groups. Anyone who engages in surveillance that is not within the guidelines of FISA is subject to criminal and civil liabilities. FISA also allows the president to authorize surveillance for a period, not to exceed 15 days, at the beginning of a war but again this surveillance should only be of a foreign government.

In addition to FISA, Congress could foresee a need to protect the privacy of Americans and put legislation in place that specifically addresses electronic communications. The Electronic Communications Privacy Act (ECPA), an amendment to the Federal Wiretap Act of 1968, was enacted in 1986. This act protects electronic communications while in transit from source to destination and also while it is stored. This act also has guidelines for pen registers and tap and trace of telephone communications. Pen registers collect the numbers/source of incoming phone calls and tap and trace is the collection of outgoing/destination phone numbers. This piece of legislation has not been updated for twenty-five years and does not fully address all of today’s technologies as in evidenced in the lawsuit
against Google for privacy violations. While taking photographs for Google Street View the technicians collected ID’s, passwords and other personal information from individuals’ Wi-Fi networks.

The attacks of September 11th brought about the US Patriot Act which is an amendment to FISA. The title USA PATRIOT is an acronym for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. This act broadens the scope of surveillance to include domestic terrorism and the types of surveillance conducted. It is this act that is used as justification for warrantless surveillance. The warrantless surveillance covers every type of electronic communication from cell phone conversations and texts to email and also includes web surfing habits. The concern with this warrantless surveillance of our electronic communications is that it violates our Fourth Amendment rights. By passing this act, Congress essentially allowed the monitoring of communications and conversations without FISA warrants. They authorized the FISA court to approve electronic surveillance without showing reasonable cause or warrants. Lisa Graves, Executive Director of the Center for Media and Democracy states, “The specially created FISA court has issued more orders for electronic surveillance in the ten years since 9/11 than in the entire previous 22 years (more than 15,661 FISA orders approved since 2001 versus 13,102 between 1978 and 2000).” (Graves, 2011) Parts of the act were extended by President Obama in May 2011. Additionally the Obama administration has granted immunity to the telecommunications companies from any lawsuits that accuse them of complicity in the eavesdropping program. The stated justifications for the warrantless surveillance have been the War on Drugs and the War on Terrorism.

The average American sleeps well at night believing their electronic communications are private. Since the attacks of September 11 this has not been the case. Our electronic communications, including email, browsing habits, cell phone conversations and even text messages have been collected by our government.

The government has taken full advantage of technology to gather information. One of the first documented forms of surveillance is wiretapping. Wiretapping came about in the 1800’s after the invention of the telegraph and telephone. The practice was made illegal in the 1890’s but in 1928 the
United States Supreme Court made wiretapping Constitutional for the police and government officials. Over the years there have been many instances of wiretapping that have become public including with infamous Watergate scandal and of Illinois Governor Rod Blagojevich over President Obama’s vacant senate seat. Wiretapping involves attaching a phone or listening device to the phone line that runs outside of the house. Installing bugs is more convenient however. A bug is a transmitter that can be installed inside a phone and then transmit the voice conversations via radio signals to a radio receiver. (Harris)

Pen register and tap trace devices have been used by the government for many years and are fairly common because warrants are not always needed and the information is easy to obtain. (Gosztola, 2012) Pen registers and tap traces began as electronic devices that were installed on the telephone circuits. As technology has progressed, software has been developed to serve the same function. Pen registers capture the phone numbers dialed along with the call time, whether the call connected and duration. Tap trace devices capture the same information for phone numbers of calls coming in to a phone. Technology has also made it possible to capture the owner of the number and in some cases the location of the receiving end of the call. (What is a Pen Register?) The use of these devices began with regular land line phone but now encompass cell phones as well. SMS text messages are also being intercepted as well as numbers dialed after connecting such as mailbox passwords. (Surveillance Self Defense "Pen Registers" and "Trap and Trace Devices")

Today everything from web surfing habits to text messages are saved. Various means are used to gather the information. Much of the information is gathered from the cellular phone providers. Black boxes are placed at the cellular provider’s data centers. These black boxes collect all the cell phone conversations as well as texts. Information is also gleaned from the Internet; our web surfing histories as well as emails are collected. The data gathering is not limited to only electronic data. Cameras to capture faces in specific locations are used as well.

Throughout the years since 9/11 there have been several projects by the Department of Justice and the National Security Administration and the military to capture the data flowing through the telecommunications networks. Most of this has been very secret. However in 2005 Mark Klein, a former
AT&T employee blew the whistle and testified as a witness against the US Government. He cited that there are connections from the NSA into AT&T in an effort to capture all telecommunications made by American citizens. Klein provided information regarding a room, 641A, located in the AT&T building in San Francisco that housed equipment, including a Narus STA 6400 used for data collection, installed by the NSA. Former director of the NSA’s World Geopolitical and Military Analysis Reporting Group, William Binney, has estimated that 10 to 20 such facilities have been installed throughout the nation. (Bamford, 2012)

That same year the Electronic Frontier Foundation (EFF) filed a lawsuit against AT&T based on Mark Klein’s claims. The lawsuit sought redress for the illegal and unconstitutional, ongoing dragnet surveillance of communications and records. The case was dismissed in 2009 due to the retroactive legislation in FISA which protects the telecommunications companies.

The advances in technology make government surveillance easier and easier to hide. Information about the surveillance programs is difficult to find and some of it is based on rumors. The current laws also seem to work to allow the surveillance and what doesn’t work is cited as State Secrets. Between technology and the current legislation it is very easy to abuse surveillance and infringe upon our privacy. Over the past decades the surveillance programs that have come to the attention of the public are the FBI’s Omnivore and Carnivore. The military operated under Threat and Local Observation Notice (TALON). The NSA has been the most secretive. As mentioned earlier, the name for their program is not known but is referred to as the Terrorist Surveillance Program, TSP. It is also rumored that they are building a network called Echelon which is sometimes confused with the FBI’s Carnivore.

The FBI started using Omnivore in 1997 and retired it in 1999. Omnivore was attached to a specific internet service provider. Omnivore was a network sniffer that targeted email traffic from a specific source.

DragonWare Suite replaced Omnivore. It provided the sniffing of email traffic but also was able to reconstruct email messages, files and web pages. The suite was comprised of Carnivore, Packeteer and Coolminer. Carnivore was the actual Windows server that the sniffing software ran on. No official
information has been published for Packeteer or Coolminer but it is assumed that Packeteer assembled packets and Coolminer was used for data mining. (Tyson)

Packet sniffers, together with a network interface card configured to operate in promiscuous mode, capture all packets that come through the network rather than just the packets that are intended for that computer. These packets can then be copied and saved in volatile memory or on the hard drive for analysis at a later time. Filters can be applied to save specific packets or all packets can be saved.

The FBI claims it obtained warrants to collect data for specific targets. It used the tool to collect data for specific crimes: terrorism, espionage, child pornography, fraud and information warfare.

Carnivore was controversial because of what it was capable of and the cooperation the FBI received from the Internet Service Providers. It was abandoned early in 2005 for commercially available eavesdropping software.

The Threat and Local Observation Notice (TALON) program being conducted by the military has also been a concern for many. TALON authorized civilian and military personnel to provide reports on persons engaged in suspicious activities. It has been rumored that the military maintains a database on persons suspected of conducting anti-war and counter-military protests and demonstrations. There was also a concern that this information was not obtained legally. The Department of Defense maintains that any information it collected was obtained legally. The DoD issued a report in response to these claims.

“The TALON report program was instituted DoD-wide on May 2, 2003, by Deputy Secretary of Defense memorandum, “Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States,” because DoD had no formal mechanism to collect and share non-validated domestic threat information between intelligence, counterintelligence, law enforcement, and force protection entities and to analyze that information for indications of foreign terrorist activity. A TALON report consists of raw information reported by concerned citizens and military members about suspicious incidents. The memorandum also directs that TALON reports be provided to the DoD Counterintelligence Field Activity for incorporation into a database repository. The Counterintelligence Field
Activity is a designated DoD law enforcement and counterintelligence organization and serves as the bridge between intelligence related to international terrorism information and domestic law enforcement information. In addition, the Commander, U.S. Northern Command’s mission is to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within its area of responsibility.

The DoD claims they are collecting this information to assist law enforcement and not for intelligence purposes. According to the report the TALON reports were deleted because it was determined that they had no analytical value or no terrorism connection. (Inspector General The Threat and Local Observation Notice, 2007)

Other successors to Omnivore, Carnivore, and TALON continue to evolve. TrapWire and Strategic Forecasting (Stratfor) have been in the news as a result of a leak from WikiLeaks posted in August 2012. Abraxas has also been implicated. The controversy is the TrapWire surveillance system that has been installed at key points around the nation to collect pictures of persons engaged in suspicious activity.

TrapWire is a predictive surveillance system that can be used for evaluating predictive behavior in counterterrorism. The system is an attack prevention system which is different than a typical surveillance system. The details of how the system is being used by the government differ. Some sources say that surveillance cameras have been installed around the country at high-profile locations. Images of people taking pictures, parked cars or any other suspicious activity is recorded and sent to a data center to be compared with other activity and analyzed. Others maintain that pictures are taken every second, encrypted and then sent to a data center at an undisclosed location. The data is then aggregated with other intelligence. (Chen, 2012) As with the other means of surveillance, data regarding the program is limited.

Stingray is a relatively new device that has been put to use by law enforcement agencies as well as the military. Stingray is a cell phone location tracking device that can track the location of a cell phone even when it is not in use. It was used to track the location of Daniel David Rigmaiden, also known as
‘the hacker’ in order to make an arrest. The details regarding the use of the devices have not been made public but guesses have been made as to how they work. It is suspected that they use an antenna, mapping software installed on a computer and an undefined device. According to Jennifer Valentino-DeVries, “The device mimics a cellphone tower and gets the phone to connect to it. It then collects the hardware numbers associated with the phone and can then ping it even though a call is not being made.”

University of Pennsylvania professor and former AT&T Labs researcher, Matt Blaze says that “the antenna can be pointed at a location and then the hardware numbers can be collected. The numbers are then used to determine which phones are in a given place at a given time.” The device can also be used when the number is known but not the location. Officials can ping the phone and once they get a signal they can use the signal strength to home in on the device. (Valentino-DeVries, 2011)

The use of drones by the US military over in the Middle East has been publicized in the news over the last year. It seems however, that many law enforcement agencies are beginning to use them as well and have made requests of the FAA to be allowed to fly them. The intent is for surveillance. The cities of Miami, Seattle and the Texas Department of public safety all use drones. They are equipped with video cameras for daytime use as well as infrared cameras for night time use. (Koebler, 2012)

The programs conducted by the NSA have been the most secret of all. Not much is known about them. Most recently it has come to light that the NSA is continuing to conduct electronic surveillance. The details of the whether or not this surveillance is constitutional or not is still a mystery as are the types of information they are collecting and whether or not that information is all unencrypted. The building of a large facility in Utah leads one to believe that they are expecting the TSP to grow. It has been reported that the facility will not only capture information flowing across the telecommunications networks but it will also be capturing financial data and have code-breaking equipment and experts.

The rapid pace of technological advancements makes surveillance of criminals very easy. This same advancement can potentially be abused and ultimately infringe upon the average citizen’s right to privacy. The current legislation has difficulty in keeping up with the pace of technology. Though the courts seem to agree that warrantless surveillance is an invasion of privacy and violates our rights under
the Fourth Amendment, these cases are often times dismissed on the grounds of State Secrets. The government continues to address the concern of National Security in different ways but the legislation seems to fall short of protecting privacy.
Bibliography


