Illegal Espionage

Levi Seibert

Athens State University

CJ301: Criminal Justice Process

Dr. Quanda Stevenson

November 13, 2021

Abstract

This essay considers the legality (primarily in concern to the Fourth Amendment of the U.S. Constitution) of multiple surveillance methods preformed by the federal government. Topics including communications interception, personal data access, and information harvesting are all investigated, and their lawfulness is discussed. Considering the programs currently in operation, it is quite clear that the U.S. government has committed crimes of constitutional weight.

Illegal Espionage

Today's world is built around technology. Nearly everyone carries around a phone, and desktop computers and laptops are available for most people at a moment's notice. With the capabilities of the World Wide Web, people use the Internet for a wide range of activities, many of which (if not most) they would consider personal and private. But what ensures their confidentiality? Are there any regulations in place to protect this data? The Fourth Amendment to the U.S. Constitution protects against unreasonable searches and seizures. That being said, the amendment only outright mentions persons, houses, papers, and effects. Do these protections also apply to modern concepts such as the use of technologies, and if so, to what extent? Thankfully, further legal rulings (and some logical deductions) add to the Fourth Amendment, explicitly prohibiting technological espionage by the government, including programs that intercept private communications, access personal information without permission, and collect "confidential" data from tech companies.

First and foremost, the interception of private communications has clearly been ruled unconstitutional. The landmark Supreme Court ruling regarding this issue is that of *Katz v. United States*. In this case, law enforcement officers had warrantlessly wiretapped a public phone booth that Mr. Katz used for private communications. The Court ruled that even though law enforcement had probable cause that he was committing a crime, the wiretap infringed upon Katz's Fourth Amendment Rights, because they did not have a warrant (Dezao, n.d.). This case set the precedence of warrantless interception of private communications being deemed illegal and unconstitutional. The government, however, seems to have an infatuation with spying on the private interactions. In 1978, Congress passed the FISA (Foreign Intelligence Surveillance Act), which established courts in which the executive branch could request warrants to surveil foreign

individuals and terrorist suspects. The FISA Court, however, handed out warrants without many requirements for criminal proof (ACLU of Massachusetts, n.d.). This allowed the government to have the legal standing to pursue "investigations" on individuals in order to protect the country. After the September 11, 2001 terror attacks, the rules began to change even more. President George Bush authorized domestic surveillance of personal telecommunications and email messages, in the name of security. This monitoring did not require a warrant and therefore was in direct contradiction to the ruling of *Katz v. United States* (and as Supreme Court ruling, this case had constitutional weight). It also did not abide by FISA, Title III, or the Electronic Communications Privacy Act, all of which set the rules regarding federal espionage ("NSA Spying on Americans is Illegal", 2006). Therefore, governmental surveillance, though not legal, has been, and still is, permitted.

In addition, the law of the country also guards against governmental access to personal data. The Fourth Amendment protects citizens' papers and effects from unreasonable searches. While the term "effects" is difficult to define, papers, during the time of the Constitution's writing, were one of the most private media of communication that existed (think of diaries, for example). If personal data was protected in the late 1700s, then should it not also be today? Unfortunately, however, the protections provided by the Constitution have been undermined by the USA/Patriot Act, passed in late 2001 as a result of the 9/11 terrorist attacks. This act, which Congress was pressured by the Bush administration into passing, altered the rules of surveillance and permitted the increase of unchecked government power. In the name of national security, it empowered the government to perform unconstitutional searches of personal records and private property, in addition to other constitutional grievances ("Surveillance Under the USA/Patriot Act", n.d.). As a result of the Patriot Act, federal law enforcement can now "legally" search

through personal data with barely any oversight. As long as the data is deemed to be related to terrorism or national security issues, the government has seemingly free reign to harvest what they desire, even without any notification to those affected. This infringes upon First, Fourth, and Fifth Amendment rights ("Surveillance Under the USA/Patriot Act", n.d.). A related issue is that of the warrantless seizure of cellphone devices, a topic of much judicial debate. Many courts (*United States v. Murphy*, *United States v. Finley*, etc.) have decided that confiscations incident to an arrest are constitutional, in accordance with the standard practice of searches and seizures incident to arrests. However, others (*United States v. McGhee*, *United States v. Park*¸ and others) have ruled that since cellphones do not necessarily pose any danger to the officer during or after an arrest, seizures of these devices are unreasonable (Brill, 2012). If cellphones do not inherently pose any danger, then why does personal data? If personal data causes no harm in of itself, then why can it be freely searched by the government?

Another form of espionage that is legally prohibited is that of the collection of information about citizens that is considered private and confidential. A distinction needs to be made between the "search" and "seizure" of personal data. In the first case, the user's data is stored by a entity and the government asserts the authority to have access to that data. In the latter, however, information (which the user might not even know exists) is actually taken by the government. The true realities of such data seizures were revealed by a man named Edward Snowden, hailed a hero by some and a traitor by others. Snowden released documents describing programs being executed by the National Security Agency that directly attacked the rights of United States citizens. One of the main programs he unveiled was that of Prism. This initiative allows the NSA to harvest individuals' metadata from tech companies, and thus have the ability to build profiles on Americans (once again, permitted by the Patriot Act). Snowden

also brought the program named Upstream to light. Upstream is very similar to Prism, but the data is basically tapped during transmission rather than handed over by a third party (Dezao, n.d.). Similar to the previously mentioned government searches of private information, these seizures by nature conflict with the Fourth Amendment protections. Although programs like Prism and Upstream apparently are permitted under FISA, they are unreasonable and unwarranted. Also, since data communications are very similar to voice communications (from a technological point of view), *Katz v. United States* seems to also have application. Because the warrantless wiretapping of Mr. Katz' phone was ruled unconstitutional, so is the collection of private data (Dezao, n.d.). Likewise, video surveillance by the government is also an infringement of personal privacy that falls under the category of confidential information. This process, like the other ones formerly mentioned, allows the government to "map" out the lives of Americans, without their permission or knowledge. Although there is not necessarily a definitive Court ruling stating that this is illegal, Pacific Legal Foundation attorney Daniel Woislow claims that the Fourth Amendment in of itself is the greatest protection against a surveillance state (2020). Perhaps someday the same will be true for all forms of confidentiality infringements.

Many personal privacy protections have been abandoned by the federal government in the name of national security. However, regardless of how pressing the need, the Fourth Amendment (and Court rulings that have followed) hold Constitutional weight and cannot be forsaken. Any infringements upon the foundational principle of privacy in the United States (especially by the government) is an instance of illegal espionage.

References

ACLU of Massachusetts. (n.d.). *Fourth Amendment Protections*. Privacy SOS. Retrieved October 17, 2021, from https://privacysos.org/Fourthamend/.

Brill, A. (2012). *Warrantless Cell Phone Searches and the Fourth Amendment: You Think You Deleted Those Text Messages…But You Have No Idea…*. Seton Hall University. Retrieved September 24, 2021, from https://scholarship.shu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1003&context=student_scholarship.

Dezao, J. (n.d.). *National Security Agency & the Fourth Amendment*. Retrieved September 24, 2021, from https://scholarship.shu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1763&context=student_scholarship

NSA spying on Americans is illegal. American Civil Liberties Union. (2006, February 6). Retrieved September 24, 2021, from https://www.aclu.org/other/nsa-spying-americans-illegal.

Surveillance under the USA/Patriot Act. American Civil Liberties Union. (n.d.). Retrieved October 17, 2021, from https://www.aclu.org/other/surveillance-under-usapatriot-act.

Woislaw, D. (2020, January 3). *How the fourth amendment can protect us from becoming a surveillance state*. Pacific Legal Foundation. Retrieved September 24, 2021, from https://pacificlegal.org/how-the-fourth-amendment-can-protect-us-from-becoming-a-surveillance-state/.