The Backdoor to Privacy in the Digital Realm

Jessica Peregrina
Pre-law

Introduction
Since the exposure of the NSA’s access to the metadata of calls made by Verizon customers back in 2013, there has been a nationwide discussion over whether or not their actions can be considered constitutional (Black). Although a majority of American citizens viewed the NSA surveillance as an “acceptable way for the government to investigate terrorism,” nevertheless, 41% of Americans still believed that it was unacceptable (Pew Research Center). In turn, this caused the ongoing debate that it was unacceptable (Black).

Fact Pattern
On March 21, 2016 during the Apple Inc. Keynote Event Tim Cook the company’s CEO announced to his audience and viewers that the company has the responsibility to protect the data and privacy of its consumers. The statement given by Apple sparked debate over security and privacy because the Federal Bureau of Investigation(FBI) asked Apple to voluntarily assist in unlocking an iPhone 5C that had been owned by the San Bernardino mass shooter, Syed Rizwan Farook who killed fourteen people and seriously injured twenty-two in December of the previous year. The iPhone was lawfully seized during a federally mandated search and seizure of a black Lexus that belonged the Farook. The FBI had discovered some encryption in the phone and asked Apple in February to assist since they believed “Apple has the exclusive technical means which would assist the government in completing its search” (Wilkinson). In a statement given by Tim Cook after the first request by the U. S. Government, he made it known that what they were asking for was something they did not have and something they considered “too dangerous” because it asked them to “build a backdoor to the iPhone” (Nakashima). Apple refused to assist in creating and installing a software that will make its users’ “most confidential and personal information vulnerable to hackers, identity thieves, hostile foreign agents and unwanted government surveillance”(Theodore J. Boutrous). The government argues they are merely seeking information from one isolated iPhone and not trying to breach any privacy. The question proposed is whether Apple’s resistance to breach their users’ privacy is inflicting a breach in national security?

My Response
As citizens of the free world, there are amendments in place that protect the individual from not only unwarranted search and seizures but also privacy. As we discovered in United States v. Jones, the violation of the subjective expectation of privacy was violated even when no physical intrusion did not take place. We can take the information from this case and apply it to the fact pattern. Justice Scalia mentioned in his opinion in Katz v. The United States that an “effect” can be protected by the Fourth Amendment and in this case the “effect” can be the already existing software that protects Apple users from losing such privacy. In turn, it would cause law abiding citizens to rebuke any rights that protects their privacy. Those who argue that they have nothing to hide are losing sites of the dangers that the backdoor creates. Not only are you giving the government permission to have unlimited access to your private information, this software allows other people from accessing your information at no cost. It is also important to remember that by no means is Apple protecting Farook, owner of the iPhone. Similar to the majority of the U.S. population, Apple demands justice in this case, just not at the expense of American citizens losing their privacy.

Significant Cases
Katz v. The United States:
Katz appealed argued the recordings of his private conversations violated his fourth amendment rights of unreasonable searches and seizures and the Supreme Court voted in a 7-1 decision in favor of Katz (Oyez). The Supreme Court to favor Katz came from the fact that the Fourth Amendment protected him because he had the intentions of keeping his conversations private regardless of it taking place in a public space. United States v. Jones:
The Supreme Court held that “the Government’s installation of a GPS device on a target’s vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a ‘search’ (Justice Scalia). In addition, Justice Scalia argued the GPS constitutes as an effect which is protected by the Fourth Amendment.

Conclusions
The debate concerning the importance between national security and privacy has wavered for a while after the NSA exposure of unwarranted surveillance but has recently restarted after Apple’s refusal to assist the FBI. Even with cases like United States v. Katz, we are still faced with some uncertainty. I believe that the only we can be protected from unwarranted searches is by either updating or creating laws that specifically include the digital realm and until this happens we are merely going through obstacles in order to protect our privacy.