Smartphones have been gaining popularity ever since the first iPhone was released in 2007. I can speak from personal experience, I have a lot of private content on my smart phone (whether it be pictures, passwords, or email) that I trust Apple to protect. But at what point does public safety outweigh privacy? The upholding of computer ethics is a delicate subject and is often publicly debated. On December 15, 2015, 2 men opened fire in San Bernardino, which resulted in the death of 14 innocent Americans. Rizwan Farook was one of two shooters, and the government has been trying to force Apple to help bypass his iPhone’s security features in order to gain information on future attacks (Laurie Segall). Apple refused to assist the FBI in hacking Farook’s iPhone because it would have set a dangerous precedent within the company. Apple is committed to upholding civil liberties and collective security of its users. An Apple executive writes, “law enforcement does not understand the consequences of creating a back door.” With this being said, the FBI decided to give up on seeking help from Apple completely and decided to contact a third party in hopes they could crack the iPhone. The iPhone was successfully hacked into. During an interview with an FBI official, he refused to disclose the name of this 3rd party company and was quoted saying “I am not at liberty to disclose if we will be sharing this (hole in the system) with Apple or not.” This raises another ethical dilemma: should tech companies be made aware of flaws in their products or should crime-fighting organizations exploit these bugs as crime fighting tools? The fact that the DOJ (Department of Justice) was able to successfully access the phone without Apple’s help is bad news for the global tech giant because it suggests Apple’s encryption technology is not as advanced as we once thought. Experts have agreed that the government has no legal obligation to provide this new-found information to Apple, but may be morally obligated. If the information is not disclosed, our enemies could soon find the same bug in Apple’s software and hack into American’s phones with ease. Even the White House’s cybersecurity coordinator has been quoted saying there are times when more people could be harmed by an unfixed security bug than helped by the government using these bugs as part of an investigation. So many moral and ethical debates have sprouted from this San Bernardino case. This topic interests me because I am an iPhone user, and I feel like my privacy is at risk. To be honest I am confused as to why Apple denied the government access to the iPhone when Edward Snowden has already exposed the government’s surveillance of its citizens (with help from large companies) a few years ago. This was a larger scale ethical dilemma that paved the way for the outcome of this San Bernardino case. I personally believe Apple should have just helped the FBI so the information was not available to this unnamed third party who could just be looking for the highest bidder in the future.
Work Cited

