Apple vs Government

The last two decades have left the world completely mutated by a new era of rapid technological development. Characterized by little widespread understanding of new technologies and absolutely no regulations on the industry’s programming practices, this new world has seen numerous complications and worries arise. The greatest of these complications has been the debate over what level of privacy these new devices should allow. In just the last five years there have been countless examples of cases where tech companies are in opposition with the government on this issue, and there is sure to be many more in upcoming years. One such example, and arguably the most important, happened in December 2015 when the FBI retrieved a work-issued iPhone 5c from one of the shooters who took part in the terrorist attack in San Bernardino, California.

The passcode protected iPhone that was recovered was set to delete all of its data after ten failed attempts at entering the code, an attribute of Apple’s iOS 7 software. Due to the way Apple programs its’ phones, it is impossible to use a hacking algorithm to gain access to one of the phone’s passcode. As a result, the FBI ordered that Apple create a backdoor into their phones for future government access. Apple declined to produce the software and trial ensued. Throughout the trial Apple strongly stuck their position of denying the request in order to uphold the privacy of their clients. The question is, was this the correct position for Apple to take?

Upon first being issued the governmental order to create the software, Apple believed the request was “unreasonably burdensome,” citing the security risks that the creation of a backdoor would pose towards customers. Tim Cook issued a statement to Apple’s customers explaining their motives saying that while the company respects the FBI, their request threatens data security by establishing a precedent that the U.S. government could use to force any technology company to create software that could undermine the security of their products. This precedent would impede on Apple’s promise of privacy within their phones and, more importantly, the existence of this software would not only give the FBI access to any iPhone, but it would also make it possible for other government agencies, hackers, and Invaders to bypass the passcode on any iPhone they want by gaining access to the software.

The FBI’s position stemmed from the belief that the creation of the software would be in the interest of the greater good. They believed by gaining access to the recovered phones of terrorists they could unveil future terrorist activity as well as potentially root out other cohorts of terrorist denominations. The FBI’s defense of the order was founded on using the All Writs Act to compel Apple to write the software. The All Writs Act authorizes the United State federal courts to “issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law” (codified at 28 U.S.C section 1651). The use of this act was unprecedented and according to experts would lead to “an epic fight pitting privacy against national security” (Dolan). They also pointed out that the implications of the legal precedent that would be established by “the success of this action against Apple would go far beyond the issues of privacy” (Davidson).

Apple stood to defend the privacy of its customers and protect their values of concealment of private client information. Against them stood the FBI looking to pursue what they believe to be the best interest of society. So, who was right? By not producing the software Apple may be protecting the information of their over 700 million iPhone users, but they could also be restricting access to critical information in preventing terrorist activities that could bring incalculable casualties and pain worldwide. On the other hand, if the FBI was granted ability to access the phones, government agencies, hackers, and others would have the ability to crack into these phones taking the information they want, but future terrorist activities might be stopped. It is a hard decision to make, and in the end, these new debates of privacy are so hard to analyze because the right answer is subjective to the person.

Support was widespread for both groups. Support for Apple came from major tech firms Microsoft, Facebook, Yahoo, Twitter, and LinkedIn. Support for the FBI stemmed from some families and victims and survivors of the attack, the National Sheriffs’ Association, and surprisingly Bill Gates. There are countless ways of looking at the situation, but the most widely used perspective is that of the utilitarian, namely, a moral ideology in which a person chooses a situation they believe would produce the greatest good for the greatest number of people. While this sounds like a good approach, inherently, any type of argument for either position in this case based on this moral ideology falls short of creating a definitive answer. It is not possible to determine how much damage letting untethered access to iPhones would cause. Regardless of the large number of users, it is impossible to tell how many of those users would be able to be attacked and moreover, how many would have information on their phone that would cause harm to them if given to the wrong people. It is also impossible to tell how many will suffer from terrorist activities that could be stopped by giving the government backdoor access.

As a result, the answer to which side is correct is impossible to answer. What is certain is this is only the beginning of the fight between companies and the government for how much of people’s privacy online is protectable and what access the protective agencies need. We see this issue with this case against Apple, Facebook’s recent issue with collecting data, and Google’s current issue with the government also concerning data collection of its users. The technological industry is developing at unprecedented rates and it is only speeding up, so as we delve deeper into the unknown territories of the wild west that is Silicon Valley, only time will tell where regulation over cyber-privacy will travel to.

Works Cited

Davidson, Amy (February 19 2016). “The Dangerous All Writs Act Precedent in the Apple Encryption Case” *New Yorker*. Retrieved February 7, 2020.

Dolan Maura; Kim, Victoria (February 18 2016) “Apple-FBI fight over iPhone encryption pits privacy against national security” *Los Angeles Times.* Retrieved February 7, 2020.