Setting Precedence: Apple vs the FBI

Author : Cat

Date : March 6, 2016

The ease of access for digital data has blurred the lines between what is an invasion of privacy and what is free for the taking. Edward Snowden opened the floodgates in 2014 when he revealed that the FBI had been using data from cell companies and social networks without users consent. This was rectified by stringent security created by the device and digital service makers. We are now at another crossroads with new technology. If a criminal has digital data that is protected by technology, what efforts are tech companies expected to take towards accessing that private data? And at what risk to all other users? That is the battle Apple is now facing with the FBI.

Background: On December 2nd 2015, a man and woman opened fire at a company party in San Bernardino where they killed 14 people and injured at least 22. Mr Syed Rizwan Farook, 28, had been employed by the county health department for 5 years and his wife, Tashfeen Malik, 29, was a stay at home mother to their 6 month old baby. The attack was premeditated and later confirmed as an intentional act of terrorism. Both shooters were killed by law enforcement in their attempt to escape the situation.

The FBI is looking to create a full picture of who is attached to their terror group and how Farook and Malik become involved. They have taken to combing social media accounts and online profiles. The FBI also retrieved Farook's phone, an iPhone 5, but were unable to unlock it. The

safety mechanisms that Apple designed to protect the device from hackers, are the same that have prevented the FBI from gaining access. The security code exists in the operating system level and cannot simply be unlocked using a magical code or sequence.

The request the FBI is making to Apple is that they create a new operating system for this device which would allow them to access the data. Sounds simple enough, but once created, this software *hack* or *backdoor*, could be used by any hacker or government agency again. Put a secret in a lockbox with only one key, that secret remains safe if the key goes missing. If it turns out that you can make a master key for all boxes, then no lockbox of that variety can ever be considered safe again.

What's troublesome in this case is that we know for a fact that the criminal in question is guilty and the FBI feels they owe it to the families of the victims, as well as the world, to see that every piece of evidence is collected to ensure this will not happen again. BUT if Apple complies, then they are compromising the security of every other user.

Apple declined to make the changes so the FBI has filed a court order to have it done. To date, over 25 tech companies, including Facebook, Twitter and Google, have filed 'amicus briefs' to back Apple in their position. The brief includes the following statement:

> Cell phones are the way we organize and remember the things that are important to us; they are, in a very real way, an extension of our memories. And as a result, to access someone's cell phone is to access their innermost thoughts and their most private affairs.

Personally, I am glad to see Apple make a stand against this request. Though enabling law enforcement to access data is important, the precedent set if tech companies are forced to do this puts us back to where we were with the government before privacy became an issue. And we'd be potentially creating tools for hackers as well.