PACIFIC COAST BUSINESS TIMES®
www.pacbiztimes.com
Feb. 26 - Mar. 3, 2016 | Proudly serving Santa Barbara, Ventura and San Luis Obispo counties | Vol. 16, No. 52

Future of privacy at stake in Apple v. FBI

By Lisa Spiwak

A highly contentious legal battle is brewing between Apple and the FBI. The FBI has been trying to hack into the encrypted iPhone belonging to Syed Farook, one of the San Bernardino shooters in the Dec. 2 attack that killed 14 people. The Apple iPhone, which was actually issued by the county of San Bernardino, has encryption software on it that completely wipes out any data on the phone after 10 failed attempts to guess the password. The FBI is very interested in retrieving the data on the telephone because they want to determine whether the shooters were working with a larger terror cell.

The FBI has not asked Apple to compromise its encryption. Instead, the FBI is asking Apple to create a custom version of iOS that disables the self-destruct feature that erases the phone's data after too many unsuccessful attempts to unlock it. Apple has refused to build a version of iOS that would bypass its encryption security. Apple has refused to do so because it believes that in the wrong hands, this software would have the potential to unlock any iPhone in someone's physical possession. Apple argues that, even if the FBI agrees that the software would only be limited to this case, there is no way to control that.

The FBI is extremely frustrated. All of this encryption software is giving criminals, terrorists and spies an unparalleled ability to communicate with each other worldwide. This gives them a huge advantage against the FBI and makes it harder for the FBI to uncover terrorist plots in order to keep us safe.

Perspective

FBI Director James Comey needs companies to figure out a way to supply necessary information to help aid investigations. He stated that "we understand that encryption is a very important part of being secure on the Internet, but we see that encryption is getting in the way of our ability to have court orders effective to gather information we need in our most important work."

On the other hand, Apple CEO Tim Cook argues that creating "backdoor" software to override their encryption software makes their systems dangerously weak. He said that once the software exists, Apple will face increasing pressure to provide it to law enforcement authorities across the world and will be unable to control who uses it and for what purpose.

A prime example of what Apple fears occurred with the first cyber weapon created, called Stuxnet. Stuxnet is a malicious computer worm built jointly by America and Israel during the Obama administration to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents. Stuxnet specifically targets machines using the Microsoft Windows operating system and networks and causes the fast-spinning centrifuges to tear themselves apart. Unfortunately, Chinese hackers got a hold of the software and used it to gain access to crucial U.S. infrastructure, including our electric power grids, oil and gas pipelines and water supplies. It was a disaster.

At first blush, it would seem that the FBI's ability to keep the American people safe should trump a cell phone user's ability to use encryption software on their telephone. However, when you see what transpired with the Stuxnet debacle, it becomes clear how problematic the creation of this "backdoor" software can become in the wrong hands. The dilemma that Apple faces in being forced to create this software is evident.

At this point, the stage has been set for a behemoth legal battle between the federal government and Silicon Valley. The outcome of this case will unquestionably determine the future for digital privacy and national security.

• *Lisa Spiwak is a partner with the firm Spiwak & Iezza in Thousand Oaks. Reach her a LSpiwak@SpiwakandIezza.com.*