Unlocking The Apple iPhone Sets A Dangerous Precedent

By Security Expert Scott N. Schober

Before jumping into the Apple vs FBI debate I must state that I've been a loyal Apple user since 1977 when I began programing on my first Apple computer. I'm also President/CEO of Berkeley Varitronics Systems, Inc. providing advanced wireless threat detection tools to various cyber groups within the U.S. government and I have a strong grasp on consumer privacy and government needs in forensic investigations involving phones and wireless data.

What Is Causing The iPhone Controversy?

The device in question is an iPhone 5c which was apprehended after the tragic San Bernardino terrorist attacks. The iPhone is password locked, encrypted and believed to contain vital evidence for the FBI. Though the smartphone was used by one of the alleged terrorists, it was technically owned by the county of San Bernardino, and given to authorities to be used in the investigation as they see fit. This is not a privacy issue, but that doesn't mean it couldn't become a privacy issue for all of us. The FBI is demanding that Apple create a software back door in this particular OS to capture the data from this single phone. Apple, who has cooperated with federal authorities many times in the past, refuses to create a backdoor saying once this software exists, it will render all iPhones susceptible to hacking. Details are unfolding but the latest involves an iCloud password reset that has FBI blaming San Bernardino, and San Bernardino blaming the FBI. Apple could have recovered information from the iPhone if the iCloud password had not been reset. Apple or the FBI could have simply taken the iPhone to a location where it recognizes the Wi-Fi network (likely at the shooter's home) and it could have been backed up to the cloud.

Apple CEO, Tim Cook, published an open letter to make a case to not allow this phone to be hacked or unencrypted by anyone including Apple – not even in this instance. He used words such as "slippery slope" and "backdoor" when faced with the idea that Apple may be forced to hack their own phone. Apple's concern is the FBI is asking for more than just data from that particular phone, but more of a cyber forensics hacking tool that would be entrusted to the FBI and federal government. NSA went on record endorsing the end-to-end encryption used in iPhone and FBI director, James Comey, accuses Apple of publicity stunts, and denies the notion that this security hack will ever be used again by any authority.

It has been less than a year since the U.S. government's Office of Personnel Management (OPM) was hacked — which does not inspire confidence in the government's ability to keep its citizens' personal data safe. Apple realized long ago that once you create any backdoor, you have foiled the security of the data you are trying to protect, no matter who has charge of the key. It's difficult to educate a scared public on security matters, so Cook took his fight public in an effort to gain supporters in both the government and tech sectors and, so far it seems to be helping.

Can The FBI Guarantee That This Hack Will Not End Up In The Hands Of Another Government Or Terrorist Organization?

Presidential candidates Donald Trump and Marco Rubio are taking shots at Apple for not complying with law enforcement. But as this story falls on an election year, their motives must be challenged. Tech companies Facebook, Google and Twitter have publicly praised Apple for their stance, which is not surprising since the end game of privacy affects all tech companies and their customers. Apple's well respected co-founder Steve Wozniak praised Apple, and tech billionaire, Mark Cuban commended Apple for doing the "exact right thing" and warns, "If you think it's bad that we can't crack the encryption of terrorists, it is far worse when those who would terrorize us can use advanced tools to monitor our unencrypted conversations to plan their acts of terror."

It's clear to experts on both sides that the government is looking to set a legal precedent because they have the facts, and probable cause to force Apple to unlock this phone. What concerns me is politicians mostly fail to see (or at least admit) that once this phone is unlocked, everyone from China to local law enforcement will line-up outside Apple's headquarters demanding that their iPhones be unlocked as evidence for their law enforcement needs as well. This creates an infinitely more dangerous landscape than any terrorist could imagine. China or Russia could spy on all our devices without our government (who also spies on us) knowing it. I am including all devices because there is no reason to doubt that as Apple falls, so will Google, Facebook, Microsoft, and the rest of our tech sector.

New Book For Keeping Small Businesses And Individuals Safe

I authored "Hacked Again" after my company BVS suffered multiple credit and debit card compromises, with $65,000 taken from our checking account, our twitter account was hacked, and our website security was "tested" by unknown hackers. I realized that I was a target of the cyber hackers that I talk about in the media every day. The ordeal was a painful process, but I learned valuable lessons on how to better protect my company and myself personally from cyber hackers. At first I wanted to hide the fact that my own company was hacked. But the more I shared my story, I learned I was not alone. As well as giving tips on how to protect yourself from identity theft, malware and spam, I explain why it's dangerous to put personal information out on social media and the importance of strong passwords.

"Hacked Again"available at www.hackedagain.com
Scott Schober CEO | Author | Speaker | Cyber Security & Wireless Expert at Scott Schober LLC lectures extensively on cybersecurity and corporate espionage around the globe. He recently oversaw the development of cell phone detection tools used to enforce a "no cell phone policy" in correctional, law enforcement, and secured government facilities. Scott regularly appears in national and international publications, and on TV — Fox, ABC, Bloomberg, Good Morning America, CNN, CNBC, CBS, and MSNBC. Scott says, "In a modern digital world, no one is safe from being hacked, not even a renown cyber-security expert."
To reach Scott:
732-548-3737
scott@bvsystems.com
www.bvsystems.com
www.ScottSchober.com