



Tech legend offers to break iPhone encryption within weeks

Rudy Takala

February 18, 2016

A self-proclaimed "cybersecurity legend" is offering to bypass the security on an iPhone for federal authorities within a month for free and says he'll "eat his shoe" if he fails.

"I will, for free, decrypt the information on the San Bernardino phone, with my team. We will primarily use social engineering and it will take us three weeks," John McAfee writes in a Thursday editorial for Business Insider.

"If you doubt my credentials, Google 'Cybersecurity legend' and see whose name is the only name that appears in the first 10 results out of more than a quarter of a million," the tech millionaire adds. McAfee developed the first commercial anti-virus software in 1987.

Using the 227-year-old "All Writs Act" of 1789, a federal judge earlier this week ordered Apple to help the FBI access the contents of an iPhone used by one of the perpetrators of a Dec. 2 terrorist attack in San Bernardino, Calif. Apple has promised to appeal the order, arguing that it would set a dangerous precedent.

"If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data," Apple CEO Tim Cook said Wednesday. "The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge."

Court documents indicate that Apple has assisted authorities with breaking into its devices at least 70 times since the iPhone's June 2007 release. However, the company contends that breaking into its advanced iOS 9 software, which was released in September 2015, would set a different precedent.

That generation of the technology destroys the contents of a device after 10 failed attempts to enter a password. The FBI is requesting that Apple build a special version of its software to

remove that protection from the killer's device. It technically would not remove encryption, but it would allow the FBI to use keep guessing the password until the agency was successful. That is also known as a "brute force" attack.

In the event that software were installed, cybersecurity expert Rob Graham calculates, the FBI would be able to ascertain the password within a day. It would take just over 13 minutes to hack a four-digit password and just over 22 hours to hack one that was six digits.

In this situation, experts suggest the government wants a legal precedent more than it wants technical assistance. "Traditionally, the All Writs Act has been used to force companies to provide information they already have about their own customers, like a phone company ordered to turn over a criminal suspect's billing records," says Julian Sanchez, a technology scholar at the Washington, D.C.-based Cato Institute.

"This situation would establish an entirely new usage and precedent," he adds.

McAfee contends the job isn't that hard, but that the government's experts aren't very good, "because the FBI will not hire anyone with a 24-inch purple mohawk, 10-gauge ear piercings, a tattooed face, who demands to smoke weed while working and won't work for less than a half-million dollars a year."

"Cyberscience is not just something you can learn. It is an innate talent," McAfee writes. "A Mozart or a Bach are genetically created, much like our modern hacking community. A room full of Stanford computer science graduates cannot compete with a true hacker without even a high school education."

"I would eat my shoe on the Neil Cavuto show if we could not break the encryption on the San Bernardino phone. This is a pure and simple fact," he promised.