Common software would have let FBI unlock shooter's iPhone

21 February 2016, by Tami Abdollah And Bree Fowler

An iPhone is seen in Washington, Wednesday, Feb. 17, 2016. The San Bernardino County-owned iPhone at the center of an unfolding high-profile legal battle between Apple Inc. and the U.S. government lacked a device management feature bought by the county that, if installed, would have allowed investigators easy and immediate access. (AP Photo/Carolyn Kaster)

The county government that owned the iPhone in a high-profile legal battle between Apple Inc. and the Justice Department paid for but never installed a feature that would have allowed the FBI to easily and immediately unlock the phone as part of the terrorism investigation into the shootings that killed 14 people in San Bernardino, California.

If the technology, known as mobile device management, had been installed, San Bernardino officials would have been able to remotely unlock the iPhone for the FBI without the theatrics of a court battle that is now pitting digital privacy rights against national security concerns.

The service costs $4 per month per phone.

Instead, the only person who knew the unlocking passcode for the phone is the dead gunman, Syed Farook, who worked as an inspector in the county's public health department.

The iPhone assigned to Farook also lacked a Touch ID feature, meaning the FBI cannot use the dead gunman's thumbprint to unlock it now. The FBI found the phone in a car after the shootings.

A U.S. magistrate last week ordered Apple to provide the FBI with highly specialized software that could be loaded onto the work-issued iPhone 5C used by Farook. He died with his wife in a gun battle with police after killing 14 people in December.

The software would help the FBI hack into the phone by bypassing a security time delay and feature that erases all data after 10 consecutive, unsuccessful attempts to guess the unlocking passcode. This would allow the FBI to use technology to rapidly and repeatedly test numbers in what's known as a brute force attack.

An Apple iPhone 6s Plus smartphone is displayed Friday,

Sept. 25, 2015 at the Apple store at The Grove in Los Angeles. On Wednesday, Feb. 17, 2016, a federal judge ordered Apple Inc. to help the FBI hack into an encrypted iPhone used by Syed Farook, who along with his wife, Tashfeen Malik, killed 14 people in December in the worst terror attack on U.S. soil since Sept. 11, 2001. Apple has helped the government before in this and previous cases, but this time Apple CEO Tim Cook said no and Apple is appealing the order. (AP Photo/Ringo H.W. Chiu)

The FBI said it wants to determine whether Farook had used his phone to communicate with others about the attack.

Apple has said it will protest the ruling and has until Friday to intervene in court.

San Bernardino had an existing contract with a technology provider, MobileIron Inc., but did not install it on any inspectors' iPhones, county spokesman David Wert said. There is no countywide policy on the matter and departments make their own decisions, he said.

Wert disputed the value of the remote management technology because he said Farook—or any other county employee—could have removed it manually. That would have alerted county technology employees and led them to intervene.

In many offices and classrooms, officially issued smartphones include the installed management software. It can unlock the phone, delete all information in case of loss or theft, track the device's physical location, determine which apps are installed, check battery life and push software updates. The technology is intended to make such products more suitable in corporate environments, where tighter controls are important to protect company secrets.

"This is the business case" for mobile device management, said John Dickson, a principal at Denim Group Ltd., a security consultancy. "The organization simply has no control or influence or anything over the device unless they have some MDM authority. The ability to do remote air updates, the ability to do remote wipe, the ability to control certain settings. Those are the standard kinds of things you do in mobile device management."

Dickson said "the big question now going forward, it builds the case for, is why this guy would have an essentially uncontrolled device."

This is the first time since the county issued its first Blackberry device in 2003 that law enforcement has needed access to a locked county-owned phone, Wert said. Prosecutors said in court filings that the county gave its consent to search the device. County policy said digital devices can be searched at any time and Farook signed such an agreement.

Apple executives said Friday that the company had worked hard to help federal investigators get information off the locked iPhone, suggesting they use an iCloud workaround while the phone was connected to a familiar wireless network so that it would begin automatically backing up and provide access to data. The executives spoke on condition of anonymity because of the ongoing legal process.

The executives said Apple sent engineers to work with the FBI on the workaround but the effort ultimately failed. In the government's filing Friday, prosecutors said in a footnote that neither the county nor the FBI knew the password to the iCloud account and the county, in an effort to get access to information on the phone in the hours after the attack, reset the password remotely—thereby eliminating the possibility of that workaround being successful.

But if the county had installed the management device it had bought onto Farook's phone, none of these efforts would have been necessary.

Gartner Inc., a technology research firm, estimated that over 60 percent of large enterprises—meaning business, government and educational entities—used some kind of MDM software as of last year, though not necessarily on all company-owned devices. That percentage is likely higher now than when the research was done months ago, said Terrence Cosgrove, a research director with Gartner's mobile and client computing research group. Cosgrove said MDM adoption rates are

generally higher among government users.

Many workers balk at the idea that the software can monitor and track their personal phones, said Alex Heid, chief research officer at the cybersecurity firm SecurityScorecard Inc. But if the company provides a phone, it's considered reasonable practice to use such software.

"If a company's assumption is that they might not be able to get back into a device one day then it's not really a company asset at that point, it's a gift," he said.

APA citation: Common software would have let FBI unlock shooter's iPhone (2016, February 21) retrieved 27 November 2022 from https://phys.org/news/2016-02-common-software-fbi-shooter-iphone.html