Here we go again: Paris attacks may renew encryption debate

November 16 2015, byBree Fowler And Michael Liedtke

In this June 2, 2014, file photo, Apple CEO Tim Cook speaks at an event in San Francisco. The deadly attacks in Paris may soon reopen the debate over whether and how tech companies should let the government sidestep the data scrambling that shields everyday commerce and daily digital life alike. The Obama administration continues to encourage tech companies to include backdoors, although it says it will not ask Congress for new law that requires them. Cook has said that the trouble with that approach is that "there's no such thing as a backdoor for the good guys only." (AP Photo/Jeff Chiu, File)

The deadly attacks in Paris may soon reopen the debate over whether—and how—tech companies should let governments bypass the data scrambling that shields everyday commerce and daily digital life.

So far, there's no hard evidence that the Paris extremists relied on encrypted communications—essentially, encoded digital messages that can't be read without the proper digital "keys"—to plan the shooting and bombing attacks that left 129 dead on Friday. But it wouldn't be much of a surprise if they did.

So-called end-to-end encryption technology is now widely used in many standard message systems, including Apple's iMessage and Facebook's WhatsApp. Similar technology also shields the contents of smartphones running the latest versions of Apple and Google operating software. Strong encryption is used to protect everything from corporate secrets to the credit-card numbers of online shoppers to intimate photos and secrets shared by lovers.

That widespread use of encryption, which was previously restricted to more powerful desktop or server computers, is exactly what worries members of the intelligence and law enforcement communities. Some are now using the occasion of the Paris attacks to once again argue for restrictions on the technology, saying it hampers their ability to track and disrupt plots like the Paris attacks.

"I now think we're going to have another public debate about encryption, and whether government should have the keys, and I think the result may be different this time as a result of what's happened in Paris," former CIA deputy director Michael Morell said Monday on CBS This Morning.

The last such debate followed 2013 disclosures of government surveillance by former National Security Agency contractor Edward

Snowden. Since then, tech companies seeking to reassure their users and protect their profits have adopted more sophisticated encryption techniques despite government opposition. Documents leaked by Snowden also shed light on NSA efforts to break encryption technologies.

In response, law-enforcement and intelligence officials have argued that companies like Apple and Google should build "backdoors" into their encryption systems that would allow investigators into otherwise locked-up devices. The Obama administration continues to encourage tech companies to include such backdoors, although it says it won't ask Congress for new law that requires them.

"The Snowden revelation showed that backdoors can be destructive, particularly when they're done in secrecy without transparency," says Will Ackerly, a former NSA security researcher and the co-founder of Virtru, which provides encryption technology for both companies and individual people.

On Monday, Attorney General Loretta Lynch said the government continues to have "ongoing discussions" with industry about ways in which companies can lawfully provide information about their users while still ensuring their privacy.

Last week in Dublin, Apple CEO Tim Cook noted that "there's no such thing as a backdoor for the good guys only. If there's a backdoor, anybody can come in." In other words, any shortcut for investigators could also be targeted by cybercriminals eager to hack major corporations—a la the devastating cyberattack on Sony late last year—or to target individuals for identity theft or extortion, as reportedly occurred following the disclosure of records from the infidelity dating site Ashley Madison.

In the same speech, Cook said Apple will resist attempts to weaken encryption in iMessage. A draft law recently introduced in Britain would require telecommunications companies to provide "wider assistance" to police and intelligence agencies in the interests of national security.

Like iMessage, Facebook's WhatsApp encrypts all communications from "end-to-end"—a technique that blocks anyone outside the conversation from reading or seeing what's being sent. Although Facebook can't see the content of the messages, it does track who is talking to whom and stores their phone numbers—information that can be valuable for law enforcement officials trying to sniff out terrorist plots and fight other criminal activity.

Steven Bellovin, a Columbia University professor and computer security researcher, says he isn't surprised by the effort to bring back discussion on encryption backdoors. But he adds that it's way too early to tie it to the Paris attacks.

"We don't know how these people were communicating and with whom," he said. "If they were communicating with homegrown software and there's some indications of that, then a mandatory backdoor is not going to do any good."

Citation: Here we go again: Paris attacks may renew encryption debate (2015, November 16) retrieved 11 May 2024 from https://phys.org/news/2015-11-paris-renew-encryption-debate.html