Why a future Apple-FBI case may go very differently

March 23 2016, by Brandon Bailey

In this Dec. 23, 2013, file photo, a woman using a phone walks past Apple's logo near its retail outlet in Beijing. Even while it fiercely opposes the FBI's demand for help unlocking an encrypted iPhone used in the San Bernardino mass shootings, Apple has never argued that it isn't capable of doing what the government wants. While the FBI may have found an alternative solution in the San Bernardino case, experts say it's almost certain that Apple and other tech companies will keep increasing the security of their products, making it harder or perhaps even impossible for them to answer government demands for customers' data. (AP Photo/Ng Han Guan, File)

Although it fiercely opposes the FBI's demand for help unlocking a San Bernardino shooter's encrypted iPhone, Apple has never argued that it simply can't do what the government wants. That might not be true for long.

At the moment, the San Bernardino case is on hold while the FBI evaluates an alternative method of getting into that phone. But experts say it's almost certain that Apple and other tech companies will keep increasing the security of their products, making it harder or perhaps even impossible for them to answer government demands for customer data.

"If I were them, I would use any means possible to avoid having to answer these information requests," said Anna Lysyanskaya, a computer scientist and cryptography expert at Brown University. "It's bad for their business, and not just in the United States but in other countries where law enforcement cannot be trusted to follow the law."

Smartphones and Internet services increasingly store a vast trove of personal information—everything from messages and photos to banking details to records of your movements. Apple won't comment on specific future plans, although it says it's constantly increasing security to protect that data from hackers and criminals. That's why, for example, its latest mobile operating system won't let anyone read files on an encrypted iPhone without knowing the user's passcode.

Its intent, Apple says, isn't to foil legitimate government investigations, but to protect its users against criminal hacking. In the San Bernardino case, the FBI wanted Apple to create a software tool that would override a "self-destruct" security feature that would activate after too many incorrect passcode attempts. Apple argued that creating such a tool would make all iPhones more vulnerable.

The magistrate judge in the San Bernardino case canceled a hearing on the dispute this week after the government said an unnamed "third party" had come forward with a possible alternative to Apple's assistance. That method, which the government hasn't described, is under testing.

Apple, however, could design future iPhone hardware and software security that would be much more difficult to circumvent. It could also lock up its iCloud backup service so that only its users would hold the keys necessary to unscramble data they store online. Apple currently retains iCloud keys so it can provide access for customers who lose their passwords. That means Apple can—as it did in the San Bernardino case—provide unscrambled iCloud files to authorities with a valid search warrant

Some commercial data-storage firms already promote services that let business customers hold the keys to their own encrypted data.

"It's the new reality," said Yorgen Edholm, CEO of Palo Alto-based file-sharing company Accellion. If a service doesn't offer that feature, he said, "they are scrambling to add that in." The first requests for his firm's encrypted service came from overseas businesses that worried about losing control of their data, he said, but demand has also been growing in the United States.

And when the police come knocking, Edholm added, "we tell them, 'We'd like to help,' but because the customer controls the decryption key, they have to go to the customer directly."

Such security comes with trade-offs, and they could be serious for consumers. Many iPhone owners, for instance, don't even bother to set a passcode on their phone. And the convenience of getting Apple's help if you lose your phone or password could be hard to give up, particularly when weighed against an abstract value like privacy.

Tech companies have reported a steady increase in government requests for customer information around the world. It can be invaluable for prosecuting known suspects and for uncovering new plots and perpetrators, said Ed McAndrew, a former federal cybercrimes prosecutor now in private practice.

Of course, those information requests complicate life for tech companies, he acknowledged. "Some companies are saying, 'We can get out of this game, because we can make it so that, technologically, we're not in a position to provide access to customer data,'" he said.

Apple and other leading tech firms say they routinely answer thousands of legal data requests every year. Microsoft president Brad Smith noted in a recent speech that his company supplied customer information to authorities investigating an extremist attack in Paris while the suspects were still at large.

Justice Department officials are alarmed by any possibility that those digital information troves might move farther out of reach. But many in the industry say that's where things seem to be heading. "You could see a world where the companies don't hold the keys," said Denelle Dixon-Thayer, chief legal and business officer at Mozilla, which makes the Firefox web browser.

"No one wants to be obstructionist," said Ted Schlein, a venture capitalist with Kleiner Perkins who invests in computer security firms. Tech companies, he said, "want to help, but that's not their mission. They're responsible to their shareholders and the users of their products."

Citation: Why a future Apple-FBI case may go very differently (2016, March 23) retrieved 25