FBI-Apple standoff puts encryption on front burner (Update)

February 17 2016

Apple's challenge of a court order to unlock an iPhone used by one of the San Bernardino killers opens up a new front in the long-running battle between technology companies and the government over encryption

Apple's challenge of a court order to unlock an iPhone used by one of the San Bernardino killers opens up a new front in the long-running battle between technology companies and the government over encryption.

The standoff brings the sensitive issue, which has been at a stalemate in Congress, into the courts, and has abruptly shifted the policy debate on encryption.

A California magistrate on Tuesday ordered Apple to provide "reasonable technical assistance" to the US Federal Bureau of Investigation to break into an iPhone used by one of the shooters in the deadly December rampage that killed 14 people and has been linked to supporters of the Islamic State organization.

Apple quickly said it would fight the judge's order. Chief executive Tim Cook called it "an unprecedented step which threatens the security of our customers," and said the order "has implications far beyond the legal case at hand."

Apple, Google and other technology firms in recent years have stepped up encryption—allowing only the customers to have "keys" to unlock their devices—claiming improved security and privacy is needed to maintain confidence in the digital world.

That drive for privacy has prompted sharp objections from law enforcement and intelligence officials, who claim that criminals and extremists are able to hide their illicit activities thanks to device encryption.

A customer uses her new smartphone after the release of the iPhone 6s at an Apple store in Shanghai on September 25, 2015

"This is a clever move by the FBI to move from the legislative arena, where they were not winning, to the courts," said Joseph Hall, chief technologist at the Center for Democracy & Technology, a digital rights group.

Raising privacy hackles

The order raised hackles among privacy advocates, which see the potential to unleash unbridled surveillance in the United States and elsewhere.

"If the FBI can force Apple to hack into its customers' devices, then so too can every repressive regime in the rest of the world," said Alex Abdo of the American Civil Liberties Union.

But Apple also came under attack for thwarting a critical security investigation.

"Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people," said Senator Tom Cotton of Arkansas, using an acronym for the Islamic State group.

"Regrettably, the position Tim Cook and Apple have taken shows that they are unwilling to compromise and that legislation is likely the only way to resolve this issue."

New York City police commissioner William Bratton welcomed the order and added, "We cannot give those seeking to harm us additional tools to keep their activity secret. I reiterate my call on Congress to act immediately in passing legislation to provide law enforcement the tools we need to keep America safe."

White House spokesman John Earnest said the White House supports the request by the FBI and Department of Justice.

"They are not asking Apple to redesign its product or to create a new backdoor to one of their products," Earnest told reporters.

"They're simply asking for something that would have an impact on this one device."

Debate on 1789 law

The case is likely to work its way through the courts, which will need to

consider a number of both technical and legal questions.

Interestingly, Magistrate Judge Sheri Pym's order is based on the 1789 All Writs Act, which lays out broad authority for the courts to help enforcement of the law.

Steve Vladeck, an American University law professor and co-editor of the Just Security blog, said the order stretches the interpretation of the centuries-old law.

"If the government can compel Apple to develop software (to get around encryption) what can't it do," Vladeck told AFP.

"There is no history of court orders compelling companies to do research and design."

Legal scholar Jonathan Turley of the George Washington University said in a blog post that Pym "seems to believe that she can order companies to become unwilling participants in surveillance research and development."

"I fail to see her legal basis for such an extraordinary order against a private company," Turley wrote.

Berin Szoka, president of the libertarian think tank TechFreedom, said the order goes against "bedrock principles of law and privacy."

"If forcing Apple to hack its own devices qualifies as 'reasonable technical assistance,' there is no practical limit to what law enforcement could force private companies to do to compromise the security of their systems," Szoka said in a statement.

Darren Hayes, a Pace University professor of computer forensics,

argued that Apple and other tech companies may have gone too far by using encryption that, in theory, makes it impossible for the firms to hand over evidence even if served with a legal warrant.

"I think that the public, once they become more educated about what is happening, might change their stance about Apple," said Hayes, who has worked as a consultant to law enforcement.

"This case is sensitive for the US public and I don't think it's particularly good public relations for Apple" to refuse to help the investigation, Hayes added.

One key question is whether Apple has the ability to provide the assistance sought by the FBI.

"Apple does not have the keys to your device—they are burned onto your chip," Hall said.

But he said it may be possible to get around that encryption with software modifications.

"Apple has never been forthcoming about the deep details of its system," Hall said.

Hayes said that no one knows for sure if Apple can circumvent the encryption, but noted "the fact that they're arguing this makes me think they may be able to do it."