Apple-FBI case has wide implications

February 28, 2016

Apple and the US government are squaring off in an epic legal battle with wide-ranging implications for how technology firms must work with law enforcement.

The iPhone maker is being asked to provide "reasonable assistance" to the investigation of the last year's deadly San Bernardino attacks by disabling security preventing the FBI from accessing the encrypted handset of one of the shooters.

The highly charged case has created a sharp divide among those who say that users of devices like smartphones should be able to keep information private through encryption, and others who claim legitimate law enforcement investigations should take precedence when courts approve.

Apple is challenging the California court order, saying the type of cooperation sought would undermine basic principles of data security and open new vulnerabilities for all its users.

The government is asking for the creation of software that doesn't exist, an abuse of the law and violation of the company's constitutional rights, Apple says.

It adds that creating a weaker "government OS" would undermine the encryption Apple and others have been introducing, and ultimately leak out to hackers and foreign governments.

"Apple wants to maintain the trust relationship with its customers, they feel deeply and firmly this is something that has to exist, and that no government should have access to this data," said John Dickson of the Texas-based Denim Group, which manages security and encryption for its customers.

"I anticipate there will be a technical response form Apple, so that it will be nearly impossible for them to be compelled to do anything."

Julian Sanchez of the libertarian Cato Institute says in a blog post the case is "a fight over the future of high-tech surveillance, the trust infrastructure undergirding the global software

ecosystem, and how far technology companies and software developers can be conscripted as unwilling suppliers of hacking tools for governments."

Life, death and encryption

Some say Apple's position is based on a core principle about security of its users' data.

"Lack of privacy can be a matter of life and death or imprisonment," said Jon Hanour, chief executive of California startup USMobile, which makes an application for encrypted mobile messaging.

"Apostasy results in a death in Saudi Arabia. Homosexual acts send people to prison in Pakistan. And in many countries, adultery is punishable by lashing and stoning."

But critics say Apple is simply providing an easy way for criminals and others to operate in the shadows.

Allowing Apple to refuse would "thwart the public interest in a full and complete investigation of a horrific act of terrorism," the Justice Department argued in its court motion.

New York County District Attorney Cy Vance, who has complained that encrypted phones have frustrated many investigations, said Apple and other makers of encryption should not be able to help skirt law enforcement.

"Apple and Google have created the first warrant-proof consumer products in American history, and the result is that crimes are going unsolved and victims are being left beyond the protection of the law," he said in a statement.

Apple argues that being forced to comply would set a dangerous precedent allowing broad access to law enforcement.

"Once the floodgates open, they cannot be closed, and the device security that Apple has worked so tirelessly to achieve will be unwound," Apple argued.

But James Lewis, a former US official who is now a senior fellow at the Center for Strategic and International Studies, said there is nothing unusual about the case.

"The court decided this was a reasonable request," Lewis told *AFP*.

"The privacy people say it will set a precedent and it will be the end of life on this planet, and it's not true."

Computer forensics researcher Jonathan Zdziarski said complying would be more complex than it appears.

In a blog post, he notes that Apple would need to develop a tool to produce "reproducible, predictable results," which "must be forensically sound and not change anything on the target."

Additionally, he said that Apple "must be prepared to defend their tool and methodology in court ... What FBI has requested will inevitably force Apple's methods out into the open."

The China question

Apple backers say weakening encryption will work against American interests by compromising security for users living under repressive regimes.

"Authoritarian regimes around the world are salivating at the prospect of the FBI winning this order," Nate Cardozo of the Electronic Frontier Foundation told *PBS*.

"If Apple creates the master key that the FBI has demanded that they created, governments around the world are going to be demanding the same access."

But Apple's critics say the company may already assist the Chinese government with modifications of the iPhone for that market and cloud computing center hosted in China.

Stewart Baker, a former Homeland Security official who is now in law practice in Washington, said Apple's lack of transparency in China raises questions.

"Maybe you can explain why a secret encryption system that everyone suspects of having a real back door is good enough for Apple's customers in China?" Baker says in a blog post.

Snowden impact

Some analysts say the conflict stems from revelations about widespread government surveillance by former intelligence contractor Edward Snowden.

"The Snowden disclosures revealed that many government agencies conduct extensive surveillance on citizens, which arguably not only undermine our privacy but compromise our entire information security infrastructure," says Rahul Telang, professor of information systems at Carnegie Mellon University.

Telang said it is a difficult issue to resolve but that he sees the privacy argument as likely to win.

"Now that we know about government snooping, there is a trust issue," he said. "Once we give you backdoor access, where will it stop?"