The New York Times | http://nyti.ms/1Ltdr0U

TECHNOLOGY

Apple Fights Order to Unlock San Bernardino Gunman's iPhone

By KATIE BENNER and ERIC LICHTBLAU FEB. 17, 2016

SAN FRANCISCO — Apple said on Wednesday that it would oppose and challenge a federal court order to help the F.B.I. unlock an iPhone used by one of the two attackers who killed 14 people in San Bernardino, Calif., in December.

On Tuesday, in a significant victory for the government, Magistrate Judge Sheri Pym of the Federal District Court for the District of Central California ordered Apple to bypass security functions on an iPhone 5c used by Syed Rizwan Farook, who was killed by the police along with his wife, Tashfeen Malik, after they attacked Mr. Farook's co-workers at a holiday gathering.

Judge Pym ordered Apple to build special software that would essentially act as a skeleton key capable of unlocking the phone.

But hours later, in a statement by its chief executive, Timothy D. Cook, Apple announced its refusal to comply. The move sets up a legal showdown between the company, which says it is eager to protect the privacy of its customers, and the law enforcement authorities, who say that new encryption technologies hamper their ability to prevent and solve crime.

In his statement, Mr. Cook called the court order an "unprecedented step" by the federal government. "We oppose this order, which has implications far beyond the legal case at hand," he wrote.

Asked about Apple's resistance, the Justice Department pointed to a statement by Eileen M. Decker, the United States attorney for the Central District of California: "We have made a solemn commitment to the victims and their families that we will leave no stone unturned as we gather as much information and evidence as possible. These victims and families deserve nothing less."

The F.B.I. said that its experts had been unable to access data on Mr. Farook's iPhone, and that only Apple could bypass its security features. F.B.I. experts have said they risk losing the data permanently after 10 failed attempts to enter the password because of the phone's security features.

The Justice Department had secured a search warrant for the phone, owned by Mr. Farook's former employer, the San Bernardino County Department of Public Health, which consented to the search.

Because Apple declined to voluntarily provide, in essence, the "keys" to its encryption technology, federal prosecutors said they saw little choice but to get a judge to compel Apple's assistance.

Mr. Cook said the order would amount to creating a "back door" to bypass Apple's strong encryption standards — "something we simply do not have, and something we consider too dangerous to create."

In 2014, Apple and Google — whose operating systems are used in 96 percent of smartphones worldwide — announced that they had re-engineered their software with "full disk" encryption, and could no longer unlock their own products as a result.

That set up a confrontation with police and prosecutors, who want the companies to build, in essence, a master key that can be used to get around the encryption. The technology companies say that creating such a key would have disastrous consequences for privacy.

"The F.B.I. may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a back door," Mr. Cook wrote. "And while the

government may argue that its use would be limited to this case, there is no way to guarantee such control."

An Apple spokeswoman declined to elaborate on the statement, but the company's most likely next step is to file an appeal.

The legal issues are complicated. They involve statutory interpretation, rather than constitutional rights, and they could end up before the Supreme Court.

As Apple noted, the F.B.I., instead of asking Congress to pass legislation resolving the encryption fight, has proposed what appears to be a novel reading of the All Writs Act of 1789.

The law lets judges "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."

The government says the law gives broad latitude to judges to require "third parties" to execute court orders. It has cited, among other cases, a 1977 ruling requiring phone companies to help set up a pen register, a device that records all numbers called from a particular phone line.

Apple, in turn, argues that the scope of the act has strict limits. In 2005, a federal magistrate judge rejected the argument that the law could be used to compel a telecommunications provider to allow real-time tracking of a cellphone without a search warrant.

Marc J. Zwillinger, a lawyer for Apple, wrote in a letter for a related case in October that the All Writs Act could not be interpreted to "force a company to take possession of a device outside of its possession or control and perform services on that device, particularly where the company does not perform such services as part of its business and there may be alternative means of obtaining the requested information available to the government."

The government says it does not have those alternative means.

Mr. Cook's statement called the government's demands "chilling."

He added: "If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge."

The Electronic Frontier Foundation, a nonprofit organization that defends digital rights, said it was siding with Apple.

"The government is asking Apple to create a master key so that it can open a single phone," it said Tuesday evening. "And once that master key is created, we're certain that our government will ask for it again and again, for other phones, and turn this power against any software or device that has the audacity to offer strong security."

The San Bernardino case is the most prominent such case, but it is not the first.

Last October, James Orenstein, a federal magistrate judge in Brooklyn, expressed doubts about whether he could require Apple to disable its latest iPhone security features, citing the failure of Congress to resolve the issue despite the urging of the Justice Department.

The judge said such requests should fall under a different law, the Communications Assistance for Law Enforcement Act of 1994, which covers telecommunications and broadband companies.

Congress has been debating whether to amend that act to include technology companies like Apple, Facebook and Google, and Judge Orenstein said he would consider ordering Apple to unlock the phone when and if Congress makes the change. That case is still pending.

Although Apple is portraying its opposition to Judge Pym's order as a

principled defense of privacy, one of its motivations is the preservation of its reputation for robust encryption, at a time of rising concerns about identity theft, cybercrime and electronic surveillance by intelligence agencies and overzealous law enforcement agencies.

Apple also says that a master key would amount to a vulnerability that hackers could exploit.

China is watching the dispute closely. Analysts say that the Chinese government does take cues from the United States when it comes to encryption regulations, and that it would most likely demand that multinational companies provide accommodations similar to those in the United States.

Last year, Beijing backed off several proposals that would have mandated that foreign firms provide encryption keys for devices sold in China after heavy pressure from foreign trade groups. Nonetheless, a Chinese antiterrorism law passed in December required foreign firms to hand over technical information and to aid with decryption when the police demand it in terrorism-related cases.

While it is still not clear how the law might be carried out, it is possible a push from American law enforcement agencies to unlock iPhones would embolden Beijing to demand the same. China would also most likely push to acquire any technology that would allow it to unlock iPhones. Just after Apple introduced tougher encryption standards in 2014, Apple users in China were targeted by an attack that sought to obtain login information from iCloud users.

Katie Benner reported from San Francisco, and Eric Lichtblau from Washington. Sewell Chan contributed reporting from London, and Paul Mozur from Hong Kong.
