Apple Fights Order to Unlock San

Bernardino Gunman’s iPhone

By ERIC LICHTBLAU and KATIE BENNER FEB. 17, 2016

WASHINGTON — Last month, some of President Obama’s top intelligence

advisers met in Silicon Valley with Apple’s chief, Timothy D. Cook, and other

technology leaders in what seemed to be a public rapprochement in their longrunning dispute over the encryption safeguards built into their devices.

But behind the scenes, relations were tense, as lawyers for the Obama

administration and Apple held closely guarded discussions for over two months

about one particularly urgent case: The F.B.I. wanted Apple to help “unlock” an

iPhone used by one of the two attackers who killed 14 people in San Bernardino,

Calif., in December, but Apple was resisting.

When the talks collapsed, a federal magistrate judge, at the Justice

Department’s request, ordered Apple to bypass security functions on the phone.

The order set off a furious public battle on Wednesday between the Obama

administration and one of the world’s most valuable companies in a dispute with

far-reaching legal implications.

“This Apple case really goes right to the heart of the encryption issue,” said Ira

Rubinstein, a senior fellow at the New York University Information Law Institute,

“and in some ways, this was a fight that was inevitable.”

This is not the first time a technology company has been ordered to effectively

Apple Fights Order to Unlock San Bernardino Gunman’s iPhone - The New York Times 5/1/16, 12:31 PM

http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-…-san-bernardino.html?smprod=nytcore-ipad&smid=nytcore-ipad-share Page 2 of 6

decrypt its own product. But industry experts say it is the most significant because

of Apple’s global profile, the invasive steps it says are being demanded and the

brutality of the San Bernardino attacks.

Law enforcement officials who support the F.B.I.’s position said that the

impasse with Apple provided an ideal test case to move from an abstract debate

over the balance between national security and privacy to a concrete one.

The F.B.I. has been unable to get into the phone used by Syed Rizwan Farook,

who was killed by the police along with his wife after they attacked Mr. Farook’s coworkers at a holiday gathering. Reynaldo Tariche, an F.B.I. agent on Long Island,

said, “The worst-case scenario has come true.”

Mr. Tariche, who is president of the agents’ association, added, “As more of these

devices come to market, this touches all aspects of the cases that we’re working

on.”

Magistrate Judge Sheri Pym of the Federal District Court for the District of

Central California issued her order Tuesday afternoon, after the F.B.I. said it had

been unable to get access to the data on its own and needed Apple’s technical

assistance.

Mr. Cook, the chief executive at Apple, responded Wednesday morning with a

blistering, 1,100-word letter to Apple customers, warning of the “chilling” breach of

privacy posed by the government’s demands. He maintained that the order would

effectively require it to create a “backdoor” to get around its own safeguards, and

Apple vowed to appeal the ruling by next week.

“The same engineers who built strong encryption into the iPhone to protect

our users would, ironically, be ordered to weaken those protections and make our

users less safe,” Mr. Cook said.

Apple argues that the software the F.B.I. wants it to create does not exist. But

technologists say the company can do it.

Apple Fights Order to Unlock San Bernardino Gunman’s iPhone - The New York Times 5/1/16, 12:31 PM

http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-…-san-bernardino.html?smprod=nytcore-ipad&smid=nytcore-ipad-share Page 3 of 6

Mr. Cook’s angry tone reflected the tense discussions, conducted mostly on the

telephone, between his company and the government’s lawyers over the San

Bernardino case. Apple executives had hoped to resolve the impasse without

having to rewrite their own encryption software. They were frustrated that the

Justice Department had aired its demand in public, according to an industry

executive with knowledge of the case, who spoke on the condition of anonymity

about internal discussions.

The Justice Department and the F.B.I. have the White House’s “full support,”

the spokesman, Josh Earnest, said on Wednesday.

His vote of confidence was significant because James Comey, the F.B.I.

director, has at times been at odds with the White House over his aggressive

advocacy of tougher decryption requirements on technology companies. While Mr.

Obama’s national security team was sympathetic to Mr. Comey’s position, others at

the White House viewed legislation as potentially perilous. Late last year, Mr.

Obama refused to back any legislation requiring decryption, leaving a court fight

likely.

The Justice Department showed no sign of backing down Wednesday.

“It is unfortunate,” the department said in a statement, “that Apple continues

to refuse to assist the department in obtaining access to the phone of one of the

terrorists involved in a major terror attack on U.S. soil.”

The dispute could initiate legislation in Congress, with Republicans and

Democrats alike criticizing Apple’s stance on Wednesday and calling for tougher

decryption requirements. Donald J. Trump, the Republican presidential contender,

also attacked Apple on Fox News, asking, “Who do they think they are?”

But Apple had many defenders of its own among privacy and consumer

advocates, who praised Mr. Cook for standing up to what they saw as government

overreach.

Many of the company’s defenders argued that the types of government

Apple Fights Order to Unlock San Bernardino Gunman’s iPhone - The New York Times 5/1/16, 12:31 PM

http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-…-san-bernardino.html?smprod=nytcore-ipad&smid=nytcore-ipad-share Page 4 of 6

surveillance operations exposed in 2013 by Edward J. Snowden, the former

National Security Agency contractor, have prompted technology companies to

build tougher encryption safeguards in their products because of the privacy

demands of their customers.

“Apple deserves praise for standing up for its right to offer secure devices to all

of its customers,” said Alex Abdo, staff lawyer for the American Civil Liberty

Union’s privacy and technology section.

Privacy advocates and others said they worried that if the F.B.I. succeeded in

getting access to the software overriding Apple’s encryption, it would create easy

access for the government in many future investigations.

“This is not the last step in the journey,” said Robert Cattanach, a former

Justice Department lawyer who works on privacy and tech security issues at the

law firm Dorsey & Whitney. “The next thing you know, they’ll be in the back door

of these systems.”

The Apple order is a flash point in a dispute that has been building for more

than a decade.

The F.B.I. began sounding alarms years ago about technology that allowed

people to exchange private messages protected by encryption so strong that

government agents could not break it. In fall 2010, at the behest of Robert S.

Mueller III, the F.B.I. director, the Obama administration began work on a law that

required technology companies to provide unencrypted data to the government.

Lawyers at the F.B.I., Justice Department and Commerce Department drafted

bills around the idea that technology companies in the Internet age should be

bound by the same rules as phone companies, which were forced during the

Clinton administration to build digital networks that government agents could tap.

The draft legislation would have covered app developers like WhatsApp and

large companies like Google and Apple, according to current and former officials

involved in the process.

Apple Fights Order to Unlock San Bernardino Gunman’s iPhone - The New York Times 5/1/16, 12:31 PM

http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-…-san-bernardino.html?smprod=nytcore-ipad&smid=nytcore-ipad-share Page 5 of 6

There is no debate that, when armed with a court order, the government can

get text messages and other data stored in plain text. Far less certain was whether

the government could use a court order to force a company to write software or

redesign its system to decode encrypted data. A federal law would make that

authority clear, they said.

But the disclosures of government surveillance by Mr. Snowden changed the

privacy debate, and the Obama administration decided not to move on the

proposed legislation. It has not been revived.

The legal issues raised by the judge’s order 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 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 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.

Eric Lichtblau reported from Washington, and Katie Benner from San

Francisco. Matt Apuzzo contributed reporting from Washington, Sewell Chan

from London, and Paul Mozur from Hong Kong.