Statement for the Record

"The Encryption Tightrope: Balancing Americans' Security and Privacy"

United States House of Representatives

Committee on the Judiciary

Bruce Sewell

Senior Vice President and General Counsel

Apple

March 1, 2016

Thank you, Mr. Chairman. It's my pleasure to appear before you and the Committee today on behalf of Apple. We appreciate your invitation and the opportunity to be part of the discussion on this important issue which centers on the civil liberties at the foundation of our country.

I want to repeat something we have said since the beginning — that the victims and families of the San Bernardino attacks have our deepest sympathies and we strongly agree that justice should be served. Apple has no sympathy for terrorists.

We have the utmost respect for law enforcement and share their goal of creating a safer world. We have a team of dedicated professionals that are on call 24 hours a day, seven days a week, 365 days a year to assist law enforcement. When the FBI came to us in the immediate aftermath of the San Bernardino attacks, we gave all the information we had related to their investigation. And we went beyond that by making Apple engineers available to advise them on a number of additional investigative options.

But we now find ourselves at the center of an extraordinary circumstance. The FBI has asked a Court to order us to give them something we don't have. To create an operating system that does not exist — because it would be too dangerous. They are asking for a backdoor into the iPhone — specifically to build a software tool that can break the encryption system which protects personal information on every iPhone.

As we have told them — and as we have told the American public — building that software tool would not affect just one iPhone. It would weaken the security for all of them. In fact, just last week Director Comey agreed that the FBI would likely use this precedent in other cases involving other phones. District Attorney Vance has also said he

would absolutely plan to use this on over 175 phones. We can all agree this is not about access to just one iPhone.

The FBI is asking Apple to weaken the security of our products. Hackers and cyber criminals could use this to wreak havoc on our privacy and personal safety. It would set a dangerous precedent for government intrusion on the privacy and safety of its citizens.

Hundreds of millions of law-abiding people trust Apple's products with the most intimate details of their daily lives – photos, private conversations, health data, financial accounts, and information about the user's location as well as the location of their friends and families. Some of you might have an iPhone in your pocket right now, and if you think about it, there's probably more information stored on that iPhone than a thief could steal by breaking into your house. The only way we know to protect that data is through strong encryption.

Every day, over a trillion transactions occur safely over the Internet as a result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better, and communications between loved ones. The US government has spent tens of millions of dollars through the Open Technology Fund and other US government programs to fund strong encryption. The Review Group on Intelligence and Communications Technology, convened by President Obama, urged the US government to fully support and not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software.

Encryption is a good thing, a necessary thing. We have been using it in our products for over a decade. As attacks on our customers' data become increasingly sophisticated, the tools we use to defend against them must get stronger too. Weakening encryption will only hurt consumers and other well-meaning users who rely on companies like Apple to protect their personal information.

Today's hearing is titled Balancing Americans' Security and Privacy. We believe we can, and we must, have both. Protecting our data with encryption and other methods preserves our privacy and it keeps people safe.

The American people deserve an honest conversation around the important questions stemming from the FBI's current demand:

Do we want to put a limit on the technology that protects our data, and therefore our privacy and our safety, in the face of increasingly sophisticated cyber attacks? Should the FBI be allowed to stop Apple, or any company, from offering the American people the safest and most secure product it can make?

Should the FBI have the right to compel a company to produce a product it doesn't already make, to the FBI's exact specifications and for the FBI's use?

We believe that each of these questions deserves a healthy discussion, and any decision should be made after a thoughtful and honest consideration of the facts.

Most importantly, the decisions should be made by you and your colleagues as representatives of the people, rather than through a warrant request based on a 220 year-old-statute.

At Apple, we are ready to have this conversation. The feedback and support we're hearing indicate to us that the American people are ready, too.

We feel strongly that our customers, their families, their friends and their neighbors will be better protected from thieves and terrorists if we can offer the very best protections for their data. And at the same time, the freedoms and liberties we all cherish will be more secure.

Thank you for your time. I look forward to answering your questions.