Statement for the Record

"Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives"

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

Bruce Sewell

Senior Vice President and General Counsel

Apple Inc.

April 19, 2016

Thank you, Chairman Murphy, Ranking Member DeGette and members of the Subcommittee. It's my pleasure to appear before you today on behalf of Apple. We appreciate your invitation and the opportunity to be part of this important discussion about encryption.

Hundreds of millions of people trust Apple's products with the most intimate details of their daily lives. Some of you might have a smartphone in your pocket right now, and if you think about it, there's probably more information stored on that phone than a thief could steal by breaking into your house.

And it's not just a phone. It's a photo album. It's a wallet. It's how you communicate with your doctor, your partner, and your kids. It's also the central command center for your car or your home. Many people also use their smartphone to authenticate and gain access to other networks, businesses, financial systems and critical infrastructure. And we feel a great sense of responsibility to protect that information and access.

For all of these reasons, our digital devices, indeed our entire digital lives, are increasingly and persistently under siege from attackers. And their attacks grow more sophisticated every day. This quest for access fuels a multi-billion dollar covert world of thieves, hackers, and crooks. We are all aware of some of the recent large-scale attacks — hundreds of thousands of social security numbers were stolen from the IRS, the U.S. Office of Personnel Management said as many as 21 million people had their records compromised and as many as 78 million people were affected by an attack on Anthem's health insurance records.

The best way we, and the technology industry, know how to protect your information is through the use of strong encryption. Strong encryption is a good thing, a necessary thing. And the government agrees. Encryption today is the backbone of our cybersecurity infrastructure and provides the very best defense we have against increasingly hostile attacks. The United States has spent tens of millions of dollars through the Open Technology Fund and other programs to fund strong encryption. And the Administration's Review Group on Intelligence and Communications Technology urged the U.S. government to fully support and not in any way subvert, undermine, or weaken generally available commercial encryption software.

At Apple, with every new release of hardware and software, we advance the safety, security and data protection features in our products. We work hard to assist law enforcement because we share their goal of creating a safer world. I manage a team of dedicated professionals that are on call 24 hours a day, 365 days a year. Not a day goes by where someone on my team is not working with law enforcement. We know from our interactions with law enforcement officials that the information we are providing is extremely useful in helping to prevent and solve crimes.

Keep in mind that the people subject to law enforcement inquiries represent far less than one-tenth of one percent of our hundreds of millions of users. But all of those users — 100% of our users would be made more vulnerable if we were forced to build a back door.

As you heard from our colleagues in law enforcement, they have the perception that encryption walls off information to them. But technologists and national security experts don't see the world that way. We see a data-rich world that seems to be full of information. Information that law enforcement can use to solve -- and prevent -- crimes.

This is the difference in perspective that we should be focused on resolving. To suggest that the American people must choose between privacy and security is to present a false choice. The issue is not about privacy at the expense of security. It is about maximizing safety and security.

We feel strongly that Americans will be better off if we can offer the very best protections for their digital lives.

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