STATEMENT OF
ERIK NEUENSCHWANDER
DIRECTOR OF USER PRIVACY, APPLE INC.

United States Senate Judiciary Committee
Hearing on "Encryption and Lawful Access:
Evaluating Benefits and Risks to Public Safety and Privacy"
December 10, 2019

Good morning Chairman Graham, Ranking Member Feinstein, and Members of the Committee. Thank you for inviting me to speak with you today about how encryption works and the important role it plays in keeping electronic data and records secure.

My name is Erik Neuenschwander, and I have been a software engineer at Apple for twelve years. I worked as the first data analysis engineer on the first iPhone, managed the software performance team for the first iPad, and founded Apple's privacy engineering team. Today, I manage the team responsible for the technical aspects of designing Apple's privacy features. I am proud to work at a company that builds great products that improve people's lives.

Today, iPhone is used for much more than phone calls. Around the world, people use them every day to store and send sensitive and important data: personal financial information, our health data, communications with our colleagues, and even information about the location of our family members. And as the Internet is making the world even more interconnected, people use their iPhones to remotely control things like home security systems, vehicles, and appliances. Your iPhone needs to be protected from hackers and criminals—and that is what strong encryption helps to do. Encryption is the underlying technology providing information security in all modern systems. We do not know of a way to deploy encryption that provides access only for the good guys without making it easier for the bad guys to break in.

Encryption not only protects a person's sensitive data, it is also one of the most important mechanisms we have as a nation to safeguard an increasingly interconnected future. Every day, over a trillion transactions—from financial transactions to the exchange of healthcare records—occur safely over the Internet because of encrypted communications. Utilizing 5G networks, connected devices will play an even larger role in the operation and maintenance of our critical infrastructure, running our electric grids, transportation networks, and healthcare and financial systems. Encryption is needed to protect from malicious actors whose attacks are growing exponentially in scope, frequency, and sophistication. And encryption will become even more important as more devices are added to the Internet and attack surfaces expand.

Encryption is woven through our software, hardware, and services for maximum security. We also challenge ourselves to collect as little customer data as possible, including through the use of tools that process data only on a person's device, rather than on Apple's servers; if we don't have your information, then nefarious insiders or malicious hackers who gain access to Apple's networks won't either. And our use of Secure Enclave, a hardware-based key manager that is isolated from the main processor, provides an extra layer of security. Overall, our approach to design improves security, reducing points of vulnerability and risk.

We understand that rapidly evolving technologies, by their very nature, can create challenges for investigators. At Apple, we share law enforcement's goal of creating a safer world, and we work closely with law enforcement every day. We have a staff of professionals, including former law enforcement personnel, on call 24 hours a day, seven days per week to assist law enforcement with lawful requests. This work is significant. Over the past 7 years, the company has responded to over 127,000 requests from U.S. law enforcement agencies for information that we've been told is critical to helping prevent or solve crimes. In addition, our teams have fielded and supported thousands of emergency requests from U.S. law enforcement, typically taking action within twenty minutes of receipt. And the number of U.S. government requests has increased over 100%, indicating that the information we are providing is valuable to investigations.

Given the pace of innovation and the growth of data in recent years, we understand that one of the biggest challenges facing law enforcement is a lack of clear information about what data are available, where they are stored, and how they can be obtained. That is why we publish a comprehensive law enforcement guide that provides this information, and our team has trained law enforcement officers in the United States and around the world on these processes. We will continue to increase our training offerings in the future, including by deploying online training to reach smaller law enforcement departments.

Chairman Graham, Ranking Member Feinstein, and Members of the Committee, thank you for the opportunity to participate in this important hearing.