**Statement of Senator Patrick Leahy (D-Vt.),**
**Ranking Member, Senate Judiciary Committee,**
**Hearing on "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"**
**July 8, 2015**

Over the past 20 years, the Internet has transformed the lives of Vermonters and the American people. We use the Internet to communicate, make financial transactions, access medical records, file taxes, and store personal information and photographs.

Critical to this digital revolution has been the development and use of strong encryption. Encryption ensures that the digital information we send or store electronically is protected against hackers, criminals, and spies. But as we will hear this morning, the increased use of encryption also presents challenges for law enforcement.

Two decades ago, during the so-called "Crypto Wars," the FBI and others argued that strong encryption prevented investigators from obtaining access to information even when they had a court order. They are voicing similar concerns today.

As a former prosecutor, I am sympathetic to these public safety concerns. Encryption can impede investigations by federal, state and local law enforcement officials. So this is an important discussion for us to have. But as we learned in the 1990s, this is a complicated problem with no easy solutions.

Some have suggested that technology companies should build special law enforcement access into their systems. But we also have to consider the risks of this approach. Strong encryption has revolutionized the online marketplace and protects American businesses and consumers from cybercrime, espionage, identity theft, stalking, and other threats on the Internet. Undermining strong encryption could make our data more vulnerable.

In the 1990s, I opposed efforts to regulate the development of encryption technology. I sponsored and otherwise supported legislation that authorized the use of any type of encryption technology in the United States; prohibited the government from requiring key recovery features; and eased export restrictions limiting the sale of encryption technology abroad. I also opposed efforts to promote the "Clipper Chip," a cryptographic device for voice communications that facilitated government access to those communications.

I was concerned that regulating encryption would stifle innovation, harm American businesses, impede technological advancements, and undercut security. In 1996, I wrote an open letter to the Internet – and became the first member of Congress to use the popular encryption program Pretty Good Privacy and sign a letter using an encrypted digital signature – arguing that regulating encryption was a "hopelessly outdated" policy that "fails to account for the real needs of individuals and businesses in the global marketplace." The Clinton administration ultimately abandoned efforts to limit encryption technology. Many experts now credit this decision for helping create the modern Internet, in which consumers use encryption to facilitate online retail, banking, social media, and other communications.

Fifteen years later, the vast majority of security experts explain that creating special access for law enforcement would still introduce into the digital space significant security weaknesses -- at a time when we need the strongest possible cybersecurity. Just yesterday, a group of the world's preeminent computer scientists and security experts released a report concluding that any special access for law enforcement would pose "grave security risks, imperil innovation, and raise thorny issues for human rights and international relations." Last month, nearly 150 security experts, tech companies, and other organizations wrote to the President making similar points. I ask that those materials be placed in the record.

The President's Review Group on Intelligence and Communications Technology also explained in their December 2013 report that "in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud."

We also have to consider the effect on U.S. government efforts to promote encryption and secure communications technology around the world. As Ranking Member of the Appropriations Subcommittee on State, Foreign Operations and Related Programs, I know we have appropriated more than $100 million dollars just in the past two years to promote Internet freedom, including providing strong encryption technology to human rights workers, journalists, and political dissidents working under repressive regimes.

Even if the United States were to take steps to facilitate law enforcement access to encrypted communications, we need to evaluate how much it would help. Strong encryption would still be available from foreign providers. Some say that any competent Internet user would be able to download strong encryption technology, or install an "app" allowing encrypted communications – regardless of restrictions on American businesses. But it would put American companies at a disadvantage in the global marketplace.

These are among many factors this Committee must consider. The Committee is hearing some important perspectives today, but there are other voices that need to be part of this conversation. When the Chairman holds further hearings on this topic, I hope that he will also include witnesses from the technology industry, which would be directly affected by any effort to regulate encryption. I ask that materials from industry trade associations be placed in the record.

I welcome Deputy Attorney General Yates, who is with us for the first time since her confirmation. And it is always good to see Director Comey, who I was pleased to host in Vermont a couple of months ago. I look forward to hearing from both of you.

# # # # #