Opening Statement of the Honorable Tim Murphy
Subcommittee on Oversight and Investigations
Hearing on "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives"
April 19, 2016

(As Prepared for Delivery)

We are meeting today to consider the deceptively complex question: Should the government have the ability to lawfully access encrypted technology and communications?

This is the question at the center of a heated public debate, catalyzed earlier this year when the FBI obtained a court order to compel Apple to assist in unlocking an iPhone used by one of the San Bernardino terrorists.

But this isn't a new question. Strong encryption has existed for decades. For years, motivated individuals have had access to the tools necessary to conceal their activities from law enforcement. And for years, the government has repeatedly tried to limit the use of or obtain access to encrypted data.

The most notable example occurred in the 1990's when the development of encrypted communications equipment sparked fears that the government would lose its ability to conduct lawful surveillance. In response, the NSA developed a new encryption chip –-called the "Clipper Chip" – that would enable encrypted communications, but would also provide the government with a key to access those communications, if necessary. This so-called "backdoor" sparked intense debate between the government and the technology community about the benefits – and risks – of government access to encrypted technology.

One of the principle arguments of the technology community was that such a backdoor would create a vulnerability that could be exploited by actors outside of the government. This concern was validated when a critical flaw was discovered in the chip's design. I should note that one of our witnesses here today, Dr. Matt Blaze, identified that vulnerability which made the government's backdoor more akin to a front door.

As a partial solution, Congress passed the Communications Assistance for Law Enforcement Act (CALEA). CALEA addressed the government's concern that rapidly evolving technologies were curtailing their ability to conduct lawful surveillance by requiring telecommunications providers to provide assistance in executing authorized surveillance. However, the law included notable caveats which limited the government's response to encrypted technologies.

After the government relaxed export controls on encryption in 2000, the Crypto Wars entered a period of relative quiet. So what has changed in recent years to renew the debate? Part of the concern is, once again, the rapid expansion of technology. At its core, however, this debate is about the widespread availability of encryption, by default.

While encryption has existed for decades, until recently it was complex, cumbersome and hard to use. It took effort and sophistication to employ its benefits, either for good or evil. Because of this, law enforcement was still able to gain access to the majority of the digital evidence they discovered in their investigations.

But now, the encryption of electronic data is the norm – the default. This a natural response to escalating concerns – both from government and consumers – about the security of digital information. The decision by companies like Apple and the messaging application WhatsApp to provide default encryption means more than a billion people – including some living in countries with repressive governments -- have the benefit of easy, reliable encryption. At the same time, however, criminals and terrorists have the

same access to secure means of communication – and they know it, and they will use it as their own mission control center.
That is the crux of the recent debate. Access to secure technologies beyond the reach of law enforcement no longer requires coordination or sophistication. It is available to anyone and everyone. At the same time, however, as more of our lives become dependent on the internet and information technologies, the availability of widespread encryption is critical to our personal, economic and national security.

Therefore, while many of the arguments in the current debate may echo those of decades past, the circumstances have changed and so too must the discussion. This can no longer be a battle between two sides, a choice between black-and-white. If we take that approach, the only possible outcome is that we all lose. This is a core issue of public safety and ethics – and it requires a very thoughtful approach. That is why we are today – to begin moving the conversation from "Apple vs. the FBI" or "right versus wrong" to a constructive dialogue that recognizes this is a complex issue that affects everyone and therefore "we are in this together." We have two very strong panels and I expect each will make strong arguments about the benefits of strong encryption and the challenges it presents for law enforcement. I encourage my colleagues to embrace this opportunity to learn from these experts to better understand the multiple perspectives, layers and complexities to this issue.

It is time to begin a new chapter in this battle – one which I hope can ultimately bring some resolution to the war. This process will not be easy but if it does not happen now, we may reach a time when it is too late and success becomes impossible. So, for everyone calling on Congress to address this issue, here we are. I can only hope, moving forward, you will be willing to join us at the table.

###