Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Hearing On "Going Dark:
Encryption, Technology, and the Balance Between Public Safety and Privacy"
Wednesday, July 8, 2015

Today's hearing is intended to start a conversation in the Senate about whether recent technological changes have upset the balance between public safety and privacy. Just a few days ago, we celebrated the birth of our country. That occasion should serve as a reminder of the gifts bestowed upon us by the Founders: not only the Declaration of Independence adopted that day, but the Constitution that followed it. And the protection of our privacy and civil liberties by the Bill of Rights, more specifically by the Fourth Amendment, provides a useful place to begin our conversation today.

The core of the Fourth Amendment is the requirement that, with limited exceptions, when a law enforcement officer is investigating a crime, the officer must obtain an individualized warrant or court order to conduct a search that would violate a person's reasonable expectation of privacy. And that order must be issued by a neutral and detached judge based on facts that demonstrate probable cause. Through this brilliant framework, for over 200 years, our constitutional system has preserved the rule of law, ensured our public safety is maintained, and protected our individual privacy and civil liberties in part through the separation of powers. But recently, prominent law enforcement officials have been questioning whether the laws Congress has enacted over the years to adapt that framework to changing technology, such as the Communications Assistance for Law Enforcement Act, or CALEA, are adequate to the task today.

What they have been telling us is that increasingly, even after they have obtained authority from a judge to conduct a search for evidence of a crime, they lack the technical means to do so. Director Comey and Deputy Attorney General Yates have recently spoken out about this issue, and I've heard about it from state and local officials in Iowa as well. They describe two distinct but related components to the problem. First, they report a decreasing ability to intercept real-time communications, such as phone calls, email, texts, and other kinds of so-called "data in motion." And second, they relate a similar concern regarding their inability to execute search warrants on encrypted phones, laptops, and other devices, which store what they refer to as "data at rest."

Companies are increasingly choosing to encrypt these devices in such a way that the company itself is unable to unlock them, even when presented with a lawful search warrant. These encrypted devices, they fear, are becoming the equivalent of closets and safes that can never be opened, even when a judge has expressly authorized a search for evidence inside them. In their view, this development has the potential to impact the fair and impartial application of our laws by effectively placing certain places, and therefore certain people, outside the law. These officials describe the cumulative effect of these changes on their ability to do their jobs as "Going Dark." It's not a new issue. But according to them, it's a problem that's getting dramatically worse, and it's having a real effect on their ability to protect the public and to bring criminals to justice.

The reason for these sweeping changes isn't difficult to understand. Rapidly changing technology has made the way we store and communicate our personal data today quite different than in 1776 – let alone even five or ten years ago.

Today's revolution, then, is a technological one. It's a revolution that's resulted in a proliferation of new devices, networks, apps, and other modes of communication. And by leading this revolution, some of our finest American companies are enriching our lives. Through their ingenuity and innovation, they are allowing us to be in closer touch with our loved ones, sharing the things important to us in new ways. However, as more of our lives have ended up on digital platforms, devices and on the internet, our data has increasingly become a target for hackers, criminals and foreign governments.

We pick up the newspaper and read about breaches that have left personal data exposed almost on a daily basis. So we want our data to remain private and secure, and it's natural that companies seek to respond to this market demand. But at the same time, these wonderful technologies are also being employed by those who seek to do us great harm.

In particular, Director Comey has talked about the challenges this issue presents the FBI in the national security context. According to the Director, ISIS is recruiting Americans on-line and then directing them to encrypted communication platforms that are beyond the FBI's ability to monitor, even with a court order. If this is accurate, it obviously represents a dangerous state of affairs.

So how do we balance the need for both public safety and privacy? Are there ways that we can provide law enforcement judicially-sanctioned access to these platforms without compromising their overall security? Or are there other potential reforms that could simply shift the balance less dramatically? These are questions that have no easy answers.

I know many in our privacy and technology communities are highly skeptical that any reform can be accomplished without unacceptably undermining both the privacy interests of our citizens as well as the international competitiveness of our technology companies. These are, no doubt, fundamentally important considerations. But as a start, we need to have an open and honest conversation that examines the costs and benefits both of potential reforms, as well as continuing down the path we are headed. And we need to do so with humility and respect for those who come to the issue from different perspectives.

Last year, the Washington Post ran an editorial on the "Going Dark" issue, describing our time as "an important moment in which technology, privacy and the rule of law are colliding." Ultimately, the newspaper called for compromise. That's the spirit the Framers brought to Philadelphia that gave us the Constitution and that eventually produced the Bill of Rights.

Today, I hope the Senate takes a first step at seeing if any consensus is possible on this important and complicated issue.