Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Hearing on "Reforming the Electronic Communications Privacy Act"
September 16, 2015

Today's hearing is intended to help inform the Committee about the most recent views of a wide variety of stakeholders concerning the need to reform the Electronic Communications Privacy Act, or ECPA, and various ways of doing so. The Committee's last hearing on the topic was four and a half years ago. Since then, numerous proposals have been advanced by members of the Committee.

In 1986, Congress enacted ECPA to both protect the privacy of Americans' electronic communications and provide the government with a means to access those communications and related records in certain circumstances. However, dramatic changes in the use of communications technology have occurred since then.

Americans now depend on email, text messages, social networking websites, web-based apps, and countless other electronic communication methods on a daily basis. And more than ever, these communications are being retained in some form, due to the dramatic reduction in the cost of storing data in the cloud.

These communication technologies are enriching all of our lives. They are of great help to me in keeping in touch with my constituents in Iowa. And for the most part, we have American technology companies to thank for this digital revolution. These companies are now a significant engine of growth for our economy by creating an increasingly global market for these communications technologies.

But of course, these technologies are also being used every day by those who intend to do our society great harm – terrorists, violent drug dealers, child predators, environmental criminals, and the like. These technologies create a digital trail that is often essential to bringing these offenders to justice.

In light of these changes, there is a growing consensus that ECPA must be modernized to adapt to this new landscape. And whatever updates to the law we make, of course, must be consistent with the requirements of the Fourth Amendment.

The privacy and technology communities have criticized ECPA for failing to provide sufficient privacy safeguards for individuals' stored electronic communications. Indeed, given the way Americans use email today, it hardly makes sense that the privacy protections for an email should turn on whether it's more than 180 days old, or whether it's been opened.

At the same time, law enforcement officials have expressed concern with certain aspects of the current ECPA framework and how it currently works in practice. And they are concerned that reform efforts to a statute they use every day do not unduly hamper their ability to investigate violations of the law.

For example, the Department of Justice has expressed concern about efforts to change the ECPA notice requirements to provide targets with unprecedented amounts of information that could compromise ongoing investigations.

Both the Department and civil law enforcement agencies have expressed the need to address an emerging gap in their authorities if the target of an investigation fails to respond to lawful civil process for email evidence in the target's possession. They contend that this gap could allow offenses such as civil rights violations, securities fraud, and consumer fraud to go unpunished.

In addition, many state and local law enforcement officials are frustrated with the current timeliness and quality of responses by providers. Unlike traditional search warrants, law enforcement agents cannot control how quickly they obtain evidence through ECPA warrants; they rely on the providers to conduct searches for them. To these officials, any heightening of ECPA's legal standards should be accompanied by changes to the law that ensure that they receive the information they need on a timely basis.

In addition, some officials have expressed concern that the voluntary nature of ECPA's emergency exception can result in unacceptable delay in important cases – for example, when a child is abducted.

Closely related to these concerns is the ongoing issue of encryption and the "Going Dark" problem, which the Committee recently held a hearing on. This is another example of a situation where agents may meet the legal standard to obtain critical evidence – but then are not able to access it quickly enough, or even at all.

As I said at our last hearing on ECPA reform in 2011, if we are considering changing the legal standards under ECPA, we should also "be working to ensure that these same providers are granting law enforcement the necessary access" to address the "Going Dark" issue. I sent a letter to the Deputy Attorney General last week to get an update from the Department about how that process is proceeding.

Reforming ECPA's treatment of stored electronic communications, therefore, is a complicated and potentially far-reaching endeavor that sits at the intersection of the privacy rights of the public, the investigative needs of law enforcement professionals, society's interest in encouraging and expanding commerce, and the dictates of the Constitution.

The key is to strike the right balance between these interests. As Ranking Member Leahy declared at our last hearing on this topic in 2011, "meaningful ECPA reform must carefully balance privacy rights, public safety, and security." I couldn't agree more. I'm grateful for the presence of all the witnesses here today and look forward to their testimony. I now recognize Senator Leahy for his opening statement.