August 4, 2015

The Honorable Chuck Grassley
Chairman
Senate Judiciary Committee

The Honorable Patrick Leahy
Ranking Member
Senate Judiciary Committee

The Honorable Mike Lee
Chairman, Subcommittee on Antitrust, Competition Policy, and Consumer Rights Subcommittee
Senate Judiciary Committee

RE: S. 356 – the Electronic Communications Privacy Act Amendments Act of 2015 and Reducing the Effects of Non-Technical Barriers to Lawful Access to Electronic Evidence

Dear Chairman Grassley, Ranking Member Leahy, and Senator Lee:

We, the undersigned organizations representing federal, state and local prosecutors, chiefs, sheriffs, and rank and file officers, understand the intent of S. 356, the Electronic Communications Privacy Act Amendments Act of 2015, is to update the law to ensure that Americans' privacy rights are reinforced in the digital age. While we support efforts to guarantee the privacy rights of all citizens, we write with serious concern about certain provisions of the bill and to ask that new provisions be considered to ensure law enforcement, with appropriate judicial supervision and approval, maintains an ability to access and recover digital evidence in order to protect the public and successfully prosecute those guilty of crimes. Failure to address these challenges will result in more missed leads, longer investigative timelines, less safety for Americans and less justice for victims of crime.

The amount of evidence that exists in the digital space is growing explosively. Our society is powered by data that lies at rest and moves across a vast range of devices. Some of that data becomes evidence every time a crime is committed, and this electronic evidence is critical to investigators who need it to generate leads, corroborate stories, identify suspects and conspirators, challenge alibis, exonerate the innocent, and obtain justice for victims of crime.

Evidence takes a variety of forms in the digital space. Evidence can be found in the content of communications and in the data that surrounds communications events. Evidence can be gathered while at rest on devices and in real time while it is in motion across networks. Law enforcement is concerned about anything that creates a barrier to lawfully accessing that

evidence, because it makes it more difficult to solve crimes. Some of the barriers that degrade our effectiveness are technological, like encryption, and others are non-technological, like elevated legal standards and a lack of responsiveness by private companies who possess electronic evidence.

The attached fact sheet provides an overview of these barriers along with a number of possible solutions that would help ensure that law enforcement maintains access to the critical digital evidence it needs to fulfill its mission. Law enforcement collects much of the electronic evidence it needs by exchanging legal process with service providers like wireless phone companies, internet providers, and application developers. The logistics of requesting and receiving information from service providers in response to these lawful process demands are antiquated, non-standardized, and often haphazard, causing a very real and under-publicized set of problems. Bringing consistency to the standard of proof that governs law enforcement access to evidence is meaningless if law enforcement cannot obtain the evidence because it hasn't been retained, because the court order is lost after being transmitted, or because the response takes weeks or months to process by the service provider.

In particular, we note that S. 356 imposes overly burdensome requirements for law enforcement to notify the targets of criminal investigations that evidence against them is being sought, and yet imposes no duty on companies to respond to legal demands like search warrants in a timely manner. The proliferation of electronic evidence means that law enforcement is seeking more legal process to obtain that evidence in more complex investigations. In many cases, the most critical evidence is behind several layers of private companies, each with their own response policies and legal compliance staff. If we must wait weeks and months for responses to our legal demands, and must at the same time devote valuable investigative resources to complying with notice requirements or seeking delays through yet more court orders, we will be less effective at our core mission. In addition, the bill would impose a dangerously short time period for service provider notice to law enforcement regarding customer notification. This could jeopardize criminal investigations by giving information to investigative targets before law enforcement has an opportunity to either seek a delay in notification or take other action.

To be clear, law enforcement is not asking for new surveillance capabilities above and beyond what is currently authorized by the U.S. Constitution or by lawful court orders, nor are we attempting to access or monitor the digital communications of all citizens. Law enforcement simply needs to be able to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders—information of potentially significant consequence for investigations of serious crimes and terrorism.

We would welcome the opportunity to discuss our concerns and potential solutions to these issues with you at your earliest convenience.

Thank you for your attention to this matter.

Sincerely,

Association of Prosecuting Attorneys
Association of State Criminal Investigative Agencies

Federal Law Enforcement Officers Association
International Association of Chiefs of Police
Major Cities Chiefs Association
Major County Sheriffs' Association
National Association of Police Organizations
National District Attorneys Association
National Fraternal Order of Police
National Fusion Center Association
National Narcotic Officers' Associations' Coalition
National Sheriffs' Association

cc: Members of the Senate Judiciary Committee
cc: Majority Leader Mitch McConnell
cc: Minority Leader Harry Reid