Federal Bureau of Investigation
Agents Association

September 24, 2015

The Honorable Charles E. Grassley
Chairman
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Patrick J. Leahy
Ranking Member
Senate Committee on the Judiciary
Washington, DC 20510

Re: Reforming the Electronic Communications Privacy Act

Dear Chairman Grassley and Ranking Member Leahy:

On behalf of the FBI Agents Association (FBIAA), a voluntary professional association currently representing over 12,000 active duty and retired FBI Special Agents, I write to express the FBIAA's concerns and thoughts regarding issues raised in the hearing held by your committee on September 16, 2015, entitled "Reforming the Electronic Communications Privacy Act." During the hearing, witnesses and Senators raised a number of important concerns about efforts to change the Electronic Communications Privacy Act (ECPA), and the FBIAA believes that legislative efforts to reform ECPA must address these concerns directly, before any ECPA reform legislation should be enacted.

Chairman Grassley, you correctly noted during the hearing that reforming ECPA 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 profession, society's interest in encouraging and expanding commerce, and the dictates of the Constitution." On behalf of the brave men and women defending this Nation as federal law enforcement officers, let me assure you that we share your commitment to adhering to the Constitution and striking the proper balance between privacy and security. It is for this very reason that we think that any ECPA reform legislation must address the serious issues raised at your recent hearing.

The FBIAA is particularly concerned about two major issues regarding the ECPA reform proposals that have been discussed to date:

Post Office Box 320215 • Alexandria, Virginia 22320
A Non-Governmental Association
(703) 247-2173 Fax (703) 247-2175
E-mail: fbiaa@fbiaa.org www.fbiaa.org

1. **ECPA reform legislation should ensure that law enforcement is able to access electronic evidence.**

As a number of witnesses and Senators noted during your recent hearing, technology has evolved significantly in recent years and has made it necessary for Congress to update the laws surrounding electronic privacy. However, such an effort must address more than the business and privacy concerns of major technology companies. Meaningful ECPA reform must also address the security and law enforcement needs of our citizens by preventing criminals from having unfettered access to secure communications, including crucial warrant exceptions, and requiring that technology companies cooperate with lawful investigations.

Going Dark

An important aspect of the recent technology revolution has been the development of hardware and software that threatens to give criminals secure tools for communication and dissemination of information and materials—tools that can make it impossible to obtain electronic evidence even when such evidence is required to be produced pursuant to a lawful warrant.

Never before in our country's history have criminals and terrorists had access to technology that could allow them to coordinate their efforts nationally or internationally without any ability for law enforcement to legally access the evidence of their conspiracies. Such a scenario—often described as "going dark"—could create new and dangerous risks of crime and terrorism. Accordingly, Congress must address the risks of going dark by ensuring that technology companies allow for lawful access to electronic data.

Warrant Exceptions

Requiring a probable cause warrant for access to all electronic information could add additional delays to the investigation process, and such delays could pose unique risks to investigations that are uniquely time-sensitive. Accordingly, the FBIAA believes that ECPA reform legislation should include explicit exceptions to the warrant requirement for emergencies and investigations of crimes such as child pornography where the time and delays associated with warrants and the risks of notification can jeopardize investigations.

Service Provider Cooperation

ECPA reform legislation that has been considered by Congress to date, such as S. 356, increases administrative burdens on law enforcement by expanding warrant requirements, but does not address the need for internet service providers to deliver timely responses to law enforcement requests. Delayed responses or a lack of communication from internet service providers in response to law enforcement requests can jeopardize sensitive investigations, and Congress should compel these providers to develop reliable and efficient procedures for responding to law enforcement requests for electronic information.

ECPA reform should include language requiring that internet service providers develop internal response protocols designating at least one individual as a "24/7" point of contact for law enforcement requests, and requiring that responses to requests be made in a timely manner. Additionally, Congress should clarify the language in 18 U.S.C. § 2709 to make it clear that service providers must provide all relevant electronic communications transaction records when they are properly requested by law enforcement officials.

2. **ECPA reform legislation should not create new obstacles for investigations**

The FBIAA understands that there are aspects of ECPA that have been rendered obsolete by changing technology and should be revised. However, ECPA reform should not result in the creation of new and unnecessary obstacles for law enforcement officials. In particular, Congress should avoid creating new and risky notification procedures, and should not include provisions that would make it more difficult for law enforcement to obtain electronic evidence housed outside of the U.S.

Notification of Targets

As discussed in our previous communications with your committee and Congress, the FBIAA is concerned that target notification requirements that have been included in ECPA reform bills may threaten the effectiveness of sensitive investigations of criminals and terrorists.

Search warrants are often obtained in the early stages of investigation, and notifying the target of a search warrant about its issuance could allow for the destruction of vital evidence. Requiring notice a few days after a warrant is issued, even with the ability to request a delay, risks administrative and technical errors that could result in targets of an investigations being told of ongoing investigations, a potential threat to public safety. Further, even if a delay order is obtained, limiting the delay to 180 days could undermine investigations that require more than 180 days to complete because targets would be notified of the ongoing investigation. While the orders can be renewed, an accidental failure to do so or a delay due to administrative error would alert the target to the investigation.

For these reasons, the FBIAA believes that changes need to be made to the proposed notification requirements that have been included in ECPA reform bills such as S. 356. Specifically, rather than a presumption of notification, there should be a presumption that notice is not required until an investigation is ended and a court finds that notification would not pose a risk to ongoing investigations.

Access to Evidence Overseas

In the era of cloud computing, electronic evidence held by U.S. companies or persons may be physically stored anywhere around the world. Access to this evidence is essential to investigations of criminal and terrorist enterprises, and U.S. service providers should not be able to refuse to comply with warrants because they have opted to locate their servers outside

of the U.S. To do so would be to create an easy method for criminals and terrorists to evade law enforcement scrutiny and execute their plots to threaten the safety and security of our country. Despite these risks, however, some are seeking to expand ECPA reform legislation to include provisions that would make it more difficult for law enforcement officials to obtain this electronic evidence.

Negotiating cross-border data issues is complicated and delicate, and Congress should not use ECPA reform to circumvent ongoing diplomatic and analytical work being put into cross-border data access. Specifically, ECPA reform legislation should not be expanded to include proposals such as the *Law Enforcement Access to Data Stored Abroad Act* (LEADS Act). The FBIAA believes these proposals have significant flaws, and could make it more difficult to investigate, thwart, and prosecute criminals and terrorists.

We greatly appreciate your consideration of these concerns, which are of critical importance to the federal law enforcement community.

We look forward to continuing to work with you as you explore the impact of ECPA changes on federal law enforcement activities. If you have any questions, please contact me at rtariche@fbiaa.org or 703-247-2173, or FBIAA General Counsel Dee Martin, dee.martin@bgllp.com, and Joshua Zive, joshua.zive@bgllp.com.

Sincerely,

Reynaldo Tariche
President