Federal Bureau of Investigation
Agents Association

February 29, 2016

The Honorable Robert W. Goodlatte
Chairman
House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member
House Committee on the Judiciary
B351 Rayburn House Office Building
Washington, DC 20510

Re: H.R. 699, the *Email Privacy Act*

Dear Chairman Goodlatte and Ranking Member Conyers:

On behalf of the FBI Agents Association (FBIAA), a voluntary professional association currently representing over 13,000 active duty and retired FBI Special Agents, I write to express the FBIAA's concerns regarding H.R. 699, the *Email Privacy Act*. H.R. 699 is far more than a simple fix to dated language in the Electronic Communications Privacy Act (ECPA), as it creates new and unnecessary obstacles to effective law enforcement investigations and fails to address a variety of issues that are central to the debate over electronic privacy. For these reasons, H.R, 699 should not be adopted as currently drafted.

Reforming ECPA is a complex endeavor that touches on the important intersection of privacy expectations and protection of public safety. 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 in this letter and by other law enforcement groups.

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

The FBIAA is particularly concerned about two major issues regarding H.R. 699:

1. **H.R. 699 Creates Dangerous New Obstacles to Effective Law Enforcement**

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. It should not be more difficult for law enforcement to access electronic data than it is for those officers to lawfully obtain private information that can be found in paper records.

- **Unreasonable and dangerous notification procedures**

H.R. 699 creates new notification requirements that would result in electronic content being treated much differently than searches for physical evidence. A traditional search warrant identifies the place or person to be searched and the items being sought, and after a search officers will typically leave a copy of the warrant behind at the physical location that was searched. H.R. 699 treats electronic content differently, requiring that law enforcement, within 10 business days, directly serve the target of investigation with both a copy of the warrant and a detailed explanation of the "nature of the law enforcement inquiry." Both the requirement to serve the target of an investigation, as opposed to the place being searched, and the mandate for a narrative description of the investigation are new and unparalleled notification requirements that could jeopardize 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. Additionally, being required to provide a narrative description of the investigation would require that law enforcement officers disclose the nature of their investigations in a manner that is wholly inconsistent with existing warrant procedures and the ability to conduct successful investigations.

Congress should significantly alter the notification provisions in H.R. 699. Specifically, the notification requirement in H.R. 699 should be removed, and delayed notice should not be subject to an arbitrary time limit.

- **Removal of necessary exceptions**

Fourth Amendment protections against unreasonable searches have long incorporated the notion that warrantless searches are not unreasonable in situations where there is the imminent risk of physical harm or destruction of evidence. However, H.R. 699 ignores these established principles and provides special treatment for electronic content.

Past iterations of ECPA legislation have included reasonable and necessary exceptions to warrant requirements. As currently drafted, H.R. 699 includes no exceptions to the new warrant requirements, and this greatly concerns the FBIAA. 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.

H.R. 699 should include explicit exceptions to the warrant requirement for emergencies, information provided with consent, publicly available information, "to:from" information from emails, and investigations of crimes such as child pornography, where the time and delays associated with warrants and the risks of notification can jeopardize investigations.

- **Expansive shielding of "remote computing services"**

H.R. 699 prohibits voluntary disclosure of information stored by remote computing services and creates new warrant requirements covering the entire expanse of remote computing services. These mandates goes far beyond the protection of electronic communications where people have a reasonable expectation of privacy, and could make it unnecessarily difficult for law enforcement investigators to access information stored by web pages in a timely and efficient manner.

Treating all remote computing services in the same manner as electronic communications providers could jeopardize sensitive investigations of matters such as child pornography or other crimes involving prohibited items. These investigations often utilize commercial and transactional records stored on web pages that traffic in this material This type of information is not currently treated as having a reasonable expectation of privacy, because it is either public or provided to a third party, and is not covered by warrant requirements. The new warrant requirements applicable to remote computing services under H.R. 699, however, would result in additional administrative burdens and delays that could place these investigations at risk in the future.

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

Congress should reconsider the expansive treatment provided to remote computing services because of the risks posed to sensitive investigations.

2. H.R. 699 Should Ensure Access to Electronic Evidence

Congress rarely acts on electronic privacy issues, and any effort to revise our privacy laws should address the pressing issues related to the careful balance between privacy and safety. 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 and requiring that technology companies cooperate with lawful investigations.

- **The need to prevent law enforcement from "Going Dark"**

It would irresponsible and dangerous for Congress to act on electronic privacy legislation without addressing one of the most important challenges currently facing law enforcement—the development of hardware and software that is giving criminals secure tools to plan and execute plots against our country and citizens.

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. Unfortunately, we have already begun to see the risks posed by this new technology. On February 16th, U.S. Magistrate Judge Sheri Pym ordered Apple to develop overrides allowing investigators to access the San Bernardino attackers' encrypted cell phone data, because Apple's technology currently locks out law enforcement—thwarting their investigation into the terrorist networks behind those attacks. Rather than working to find a cooperative solution to these challenges, Apple and other technology companies have committed millions of dollars and scores of lawyers and lobbyists to fighting to any effort to allow lawful access to this information.

If Congress chooses to address electronic privacy issues through a vehicle such as H.R. 699, the FBIAA believes it would irresponsible to not also address the risks posed by going dark. In the effort to strike a balance between privacy and safety, Congress should take steps to ensure that technology companies allow for lawful access to electronic data, and that

terrorists and criminals are not provided easy means to escape detection, investigation, and prosecution.

- **Requiring Service Provider Cooperation**

H.R. 699 increases administrative burdens on law enforcement by expanding warrant requirements, but does not adequately 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.

H.R. 699 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.

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

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