(Best Viewed With Bookmarks Showing)

Department of Justice

STATEMENT OF
THE DEPARTMENT OF JUSTICE

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"H.R. 699, THE 'EMAIL PRIVACY ACT'"

PRESENTED
DECEMBER 1, 2015

Statement of
The Department of Justice

Before the
Committee on the Judiciary
U.S. House of Representatives

At a Hearing Entitled
"H.R. 699, the 'Email Privacy Act'"

December 1, 2015

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for the opportunity to submit a statement for the record on behalf of the Department of Justice regarding the Electronic Communications Privacy Act (ECPA). This topic is particularly important to the Department because of the wide-ranging impact the statute has on public safety and both criminal and civil law enforcement operations. We are pleased to engage with the Committee in discussions about how ECPA is used and how it might be updated and improved.

ECPA includes the Pen Register Statute and the Stored Communications Act (SCA), as well as amendments to the Wiretap Act. These statutes are part of a set of laws that control the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. Although originally enacted in 1986, ECPA has been updated several times since, with significant revisions occurring in both 1994 and 2001.

We intend to focus the majority of this statement on the SCA, which contains three primary components that regulate the disclosure of certain communications and related data. First, section 2701 of Title 18 prohibits unlawful access to certain stored communications: anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Second, section 2702 of Title 18 regulates voluntary disclosure by service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates the government's ability to compel disclosure of both stored content and non-content information from a service provider; it creates a set of rules that governmental entities generally must follow in order to compel disclosure of stored communications and other records.

Since its inception, the SCA has served multiple purposes. It provides rules governing how providers of communications services disclose stored information—including contents of communications, such as the body of an email, and non-content information—to a wide variety of government entities. In doing so, it imposes requirements on the government and providers to ensure that the privacy of individuals is protected. The statute thus seeks to ensure public safety and other law enforcement imperatives, while at the same time ensuring individual privacy. It is important that efforts to amend the SCA remain focused on maintaining both of these goals.

I. The Stored Communications Act Plays an Important Role in Government Investigations

Any consideration of the SCA must begin with an understanding of the statute's extremely broad scope. The paradigm that generally comes to mind in discussions of the SCA is a law enforcement agency conducting a criminal investigation and seeking a target's email from a service provider that makes its services available to the public. And, indeed, the SCA is critical to all sorts of criminal investigations into murder, kidnapping, organized crime, sexual abuse or exploitation of children, financial fraud, and more. As technology has advanced, electronic communications and electronic data storage have augmented traditional means of communicating and storing information. Appropriate governmental access to electronic communications and stored data, including both content and non-content information, has thus become even more important to upholding our law enforcement and national security responsibilities.

Even within these criminal investigations, it is important to understand the kind of information that the government obtains under the SCA as well as how that information is used. Under the SCA, the government may use legal process to compel service providers to produce both content and non-content information related to electronic communications. It is clear that the contents of a communication—for example, a text message related to a drug deal, an email used in a fraud scheme, or an image of child pornography—can be important evidence in a criminal case. But non-content information can also be essential to building a case.

Generally speaking, service providers use non-content information related to a communication to establish a communications channel, route a communication to its intended destination, or bill customers or subscribers for communications services. Non-content information about a communication may include, for example, information about the identity of the parties to the communication, and the time and duration of the communication. During the early stages of an investigation, it is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity. Importantly, non-content information gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant. Without a mechanism to obtain non-content information, it may be impossible for an investigation to develop and reach a stage where agents have the evidence necessary to obtain a warrant.

For example, the SCA has been critical to tracking down violent criminals. In one case, law enforcement obtained graphic photographs of a man sexually abusing his prepubescent son. Because of the offender's careful protection of his true identity, including the use of an anonymous online network, investigators needed to engage in a number of steps to ascertain the offender's location. Using information obtained from undercover chat sessions, officers identified a "proxy computer" – an intermediate computer used to obscure the offender's communication. Law enforcement obtained computer routing information from the proxy computer, and from that routing information, identified an IP address from which the offender's Internet traffic appeared to originate. After taking additional steps to confirm that the IP address

was associated with the unlawful conduct, pursuant to ECPA agents served a subpoena on the offender's Internet service provider to obtain his physical address, leading to the eventual arrest of three individuals involved in the offense and the rescue of a minor victim from extreme, ongoing abuse.

Similarly, agents used evidence gathered using a process under ECPA in the investigation of the Boston Marathon bombing. Subpoenas to phone companies provided subscriber information and call detail records, which were critical during the investigation to help identify the bombers and their associates, and some of which were used at trial to show the communications between the bombers at critical times.

The SCA has broad effect in other ways as well. The statute applies not only to public and widely accessible service providers but also to non-public providers, such as companies or governments that provide email to their employees. Moreover, federal criminal investigations are only a subset of the circumstances in which the SCA applies. The statute applies to the federal government in civil contexts as well as to state and local governments when they seek to obtain content or non-content information from a service provider. This means that the statute also applies when the government is acting as a civil regulator—or even as an ordinary civil litigant. For instance, the SCA applies in all of the following circumstances that could arise, just within the Department of Justice:

- Civil Rights Enforcement: DOJ's Civil Rights Division brings a civil suit against a landlord who is sending racially harassing text messages to tenants. The target of the messages deletes them, and the landlord denies ownership of the account from which they were sent. The SCA governs the Division's ability to obtain those messages from the provider during civil discovery.

- False Claims Act: The DOJ Civil Division investigates a business for submitting false claims to the Federal government. The Division has reason to believe that the defendant's employees used email messages sent via the business's customer service email accounts to orchestrate the fraud. However, the defendant claims that it did not use email for business purposes. The SCA governs the ability of the Division to compel the Internet service provider that hosted the company's website to disclose the contents of the business's email account.

- Environmental Litigation: The Department's Environment and Natural Resources Division brings a civil enforcement suit under the Superfund statute, a company relevant to the litigation has gone bankrupt, and the company's cloud provider has the only copies of that company's relevant corporate email. The SCA governs the Division's ability to obtain that email during civil discovery.

- Antitrust Investigations: The Department's Antitrust Division is conducting a civil investigation of several companies for engaging in an unlawful agreement to restrain

trade. During the course of the investigation, DOJ attorneys discover that executives of those companies are using their personal email accounts to continue communications about the agreement. The SCA governs the Division's ability to obtain that email from the service provider.

- Tax Enforcement: The DOJ Tax Division investigates a tax preparation service that advertises via social networking sites. The company fraudulently inflates the amount of refunds due to the taxpayer and profits from taking a significant share of the fraudulent refund. Based on complaints about the preparer, the social networking site closes the company's account. The SCA governs the Tax Division's ability to obtain the posts advertising the company's tax preparation services.

During any discussions of possible changes to the SCA and ECPA more broadly, it is important to keep in mind its wide-ranging application and scope.

II. Modernizing the Rules for Compelled Disclosure of Email and Other Similar Stored Content Information

As mentioned above, ECPA was originally enacted in 1986—a time when the Internet was still a nascent technology and landline telephones predominated. Although ECPA has been updated several times since its enactment, the statute—and specifically the portion of the SCA addressing law enforcement's ability to use legal process to compel disclosure of the stored contents of communications from a service provider—has been criticized for making outdated distinctions and failing to keep up with changes in technology and the way people use it today.

Many have noted—and we agree—that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.

Acknowledging that the so-called "180-day rule" and other distinctions in the SCA no longer make sense is an important first step. The harder question is how to update those outdated rules and the statute in light of new and changing technologies while maintaining protections for privacy and adequately providing for public safety and other law enforcement imperatives.

Personal privacy is critically important to all Americans—including those of us who serve in the government. It is also of increasing importance to individuals around the world, many of whom use communications services provided by U.S. companies. All of us use email and other technologies to share personal and private information, and we want it to be protected appropriately. We also know that companies in the United States and elsewhere depend on privacy as a driver of innovation and competitiveness. Some have suggested that the best way to enhance privacy under the SCA would be to require law enforcement to obtain a warrant based on

probable cause to compel disclosure of stored email and similar stored content information from a service provider. We appreciate the appeal of this approach and believe that it has considerable merit, provided that Congress consider contingencies for certain, limited functions for which this may pose a problem.

In the past several years, we have worked to help facilitate a better understanding of how the warrant requirement affects the Department of Justice's ability to enforce the law. And the Department appreciates, for example, that most recent proposals (*i.e.*, the "ECPA Amendments Act" (S. 356)), would not impose a warrant requirement in investigations involving corporate email. This type of provision would help preserve the manner in which corporate investigations have historically been conducted. Corporations often act as "electronic communications service providers" under the SCA when they provide email and Internet service to their employees. It would be anomalous, however, for the SCA to afford greater protection to electronic corporate records than to the identical records in hard copy, and such a rule could be abused by organizations and individuals seeking to avoid accountability for violating the law. Retaining the current use of subpoenas in that context therefore makes sense.

The Department remains concerned, however, about the effect a blanket warrant requirement would have on its civil operations. Civil regulators and litigators do extremely important work. But they typically are investigating conduct that, while unlawful, is not a crime. Criminal search warrants are only available if an investigator can show probable cause that a crime has occurred. Lacking warrant authority, civil investigators enforcing civil rights, environmental, antitrust, and a host of other laws would be left unable to obtain stored communications content from providers. As information is increasingly stored electronically, and as wrongdoers take new steps to shield that information from civil investigators, the amount of critical information off-limits to government regulators and litigators will only increase. It is also not the case that these civil regulators and litigators can ask criminal law enforcement officers to obtain a warrant on their behalf, because such warrants can only be obtained in furtherance of a criminal investigation—a step that would be impermissible unless the underlying conduct appeared to be criminal in nature.

Nor could civil litigators and regulators reliably obtain email and other content information solely by serving a subpoena directly on a subscriber (rather than a provider). As several of the examples described above demonstrate, serving a subpoena on a provider may be the only way for civil law enforcement to obtain certain stored communications. For example, where the subscriber no longer exists—as in the case of a bankrupt corporation or a deceased individual—or a purported subscriber denies ownership of the communications and therefore refuses to comply with a subpoena, civil litigators and investigators without the ability to obtain relevant evidence from a provider would be unable to obtain that evidence. Moreover, many individuals who violate the law may be tempted to destroy their communications rather than turn them over. Having the ability to seek records only from the individual, rather than the provider, could serve to encourage such illegal obstruction of justice. Thus, it is important that any proposed changes to ECPA take into account the ability of civil regulators and litigators to ask a court to compel disclosure of information from providers.

The Department also has several more technical, yet important, concerns that we believe merit consideration, including ensuring that the definition of "remote computing service" is appropriately scoped.

Finally, given the increasing prevalence of electronic communications, critical investigations involving widespread or complex crimes – such as those involving terrorism, transnational crime, financial fraud, or child exploitation – can last years and involve hundreds of search warrants, court orders, and subpoenas issued pursuant to ECPA to a variety of providers. ECPA reform proposals should account for investigations of this type and avoid enacting new obstacles to investigations that are already among the most challenging and important ones that law enforcement undertakes.

Efforts to update ECPA can reflect these considerations and, at the same time, incorporate strong mechanisms that protect individual privacy and ensure appropriate judicial oversight of government access to individual's communications.

III. The Need for Additional Updates to the SCA and ECPA

Although discussions about updating ECPA have often focused on the standard for governmental access to stored content information, we also believe there are a number of other parts of the statute that merit further examination during any process of updating and clarifying the statute.

(A) Clarifying Exceptions to the Pen Register Statute

First, Congress could consider clarifying the exceptions to the Pen Register statute. The Pen Register statute governs the real-time collection of non-content "dialing, routing, addressing, or signaling information" associated with wire or electronic communications. This information includes phone numbers dialed as well as the "to" and "from" fields of email. In general, the statute requires a court order authorizing such collection on a prospective basis, unless the collection falls within a statutory exception. The exceptions to the Pen Register statute, however, are actually less extensive than the exceptions to the Wiretap Act. This makes little sense—if the government is authorized to intercept communications in real-time, it is reasonable that the government should also be permitted to acquire the accompanying non-content information. Congress could harmonize the exceptions in these two sections of the statute by amending the Pen Register Act to bring it into line with the Wiretap Act. Moreover, the Pen Register Act's consent provision may be read so that a user can only consent to the use of a pen/trap device by the provider as opposed to by the government or the user herself. The Pen Register Act's consent provision could be clarified to allow the user to provide direct consent for implementation of a pen/trap device by the government.

(B) Clarifying the Standard for Issuing 2703(d) Orders

Second, Congress could consider clarifying the standard for the issuance of a court order under § 2703(d) of the SCA, which can be used by criminal law enforcement authorities to compel disclosure of various types of stored records. According to that provision of the statute, "[a] court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the [records] sought are relevant and material to an ongoing criminal investigation."

The Fifth Circuit has interpreted this provision to require a court to issue a 2703(d) order when the government makes the "specific and articulable facts" showing specified by § 2703(d). *See In re Application of the United States*, 724 F.3d 600 (5th Cir. 2013). However, the Third Circuit has held that because the statute says that a § 2703(d) order "may" be issued if the government makes the necessary showing, judges may choose not to sign an application even if it provides the statutory showing. *See In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit's approach makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not.

(C) Making the Standard for Non-content Records Technology-Neutral

Third, Congress could consider modernizing the SCA so that the government can use the same legal process to compel disclosure of addressing information associated with modern communications, such as email addresses, as the government already uses to compel disclosure of telephone addressing information. Historically, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA endorsed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Therefore, while law enforcement can obtain records of calls made to and from a particular phone using a subpoena, the same officer can only obtain "to" and "from" addressing information associated with email using a court order or a warrant, both of which are only available in criminal investigations. This results in a different level of protection for the same kind of information (*e.g.*, addressing information) depending on the particular technology (*e.g.*, telephone or email) associated with it.

Addressing information associated with email is increasingly important to criminal and national security investigations. Congress could consider updating the SCA to set the same standard for addressing information related to newer technologies as that which applies in traditional telephony.

(D) Clarifying that Subscribers May Consent to Law Enforcement Access to Communications Content

Fourth, Congress could consider clarifying the consent provision of the SCA. Under section 2702, a provider *may* disclose the contents of communications with the consent of a user or customer, but the provider is not required to do so. This has the impact of allowing the provider to overrule its customer's direction to disclose content associated with the customer's account. Thus when the victim of a crime seeks to share his or her own emails or other messages that may provide evidence, providers can refuse to disclose that information to law enforcement, even when provided with a written release from the account owner or subscriber.

(E) Appellate Jurisdiction for Ex Parte Orders in Criminal Investigations

Fifth, Congress could consider clarifying that higher courts have appellate jurisdiction over denials of warrants or other ex parte court orders in criminal investigations. Under existing law, the government may have no mechanism to obtain review of the denial of a court order or search warrant, even when the denial is based primarily on questions of law rather than questions of fact. Congress may wish to consider clarifying that these denials are appealable so that the disagreements among courts are resolved and the law becomes standardized.

IV. Obtaining Stored Information Abroad

Some discussion concerning ECPA has focused on changing the standards and protocols for law enforcement access to content that a provider has chosen for its own business reasons to store outside the United States. The Administration is studying these legislative proposals, but the Department has significant concerns about aspects of these proposals.

* * *

In conclusion, we would like to reemphasize that in discussing any efforts to modernize ECPA, it is important to take into account the statute's broad application. As technology continues to advance, ECPA's importance to both criminal and civil law enforcement will only increase.

The Department of Justice stands ready to work with the Committee as it considers potential changes to ECPA. We look forward to continuing to work with you on this issue.

Federal Bureau of Investigation
Agents Association

November 24, 2015

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 thoughts regarding H.R. 699, the *Email Privacy Act*. The FBIAA has a number of concerns about H.R. 699, and believes that legislative efforts to reform ECPA must address these concerns directly, before any ECPA reform legislation should be enacted.

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.

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

Post Office Box 12650 • Arlington, Virginia 22219
A Non-Governmental Association
(703) 247-2173 Fax (703) 247-2175

1. **H.R. 699 should ensure that law enforcement is able to access electronic evidence.**

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. Unfortunately, we have already begun to see the risks posed by this new technology. In the wake of the recent attacks in Paris, FBI Director Comey recently explained that, "[t]he threat posed to us by the group called ISIL, the so-called Islamic State, which, in the United States we talk about what they've been doing here, the recruiting through social media, if they find a live one, they move them to Twitter direct messaging. Which we can get access to through judicial process…But if they find someone they think may kill on their behalf, or might come and kill in the caliphate, they move to a mobile messaging app that's end-to-end encrypted."

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.

Warrant Exceptions

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. Accordingly, the FBIAA believes that ECPA reform legislation 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.

Service Provider Cooperation

H.R. 699 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.

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.

2. **H.R. 699 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 Congress, the FBIAA is concerned that target notification requirements that have been included in H.R. 699 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 H.R. 699. 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

Post Office Box 12650 • Arlington, Virginia 22219
A Non-Governmental Association
(703) 247-2173 Fax (703) 247-2175

NATIONAL ASSOCIATION OF POLICE ORGANIZATIONS, INC.

Representing America's Finest

317 South Patrick Street. ~ Alexandria, Virginia ~ 22314-3501
(703) 549-0775 ~ (800) 322-NAPO ~ Fax: (703) 684-0515
www.napo.org ~ Email: info@napo.org

November 30, 2015

The Honorable Robert W. Goodlatte
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

The Honorable John Conyers
Ranking Member
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Goodlatte and Ranking Member Conyers:

On behalf of the National Association of Police Organizations (NAPO), I am writing to you to express our deep concerns regarding the Email Privacy Act (H.R. 699).

NAPO is a coalition of police unions and associations from across the United States that serves to advance the interests of America's law enforcement through legislative and legal advocacy, political action, and education. Founded in 1978, NAPO now represents more than 1,000 police units and associations, 241,000 sworn law enforcement officers, and more than 100,000 citizens who share a common dedication to fair and effective crime control and law enforcement.

We are very concerned that the warrant requirements included in the Email Privacy Act would negatively impact public safety. This legislation does not account for immediate law enforcement needs, when seconds matter. Warrants take much longer to secure as compared with the current practice of officers obtaining a court order. This is of particular concern in time-critical cases, such as active kidnapping or child abduction cases.

Moreover, warrants require an affidavit, which generally becomes public. These documents have the potential to expose law enforcement and informant identities and methods. This is especially concerning in the light of the increased number of attacks on police officers across the country.

The warrant requirement included in H.R. 699 would present a huge obstacle to legitimate law enforcement needs. Additionally, NAPO does not feel that a "one size fits all" approach is appropriate for these matters, especially when there are effective law enforcement policies and procedures already in place at the state and local level.

We urge you to take our concerns into consideration. If you would like to discuss this bill further, please feel free to contact me at: (703) 549-0775.

Sincerely,

William J. Johnson
Executive Director

Cc: Members, Committee on the Judiciary, U.S. House of Representatives

November 24, 2015

The Honorable Bob Goodlatte
Chairman
House Judiciary Committee
2309 Rayburn House Office Building
Washington, DC 20515

The Honorable John Conyers
Ranking Member
House Judiciary Committee
2426 Rayburn House Office Building
Washington, DC 20515

RE: HR 699 – Updating the Electronic Communications Privacy Act (ECPA) and Reducing the Effects of Non-Technical Barriers on Lawful Access of Electronic Evidence

Dear Chairman Goodlatte and Ranking Member Conyers:

We, the undersigned organizations representing federal, state and local prosecutors, chiefs, sheriffs, and rank and file officers, understand the intent of HR 699 - the "Email Privacy Act" - 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, it is imperative that we ensure that law enforcement, with appropriate judicial supervision and approval, maintain its ability to access and recover digital evidence in order to protect the public and successfully prosecute those guilty of crimes.

Therefore, we ask that any legislation relating to this issue also address the very real challenges that law enforcement faces as it attempts to gather electronic evidence. 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. 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 maintain 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.

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 (APA)
Association of State Criminal Investigative Agencies (ASCIA)
Federal Law Enforcement Officers Association (FLEOA)
Fraternal Order of Police (FOP)
International Association of Chiefs of Police (IACP)
Major Cities Chiefs Association (MCCA)
Major County Sheriffs' Association (MCSA)
National Association of Assistant United States Attorneys (NAAUSA)
National Association of Police Organizations (NAPO)
National District Attorneys Association (NDAA)
National Fusion Center Association (NFCA)
National Narcotic Officers' Associations' Coalition (NNOAC)
National Sheriffs' Association (NSA)

cc: House Judiciary Committee
Senate Judiciary Committee

Virginia Association of Commonwealth's Attorneys

July 10, 2015

The Honorable Robert Goodlatte
United States House of Representatives
2309 Rayburn House Office Building
Washington, D.C. 20515-4606

RE: House Resolution 699: Email Privacy Act

Dear Chairman Goodlatte:

We, the Virginia Association of Commonwealth's Attorneys (VACA), are writing to express our deep concerns about certain provisions of HR 699, the Email Privacy Act. This act, while making some important improvements to the Electronic Communications Privacy Act (ECPA), also imposes enormous, unworkable, and dangerous burdens on law enforcement to provide unprecedented disclosures to criminal suspects regarding ongoing investigations of crimes such as child pornography, gang violence, identity theft, and terrorism. We are particularly concerned with the notification requirements imposed by HR 699.

VACA was founded in 1939 to be the "Voice of Virginia's Prosecutors." For 75 years, our association has worked diligently to represent our communities in the criminal courtrooms and in government. Our members are prosecutors from the 120 independently elected Commonwealth's Attorneys that represent the people of the Commonwealth in the criminal justice system.

HR 699 addresses evolving issues in the 21st century. Before Congress enacted the ECPA, the United States Supreme Court had held that the Fourth Amendment to the Constitution does not govern the information held by 3rd parties, such as Google and Facebook, since by sharing that information with these "3rd parties," citizens lose any reasonable expectation of privacy in that same information. In response, in

Nancy G. Parr
307 Albemarle Drive, Suite 200A
Chesapeake, VA, 23322

General Correspondence:
P.O. Box 3549
Williamsburg, Virginia, 23187-3549

1986 Congress enacted the (ECPA) and created statutory protections for certain communications, requiring government entities to obtain legal process electronic data stored by 3rd parties.

Because of ECPA, (and more specifically within ECPA, the Stored Communications Act or "SCA") most police and prosecutors seeking content information from 3rd party service providers rely on one tool: the Search Warrant. Under the Constitution, the search warrant issues only upon a showing of probable cause to a neutral and detached judicial officer. This considerable legal filter benefits the government and the public, by guaranteeing the integrity of the legal process before delivery of an individual's electronic records to the government.

While much has changed since 1986, the emerging digital world is more hostile and impenetrable to law enforcement than ever, making congressional intervention, if done only for the sake of individual privacy, equally unbalanced. HR 699's lopsided response to these changes is to grant more statutory privacy rights to an individual with an internet account than to a person has in his own home. At the same time, law enforcement gets nothing from HR 699 to help it battle serious crime or meet the challenges of these new technologies.

To put this into perspective, consider the implications of HR 699's delayed notification requirement during a grand jury investigation of a series of gang-related homicides. During the course of the investigation, law enforcement officers obtain a search warrant for the contents of a social media account used to send out gang videos and pictures. Law Enforcement only has an internet address and does not know to whom the address actually belongs. The only known information is that, from the account, gang members send messages to fellow gang members about where to meet, what rival gangs are current targets, who in their own gang is a target because of that member's work with law enforcement, and so on.

It is crucial to recognize that HR 699, the "Email Privacy Act," actually protects a great deal more than email; it protects photos and videos, including photos of minor children being sexually assaulted, internet chat solicitations by international terrorists and child molesters, stolen computer data, such as credit card numbers, social security numbers, and the like, and any data of any kind stored in remote digital storage. In other words, this act in fact protects the very objects that criminals themselves want to protect from the eyes of law enforcement and the public.

Once a Judge reviews the affidavit in support of the search warrant and finds probable cause, HR 699 allows law enforcement to delay notification to the "subscriber" operating the social media account – but only for a limited time. After that delay expires, law enforcement has to provide the search warrant to the subscriber[1], even though law enforcement may still have no idea who it is. In addition, law enforcement must now also provide the subscriber with the nature of the law enforcement inquiry with reasonable specificity[2], resulting in the mandatory disclosure of investigative details unheard of in any other context while simultaneously causing a likely violation of the grand jury secrecy laws that forbid law enforcement from sharing the details of an ongoing grand jury proceeding. It is no choice at all if it depends upon choosing between violating state law (or a judicial deal order) or federal law.

---

[1] In Virginia, providing a copy of the search warrant includes the affidavit of supporting facts.

[2] Presumably this requirement is not met by the affidavit to the search warrant, since it is a separate obligation under HR 699.

What's more, the "target" (in this case the subscriber) of the investigation may be a gang or terrorist member in another country, orchestrating his or her gang's or criminal enterprise's operation from foreign soil. To what extent would local law enforcement be beholden to such terrorist and organized crime leaders due to the notification requirement? Or to any other foreign national? It is a laudable goal to create greater transparency in government, but it seems oxymoronic to command the protection of a foreign national's non-existent Fourth Amendment rights outside our country, or to deliver sensitive information to those who seek our destruction or the injury of our citizens. A fair balance between the rights and interests of our citizens and the legitimate security concerns of both national and local law enforcement can be achieved, but not with this unbalanced bill.

HR699 also establishes a brand-new, unprecedented time limit on all law enforcement investigations. Once law enforcement obtains a search warrant and seeks delayed notification under HR699, law enforcement may obtain only one 180-day extension for non-disclosure. Even though investigations into cross-border identity theft, cybercrime, and child pornography rings often take more than a year to complete, as soon as law enforcement obtains a search warrant, the clock begins to count down to the date when they will be required to disclose the details of the investigation to the criminals being investigated. Law enforcement could delay their search warrant, but unfortunately HR699 offers no requirement that electronic service providers preserve data for any amount of time.

As criminal prosecutors, we can only speak to our own experience in bringing murderers, child pornographers, violent criminal street gangs, stalkers, identity thieves, computer hackers, drug dealers, and other offenders to justice. However, HR699 appears to deprive our counterparts in civil enforcement of the ability to request judicial authority to obtain the contents of data in remote storage. Investigators of securities fraud, Medicare and Medicaid fraud, environmental offenses, and other civil agencies would be denied an important tool in their investigations.

Many private internet service providers advocate for the kind of disclosure required by HR 699. However, these same internet service providers and their many affiliates routinely sell their subscribers' information, content and all, for profit. (See Google[3], Facebook[4], and many other, terms of service). While certainly not an excuse for unwarranted governmental intrusion, this fact does raise the question of why law enforcement has been girded with these demanding conditions to obtain the same information that private industry shares openly without any restriction.

---

[3] Google Docs [Terms of Service]: When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services.

[4] Facebook Terms of Service: We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. [W]e use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission

The Virginia Association of Commonwealth's Attorneys is asking that more time be invested in finding practical solutions. We believe a more meaningful review of the impact of this legislation on all interested parties will reveal the full breadth of this proposal while highlighting the unintended consequences of hasty lawmaking. The Virginia Association of Commonwealth's Attorneys stands ready to assist Congress as it crafts measured legislation that is at once protective of our citizenry and sensible to the needs of law enforcement to combat crime in our digital society.

Sincerely,

Michael R. Doucette
Commonwealth's Attorney
City of Lynchburg
Chair, VACA Legislative Committee

November 30, 2015

The Honorable Bob Goodlatte
Chairman, House Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

The Honorable John Conyers, Jr.
Ranking Member, House Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

RE: Support for Reform of the Electronic Communications Privacy Act (ECPA)

Dear Chairman Goodlatte and Ranking Member Conyers:

On behalf of the undersigned technology associations across the United States, we are writing to urge Congress to pass legislation to reform ECPA by requiring a warrant for government entities to gain access to all emails, text messages, and other electronic communications. H.R. 699 – The Email Privacy Act, introduced by Congressmen Kevin Yoder (R-KS) and Jared Polis (D-CO), currently has overwhelming bipartisan support with 304 co-sponsors, the highest total of any bill in the House not to earn a floor vote.

ECPA was originally passed in 1986, when email was still a nascent technology, and deemed all electronic communications over 180 days old to be "abandoned." Technology has changed significantly over the last 29 years, however, necessitating reform.

Under ECPA today, law enforcement and government agencies can acquire "abandoned" communications in electronic storage from an email or cloud computing provider without a warrant, simply needing a subpoena (and a lower burden of proof) to obtain access. This presents a significant problem for both users of email and cloud services *and* the service providers themselves, who want to protect the privacy of their users.

The Sixth Circuit Court of Appeals ruled in a 2010 case that, under the 4th Amendment, law enforcement must use a warrant to acquire this content from providers, but it hasn't stopped them from trying to get it through subpoenas. At this point, most large providers treat the Sixth Circuit decision as the law of the land, but smaller providers may not have the knowledge or resources to know how to comply. Further, given that this decision is only law in one of eleven judicial circuits, a conflicting decision from another circuit court could upend the law.

Support for some sort of ECPA reform is bordering on unanimous, but there is still some debate about how to proceed. Two potential problematic amendments to the bills have emerged. The first is an exception for civil agencies (led primarily by the SEC), which do not have the ability to issue warrants. Such an exception would destroy the privacy benefits of ECPA reform by codifying new ways for civil agencies to obtain private information. Civil agencies can still access content through other channels, namely by serving subpoenas on users, not service providers. The SEC even testified in April that it does not currently serve subpoenas on service providers to obtain emails in its investigations.

The other potential amendment stems from a request from law enforcement to codify an emergency exception. Under ECPA today, a government entity may request content from providers without a warrant by declaring an emergency. Providers then determine, based on the circumstances, whether or not to comply. Law enforcement is now asking for a requirement for providers to comply any time the government declares an emergency. This has dangerous potential for abuse, especially when some companies are already complying with ~75% of emergency requests. Companies do not want to be responsible for derailing an investigation into a legitimate emergency, but requiring providers to comply with all "emergencies" could result in law enforcement declaring emergencies far more often than they should.

These potential amendments to the Email Privacy Act would severely weaken a much-needed change to an outdated law. ECPA reform is necessary to protect the privacy of Americans and to ensure that email users can trust their providers to protect that privacy. To ensure this is carried out properly, Congress should pass the Email Privacy Act as it is today, and not amend it in such a way that would weaken the privacy protections it would put in place.

Thank you for your time and attention to this vitally important matter.

Sincerely,

CompTIA
Technology Councils of North America

Arizona Technology Council (AZTC)
Austin Technology Council (ATC)
California Technology Council
Chesapeake Regional Tech Council (CRTC)
Colorado Technology Association
CONNECT

Connecticut Technology Council (CTC)
Idaho Tech Council (ITC)
Illinois Technology Association (ITA)
KCnext - The Technology Council of Greater Kansas City
Massachusetts Technology Leadership Council (MassTLC)
Metroplex Technology Business Council (MTBC)
Minnesota High Tech Association (MHTA)
Nashville Technology Council
New Hampshire High Tech Council (NHHTC)
New Jersey Tech Council (NJTC)
New York Technology Council (NYTECH)
North Carolina Technology Association (NCTA)
OCTANe
OHTech
Orange County Technology Alliance
Software San Diego
Tech Collective
Technology Association of Georgia (TAG)
Technology Association of Louisville Kentucky (TALK)
Technology Association of Oregon (TAO)
Utah Technology Council
Washington Technology Industry Association (WTIA)
Wisconsin Technology Council

Statement of

Grover G. Norquist
Americans for Tax Reform

House Committee on the Judiciary
Hearing on H.R. 699, the Email Privacy Act

December 1, 2015

Chairman Goodlatte, Ranking Member Conyers, and Members of the House Judiciary Committee, thank you for the opportunity to submit written testimony in favor of the Email Privacy Act, H.R. 699.

My name is Grover Norquist. I am the president of Americans for Tax Reform. Americans for Tax Reform advocates on behalf of taxpayers for a system in which taxes are simpler, flatter, more visible, and lower than they are today.

The Email Privacy Act will bring the law into line with the advances of technology by reforming the Electronic Communications Privacy Act (ECPA). ATR supports this legislation, and urges the committee to expedite a mark-up following the hearing, so the bill can receive a floor vote. We would like to add our voice of support to that of more than 300 Congressmen already co-sponsoring this legislation.

Technology changes. The Fourth Amendment does not.

Most Americans believe that our Fourth Amendment right "to be secure in [our] persons, houses, papers, and effects against unreasonable search and seizure" already applies to private communications sent or stored electronically, just as it applies to telephone calls or letters sent through the mail.

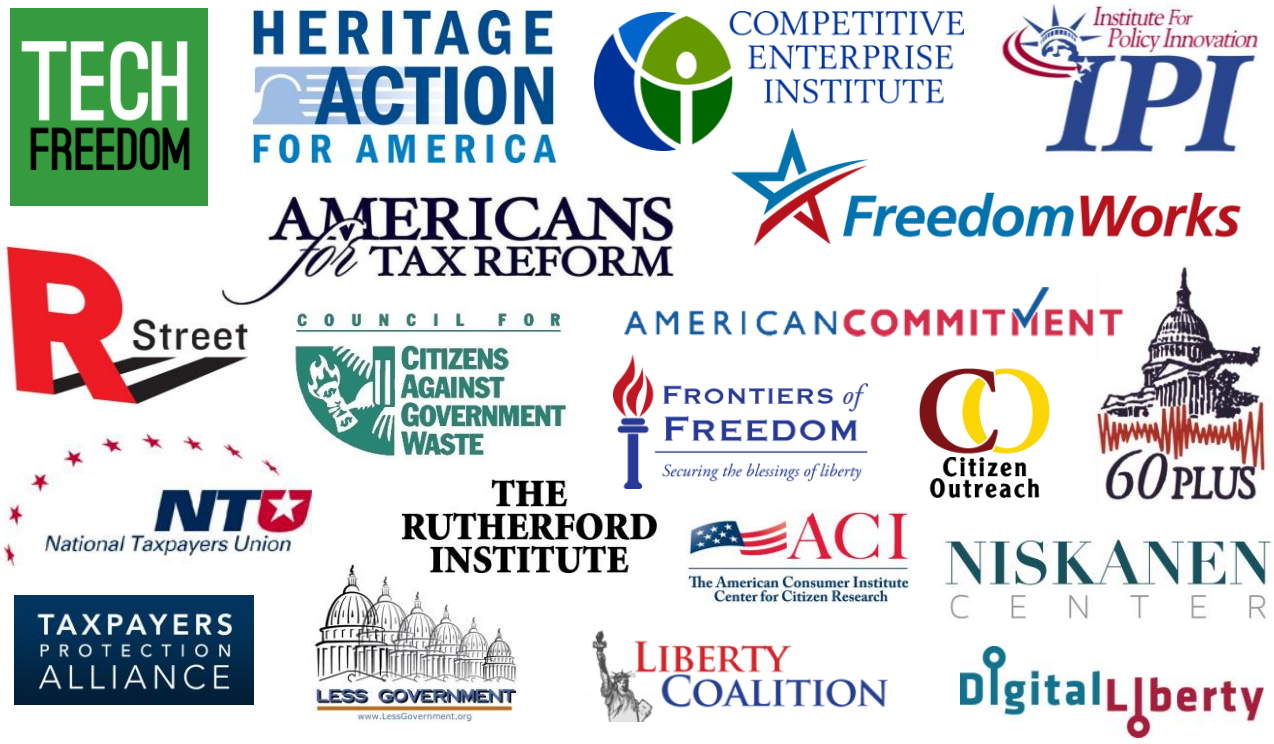
The principle behind ECPA reform is simple: if any government agency wants access to a person's emails or other private documents stored online, it should demonstrate to a judge that there is probable cause to believe the person is committing a crime, and the judge should issue a warrant.

The Fourth Amendment guarantees Americans protection against warrantless search and seizure. H.R. 699 outlines a simple procedure to ensure that email and cloud documents receive the same protection as paper documents stored in a local file cabinet. The warrant-for-content standard does not impede law enforcement. The U.S. Justice Department already follows this as a rule.

The IRS exceeded its own rules to harass people because of their political affiliation, and their training handbook explicitly said they did not need a warrant to go to a service provider for private documents or communications. As these policies came to light, the IRS quickly changed its policies.

Civil regulatory agencies continue to pursue expanded power. They want an exemption from ECPA reform that would allow them to obtain the content of customer documents and communications directly from a service provider. The Securities and Exchange Commission, and the Federal Trade Commission are the faces of the push, but an exemption would apply to all agencies: IRS, OSHA, CFPB, FCC, DOE, EPA, etc…

As civil agencies ask for a carve-out from this legislation, saying that their investigations should only require a subpoena, we urge Congress to assert its authority over these agencies. Neither side of the aisle can deny that agencies have expansively interpreted the definitions of their jurisdiction. Agency actions should be "more visible." The warrant requirement in the Email Privacy Act will enhance transparency and bring agency actions in line with the Fourth Amendment.



November 30, 2015

The Honorable Charles Grassley
Chairman, Committee on the Judiciary

The Honorable Bob Goodlatte
Chairman, Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary

United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

United States House of Representatives
2426 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Grassley, Chairman Goodlatte, Ranking Member Leahy, Ranking Member Conyers, and Members of the Committees:

We, the undersigned, write in support of a simple principle: that law enforcement must convince a judge to issue a warrant before obtaining emails and the contents of other private online communications. This principle, enshrined in the Fourth Amendment — and before that, in the June, 1776 Virginia Declaration of Rights — is the crown jewel of American civil liberties. Yet it is not given effect in the Electronic Communications Privacy Act (ECPA), the 1986 law that governs law enforcement access to digital communications.

For over five years, support has been growing in Congress to reform ECPA to protect Americans' privacy. The Email Privacy Act (H.R. 699), and its Senate counterpart, the ECPA Amendments Act (S. 356), would impose a consistent warrant requirement for stored content. The House bill has the support of 304 Representatives: a veto-proof majority. Such overwhelming support for significant legislation is extraordinary in Congress.

Yet efforts to update the woefully outdated ECPA have stalled due to the stubborn insistence from some regulators that they should be exempt from a warrant requirement. They want to be able to compel a third party that hosts an investigative target's content (e.g., a cloud email provider) to disclose it *without* a warrant based upon a showing of probable cause. This would allow a wide range of regulatory agencies — including the IRS, EPA, SEC, FTC and an endless number of state agencies — to obtain sensitive personal information unrelated to an investigation and protected by privilege since service providers are in no position to assess the relevance of the materials requested or assert privilege (as targets generally do). This could include, for example, personal emails sent on work email addresses. This burden would fall most heavily on the owners and employees of small businesses, who are far more likely to rely on cloud email services (while large companies often host their own email). It is difficult to imagine how Congressional Republicans could consider granting such new power to regulators, given the vast (and increasing) overreach of the regulatory state.

Regardless, there is no need for such a carve-out. Administrative agencies can already serve a subpoena, enforceable in court, and demand production of relevant materials. The courts have regularly compelled individuals and companies to disclose their data and imposed sanctions those who don't comply.

Instead of allowing regulatory agencies to compel email and other cloud service providers to produce private data without a warrant, Congress should codify the trend of courts confronted with such situations: that the *targets* of regulatory investigations themselves remain subject to administrative subpoenas — and if they refuse to comply, they will be subject to appropriate sanctions.[1] This, in turn, will encourage targets' compliance with legitimate requests.

In addition, some law enforcement agencies are calling for an "emergency situation" exception amendment to force service providers to disclose the contents of communications — again, without a warrant. Current law already permits a provider to disclose the contents of a communication or customer records when the provider has a "good faith" belief that disclosure is necessary to avoid the death or serious physical injury of any person.[2] Law enforcement requests the content of communications only sparingly, and providers already comply overwhelmingly.[3]

This exception was written at a time (1986) when courts were frequently unavailable. But today, Article III judges are available around the clock to issue warrants, if only by telephone. So there is no need to bypass the courts. Law enforcement simply has not shown that there

---

1. *See, e.g.*, Mintz v. Mark Bartelstein & Assocs., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) ("Defendants may request documents reflecting the content of Plaintiff's relevant text messages, consistent with the [Stored Communications Act], by serving a request for production of documents on Plaintiff pursuant to Rule 34. … Of course, Plaintiff may raise privacy or other objections to any Rule 34 document request … ."); O'Grady v. Superior Court (Apple Computer, Inc.), 44 Cal. Rptr. 3d 72, 88 (2006) ("Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions.").
2. 18 U.S.C. § 2702(b)(8), (c)(4).
3. In the second half of 2014, for instance, Google received 171 emergency data requests and produced data in 80% of those cases. These emergency requests made up about 1.7% of the total requests Google reported in its latest transparency report, which is available at http://www.google.com/transparencyreport/userdatarequests/US/. Verizon reported receiving 26,237 during the same period, the overwhelming majority of which were for user records and not message content.

is a problem that needs solving. Requiring disclosure in "emergency situations" will incentivize agencies to cry "wolf" in order to avoid judicial oversight.

We would oppose any amendments that would weaken the core privacy protections in this bill. But in particular, any amendment to circumvent the warrant requirement — whether by adding a carve-out for regulatory agencies or turning emergency requests into emergency orders — would likely be a poison pill for ECPA reform in general.

We urge you to finally move forward on bipartisan legislation to reform ECPA — *without these unnecessary and troubling exceptions to warrant protection for Americans' private digital content.*

Respectfully,

TechFreedom
60 Plus Association
American Commitment
American Consumer Institute
Americans for Tax Reform
Center for Financial Privacy and Human Rights
Citizen Outreach
Competitive Enterprise Institute
Council for Citizens Against Government Waste
Digital Liberty
FreedomWorks
Frontiers of Freedom
Heritage Action for America
Institute for Liberty
Institute for Policy Innovation
Less Government
Liberty Coalition
National Taxpayers Union
Niskanen Center
R Street
Taxpayers Protection Alliance
The Rutherford Institute

Bob Barr, Member of Congress, 1995–2003 (GA-7), and President, Liberty Guard*
Bartlett D. Cleland, Madery Bridge Consulting*
Hance Haney, Discovery Institute*
Julian Morris, Reason Foundation*

*Institutional affiliation listed for identification purposes only