Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google Inc.
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 Committee, thank you for the opportunity to appear before you this morning to discuss H.R. 699, the Email Privacy Act.

My name is Richard Salgado. As the Director for Law Enforcement and Information Security at Google, I oversee the company's response to government requests for user information under various authorities, including ECPA. I am also responsible for working with teams across Google to protect the security of our networks and user data. I have served as a Senior Counsel in the Computer Crime and Intellectual Property Section in the U.S. Department of Justice, and have taught and lectured on these issues at Georgetown University Law Center, George Mason University Law School, and Stanford Law School.

Google is a member of the Digital Due Process (DDP) Coalition, which supports updating ECPA. More than 100 organizations, trade associations, and corporations are DDP members. DDP members span the ideological spectrum, ranging from the American Civil Liberties Union (ACLU) and the the Center for Democracy & Technology (CDT) to Americans for Tax Reform (ATR) and FreedomWorks. The diverse array of organizations, trade associations, and corporations that comprise the Digital Due Process Coalition is a testament to the breadth of support for updating ECPA in the Internet era.

Google strongly supports H.R. 699, the Email Privacy Act, which is sponsored by Representatives Yoder (R-KS) and Polis (D-CO). H.R. 699 currently has 304 cosponsors, more than any other bill that is pending in Congress. It is undeniable that there is strong interest in aligning ECPA with the Fourth Amendment and users' reasonable expectations of privacy.

ECPA Reflects the Pre-Cloud Computing Landscape of the 1980s

ECPA was enacted in 1986, well before the web as we know it today even existed. The ways in which people use the Internet in 2015 are dramatically different than in 1986.

- In 1986, there was no generally available way to browse the World Wide Web, and commercial email had yet to be offered to the general public. Only 340,000 Americans

subscribed to cell phone service, and not one of them was able to send a text message, surf the web, or download applications. To the extent that email was used, users had to download messages from a remote server onto their personal computer. Holding and storing data was expensive, and storage devices were limited by technology and size.

- In 2015, hundreds of millions of Americans use the web every day, to work, learn, connect with friends and family, entertain themselves, and more. Data transfer rates are significantly faster than when ECPA became law, making it possible to share richer data, collaborate with many people, and perform more complicated tasks in a fraction of the time. Video sharing sites, video conferencing applications, search engines, and social networks, all the stuff of science fiction in 1986, are now commonplace. Many of these services are free. As a result of these technological advances, Americans are increasingly relying on third party service providers to store their online content, including videos, family photos, and confidential communications. The expectation is that such service providers can and will provide infinite storage indefinitely.

The distinctions that ECPA made in 1986 were foresighted in light of technology at the time. But in 2015, ECPA frustrates users' reasonable expectations of privacy. Users expect, as they should, that the documents they store online have the same Fourth Amendment protections as they do when the government wants to enter the home to seize documents stored in a desk drawer. There is no compelling policy or legal rationale for this dichotomy, but it is one that ECPA continues to make, despite widespread agreement that the statute should be updated.

ECPA Must Be Updated

Although the benefits of cloud computing have become more obvious and widespread, the outdated technology assumptions baked into parts of ECPA do not reflect the reasonable expectations of privacy of users. This is an unfortunate and unintended consequence of technological advancement, as Congress passed ECPA in 1986 in order to protect the privacy of users of electronic services in light of innovation. ECPA worked well for many years, and much of it remains vibrant and relevant. In significant places, however, a large gap has grown between the technological assumptions made in ECPA and the reality of how the Internet works today. This leaves us, in some circumstances, with complex and baffling rules that are both difficult to explain to users and difficult to apply.

One of the most complex and baffling set of rules is around compelled disclosure of communications content. ECPA provides that the government can compel a service provider to disclose the contents of an email that is older than 180 days with nothing more than a subpoena (and notice to the user, which can be delayed in most cases). If the email is 180 days old or newer

and unopened, the government will need a search warrant. In its testimony before the House Judiciary Committee in 2013, and again before the Senate Judiciary Committee in September, the Department of Justice (DOJ) acknowledged that there is "no principled basis to treat email less than 180 days old differently than email more than 180 days old." DOJ also recognized in its testimony that the statute should "not accord lesser protection to opened emails than it gives to emails that are unopened."

In 2010, the Sixth Circuit opined in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), that ECPA violates the Fourth Amendment to the extent that it does not require law enforcement to obtain a warrant for email content. In so doing, the Sixth Circuit effectively dispensed with ECPA's 180 day rule and the distinction between opened and unopened emails as irreconcilable with the protections afforded under the Fourth Amendment. Google believes the Sixth Circuit's interpretation in *Warshak* is correct, and we require a search warrant in all instances when law enforcement seeks to compel us to disclose the contents of Gmail accounts and other Google services. *Warshak* lays bare the constitutional infirmities with the statute and underscores the importance of updating ECPA to ensure that a warrant is uniformly required when governmental entities seek to compel third party service providers to produce the content of electronic communications.

Warshak is effectively the law of the land today. It is embraced by companies and observed by governmental entities. In many ways, then, H.R. 699 is a modest effort to codify the status quo and implement the Sixth Circuit's conclusion that the Fourth Amendment requires a warrant in all cases where the government seeks to compel a provider to disclose communications content from a company covered under ECPA. Notably, the bill explicitly carves out the acquisition of communications content pursuant to statutes such as the Wiretap Act and the Foreign Intelligence Surveillance Act. H.R. 699 will have no impact, therefore, on the government's efforts to combat terrorism under those authorities. Similarly, because *Warshak* is effectively the law of the land today, codifying a bright-line, warrant-for-content rule will not result in any substantive changes in how terrorism is investigated using ECPA authorities.

The inconsistent, confusing, and uncertain standards that currently exist under ECPA fail to preserve the reasonable privacy expectations of Americans today. Moreover, providers, judges, and law enforcement agencies alike have difficulty understanding and applying the law to today's technology and business practices. By creating inconsistent privacy protection for users of cloud services and inefficient and confusing compliance hurdles for service providers, ECPA has created an unnecessary disincentive to move to a more efficient, more productive method of computing.

The Supreme Court and Many State Legislatures Recognize the Importance of Affording the Highest Privacy Protections to Electronic Communications

Two important developments have occurred since I last testified before the House Judiciary Committee in support of updating ECPA in March 2013, both of which have a significant bearing on efforts to update ECPA.

First, the Supreme Court issued a landmark decision in *Riley v. California*, 134 S.Ct. 2473 (2014), where it unanimously held that officers must generally obtain a warrant before searching the contents of a cell phone incident to an arrest. Writing for the Court, Chief Justice Roberts rejected the government's invitation to create "various fallback options for permitting warrantless cell phone searches under certain circumstances," noting that a regime with various exceptions and carve-outs "contravenes our general preference to provide clear guidance to law enforcement through categorical rules." To reinforce the constitutional imperative for clear rules in this area, Chief Justice Roberts concluded his opinion with unambiguous direction to law enforcement:

> "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple - get a warrant."

Notably, this Committee is being asked by some today to jettison precisely the type of categorical rules that Justice Roberts sought to revitalize in *Riley*. But doing so would undermine users' reasonable expectations of privacy and encroach upon the core privacy protections afforded by the Fourth Amendment. We urge the Committee to reject such entreaties and to codify the bright-line, warrant-for-content standard that is reflected in H.R. 699.

Second, since the last ECPA hearing held by the House Judiciary Committee, many states have enacted bright line statutes to bring their state law in accord with the Fourth Amendment. Hawaii, Texas, and Maine have all done this. In addition, earlier this year, the California legislature overwhelmingly approved landmark legislation to update California's electronic privacy laws (colloquially referred to as "CalECPA"). Not only does CalECPA require the government to obtain a warrant before it can compel third party services providers to disclose users' communications content, but it also extends the warrant requirement to communications metadata, including location information, as well as data stored on electronic devices.

To be clear, H.R. 699 does not even go this far. It merely preserves and codifies the constitutionally required warrant-for-content standard that has been observed by law enforcement and providers alike for many years now. Even so, and despite overwhelming support in both the

House of Representatives and the Senate, some agencies are continuing to urge Congress to put the brakes on important and long overdue reforms.

Congress Should Reject Proposals That Weaken the Core Privacy Protections in H.R. 699

Civil Government Agency Issue

Some governmental entities have argued that the *Warshak* rule hampers their ability to investigate and enforce civil violations because civil agencies do not have warrant authority and thus lack the ability to obtain content from providers. These governmental entities have proposed amending ECPA so that agencies can ultimately bypass the target of, or even potential witnesses in, civil investigations and issue legal process (on something less than a warrant) to third party service providers covered by ECPA.

It makes little sense, however, to enact a bright-line, warrant-for-content standard while simultaneously creating a new carve-out that would eviscerate that bright-line rule. Congress should eschew proposals that would create a civil agency carve-out for the following reasons.

First and foremost, a civil agency carve-out would contravene *Warshak* and the Fourth Amendment principles that animated the Sixth Circuit's conclusion in that case. Civil government agencies are still government agencies. The power to compel providers to disclose the content of users' communications should be reserved for criminal cases. Congress should be deeply skeptical of efforts to draft around the Fourth Amendment, which is what some governmental entities are asking it to do.

Second, civil agencies have long done their job without such an exception. They can and do directly subpoena the targets of or witnesses in civil investigations to obtain relevant evidence, including emails and other content the targets or witnesses have stored with providers. This is, of course, how civil litigation routinely works; a discovery request is served on a party or witness and the party or witness is expected to produce responsive material in her possession, custody, or control. There is no reason to radically alter our civil litigation system simply because of the advent of cloud computing, which enables litigants to theoretically obtain the same data from service providers like Google. Electronic communication and remote computing service providers are not, nor should they be, discovery agents for governmental entities that are conducting civil litigation.

Third, if targets and witnesses of civil investigations are intransigent or uncooperative, governmental entities have a broad array of tools to compel compliance. Civil agencies can always enforce subpoenas when a person fails to produce responsive documents. If a target or witness subsequently fails to produce responsive material pursuant to a court order to do so, the judge may

impose sanctions, which could include the denial of counter-claims, adverse inferences as a result of the target's intransigence, fines, default judgments, and even jail time.

Fourth, there is no heightened risk of spoliation or destruction of evidence by requiring civil agencies to subpoena the targets of their investigations. To the extent that civil agencies are concerned about spoliation or destruction of evidence, those concerns are exogenous to ECPA reform. If civil agencies believe that targets and witnesses of investigations, or adversaries in litigation altogether, can't be trusted to produce responsive material, that is a problem neither unique to ECPA, nor addressable by compromising the constitutional requirement for clear rules about government access to user communications.

Fifth, civil discovery often brings with it complex and difficult disclosure issues around relevance, attorney-client privilege and other privileges, trade secrets, confidential business information and the like. If served with civil process to disclose a user's content, a provider will be ill suited to raise these objections or assert privileges; that is something the user should do as part of responding to record requests directed to the user. Congress should eschew any legislative change that would put service providers in the untenable position of making these types of critical judgment calls, which have enormous implications for privacy and due process. The risks of a provider turning over privileged or otherwise protected material increases significantly with the volume of material that is sought by a civil agency. If a civil agency seeks three years' worth of email, it is likely, if not a foregone conclusion, that irrelevant and privileged material about a user will be produced.

Sixth, it is important to remember that civil agencies, even pre-*Warshak,* have operated under ECPA, and have never been able to compel production of all content. Despite this, civil agencies prosecute offenses and undertake enforcement actions against violators with regularity. In its 2014 annual report, the SEC notes that it brought a "record number of cutting edge enforcement actions." In that same report, the SEC said that it brought "more cases than ever before", including "a number of first-ever cases that span the securities industry." It did so, as Chairman White testified earlier this year, without issuing subpoenas for content from providers under ECPA.

Seventh, the proposition that civil regulatory agencies should be conferred with powers similar to criminal authorities to intrude into private communications would, if adopted, have serious implications for the privacy interests of users and the broader judicial administration of the statute, with no demonstrated need. In recent testimony before the Senate Judiciary Committee, the Securities and Exchange Commission (SEC) alluded vaguely to a potential statutory expansion of powers whereby civil agencies could compel providers to disclose communications content through some novel and undefined legal process.

The SEC's notion, which it only outlines in the broadest parameters, leaves many questions unanswered. For example, under what standard would the SEC be able to compel third party service providers to disclose the content of users' electronic communications? And how would such a standard comport with the Fourth Amendment, given the significant nature of the intrusion and the lower evidentiary standards and burden(s) of proof in civil cases? Moreover, would the ability to obtain electronic communications content under this new standard exist just for the SEC, or would it apply to any "governmental entity" under ECPA, which by definition includes thousands of state and local governmental entities, as well as other federal governmental entities? In determining which governmental entities are empowered with this new authority, should Congress make value judgments about the worthiness of the missions served by each of these governmental entities? It also raises the question of why, if the agency is able to give notice to the user and give the user an opportunity to respond, as the concept sets out, the agency can't just serve legal process on the user like every other litigant, as is done for other evidence in the possession of witnesses and defendants. The notion raises the specter of providers, large and small, conscripted into serving as civil discovery vendors, unnecessarily placed in the middle of messy and protracted litigation of others. It could also offer the government an irresistible path to circumvent the warrant requirement by using this new civil power for a case that will ultimately turn into a criminal matter.

Finally, although some civil agencies have raised hypothetical concerns that a bright line, warrant-for-content rule would frustrate their investigations, there is no evidence that civil agencies typically encounter such scenarios or that, even if they do, the investigations are hindered. In an April 2013 letter to Senator Leahy, the SEC cited a single example where it ostensibly could not have brought a case but for the ability to serve a subpoena directly on a provider to obtain email content about the target. After examining the record in that case, however, the Center for Democracy and Technology found that it "actually shows that the need for new authority is greatly overstated, if not totally unjustified," and that it "illustrates precisely the risk of indiscriminate production of personal emails that we have warned about."

Emergency Exception

Under current law, service providers *may* disclose the contents of communications or customer records to a governmental entity in an emergency involving danger of death or serious physical injury to any person. Some law enforcement agencies, however, propose *requiring* service providers to disclose the contents of communications and customer information whenever any federal, state, or local governmental entity believes there is an emergency under ECPA.

In November 2013, Google began including information about emergency requests in its bi-annual transparency report covering government demands for user data. Other service providers, including Facebook, Microsoft, and Yahoo, also now include information about emergency requests

in their transparency reports.

This data helps shed light on the volume of emergency requests that service providers receive, which is very low in comparison to the total number of compulsory legal demands that service providers receive under ECPA. In the second half of 2014, for example, Google received 171 emergency requests affecting 272 user accounts in the U.S. That figure represents less than 2% of all compulsory legal demands in the U.S. received by Google. Moreover, Google voluntarily disclosed data in response to 80% of such emergency requests. (By comparison, Google disclosed data in response to 78% of compulsory legal demands in the U.S. in the second half of 2015.) Effectively, what this means is that Google did not disclose user data in response to an emergency request on only 34 occasions in the second half of 2014. Further information about Google's handling of emergency requests appears in the table below.

Timeframe	Emergency Requests	Users/Accounts Impacted by Emergency Requests	Percentage of Cases Where Data Provided in Response to Emergency Requests
July - December 2014	171	272	80%
January-June 2014	171	241	65%
July-December 2013	153	217	78%
January-June 2013	119	175	81%

There are many reasons why a service provider may decline to voluntarily disclose the contents of communications or customer records in response to an emergency request.

For example, the service provider may not have any responsive data that pertains to the target of an investigation. For Microsoft, according to its transparency report, this accounts for more than 26% of requests for which no data is provided in the U.S.; Microsoft simply doesn't have any responsive data to provide.

In addition, the government agency may try to use the process where there is no "emergency involving danger of death or serious physical injury to any person". Service providers take seriously their obligation to protect their users' privacy. It unfortunately appears to be the case that some law enforcement officials make emergency disclosure requests because it is easier than getting legal process, with the checks that come with it, even though legal process is available in a timely manner.

It's not unusual, when we turn down an emergency request because of the lack of a life or limb emergency, that we receive legal process shortly thereafter. Notably, in 2010, the Inspector General of the Department of Justice, in a report concerning the FBI's use of exigent letters and other informal requests to obtain certain customer records on an emergency basis, concluded that the abuses found made it "critical for the Department and Congress to consider appropriate controls on any use by the FBI of its authority to obtain records voluntarily..."

By granting providers the right to disclose when they believe there is such an emergency, but not an obligation to disclose when the authorities assert there is, we help ensure that law enforcement uses legal process as the preferred means to obtain user data, and the emergency process only in true exigent circumstances.

Delay in securing legal process should not be an issue. In every judicial district, a search warrant is a telephone call away. Rule 41(d)(3) permits a magistrate to respond to a telephonic request for a warrant any time, including after-hours where it is inconvenient to go to court or in an exigent situation where time is of the essence or evidence could be lost. Governmental entities avail themselves of this option and consequently obtain user data in a timely manner when exigent circumstances exist.

Finally, it is somewhat ironic to hear law enforcement agencies express misgivings about statutory authority sought by and granted to the government by the USA PATRIOT Act of 2001. Prior to the PATRIOT Act, the Stored Communications Act had no express carve out for emergency situations at all. The PATRIOT Act actually expanded the ability of government to get stored information, including content, in emergency situations. Congress should decline the request to further expand the ability of the government to compel the production of content without a warrant.

Time Limits

Some law enforcement officials propose imposing rigid time limits for providers to respond to legal process issued under ECPA. Judges, however, routinely prescribe deadlines for compliance that are tailored to the exigencies and gravity of particular cases, as well as the need for the underlying evidence. It is unclear why such a proposal is necessary or why Congress is in a better position to manage the individual dockets of judges that oversee cases. Courts, not legislatures, are better positioned to determine compliance deadlines in particular cases based on the needs of law enforcement and the underlying facts of such cases.

Statutorily prescribing time limits in a manner that is divorced from the context of individual cases would have unintended consequences that likely redound to the detriment of law enforcement.

A code-bound time limit would significantly weaken the flexibility that covered service providers currently have to address emergency requests, diverting their attention instead to the longest outstanding requests, even if there is far less urgency attached to such requests. Service providers that now expedite emergency requests from law enforcement in the absence of a rigid statutory timeframe for production would be constrained to do so in the future if they faced penalties for failing to comply with an arbitrary time limit codified under ECPA. Flexibility, not rigidity, is key for triaging unexpected volume, particularly when it relates to emergency requests.

An artificial and arbitrary time limit for production would also reduce the ability of service providers to verify the validity of legal process. There are more than ten thousand agencies that have subpoena power in the U.S. alone, and it is a challenge to make sure that any particular demand is valid. This is not just a theoretical concern. We do receive fake legal process designed to trick us into releasing user information. Current law enables providers to scrutinize and validate legal process, and, as a result, providers are able to identify fraudulent activity and report it to authorities.

Response rates can be attributable to factors that are beyond the control of service providers. For example, when Google receives legal process that is overbroad, vague, or ambiguous, that will invariably slow our response time. Moreover, a single legal request can ask for information covering multiple products and concern multiple account holders, which obviously increases the time and resources necessary to respond. Finally, law enforcement agencies often demand nondisclosure to users without proper nondisclosure orders. That, too, leads to delay. There is no responsible way to codify a statutory time limit to respond.

Proposals to impose time limits pursuant to ECPA legal process should also consider the significant increase in concomitant demands that service providers receive. Since 2009, government requests for user data issued to Google in criminal matters in the U.S. alone have increased 179%. Such proposals should also account for the explosive growth in demands for location information that wireless carriers and other providers are receiving from law enforcement.

Compelled Consent

Some agencies also recommend that Congress amend the voluntary disclosure provision under 18 U.S.C. 2702(b)(3) to require providers to disclose content with the consent of users. While this proposal may have intuitive surface appeal, there are important practical considerations that militate against adoption.

First, if the government obtains the consent of a user to disclose content, the providers are an unnecessary and inefficient conduit for disclosing this content. As noted above, providers are poorly situated to determine relevance and applicable privileges, even assuming the user has actually

consented. Providers should not be discovery agents for agencies under circumstances where users have consented to providing content. Agencies can obtain content directly from targets or witnesses if they obtain consent.

Second, Congress should be wary of proposals that would presume or deem consent based on unavailability, death, minor status, or other circumstances where users have not provided actual consent. Nor should consent be presumed or deemed given merely because the target or witness of an investigation did not respond to a legal request. As mentioned above, agencies have a broad array of tools in their arsenal in the event that uncooperative or intransigent witnesses fail to respond to legitimate requests for information.

Third, authenticating users and verifying consent is not always simple. Providers "authenticate" their users through the account information provided, and if a user confirms receipt of the authentication request, a provider is entitled to rely on it. That process is time-consuming, labor-intensive and often results in more questions than answers as users "object" to production or ask about the nature of inquiry. If a user doesn't respond, or for example, if a user is locked out of her account, service providers may rely on other factors to authenticate users, some of which may not always be useful proxies for verifying identity. Moreover, even if a user consents to provide content pursuant to legal process, there may be others (including joint account holders) whose consent may be required. But all of this is an unnecessary burden because users should be required in the first instance to comply with their discovery obligations without entangling service providers.

Notice to User

H.R. 699 requires law enforcement agencies to provide notice to a subscriber or customer of a provider within ten business days of receiving communications content pursuant to the issuance of a warrant. Notice is a core privacy protection in H.R. 699 that must be preserved. Notice from the government may be the only way that a user may ever learn of the warrant. Without notice, the user may never have an opportunity to seek relief where the warrant was improperly obtained, where privileges were violated or the disclosure of the user's communications was otherwise improper. Significantly, very similar user notice requirements exist in ECPA currently, and there has been no indication this has caused any problems.

In the physical world, of course, notice by the government of a warrant is direct and palpable at the time of execution. The notice provision in the Email Privacy Act is less exacting on the government, and gives the government time after receiving the communications to give notice. Moreover, there are no statutory rules in the physical world that authorize the government to prohibit comparable third party service providers (e.g. Public Storage) from notifying customers of search warrants served on the storage company for customer property. Seizure of a computer from

the home or workplace containing the same email stored with a provider, for example, would come with direct notice to the property owner who in turn is free under the law to tell anyone that a warrant was executed.

Currently under ECPA, on the other hand, governmental entities may obtain non-disclosure orders that preclude service providers from notifying users of legal demands for a period of up to 90 days, which can be renewed for additional periods of 90 days. The Email Privacy Act imposes a new requirement on providers. Under the bill, any provider that intends to give notice to a user about a legal demand after expiration of a gag order must give advance notice to the government. Although the National Association of Assistant United States Attorneys argues that the notice should be extended by a few days, there is currently no such advance notice requirement on providers and no indication that this has caused any problem. In 2015, it is anachronistic that service providers with hundreds of millions (if not billions) of users are more constrained to notify users of legal demands than comparable service providers in the physical world or individuals or businesses would be if their property were seized directly from them. This makes it all the more critical that the government provide notice to the user.

Notably, H.R. 699 not only allows law enforcement agencies to delay notification to users under ECPA in some cases, but also increases the timeframe for delayed notification from 90 to 180 days in response to concerns raised by law enforcement agencies. Law enforcement agencies sought and secured this particular provision to the bill. Specifically, it allows governmental entities to seek an initial delay of up to 180 days if notification to a user would lead to an adverse result, and governmental entities can seek an extension of this delay for an additional 180 days (with no limitation on additional 180 day renewals) to the extent an adverse result would persist. In light of these generous delay provisions sought by law enforcement to accommodate situations where an adverse result might occur, it is critical to preserve the direct notification provisions that afford users a meaningful opportunity to, for example, challenge warrants that may violate the Fourth Amendment and to petition for return of their seized property.

* * * * *

It is axiomatic that ECPA no longer reflects users' reasonable expectations of privacy and no longer comports with the Fourth Amendment. H.R. 699 represents an overdue update to ECPA that would ensure electronic communications content is treated in a commensurate manner to other papers and effects stored in the home, which are protected by the Fourth Amendment. It is long past time for Congress to pass a clean version of H.R. 699.

Thank you for your time and consideration.