Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google Inc.
Senate Judiciary Committee
Hearing on "Reforming the Electronic Communications Privacy Act"
September 16, 2015

Chairman Grassley, Ranking Member Leahy, and members of the Committee, thank you for the opportunity to appear before you this morning to discuss updating the Electronic Communications Privacy Act (ECPA).

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 S. 356, the Electronic Communications Privacy Act Amendments Act of 2015, which currently has 23 cosponsors. The House companion measure, the Email Privacy Act, now has 292 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 frustrate users' reasonable expectations of privacy. 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 baffling and complex 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 or newer, the government will need a search warrant. In its testimony before the House Judiciary Committee in 2013, 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 2013 testimony that the statute should "not accord lesser protection to opened emails than it gives to emails that are unopened", which is another problematic distinction that ECPA makes.

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, S. 356 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.

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 Recognizes the Importance of Affording the Highest Privacy Protections to Electronic Communications

Between the last time I testified in support of updating ECPA in March 2013 and now, 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 S. 356, which is sponsored by Senators Lee and Leahy.

Congress Should Reject Proposals That Weaken the Core Privacy Protections in S. 356

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. 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. SEC Chairwoman Mary Jo White alluded to such an idea in an April 2013 letter to Senator Leahy.

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 to such a bright-line rule 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 that is 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 ("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.

Finally, while some civil agencies have raised hypothetical concerns that a bright line, warrant-for-content rule would frustrate their investigations, there is scant evidence to suggest that civil agencies typically encounter such scenarios or that, even when they do, the investigations are hindered. In the 2013 letter from SEC Chairman White 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 the case cited by the SEC "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 some or all data in response to 80% of such emergency requests. (By comparison, Google disclosed some or all 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 only withheld user data in response to an emergency request on approximately 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 Some or All 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 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.

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, 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...." Legislation that would require service providers to disclose the content of users' communications or customer records upon the mere assertion of an emergency would have the opposite effect, wholly stripping service providers of any discretion to ensure that the emergency authority under ECPA is utilized appropriately and subject to reasonable checks and balances.

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. Presumably it is because some law enforcement officials believe that providers covered under ECPA do not comply quickly enough with legal process. But 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. If there is an arbitrary deadline to produce, with penalties for late production, service providers will be compelled to focus on older requests, even when law enforcement agencies might want service providers to focus on more recent requests that have greater urgency.

A rigid 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 limits 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.

Slow 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 has 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 (including the attorney-privileged material), even assuming the user has actually consented. Providers should not be discovery agents for civil agencies under circumstances where users have consented to providing content. Civil 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, civil 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.

Direct Notice

S. 356 requires law enforcement agencies to provide notice directly to a subscriber or customer of a provider within ten business days of receiving communications content pursuant to the issuance of a warrant. Direct notice is a core privacy protection in S. 356 that must be preserved. Absent direct notice, users may not have a meaningful opportunity to challenge the legality of the warrant in a criminal proceeding. Moreover, absent direct notice, users may not have the opportunity to assert relevant legal privileges or challenge the breadth of information that may be sought. In the physical world, of course, notice of a warrant is direct and palpable at the time of execution.

Notably, S. 356 allows law enforcement agencies to delay notification to users under ECPA in some cases. Specifically, it allows governmental entities to seek initial delays 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 to the extent an adverse result would persist. In light of these generous delay provisions to accommodate situations where an adverse result might occur, it is critical to preserve direct notification provisions that afford users a meaningful opportunity to challenge warrants that may violate the Fourth Amendment.

* * * * *

It is axiomatic that ECPA no longer reflects users' reasonable expectations of privacy and no longer comports with the Fourth Amendment. S. 356 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 S. 356.

Thank you for your time and consideration.