October 7, 2015

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

Question for the Record from Senator Grassley

Q1: **In 2014, Apple implemented a new operating system that employed a system of encryption that effectively prevented it from providing certain user content in response to a judicially-authorized search warrant or otherwise bypassing a user's passcode. I understand that Google does not currently employ such a system. Does Google intend on implementing an Apple-like encryption system or will Google continue to employ strong encryption technology that still allows law enforcement to access platforms and devices with court authorization?**

A: As I mentioned in the hearing, keeping user data secure is important to Google and to the people who use the services Google offers. Encryption is a valuable tool in the suite of tools that Google can use to secure information that users have shared with Google. There are many types of encryption, and, depending on the product, one type of encryption may be more appropriate than another to keep the information secure while also providing the underlying services. It is important that Google, and companies that handle the data of Americans, have the ability to use technological means to combat the serious threats to the nation's networks; it would be shortsighted to hamstring the ability of network operators to employ key security defenses to protect the nation's data.

Since 2011, Google's Android operating system has allowed an Android user to secure the data on the device with the key in the control of the user, much as users have been able to do with computers and laptops of all sorts for many years now. The newest version of the Android operating system, known as Marshmallow, continues this approach and makes it easier for those with Android phones to secure their devices to protect against the event that the phone is lost or stolen. The data on the device, as well as the device itself, is in the control of the owner. The device and the data are available to investigators from the user in response to court authorization no less than any other item or data that a user may have in his or her unique possession.

Many former national security officials, current government officials, and security experts believe that this type of device encryption is important to protect the public from identity theft, privacy invasions and other crimes:

- *"We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."*

Mike McConnell (former NSA Director)
Michael Chertoff (former DHS Secretary)
William Lynn (Former Deputy Secretary of Defense)
Washington Post op-ed on 7/28/15

- *"If consumers cannot trust the security of their devices, we could end up stymieing innovation and introducing needless risk into our personal security. In this environment, policy makers should carefully weigh the potential impact of any proposals that may weaken privacy and security protections for consumers."*

Terrell McSweeny
FTC Commissioner
Huffington Post op-ed on 9/3/15

- *"The US Government should take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage."*

The President's Review Group on Intelligence and Communications Technologies
on 12/12/2013

Question for the Record from Senator Leahy

Q1: **In its testimony, the SEC asked Congress for the authority to obtain the contents of electronic communications from third-party service providers without a warrant. How do you respond to this proposal? What are the implications of requiring providers to go into their users' accounts to look for and produce communications and documents that are responsive to a civil investigation?**

A: There are several reasons why civil administrative agencies should not be granted the power to compel service providers to disclose the content of user communications.

First, granting civil agencies the power to compel service providers to disclose the content of communications stored with the provider by users would run afoul of the Constitution. The reasoning in *United States v. Warshak*, concluding that the Fourth Amendment protects the content of communications stored with a service provider, is persuasive. The SEC has set out an abstraction from which, it contends, one could draft a special Fourth Amendment carve-out. Even assuming that there is a way to draft a bespoke rule for the SEC that passes constitutional muster, this is the sort of exercise that Chief Justice Roberts warned against in in Riley v. California, 134 S.Ct. 2473 (2014). In that decision, Chief Justice Roberts wrote that a regime with various exceptions and carve-outs "contravenes our general preference to provide clear guidance to law enforcement through categorical rules." *Riley*, 134 S.Ct. at 2493.

Second, there is no need to create a carve out of this constitutional doctrine for civil administrative agencies. The SEC and the thousands of other administrative agencies in the United States have ample authority to obtain communications of targets and witnesses without also granting them powers reserved to criminal and national security authorities.

As I discussed in my responses to questions posed by Senator Whitehouse, civil administrative agencies can issue subpoenas to the targets or witnesses to obtain their records. There is no need for a provider, or even a court, to get involved. If the recipient of the subpoena is intransigent or uncooperative, the administrative agency has a broad array of tools to compel compliance. Civil agencies can always enforce subpoenas when a person fails to produce responsive documents and secure a court order. If a target or witness subsequently fails to produce responsive material pursuant to that 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. As Andrew Ceresney, who testified for the Securities Exchange Commission noted, the intransigence of a witness can be discovered by issuing subpoenas to others.

It is thus not surprising that when asked at the hearing if there were cases that were affected by the inability of the SEC to obtain content from providers, Mr. Ceresney gave no examples. This in spite of the fact that the the SEC and all other civil administrative agencies have never had the authority the SEC now seeks. Previously, in an April 2013 letter to Senator Leahy, the SEC discussed what it purported to be an example of a case where the lack of authority to delve into the constitutionally protected online accounts of others negatively impacted an investigation. In that letter, SEC Chairman Mary Jo White asserted that "absent ECPA authority to subpoena the ISP directly, the Commission would not have had in its possession this critical piece of evidence." Upon closer analysis, this example was debunked.

Third, a provider will make a very poor substitute for the user in searching for and selecting documents to produce. The provider will likely have little knowledge about the case in order to determine what communications are in and what are outside the scope of the legal process, and no ability to determine what materials are privileged, are trade secrets or confidential, or subject to special handling rules like health information. As in any civil case, it should be the witnesses

who are responsible for finding and producing the documents over which they have control. There is no reason that there should be a different rule for documents a witness has stored online than for documents stored by the witness at home. Even in cases where the user consents to disclosure, providers should not be forced into becoming discovery vendors for parties in civil litigation.

Finally, it is worth noting that there are thousands of civil administrative agencies in the United States with some flavor of subpoena power. Each no doubt has a case to make as to why the authority the SEC seeks would be useful. Granting such authority to these agencies would be a significant expansion of power for all of these agencies, large and small, at the expense of the Fourth Amendment. We would never grant civil administrative agencies the power to convert landlords into police officers to search for documents in the basement of a home, and we should tolerate that no less with the same documents stored online.

Question for the Record from Senator Lee

Q1: **In his testimony, Mr. Littlehale described the difficulties that law enforcement agencies encounter when making emergency requests to service providers. In particular, he noted that the determination of an emergency is left to the providers rather than with those agents on the ground and that the response rate is too low or too slow.**

- **Do you believe that an emergency exception that would compel compliance from service providers is necessary?**

A: No. The current emergency authorities codify important checks and balances that ought to be preserved by Congress. Moreover, users expect Google to scrutinize requests for communications content that otherwise are not reviewed by a judge to ensure that statutory criteria for emergency situations (i.e. danger of death or serious physical injury to any person) are met.

In his testimony, without identifying any providers, Mr. Littlehale asserts that some "providers make a decision never to provide records in the absence of legal process, no matter the circumstances, as baffling as that may sound in the light of day." Vis a vis the largest Internet companies in the world, including Google, it is clear that this is not the case. The transparency reports published by Google, Facebook, Microsoft, and Yahoo!, each disclose data about the number of emergency requests received and the percentage of cases where responsive data is provided. Google takes emergency requests under ECPA very seriously, and those requests receive the highest priority.

It is not a little ironic to hear a representative of local 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 struck the right balance in granting providers the discretion to reject requests that did not meet the statutory criteria for emergencies, and it should decline the invitation to weaken the core protections of S. 356 by amending the emergency provisions under ECPA in ways that do not comport with the Fourth Amendment.

- **Does it make sense for the service provider to be able to decline a request in an emergency? Why?**

A: Yes. The current statutory provision has proven to work well, and there is no need to convert this into a new authority, which necessarily would have very little pre-disclosure oversight to prevent abuse. Google has set up a 24/7 emergency request system to respond to life and limb emergencies wherever in the world the emergency may happen. The requests are handled immediately as they come in by trained specialists. We take this very seriously. As our Transparency Report shows, Google is able to help in the majority of requests, 80% in the last reporting period, that come to us through this authority.

Of course, there are situations in which a provider will not disclose the contents of communications or customer records in response to a request that is purported to be an emergency. For example, the service provider may not have any responsive data. 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 some situations, a government agency may make a request where there is no "emergency involving danger of death or serious physical injury to any person" and there is time to secure legal process. At Google, we take seriously our obligation to protect users' privacy. Unfortunately, at times government investigators try to invoke the 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.

To the extent a government investigator prefers to compel the disclosure, delay in securing legal process should not be an issue. In every federal judicial district, a search warrant is a telephone call away. Federal Rule of Criminal Procedure 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.

- **What is Google's response rate to emergency requests? What reasons could a service provider have for not complying?**

A: 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 issued to Google by authorities in the U.S. As I mentioned above, Google voluntarily disclosed data in response to 80% of those 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.)

Further information about Google's handling of emergency requests appears in the table below. (Some of the reasons why a service provider may not comply with an emergency request are discussed in response to the previous question.)

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

- **In what ways can the response time be improved in cases where an emergency exists?**

A: As noted above, emergency requests receive the highest priority. We strive to respond to emergency requests in about an hour. Of course, some are resolved much faster, and others may be more complex and take longer to close out, but they all receive immediate attention when sent through the emergency system.

Q2: **Several witnesses have discussed the slow response rates from service providers as reasons to hold up codifying a warrant-for-content standard.**

- **Why are response rates perceived as being slow?**

A: It is difficult to speculate why law enforcement agencies perceive that service providers are slow to respond to legal demands; it's likely that response times vary among companies that receive ECPA legal process just as it would with companies that receive non-ECPA process. The substantial increase in law enforcement demands to service providers like Google may fuel this perception. Since 2009, government requests for user data issued to Google in criminal matters in the U.S. alone have increased 179%. Notwithstanding this fact, Google responds to law enforcement demands in a timely manner.

Judges of course can prescribe deadlines for compliance that are tailored to the exigencies and gravity of particular cases, as well as the need for the underlying evidence. If service providers are uncooperative or otherwise non-compliant, law enforcement agencies can take remedial actions with a court to enforce such deadlines. Taking that discretion away from judges and trying to craft a one-size-fits-all statutory deadline makes little sense.

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, ambiguous, illegible, riddled with typographical errors, or issued without proper authority, that will invariably slow our response time in responding to that process, and of course takes resources away from properly issued process. Moreover, a single legal request can ask for information covering multiple products and concern multiple account holders, and may require engineering resources, each of 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.

- **What is Google doing to improve response times?**

A: Google is always looking for ways to improve the process, while making sure that we are not compromising the quality of review to protect users. We do this in many ways. For example, as the volume of requests increases, we increase the number of legal specialists to handle them. As you might expect, we also are able to take advantage of the technical expertise of the company to offer faster and more secure ways for government agencies to submit requests and receive responses.

The huge number of agencies, with different technical competencies and legal authorities, make it impossible to have a single approach for all. Nonetheless, we have been able to reduce response time even as volume has grown. Time varies between legal process, of course, as some are more urgent than others and some have shorter deadlines than others. In addition, after hearing the testimony of Mr. Littlehale, we reached out to make sure that if any of his perceptions applied to Google, we find ways to address them.

Q3: **The administration witnesses on the first panel spent a great deal of time talking about how onerous it would be to face a warrant requirement for email content. Yet, they have been operating for years under a bright-line, warrant-for-content standard.**

- **In what ways would enacting the warrant requirement laid out in the ECPA Amendments Act change the ability of these agencies to gather information?**

A: It would change nothing at all. As you note, civil agencies have been operating under a bright-line, warrant-for-content standard since 2010, when the Sixth Circuit Court of Appeals opined in *United States v. Warshak* that ECPA is unconstitutional to the extent it does not require a warrant for all content. Even before then, going all the way back to 1986 when ECPA was passed, the civil agencies could not get email that was unread and fresh from providers, per the limitations in the statute.

There is no evidence to suggest that *Warshak* decision, or the limits in ECPA before that, have prevented civil agencies from investigating cases. 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.

Warshak is effectively the law of the land today. It is embraced by companies and observed by governmental entities. In many ways, 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.

Question for the Record from Senator Franken

Q1: **I am interested in better understanding the various circumstances in which Google satisfies government requests for user data. The statistics I've seen indicate that Google receives more than 20,000 requests per year from government agencies in the United States, and is able to provide at least some data in response to approximately 80% of these requests. Of course, not all of these requests are for content or are accompanied by**

criminal warrants. Please describe the range of requests typically received. How often does Google voluntarily comply with requests based on an exception for emergencies?

A:

Range of Requests

Google receives a broad array of government demands seeking user data, which includes demands for basic subscriber information (which is defined in the statute, such as name, account creation information, associated email addresses, phone numbers), other non-content data (e.g. the IP address associated with a YouTube video upload, records of who a user emailed and who emailed the user) and content (e.g., the body of Gmail messages).

Approximately 60-70% of US demands for user data that Google receives are subpoenas, through which the government can obtain basic subscriber information. About 10% are court orders through which the government can seek basic subscriber information and often the more detailed non-content information. Another 20-30% are search warrants, through which government can seek the non-content information as well as content. Not all warrants require production of content. We also receive a small number of orders issued under pen register and trap and trace statutes, and an even smaller number under wiretap authorities.

Since 2014, we have also reported data about the volume and type of national security demands that we receive. We look forward to the effective date of the USA Freedom Act, under which we will be able to increase the granularity of those reports, and we greatly appreciate your leadership in ensuring the enactment of these provisions.

Emergency Requests

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.)

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
July - December 2014	171	272	80%
January-June 2014	171	241	65%
July-December 2013	153	217	78%
January-June 2013	119	175	81%