**Written Testimony of Richard Salgado**
**Director, Law Enforcement and Information Security, Google Inc.**
**House Judiciary Subcommittee on Crime, Terrorism, Homeland Security and Investigations**
**Hearing on "ECPA Part 1: Lawful Access to Stored Content"**
**March 19, 2013**

Chairman Sensenbrenner, Ranking Member Scott, and members of the Subcommittee, 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 Coalition, which supports updating ECPA. More than 80 organizations, trade associations, and corporations, including a number of which have joined in recent months, are now members of the Digital Due Process Coalition. Digital Due Process Coalition members include the American Civil Liberties Union, Americans for Tax Reform, the Center for Democracy & Technology, the Competitive Enterprise Institute, and the Electronic Frontier Foundation. Notably, these entities span the political spectrum. The diverse array of organizations, trade associations, and corporations that comprise the Digital Due Process Coalition is a testament to the recognition across the political spectrum and in the corporate community that there is a need to update ECPA.

The statute, though ahead of its time in many ways when enacted, needs to be brought in line with how people use the Internet today, provide them with the privacy they reasonably should expect, and allow the growth of the Internet — and the job creation and economic opportunity that such growth brings — to continue. Google believes this can be done while also ensuring that government agencies have the legal tools they need to efficiently and effectively protect public safety.

**ECPA Reflects the Pre-Internet 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 2013 are dramatically different than 25 years ago.

- 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 2013, 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.

The distinctions that ECPA made in 1986 were foresighted in light of technology at the time. But in 2013, 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.

**The Internet is Now Part of Everyday Life**

New forms of Internet computing, more popularly known as "cloud computing," have emerged since ECPA was first signed into law. This computing model is used today by significant numbers of consumers, businesses, and the public sector. Companies like Google offer users the ability to store, process and access their data from servers located in offsite data centers, rather than on the user's premises. We provide our users with the ability to get work done on any device, store important documents, easily share and collaborate, and receive a service's latest innovations just by refreshing your browser.

For example, Google's services, including Google Search, Gmail, YouTube, Blogger, Google Drive, and Google Calendar, allow our users to run programs and store data on our geographically distributed and secured data centers. Businesses are increasingly choosing to use such data centers — managed by Google and many other technology companies — the same way they once used

their desktop computers or on-premise file servers. In the process, they are saving money, becoming more efficient, and improving their security.

More than five million businesses are now running on Google Apps and benefiting from more modern technology at a lower cost. These include Global 500 companies, top American universities, and state and local agencies in 45 states. Everyday processes and information that are typically run and stored on local computers — such as email, documents, and calendars — can now be accessed securely anytime, anywhere, and with any device through an Internet connection.

Internet computing also enables services like online video and shared document collaboration among people across the country or around the world. As customer needs grow, the services they use can be expanded on demand, without requiring slow and burdensome procurement processes.

These services have created enormous and tangible value in the economy, spawning new businesses and spurring innovation and further growth in the tech sector. As communications and networks become faster and more data intensive, this sector will continue to create new jobs and more opportunities for investors, innovators, and small businesses.

It is increasingly difficult for individual business and organizations to keep up with the growing sophistication of cyber attacks. However, web services leverage significant economies of scale to bring both human and technology resources to bear in defense against such attacks. Google's services are delivered on a multi-billion dollar infrastructure that is designed and maintained with security as a top priority. The latest security updates can be pushed quickly across all of our data centers globally, protecting all of our customers in a more effective and uniform way than traditional software would allow. We've also made the Internet safer for millions of users by providing them with with free, strong-authentication mechanisms — such as two-step verification — and secured connections through SSL encryption.

Information technology (IT) departments within companies and other organizations are vulnerable to sophisticated attackers. Often underfunded and undermanned, these IT departments are further susceptible to cuts when financial constraints require it. Removing artificial and counterproductive legal standards that hinder movement to services offered by providers like Google will help strengthen our nation's network security.

**ECPA Should be Updated**

As the benefits of Internet computing become more obvious and widespread, its growth shouldn't be artificially slowed by the outdated technology assumptions that are currently baked into parts of ECPA. Nor should the progression of innovation and technology be hobbled by pre-Internet ECPA provisions that no longer reflect the way people use the services or the reasonable expectations they have about government access to information they store on Internet services.

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.

The current complexity can be demonstrated by the requirements to compel production of communications content such as email. 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 certain circumstances). If the email is 180 days or newer, the government will need a search warrant. The Department of Justice also takes the position that a subpoena is appropriate to compel the service provider to disclose the contents of an email even if it is not older than 180 days if the user has already opened it. The Ninth Circuit Court of Appeals has rejected this view.

In 2010, the Sixth Circuit held in *United States v. Warshak* that ECPA violates the Fourth Amendment to the extent that it does not require law enforcement to obtain a warrant for email content. Google believes the Sixth Circuit's interpretation in *Warshak* is correct, and we require a search warrant when law enforcement requests the contents of Gmail accounts and other 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 government entities seek to compel production of the content of electronic communications.

The inconsistent, confusing, and uncertain standards that currently exist under ECPA illustrate how the law fails to preserve the reasonable privacy expectations of Americans today. Moreover, providers, judges, and law enforcement 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, confusing compliance hurdles for service providers, ECPA has created an unnecessary disincentive to move to a more efficient, more productive method of computing. ECPA must be updated to help encourage the continued growth of the cloud and our economy.

**Improving Transparency**

We believe that better data about the requests that governmental entities make under ECPA can help inform the broader debate around updating ECPA. We are the first Internet company to launch a Transparency Report, which provides data about government requests we have received since 2009. Google's Transparency Report provides data about the volume of requests we receive from governments around the world. Other companies, including Twitter, Dropbox, Linkedin, and Sonic.net, are now publishing their own transparency reports. These efforts to provide transparency to users are important, and we hope others will join them.

Over the three years that we've provided these reports, government requests for user data issued to Google in criminal matters in the U.S. have increased by 136%. We recognize that local, state, and federal law enforcement agencies have legitimate needs for data. We also recognize the need to ensure that disclosure laws such as ECPA properly honor the privacy that users of communications services reasonably expect. Our hope is that the Transparency Report will inform that discussion.

In 2013 alone, we've taken several steps to be more transparent with our users about government requests that we receive:

- On January 23, we began publishing more detailed data about the types of government requests that we receive in the United States pursuant to ECPA.

- On January 28, we published a new section to our Transparency Report and a blog post that explains how we handle and respond to government requests.

- On March 5, we began including some data about the number of National Security Letters (NSLs) that we receive.

Going forward, we're committed to exploring ways to surface more data and provide greater insight into the government requests we receive. Transparency in this context has had a salutary effect in encouraging a broader discussion about the importance of updating ECPA.

* * * * *

We look forward to working with this Subcommittee, the full Judiciary Committee, and Congress as a whole to strengthen the legal protections for individuals and businesses that rely on our services so that technological innovation can continue to drive economic growth, while ensuring that law enforcement continues to have the legal tools needed to investigate and prosecute crime.

Thank you for your time and consideration.