Written Testimony of Richard Salgado
Senior Counsel, Law Enforcement and Information Security, Google Inc.
House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Hearing on "ECPA and the Cloud"
September 23, 2010

Google thanks Chairman Nadler, Ranking Member Sensenbrenner, and members of the Subcommittee for examining the need to modernize the Electronic Communications Privacy Act of 1986 (ECPA).

My name is Richard Salgado. As the Senior Counsel 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 also 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.

It is vital for online providers and for Americans who use Internet communications services that Congress update ECPA to address the tremendous technological advances in communications and computing technology that the world has witnessed since 1986, when the statute was passed. This is why Google played a lead role in founding the Digital Due Process coalition (www.digitaldueprocess.org), an ECPA reform advocacy coalition that includes other technology companies, public interest organizations, and academics. The coalition believes that our laws should protect individuals from unwarranted government intrusion in the online world no less than they do in the home, even as communications and computing technology continue to advance. At the same time, ECPA must offer law enforcement the tools necessary to perform its important work.

ECPA reflects the pre-Internet computing landscape of the 80s

ECPA was written for the communications and computer technology of 1986. The ways in which we communicate and compute today, however, bear little resemblance to those of a quarter century ago. When ECPA became law, communication through the Internet was the province of academic researchers and government agencies. There was no generally available way to browse the World Wide Web. Commercial email had yet to be offered to the general public. Instant messaging wasn't widely used until the late 1990s. In 1986, only 340,000 Americans subscribed to cell phone service -- the equivalent of one line for every citizen of Tampa, Florida -- and not one of them was able to send a text message.

Since 1986, we have experienced unprecedented advances in communications technology and

services, and a fundamental shift in how individuals communicate with each other. The web, search engines, video sharing sites, social networks and voice-over-IP services are only a few of the technologies that have become commonplace and part of everyday life, yet would have seemed like science fiction at the time ECPA was enacted.

We've seen a profound transformation in the way we store, access, and transfer data. In 1986, holding and storing data was expensive, and storage devices were limited by technology and size. A 10 megabyte hard drive that had room to store about two high resolution photos cost $650 (or 10 dollars per megabyte). In 2010, thanks to innovation and advances in technology, a 1.5 terabyte hard drive can be purchased for less that $100 (under $0.000094 per megabyte) and hold 300,000 photos. Complimenting the growth in storage capacity, data transfer rates are nearly one hundred and sixty times faster than in 1986 -- making it possible to share richer data, to collaborate among many users, and to perform more complicated tasks in a fraction of the time it took when ECPA became law.

This massive drop in cost and increase in the speed of storing and accessing data has had a huge and positive impact on all classes of online users, fostering improvements in efficiency and innovation. The development of Internet-based computing and storage -- widely known as "cloud computing" -- is one direct benefit.

The growth of the cloud

Cloud computing is a relatively new term for some, but the cloud is being used today by significant numbers of consumers, businesses, and the public sector. Companies like Google are now able to offer their users the ability to store, access, use and share their data from servers located in offsite data centers, rather than on the user's premises. Instead of loading various software packages onto their computers, users access applications and services over the Internet.

For example, Google's cloud applications, including Gmail, Google Docs, and Google Calendar, allow our users to store data or run programs on our geographically distributed, secure data centers. Businesses increasingly are choosing to use such data centers -- managed by Google and many other technology companies -- the same way they used to use their desktop computers or on-premise file servers. In the process they are saving money, becoming more efficient, and improving their security.

Leading analysts confirm an acceleration of adoption of cloud computing, with the scale of deployments growing. As Google just announced, over three million businesses now use our cloud service, Google Apps, and every day more than 3,000 businesses sign up. Other providers appearing before the Subcommittee today can tell similar stories about their growth and the benefits seen by their customers.

In the cloud, everyday processes and information that are typically run and stored on local computers -- email, documents, calendars -- can be accessed securely anytime, anywhere, and with any device through an Internet connection. Rather than invest in expensive and specialized

IT equipment and personnel, customers can rely on the scale and security offered by the cloud providers to access data anywhere Internet access is available. The cloud also enables services like online video, shared document collaboration among people across the country or around the world, and many other services. As a customer's needs grow, the cloud services she uses can expand as needed without the customer having to go through a slow procurement process.

The "virtual" services offered in the cloud have created enormous and tangible value in the economy, spawning new businesses and a spurring innovation and further growth of 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 and innovators.

The need for an ECPA update

Millions of Americans already use the cloud every day -- to send messages, to collaborate with co-workers, to store important records and documents. More and more computing functions and communications will move to the cloud as its benefits are more widely felt. This is a valuable and important trend that shouldn't be slowed artificially by outdated technology assumptions 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 in the cloud.

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, leaving 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 U.S. 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 retrieved it. The Ninth Circuit Court of Appeals has rejected this view.) It's difficult to imagine a justification for a rule that lowers the procedural protection for a message merely because it is six months old or has been viewed by the user.

The inconsistent, confusing and uncertain standards raised by examples like this one reveal how ECPA 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 cloud providers, ECPA has perversely created an artificial and unnecessary disincentive to move to a more efficient, more

productive business model. ECPA must be updated to help encourage the continued growth of the cloud.

A roadmap for reform: Digital Due Process

The Digital Due Process coalition has put forward principles that are designed to help ensure that content stored in the cloud receives no less due process protection as data held on computers at home or in the office, to simplify and adjust the rules to match the reasonable privacy interests of today's online citizens, and to ensure that government has the legal tools needed to enforce the laws.

There are four key ways ECPA should be updated:

- **Create a consistent process for data stored online:** Treat private communications and documents stored online the same as if they were stored at home and require the government to get a search warrant before compelling a service provider to access and disclose the information.

- **Create a consistent process for location information:** Require the government to get a search warrant before it can track movements through the location of a cell phone or other mobile communications device.

- **Clarify the process for real-time monitoring of when and with whom communications are being made:** To require a service provider to disclose information about communications as they are happening (such as who is calling whom, or "to" and "from" information associated with an email that has just been sent or received), the government would first need to demonstrate to a court that the data it seeks is relevant and material to a criminal investigation.

- **Clarify the process for bulk data requests:** A government entity investigating criminal conduct could compel a service provider to disclose identifying information about an entire class of users (such as the identity of all people who accessed a particular web page) only after demonstrating to a court that the information is needed for the investigation.

Modernizing ECPA along these lines will benefit everyone who uses cloud services -- including individual users, businesses small and large, and enterprise customers -- all of whom depend on having their data available everywhere, kept secure, and offered at low cost. It will also make users of cloud services confident that the privacy of what they store virtually in the cloud is respected no less than the privacy of information stored at home. As confidence grows and users put more of their data on the cloud, those benefits will be felt throughout the American economy in the form of lower costs and higher productivity. Further, these updates will provide clear guidance and consistency to law enforcement agencies, and will not impede the ability of law enforcement agents to obtain evidence stored in the cloud.

The issue of due process in the cloud is one of increasing interest to our users. Earlier this year, Google released a new government requests transparency tool that gives our users information about the requests for user data or content removal we receive from government agencies around the world (www.google.com/transparencyreport). This week we updated the tool to reflect more recent data. This tool has served to raise attention to the issue of what rights users have when it comes to their data. We believe that the U.S. should lead the way in ensuring that data requests for online data receive the kind of due process that citizens expect and deserve.

Advances in technology rely not just on the smart engineers who create the new services, but also on smart laws that provide the critical legal underpinning for continued innovation and adoption of the technology. We look forward to working with this Subcommittee and with Congress as a whole to strengthen the legal protections for individuals and businesses that rely on our services so that technology innovation can continue to lead our economic recovery, while ensuring that law enforcement continues to have the legal tools needed to satisfy it's important responsibilities.

Thank you.