MARCH 19, 2013

ECPA PART 1: LAWFUL ACCESS TO STORED CONTENT

UNITED STATES HOUSE OF REPRESENTATIVES, COMMITTEE ON THE JUDICIARY,

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY AND INVESTIGATIONS

ONE HUNDRED THIRTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

COMPILED FROM:

- *http://judiciary.house.gov/hearings/113th/hear_03192013_2.html*

Statement of Judiciary Committee Chairman Bob Goodlatte Subcommittee on Crime, Terrorism, Homeland Security, and Investigations Hearing on "ECPA Part 1: Lawful Access to Stored Content"

Contact: Kathryn Rexrode or Jessica Baker, (202) 225-3951

For Immediate Release
March 19, 2013

Statement of Judiciary Committee Chairman Bob Goodlatte
Subcommittee on Crime, Terrorism, Homeland Security, and Investigations
Hearing on "ECPA Part 1: Lawful Access to Stored Content"

Chairman Goodlatte: The dawn of the digital age and the explosive development of communication methods has brought with it faster ways to compile, transmit and store information. These developments have produced faster and more efficient ways to do everything from conducting commerce to connecting with friends.

Unfortunately, criminals have found ways to convert the benefits offered by new technology into new ways to commit crimes. At the intersection of these activities are the privacy rights of the public, society's interest in encouraging and expanding commerce, the investigative needs of law enforcement professionals, and the demands of the Constitution.

The Electronic Communications Privacy Act (ECPA) was designed to provide rules for government surveillance in the modern age. The technology of 1986 now seems ancient in comparison to today's. The interactive nature of the Internet, now including elements such as home banking and telecommuting, has produced an environment in which many people may spend hours each day "on-line." In this context, a person's electronic communications encompass much more today than they did in 1986. Indeed in 2013, a person's electronic communications encompass much more than they did in 2000, when Congress acknowledged that much had changed since the original ECPA of 1986. ECPA reform must be undertaken so that despite the evolution of technology and its use in the world, the constitutional protections reinforced by ECPA will endure.

ECPA was intended to establish a balance between privacy and law enforcement. In addition, ECPA sought to advance the goal of supporting the development and use of new technologies and services. Those original tenets must and will be upheld as this law is improved.

There are many investigations in which ECPA is working, and working well. Pedophiles who sexually assault children and distribute video recordings over the Internet have become increasingly savvy. They encrypt their communications and use technologies to hide their identities and whereabouts. Investigators routinely use court orders under ECPA to identify these offenders, uncover caches of child pornography that has been stored remotely "in the cloud," and develop probable cause to execute warrants and arrest them.

ECPA reform is one of the top priorities of the House Judiciary Committee. Technology will help us solve many of the pressing problems our nation currently faces. We need to make sure that the federal government's efforts are focused on creating incentives that encourage innovation and eliminating policies that hinder it. In updating a law passed before the creation of the Internet, the modernization of ECPA needs to provide electronic communications with protection comparable to their more traditional counterparts and take into account the recent boom in new technologies like cloud computing, social networking sites and video streaming. That's why we will modernize the decades-old Electronic Communications Privacy Act to reflect our current digital economy while preserving constitutional protections.
This particular hearing focuses on issues related to the lawful access to stored communications under the current law. It is becoming clear that some reforms are necessary, but this committee will move toward modernization and reform after a thorough review and with input from all stakeholders.

I look forward to working with all members on both sides of the aisle to modernize the Electronic Communications Privacy Act.

US House of Representatives Committee on the Judiciary
2138 Rayburn House Office Building Washington, DC 20515 p\202.225.3951

Department of Justice

STATEMENT OF
ELANA TYRANGIEL
ACTING ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGAL POLICY

BEFORE THE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

REGARDING
THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

PRESENTED
MARCH 19, 2013

Statement of
Elana Tyrangiel
Acting Assistant Attorney General
Office of Legal Policy

Committee on The Judiciary
Subcommittee on Crime, Terrorism, Homeland Security, and Investigations
United States House of Representatives

Electronic Communications Privacy Act ("ECPA")
March 19, 2013

Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee, thank you for the opportunity to testify on behalf of the Department of Justice regarding the Electronic Communications Privacy Act (ECPA). This topic is particularly important to the Department because of the wide-ranging impact the statute has on public safety and both criminal and civil law enforcement operations. We are pleased to engage with the Subcommittee in discussions about how ECPA is used and how it might be updated and improved.

ECPA includes the Pen Register Statute and the Stored Communications Act (SCA), as well as amendments to the Wiretap Act. These statutes are part of a set of laws that control the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. Although originally enacted in 1986, ECPA has been updated several times since, with significant revisions occurring in both 1994 and 2001.

I intend to focus the majority of my testimony on the SCA, which contains three primary components that regulate the disclosure of certain communications and related data. First, section 2701 of Title 18 prohibits unlawful access to certain stored communications: anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Second, section 2702 of Title 18 regulates voluntary disclosure by service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates the government's ability to compel disclosure of both stored content and non-content information from a service provider; it creates a set of rules that all governmental entities must follow in order to compel disclosure of stored communications and other records.

Since its inception, the SCA has served multiple purposes. It provides the rules governing how providers of communications services disclose stored information—including contents of communications, such as the body of an email, and non-content information—to a wide variety of government entities. In doing so, it imposes requirements on the government and providers to ensure that the privacy of individuals is protected. The statute thus seeks to ensure

public safety and other law enforcement imperatives, while at the same time ensuring individual privacy. It is important that efforts to amend the SCA remain focused on maintaining both of these goals.

I. The Stored Communications Act Has a Broad Scope

Any consideration of the SCA must begin with an understanding of the statute's extremely broad scope. The paradigm that generally comes to mind in discussions of the SCA is a law enforcement agency conducting a criminal investigation and seeking a target's email from a service provider that makes its services available to the public. And, indeed, the SCA is critical to all sorts of criminal investigations into murder, kidnapping, organized crime, sexual abuse or exploitation of children, identity theft, and more. As technology has advanced, appropriate governmental access to certain electronic communications, including both content and non-content information, has become even more important to upholding our law enforcement and national security responsibilities.

Even within these criminal investigations, it is important to understand the kind of information that the government obtains under the SCA as well as how that information is used. Under the SCA, the government may compel service providers to produce both content and non-content information related to electronic communications. It is clear that the contents of a communication—for example, a text message related to a drug deal, an email used in a fraud scheme, or an image of child pornography—can be important evidence in a criminal case. But non-content information can be equally important to building a case.

Generally speaking, service providers use non-content information related to a communication to establish a communications channel, route a communication to its intended destination, or bill customers or subscribers for communications services. Non-content information about a communication may include, for example, information about the identity of the parties to the communication, and the time and duration of the communication. During the early stages of an investigation, it is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity. Importantly, non-content information gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant. Without a mechanism to obtain non-content information, it may be impossible for an investigation to develop and reach a stage where agents have the evidence necessary to obtain a warrant.

For example, the SCA has been critical to tracking down violent criminals. In one case, a suspected serial killer who had killed more than ten people sent an anonymous letter to a newspaper reporter that identified the location of a victim's body with an "X" drawn on a map. Investigators recognized the mapping website on which the serial killer generated the map. They obtained from that website the IP address of the user who had generated the map and then used ECPA process served on the user's internet service provider to obtain the physical address of the subscriber who had visited the mapping website. Using this information, the FBI and local

police were able to arrest the suspect and stop his killing spree. ECPA process thus allowed law enforcement to trace an anonymous printout from the Internet back to the physical location of the target, in an extremely time-sensitive setting.

The SCA has broad effect in other ways as well. The statute applies not only to public and widely accessible service providers but also to non-public providers, such as companies or governments that provide email to their employees. Moreover, criminal investigations are only a subset of the circumstances in which the SCA applies. The statute applies to *all* government entities—federal, state, and local—when they seek to obtain content or non-content information from a service provider. This means that the statute also applies when the government is acting as a civil regulator—or even as an ordinary civil litigant. For instance, the SCA applies in all of the following circumstances that could arise, just within the Department of Justice:

- Civil Rights Enforcement: DOJ's Civil Rights Division brings a civil suit against a landlord who is sending racially harassing text messages to tenants. The target of the messages deletes them, and the landlord denies ownership of the account from which they were sent. The SCA governs the Division's ability to obtain those messages from the provider during civil discovery.

- False Claims Act: The DOJ Civil Division investigates a business for submitting fraudulent claims to the Federal government. The Division has reason to believe that the defendant's employees used email messages sent via the business's customer service email accounts to orchestrate the fraud. However, the defendant claims that it did not use email for business purposes. The SCA governs the ability of the Division to compel the internet service provider that hosted the company's website to disclose the contents of the business's email account.

- Environmental Litigation: The Department's Environment and Natural Resources Division brings a civil enforcement suit under the Superfund statute, a company relevant to the litigation has gone bankrupt, and the company's cloud provider has the only copies of that company's relevant corporate email. The SCA governs the Division's ability to obtain that email during civil discovery.

- Antitrust Investigations: The Department's Antitrust Division is conducting a civil investigation of several companies for engaging in an unlawful agreement to restrain trade. During the course of the investigation, DOJ attorneys discover that executives of those companies are using their personal email accounts to continue communications about the agreement. The SCA governs the Division's ability to obtain that email from the service provider.

- Tax Enforcement: The DOJ Tax Division investigates a tax preparation service that advertises via social networking sites. The company fraudulently inflates the amount of refunds due to the taxpayer and profits from taking a significant share of the fraudulent

refund. Based on complaints about the preparer, the social networking site closes the company's account. The SCA governs the Tax Division's ability to obtain the posts advertising the company's tax preparation services.

During any discussions of possible changes to the SCA and ECPA more broadly, it is important to keep in mind its wide-ranging application and scope.

II. Modernizing the Rules for Compelled Disclosure of Email and Other Similar Stored Content Information

As I mentioned, ECPA was originally enacted in 1986—a time when the internet was still a nascent technology and landline telephones predominated. Although ECPA has been updated several times since its enactment, the statute—and specifically the portion of the SCA addressing law enforcement's ability to compel disclosure of the stored contents of communications from a service provider—has been criticized for making outdated distinctions and failing to keep up with changes in technology and the way people use it today.

Many have noted—and we agree—that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.

Acknowledging that the so-called "180-day rule" and other distinctions in the SCA no longer make sense is an important first step. The harder question is how to update those outdated rules and the statute in light of new and changing technologies while maintaining protections for privacy and adequately providing for public safety and other law enforcement imperatives.

Personal privacy is critically important to all Americans—including those of us who serve in the government. It is also of increasing importance to individuals around the world, many of whom use communications services provided by U.S. companies. All of us use email and other technologies to share personal and private information, and we want it to be protected appropriately. We also know that companies in the United States and elsewhere depend on privacy as a driver of innovation and competitiveness. Some have suggested that the best way to enhance privacy under the SCA would be to require law enforcement to obtain a warrant based on probable cause to compel disclosure of stored email and similar stored content information from a service provider. We appreciate the appeal of this approach and believe that it has considerable merit, provided that Congress consider contingencies for certain, limited functions for which this may pose a problem.

For example, civil regulators and litigators do extremely important work. But they typically are investigating conduct that, while unlawful, is not a crime. Criminal search warrants are only available if an investigator can show probable cause that a crime has occurred. Lacking

warrant authority, civil investigators enforcing civil rights, environmental, antitrust, and a host of other laws would be left unable to obtain stored contents of communications from providers. As increasing amounts of information are stored electronically, the amount of information that would be unobtainable to government regulators and litigators will only increase. It is also not the case that these civil regulators and litigators can ask criminal law enforcement officers to obtain a warrant on their behalf. For them to do so would be inappropriate because it would require the opening of a criminal investigation—a step that would be impermissible unless the underlying conduct appeared to be criminal in nature.

Nor could civil litigators and regulators reliably obtain email and other content information solely by serving a subpoena directly on a subscriber (rather than a provider). As several of the examples described above demonstrate, serving a subpoena on a provider may be the only way for civil law enforcement to obtain certain stored communications. For example, where the subscriber no longer exists—as in the case of a bankrupt corporation or a deceased individual—or a purported subscriber denies ownership of the communications and therefore refuses to comply with a subpoena, civil litigators and investigators without the ability to subpoena a provider would be unable to obtain relevant evidence. Moreover, many individuals who violate the law may be tempted to destroy their communications rather than turn them over. Serving a subpoena on the individual, rather than the provider, could serve to encourage such illegal obstruction of justice. Thus, it is important that any proposed changes to ECPA take into account the ability of civil regulators and litigators to compel disclosure of information from providers.

Reform efforts must also account for existing practices as to entities, such as corporations, that provide email to their employees. Investigations of corporate malfeasance—both civil and criminal—have long been conducted by subpoena. For example, it is settled law that a government investigator may use a subpoena to obtain corporate records such as memoranda, letters, or even printed emails. It would be anomalous for the SCA to afford greater protection to electronic corporate records than to the identical records in hard copy. In fact, the voluntary disclosure provision of the SCA already recognizes that this context is different: non-public providers may voluntarily disclose user communications without restriction. To be clear, it is decidedly not our view that subpoenas are blanket substitutes for warrants. But, in the narrow context of corporate investigations, it is important to remember that subpoenas are the norm for obtaining business records, and creating a different standard for different means of communications would hamper many such investigations.

Efforts to update ECPA can account for these considerations and, at the same time, incorporate strong mechanisms that protect individual privacy and ensure appropriate judicial oversight of government access to individual's communications.

III. The Need for Additional Updates to the SCA and ECPA

Although discussions about updating ECPA have often focused on the standard for governmental access to stored content information, we also believe there are a number of other

parts of the statute that may merit further examination during any process updating and clarifying the statute.

(A) Clarifying Exceptions to the Pen Register Statute

First, Congress could consider clarifying the exceptions to the Pen Register statute. The Pen Register statute governs the real-time collection of non-content "dialing, routing, addressing, or signaling information" associated with wire or electronic communications. This information includes phone numbers dialed as well as the "to" and "from" fields of email. In general, the statute requires a court order authorizing such collection on a prospective basis, unless the collection falls within a statutory exception. The exceptions to the Pen Register statute, however, are not coextensive with the exceptions to the Wiretap Act. This creates an unnecessarily complicated scheme where non-content information associated with a communication is subject to more extensive protection than the content itself. Congress could consider harmonizing the exceptions in these two sections of the statute. Moreover, the Pen Register Act's consent provision could helpfully be clarified to allow the user to provide direct, express consent for implementation of a pen/trap device by the government.

(B) Clarifying the Standard for Issuing 2703(d) Orders

Second, Congress could consider clarifying the standard for the issuance of a court order under § 2703(d) of the SCA, which can be used by criminal law enforcement authorities to compel disclosure of various types of stored records. According to that provision of the statute, "[a] court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the [records] sought are relevant and material to an ongoing criminal investigation."

Until recently, no court had questioned that the United States was entitled to a 2703(d) order when it made the "specific and articulable facts" showing specified by § 2703(d). However, the Third Circuit has held that because the statute says that a § 2703(d) order "may" be issued if the government makes the necessary showing, judges may choose not to sign an application even if it provides the statutory showing. *See In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit's approach makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not.

(C) Treating Civil Discovery Subpoenas Like Other Subpoenas

Third, Congress could consider ensuring that—where and to the extent subpoenas are already an acceptable means of obtaining information—courts treats civil discovery subpoenas just like they already treat grand jury subpoenas, trial subpoenas, and administrative subpoenas, in order to avoid unnecessarily impeding the government's ability to conduct civil litigation.

(D) Making the Standard for Non-content Records Technology-Neutral

Fourth, Congress could consider modernizing the SCA so that the government can use the same legal process to compel disclosure of addressing information associated with modern communications, such as email addresses, as the government already uses to compel disclosure of telephone addressing information. Historically, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA endorsed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Therefore, while law enforcement can obtain records of calls made to and from a particular phone using a subpoena, the same officer can only obtain "to" and "from" addressing information associated with email using a court order or a warrant, both of which are only available in criminal investigations. This results in a different level of protection for the same kind of information (*e.g.*, addressing information) depending on the particular technology (*e.g.*, telephone or email) associated with it. Congress could consider updating the SCA to set the same standard for addressing information related to newer technologies as that which applies in traditional telephony.

(E) Clarifying that Subscribers May Consent to Law Enforcement Access to Communications Content

Fifth, Congress could consider clarifying the consent provision of the SCA. Under section 2702, a provider *may* disclose the contents of communications with the consent of a user or customer, but the provider is not required to do so. This has the impact of allowing the provider to overrule its customer's direction to disclose content associated with the customer's account. Thus when the victim of a crime seeks to share his or her own emails or other messages that may provide evidence, providers can refuse to disclose that information to law enforcement, even when provided with a written release from the account owner or subscriber.

(F) Appellate Jurisdiction for Ex Parte Orders in Criminal Investigations

Sixth, Congress could consider clarifying that higher courts have appellate jurisdiction over denials of warrants or other ex parte court orders in criminal investigations. Under existing law, the government may have no mechanism to obtain review of the denial of a court order or search warrant, even when the denial is based primarily on questions of law rather than questions of fact. Congress may wish to consider clarifying that these denials are appealable so that the disagreements among courts are resolved and the law becomes standardized.

* * *

In conclusion, I would like to reemphasize that in discussing any efforts to modernize ECPA, it is important to take into account the statute's broad application. As technology

continues to advance, ECPA's importance to both criminal and civil law enforcement will only increase.

The Department of Justice stands ready to work with the Subcommittee as it considers potential changes to ECPA. We appreciate the opportunity to discuss this issue with you, and we look forward to continuing to work with you.

This concludes my remarks. I would be pleased to answer your questions.

Before the

Committee on the Judiciary

Subcommittee on Crime, Terrorism, Homeland Security and Investigations

Rayburn House Office Building Room 2141

Washington, D.C. 20515

HEARING ON ECPA PART 1: LAWFUL ACCESS TO STORED CONTENT

March 19th, 2013

Written Testimony
of
Richard Littlehale
Assistant Special Agent in Charge
Technical Services Unit
Tennessee Bureau of Investigation

Chairman Sensenbrenner, Ranking Member Scott, and members of the subcommittee, my name is Richard Littlehale, and I am the Assistant Special Agent in Charge of the Technical Services Unit of the Tennessee Bureau of Investigation. We are the high-tech investigative unit of Tennessee's statewide criminal investigation agency. One of my unit's most important responsibilities is to help law enforcement agencies at all levels of government throughout Tennessee use communications records in support of their criminal investigations. I have used these techniques for the better part of eighteen years in support in cases ranging from searches for violent fugitives to efforts to recover abducted children.

I am grateful to the subcommittee for giving me the opportunity to share a law enforcement electronic surveillance practitioner's perspective on how access to stored communications evidence can be invaluable in the most critical of law enforcement investigations, and how improvements in the law can help my colleagues and I work faster and more efficiently to bring the guilty to justice and exonerate the innocent. My fellow practitioners and I especially appreciate the signal sent by your invitation to today's hearing, because state and local law enforcement conducts the vast majority of investigations in this country. Our community appreciates your recognition that our expert perspective should be a central consideration of any update to ECPA.

I offer testimony here today both on behalf of my agency, and as a representative of the Association of State Criminal Investigative Agencies (ASCIA), led by President Ron Sloan, the Director of the Colorado Bureau of Investigation. My agency's chief executive, TBI Director Mark Gwyn, is a member of ASCIA's Executive Board and a member of ASCIA's Technology Committee. He and the ASCIA Technology Committee chairman Steve Schierholt, Assistant Superintendent of the Ohio Bureau of Criminal Investigation, have asked me to serve as the ASCIA's subject matter expert on issues such as those before this subcommittee today.

Access to Evidence in the Digital Crime Scene

The crime scene of the 21st century is filled with electronic records and other digital evidence. The contents of this digital crime scene, including electronic communications records, often hold the key to solving the case. They also hold the key to ruling out suspects and exonerating the innocent. Law enforcement's ability to access those records quickly and reliably under the law is fundamental to our ability to carry out our sworn duties to protect the public and ensure justice for victims of crime.

To date, much of the scholarly and media attention given to the question of lawful access to stored content has focused almost entirely on the level of proof required for law enforcement to obtain it, and to a lesser extent on accountability considerations like customer notification and reporting requirements. From the law enforcement perspective, a set of concerns that is critical to our ability to use these records has been largely absent from the ECPA reform debate. If Congress desires to update ECPA, it must do so in a way that addresses these concerns.

The simple truth is that legal barriers are not the only ones that keep communications records out of law enforcement hands. In many instances, we are unable to utilize evidence that would be of enormous value in protecting the public because the technologies used to carry and store that information are not accessible to us, no matter what legal process we obtain. That may be because of technological problems, but even more frequently it is because of logistical hurdles. The companies that retain these records are many times unable or unwilling to respond to law enforcement's lawful demands in a timely manner. The primary emergency disclosure provision in the section of ECPA that we use to obtain stored content is voluntary for the providers, not mandatory, and even where emergency access is granted to law enforcement, in some instances, there is insufficient service provider compliance staff to process legitimate emergency requests quickly.

If you or a member of your family were a victim of a crime, and law enforcement needed timely access to electronic communications records to identify and apprehend the offender, would you be satisfied with this reality?

As Congress considers simplifying the legal requirements for obtaining communications records, and whether or not to change the standards law enforcement must meet to obtain those records, these other barriers to access must have a place in the discussion. **I urge Congress to ensure that regardless of the level of process it ultimately decides is appropriate, steps are taken to guarantee that law enforcement will be able to access the required communications transactional records reliably and quickly once that process is obtained.**

As we consider various law enforcement concerns, we must keep in mind a simple fact that is nevertheless often overlooked in the public discourse on this topic: we are talking about law enforcement's ability to gather *evidence*. Not "information" or "content" or "communications records," but *evidence*. All hammers are tools; a hammer only becomes *evidence* if it is relevant to a criminal investigation. Similarly, law enforcement has no interest in communications records unless they advance a criminal investigation, whether to prove guilt or exonerate the innocent. The complete lack of a demonstrated

pattern of misuse or abuse by law enforcement to access electronic communications records bears out this truth.

A Law Enforcement Perspective on Lawful Access to Stored Content

Timeliness and quality of service provider response. The timeliness and quality of service provider responses to lawful demands is of primary importance to the law enforcement community. We continue to encourage a thorough review of constructive measures to enhance service provider responsiveness to legitimate law enforcement process requests to ensure that investigative timelines are as short as possible. That is what we owe to the citizens we protect. There is no requirement in current law – including search warrant practice – for providers to respond in a timely fashion to lawful process requests by governmental entities. Some providers routinely respond in a timely way, but others do not. This has resulted in unnecessary investigative delays that adversely impact public safety.

Any contemplated change in the law that would result in a lengthening of the investigative timeline – including moving to a probable cause standard where it is not currently required – should be accompanied by provisions that ensure accountability and prompt response by service providers to legitimate law enforcement requests. These responsiveness issues are important to address even in the absence of an enhanced standard.

Service providers will often cite the high volume of law enforcement requests as a reason for response times that stretch on into months, threatening the underlying investigation. They say they do not have the staff necessary to process the volume of requests more quickly. We would urge the committee to consider that many of these companies are in the business of finding technological solutions to just this sort of problem. Further, they are well acquainted with monitoring customer service centers and determining adequate staffing levels. It is not a matter of capability, but rather a matter of will. Responding to law enforcement legal demands costs service providers money and does not generate revenue, however, and so there is little financial incentive to innovate or increase staffing levels. Therefore, a reasonable legal mandate for responsiveness may be the best solution to this problem. Such a solution need not be overly costly or burdensome to the providers. In a time when Congress is reluctant to impose new regulations on private industry, I would argue that this is one type of regulation that has a clear positive impact for the public. It protects citizens and allows victims of crime to see justice done. It should be addressed in any reform of ECPA, and we look forward to working with the providers and this subcommittee to consider the best way forward.

Notification provisions may put a greater burden on law enforcement than an increased proof requirement. Several ECPA reform proposals have borrowed language from wiretap law requiring notification of customers of legal demands, or securing a series of separate court orders delaying notification. These provisions risk diverting critical law enforcement resources from investigations simply to comply with burdensome notification provisions or delay orders that do not offer any additional constitutional protections, and may actually threaten ongoing investigations. We urge the committee to carefully balance the need for notification and reporting against the resources it will drain away from a range of investigative priorities.

Concerns about the volume of law enforcement legal demands. As I address the issue of volume of legal process and its effect on timeliness of service provider response, I must also address a common talking point used by those who would further restrict law enforcement access to stored content: namely, that the number of law enforcement requests for this information is growing. Our response is simple: of course it is. That is because in the digital age, a growing percentage of the available evidence in any criminal case is going to exist in the digital crime scene. Communications records have taken their place alongside physical evidence, biological evidence, testimonial evidence, and the other traditional categories. Laws and policy should reflect this reality and ensure law enforcement access to evidence that by its nature can't make a mistaken identification in a lineup or testify untruthfully.

Google has provided an excellent example of how law enforcement demands truly relate to the new digital reality. Google now regularly publishes statistics on the number of government requests for information that it receives, broken down by the rate that it complies, proof standard, and a number of other factors. Public reporting on these statistical releases has tended to focus on the perception that law enforcement agencies are seeking access to this information at an excessive rate.

I applaud Google for this transparency initiative, but I believe some context is appropriate for the subcommittee's understanding. In June of 2012, Google claimed 425 million individual account holders for its Gmail product alone. In 2012, it reported receiving over 40,000 government requests for communications records worldwide, affecting about 68,000 users or accounts globally. In the U.S., Google reported a total of just over 16,000 government requests affecting just over 31,000 accounts. That means just a tiny fraction of one percent of Google's accounts were affected by government demands.

Consider that in the context of more than 17,000 law enforcement agencies in the United States. This means that on average, there was less than one request for information per law enforcement agency per year for Google

records. Contrast that with crime reporting statistics, which reflect that in 2011, more that 14,000 Americans were murdered, more than 83,000 were forcibly raped, and there were over 350,000 robberies. It is hard to conclude from these numbers that law enforcement demands for records are excessive.

My fellow professionals and I deal with cases like that every day, and stored communications are a critical part of the constellation of evidence that allows us to identify the guilty and keep the public safe. I encourage the committee to keep these numbers in mind when some parties claim that law enforcement is "snooping" without regard to privacy. When we request these records, it is for a reason – we believe that the records constitute evidence that will lead to identification of sexual predators, the recovery of kidnapping victims, or the successful prosecution of a murderer. Any consideration of changes to ECPA that will make obtaining communications records more time-consuming and laborious should reflect an understanding of how those changes will impact our ability to do our job, and whether or not the public would truly be upset about the balance as it is currently struck.

Current emergency provisions within ECPA are not adequate to allow law enforcement to respond effectively in all cases. Few dispute that law enforcement should have rapid access to communications records in a life-threatening emergency, but few outside of our community truly understand how flawed the current emergency options are. The "emergency" provision in current law (18 USC 2702(b)(8)) puts the decision to release records before legal process is obtained, and about whether a situation is an "emergency," in the hands of the provider, rather that the law enforcement experts with their boots on the ground. This has led to situations where responses to legitimate law enforcement requests have been delayed. In some cases, providers make a decision never to provide records in the absence of legal process, no matter the circumstances.

We would further point out that 18 USC 2258, which has been erroneously cited as an emergency option for law enforcement in child exploitation cases, is in fact a requirement that service providers send information about online child exploitation to the National Center for Missing and Exploited Children. Law enforcement cannot use it as a means to obtain records directly. The service providers still require legal process or an emergency declaration under 2702 before they will provide the evidence that generated the referral to law enforcement.

Records retention is an issue that should be considered in any effort to update ECPA. Certain types of widely used electronic communications are not retained by some providers, which can hinder law enforcement investigations. In particular, most cellular service providers do not retain stored

text messages accessible to law enforcement for any time at all. Billions of texts are sent every day, and some surely contain key evidence about criminal activity. In some cases, this means that critical evidence is lost. Text messaging often plays a big role in investigations related to domestic violence, stalking, menacing, drug trafficking, and weapons trafficking. I am well aware that retention means a cost for service providers. I would urge Congress to find a balance that is not overly burdensome to service providers, but that ensures that law enforcement can obtain access to critical evidence with appropriate legal process for at least some period of time.

Preservation provisions under current law should be revisited to ensure that law enforcement could prevent service providers from notifying customers of the existence of the request. Some proposals for ECPA reform would cause prior notification to law enforcement before a provider notifies a customer or subscriber about the existence of a warrant, order, or subpoena, and we believe that provision is important. However, a similar provision relating to preservation should be considered. There are service providers who have stated a policy of notifying customers of any government inquiry unless they are in receipt of process ordering them not to do so. The principle behind their stance is laudable, but the real-world impact can be harmful to criminal investigations. Section 2705 offers a delay of notification scheme for court orders and subpoenas, but does not address preservation letters directly. If there is reason to believe that customer notification of the existence of a warrant, subpoena, or court order may result in:

1) endangering the life or physical security of an individual;
2) flight from prosecution;
3) destruction of or tampering with evidence;
4) intimidation of potential witnesses; or
5) otherwise seriously jeopardizes and investigation or unduly delays a trial,

then it seems that the ability to prevent early notification of the existence of a preservation letter issued in the early stages of an investigation with the intent to assemble a quantum of proof – such as probable cause – would be essential.

The definition of content must be clear and carefully considered. Definitions of "content" and "non-content" information need to be clear and comprehensive. Efforts to update ECPA should constrain the definition of content so that it does not expand over time to cover parts of an electronic communication that are ancillary to the actual purport, idea or intent of the writing, such as signaling, addressing, routing or URL information.

Any move to alter the standard of proof required to access stored content should be carefully considered in the broader context of the concerns identified above. If governing law is changed to require probable

cause for any type of location information, there will be a negative impact on the time required for law enforcement to conduct certain types of investigations. Some of this impact can be balanced by changes in the law with respect to records retention and quality of service in response to law enforcement legal demands. Any effort to modify the standard of proof for access to stored content that does not address the concerns outlined above will lengthen law enforcement's investigative timeline, and therefore reduce our effectiveness and negatively impact our ability to bring criminals to justice.

Conclusion

A robust debate about balancing personal privacy and security is beneficial to all Americans, but the people and their representatives must be able to make an educated judgment about what they are giving up and what they are getting. There is no question that a growing number of personal details about all Americans are moving around the digital world, and some of those details make their way into digital crime scenes. Just as there is no question that people have an interest in preserving the privacy of that information, there can be no question that some of that information holds the keys to finding an abducted child, apprehending a dangerous fugitive, or preventing a terrorist attack. Whenever we move forward with the privacy/safety debate, we should be mindful that any restriction of law enforcement's access to that information, whether by redefining legal barriers or allowing service providers to erect new technological barriers, may well come at a price, and some of that price could be paid by our most vulnerable citizens. We should be sure we are willing to require them to pay it.

The thousands of law enforcement officers across this country who utilize communications evidence in the course of their duties recognize that we are guardians of a free society, a society that embraces in its founding law the decision to elevate the rights of the individual above incremental increases in public safety. The truth is that no one has put forward any evidence of pervasive law enforcement abuse of ECPA provisions. Law enforcement professionals also recognize that times are changing, and as a profession we are moving forward to utilize all available evidence in a responsible and effective way.

Ours is also a society that requires an open exchange of ideas on topics critical to the public interest, however, and we believe that the ECPA reform debate has been largely one-sided to date. As I hope to have shown, redrafting the laws governing law enforcement access to communications records raises significant implications for law enforcement's ability to protect the public. I urge the members of this subcommittee to ensure that the law enforcement community is given the opportunity to continue to share its perspective on the

potential human implications of any proposed reform of the Electronic Communications Privacy Act, so that all the competing factors may be balanced appropriately.

I have always been proud of the Tennessee Bureau of Investigation motto, borrowed from the United States Supreme Court in Berger v. United States. It seems particularly appropriate in this context. The evidence in the digital crime scene, now more than ever, will help law enforcement to ensure "that guilt shall not escape, nor innocence suffer."

Thank you for the invitation to testify and I look forward to working with you on these important issues.

United States House of Representatives
Subcommittee on Crime, Terrorism, Homeland Security and Investigations

"ECPA Part 1: Lawful Access to Stored Content"
Tuesday, March 19, 2013
2141 Rayburn House Office Building, 10:00 a.m.

WRITTEN STATEMENT OF ORIN S. KERR
FRED C. STEVENSON RESEARCH PROFESSOR
GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

It is my pleasure to testify this morning about the Electronic Communications Privacy Act ("ECPA"), and specifically about the provisions of ECPA that regulate government access to stored contents held by Internet providers. In my view, these important provisions are badly flawed and badly outdated.

My testimony will focus on five major problems with the statute governing access to stored contents under ECPA. First, the statute provides very weak protection for contents of communications held for more than 180 days. Second, the statute appears to offer no protection for search engine queries. Third, the scope of the statute's warrant protection is uncertain. Fourth, part of the existing statute does not satisfy the Fourth Amendment. And fifth, the statute imposes no requirements of minimization, particularity, or non-disclosure for contents obtained under its provisions.[1]

These five problems point to a pressing need for Congress to revisit ECPA's provisions on lawful access to stored contents. My testimony will begin by summarizing the existing provisions of the law as they were enacted in 1986. I will then turn to the five major problems with those provisions from the perspective of 2013.

[1] Parts of my testimony are adapted from a forthcoming article on ECPA reform that will be published in Volume 162 of the *University of Pennsylvania Law Review.*

Understanding ECPA's Current Provisions on Compelled Access to Contents of Communications

The provisions of ECPA governing lawful access to stored content are found in 18 U.S.C. § 2703(a)-(b), which was enacted in 1986. These provisions create statutory privacy rights for "subscribers or customers" of two kinds of computer network services that existed at the time. The first kind of service is an "electronic communications service" provider ("ECS"), which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Translated into plain English, an ECS is any service that provides connectivity, e-mail, or text messaging services. 18 U.S.C. § 2703(a) identifies the rules that the government must follow to compel contents of communications held by ECS providers. According to its provisions, the government needs a warrant to compel contents from an ECS provider if the contents have been stored for 180 days or less. If the contents have been stored for more than 180 days, however, the government can use lesser process pursuant to 18 U.S.C. § 2703(b).

The second type of Internet service regulated by the law is a "remote computing service" ("RCS"), defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). In layman's terms, an RCS is a remote storage service that any member of the public can use, such as a cloud storage service. 18 U.S.C. § 2703(b) offers three ways that the government can compel contents held by an RCS or contents held by an ECS for more than 180 days. First, investigators can use a subpoena with either prior notice or delayed notice. Second, investigators can use a "specific and articulable facts" court order under 18 U.S.C. § 2703(d) with either prior notice or delayed notice. Third, investigators can use a warrant to obtain contents and do not need to satisfy a notice requirement.

Problem 1: No Warrant Protection for Storage More Than 180 Days

The current language of 18 U.S.C. § 2703(a)-(b) has five major problems. The first problem is that the statute does not require a warrant for remotely–stored contents held for more than 180 days. The government can compel contents held for more than 180 days with a mere subpoena. This is a strange result because most people use their e-mail accounts as a permanent storage site akin to a virtual home online. According to one recent report, a typical

user of the popular Gmail e-mail service stores more than 17,000 e-mails in her account at any given time.[2] Almost 12,000 of those e-mails are received e-mails stored in the inbox, and almost 6,000 are sent e-mails directed elsewhere.[3] It is likely that most of those communications have been stored for more than 180 days. Under ECPA, however, only e-mails stored 180 days or less can receive statutory warrant protection. Anything stored for a longer time can be accessed by the government without a warrant. I find that aspect of the statute impossible to justify. It is a puzzling result that makes no sense for today's Internet and today's Internet users.

Problem 2: No Protection for Search Engine Requests

A second problem with the current statute is that private communications held by Internet services that do not fit within the definition of ECS or RCS receive no protection at all. Search engine requests provide the most important example. According to one study, search engines analyzed about 18.4 billion search requests from the United States in the month of March 2012 alone.[4] Search engine requests can reveal a person's innermost thoughts, and as a result such requests contain highly sensitive information. But it appears likely that search queries stored with services like Google are not protected under current law because they provide neither ECS nor RCS.

Search engines plainly do not provide ECS. They are destinations for communications, not providers of connectivity or messaging. And search queries do not appear to provide RCS, either. Recall that a remote computing service is defined by ECPA as a service that provides the public "computer storage or processing services by means of an electronic communications system."[5] Users do not send their search queries to search engines for storage purposes. Storage is a bug for users, not a feature. Whether ECPA protects search queries therefore hinges on whether search engines provide "processing services." The relevant text and legislative history suggests that they do not. In the

[2] *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, Wired, available at http://www.wired.com/insights/2012/07/gmail-account-worth/

[3] *See id.*

[4] *See* Press Release, *comScore Releases March 2012 U.S. Search Engine Rankings*, http://www.comscore.com/Insights/Press_Releases/2012/4/comScore_Releases_March_2012_U.S._Search_Engine_Rankings

[5] 18 U.S.C. § 2711(2).

context of computer data, the word "process" suggests operations on that data rather than a response to a query. The Senate Report accompanying ECPA clarifies the point: remote processing meant the outsourcing of tasks, such as number-crunching, that a computer of the 1980s might not be able to complete easily.[6] Search engines do not appear to fit the mold, as users do not use search engines as substitutes for the storage or processing powers of their own machines. For those reasons, it appears that likely that search engine queries are not protected by current law. The issue is not free from doubt, and courts have not ruled definitely on the issue.[7] But it appears that likely that search queries receive no statutory protection at all from the compelled storage provisions of ECPA.

Problem 3: The Scope of the Warrant Requirement Is Uncertain

A third important problem with the current statute is its uncertain scope. The most important example is opened e-mail stored for 180 days or less. Courts are presently divided on whether opened e-mails stored on a server will generally be covered by the ECS rules (which require a warrant) or the RCS rules (which do not). The source of the difficulty is the complex definition of "electronic storage" in 18 U.S.C. § 2510(17), which is critical because

---

[6] The Senate Report accompanying the passage of ECPA offered the following explanation of the concept of a "remote computing service" :

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer.

S. Rep. No. 99-541 (1986), at 10-11.

[7] Notably, Google has claimed that its search engine queries are covered by ECPA on the ground that it provides RCS. In litigation over the disclosure of Google search queries, Google made the following argument that its services are protected by the SCA:

> Google processes search requests as directed by, and for, its users who in turn retrieve the search results of their choosing from Google's index, or Google sends the results by email or text messages to individuals, to wireless phones or other designated mobile devices. Said in plain language, users rely on the remote computer facilities of Google to process and store their search requests and to retrieve by electronic transmission their search results.

See Google's Opposition to the Government's Motion to Compel in Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006), available at 2006 WL 543697.

only contents in "electronic storage" receive ECS protections. Some courts read the definition to include opened e-mails in the statute's ECS coverage on the theory that they are copies of e-mails stored "for backup purposes" under § 2510(17)(b). *See Theofel v. Farey–Jones*, 359 F.3d 1066, 1075-76 (9th Cir. 2004). On the other hand, other courts have concluded that opened e-mails are not covered by the ECS rules but rather are covered under the RCS rules on the theory that a user stores opened e-mails like other remotely stored files. The disagreement is presently the subject of a petition for certiorari before the United States Supreme Court seeking review of a decision from the Supreme Court of South Carolina. *See Jennings v. Jennings*, 736 S.E.2d 242 (S.C. 2012).[8]

Problem 4: The Statute Fails to Satisfy the Required Constitutional Standard

The fourth problem is the Fourth Amendment – or, more specifically, the statute's failure to measure up to constitutional standards. Existing lower court caselaw indicates that the provisions of 18 U.S.C. § 2703(b) fail to satisfy constitutional standards because they allow the government to obtain access to the contents of communications with less protection than a warrant based on probable cause. The leading case is *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), a Sixth Circuit decision involving government access to e-mails held by Yahoo!. Investigators relied on 2703(b) to subpoena Yahoo! for the contents of stored e-mails relating to a criminal enterprise. Yahoo! complied, and it gave investigators copies of thousands of e-mail messages without a warrant. The Sixth Circuit held that obtaining the contents of e-mails without a warrant was unconstitutional because users have a reasonable expectation of privacy in their e-mails just like their letters and phone calls. As a result, the provision of the SCA permitting the government to obtain e-mails with less process than a warrant did not satisfy the required Fourth Amendment standard. *See id.* at 288 ("[T]o the extent that the SCA purports to permit the government to obtain such emails warrantlessly, [that portion of] the SCA is unconstitutional.").

A number of courts have agreed with the Sixth Circuit since *Warshak*, including federal courts in Kansas[9] and the District of Columbia,[10] and the state of Washington Court of

[8] The Petition for Certiorari, Brief in Opposition, and an amicus brief filed before the United States Supreme Court are available at http://www.scotusblog.com/case-files/cases/jennings-v-broome/.

[9] In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917 at *5 (D.Kan. 2012) ("The Court finds the rationale set forth in *Warshak* persuasive and therefore

Appeals.[11] Other courts have applied *Warshak* to find a reasonable expectation of privacy in stored Facebook messages,[12] text messages,[13] faxes,[14] and password-protected websites.[15] The case law is not entirely settled, to be sure. Only one federal court of appeals has squarely addressed the issue. But the trend in the case law is to recognize fairly broad Fourth Amendment protection, backed by a warrant requirement, for stored contents such as e-mails.

Further, in my view *Warshak* is correct. Government access to remotely stored contents generally requires a warrant, meaning that the standards of § 2703(b) do not satisfy the constitutional floor provided by the Fourth Amendment. *See generally* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1017-31 (2010).

Problem 5: Disclosure to Law Enforcement Allows All Disclosure Without Limits

The fifth problem with the current statute is that permitted disclosure comes without limits. When a provider must disclose the contents of communications, there are no limits on how many contents it can disclose or what the government can do with the contents it receives. Recall that a typical Gmail user stores more than 17,000 e-mails in his account at any given time.[16] If the government obtains a subpoena or even a warrant requiring a provider to disclose contents in a suspect's account, current law contains no limits on what gets disclosed or used. The provider will send the government the entire contents of the

---

holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received thorough an electronic communications service provider.")

[10] United States v. Ali 870 F.Supp.2d 10 (D.D.C. 2012)

[11] State v. Hinton, 280 P.3d 476, 483(Wash.App. Div. 2 2012) ("While *Warshak* does not aid Hinton, its comparison of e-mails with traditional forms of communication is helpful and we adopt it to hold that text messages deserve privacy protection similar to that provided for letters.")

[12] R.S. ex rel. S.S. v. Minnewaska Area School Dist. No. 2149 --- F.Supp.2d ----, 2012 WL 3870868 at 12 (D.Minn. 2012).

[13] State v. Hinton, 280 P.3d 476, 483(Wash.App. Div. 2 2012) ("While Warshak does not aid Hinton, its comparison of e-mails with traditional forms of communication is helpful and we adopt it to hold that text messages deserve privacy protection similar to that provided for letters.")

[14] In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917 at *5 (D.Kan. 2012)

[15] United States v. D'Andrea, 497 F. Supp.2d 117, 121 (D. Mass. 2007).

[16] *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, Wired, available at http://www.wired.com/insights/2012/07/gmail-account-worth/

account. The government then has access to all of those contents. Investigators can scan through all of the contents of a person's digital life without limit.

To phrase this problem in legal jargon, the existing statutory provisions contain no requirement of particularity, minimization, or non-disclosure. Particularity requires the government to specify which records it is seeking. Minimization requires the government to set up a filtering system: One person can go through the records and pass on the pertinent communications to investigators. And non-disclosure rules limit what the government can do with communications it has obtained. The current statute contains no such limits. That absence may be explained by the statute's relatively ancient origin. In 1986, few remotely stored records were kept. But today it is common for computer users to store tens of thousands of records of their daily life online. Remote storage has become cheap, allowing users to store everything.

As a result, government access to stored records raises a needle-in-a-haystack problem. The current statute allows the providers to simply hand over the entire haystack to investigators. Investigators can then look through the haystack at their leisure without limits and can use or disclose whatever they find regardless of its relevance to the investigation. Given the highly sensitive information commonly found in a personal e-mail account, the statute should take more care to protect the non-pertinent communications that ordinarily will make up the bulk of the contents of communications found in an e-mail account. The Fourth Amendment may already impose some of these limits, and statutory authorities from the Wiretap Act adopt other limits when the government obtains a wiretap order.[17] The same protections should be written into the provisions for lawful access to stored content.

——

Thank you for the opportunity to testify. I look forward to your questions.

[17] *See, e.g.*, In re Applications for Search Warrants for Information Associated with Target Email Address, 2012 WL 4383917 (D. Kan. 2012) (imposing particularity requirements on a warrant for the contents of an e-mail account under the Fourth Amendment); *See* United States v. McGuire, 307 F.3d 1192 (9th Cir. 2002) (discussing minimization requirements for electronic communications under the Wiretap Act).

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.