ECPA (PART I): LAWFUL ACCESS TO STORED CONTENT

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MARCH 19, 2013

Serial No. 113–16

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

80–065 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
SPENCER BACHUS, Alabama
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
MARK AMODEI, Nevada
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
KEITH ROTHFUS, Pennsylvania

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

HOWARD COBLE, North Carolina
SPENCER BACHUS, Alabama
J. RANDY FORBES, Virginia
TRENT FRANKS, Arizona
JASON CHAFFETZ, Utah
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho

ROBERT C. "BOBBY" SCOTT, Virginia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MARCH 19, 2013

ECPA (PART I): LAWFUL ACCESS TO STORED CONTENT

TUESDAY, MARCH 19, 2013

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 10:02 a.m., in room 2141, Rayburn Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Goodlatte, Coble, Gohmert, Labrador, Scott, Conyers, Bass, Richmond, and Chu.

Staff present: (Majority) Caroline Lynch, Chief Counsel; Anthony Angeli; Counsel; Alicia Church, Clerk; (Minority) Bobby Vassar, Minority Counsel; Joe Graupensperger, Counsel.

Mr. SENSENBRENNER. The Subcommittee on Crime, Terrorism, Homeland Security, and Investigations will come to order.

The Chair recognizes himself for 5 minutes for an opening statement.

The Electronic Communications Privacy Act of 1986, or ECPA, is complicated, outdated, and largely unconstitutional. ECPA made sense when it was drafted, but the role of the Internet and electronic communications in our daily lives is vastly different now than it was during the Reagan administration. Needed reforms can better protect privacy and allow the growth of electronic communications in the economy without compromising the needs of law enforcement.

ECPA was drafted in 1986, the same year Fox News was launched. That year, President Reagan ordered a strike against Muammar Qaddafi. Arnold Schwarzenegger married Maria Shriver, and at this time in 1986, Mark Zuckerberg was 1 year old. The world is a different place. I think we all can agree on that. The 1986 law governing the Internet is like having a national highway policy drafted in the 19th century.

Today's hearing is the first in a series the Subcommittee will hold to examine ECPA. Today we will explore the needs of Government to access the contents of stored electronic communications and the level of judicial review currently required to obtain them.

ECPA was the necessary response to the emergence and rapid development of wireless communications services and electronic

communications in the digital era. At that time, electronic mail, cordless phones, and pagers were in their infancy.

The Federal wiretap statute has been limited to voice communications and addressed an area of communications for which there is a Fourth Amendment right to privacy. ECPA extended the wiretap provisions to include wireless voice communications and electronic communications such as e-mail and other computer-to-computer transmissions. It established a framework for law enforcement to obtain the content of communications.

The evolution of the digital age has given us devices and capabilities that have created conveniences for society and efficiencies for commerce, but they also have created convenience and efficiencies for criminals, as well as innovative new ways to commit crimes. Fortunately, new ways to detect and investigate crimes and criminals have also evolved.

At the intersection of all of these developments and capabilities are the privacy rights of the public, economic interests in expanding commerce, public policy of encouraging the development of even better technologies, and the legitimate investigative needs of law enforcement professionals.

We are eager to hear about the constitutional considerations that would require changes to the level of judicial review for access to stored communications. We must also consider the lawful access to stored content by the Government in civil litigation, particularly when the Government is a defendant.

Lastly, we must examine the effect that ECPA reform would have on investigations at the State and local levels.

Today's hearing will focus on the actual contents of electronic stored communications. Email content is the body of a private electronic communication transmitted from the sender to one or more recipients. The primary question is whether the Fourth Amendment protections apply and to what type of stored communications. Our ultimate goal is to enact reforms that will endure for decades. This will give everyone the certainty they need to move forward in the digital age.

It is no secret in the digital age privacy is harder to maintain, but Americans should not have to choose between privacy and the Internet. In 1986, if you wanted privacy, you might keep a personal document in the filing cabinet instead of posted on a cork bulletin board. Today, you would probably save the same document behind the password in the Google account rather than to post it on your Facebook wall.

But our expectations of privacy have not changed. The Fourth Amendment protects more than just Luddites. If our laws fail to recognize this, we needlessly risk stunting technological progress and economic growth.

I look forward to hearing from all of our witnesses today.

And I now recognize the Ranking Member, the gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Today the Subcommittee follows last week's hearing about cyberthreats and our computer crime laws with a hearing about privacy of stored electronic communications content. Whether the issue is countering the use of computers to commit crime or setting

standards for law enforcement's access to stored electronic information in order to investigate crime, the pace of the technology change has exceeded the limits of our statutes in these areas.

The Electronic Communications Privacy Act, a statute designed in 1986 to govern law enforcement's access to the then emerging electronic and wireless technologies, is now outdated. Because of the growth of the Internet and related technologies, most of our private communications and other sensitive information are transmitted online and are stored in computer networks. To the extent that this has taken place and the ways in which technologies have evolved, that was not envisioned by Congress when we adopted the current statute. The result is that the standards for compelled disclosure under the statute are not adequate and their application is inconsistent.

For example, under the statute a single e-mail or electronic document could be subject to multiple legal standards in its lifetime from the moment it is typed to the moment it is opened by the recipient or uploaded into a user's account in the cloud where it may be subject to an entirely different standard. This occurs because content may be stored in places governed by different statutory definitions from moment to moment.

While a warrant is required to access the content of e-mails while it waits in electronic communications service storage to be read by the recipient, the instant the e-mail is opened by the recipient, it may lose that high standard of protection and become accessible by subpoena rather than by a warrant.

Also, following the disclosure rules can prove difficult if the service provider is unsure whether the data is stored by an electronic communications service or a remote computing service. Indeed, the distinction is made somewhat confusing because most network services are multi-functional. They can act as providers of a communications service in some context or a remote service in others and neither in still others. And to address these concerns, we need clarity, fairness of application, and appropriate protection of the privacy rights expected by our citizens.

So I look forward to our discussion today from the various people who have an interest in this, and I thank you for holding the hearing.

Mr. SENSENBRENNER. Thank you, Mr. Scott.

The Chair now recognizes the gentleman from Virginia, Mr. Goodlatte, the Chair of the full Committee.

Mr. GOODLATTE. Thank you, Chairman Sensenbrenner. I appreciate your holding this hearing.

The dawn of the digital age and the explosive development of communication methods have 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 United States Constitution.

The Electronic Communications Privacy Act 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 spend many hours each day online. In this context, a person's electronic communications encompass much more 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 is 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.

And I yield back to the Chairman.

Mr. SENSENBRENNER. Thank you, Mr. Goodlatte.

The Chair now recognizes the Chairman emeritus and Ranking Member of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Chairman Sensenbrenner, Members of the Committee, we have heard in opening statements that we are all for

modernizing. This hearing could be very important with our witnesses telling us what kind of modernization do we want. That is where this is all going, and I am glad to hear both the Chairman of the Committee and the Chairman of the Subcommittee hit those points along, of course, with our Ranking minority Member, Mr. Scott.

I have a list of Digital Due Process Coalition members, some 80 or more organizations that are with us on this, and I would like unanimous consent to include this in the record.

Mr. SENSENBRENNER. Without objection.

[The information referred to follows:]

List of Digital Due Process Coalition Members

American booksellers Foundation for Expression

American Civil Liberties Union

ACT (international grassroots advocacy and education organization which represents more than 5,000 small and mid-size app developers and information technology firms)

Adobe

American Legislative Exchange Council

Amazon.com

American Library Association

Americans for Tax Reform

AOL

Association of Research Libraries

AT&T

Automattic

Autonet Mobile

Bill of Rights Defense Committee

Brennan Center for Justice

BSA

Campaign for Liberty

Computer and Communications Industry Association

Center for Democracy and Technology

Center for Financial Privacy and Human Rights

Center for National Security Studies

Century Link

Citizens Against Government Waste

Common Sense Media

Competitive Enterprise Institute

The Constitution Project

Consumer Action

Data Foundry

Distributed Computing Industry Association

Dell

Diaspora

Discovery Institute

Dropbox

eBay

Educause

Electronic Frontier Foundation

Engine Advocacy

Evernote

Facebook

Future of Privacy Forum

FreedomWorks

Google

Hackers and Founders

Hattery Labs

Hewlett Packard

Interactive Company

International Business Machines

Inflection

Integra Telecom

Intel

Intelius

Internet Association

Internet Infrastructure Coalition

Intuit

Information Technology and Innovation Forum

Joint Center for Political and Economic Studies

Lean Startup Forum

Liberty Coalition

Linden Lab

LinkedIn

Microsoft

Newspaper Association of America

The National Workrights Institute

NetCoalition.Com

Neustar

Open Technology Institute

Oracle

Personal

RStreet

Reddit

Records Preservation and Access Committee

Salesforce.com

Software & Information Industry Association

Sonic.net

TMobile

Tech America

Tech Freedom

TechNet

TechStars

Telecommunications Industry Association

TRUSTe

Twitter

US Chamber of Commerce

Vaporstream

500 different start-up companies

Individuals:

Patricia Bellia, Notre Dame Law School
David Berger, Wilson, Sonsini Goodrich & Rosati
Michael Carroll, American University, Washington School of Law
Fred Cate, Indiana University Law School
Danielle Keats Citron, University of MAryland School of Law
Ralph D. Clifford, University of Massachusetts School of Law
Susan Crawford, Universtiy of Michigan Law School
Susan Freiwald, University of San Francisco Law School
Eric Goldman, Santa Clara University School of Law
David Gray, Univeristy of Maryland Law School
James Grimmelmann, New York Law School
Robert A. Heverly, Michigan State University College of Law
Charles H. Kennedy, Wilkinson Barker Knauer, LLP
Liza Barry-Kessler, Privacy Counsel LLC
Mark A. Lemley, Stanford Law School
Jennifer Lynch, UC Berkeley Law School
Rebecca MacKinnon, Center for Information Technology Policy, Princeton University
Deirdre Mulligan, UC Berkeley iSchool
Dan Hunter, Hunter
Paul Ohm, Professor of Law, University of Colorado
Scott Parsons, Portland State University
Frank A. Pasquale, Seton Hall Law School
David G. Post, Beasley School of Law, Temple University
Ira Rubinstein, NYU Law School
Pam Samuelson, UC Berkeley Law School and iSchool
Peter Scheer, First Amendment Coalition
Katherine J. Strandburg, New York University Law School
Jennifer Urban, UC Berkeley Law School
Michael Zimmer, School of Information Studies, University of Wisconsin-Milwaukee
Marc Zwillinger, Zwillinger Genetski LLP

Mr. CONYERS. Thank you.

And I conclude by raising the two issues that I will be looking at most carefully, one, that the standard of probable cause should apply to the Government's ability to compel a communications provider to disclose the customer's e-mail message no matter how old the message is. And we have got the Warshak case that has now come down. It makes no sense for the Government to need a subpoena to obtain e-mail messages that are older than 180 days.

And finally, the law does not adequately protect communications stored in the cloud by third parties on behalf of consumers. And a probable cause warrant should be required for Government access.

These are very important considerations, and I think we will be observing the Fourth Amendment, the right to be free from unreasonable searches and seizures, and still move into the 21st century.

I thank the Chairman, and I return any unused time.

Mr. SENSENBRENNER. Thank you, Mr. Conyers.

We have a very distinguished panel today, and I will begin by swearing in our witnesses before introducing them. So could all of you please stand and raise your right hands?

[Witnesses sworn.]

Mr. SENSENBRENNER. Let the record show that each of the witnesses answered in the affirmative.

The first witness is Ms. Tyrangiel who currently serves as the Assistant Attorney General for the Office of Legal Policy. She joined OLP in 2009 and has served in various roles since then, including chief of staff, deputy assistant attorney general, and principal deputy. Ms. Tyrangiel worked in the Office of White House Counsel before joining OLP. From 2000 to 2009, she was an assistant United States attorney in the U.S. Attorney's Office for the District of Columbia where she served as deputy chief of the Sex Offense and Domestic Violence Section.

Ms. Tyrangiel graduated from Brown University and received her law degree from the University of Michigan Law School.

Mr. Richard Littlehale, currently serves as the Assistant Special Agent in charge of the Tennessee Bureau of Investigations Technical Service Unit. He coordinates and supervises the use of a wide range of advanced technologies in support of law enforcement operations. This includes supervision of TBI's Internet Crimes Against Children Task Force and TBI's Joint Cybercrime and Child Exploitation Task Forces with the FBI.

Mr. Littlehale and the TBI agents he supervises developed intelligence and evidence from communications records in a wide range of cases, including homicide investigations, the search for dangerous fugitives, Internet crimes against children, computer intrusions, and child abduction responses.

He ensures that TBI agents are trained to use electronic surveillance techniques in strict compliance with State and Federal law. He also provides instruction to law enforcement officers at all levels of government in techniques for obtaining and using communications evidence in support of criminal investigations and is active in national groups of law enforcement technical and electronic surveillance specialists.

He graduated from Bowdoin College and received his law degree from Vanderbilt Law School.

Professor Orin Kerr is a professor of law at George Washington University where he teaches criminal law, criminal procedure, and computer crime law. Before joining the faculty in 2001, Professor Kerr was an honors program trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, as well as a special assistant U.S. attorney for the Eastern District of Virginia.

He is a former law clerk for Justice Anthony M. Kennedy of the U.S. Supreme Court and Judge Leonard I. Garth of the U.S. Court of Appeals for the Third Circuit. In the summer of 2009 and 2010, he served as special counsel for Supreme Court nominations to Senator John Cornyn on the Senate Judiciary Committee.

He has been a visiting professor at the University of Chicago Law School and the University of Pennsylvania Law School.

He received his bachelor of science degree in engineering from Princeton and his master of science from Stanford. He earned his juris doctor from Harvard Law School.

Mr. Salgado serves as Google's Director of Information Security and Law Enforcement Matters. He has also served as senior counsel in the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. As a Federal prosecutor, he specialized in investigating and prosecuting computer network cases such as computer hacking, illegal computer wiretaps, denial of service attacks, malicious code, and other technology-driven privacy crime.

He graduated from the University of New Mexico and received his law degree from Yale Law School.

Each of you will be recognized for 5 minutes. Without objection, each of your full written statements will appear in the record after your statement has been completed.

And also without objection, all Members' opening statements will be placed in the record as well.

Ms. Tyrangiel, you are first.

TESTIMONY OF ELANA TYRANGIEL, ACTING ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL POLICY, DEPARTMENT OF JUSTICE

Ms. TYRANGIEL. Thank you. Chairman Sensenbrenner, Ranking Member Scott, Chairman Goodlatte, Ranking Member Conyers, 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, or ECPA. This topic is particularly important to the Department. We are pleased to engage with the Subcommittee in discussions about how ECPA is used and how it might be updated and improved.

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

During any discussions of possible changes to ECPA, it is important to keep in mind its wide-ranging application and scope. The typical scenario that comes to mind is a law enforcement agency conducting a criminal investigation and seeking a target's e-mail from a service provider that makes its services available to the public. And indeed, ECPA is critical to all sorts of criminal inves-

tigations into murder, kidnapping, organized crime, sexual abuse, or exploitation of children, identity theft, and more.

But 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 applies not only to criminal investigators but also when the government is acting as a civil litigator or even as an ordinary civil litigant. Moreover, the statute applies not only to public and widely accessible service providers, but also to non-public providers such as companies that provide e-mail to their employees.

Although ECPA has been updated several times since its enactment in 1986, many have noted—and we agree—that some of the lines drawn by the statute have failed to keep up with the development of technology and the ways in which we use electronic and stored communications. We agree, for example, that there is no principal basis to treat e-mail less than 180 days old differently than e-mail more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to open e-mails than it gives to e-mails that are unopened.

Acknowledging these things is an important first step. The harder question is how to update 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 and individuals around the world. All of us use e-mail and other technologies to share personal and private information, and we want it to be protected appropriately.

Some have suggested that the best way to enhance privacy under ECPA would be to require law enforcement to obtain a warrant based on probable cause to compel disclosure of stored e-mail and similar stored content information from a service provider. We believe that this approach 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 typically investigate conduct that, while unlawful, is not a crime. But 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, if they could no longer use a subpoena.

Reform efforts must also account for existing practices as to entities such as corporations that provide e-mail 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 e-mails. It would be anomalous for ECPA to afford greater protection to electronic corporate records than to the identical records in hard copy. 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.

Finally, we also believe that there are a number of other parts of the statute that may merit further examination as you consider ways to update and clarify the statute, and I have noted some of them in my written statement.

The Department of Justice appreciates the opportunity to discuss this issue with the Subcommittee and I look forward to your questions here today.

[The prepared statement of Ms. Tyrangiel follows:]

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.

Mr. SENSENBRENNER. Thank you very much.
Mr. Littlehale.

TESTIMONY OF RICHARD LITTLEHALE, ASSISTANT SPECIAL AGENT IN CHARGE, TECHNICAL SERVICES UNIT, TENNESSEE BUREAU OF INVESTIGATION

Mr. LITTLEHALE. Chairman Sensenbrenner, Ranking Member Scott, Chairman Goodlatte, and Ranking Member Conyers, Members of the Subcommittee, thank you for inviting me to testify. My

name is Richard Littlehale and I am Assistant Special Agent in Charge of the TBI Technical Services Unit. I also serve on the Technology Committee of the Association of State Criminal Investigative Agencies and am representing their position today.

I will make eight points very briefly, and I welcome your questions if you would like to explore them further.

First, setting the standard necessary for government to obtain content is just the first step. We also have to make sure we can actually get it. To date, much of the attention given to the question of lawful access to stored content has focused on the level of proof required for law enforcement to obtain it. The reality is that legal barriers are not the only ones that keep communications records out of our hands. Technological barriers and a lack of a mandatory compliance framework regarding service provider response slow our efforts as much or more as a change in the standard of proof might. I urge you to ensure that whatever standard of proof you decide is appropriate, you also ensure that law enforcement can access evidence reliably and quickly.

Second, timeliness and quality of service must be addressed. There is no requirement in current law that compels providers to respond in a timely fashion to our legal demands. Some respond relatively quickly but others do not. In particular, this sometimes prevents us from efficiently processing large volumes of leads like cybertips from the National Center for Missing and Exploited Children. In those leads, there may be an emergency, but we cannot know about it until we get the routine response back from the service provider. Speed is important. A reasonable legal mandate for responsiveness should be considered as a part of any ECPA reform proposal.

Third, emergency provisions. Law enforcement must have rapid access to communications evidence in a life-threatening emergency, but that is not always the reality. The emergency provision in today's ECPA is voluntary for the providers, not mandatory. Even when emergency access is granted, there is no guarantee we will get the records immediately. In some cases, there is insufficient service provider compliance staff to process these requests quickly. In other cases, providers have chosen never to provide evidence in the absence of legal process no matter the circumstances, and the current emergency provision does not preclude this.

Fourth, notification requirements. Requiring law enforcement to seek additional process to prevent providers from informing customers of the existence of a demand is a labor-intensive process. We urge the Committee to carefully balance the need for notification and reporting against the practical resource burden it places on law enforcement.

Fifth, records retention. Some cellular service providers claim they do not retain text messages for any time at all or retain them for very short periods of time. Millions of texts are sent every day and some contain key evidence about criminal activity. I urge you to find a balance on retention policy that is not overly burdensome to service providers but that ensures that law enforcement can obtain access to critical evidence with appropriate legal process.

Sixth, preservation. Preservation under section 2703 has been offered by some as an alternative to records retention, but some serv-

ice providers have a stated policy of notifying customers of the demand unless a court tells them not to. A 2703 preservation request does not allow law enforcement to gain access to information but merely ensures it exists when we serve appropriate process. There should be no customer notice for preservation.

Seventh, the definition of content. Definitions of content and noncontent information need to be clear and comprehensive. If Congress determines that any kind of content whatsoever requires a probable cause standard of access, then ECPA should define content explicitly and not infer it from less explicit definitions in other parts of the code.

Finally, the volume of law enforcement legal demands. Recent media reports have expressed alarm that the number of law enforcement requests for communications evidence is growing. Of course, the requests are growing because today a rapidly growing percentage of the available evidence in any criminal case exists in the digital world.

Google's transparency initiative puts the volume of law enforcement demands in perspective. In June of 2012, Google claimed 425 million individual account holders for its Gmail service. In the U.S., Google reported just over 16,000 government requests affecting over 31,000 accounts. That means a tiny fraction of 1 percent of Google's accounts were affected by government demands, and given that there are 17,000 law enforcement agencies in the United States, on average there was less than one request for information per law enforcement agency per year for Google records. It is hard to conclude from these numbers that law enforcement demands were excessive.

I will close by reemphasizing the importance of ensuring that law enforcement concerns about access to evidence become a central part of this ECPA reform discussion. My fellow electronic surveillance practitioners and I are well aware of the need to balance privacy and public safety, and we look forward to working with the Subcommittee to get ECPA reform right.

Thank you for having me here and I look forward to your questions.

[The prepared statement of Mr. Littlehale follows:]

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.

Mr. SENSENBRENNER. Thank you very much.
Professor Kerr.

TESTIMONY OF ORIN S. KERR, FRED C. STEVENSON RESEARCH PROFESSOR, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

Mr. KERR. Chairman Sensenbrenner, Ranking Member Scott, Members of the Subcommittee, thank you for the invitation to testify here this morning.

I wanted to focus on the constitutional issues raised by the Stored Communications Act.

As several of you noted in your opening statements, the leading cases so far in the lower courts indicate that the Fourth Amendment fully protects the contents of e-mail and other remotely stored files in the cloud, meaning that the constitutional standards or the standards adopted by the statute in 1986 are currently below the constitutional threshold. So one pressing reason to amend the statute is because the Constitution requires more privacy protection than current statutory law requires.

The lower court case law is, as of yet, not fully developed. We have one significant decision from the Sixth Circuit Court of Appeals. We do not yet have a decision from the United States Supreme Court, and also we are still in the beginning stages of getting case law on fact patterns beyond e-mail. So, for example, in addition to storing contents, remotely stored contents by e-mail, individuals may have stored Facebook messages, Google documents stored in the cloud, lots of information that is available on remote servers that does not fit the specific category of e-mail. The lower court cases so far suggest that they are also fully protected by the Fourth Amendment's warrant requirement, but as of yet, we do not have a lot of case law in the lower courts to indicate whether that is the case.

I think it is correct, though. I think it is difficult to distinguish between e-mail, for example, and Facebook messages and documents in the cloud. In my view, they are all protected under the Fourth Amendment under the reasonable expectation of privacy test.

The difficulty then with the existing statute is not only that it is below the constitutional threshold, but that because it is below the constitutional threshold, it actually becomes significantly harder for the constitutional protections to be recognized, thanks to the good faith exception under the Fourth Amendment when the government relies on a statute that allows a search or seizure. The key case here is another 1986 decision, *Illinois v. Krull*, which held that when the government reasonably relies on a statute that might be considered constitutional, the exclusionary rule does not apply under the good faith exception.

What that means as a practical matter is that the existence of ECPA actually makes it harder to recognize constitutional rights. It actually cuts constitutional protection rather than adds privacy protection because the government under current law can rely on the good faith exception to rely on the statute to obtain contents with less process than a warrant. As the case law becomes more established, it will be harder for the government to do that. But

ironically, the existing statute actually makes it harder for Americans to recognize their constitutional rights and to get those constitutional rights recognized in cases than there would be if there were no statute at all.

Ultimately the ECPA statute was designed to fill in constitutional protections where at the time in the 1980's it was not clear how the Fourth Amendment would apply. So it may be as we get more and more case law establishing those Fourth Amendment protections, there is less and less of a need for statutory protections that regulate that same territory, and at the very least, it is important for those statutory protections to not be below the threshold of the constitutional protection in light of the good faith exception.

I also wanted to address a few aspects of the Justice Department's testimony. I think it is very significant that the Justice Department is taking the view agreeing generally to the idea that there needs to be a rewrite of the statute and that there is merit to the idea of a general warrant requirement.

The Justice Department's testimony suggests that there are two potential exceptions to that, one of which I think is justified and one of which I am skeptical about.

The one that I think is justified is allowing a subpoena authority when the government is investigating a company and its own e-mail services in the corporate crime context where traditionally the Justice Department and State prosecutors as well have relied on subpoena authorities to investigate, say, a company engaged in some sort of white-collar crime. I think it makes a lot of sense to have an exception to the general warrant requirement for that particular context.

On the other hand, I am skeptical about the idea of having civil discovery subpoenas widely used in the ECPA setting. I do not think we want to have our service providers turned into essentially places where anyone who files a civil lawsuit can go and get somebody else's e-mail to look through in a routine civil investigation. Maybe there are some reasons to treat Federal Government investigations differently in some cases, but I think it is dangerous to allow providers to be used in this way. In general, in civil litigation, it should be the people go through the parties not through service providers.

I thank you and I look forward to your questions.

[The prepared statement of Mr. Kerr follows:]

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).

Mr. SENSENBRENNER. Thank you very much.
Mr. Salgado.

TESTIMONY OF RICHARD SALGADO, DIRECTOR, LAW ENFORCEMENT AND INFORMATION SECURITY, GOOGLE, INC.

Mr. SALGADO. Chairman Sensenbrenner, Chairman Goodlatte, Ranking Member Scott, Ranking Member Conyers, and Members of the Subcommittee, thank you very much for the opportunity to appear before you this morning.

I am Richard Salgado. As Director for Law Enforcement and Information Security at Google, I oversee the company's compliance with legal requests for data, including those submitted under the Electronic Communications Privacy Act of 1986, otherwise known as ECPA.

In the past, I worked on ECPA issues in my capacity as senior counsel in the Computer Crime and Intellectual Property Section in the Department of Justice.

In 2010, I appeared before what was then the House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties. When I spoke then, I highlighted the numerous ways in which the Internet has contributed to our economy and our society as a whole.

Today, not surprisingly, the impact is greater. In addition to the millions of jobs that have been created, the Internet economy accounts for almost 5 percent of our gross domestic product, according to a recent Boston Consulting Group study. The Internet has put information and opportunity at the fingertips of millions of users, and we need updated laws to allow this ecosystem to continue growing.

On a nearly daily basis, I see the challenges created by ECPA. In 2010, Google launched a Transparency Report which details the volume of requests for user data that we receive from government entities. In the last half of 2012, the number of requests Google received from government agencies in the United States in criminal cases more than doubled compared to the same period in 2009.

ECPA was passed in 1986 when electronic communications services were in their infancy. With the dramatic changes that we have seen since then, the statute no longer provides the privacy protection that user of these services reasonably expect. And one example that the Committee may already be familiar with is from the ECPA rules around compelled disclosure of e-mail. As a general rule, law enforcement under the statute needs to obtain a warrant to compel an electronic communications service provider to disclose content that is held in electronic storage, as that term is defined in the statute, for 180 days or less. Once that message becomes 181 days old, it loses that level of statutory protection and a government entity can compel its disclosure with a mere subpoena which, of course, is issued on a much lower standard than a search warrant and without any judicial review.

I will also note that the Department of Justice has taken the position that government can use a subpoena to compel the production of e-mail that has been opened even if it is younger than 181 days. It is a position that has been rejected by one court of appeals in the Federal system.

If one could discern a policy rationale for this 180-day rule in 1986, it is not evident any longer and contravenes users' reasonable expectations of privacy. We are encouraged to hear that the Department of Justice seems to acknowledge this as well.

In fact, the Sixth Circuit in the latter part of 2010 held that ECPA violates the Fourth Amendment to the extent that it allows government to use legal process less than a warrant to compel the production of content from a service provider. Google believes this is correct, and to the extent ECPA provides otherwise, it is unconstitutional.

The 180-day rule reveals the gap between where the statute is and where users' reasonable expectations of privacy lie. The privacy protection afforded to e-mail content from law enforcement should not vary based on a communication's age or its opened state. ECPA should be updated to require a warrant to compel the production of any content. Updating ECPA should be a top privacy priority for the 113th Congress.

And Google is not alone in taking this view. More than 80 companies and organizations that span the political spectrum are now members of the Digital Due Process Coalition which supports updating ECPA. And these include Americans for Tax Reform, the American Civil Liberties Union, the Center for Democracy & Technology, the Competitive Enterprise Institute, and the U.S. Chamber of Commerce. Notably, these organizations do not always agree on other privacy issues, but they are united in the effort to support updated provisions in ECPA for the requirement of a warrant for the production of content.

As the benefits of Internet computing become more obvious, including the data security benefits, the growth of the Internet should not be artificially slowed by outdated technological assumptions that are currently baked into part of ECPA. And the progression and innovation in technology should not be hobbled by pre-Internet ECPA provisions that no longer reflect what users should expect.

We look forward to working with the Subcommittee and the full Judiciary Committee and Congress as a whole to update the statute.

Thank you for your time and consideration. I would be happy to answer any questions.

[The prepared statement of Mr. Salgado follows:]

Google

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.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The Chair will withhold his questions until the end and now recognizes the gentleman who is the Chairman of the full Committee, the gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Let me direct this question to each of you. To obtain a document from someone's home requires a warrant. When the same person

gives and stores that document with another person or a company, a subpoena can be used to obtain it.

What is an individual's expectation of privacy when electronic documents are stored with third parties? Why should stored electronic communications be treated any differently under the Fourth Amendment?

We will start with you, Ms. Tyrangiel. Is that how you pronounce your name?

Ms. TYRANGIEL. Tyrangiel.

Mr. GOODLATTE. Sorry. Thank you.

Ms. TYRANGIEL. That is okay.

So as to what can be obtained in what circumstances, the Fourth Amendment is very fact-specific and dependent on circumstances. So with that caveat, in obtaining documents from someone's home, certainly if there is a desire to go in and compel that document, there can be a search warrant used. You can also subpoena people to bring you documents that they have in their home. So depending on the circumstances, even in the paper world, there can be permutations of what rules apply.

With respect to what the standard should be for electronic communications, we have suggested that many have advocated on behalf of a warrant requirement for the government to compel stored communications from providers. And in those circumstances, as a general matter, we think that idea has some merit, and we understand the appeal of that.

Mr. GOODLATTE. Let me interrupt because I have got a lot of people and a couple more questions.

Mr. Littlehale.

Mr. LITTLEHALE. Mr. Chairman, I welcome the question, and I would suggest that it suggests that even beyond ECPA, search warrant law, statutory search warrant law, in general is also a little bit behind the times in terms of technology. For example, if I serve a search warrant on a residence, then it is up to me and the fellow agents to determine what we are going to take. We decide what we are going to get and we get it and we leave in a quick fashion or as quick as we choose to, as quick as we choose to expedite that warrant.

On the other hand, even if the Committee chooses that law enforcement needs probable cause to obtain these records, we are at the mercy of the service providers to determine how long it is going to take them to comply with that request.

So in keeping with my testimony, I would suggest that whatever the level of standard of proof, the thing that really matters most to those of us in State and local law enforcement——

Mr. GOODLATTE. Is prompt response.

Mr. LITTLEHALE [continuing]. Is prompt response.

Mr. GOODLATTE. Professor Kerr?

Mr. KERR. Mr. Goodlatte, the answer in the physical world would really depend on whether the documents that you handed to the other person were sealed or not. If it is an open set of documents, you would be relinquishing your expectation to privacy. The government could get that information from the other person without a warrant. If it is sealed documents, for example, in a sealed envelope or a sealed box, then it would be protected.

Mr. GOODLATTE. So if it is stored in the cloud but no one else—is that the equivalent of a sealed document?

Mr. KERR. Yes, I think it is the equivalent of a sealed document, and that is the right analogy that the Warshak court adopted.

Mr. GOODLATTE. Thank you.

Mr. Salgado.

Mr. SALGADO. Mr. Chairman, we do not see a distinction there. There needs to be Fourth Amendment protection to documents that a user stores in the cloud just the same as if they had stored them in their office or their home. The reasonable expectation to privacy of the Fourth Amendment requires that result, and we would like to see ECPA updated to reflect that.

Mr. GOODLATTE. All right.

And then to follow up on Professor Kerr's statement, we will ask both of you. So is there a diminished expectation of privacy when a document is stored in the cloud but multiple people have access to it for editing purposes or for whatever purpose?

Mr. KERR. No, there is no diminished expectation of privacy in the same way that there would be in—if you live with several other people in your home, there is still warrant protection for the home. In the physical world, the slight exception to that would be that other people who share the space can consent to the government going in and looking at your stuff.

And where ECPA plays an important role is in section 2702, limiting the ability of the provider—that is the sort of third party there—from voluntarily disclosing information to the government. So it is a very important protection that effectively recognizes the fact that in the cloud, it is the provider who has access to the information and also the user who has access.

Mr. GOODLATTE. Very good.

And, Mr. Salgado, would you elaborate on some of the "in the cloud" services that are currently being marketed by Google and by others? And will a higher standard for law enforcement to access the information stored in the cloud make such a service more attractive to consumers? And similarly, will it make it more attractive to criminals?

Mr. SALGADO. Thank you, Mr. Goodlatte.

The answer is yes. The services that we offer are very popular. But the failure of current law to keep up with the reasonable expectation of privacy has been a drag on the adoption of these services, and there is certainly resistance to it both in the United States but also from markets outside of the United States where customers may be concerned that the U.S. Government has access to the materials with a standard that is lower than what they ought to expect—the users ought to expect.

Some of the services that we can point to as examples of this include, of course, the Gmail product, but there are also other services like our YouTube video upload and viewing service; Docs, which allows users to collaborate on the drafting and editing of documents; Blogger, which is a very popular site for the publication of blogs which can at times be private or shared among a limited group of people.

Mr. GOODLATTE. What about criminals?

Mr. SALGADO. I am sorry?

Mr. GOODLATTE. Criminals, the other part of my question.

Mr. SALGADO. Well, we have certainly recognized that the services we offer can be misused. There are some miscreants out there who will, whatever communications service is available, find ways to turn it against the good. And we are very much in favor of an amendment to ECPA that still allows law enforcement to conduct the investigations it needs and to fulfill its important responsibilities.

Mr. SENSENBRENNER. The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

I would like to follow up on this, Mr. Salgado. Do people generally know where the e-mail is physically stored and should that make a difference in terms of the privacy expectations?

Mr. SALGADO. Mr. Chairman, I do not think people necessarily know where their e-mail is stored. Part of the reason for that, of course, is the, if you will, magic of the cloud as it is, which is by having data spread throughout lots of data centers in different locations, even the existence of a single e-mail may itself have been scattered among different data centers to provide for security, for robust services, to reduce latency. The rules around disclosure of the data should not have anything to do with the location of it, which is, in some sense, driven by the physics and architecture of the Internet and not by choice of users or companies. It is more to make——

Mr. SCOTT. And should that affect the expectation of privacy? I mean, you would expect the e-mail to be private, whatever Google does with it.

Mr. SALGADO. That is right. We agree with that, that the e-mail ought to be private regardless of where it is located and the state of its storage or the age of the message itself.

Mr. SCOTT. Professor Kerr, you mentioned the case law as being worked on through the courts. How much of that case law is statutory interpretation, which we could clearly clarify, and how much of it is constitutional law that we would have no control over?

Mr. KERR. Well, the case law that I was referring to was constitutional case law. So we have the Sixth Circuit Court of Appeals, a few district courts, a few State intermediate courts. Those are Fourth Amendment interpretations governing e-mail which, of course, Congress could not change.

Mr. SCOTT. Thank you.

Mr. Littlehale, you referred to content and said you might want to say a little bit more about it. Are there different levels of information that we are talking about whether it is the fact that the e-mail was sent or the content of the e-mail and there ought to be possible different standards for that?

Mr. LITTLEHALE. Well, the first level of categories that I would suggest we need to be cautious of, as we reform ECPA, is making a clear distinction between the actual content of a communication, the substance of the communication, and signaling and routing information, stored transactional information, that law enforcement can use, we believe, at a lesser standard whether it is determined the pattern of contact between two individuals, what communications technologies they are using, use that as a component of probable cause to further our investigation. So in my oral remarks, I

was referring to clarifying the standard of content so whatever the level of access we determine for content, we are sure what content is.

Mr. SCOTT. Ms. Tyrangiel, is there a problem now with the emergency provisions in getting information?

Ms. TYRANGIEL. That is not something on which we have an Administration position here today. We are certainly happy to talk further with you about the robustness of the emergency provisions and whether any situation——

Mr. SCOTT. You have access to information on an emergency basis now. You can skip a couple of steps if there is, in fact, an emergency. Has that been a problem?

Ms. TYRANGIEL. So currently the law allows for an exception for life and limb, essentially when there is physical harm or danger to physical life. With respect to Mr. Littlehale and the additional emergencies that might be necessary, we do not have a position on that right now, but we are eager to discuss the matter with Congress and with the Subcommittee and find a way forward.

Mr. SCOTT. Is there any problem with—in civil litigation you can get a lot of information that may not have been able to be obtained on a criminal warrant. If someone obtains information through civil litigation, can that be converted into criminal evidence?

Ms. TYRANGIEL. So with respect to what we are suggesting that Congress consider, there would be much opportunity—and, in fact, there would need to be an opportunity—to consider the means by which information could be used between civil and criminal; that is, in suggesting that there be an opportunity for civil components to obtain contents of e-mail, there would still need to be discussions about how the practicalities of that would play out. So there are currently—and it depends on context—ways in which information is passed from civil to criminal, but it need not always be the case depending on the situation.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. Thank you.

The gentleman from North Carolina, Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman, and thank you for calling this hearing, Mr. Chairman.

I thank the witnesses for appearing.

I was going to start with Chairman Goodlatte's first question. So you beat me to the punch, Bob. Let me go to another.

Mr. Littlehale, is there any evidence at all that even hints that the current law in place since 1986 has in any way inhibited either the development or the use of the Internet or other technologies?

Mr. LITTLEHALE. I am not aware of any, no, sir.

Mr. COBLE. Any other witnesses? Professor?

Mr. KERR. I think it is a difficult question to answer because, of course, it is a counter-factual issue. We do not know what the world would look like if the statute were different. So I think it is just a difficult question to answer one way or the other.

Mr. COBLE. Thank you, sir.

Anybody else want to be heard on it?

Mr. SALGADO. For companies like Google—and there are others—that have been following Warshak for a couple of years, we actually have seen what the world looks like where there is a warrant re-

quirement for content. So we have had that for a couple years now. I am not aware of this presenting any difficulties in any context.

Mr. COBLE. I thank you for that.

Mr. Littlehale, this may have been discussed, but let me try it again if it has. Do heightened legal standards result in a slower police response which may have real life or death consequences? And if so, give me an example.

Mr. LITTLEHALE. Well, sir, let me begin by saying that the case that was discussed earlier—Tennessee is in the Sixth Circuit. So for us now we live under a probable cause standard for all stored content.

Having said that, in talking with practitioners across the country, there are some who believe that the 180-day distinction is appropriate and should remain and others who do not.

I will say that, again returning to my earlier point, anytime you talk about raising the level of proof, in some cases you do reduce the number of leads we can process in the same amount of time. If that is the will of Congress, certainly we will operate within those parameters, but we also would urge you that if there are going to be proof—you know, the levels of proof are going to be raised and we are going to be able to process a large number of leads a little bit slower in that context, that if you can give us assistance in these other areas, timeliness of service provider respond, records retention, and so on, then that will allow us to contract the investigative timeline and make sure that we are able to perform our responsibilities even with a higher standard.

Mr. COBLE. I thank you, sir.

Anyone else want to be heard on that?

Thank you all for being with us today.

Thank you, Mr. Chairman. I yield back.

Mr. SENSENBRENNER. Thank you.

The gentleman from Louisiana, Mr. Richmond.

Mr. RICHMOND. Thank you, Mr. Chairman and Ranking Member, especially for calling this meeting today.

And I would just pick up where you left off because, Mr. Littlehale, I have heard you mention timeliness of response a number of times. So I guess my question would be if we went to almost like a subpoena-type model for some things, would it not be up to you all to request the return or a judge to give that date by which the provider has to respond to the subpoena?

Mr. LITTLEHALE. Well, sir, partly that depends on which statute we are proceeding under. Under ECPA, there are provisions for State orders to have federally expansive effect. That is going to vary from State to State, whether we are permitted to require a certain response or not. I am certainly aware of a number of instances over the course of my career where, regardless of what the court order said on it or what the subpoena said on it, the response was still delayed. And frankly, again as a practical matter as a practitioner, is it worth my taking my time and prosecutors' time away from investigations in order to seek a motion for a show cause hearing and try to bring a provider into town? Very often we just do not have the time to do that. So often we just live with what we can get. So regardless of the level of process, a universal

mandate for some more structured form of service provider response is critical to our effectiveness.

Mr. RICHMOND. Right, but it would still have to have teeth in it. I mean, we can have a mandated time that they have to respond, but if you are telling me that if they ignore it, you have to make a decision whether it is worth your time and energy and using an agent to go to court to do a motion to compel or a contempt hearing, then whether we put a date in or not, you would still have to make that decision.

Mr. LITTLEHALE. Yes, sir. I think a mandate would have several benefits. First, it would allow all service providers to build to the same standard as opposed to the situation we have now where some make different corporate choices than others and may be penalized because of it.

The truth is we would prefer to work with the service providers and, of course, the law enforcement electronic surveillance community has historically. We would rather resolve this in a cooperative manner and find a mandate that they could all build to rather than making an adversarial situation because the truth is we depend on these people every day to partner with us, save the victims, and get us the information we need.

Mr. RICHMOND. Now, anyone can answer this question because, in fact, we are talking about the subpoena aspect of it now.

One thing that I like about subpoenas, at least in my practice, is that if the person whose records you are asking for feels that it is just a fishing expedition or some other violation of their rights, they have an option to file a motion to quash or go see a judge or a court of jurisdiction to say, you know, this is just a fishing expedition and I do not want to do it, and then have a judge make a determination. How do you all envision encompassing that same protection, the same right, in what we are talking about now? Mr. Kerr.

Mr. KERR. I think it depends on whether we are discussing a probable cause-like regime, a traditional warrant approach, or a subpoena that is not based on probable cause. If it is a subpoena approach, then generally there would need to be some prior notice. The current ECPA statute allows for prior notice, requires prior notice when the government is pursuing a subpoena, but then allows for delayed notice which, unfortunately, is obtained in the routine case. As a result, nobody ever finds out that their e-mails are being accessed or at least does not find out until much later if they are ultimately notified. As a result, you do not see those challenges which should be available.

Under the warrant authority—and this is, I think, a complex question—if the government proceeds under the warrant authority, what notice should there be? The current statute says if the government obtains a probable cause-based warrant, there is no notice requirement. Of course, there is notice to the provider, but not to the user.

Mr. RICHMOND. Right. Well, under a warrant, the theory is that you have an independent person who has looked at it and determined that, one, it is reasonable; two, there is probable cause and it is not a fishing expedition.

So now my question is with the delayed notice, what standard is there for law enforcement to ask for and receive the ability or permission to do delayed notice as opposed to immediate—allowing the provider to immediately notify someone that their e-mails have been requested, seized, searched, or whatever.

Mr. KERR. The exact phrasing of the statute is—I cannot recall off the top of my head, but it is essentially if it would interfere with an ongoing investigation. And of course, notice to a suspect could interfere with a lot of investigations possibly. So that is obtained, unfortunately, pretty routinely. And the notice requirement written into the statute, unfortunately, ends up being a non-notice requirement in practice.

Mr. RICHMOND. Well, I see my time has expired.

Ms. Tyrangiel, if you could just, at some point, think about—and you do not have to answer it now—just how do we do it in the regulatory scheme in terms of enforcement without hampering the government's ability.

Thank you, Mr. Chairman.

Mr. SENSENBRENNER. If Ms. Tyrangiel, the Justice Department can answer Mr. Richmond's question promptly, without objection, we will put that answer in the record because all of us would like to know that.

The gentlewoman from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair.

Ms. Tyrangiel, in your testimony you raise the point that if ECPA is amended to require the government to get a warrant to compel a service provider to disclose private communications, that this would hinder civil investigations. And you say that since civil regulators and litigators lack warrant authority, they would be left unable to obtain stored contents of communications from providers.

I am trying to understand the scope of the problem if this is the case. Do you know how frequently civil investigators try to obtain information from third party service providers? Why could they not just get a subpoena for e-mails directly from the party? And in fact, would it not be more likely the case that they would do such a thing? In other words, is the frequency more or less than the requests for criminal investigators?

Ms. TYRANGIEL. So thank you for that question.

There are a couple of reasons why going to a subscriber directly is not a reliable way of always getting the content that is being sought. One is there are times when the subscriber has gone out of business, is bankrupt, is deceased. Another reason is that occasionally or with some frequency a subscriber will deny ownership of the account or of the communications at issue. And a third is that there are also those who would violate the law may be tempted to destroy rather than hand over evidence to the government. So those are a couple of reasons why going to a subscriber directly does not solve the problem.

And perhaps a couple of examples would point this out. For instance, in a civil civil rights investigation, if a landlord sends racially harassing texts to tenants and the tenants delete them because they recoil and their first instinct is to get them off their phone, and the landlord denies having sent those e-mails and de-

nies ownership of the account, the Stored Communications Act is going to govern whether the government can get those e-mails.

In the False Claims Act context, when the civil division is seeking information about a fraud perpetrated on the government and wants to get e-mails that it has reason to believe exist that show the fraud was perpetrated but the corporation says we do not actually use e-mail for business purposes, the Stored Communications Act is going to govern that as well.

So I could provide additional examples, but those are the sorts of ways in which civil investigations and suits would be impacted.

Ms. CHU. Well, for e-mail in transit, you have to have a warrant. For e-mail in storage, you have to have a warrant. For e-mail in remote storage stored for 180 days or less, you have to have a warrant. So do you not have to have probable cause anyway?

Ms. TYRANGIEL. So the laws of ECPA are somewhat complicated on this point. That is, with respect to e-mail that is older than 180 days and opened or unopened, a subpoena under ECPA would suffice. With respect to e-mail that is unopened and younger than 180 days, you would need a warrant, and with e-mail that is opened and younger than 180 days, ECPA provides for a subpoena.

Now, there is case law that is layered on top of that, but there are different rules that apply in different scenarios. And one of the things that we have said in our written testimony is we recognize that these 180-day rules and the opened/unopened distinctions have not kept pace with the way technology is used today.

Ms. CHU. Yes, but my point is you have had to prove probable cause for these other cases that are 180 days or less.

Ms. TYRANGIEL. So in a small category of cases under ECPA, there is currently a warrant requirement, but in a larger category of cases under ECPA, there is the subpoena requirement.

If your question is how, after Warshak, the Department is operating, the answer in part is that civil components are already feeling this harm, and it is harmful.

Ms. CHU. Well, do you have a solution to deal with this disparity between the civil and criminal investigations?

Ms. TYRANGIEL. So we are asking that Congress—or suggesting that Congress could consider formulating a contingency to ensure that civil regulators and litigators can do their work effectively. We do not have a specific proposal on that here today, but we are eager to discuss that further with you as you move forward.

Ms. CHU. And, Mr. Salgado, do you have a sense for how many requests received by Google are from civil investigators?

Mr. SALGADO. Chairwoman, we do not have a specific breakout for those types of requests. I can tell you that Google would not honor subpoenas for the production of content from government agencies, civil or criminal. Our understanding is that the civil agencies get the content through other means, more precisely through the customer directly, after subpoenaing Google to identify who the subscriber is.

Mr. SENSENBRENNER. The gentlewoman's time has expired.

The gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman.

Thank you to the witnesses. Professor Kerr, nice to see you back.

Mr. Salgado, I was curious. Does Google not sell information acquired from e-mails to different vendors so that they can target certain individuals with their promotions?

Mr. SALGADO. Mr. Congressman, no, we do not sell e-mail content. We do have a system, similar to the system we use for scanning for spam and malware, that can identify what type of ads are most relevant to serve on e-mail messages. It is an automated process. There is no human interaction, and certainly the e-mail is not sold to anybody or disclosed.

Mr. GOHMERT. So how do these other vendors get our e-mail and think that we may be interested in the products they are selling?

Mr. SALGADO. They do not actually get your e-mail. What they are able to do is, through our advertising business, be able to identify key words that they would like to trigger the display of one of their ads, but they do not get information about who the user is or——

Mr. GOHMERT. Okay. Well, that brings me back. So they get information about key words in our e-mails that they use to decide who to send promotions to, albeit it automatically done. Correct?

Mr. SALGADO. The e-mail context is used to identify what ads are going to be most relevant to the user.

Mr. GOHMERT. Do they pay for the right or the contractual ability to target those individuals that use those key words?

Mr. SALGADO. I might phrase that slightly differently, but the gist is correct, that advertisers are able to bid for the placement of advertisements to users who our system has detected might be interested in the advertisement.

Mr. GOHMERT. Okay. So what would prevent the Federal Government from making a deal with Google so they could also scroogle people and saying I want to know everyone who has ever used the term "Benghazi" or I want everyone who has ever used a certain term? Would you discriminate against the government or would you allow the government to know about all e-mails that included those words?

Mr. SALGADO. Sir, I think those are apples and oranges. I think the disclosure of the identity——

Mr. GOHMERT. Well, I am not asking for a fruit comparison. I am just asking would you be willing to make that deal with the government, the same one you do with private advertisers, so that the government would know which e-mails are using which words.

Mr. SALGADO. Thank you, sir. I meant by that that it is not the same deal that is being suggested there. We certainly would not——

Mr. GOHMERT. But I am asking specifically if the same type of deal could be made by the Federal Government, heck, the same Government that will make a commercial and pay for it to air overseas saying we had nothing to do with the video, which we know now had nothing to do with Benghazi, but if that same government will spend tens of thousands of dollars to do a commercial, they might under some harebrained idea like the idea of cutting a deal with Google to get all the addresses, all the e-mail addresses that use certain words. Could they not make that same kind of deal that private advertisers do?

Mr. SALGADO. We would not honor a request from the Government for such a——

Mr. GOHMERT. So you would discriminate against the Government if they tried to do what your private advertisers do.

Mr. SALGADO. I do not think that that describes what private advertisers——

Mr. GOHMERT. All right. Does anybody here have any—obviously, you are doing a good job protecting your employer. But does anybody have any proposed legislation that would assist us in what we are doing?

I see my time is running out. I would be very interested in any phrase, any clauses, any items that we might add to legislation or take from existing legislation to help us deal with this problem because I am very interested and very concerned about our privacy in our e-mail.

Mr. SENSENBRENNER. If the gentleman will yield, I am sure as this debate goes on, we will be getting a lot of advice from a lot of different sources, some of which will be trying to twist the law in favor of somebody or another. So stay tuned.

Mr. GOHMERT. And just so that the simpletons that sometimes write for Huffington Post understand, I do not want the Government having all that information.

Thank you. I yield back.

Mr. SENSENBRENNER. With a point of personal privilege, my son writes for the Huffington Post. [Laughter.]

Mr. GOHMERT. Well, then maybe he is not one of the simpletons I was referring to.

Mr. SENSENBRENNER. He does have a Ph.D.

The gentlewoman from California, Ms. Bass.

Ms. BASS. Thank you, Mr. Chair.

I wanted to ask a couple of questions, one of Mr. Salgado from Google. You said that the criminal cases that are investigated have doubled the requests, and I was wondering if you could give me some examples of the type of cases and then also why do you believe that the numbers have doubled.

Mr. SALGADO. Thank you, Congresswoman.

The types of cases that we see come in in the form of legal process are a huge variety of cases. Certainly the cases you would be very familiar with, you might have seen press reports on, those types of cases are very common, kidnapping cases, child exploitation, fraud cases. You could almost open up title 18 of the U.S. Code and walk through it, and at some point in the history of Google, there will have been some request about one of those crimes charged there.

I must say that the legal process we receive very rarely describes the case that is under investigation. So on your average legal process, we do not actually know what the crime is that is under investigation.

As to the second part of the question as to why we might have seen such an increase, it is a little bit speculative. I think part of that, though, is likely the result of the fact that our user base has grown, and as a necessary sort of result of that or inevitable result of that, there is going to be some more accounts that are used or have evidence relating to criminal conduct.

Ms. BASS. Thank you. I appreciate this.

And this might be for you or it also might be for Ms. Tyrangiel. You know, there is the Web site Backpage, and Backpage everybody knows is involved in sex trafficking and especially sex trafficking of minors. And I wanted to know how we can get at that. So, for example, if anybody monitors Backpage, there are e-mails that go back and forth requesting the services of the females that are advertised there, and what role can the Justice Department have in terms of trying to shut that down where you know it is taking place. And I do not know if the Federal Government routinely investigates that or what. I know that Craigslist used to do the same type of advertising and they stopped after public pressure, but because of First Amendment rights, of course, it is difficult to shut it down. But when we know that there is criminal behavior taking place and it is on display.

Ms. TYRANGIEL. Thank you for that question.

I am not sufficiently versed with the specific facts of Backpage to answer to that circumstance with particularity, and if there were an ongoing investigation, I would not be able to speak about it in any event.

But I can tell you with respect to sex trafficking and other sorts of crimes that the Government is investigating and trying to learn more about, the Government depends not only on the kind of content that we have been talking about here today, but also non-content information that forms the building blocks of investigations. And part of why ECPA is so important and part of why all the reform efforts should take into account not only privacy but also government needs and its law enforcement needs is because it is used with such breadth and it is used for non-content, it is used for content, it is used for civil cases, it is used for criminal cases and then within those categories for a wide variety of things.

Ms. BASS. What do you mean by non-content?

Ms. TYRANGIEL. Non-content can range all the way from basic subscriber information and things like that to information about the way people use—sort of the traffic that they use. And there are different standards that apply to different kinds of non-content. But these are the sorts of things that can form the building blocks of investigations that allow us to focus on the right people, that allow us to free others from suspicion, and then allow us to build to probable cause to a place where we can go get a search warrant or where we can make an arrest.

Ms. BASS. One of my concerns about the females or the girls, I should say, because they are not adults is that many of them are in the child welfare system. And so that means technically the government has removed them from a home which means we are in charge. And so I am wondering if there is any coordination between the Federal Government and—well, DOJ rather and child welfare departments.

Ms. TYRANGIEL. Certainly I am aware of coordination that occurs between Federal law enforcement and State jurisdictional enforcement so that they are talking to each other. So I think there is some coordination going on with respect to that. Whether there is direct communication between the Federal authorities and the

child welfare authorities I cannot speak to, but I am happy to try and find out more and get back to you.

Mr. SENSENBRENNER. The gentlewoman's time has expired.

The Chair will recognize himself for a final series of questions.

Let me say that to amend ECPA, we are going to need to have a balancing act, which means that neither law enforcement nor the service community are going to get everything they want. I would say let me admonish you and others who may be in the audience that trying to do a balancing act to come up with something that protects the privacy of Americans, as well as allows law enforcement to do their job, particularly against people who use the Internet for criminal purposes, is going to be kind of a tough nut to crack. We tried it in the last Congress, and we were not able to get the ball over the goal line.

Let me say that I think the different standards between a warrant and a subpoena is outdated and probably unconstitutional. And I think we are going to have to require a warrant with probable cause on most of the stuff that you can get from a subpoena, at least in criminal investigations, maybe not so in the civil ones, but at least in the criminal investigations.

I also think that 180 days is too short to require the retention of material. And I would like to ask you both, Ms. Tyrangiel and Mr. Littlehale, what time do you think we ought to have in terms of requiring a service provider or somebody who stores e-mails in the cloud to retain that material? And I recognize that this will just be an arbitrary time just like the 180 days is.

Ms. TYRANGIEL. Well, I will start by saying that data retention is a very complicated and tricky issue. It is not something——

Mr. SENSENBRENNER. Believe me, we know that. [Laughter.]

Ms. TYRANGIEL. And certainly law enforcement's ability to get data is very important.

The 180-day rule, I might also comment, has frankly in ECPA to do with sort of the ability to use——

Mr. SENSENBRENNER. Can you just give me a time period? At least we know what we are talking about then.

Ms. TYRANGIEL. I cannot today, but we are eager to discuss with you and understand that part——

Mr. SENSENBRENNER. I am sorry that you cannot today.

Mr. Littlehale.

Mr. LITTLEHALE. Let me suggest, Mr. Chairman, that the answer to that question is linked to service provider timeliness because in many instances in these cases, for example, in the commercial and sexual exploitation of children case that we were just discussing, there are many layers of service providers that we have to jump through to identify that child victim. And so if I know that I am going to get those responses back in 7 days each time or in 3 days each time, then I do not need the records retained as long because I might not know, until I get two or three layers of subpoena responses or search warrant responses back, where I need to send a preservation request. If, however, those times are allowed to continue to be a month or 2 months, then my answer would be 6 months or a year in many cases because it might take us that long to get to the records we need.

Mr. SENSENBRENNER. Okay.

Now, I have a question for Ms. Tyrangiel. The Fourth Amendment recognizes emergency exceptions. Why does DOJ not have a position on looking at or defining the life or limb exception? I think that it would be very advisable to codify that so you do not have a multitude of different court decisions on what is life or limb and what is not.

Ms. TYRANGIEL. I am certainly happy to engage with the Subcommittee and with Congress to talk about that area and any others that the Committee would like to explore, certainly an important exception and one that the government, both at the Federal and State and local level, makes use of.

Mr. SENSENBRENNER. Well, you know, let me express my discomfort that you do not seem to have any answers to questions that have been asked, and it is not just by me but by other Members of the Subcommittee. And this really should not be any surprise to you that the questions were coming because this is not a new issue. This is not the first hearing that a congressional committee has had on the subject of modernizing ECPA. And I would hope that the Justice Department, when they come back next time to talk about this subject, can anticipate the questions and have an answer. You know, I can say that if this were a trial, there would be a lot of people that would not be happy about the counsel at the trial being as ill-prepared as you have been.

So with that admonition, let me say, without objection, this hearing is adjourned.

[Whereupon, at 11:21 a.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION
1100 Connecticut Ave., NW Suite 900
Washington D.C. 20036
www.fleoa.org
(202) 293-1550

March 21, 2013

The Honorable Bob Goodlatte
Chairman
House Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member
House Committee on the Judiciary

Re: House EPCA Hearings

Dear Chairman Goodlatte and Ranking Member Conyers:

On behalf of the 26,000 members of the Federal Law Enforcement Officers Association (FLEOA), we are writing to express our collective expertise regarding the Electronic Crimes Privacy Act (EPCA) and any proposed changes to this important tool in the law enforcement arsenal.

Last year, we wrote to both the Chairman and Ranking Member of the Senate Judiciary Committee about our disappointment with both the content of a proposed amendment to EPCA, and the exclusion of federal law enforcement stakeholder input.

A letter was also submitted to that same Committee by a group of state and local law enforcement organizations (Law Enforcement Perspectives on ECPA Reform – September 18th, 2012), which FLEOA endorses and whose views the House Judiciary Committee should also consider.

From all appearances, it seems that current efforts to reform EPCA represent only the interests of the electronic communications industry and privacy advocate groups.

In its letter to the Senate Judiciary Committee, FLEOA stated its opposition to the elimination of the 180-Day Rule. We also opposed the implementation of a three-day notification requirement of suspects who are under investigation. Furthermore, it remains unclear what impact the current proposed Senate EPCA changes would have on law enforcement's use of pen registers, subpoenas and court orders

Our membership is also concerned with the possible impact of EPCA changes on National Security letters issued under section 2709.

The questions we asked were: Will the current Senate proposed legislation be interpreted as elevating the requirement to the warrant level? We all know

that terrorists won't take pause to accommodate our efforts to navigate through added bureaucracy.

We view many of the proposed EPCA reforms as over-reaching, and it raises questions as to how it would impact law enforcement's access to other forms of online information, i.e., information provided to third parties such as accountants or online retailers. Since the original Senate EPCA amendment did not distinguish between public and private providers, will a grand jury subpoena no longer be a valid legal instrument to obtain an employee's work emails from a corporation?

It is clear that the position of privacy advocates and electronic communications industry lobbyists has resonated with the Congress. FLEOA also questions whether anyone queried the federal Inspector General community and the Office of Professional Responsibility to determine if there was a pattern of federal law enforcement abuses of EPCA related statues.

Some experts have said cell phone, texting and email usage has risen over 400 percent within the last decade. As a matter of math, it's not a far guess why electronic communications corporations and privacy advocacy groups have lobbied together - they appear to want to reduce the amount of requests law enforcement officers make to access critical electronic information.

The realities are that this is the way people, including criminals, communicate. For criminals, this has become a choice venue to commit crimes. Since the Genie of electronic communications has been unleashed, its benefits apply to law abiding citizens and criminals and terrorists who can easily hide their activities in the "cyber world." In many cases, throwing up more barriers to law enforcement's access of this information is like barring the doors to the hospital emergency room after a catastrophe.

Due to the mission of federal law enforcement officers to: defeat terrorists; stop money launders; investigate international financial crimes; and, thwart drug and weapon traffickers, investigating these crimes entails a varied use of EPCA provisions.

Before we throw the horse out of the barn, shouldn't the law enforcement perspective factor into a substantive debate and/or review of the need for any ECPA reform?

Given the gravity of this matter for all interested parties, we recommend that the House conduct a comprehensive review of ECPA to ensure that its applications and use are consistent with the Constitution and law enforcement's need to access information to best protect the American people.

We respectfully request that this process include the views of FLEOA, the largest federal law enforcement stakeholder association.

We respectfully request this letter be included in the Committee record and be distributed to the full Committee.

Thank you for considering the perspective of federal law enforcement officers nationwide.

Fraternally,
Jon Adler

National President
FLEOA

The Federal Law Enforcement Officers Association (FLEOA) is the nation's largest organization of Federal criminal investigators, representing more than 26,000 members in 65 agencies nationwide.

WRITTEN STATEMENT OF
THE AMERICAN CIVIL LIBERTIES UNION

For a Hearing on

"ECPA Part 1: Lawful Access to Stored Content"

Submitted to the House Judiciary Committee
Subcommittee on Crime, Terrorism, Homeland Security and Investigations

March 19, 2013

ACLU Washington Legislative Office
Laura W. Murphy, Director
Christopher Calabrese, Legislative Counsel

The American Civil Liberties Union (ACLU) submits this statement to the House Judiciary Committee, on the occasion of its hearing addressing "ECPA Part 1: Lawful Access to Stored Content."[1] We offer this statement to highlight the changes in technology that have eroded American's traditional expectation of privacy and to urge the committee to take steps toward modernizing the Electronic Communications Privacy Act (ECPA) to address those changes.

The Importance of Privacy in the Digital Age

The Founding Fathers recognized that citizens in a democracy are entitled to privacy, writing in the Fourth Amendment that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause." That remains as true as ever. But our privacy laws have not kept up as technology has changed the way we hold information. Thomas Jefferson knew the papers and effects he stored in his personal rooms at Monticello would remain private. Today's citizens deserve no less protection just because their "papers and effects" might be stored electronically.

The warrant and probable cause requirements are essential components of the Fourth Amendment. The function of the warrant clause is to safeguard the rights of the innocent by preventing the state from conducting searches solely at its discretion:

> Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done not to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted.[2]

This principle has long applied to communications as well. A probable cause warrant has been required for access to postal mail since at least the 1870s and for access to landline telephone calls since the 1960s.[3]

The warrant and probable cause requirements are especially important today given the extraordinary intrusiveness of modern-day electronic surveillance. As technology has advanced and we have entered the digital age, more and more of our personal information has been gathered, compiled, and stored in easily accessible forms. Private correspondence once took the form only of letters sent through the postal service. They were typically stored within the home, and were often irretrievably discarded after a few days. By contrast an individual's emails are

[1] The ACLU is a nationwide, non-partisan organization of more than a half-million members, countless additional activists and supporters, and 53 affiliates nationwide dedicated to enforcing the fundamental rights of the Constitution and laws of the United States. The ACLU's Washington Legislative Office (WLO) conducts legislative and administrative advocacy to advance the organization's goal of protecting the privacy rights of every American.

[2] *McDonald v. United States*, 335 U.S. 451, 455 (1948).

[3] *United States v. Warshak*, 631 F.3d 266.

typically stored by a third party on a centralized, remote server, can be searched easily for key terms or topics, and may never be deleted permanently.

Similarly, tracking an individual's movements for days or searching for the presence of one person over a large area would have once required a great deal of effort and enormous resources. But the rise of cell phone and GPS technology has made such operations as simple as a quick request to a service provider. As Justice Alito wrote in *United States v. Jones*,

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken… [technological advancements], however, make long-term monitoring relatively easy and cheap.[4]

The danger posed by unwarranted government intrusions into Americans' private lives has not changed, but the ease with which those intrusions can be undertaken has. Creating legal protections to safeguard the fundamental American value of privacy, as laid out by our Founders in the Fourth Amendment, has become ever more important. In order to protect that value, Congress must update the law surrounding the privacy of our electronic communications by modernizing ECPA.

Law Enforcement Access to the Content of Communication

When the original Electronic Communications Privacy Act was passed in 1986, the Web had not yet been invented and cell phones were large clunky objects that few people owned. Since then, technological advancements have transformed the way Americans communicate. Electronic forms of communication are used for virtually every type of private exchange, from sharing personal advice and sending love letters to discussing medical ailments and conveying confidential business information.

Electronic communications are not just augmenting postal mail and the telephone, they are replacing them. Nearly all Americans on the Internet send or read email, and almost 60% do so at least once a day.[5] Moreover, 80% of Americans with cell phones use their devices to send text messages.[6] And postal mail volume has plummeted dramatically over the last few years. The volume of private, personal correspondence has fallen even more sharply than the overall mail volume.[7]

Evidence shows that as the majority of Americans have begun to replace older forms of communication like postal mail and landline telephones with electronic communications, they have tried to bring many of their old privacy practices with them. Email accounts have passwords to make sure no one can read messages without authorization, just as envelopes are

---

[4] *United States v. Jones*, 132 S. Ct. 945, 963-64 (2012) (J. Alito, concurring).
[5] Kristen Purcell, Pew Internet & American Life Project, *Search and email still top the list of most popular online activities*, Aug. 9 , 2011, http://www.pewinternet.org/Reports/2011/Search-and-email.aspx
[6] Joanna Brenner, Pew Internet & American Life Project, *Pew Internet: Mobile*, Jan. 31, 2013, http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx
[7] United States Postal Service. "Facts and figures about your Postal Service 2013." available at: http://about.usps.com/who-we-are/postal-facts/welcome.htm#H2

sealed to give letters the same protection. It is considered highly invasive for one person to read through another's text messages without permission, and many cell phones have the ability to be locked with a code to prevent just that.[8] American cell phone users are worried about privacy: more than half of mobile app users have uninstalled or avoided a cell phone app due to privacy concerns.[9] But despite these clear expectations, ECPA arguably authorizes the government to access many of these private, password-protected communications without obtaining a probable cause warrant, something that would certainly be needed to access the very same messages if they had been sent through an older medium like a written letter or a landline telephone.

This distinction arises in spite of the fact that ECPA contemplates warrants for the content of communication. However, changes in how electronic communications are stored and provided over the years have eroded that protection. When ECPA was written in 1986, users stored their communications on third party servers only briefly. They then downloaded these messages onto their personal computers, where it enjoyed Fourth Amendment protection, and the third party did not keep a copy. ECPA was created with this reality in mind: under the statute, the government may obtain opened emails that are left on servers and unopened emails left on servers for more than 180 days, without a warrant, having only to establish that the messages are "relevant and material" to an ongoing criminal investigation. The rationale for this lower standard was that these emails were the equivalent of abandoned property and hence should be treated like any other business record.

However today, few people download their email onto their own computers. The market has been overtaken by webmail applications provided by companies like Yahoo and Google, where email is stored continuously by third parties. Leaving mail on a server allows you to access your email from other multiple locations, whether home, work, a coffee shop, etc. In addition, many people are increasingly storing their emails for extended periods of time rather than deleting them. ECPA has not been updated to account for these changes in technology and the result is that the government is now arguing that it is entitled to many communications on a standard that common sense and some courts suggests does not satisfy the Constitution.[10]

Similarly antiquated technical distinctions underpin another part of ECPA, the protections for so-called 'remote computing services' (RCS). RCSs provide to the public "computer storage or processing services" and under ECPA that information can be access with a subpoena. In 1986, the only companies providing such services were payroll providers and other companies that handle business records, so a subpoena seemed analogous. Today, companies that provide storage have become the digital equivalent of desk drawers, storing photos, letters,

[8] In a recent survey, 12% of cell phone owners said that another person had accessed their cell phone "in a way that made them feel that their privacy had been invaded." For the 18-24 year old age group, that number jumps to almost a quarter of cell users. Jan Lauren Boyles, Aaron Smith, and Mary Madden, Pew Internet & American Life Project, *Privacy and Data Management on Mobile Devices*, Sep. 5, 2012, http://www.pewinternet.org/Reports/2012/Mobile-Privacy/Key-Findings.aspx

[9] Id.

[10] *Warshak*, at 282.

diaries and every type of sensitive electronic communication. It is clear that these types of communications are equally deserving of a warrant.[11]

In short, the law has not kept pace with technological change. Americans now communicate electronically, and they do so with the expectation that communication can still be private. And, they are right to have that expectation because they should have the same privacy in new technology as they had with old.

Electronic Communications and Location Tracking

In 1986, very few Americans owned a cell phone. Today around 85% of American adults have a cell phone, and many carry their cell phones with them almost everywhere they go.[12] In fact, almost a third of cell phone users describe their cell phone as "something I can't imagine living without."[13]

Although the primary purpose of a cell phone is to make phone calls, a side effect of that communication is the transmission of location information. For the many Americans that travel with and use their cell phones throughout the day, these devices are more than just phones; they are also trackers constantly logging location, often with enough accuracy to pinpoint a particular address.[14] Creation of location information is an inevitable byproduct of this technology: phones must constantly communicate with cell towers in order to make and receive calls. Communications to those towers can in turn be used to determine location. With the increasing use of smart phones, location determination can also be made in a wide variety of other ways including by activating GPS devices in the phones and logging where phones accessed fixed wi-fi hotspots.

The practical result is that law enforcement officers and government officials have the ability to find out exactly where a person was at a given time, or to find out where he or she is in real-time, as long as the person in question carries a cell phone. In addition to tracking individuals, this technical capacity also allows law enforcement to discover every individual who is in the range of a particular cell tower at a particular time. In fact, requests by law enforcement to phone companies are very common and more than 1.3 million such requests took place in 2011 alone.[15]

---

[11] For more on the history of the technology that shaped ECPA please see Orin S. Kerr, A USER'S GUIDE TO THE STORED COMMUNICATIONS ACT, AND A LEGISLATOR'S GUIDE TO AMENDING IT, 72 Geo. Wash. L. Rev. 1208.

[12] Aaron Smith, Pew Internet & American Life Project, *The Best (and Worst) of Mobile Connectivity*, Nov. 30, 2012, http://pewinternet.org/Reports/2012/Best-Worst-Mobile.aspx

[13] Id.

[14] *Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. (2010) (statement of Professor Matt Blaze at 5), *available at* http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf; Thomas Farely & Ken Schmidt, Cellular Telephone Basics: Basic Theory and Operation (2006), http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/

[15]

Location tracking enables law enforcement to capture details of someone's movements for months on end, unconstrained by the normal barriers of cost and officer resources. In a concurrence in the recent Supreme Court case, *U.S. v. Jones,* Justice Sonia Sotomayor described why this was so problematic, emphasizing the intimate nature of the information that might be collected by the GPS surveillance, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[16]

While even the limited collection of geolocation information can reveal intimate and detailed facts about a person, the privacy invasion is multiplied many times over when law enforcement agents obtain geolocation information for prolonged periods of time. As the D.C. Circuit Court of Appeals has observed, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[17]

In addition, there have always been facets of American life that have been uniquely safeguarded from the intrusive interference and observation of government. Geolocational surveillance threatens to make even those aspects of life an open book to government. As Justice Sotomayor pointed out in *Jones*, "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[18]

Finally, while the government routinely argues that records of a person's prior movements deserve less privacy protection than records of where a person travels in real time, this is a meaningless distinction. As one judge has noted, "[t]he picture of [a person]'s life the government seeks to obtain is no less intimate simply because it has already been painted."[19] A contrary conclusion would eliminate privacy protections even in real-time data, because police officers would be free to use GPS devices to record vehicles' travels so long as they waited some minutes before accessing those records, thereby rendering them "historical."

Reporting, Oversight, and Remedies

While protecting the content of electronic communications and location records are crucial elements of ECPA reform, other parts of the law also need to be improved. Specifically, we urge the committee to explore the following additional elements in any ECPA reform proposal:

---

[16] *United States v. Jones*, 132 S. Ct. 945, 955 (2012).
[17] *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010)
[18] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quotations omitted).
[19] *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010) (citation omitted).

1. **Institute Appropriate Oversight and Reporting Requirements**. Because electronic record keeping enables easy collection and aggregation of records, current low standards under ECPA allow the government to engage in a largely unsupervised and unreported "shopping spree" through the treasure trove of personal information held by private companies. To ensure adequate oversight by Congress and adequate transparency to the public, existing reporting requirements for wiretap orders must be extended to all types of law enforcement surveillance requests.

2. **Require a Suppression Remedy**. If a law enforcement official obtains non-electronic information illegally, that information usually cannot be used in a court of law. The same rule, however, doesn't apply to illegally-obtained electronic information. Such a rule only encourages government overreaching and must be changed to require a judge to bar the use of such unlawfully obtained information in court proceedings.

3. **Craft Reasonable Exceptions.** Overbroad exceptions are also depriving Americans of their rightful privacy protection. Currently ECPA sometimes allows access to the content of communications without a true emergency, without informed consent, and without prompt notice to the subject. ECPA must be amended on each of these fronts if electronic records are to receive the protections Americans need.

Conclusion

We applaud the Committee for holding this hearing and for undertaking the task of reforming ECPA. Comprehensive reform of ECPA is a needed legislative initiative that will help preserve our fundamental liberties even as the technologies that underpin our lives change. For additional information on ECPA reform or communications privacy please contact ACLU Legislative Counsel Chris Calabrese at 202 715 0839, ccalabrese@dcaclu.org.

○