EMAIL PRIVACY ACT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

ON

H.R. 699

DECEMBER 1, 2015

Serial No. 114–53

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PUBLISHING OFFICE

97–726 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing 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
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
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
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
MIMI WALTERS, California
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
DAVE TROTT, Michigan
MIKE BISHOP, Michigan

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
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
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California

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

CONTENTS

DECEMBER 1, 2015

Page

THE BILL

H.R. 699, the "Email Privacy Act" 2

OPENING STATEMENTS

The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary 1
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 20

WITNESSES

Andrew Ceresney, Director, Division of Enforcement, United States Securities and Exchange Commission
Oral Testimony 23
Prepared Statement 25
Steven H. Cook, President, National Association of Assistant United States Attorneys
Oral Testimony 31
Prepared Statement 33
Richard Littlehale, Assistant Special Agent in Charge, Tennessee Bureau of Investigation
Oral Testimony 47
Prepared Statement 49
Chris Calabrese, Vice President, Policy, Center for Democracy and Technology
Oral Testimony 58
Prepared Statement 60
Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.
Oral Testimony 75
Prepared Statement 77
Paul Rosenzweig, Visiting Fellow, The Heritage Foundation, Founder, Red Branch Consulting
Oral Testimony 89
Prepared Statement 91

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable Jared Polis, a Representative in Congress from the State of Colorado, submitted by the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 102

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Doug Collins, a Representative in Congress from the State of Georgia, and Member, Committee on the Judiciary .. 129

Page

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary 131
Prepared Statement of the Honorable Kevin Yoder, a Representative in Congress from the State of Kansas 133
Letter from the Honorable Brad R. Wenstrup, a Representative in Congress from the State of Ohio 136

OFFICIAL HEARING RECORD

UNPRINTED MATERIAL SUBMITTED FOR THE HEARING RECORD

Material submitted by the Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary. This material is available at the Committee and can also be accessed at:

http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104232.

EMAIL PRIVACY ACT

TUESDAY, DECEMBER 1, 2015

HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to call, at 10:12 a.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte (Chairman of the Committee) presiding.

Present: Representatives Goodlatte, Sensenbrenner, Chabot, Issa, King, Gohmert, Jordan, Poe, Chaffetz, Marino, Gowdy, Collins, DeSantis, Walters, Buck, Ratcliffe, Trott, Bishop, Conyers, Nadler, Lofgren, Jackson Lee, Johnson, Chu, DelBene, Jeffries, and Cicilline.

Staff Present: (Majority) Shelley Husband, Chief of Staff & General Counsel; Branden Ritchie, Deputy Staff Director & Chief Counsel; Allison Halataei, Parliamentarian & General Counsel; Kelsey Williams, Clerk; Caroline Lynch, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; (Minority) Perry Apelbaum, Staff Director & Chief Counsel; Aaron Hiller, Chief Oversight Counsel; Joe Graupensperger, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Tiffany Joslyn, Deputy Chief Counsel, Crime, Terrorism, Homeland Security, and Investigations; and Veronica Eligan, Professional Staff Member.

Mr. GOODLATTE. Good morning. The Judiciary Committee will come to order, and without objection, the Chair is authorized to declare recesses of the Committee at any time. We welcome everyone to this morning's legislative hearing on H.R. 699, the "Email Privacy Act," and I'll begin by recognizing myself for an opening statement.

[The bill, H.R. 699, follows:]

I

114TH CONGRESS
1ST SESSION

H. R. 699

To amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 4, 2015

Mr. YODER (for himself, Mr. POLIS, Mr. ADERHOLT, Mr. ALLEN, Mr. AMASH, Mr. AMODEI, Mr. BABIN, Mr. BARLETTA, Mr. BARR, Mr. BARTON, Mr. BENISHEK, Mr. BEYER, Mr. BILIRAKIS, Mr. BISHOP of Utah, Mrs. BLACK, Mrs. BLACKBURN, Mr. BLUM, Ms. BONAMICI, Mr. BOUSTANY, Mr. BRADY of Texas, Mr. BROOKS of Alabama, Ms. BROWN of Florida, Ms. BROWNLEY of California, Mr. BUCHANAN, Mr. BUCSHON, Mr. BURGESS, Mr. BYRNE, Mr. CALVERT, Mrs. CAPPS, Mr. CAPUANO, Mr. CÁRDENAS, Mr. CARTER of Georgia, Mr. CARTWRIGHT, Mr. CHABOT, Mr. CHAFFETZ, Ms. CHU of California, Mr. CICILLINE, Ms. CLARK of Massachusetts, Ms. CLARKE of New York, Mr. CLAWSON of Florida, Mr. CLEAVER, Mr. COHEN, Mr. COLE, Mr. COLLINS of New York, Mr. CONNOLLY, Mr. CONYERS, Mr. CRAMER, Mr. CRENSHAW, Mr. CULBERSON, Mr. CUMMINGS, Mr. CURBELO of Florida, Mr. RODNEY DAVIS of Illinois, Mr. DANNY K. DAVIS of Illinois, Mr. DEFAZIO, Ms. DEGETTE, Ms. DELBENE, Mr. DENHAM, Mr. DENT, Mr. DESAULNIER, Mr. DESJARLAIS, Mr. DEUTCH, Mr. DIAZ-BALART, Mr. DOLD, Mr. MICHAEL F. DOYLE of Pennsylvania, Ms. DUCKWORTH, Mr. DUFFY, Mr. DUNCAN of South Carolina, Mr. DUNCAN of Tennessee, Ms. EDWARDS, Mr. ELLISON, Mrs. ELLMERS, Mr. EMMER, Ms. ESHOO, Ms. ESTY, Mr. FARENTHOLD, Mr. FARR, Mr. FITZPATRICK, Mr. FLEISCHMANN, Mr. FLORES, Mr. FORTENBERRY, Mr. FRANKS of Arizona, Mr. FRELINGHUYSEN, Ms. FUDGE, Ms. GABBARD, Mr. GARAMENDI, Mr. GARRETT, Mr. GIBBS, Mr. GIBSON, Mr. GOSAR, Mr. GOWDY, Mr. GRAVES of Georgia, Mr. GRIJALVA, Mr. GROTHMAN, Mr. GUINTA, Mr. GUTHRIE, Mr. HANNA, Mr. HARRIS, Mrs. HARTZLER, Mr. HASTINGS, Ms. HERRERA BEUTLER, Mr. HILL, Mr. HIMES, Mr. HONDA, Mr. HUDSON, Mr. HUELSKAMP, Mr. HUIZENGA of Michigan, Mr. HULTGREN, Mr. HUNTER, Mr. HURD of Texas, Mr. ISRAEL, Ms. JACKSON LEE, Ms. JENKINS of Kansas, Mr. JOHNSON of Georgia, Mr. JOLLY, Mr. JONES, Mr. JORDAN, Mr. JOYCE, Ms. KAPTUR, Mr. KILMER, Mr. KINZINGER of Illinois, Ms. KUSTER, Mr. LABRADOR, Mr. LAMALFA, Mr. LANCE, Mr. LATTA, Ms.

LEE, Mr. LEVIN, Mr. LEWIS, Mr. LIPINSKI, Mr. LOBIONDO, Mr. LONG, Mr. LOUDERMILK, Mrs. LOVE, Mr. LOWENTHAL, Mr. LUETKEMEYER, Mr. BEN RAY LUJÁN of New Mexico, Ms. MICHELLE LUJAN GRISHAM of New Mexico, Mrs. LUMMIS, Mr. MARCHANT, Mr. MARINO, Mr. MASSIE, Mr. MCCLINTOCK, Ms. MCCOLLUM, Mr. MCDERMOTT, Mr. MCGOVERN, Mr. MCHENRY, Mr. MCKINLEY, Mr. MEADOWS, Mr. MEEHAN, Mr. MEEKS, Mr. MESSER, Mr. MOOLENAAR, Mr. MULLIN, Mr. MULVANEY, Mr. NADLER, Mr. NEWHOUSE, Mrs. NOEM, Mr. NOLAN, Ms. NORTON, Mr. NUGENT, Mr. NUNES, Mr. OLSON, Mr. O'ROURKE, Mr. PALAZZO, Mr. PAULSEN, Mr. PEARCE, Mr. POCAN, Mr. POE of Texas, Mr. POLIQUIN, Mr. POMPEO, Mr. POSEY, Mr. QUIGLEY, Mr. RANGEL, Mr. REED, Mr. RIBBLE, Mr. RICE of South Carolina, Mrs. ROBY, Mr. ROE of Tennessee, Mr. ROKITA, Mr. ROONEY of Florida, Mr. ROUZER, Mr. RUIZ, Mr. RUSH, Mr. RYAN of Ohio, Mr. SABLAN, Mr. SALMON, Mr. SANFORD, Mr. SCALISE, Mr. SCHOCK, Mr. SCHRADER, Mr. SCHWEIKERT, Mr. AUSTIN SCOTT of Georgia, Mr. SCOTT of Virginia, Mr. SENSENBRENNER, Mr. SERRANO, Mr. SESSIONS, Mr. SHUSTER, Mr. SIMPSON, Ms. SLAUGHTER, Mr. SMITH of Missouri, Mr. SMITH of Texas, Ms. SPEIER, Mr. STIVERS, Mr. STUTZMAN, Mr. SWALWELL of California, Mr. TAKANO, Mr. THOMPSON of Pennsylvania, Mr. TIBERI, Mr. TIPTON, Mr. TONKO, Ms. TSONGAS, Mr. TURNER, Mr. VALADAO, Mrs. WAGNER, Mr. WALKER, Mr. WEBER of Texas, Mr. WEBSTER of Florida, Mr. WELCH, Mr. WENSTRUP, Mr. WESTERMAN, Mr. WHITFIELD, Mr. WILLIAMS, Mr. WILSON of South Carolina, Mr. WOMACK, Mr. YARMUTH, Mr. YOHO, Mr. YOUNG of Indiana, Mr. YOUNG of Iowa, Ms. GRANGER, Mr. MCNERNEY, Mr. RICHMOND, Miss RICE of New York, Mr. SHERMAN, and Ms. PINGREE) introduced the following bill; which was referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Email Privacy Act".

SEC. 2. CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS.

Section 2702(a)(3) of title 18, United States Code, is amended to read as follows:

"(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge to any governmental entity the contents of any communication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such service.".

SEC. 3. ELIMINATION OF 180-DAY RULE; SEARCH WARRANT REQUIREMENT; REQUIRED DISCLOSURE OF CUSTOMER RECORDS.

(a) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(1) by striking subsections (a), (b), and (c) and inserting the following:

"(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS.—A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of

Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure.

"(b) NOTICE.—Except as provided in section 2705, not later than 10 business days in the case of a law enforcement agency, or not later than 3 business days in the case of any other governmental entity, after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service or remote computing service under subsection (a), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

"(1) a copy of the warrant; and

"(2) a notice that includes the information referred to in clauses (i) and (ii) of section 2705(a)(4)(B).

"(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—

"(1) IN GENERAL.—Subject to paragraph (2), a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information per-

taining to a subscriber or customer of the provider or service (not including the contents of communications), only if the governmental entity—

"(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure;

"(B) obtains a court order directing the disclosure under subsection (d);

"(C) has the consent of the subscriber or customer to the disclosure; or

"(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of the provider or service that is engaged in telemarketing (as defined in section 2325).

"(2) INFORMATION TO BE DISCLOSED.—A provider of electronic communication service or remote computing service shall, in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery sub-

poena, or any means authorized under paragraph (1), disclose to a governmental entity the—

"(A) name;

"(B) address;

"(C) local and long distance telephone connection records, or records of session times and durations;

"(D) length of service (including start date) and types of service used;

"(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

"(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber or customer of such service.

"(3) NOTICE NOT REQUIRED.—A governmental entity that receives records or information under this subsection is not required to provide notice to a subscriber or customer."; and

(2) by adding at the end the following:

"(h) RULE OF CONSTRUCTION.—Nothing in this section or in section 2702 shall be construed to limit the authority of a governmental entity to use an administrative subpoena authorized under a Federal or State statute or

to use a Federal or State grand jury, trial, or civil discovery subpoena to—

"(1) require an originator, addressee, or intended recipient of an electronic communication to disclose the contents of the electronic communication to the governmental entity; or

"(2) require an entity that provides electronic communication services to the officers, directors, employees, or agents of the entity (for the purpose of carrying out their duties) to disclose the contents of an electronic communication to or from an officer, director, employee, or agent of the entity to a governmental entity, if the electronic communication is held, stored, or maintained on an electronic communications system owned or operated by the entity.".

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2703(d) of title 18, United States Code, is amended—

(1) by striking "A court order for disclosure under subsection (b) or (c)" and inserting "A court order for disclosure under subsection (c)"; and

(2) by striking "the contents of a wire or electronic communication, or".

SEC. 4. DELAYED NOTICE.

Section 2705 of title 18, United States Code, is amended to read as follows:

"SEC. 2705. DELAYED NOTICE.

"(a) DELAY OF NOTIFICATION.—

"(1) IN GENERAL.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

"(2) DETERMINATION.—A court shall grant a request for delayed notification made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions of the delay of notification granted under paragraph (2) of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

"(4) EXPIRATION OF THE DELAY OF NOTIFICATION.—Upon expiration of the period of delay of notification under paragraph (2) or (3), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court approving the search warrant, the customer or subscriber—

"(A) a copy of the warrant; and

"(B) notice that informs the customer or subscriber—

"(i) of the nature of the law enforcement inquiry with reasonable specificity;

"(ii) that information maintained for the customer or subscriber by the provider of electronic communication service or remote computing service named in the process or request was supplied to, or requested by, the governmental entity;

"(iii) of the date on which the warrant was served on the provider and the date on which the information was provided by the provider to the governmental entity;

"(iv) that notification of the customer or subscriber was delayed;

"(v) the identity of the court authorizing the delay; and

"(vi) of the provision of this chapter under which the delay was authorized.

"(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—

"(1) IN GENERAL.—A governmental entity that is obtaining the contents of a communication or information or records under section 2703 may apply to a court for an order directing a provider of electronic communication service or remote computing service to which a warrant, order, subpoena, or other directive under section 2703 is directed not to notify any other person of the existence of the warrant, order, subpoena, or other directive for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

"(2) DETERMINATION.—A court shall grant a request for an order made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant, order, subpoena, or other directive may result in—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions of an order granted under paragraph (2) of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

"(4) PRIOR NOTICE TO LAW ENFORCEMENT.—Upon expiration of the period of delay of notice under this section, and not later than 3 business days before providing notice to a customer or subscriber, a provider of electronic communication service or remote computing service shall notify the gov-

ernmental entity that obtained the contents of a communication or information or records under section 2703 of the intent of the provider of electronic communication service or remote computing service to notify the customer or subscriber of the existence of the warrant, order, or subpoena seeking that information.

"(c) DEFINITION.—In this section and section 2703, the term 'law enforcement agency' means an agency of the United States, a State, or a political subdivision of a State, authorized by law or by a government agency to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of criminal law, or any other Federal or State agency conducting a criminal investigation.".

SEC. 5. EVALUATION BY THE GOVERNMENT ACCOUNTABILITY OFFICE.

Not later than September 30, 2017, the Comptroller General of the United States shall submit to Congress a report regarding the disclosure of customer communications and records under section 2703 of title 18, United States Code, which shall include—

(1) an analysis and evaluation of such disclosure under section 2703 of title 18, United States

Code, as in effect before the date of enactment of this Act, including—

(A) a comprehensive analysis and evaluation regarding the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which Federal, State, or local law enforcement officers used section 2703 of title 18, United States Code, to obtain information relevant to an ongoing criminal investigation;

(B) an analysis of the average length of time taken by a provider of an electronic communication service or a remote computing service to comply with requests by law enforcement officers for information under section 2703 of title 18, United States Code;

(C) the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which information was requested by law enforcement officers from a provider of an electronic communication service or a remote computing service under a warrant as authorized under section 2703(a) of title 18, United States Code;

(D) the number of individual instances and type of request, in each of the 5 years before the year in which this Act is enacted, in which information was requested by law enforcement officers from a provider of an electronic communication service or a remote computing service under the other information request provisions in section 2703 of title 18, United States Code; and

(E) the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which law enforcement officers requested delayed notification to the subscriber or customer under section 2705 of title 18, United States Code; and

(2) an analysis and evaluation of such disclosure under section 2703 of title 18, United States Code, as amended by this Act, including—

(A) an evaluation of the effects of the amendments to the warrant requirements on judges, court dockets, or any other court operations;

(B) a survey of Federal, State, and local judges and law enforcement officers to determine the average length of time required for

providers of an electronic communication service or a remote computing service to provide the contents of communications requested under a search warrant, which shall include identifying the number of instances in which a judge was required to order a provider of an electronic communication service or a remote computing service to appear to show cause for failing to comply with a warrant or to issue an order of contempt against a provider of an electronic communication service or a remote computing service for such a failure; and

(C) determining whether the amendments to the warrant requirements resulted in an increase in the use of the emergency exception under section 2702(b)(8) of title 18, United States Code.

SEC. 6. RULE OF CONSTRUCTION.

Nothing in this Act or an amendment made by this Act shall be construed to preclude the acquisition by the United States Government of—

(1) the contents of a wire or electronic communication pursuant to other lawful authorities, including the authorities under chapter 119 of title 18 (commonly known as the "Wiretap Act"), the For-

eign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this Act; or

(2) records or other information relating to a subscriber or customer of any electronic communications service or remote computing service (not including the content of such communications) pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119 of title 18 (commonly known as the "Wiretap Act"), or any other provision of Federal law not specifically amended by this Act.

○

Mr. GOODLATTE. Today's hearing examines H.R. 699, the "Email Privacy Act," and the need to modernize the Electronic Communications Privacy Act, or ECPA. In enacting ECPA nearly 30 years ago, Congress declared that the law's purpose was to achieve a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies. Reforming this decades old outdated law has been a priority for me as Chairman of this Committee, and I've been working with Members of Congress, advocacy groups, and law enforcement for years on many complicated nuances involved in updating this law.

I am pleased to now hold this important hearing to examine the leading reform proposal in the House, H.R. 699, and to examine in more detail the nuances Congress must consider in updating this law. While technology has undoubtedly outpaced the law in the last three decades, the purpose of the law remains steadfast. I am confident that Congress will once again strike that balance and do so in a way that continues to promote the development and use of new technologies and services, and create a statutory framework that will modernize the law to reflect how people communicate with one another today and in the future.

ECPA reform has broad sweeping implications. ECPA, and more specifically, the Stored Communications Act, governs Federal, State, and local government access to stored email, account records, and subscriber information from telephone, email, and other service providers. ECPA not only applies when law enforcement seeks information in a criminal investigation, but also in civil investigations and for public safety emergencies.

H.R. 699, at its core, establishes for the first time, in Federal statute, a uniform warrant requirement for stored communications content in criminal investigations, regardless of the type of service provider, the age of an email, or whether the email has been opened. I support the core of H.R. 699, which would establish a standard that embodies the principles of the Fourth Amendment and reaffirms our commitment to protecting the privacy interests of the American people.

However, our adherence to the Fourth Amendment should not end there. Congress can ensure that we are furthering the legitimate needs of law enforcement through ECPA reform by joining with the warrant requirement recognized exceptions and procedures designed to further the legitimate needs of law enforcement. One of the goals of this legislation is to treat searches in the virtual world and the physical world equally, so it makes sense that the exceptions to the warrant requirement and the procedures governing service of warrants should also be harmonized.

It is well settled law that the government may conduct a search in the absence of a warrant in certain instances, including when the government determines that an emergency exists requiring the search, or when the government obtains the consent of the owner of the information. The Stored Communications Act, however, created a framework unique to the electronic world in which even in an emergency or with a consent of the customer, disclosure of email content or even noncontent records is voluntary at the discretion of the provider. It is also well established law that a search warrant must be served at the place where the search or seizure occurs.

For 3 decades, ECPA warrants have been executed with the provider because, as with any other third-party custodian, the information sought is stored with them. H.R. 699 would now require the government to also serve the warrant directly on the criminal suspect, a proposal which has raised serious public safety and operational concerns across the law enforcement community.

Congress should also continue to ensure that civil investigative agencies are able to obtain electronic communication information for civil violations of Federal law. Courts have routinely held that subpoenas satisfy the reasonableness requirement of the Fourth Amendment. Unlike a warrant, which is issued without prior notice, and is executed often by force with an unannounced and unanticipated physical intrusion. A subpoena commences an adversarial process during which the person served with the subpoena may challenge it in court before complying with its demands.

The Stored Communications Act currently authorizes the issuance of a subpoena directly to the provider, albeit with a requirement that the government notify the customer. But Congress can go further to ensure that ECPA satisfies the Fourth Amendment by requiring that any civil process authorized by the law begin with service of a subpoena directly on the customer.

In this context, the customer is provided notice and the opportunity to contest the subpoena. Enforcement of the subpoena through a court order issued by a Federal judge that protects the rights and privileges of the customer, while ensuring that evidence of illegal activity is not insulated from investigators, would afford heightened protections beyond that which the courts have deemed necessary to comport with the Fourth Amendment.

Congress has enacted laws that impose penalties for certain conduct, sometimes criminal penalties and sometimes civil. We have established Federal agencies to enforce these laws with the tools necessary to carry out that enforcement. Congress should ensure that, in its efforts to modernize ECPA, we do not eliminate access to evidence of violations of Federal law simply because Congress chose to make those violations punishable by civil penalties.

I want to thank our distinguished witnesses for being here today, and I look forward to hearing from each of you on H.R. 699 and how to properly balance the privacy expectations of American citizens and the legitimate needs of law enforcement. And I look forward to working with all Members on both sides of the aisle to modernize the Electronic Communications Privacy Act. It is worth noting today that we also plan to hold a separate hearing in the future on the issue surrounding law enforcement access to information located on servers outside the U.S. As with the broader topic of ECPA reform, that is an issue with many nuances that we should carefully examine.

I would now like to ask unanimous consent to enter the following items into the record: a statement dated December 1, 2015, from the Department of Justice; a letter from the Federal Bureau of Investigation Agents Association dated November 24, 2015; a letter from the National Association of Police Organizations dated November 30, 2015; a letter from the Association of Prosecuting Attorneys dated November 24, 2015; a letter from the Virginia Association of Commonwealth Attorneys dated July 10, 2015; a letter from

the Technology Councils of North America dated November 30, 2015; a statement from Americans for Tax Reform dated December 1, 2015; and a coalition letter signed by Tech Freedom and other coalition members dated November 30, 2015.*

Without objection, the items have been entered into the record.

It's now my pleasure to recognize the Ranking Member of the Judiciary Committee, the gentleman from Michigan, Mr. Conyers for his opening statement.

Mr. CONYERS. Thank you, Chairman Goodlatte, Members of the Committee, and our honored witnesses here for the hearing, and those who are in 2141 to participate in the listening of this very important measure.

H.R. 699, the "Email Privacy Act," enjoys I'm pleased to say, the overwhelming bipartisan support in the House. As of this morning, the bill has earned 304 cosponsors; 191 Republicans, 113 Democrats; and 27 Members of the House Judiciary Committee.

Now, what do all of these Members have in common? First of all, we agree that the Electronic Communications Privacy Act is outdated and provides unjustifiably inconsistent standards for government access to our stored communication. This statute continues to serve as one of the main guarantees of our digital privacy, but the law was designed in 1986, when few of us used email, and even fewer imagined a world in which we could so freely share information online.

The consequences of applying a 30-year-old understanding of technology to modern communications are inconsistent, at best. For example, the law seems to apply different standards for government access to the same email at different points in its lifecycle, when it's drafted, when it's transmitted, when it's opened by its recipient, and when it is archived in the cloud. We are not well served by a law whose application is unpredictable and that the courts have had great difficulty in interpreting. Because of the rapid pace of technological change, this situation will only get worse if we do not act.

Secondly, the sponsors of this bill agree that the government should be obligated to show probable cause before it can require a provider to disclose the content in its customer's mail, no matter how old the message is. This standard is consistent with the holding of the Sixth Circuit court in the *Warshak* case in 2010. That case motivated the Department of Justice to voluntarily adopt a warrants for email standard. It also effectively ended the unconstitutional use of subpoenas to compel third parties to produce content in civil enforcement actions.

Current law requires the government to show probable cause and obtain a warrant only for email that has been in storage for 180 days or less. But the government can use and subpoena for the same email if it's stored for 1 day longer. This is no longer acceptable to most Americans. As the Sixth Circuit rightly observed, citizens have the same reasonable expectation of privacy in their email before and after the 180-day mark, and as the Department of Justice testified soon thereafter, there is no principal basis to treat

*__Note:__ The material submitted by Mr. Goodlatte is not printed in this hearing record but is on file with the Committee. See also "For the Record Submission—Rep. Goodlatte" at:
http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104232.

email less than 180 days old differently than email more than 180 days old.

Thirdly, the sponsors of H.R. 699 all agree that current law is not adequate to protect new forms of digital communication. Content is content. Our expectation of privacy does not diminish merely because Congress didn't think of the medium when it last visited the statute. The law should protect electronic communications across the board, email, text messages, private messages of all sorts, and other forms of digital information stored in the cloud.

Finally, the sponsors of this bill agree that we must act without delay. We have an obligation to provide clear standards to law enforcement with respect to emerging technologies. We should also recognize that American businesses cannot sustain these new technologies if consumers cannot trust them.

As the Committee takes up this bill, we should ensure that it does not conflict with the basic notion that the government's seizure of our email without a warrant violates the Fourth Amendment, but we should note that this principle has already taken hold across the Federal Government. The Department of Justice already uses warrants for email in criminal cases. The government stopped using lesser process in the civil context years ago.

In short, Mr. Chairman and Members, this legislation accomplishes two vital tasks. It updates the statute for modern use, and it does so without any significant interruption to law enforcement. We should all come together on this bill as soon as possible, and I want to personally thank the witnesses for being with us today and for their testimony, and I urge my colleagues to give this measure their full support, and I thank the Chairman.

Mr. GOODLATTE. Thank you, Mr. Conyers. And before we swear in the witnesses, I'd like to recognize the presence of the chief sponsor of the legislation, the gentleman from Wisconsin, Mr. Yoder. Thank you for being with us today. Kansas, Kansas, Kansas. The gentleman from Wisconsin says he'll take you.

We welcome our distinguished witnesses today, and if you would all please rise, I'll begin by swearing you in. If you'd please raise your right hand.

Do you and each of you swear that the testimony that you are about to give shall be the truth, the whole truth, and nothing but the truth, so help you God?

Thank you very much. You may please be seated, and let the record reflect that the witnesses have responded in the affirmative.

Mr. Andrew Ceresney is the director of the enforcement division at the United States Securities and Exchange Commission, where he has served since 2013. Prior to joining the SEC, Mr. Ceresney served as the assistant United States Attorney in the U.S. Attorneys Office for the Southern District of New York where he was a deputy chief appellate attorney and a member of the Securities and Commodities Fraud Task Force in the Major Crimes Unit. As a prosecutor, Mr. Ceresney handled numerous white-collar criminal investigations, trial and appeals, including matters related to securities fraud, mail and wire fraud, and money laundering. He is a graduate of Columbia College and Yale law school.

Mr. Steven Cook is president of the National Association of Assistant U.S. Attorneys. He currently serves as the chief of staff of

the criminal division of the U.S. Attorney's Office for the Eastern District of Tennessee. He has been an assistant U.S. Attorney for 29 years. In this capacity, he has worked in the Organized Crime Drug Enforcement Task Force and the General Crimes Section where he handled white-collar crime, fraud, and public corruption. He also served as the deputy criminal chief in the narcotics and violent crime section. Prior to joining the U.S. Attorney's Office, Mr. Cook was a police officer for 7 years in Knoxville, Tennessee. He earned a JD from the University of Tennessee.

Mr. Richard Littlehale is the assistant special agent in charge at the Tennessee Bureau of Investigation. In addition to his duties as an investigative supervisor, Mr. Littlehale serves as an advisor and trainer in criminal law and procedure, as well as the Bureau's chief firearms instructor. Mr. Littlehale is a frequent presenter to community organizations on ways to protect children online. He is active in engaging the legal community on better ways to protect children from victimization. Mr. Littlehale received a bachelor's degree from Bowdoin College and JD from Vanderbilt University.

Mr. Chris Calabrese is the vice president for policy at the Center for Democracy and Technology where he oversees the center's policy portfolio. Before joining CDT, Chris served as legislative counsel at the American Civil Liberties Union legislative office where he led advocacy efforts relating to privacy, new technology, and identification systems. Prior to joining the ACLU, Chris served as legal counsel to the Massachusetts Senate majority leader. Chris is a graduate of Harvard University and holds a JD from the Georgetown University Law Center.

Mr. Richard Salgado is the director of law enforcement and information security at Google. Mr. Salgado oversees Google's global law enforcement and national security efforts and legal matters relating to data, security, and investigations. Previously, Mr. Salgado worked with Yahoo and also served as senior counsel in the computer crimes section of the U.S. Justice Department. As a prosecutor, he specialized in computer network crime, such as hacking, wiretaps, denial of service attacks, malicious code, and other technology driven privacy crimes. In 2005, he joined Stanford law school as a legal lecturer on computer crime, Internet business legal and policy issues, and modern surveillance law. He received his JD from Yale law school.

Mr. Paul Rosenzweig is the founder of Red Branch Consulting, a homeland security consulting company and a senior advisor to the Chertoff Group. Mr. Rosenzweig formerly served as deputy assistant secretary for policy in the Department of Homeland Security. He is a distinguished visiting fellow at the Homeland Security Studies and Analysis Institute. He also serves as a lecturer in law at George Washington University and adjunct professor at the National Defense University, a senior editor of the Journal of National Security Law and Policy, and is a visiting fellow at the Heritage Foundation. He earned a bachelor's degree from Haverford College, a master's from Scripps Institution of Oceanography, and a JD from the University of Chicago law school.

Your written statements will be entered into the record in their entirety, and we ask that each of you summarize your testimony in 5 minutes. To help you stay within that time, there's a timing

light on your table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, that's it, time's up, and it signals that your time has expired.

Mr. Ceresney, am I pronouncing your name correctly?

Mr. CERESNEY. You are.

Mr. GOODLATTE. Thank you very much, and you may begin.

TESTIMONY OF ANDREW CERESNEY, DIRECTOR, DIVISION OF ENFORCEMENT, UNITED STATES SECURITIES AND EXCHANGE COMMISSION

Mr. CERESNEY. Good morning, Chairman Goodlatte. Good morning, Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee. Thank you for inviting me to testify today on behalf of the commission concerning Email Privacy Act, H.R. 699, pending before your Committee.

The bill seeks to modernize portions of the Electronic Communications Privacy Act, ECPA, which became law in 1986. I share the goal of updating ECPA's evidence collection procedures and privacy protections to account for the digital age, but H.R. 699, in its current form, poses significant risks to the American public by impeding the ability of the SEC and other civil law enforcement agencies to investigate and uncover financial fraud and other unlawful conduct.

I firmly believe there are ways to update ECPA that offer stronger privacy protections and observe constitutional boundaries without frustrating the legitimate ends of civil law enforcement.

The SEC's tripartite mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The SEC's division of enforcement furthers this mission by, among other things, investigating potential violations of the Federal securities laws, recommending that the commission bring cases against alleged fraudsters and other securities law wrongdoers, and litigating the SEC's enforcement actions.

A strong enforcement program is a critical piece of the commission's efforts to protect investors from fraudulent schemes and promotes investor trust and confidence in the integrity of the Nation's securities markets.

Electronic communications often provide critical evidence in our investigations as email and other message content can establish timing, knowledge or relationships in certain cases, or awareness that certain statements to investors were false or misleading. When we conduct an investigation, we generally will seek emails and other electronic communications from the key actors through an administrative subpoena.

In some cases the person whose emails are sought will respond to our request, but in other cases, the subpoena recipient may have erased email, tendered only some emails, asserted damaged hardware, or refused to respond. Unsurprisingly, individuals who violate the law are often reluctant to produce to the government evidence of their own misconduct.

In still other cases, email account holders cannot be subpoenaed because they are beyond our jurisdiction. It is at this point in the investigation that we may, in some instances, need to seek infor-

mation from an Internet service provider, also known as an ISP. The proposed amendment would require government entities to procure a criminal warrant when they seek the content of emails and other electronic communications from ISPs.

Because the SEC and other civil law enforcement agencies cannot obtain criminal warrants, we would effectively not be able to gather evidence, including communications such as emails directly from an ISP, regardless of the circumstances, even in instances where a subscriber deleted his emails, related hardware was lost or damaged, or where the subscriber fled to another jurisdiction. Depriving the SEC of authority to obtain email content from an ISP would also incentivize subpoena recipients to be less forthcoming in responding to investigatory requests, because an individual who knows that the SEC lacks the authority to obtain his emails may thus feel free to destroy or not produce them.

These are not abstract concerns for the SEC, or for the investors we are charged with protecting. Among the type of scams we investigate are Ponzi schemes and "pump and dump" market manipulation schemes, as well as insider trading activity. In these types of fraud, illegal acts are particularly likely to be communicated via personal accounts, and parties are more likely to be noncooperative in their document productions.

Technology has evolved since ECPA's passage, and there is no question that the law ought to evolve to take account of advances in technology and protect privacy interests, even when significant law enforcement interests are also implicated. But there are various ways to strike an appropriate balance between those interests as the Committee considers the best way to advance this important legislation.

Any reform to ECPA can and should afford a party whose information is sought from an ISP in a civil investigation an opportunity to participate in judicial proceedings before the ISP is compelled to produce this information. Indeed, when seeking email content from ISPs in the past, the division has provided notice to email account holders in keeping with longstanding and just recently reaffirmed Supreme Court precedent.

If the legislation were so structured, an individual would have the ability to raise with a court any privilege, relevancy, or other concerns before the communications are provided by an ISP, while civil law enforcement would still maintain a limited avenue to access existing electronic communications in appropriate circumstances from ISPs. Such a judicial proceeding would offer even greater protection to subscribers than a criminal warrant in which subscribers receive no opportunity to be heard before communications are provided.

We look forward to discussing with the Committee ways to modernize ECPA without putting investors at risk, and impairing the SEC from enforcing the Federal securities laws. I'm happy to answer any questions you may have.

[The prepared statement of Mr. Ceresney follows:]

Testimony on Updating the Electronic Communications Privacy Act

by

Andrew Ceresney
Director, Division of Enforcement

U.S. Securities and Exchange Commission

Before the
Committee on the Judiciary
United States House of Representatives
December 1, 2015

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee:

Thank you for inviting me to testify today on behalf of the Commission concerning the Email Privacy Act (H.R. 699) pending before your Committee. The bill seeks to modernize portions of the Electronic Communications Privacy Act (ECPA), which became law in 1986. I share the goal of updating ECPA's evidence collection procedures and privacy protections to account for the digital age. But H.R. 699, in its current form, poses significant risks to the American public by impeding the ability of the SEC and other civil law enforcement agencies to investigate and uncover financial fraud and other unlawful conduct. As described in more detail below, I firmly believe there are ways to update ECPA that offer stronger privacy protections and observe constitutional boundaries without frustrating the legitimate ends of civil law enforcement.

The SEC's tripartite mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The SEC's Division of Enforcement furthers this mission by, among other things, investigating potential violations of the federal securities laws, recommending that the Commission bring cases against alleged fraudsters and other securities law wrongdoers, and litigating the SEC's enforcement actions. A strong enforcement program is a critical piece of the Commission's efforts to protect investors from fraudulent schemes and

promotes investor trust and confidence in the integrity of the nation's securities markets. The Division is committed to the swift and vigorous pursuit of those who have broken the securities laws through the use of all lawful tools available to us.

Electronic communications often provide critical evidence in our investigations, as email and other message content (e.g., text and chat room messages) can establish timing, knowledge, or relationships in certain cases, or awareness that certain statements to investors were false or misleading. In fact, establishing fraudulent intent is one of the most challenging issues in our investigations, and emails and other electronic messages are often the only direct evidence of that state of mind. When we conduct an investigation, we generally will seek emails and other electronic communications from the key actors via an administrative subpoena – a statutorily authorized mechanism for gathering documents and other evidence in our investigations.[1] In certain instances, the person whose emails are sought will respond to our request. But in other instances, the subpoena recipient may have erased emails, tendered only some emails, asserted damaged hardware, or refused to respond – unsurprisingly, individuals who violate the law are often reluctant to produce to the government evidence of their own misconduct. In still other instances, email account holders cannot be subpoenaed because they are beyond our jurisdiction.

It is at this point in an investigation that we may in some instances, when other mechanisms for obtaining the evidence are unlikely to be successful, need to seek information from the internet service provider (ISP). H.R. 699 would require government entities to procure a criminal warrant when they seek the content of emails and other electronic communications from ISPs. Because the SEC and other civil law enforcement agencies cannot obtain criminal warrants, we would effectively not be able to gather evidence, including communications such as

[1] *See* Section 21(b) of the Securities Exchange Act of 1934, Section 19(c) of the Securities Act, Section 209(b) of the Advisers Act, and Section 42(b) of the Investment Company Act.

emails, directly from an ISP, regardless of the circumstances.[2] Thus, if the bill becomes law without modifications, the SEC and other civil law enforcement agencies would be denied the ability to obtain critical evidence, including potentially inculpatory electronic communications from ISPs, even in instances where a subscriber deleted his emails, related hardware was lost or damaged, or the subscriber fled to another jurisdiction.[3] Depriving the SEC of authority to obtain email content from an ISP would also incentivize subpoena recipients to be less forthcoming in responding to investigatory requests because an individual who knows that the SEC lacks the authority to obtain his emails may thus feel free to destroy or not produce them.

These are not abstract concerns for the SEC or for the investors we are charged with protecting. An effective enforcement program protects investors and the integrity of the capital markets by deterring securities law violations, punishing violators, returning money to injured investors, and preventing fraud. Among the types of scams we investigate where the ability to obtain content from ISPs would be most helpful include schemes – often perpetrated by individuals or small groups of actors – that target or victimize the elderly or other retail investors, including Ponzi schemes and "pump and dump" market manipulation schemes,[4] as

[2] Our cases are often the sole actions against wrongdoers: while we often conduct investigations in parallel with criminal authorities, the vast majority of our investigations do not have any criminal involvement. For example, although the criminal authorities have brought a significant number of insider trading cases in recent years, we have charged than more than 650 defendants with insider trading violations in the last 6 years, most of whom were not charged criminally.

[3] Chair White first raised these concerns in an April 2013 letter to Senator Leahy. A copy of that letter is attached.

[4] "Pump-and-dump" schemes involve the touting of a company's stock (typically microcap companies) through false and misleading statements to the marketplace. These false claims are often made on social media such as Facebook and Twitter, as well as on electronic bulletin boards and chat rooms. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.

well as insider trading activity that provides insiders with an unfair trading advantage over average investors and undermines our markets.

In these types of frauds, illegal acts are particularly likely to be communicated via personal accounts and parties are more likely to be non-cooperative in their document productions. For example, in an insider trading case, there appeared to be gaps in the emails the suspected tipper produced pursuant to the SEC's administrative subpoena. We were able to obtain the individual's personal emails from the ISP under ECPA and among the messages provided by the ISP was an email containing the alleged tip, which became a critical piece of evidence in our successful actions against the tipper and tippee. Similarly, in an investigation into a market manipulation scheme conducted by foreign stock promoters that used personal email for certain sensitive communications regarding the scheme, it was essential to obtain the emails from an ISP because the principals were in a foreign country, and we could not compel them to produce information. The resulting emails provided key evidence on multiple issues: the emails showed planning discussions for the illegal scheme and control by the defendants of the companies that proved to be central to the manipulation.

Technology has evolved since ECPA's passage, and there is no question that the law ought to evolve to take account of advances in technology and protect privacy interests, even when significant law enforcement interests are also implicated. There are various ways to strike an appropriate balance between those interests as the Committee considers the best way to advance this important legislation. Any reform to ECPA can and should afford a party whose information is sought from an ISP in a civil investigation an opportunity to participate in judicial proceedings before the ISP is compelled to produce the information; indeed, when seeking email content from ISPs in the past, the Division has provided notice to email account holders in

keeping with longstanding (and just recently reaffirmed) Supreme Court precedent.[5] Thus, in contemplating potential solutions, the Committee could consider language that would (1) require civil law enforcement agencies to attempt, where possible, to seek electronic communications directly from a subscriber before seeking them from an ISP; and (2) should seeking them from an ISP be necessary, give the subscriber or customer the opportunity to challenge the request in a judicial proceeding. If the legislation were so structured, an individual would have the ability to raise with a court any privilege, relevancy, or other concerns before the communications are provided by an ISP, while civil law enforcement would still maintain a limited avenue to access existing electronic communications in appropriate circumstances from ISPs. Such a proceeding would offer even greater protection to subscribers than a criminal warrant, in which subscribers receive no opportunity to be heard before communications are provided.

Some have asserted that providing civil law enforcement with an ability to obtain electronic communications from ISPs in limited circumstances would mean electronic documents enjoy less protection than paper documents. That is not accurate. Indeed, as currently drafted, H.R. 699 would create an unprecedented digital shelter – unavailable for paper materials – that would enable wrongdoers to conceal an entire category of evidence from the SEC and civil law enforcement.

---

[5] *See City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2452 (2015) ("The Court has held that absent consent, exigent circumstances, or the like, in order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain precompliance review before a neutral decisionmaker."); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) (holding subpoenas "provide protection for a subpoenaed employer by allowing him to question the reasonableness of the subpoena, before suffering any penalties for refusing to comply with it, by raising objections in an action in district court. . . . We hold only that the defenses available to an employer do not include the right to insist upon a judicial warrant as a condition precedent to a valid administrative subpoena."); *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000) (stating issuance of a subpoena "commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands . . . As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process").

This should not be the case. The bill in its current form would harm the ability of the SEC and other civil law enforcement agencies to protect those we are mandated to protect and to hold accountable those we are responsible for holding accountable. There are multiple ways to modernize ECPA consistent with the law that would not impede our ability to protect investors and the integrity of the markets. We look forward to discussing with the Committee ways to modernize ECPA without putting investors at risk and impairing the SEC from enforcing the federal securities laws.

Thank you again for the opportunity to appear here today, and I would be happy to answer any questions you may have.

Mr. GOODLATTE. Thank you. Mr. Cook, welcome.

TESTIMONY OF STEVEN H. COOK, PRESIDENT, NATIONAL ASSOCIATION OF ASSISTANT UNITED STATES ATTORNEYS

Mr. COOK. Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, first of all, thank you very much for giving me the opportunity to address you and to give you the perspective of career prosecutors with respect to H.R. 699.

And let me get right to it. The importance of the Stored Communications Act or SCA, to the law enforcement community simply cannot be overstated. At issue are records of contact and communication by Internet and cell service providers. To understand the importance of these records to the law enforcement world, I'd ask you to pause and think for a minute about how these powerful resources are being used in the criminal world.

Child predators troll the Internet 24/7 for children to lure them away from their parents and their homes. Purveyors of child pornography often, with graphic pictures of children, sometimes infants being sexually molested, sell those images electronically across the Internet. Terrorists boast of their horrific crimes posting pictures of those online, and international drug dealers, gangs, and others involved in organized crime communicate effectively with coconspirators through email and texts.

When you realize how pervasive this technology is in the criminal world, you quickly realize that the evidence covered by the SCA, or the Stored Communications Act, is central to our ability to solve virtually every type of crime. And our ability to access this information covered by the SCA and to access it quickly, can literally mean the difference between life and death. It can mean the difference between recovering a child alive and returning her to her parents, instead of the child being a victim of a vicious predator determined to commit unspeakable crimes.

And even beyond the critical role of stopping violent crimes in progress and rescuing victims, evidence covered by the Stored Communications Act is often central to the search for truth in our courts and our ability to bring those most dangerous in our community to justice.

But here are the problems with ECPA, and both the opening statements by the Chair and Ranking Member recognize this, ECPA and the Stored Communications Act were enacted in 1986. That was before much of this technology was in use, before any of us had any idea of its capabilities. And to continue to use a statutory framework with definitions that were enacted before any of this technology was known is just simply not workable. It does not fit.

That brings me back to H.R. 699. The primary goal of this bill seems to be to codify, correctly we would submit, *Warshak* and the extension of the Fourth Amendment protections to email in storage, and text in storage over 180 days. This is an issue on which we can all agree, but the bill goes farther. It goes much farther, and we respectfully submit, demonstrates a need for a comprehensive, not piecemeal reform. In my written testimony, I have addressed a number, but by far, not all of the concerns that we have.

I'd like to highlight two places where this bill creates or perpetuates limitations on law enforcement that far exceed those imposed, far exceed those imposed anywhere else in the law, burdens greater than those related to the search of a home, burdens greater than those related to the search of a body cavity.

While the Email Privacy Act expands Fourth Amendment protections and imposes a warrant requirement to compel disclosure of stored email or text, the statute does not recognize any of the well-established exceptions to the warrant requirement that would be applicable in every other circumstance. I know of no other area of the law where this is the case.

Second, the Email Privacy Act also imposes notice requirements unlike those found anywhere else in the law. The government has long been required to serve a copy of the search warrant on the person at the property being searched, and that requirement makes sense. It demonstrates to the homeowner or the business operator the authority for the search, and that homeowner or property owner is then free, in the usual course, to tell whoever they wish about it.

But the government has never been required and the law has never required the government to reach out to third parties and notify them of the search. It's not a discovery provision designed to alert those who are under criminal investigation of the ongoing investigation. And although there are specific, in fact, two-and-a-half pages of rules that would control when that can be extended, this simply is a rule that has never been imposed in any other context.

In conclusion, I'd just like to say that criminals have, and we have seen that they have unlimited access to these modern and powerful resources, and they make full use of them. For us on the law enforcement side to do our job, access to this information is critical. Information covered by the SCA has to be accessible to us.

That access, we respectfully recognize, of course, should be consistent with the privacy protections afforded by the Constitution, but Congress should not, as this bill proposes, impose new unprecedented and unwarranted limitations that will tie our hands in doing our jobs. Thank you.

[The prepared statement of Mr. Cook follows:]

Statement of

Steven H. Cook
President
National Association of
Assistant United States Attorneys

Before the United States House of Representatives
Judiciary Committee

Hearing on H.R. 699
"The Email Privacy Act"

December 1, 2015

I. Introduction

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for the opportunity to address you today. I am the president of the National Association of Assistant United States Attorneys, a professional association representing the interests of Assistant United States Attorneys employed by the Department of Justice. Assistant United States Attorneys (AUSAs) are the career-level attorneys in the 94 United States Attorney Offices responsible for federal criminal prosecutions and civil cases involving the United States Government.

AUSAs are responsible for enforcing of the nation's criminal laws, including those addressing violent crime, drug trafficking, firearms, and terrorism. AUSAs also enforce civil laws, including those designed to combat fraud against the government. I am grateful to the Committee for the opportunity to share a career federal prosecutor's perspective on how the enforcement of the nation's laws would be altered by the Email Privacy Act, H.R. 699.

By way of background, I earned my undergraduate degree and law degree, graduating from the University of Tennessee College of Law with high honors. At the conclusion of law school, I served as a law clerk to a judge on the U.S. Court of Appeals for the Sixth Circuit Court. For the last 29 years, I have served as an Assistant United States Attorney in the Eastern District of Tennessee. During that time, I have been assigned to the Organized Crime Drug Enforcement Task Force; the General Crimes Section handling white collar crime, fraud, and public corruption; and as the Narcotics and Violent Crime Section Deputy Criminal Chief. For the past seven years, I have served as the Chief of the Criminal Division. It is important for me to emphasize, however, that the views I express today are mine and those of the National Association of Assistant United States Attorneys, not of the U.S. Department of Justice.

II. The Stored Communications Act and the Email Privacy Act

a. The Stored Communications Act, General Observations and the 180-Day Rule Fix of the Email Privacy Act

The Email Privacy Act, H.R. 699, proposes changes to the Stored Communications Act (SCA) a subpart of the Electronics Communications Privacy Act (ECPA) originally enacted in 1986. As our world has become increasingly reliant on technology, the SCA has come to play a pivotal role in law enforcement. In fact, electronic evidence—access to which is covered in large part by the SCA—is often critical to the apprehension of terrorists, child molesters, carjackers, drug traffickers, kidnappers, and murderers. It would be no exaggeration to say that lives often hang in the balance when law enforcement officials seek information under the SCA. For example, in a kidnapping case electronic information of the type covered by the SCA may provide law enforcement with the location of the kidnapper and child. Time is of the essence in such cases,

which unfortunately happen throughout our nation on a regular basis. Likewise, even in non-exigent circumstances information covered by the SCA very often is the lynchpin to solving crimes. Such information is often important to convicting the offender, vindicating the victim, protecting society, and exonerating the innocent.

Nevertheless, as one respected commentator has observed, "[d]espite its obvious importance, the statute remains poorly understood. Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA."[1] To be more direct, the SCA is a confusing statute even to those who use it regularly and study it carefully. It should therefore be no surprise that the SCA has spawned endless litigation. The result of that litigation has often been inconsistent rulings between the circuit courts, and in some circumstances inconsistency within the same circuit or district.[2] Among the most confusing, some would say illogical, provisions in the SCA is the so-called 180-day rule. As written, this rule allows law enforcement officials to obtain the content of email communications from an electronic communication service (ECS) provider without a showing of probable cause if the email has been stored by the ECS for more than 180 days.

The 180-day rule was a part of a legislative scheme enacted in 1986, and by 2010 the rule was so inconsistent with developing email usage and storage practices that one circuit court held it to be a violation of the Fourth Amendment. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The Email Privacy Act eliminates the 180-day rule and brings the SCA in-line with *Warshak*. More specifically, the Act provides broader privacy protections for email communications by requiring that law enforcement officers obtain a search warrant before accessing email content, regardless of how long the email has been stored by the ECS. NAAUSA applauds this change and is pleased to support that particular provision of the Act.

b. <u>The Email Privacy Act Beyond the 180-Day Rule: Problems Created</u>

The Email Privacy Act, however, goes much further than correcting the problem created by 180-day rule. It is those further steps that are problematic and raise important concerns that the

---

[1] Orin S. Kerr, *The Future Of Internet Surveillance Law: A Symposium To Discuss Internet Surveillance, Privacy & The USA Patriot Act: Surveillance Law: Reshaping The Framework: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It* 72 Geo. Wash. L. Rev. 1208, 1208 (2004). *See also,* Comment: *Blue Skies Ahead: Clearing The Air For Information Privacy In The Cloud*, 55 Santa Clara L. Rev. 467, 468 (2015) (describing the SCA as "outdated and disjointed" and "struggling to maintain applicability and legitimacy").

[2] *See, e.g., In re Application of the United States,* 620 F.3d 304, 310 n. 6 (3d Cir. 2010)(describing the many divergent opinions on just one issue dealing with 3703(d) orders); *In re Cell Tower Records Under 18 U.S.C. § 2703(D),* 90 F. Supp. 3d 673, 674 (S.D. Tex. 2015) (noting a split of authority within the district on whether cell tower records are available to the government under the SCA).

Committee should address. The remainder of my testimony will focus on those concerns. I will briefly mention those concerns before discussing each of them in more detail in later portions of my testimony.

First, and most importantly, the Email Privacy Act fails to recognize the exceptions to the warrant requirement including the emergency aid, exigent circumstances and consent exceptions. These exceptions are longstanding rules of Fourth Amendment law that have been recognized and applied by the Supreme Court for decades. By failing to specify these exception for email searches covered by the Act, Congress will be creating an unprecedented and unnecessary barrier to law enforcement access. It is also creating a dangerous barrier—a barrier that will lead to the loss of potentially lifesaving information in cases where time is of the essence. It is well settled that a warrantless search may be conducted of a person's most private place—his or her home—if exigent circumstances exist. There is simply no reason to provide email communications with more protection than that afforded to a person's home.

Second, the Email Privacy Act will pour more dirt into an already muddy pond by creating internally inconsistent definitions and adding more unfamiliar and unique legal requirements to an already complicated body of law. Third, and relatedly, the Email Privacy Act does very little to address the antiquated, inappropriate, and confusing provisions of the current law.

Finally, in the face of a rising a wave of violent crime, unprecedented heroin and opioid addiction, and well placed heightened concern about the risks and spread of terrorism, this is the wrong time to create new and confusing rules. It is also the wrong time to impose barriers to law enforcement that far exceed those imposed by the Constitution—barriers that will unnecessarily impede saving lives and the search for truth while doing little to protect privacy.

c. The General Structure of the SCA

For purposes of my testimony, the SCA can be divided into three oversimplified parts: (1) section 2701 creates a general rule limiting access to certain stored communications; (2) section 2702 allows the service provider to voluntary disclose stored content (e.g., email and text messages) and non-content information under enumerated circumstances; and (3) section 2703 establishes rules under which the government can compel disclosure of stored content and non-content information from a service provider.

d. By failing to recognize the longstanding search warrant exceptions, the Email Privacy Act will create unnecessary barriers to information critical to law enforcement operations

The Email Privacy Act requires law enforcement officials to obtain a search warrant in order to

access email or other content covered by the SCA. That, again, is a requirement NAASUA supports as a general matter. What NAASUA does not support is the failure of the Act to recognize and incorporate the longstanding and well-settled exceptions to the search warrant requirement. Those exceptions have been created in recognition of the fact that, at times, it may impracticable or imprudent for law enforcement officers to obtain a warrant. There is simply no principled reason why law enforcement officers would *always* need a warrant to obtain information covered by the SCA when they can search a person's most intimate space (the home) without a warrant if certain circumstances are present.

By requiring law enforcement officials to secure a search warrant, Congress, through the Email Privacy Act would provide email content the same level of protection as our most private and intimate possessions, including the home. The home has always been viewed as particularly in need of protection because "[a]t the very core [of the personal rights protected by the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[3] The general rule, therefore, is that law enforcement officers may not search a person's home without a warrant.

The hurdles imposed by the warrant requirement are not insignificant. Fundamentally, law enforcement officials must show that there is probable cause to believe a crime has been committed, they must particularly describe the place to be searched and the items to be seized, and they must present this information for independent judicial review. In addition, state and federal rules and statutes impose often technical requirements that must be met. For example, with respect to federal search warrants, rule 41 of the Federal Rules of Criminal Procedure addresses who has the authority to issue the warrant; lists specific categories of property subject to search; limits who can request the warrant; imposes recording requirements; establishes procedures covering execution including time limits, time of day parameters, requirements for documenting warrant execution times; sets rules regarding creating an inventory and providing a copy of the warrant to the person from whose premises the property was taken; and establishes a requirement for creating a receipt and making a return to the issuing judge. Additionally, rule 41 imposes special rules for seizing electronic storage media and tracking devices. Even beyond that, there are several statutes with additional limitations or directives.[4]

---

[3] *Silverman v. United States*, 365 U.S. 505, 511-12 (1961). *See also Steagald v. United States*, 451 U.S. 204, 211 (1981); *Payton v. New York*, 445 U.S. 573, 586 (1980) ("the 'physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed.'") (*quoting United States v. United States District Court*, 407 U.S. 297, 313 (1972)). *Silverman v. United States*, 365 U.S. 505, 511-12 (1961) ("The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (citation omitted).

[4] *See* 18 U.S.C, § 3105 (persons authorized to serve search warrant); 18 U.S.C. § 3109 ("[b]reaking doors or windows for entry or exit"—or the so-called knock and announce rule); 18

It is important to note that the constitutional rules that require search warrants are not ironclad. They are subject to a limited number of exceptions where the Supreme Court has concluded that it is reasonable to conduct a search without a warrant. Those exceptions include, but are not limited to, exigent circumstances, emergency aid, and consent. If one of those exceptions is present, a law enforcement officer may conduct a search—even of the most sacred enclave, a house—without a search warrant.

As it is currently written, the Email Privacy Act imposes a statutory search warrant requirement mirroring the presumptive warrant requirement of the Fourth Amendment. The Act, however, glaringly fails to recognize any of the longstanding and deeply rooted exceptions to the warrant requirement. Put another way, the Email Privacy Act provides *greater* protection to email communications than *any* other item or place. That simply does not make good sense. And, it could cripple law enforcement efforts in cases where time is an unavailable luxury.

This concern can be highlighted by an all too likely example. Two gunmen storm a crowded public place and use firearms and explosives to kill and maim dozens of people before escaping. The gunmen are quickly identified as ISIS operatives, and investigators determine that an apartment and particular cell phone numbers and email addresses are associated with them. At this point in the investigation, there are two immediate law enforcement concerns: (1) determining (and preventing) any imminent future attacks the gunmen and/or their affiliates may have planned; and (2) capturing and prosecuting the gunmen.

To address those concerns, law enforcement officials would need to immediately know: (1) where the terrorists had recently been (that is, location information for the recent past); (2) with whom they had been communicating; (3) the content of those communications; and (4) whether there were conspirators, explosives, or other dangerous instrumentalities inside the apartment.[5] The first three categories of information would typically be in the possession of the cell phone service provider(s) and, therefore, covered by the SCA. Although time would be of the essence and the risk of delay potentially catastrophic (in other words, a textbook example for application of the emergency aid and exigent circumstances exceptions), a warrant would be required to obtain the communication information under the proposed provisions of the Email Privacy Act. Ironically, at the same time, well-established law would permit law enforcement authorities to conduct a warrantless search of the apartment—the location that has always received the highest level of protection. Perhaps even more ironic, the Supreme Court recently held that police

---

U.S.C. § 3117 (mobile tracking devices warrant); 18 U.S.C § 3103a (additional grounds for issuing warrant—or the so-called sneak and peek warrant); 18 U.S.C. § 3105 (persons authorized to serve search warrant—broadening the common law rule regarding who can serve a search warrant) 18 U.S.C. § 3107 (service of warrants and seizures by Federal Bureau of Investigation).

[5] Of course, subscriber and toll record information would be available under 18 U.S.C. § 2709 once appropriate approvals were secured.

officers who obtain a suspect's cellular phone may search that phone (which may also serve as a repository for email communications) without a warrant if there are exigent circumstances.[6] The same should be true for searches of information such as email that is covered by the SCA.

Some might point out that in a situation like the one described above, the service provider could voluntarily choose to provide the information to law enforcement under 18 U.S.C. § 2702. While that may be true, it would be a novel and anomalous development in the law to allow the possessor of potentially lifesaving information to stop law enforcement from obtaining information that they could otherwise constitutionally access. Allowing the service provider to decide whether to turn information over in an emergency situation is no different than allowing the terrorists' apartment manager to decide whether to grant the police admission into the apartment to search for explosives or evidence.[7]

And these concerns—about leaving the determination to the service provider rather than law enforcement in an emergency situation—are not remote or hypothetical. Failures have led to disastrous and highly publicized tragedies.

One such example was the abduction of Kelsey Smith. As described in one article:

> Kelsey was an 18-year-old girl from Overland Park, Kan., who was abducted in broad daylight in the parking lot of a Target store just a couple of miles from my house on June 2, 2007.
>
> Sixteen seconds. That's how long it took Kelsey's killer to overtake her when she put a package in her car. He abducted her, raped her and strangled her with her own belt.

---

[6] *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) ("In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone. The defendants here recognize — indeed, they stress — that such fact-specific threats may justify a warrantless search of cell phone data.")

[7] *Ryburn v. Huff*, 132 S. Ct. 987, 990 (2012)(construing current emergency aid doctrine and holding that entry into home not a violation of residents' rights because there was a "reasonable basis for concluding that there [was]an imminent threat of violence"); *Michigan v. Fisher*, 558 U.S. 45, 49 (2009) ("Officers do not need ironclad proof of 'a likely serious, life-threatening' injury to invoke the emergency aid exception."); *Brigham City v. Stuart*, 547 U.S. 398, 400(2006) (officers may enter a residence without a warrant when they have "an objectively reasonable basis for believing that an occupant is . . . imminently threatened with [serious injury].")

> It was four days before Kelsey's body was found in a wooded area in Kansas City, Mo. It took those four days for Verizon Wireless, her cellphone carrier, to hand over information about the location of her cellphone, which she had on her when she was abducted. When they did, her body was found within an hour.[8]

In response to this tragedy and others like it, twenty-one states across the country are reported to have enacted legislation, often called the Kelsey Smith Act, to provide mandatory access to law enforcement authorities in certain emergency circumstances.[9] Similarly, a Kelsey Smith Act was introduced in the last Congress in both the House, H.R. 1575, and in the Senate, S. 721.

Consistent with these considerations, any warrant requirement provision in the SCA should contain an emergency aid exception that parallels the applicable, long standing exception recognized in Fourth Amendment jurisprudence. To be clear, law enforcement officials, not service providers, should decide whether the requirements for the exception have been met.

The operation of the consent exception is problematic for the same reason. For example, if a subscriber to the cell phones associated with the terrorists consented to turning the information over to law enforcement authorities, further process would still be required, again, unless the service provider agreed. Allowing the service provider to decide whether to turn over information when the consent exception to the warrant requirement is met turns the law on its head. To use the same analogy, if police investigating terrorist activity secured consent from an occupant to search an apartment believed to be used to build bombs (or for that matter by a petty thief believed to be hiding stolen property) the landlord would not be free to deny the police access. The opposite is true: the landlord is obligated under the law to comply with the police demand for admission.

There is no principled reason for the law to treat service providers any differently than other third parties who are in possession of or have access to evidence or information needed by law enforcement. If law enforcement officials determine that one of the narrow and limited exceptions to the warrant requirement exists and they inform the service provider that they need specific information, the service provider should be duty-bound to provide that information, just as any other third party intermediary would be. These same considerations should apply to the Email Privacy Act. But as written, the Email Privacy Act imposes a warrant requirement for

---

[8] Diana Reese, *Kelsey Smith Act Would Save Lives, Cost Taxpayers Nothing* The Washington Post (April 18, 2013), *available at* https://www.washingtonpost.com/blogs/she-the-people/wp/2013/04/18/kelsey-smith-act-would-save-lives-cost-taxpayers-nothing/

[9] The Kelsey Smith Foundation, http://kelseysarmy.org/#ks-act

certain information, yet does not recognize any of the well-established exceptions to the warrant requirement; it further insulates service providers from the obligation shared by every other member of our society by allowing service providers to decide when they deem it appropriate to disclose information.

It is one thing for Congress to offer enhanced privacy protections for email and related communications by requiring a search warrant. It is quite another thing for Congress to afford such communications an unparalleled level of protection that will potentially jeopardize public safety. NAAUSA respectfully, but strongly, recommends that Congress amend the Email Privacy Act to make clear that the Act's search warrant requirement is subject to same the longstanding exceptions that apply to the Fourth Amendment's search warrant requirement.

e. The Email Privacy Act places rules and burdens on the government that are not imposed for any other searches

The Email Privacy Act imposes other unnecessary rules that go beyond those created by the Fourth Amendment, the United States Code, or the Federal Rules of Criminal Procedure for searches in any other context. It has long been the case that when law enforcement officials execute a search warrant they provide "a copy of the warrant and a receipt for the property taken to the person from whom, or whose premises, the property was taken . . .."[10] The purpose of this rule is obvious: it demonstrates the lawful authority of the law enforcement agency to conduct the search and collect evidence.

Thus, if a law enforcement agency executes a search warrant at a house where the target of the investigation does not live, but has stored, for example, his bomb making materials (or anything else of evidentiary value), the law enforcement agency must provide the resident of the home with a copy of the search warrant. And, although the resident can normally call the target, the law enforcement agency has no obligation to notify the target of when the search occurred, what was seized, under what authority the search was conducted, or even that there was a search at all. That is true even if the law enforcement agencies are conducting an ongoing investigation of the target and even if they know they intend to use the items as evidence against the target in a future criminal prosecution. The search warrant notice provision is not a "red alert" tool designed to notify an individual that he is under investigation, who is investigating him, why he is being investigated, or what evidence the government has developed up to that point.

In the context of electronic evidence, the rules should be the same: if law enforcement agencies serve a search warrant and seize evidence, they should be obligated to provide a copy of the search warrant to the person in possession of the evidence—the service provider. The service provider, therefore, should be treated no differently than the friend of a defendant whose home is

[10] Fed. R. Crim. P. 41(f)(1)(C).

searched because he happens to be storing some material belonging to the defendant. Absent a court order directing otherwise, the service provider (as a matter of contract, customer relations, or otherwise) is, of course, free to disclose that information as it chooses.

The Email Privacy Act goes far beyond requiring that the search warrant be served on the person whose premises is being searched (the service provider) and creates additional unprecedented, problematic burdens and obligations on law enforcement agencies. The Email Privacy Act adds a somewhat complex set of rules requiring the government (and then allowing the government to seek delay(s) in the obligation) to serve a copy of the search warrant not only on the person on whose premises the evidence exists, but on the target of the investigation. That alone is unprecedented. And yet the Email Privacy Act goes even further by requiring the government to provide six categories of information. To be clear, if the government searched from top to bottom the home of a friend of the target where all the evidence of a crime was being hidden, the law would impose no obligation during the investigative stage to serve the search warrant on anyone other than the person in possession of the evidence, much less would it require the law enforcement agencies to disclose these six categories of information.

Most troubling among the six categories of information, the Email Privacy Act would require the government to reveal "the nature of the law enforcement inquiry" to the subscriber. No historical practice or public policy consideration can, on balance, support this new and novel rule. Moreover, exactly how much information is needed to meet this standard—notifying the target of the investigation of "the nature of the law enforcement inquiry"—is not clear and will undoubtedly result in needless and time-consuming litigation. Finally, it should be noted that this new and unprecedented notice requirement is imposed regardless of whether the law enforcement agency has been able to determine the true identity of the subscriber. That is important for the Committee to recognize because very often email accounts used in criminal activities are operated under false names and/or are created in foreign countries.

The Email Privacy Act also creates a set of rules (in fact, two-and-a-half pages of rules) allowing the government to ask the court for permission to delay notice under narrow, specific, and limited circumstances. Assuming a judge agrees with the initial application to delay notice, if, for whatever reason (even clerical mistake), and without regard for the seriousness or nature of the criminal activity under investigation, a deadline is missed for extending the delayed notice, on its face the new early disclosure rules mandate immediate notice to the subscriber.

One final point on the newly-created notice provisions must be made. Many federal investigations are expansive in scope and are frequently interstate and often international in nature. Such investigations also often involve dozens, sometimes hundreds, of targets and span many years. Increasingly evidence of guilt is developed under the SCA and imposing these increased and unprecedented obligations will substantially burden law enforcement while

delivering very little benefits. Someone will have to track every delayed notice, prepare a motion and proposed order for an extension, and present it to a court. The motions, in turn, will be an additional draw on limited judicial resources—resources that could be put to use much more productively—since every motion will have to be processed by the court and then reviewed by a judge.

In summary, the Email Privacy Act creates new and unprecedented notice and information disclosure rules and obligations that far exceed those needed to accomplish the legitimate historical purpose of notice—to demonstrate the lawful authority for and scope of the search. The Email Privacy Act should simply incorporate the same notice requirements that apply for other searches that are carried out daily throughout our country.

f. The Email Privacy Act will further complicate an already confusing area of the law

As observed earlier, courts, commentators, and practitioners alike have found the SCA to be confusing. By creating even more rules and introducing internal inconsistencies, the Email Privacy Act will further complicate the SCA. With regard to new rules, as noted the Email Privacy Act imposes a rule 41 warrant requirement which in and of itself carries with it a wide range of rules and limitations. By then imposing unique notice requirements, delayed notice rules, and ambiguous information disclosure obligations, the Email Privacy Act simply adds more confusion.

In addition to unnecessarily adding to the complexities of the SCA, the Email Privacy Act creates additional ambiguities. For example, section 2705(a) provides in part:

> (1) IN GENERAL.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

(underscoring added.)

Since search warrants are uniquely a criminal enforcement tool used to gather evidence of criminal activity (that is to enforce criminal laws), it would seem that by definition the entity seeking the warrant would be a law enforcement agency. Thus, it is difficult to determine what other "government entity" other than federal law enforcement agencies may apply for a warrant. So, when exactly does the 90-day notice provision apply? Perhaps the intent of the provision is

to allow agencies other than law enforcement agencies to be authorized to obtain search warrants for information covered under the SCA. But, given the historical limited use of search warrants, if Congress desires to allow non-law enforcement agencies to apply for warrants under the Email Privacy Act, it must make its intent much more clear. Confusion and litigation is all that will result from the current language.

g. The Email Privacy Act does nothing to address the antiquated, inappropriate, and confusing provisions of the existing version of the SCA

If Congress is going to make revisions to the SCA, it should do so in a way that remedies the antiquated and confusing provisions. As observed earlier, section 2702 is the voluntary disclosure section—that is, after creating a general rule prohibiting disclosure of content and non-content information, this section of the SCA allows, but does not require, the service provider to disclose information under listed circumstances. One voluntary exception allows the service provider to disclose non-content on consent of the subscriber and (under narrower circumstances) content information on consent of a subscriber or party to the communication.[11]

Examples abound when the consent exception could quickly result in apprehension of a dangerous criminal or otherwise avert loss of life or property. In the context of a missing child this exception could prove to be a lifesaver. As is often the case during the first few critical minutes when a child is discovered to be missing, a review of records revealing who the child last communicated with, where he was at the time, and the substance of that communication could lead to a swift and safe recovery of the child. However, delaying until evidence develops demonstrating foul play (thus possibly triggering the voluntary emergency disclosure section should the provider in its discretion elect to assist under that provision) could prove disastrous.

In this setting, a parent is nearly always the subscriber and with the parent's consent the provider may disclose important records information to law enforcement officials without delay. But the provider is not required to do so and, despite this clear authority, providers rarely honor the subscriber's wishes to provide law enforcement this critical information. As noted earlier in connection with the 2703 mandatory disclosure section, this is analogous to allowing the apartment manager the authority to deny police access to a suspect's apartment when the police have consent of the tenant. Any reforms to the SCA should include a fix for this anomaly.

The provision of the SCA addressing the standard for issuing a disclosure order, 18 U.S.C. § 2703(d), should also be clarified. That provision provides in part:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and

[11] 18 U.S.C. § 2702(b)(3) and (c)(2).

> shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

(Underscoring added.) The underscored language has led to a split in the federal appellate courts on whether the courts are obligated to enter an order when the standard of proof is met. [12] It seems reasonable to conclude that Congress intended that courts would perform their responsibilities to administer this whenever the evidentiary standard is met but the law need to be clarified.[13]

Additionally, section 2703(c)(2) should be amended to require the disclosure of "to/from" information in email communications with a subpoena. This would simply make the SCA consistent with the practice regarding telephone calls where that non-content information is available by subpoena.

Finally, but importantly, by imposing a warrant requirement as the exclusive vehicle through which the government can compel service providers to disclose content information, Congress has essentially placed this evidence beyond the reach of Assistant U.S. Attorneys, Department of Justice trial attorneys and other state civil litigators investigating illegal conduct of all sorts. For example, virtually every U.S. Attorney's office has an Affirmative Civil Enforcement Unit responsible for pursuing, among others, health care fraud and false claim act violations. Since a search warrant is a criminal investigative tool—requiring a showing that a crime has been committed—a wide range of evidence will be shielded by the Email Protection Act from the truth seeking process in these cases.

---

[12] *Compare In re Application of the United States,* 724 F.3d 600 (5th Cir. 2013) (interpreting this provision to require a court to issue a 2703(d) order when the government makes the "specific and articulable facts" showing), *with In re Application of the United States,* 620 F.3d 304 (3d Cir. 2010) (concluding 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 the government makes the requisite showing).

[13] *Cf.* Fed. R. Crim. P. 41(d)(1)("In General. After receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.") (emphasis added).

III. Conclusion

NAAUSA agrees that imposing a warrant requirement for the government to secure stored email in a criminal investigation is appropriate as a general rule. The Email Privacy Act, unfortunately, goes much further and in the process creates more problems than it solves First, and most importantly, the Email Privacy Act creates unprecedented and unnecessary barriers to this often lifesaving information—barriers that substantially exceed what would be required to search any other location, including the search of a home. Second, the Email Privacy Act will further complicate an already confusing area of the law by creating internally inconsistent definitions and layering more unfamiliar, unprecedented and unique legal requirements. Third, the Email Privacy Act does nothing to address the antiquated, inappropriate, and confusing provisions of the existing version of the SCA.

The SCA is desperately in need of comprehensive reform to bring it in-line with modern computing and communication technology. NAAUSA, therefore, is pleased to see that the Committee is considering revisions to the SCA. But, the Email Privacy Act as it is currently written is not an effective way of addressing the problems that currently exist with the SCA. NAAUSA stands ready and willing to further assist the Committee in drafting a bill that appropriately strikes the delicate balance between individual privacy and the need to protect society from dangerous criminals intent on wreaking havoc throughout this great country.

Mr. GOODLATTE. Thank you, Mr. Cook.
Mr. Littlehale, welcome.

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

Mr. LITTLEHALE. Chairman Goodlatte, Ranking Member Conyers, Members of the Committee, thank you for inviting me to testify. I'm a technical investigator in Tennessee, and I serve on the technology committee of the Association of State Criminal Investigative Agencies. As you know, State and local law enforcement agencies work the vast majority of criminal investigations in this country. Lawful access to electronic evidence is critical for us in those cases every day, and H.R. 699, in its current form, does not sufficiently protect that access.

To give you some sense of the volume of potential electronic evidence in our cases, consider a stranger abduction of a 4-day-old infant in Nashville. Over the course of an intensive 4-day investigation, my unit processed and explored leads on hundreds of telephone numbers, social media accounts, computers, and mobile devices. At a time when every second counts, my fellow agents and I spend a significant amount of time simply trying to make contact with various providers to declare an emergency, calling and recalling to make sure that our process was received and expedited. We had to process hundreds of leads, any one of which could have been the key to finding the victim.

Volume alone isn't the only issue. We must also contend with a lack of structure governing responsiveness. In another Amber alert investigation, we received a lead that the creator of a posting on a social media platform may have information about the child's location. When we contacted the provider, they noted that ECPA's emergency provision is permissive rather than mandatory and demanded legal process before they turn over the records.

We know H.R. 699 has a great deal of support, but we believe much of that support is based on only one part of the bill, creating a uniform probable cause standard for stored content. Advocates for ECPA reform argue that the contents of an email or document stored in the cloud should be subject to the same protections as a letter in your desk drawer at home. H.R. 699 would do that, but it goes farther to create an enhanced statutory framework of proof standards, notice requirements, and expand the definitions of covered records that you would give greater protection for records stored by third-party service providers than for that envelope in your desk. And it would do this without extending any of the tools that law enforcement can use to obtain evidence in the physical world after we demonstrate probable cause to a neutral magistrate and get a warrant, like law enforcement controlled warrant exceptions and warrant execution timelines.

Bringing ECPA into balance should put the physical and digital worlds on the same plane, not favor digital evidence over physical evidence. H.R. 699 should be amended to reflect a more balanced approach that protects privacy and ensures that law enforcement can access the evidence it needs, and when we get a warrant, it should behave like a warrant not a subpoena with a higher proof requirement.

Demonstrating probable cause to a neutral magistrate should allow us to gather evidence with the same timeliness and effectiveness that we would expect in the real world.

The notice provisions in the bill would require us to describe our case to targets of a criminal investigation, even as we're pursuing leads. That endangers investigations. We also urge the Committee to carefully balance the need for notification against the resource burden it places on us. Time spent complying with arbitrary timelines means less time investigating crimes and could compromise sensitive information.

I urge you to ensure that whatever standard of proof you decide is appropriate, you also ensure that law enforcement can access the evidence we need reliably and quickly. Speed is important in all investigations, and ECPA reform should impose structure on service providers' response to legal demands. A requirement for automated exchange of legal process and records with service providers would help speed access to evidence, provide transparency, and authenticate law enforcement process.

Warrants under EPCA should look like warrants everywhere else. That means that standard exceptions to the warrant requirement like exigency and consent should exist, and law enforcement should control whether or not they are invoked, just like we can do when executing warrants in the physical world. Everybody agrees that law enforcement should have rapid access to communications evidence in a life-threatening emergency, but that is not always the reality.

Industry and privacy groups suggest that some law enforcement emergency declarations are unfounded, but those are unreviewed unilateral determinations. Isn't law enforcement on the ground in the best position to assess the presence or absence of defensible exigency in a particular case? We already do it in other contexts all the time, and there is an existing body of case law in the courts to determine whether or not we are correct.

In closing, I want to re-emphasize how important both aspects of ECPA are to our Nation's criminal investigators. We agree that ECPA should be updated, but any effort to reform it should reflect its original balance between assuring law enforcement access to evidence through legal demands and protecting customer privacy.

The balance proposed by H.R. 699 goes too far in extending all the burdens of the traditional search warrant scheme to a much broader range of records without any of the common law exceptions, while requiring us to give unprecedented notice to investigative targets just because the evidence we're seeking is electronic.

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

[The prepared statement of Mr. Littlehale follows:]

Written Statement by

Richard Littlehale
Assistant Special Agent in Charge
Tennessee Bureau of Investigation

Before the United States House of Representatives Committee on the Judiciary

Hearing on
"H.R. 699, the Email Privacy Act"

December 1, 2015

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for the opportunity to speak to you today. 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 twenty years in support of cases ranging from searches for violent fugitives to efforts to recover abducted children and victims of minor sex trafficking.

I am grateful to the Committee for the opportunity to share a criminal investigator's perspective on the challenges that law enforcement faces when gathering digital evidence. The evidence regulated by ECPA can be invaluable in the most critical of law enforcement investigations, and 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. As I noted in testimony on ECPA reform before the Senate Judiciary Committee in October, 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 criminal investigations in this country. Since the laws before the Committee today govern our access to much of the digital crime scene, any change in the law will impact us greatly. Our community appreciates your recognition that our expert perspective should be a central consideration of any update to ECPA.

I offer testimony here today as a representative of the Association of State Criminal Investigative Agencies (ASCIA). The Director of the Tennessee Bureau of Investigation, Mark Gwyn, is the current president of ASCIA.

H.R. 699 and the Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA") is one of law enforcement's primary tools for gathering the electronic evidence that forms the building blocks of the state's case in a wide range of critical investigations. As I will outline in greater detail below, H.R. 699 goes far beyond the commonly stated goal of modernizing ECPA by requiring a search warrant for all stored content. In fact, it creates protections for a wider range of stored electronic evidence that could pose a greater hindrance to law enforcement than protections afforded evidence stored on a computer inside a house or office. Searches in response to ECPA process are performed by service providers, not by law enforcement officers, and H.R. 699 extends the notice provisions previously necessary only with lesser levels of process like subpoenas along with the probable cause standard. The end result is that law enforcement has to get a search warrant to access more evidence, and must bear the added burden of notice requirements that were previously limited to lesser process, without the benefit of controlling the execution of the warrant.

In addition, H.R. 699 fails to include any of the provisions that state and local law enforcement has sought for some time to lessen the investigative impact of an expansion of the probable cause standard. With a traditional warrant, law enforcement controls when we execute the warrant, how quickly we gather the evidence, and how many searchers we take along. We gather the evidence that we believe the warrant covers, and we afford the accused an opportunity to challenge the manner in which it was gathered in court. In the ECPA scheme, law enforcement is at the mercy of virtually unregulated service provider response. Simply put, H.R. 699 does a number of things to make our job harder, and nothing to make it easier; as a result, it will negatively impact our investigations in areas ranging from online child exploitation and kidnapping response to murder, drug trafficking, and organized crime. It may be that some parties will be content if our jobs are harder, but we expect that crime victims and their families won't be among them.

Congress has always recognized that ECPA is meant to provide access to evidence as well as to protect privacy. We agree that the law should be updated, but we strongly urge that any effort to reform ECPA also reflect this two-fold aim of protecting privacy AND assuring law enforcement's ability to obtain digital evidence when we are lawfully authorized to do so. H.R. 699 creates extra burdens on access, and does nothing to address law enforcement concerns about the timeliness, completeness, and quality of service provider responses to legal demands.

A probable cause standard may well be appropriate for access to evidentiary content on private servers, but we do not believe it is in the interest of justice to create a new statutory framework that affords that evidence more protection that it would receive in the real world simply because it is digital. In addition, any effort to amend ECPA should include provisions that will soften the impact of higher proof standards on investigations and guarantee that the process law enforcement does obtain is answered appropriately. Because H.R. 699 in its current form imposes burdens that will make our job harder without offering any relief in other areas, we urge the committee not to pass H.R. 699 without amending the bill to reflect greater sensitivity to the concerns of the state and local law enforcement community. When we have to get a warrant, it should mean something; right now, H.R. 699 turns the compulsory process of a search warrant into a subpoena with a higher proof requirement.

Access to Evidence in the Digital Crime Scene

The crime scene of the 21st century is often replete with digital evidence. This digital crime scene, including electronic communications records in the possession of private companies, often holds the key to solving the case. It also holds the key to ruling out suspects and exonerating the innocent. Investigators' ability to access that evidence 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, the lion's share of the scholarly, media, and advocacy attention given to the question of lawful access to stored content has focused on the level of proof required to obtain digital evidence. This narrow focus neglects a set of critical issues that impact law enforcement's ability to gather digital evidence from private companies every day across the country. I am referring to the quality and character of service provider responsiveness to law enforcement legal demands, as well as well-intentioned but overly burdensome accountability considerations like customer notification and reporting requirements. From the perspective of an investigator working the digital crime scene, these concerns impact our ability to gather the digital evidence we need as much or more than any other, and they have been noticeably absent from the ECPA reform debate.

The simple truth is that legal and technological 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 just as frequently it is because of **non-technical barriers to access**. The companies that retain these records are often unable or unwilling to respond to law enforcement's lawful demands in a timely manner, and there are few consequences for an incomplete or inaccurate response. 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.

As Congress considers simplifying the legal requirements for obtaining communications content and non-content records, and whether or not to change the standards law enforcement must meet to obtain that evidence, the full range of non-technical barriers to access must have a place in the discussion. I would 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 digital evidence that we need to do our jobs reliably and quickly once that process is obtained.

In an effort to better inform the committee, I solicited feedback on these non-technical barriers to access from a wide range of law enforcement agencies, specialties, and investigative focuses. More often than not, the responses were along the lines of "oh, you mean beyond the usual?" Be-

yond routine turnaround times measured in months, the inability to speak to a human being about your case in a timely manner, uneven access to records in emergencies? Beyond service providers who routinely pre-litigate the legal process instead of leaving that to the courts, who return legal demands without complying because the demand failed to use the magic language of the moment that the provider prefers, regardless of whether or not it is statutorily or constitutionally compelled? These are the day-to-day realities of professionals working the digital crime scene, not isolated and unfortunate bumps in the road.

Consider a case a few years ago regarding the stranger abduction of a 4-day-old infant in Nashville where my unit was tasked to work the digital crime scene. Over the course of an intensive four-day investigation, my unit processed and explored leads on hundreds of telephone numbers, social media accounts, computers and mobile devices. At a time when every second counts, my fellow agents and I spent a significant amount of time simply trying to make contact with various providers to declare an emergency, calling and recalling to make sure that our process was received and expedited as necessary. In one instance, a voice mail that contained potentially critical evidence for the prosecution of the kidnapper was lost because a cellular provider mishandled a preservation request. In another, we had to spend precious time trying to get a service provider on the phone to figure out the time stamps of phone records, because it was unclear on the face of the records when the critical calls were made. All while processing hundreds of electronic leads, any one of which could be the one that holds the key to rescuing the victim. These issues are obviously problematic, but this is a routine part of a criminal investigator's day working the digital crime scene.

Another example that highlights a need for reform of current law started with a threat of a mass casualty attack on a high school in a large Texas city. An unknown party threatened a high school and responding police in March 2015 on a popular social media platform, and backed it up with a picture of an assault rifle; this caused the school to go into lockdown. Law enforcement issued a subpoena and a judicial non-disclosure order (to keep the provider from notifying the user) to attempt to identify the user who posted the threat. Even though the threats were posted on social media for everyone to see, the provider still would not turn over records under the emergency exception and required law enforcement to get a search warrant before they would release content. Fortunately, the attack did not materialize that day, and the investigation continued. By late April, investigators had determined that the sender used a free virtual private network (VPN) service to mask their Internet Protocol address while posting the threats, and investigators issued a court order to the VPN provider. Two and a half weeks later, they received a response stating that the provider found no responsive records, and indicated that "unfortunately due to limited resources our logs are purged at the latest every 48 hours." Was the threat real, or a hoax? Was the sender serious about the attack but deterred by the lockdown, or simply wasting resources and scaring children for their own amusement? The community and Texas authorities may never know.

These examples highlight the ways in which H.R. 699 provides more protection for digital evidence than evidence in the physical world. We have to comply with an extra range of notice provisions, and we are at the mercy of the service providers for responsiveness. We can't simply execute the search warrant the way we can in the physical world. That is a major concern, and if the

intent is to bring the law into balance for the 21st Century, we strongly believe legislation should not create higher protections for a particular piece of evidence that is stored electronically rather than in a filing cabinet, nor should it elevate burdens on law enforcement without providing assistance with long-standing problems like the ones outlined below.

Non-Technical Barriers to Access

As we consider non-technical barriers to access in more detail, we should be mindful of a simple fact that is 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.

Timeliness and quality of service provider response. The importance of the timeliness and quality of service provider responses to lawful demands from criminal investigators for digital evidence cannot be overstated. Of all the issues that we are concerned about in this ECPA reform discussion that could increase the safety of the American citizens we serve without negatively impacting their privacy, this is the most significant. When we get the legal process that we need, let's make sure we get the records quickly, and make sure that they are complete and responsive. Let's minimize administrative latency in the compliance process. That is what would help us solve crimes more effectively.

There is no requirement in current law – including the service and execution of search warrants based upon probable cause – for providers to respond in a timely fashion to lawful process requests by governmental entities. Voluntary compliance has not worked as effectively as we need, because a truly efficient compliance operation might put a provider at a competitive disadvantage, because their competitors aren't required by law to spend the same resources. Any contemplated change in the law that would result in a lengthening of the investigative timeline – including moving some evidence to a probable cause standard that can currently be obtained on a lesser showing – should be accompanied by provisions that ensure accountability and prompt response by service providers to legitimate law enforcement requests.

It is worth considering the traditional legal framework surrounding search warrants as we consider these questions. In the traditional physical world context, when law enforcement demonstrates probable cause to a neutral magistrate and the magistrate issues a warrant, it then becomes the law enforcement officer's decision about when to execute the warrant, how hard to search, and so on, based on the facts and circumstances of the case. In the digital space, it is the providers who actually conduct the search. Law enforcement typically has no visibility into the process of conducting the search or how thorough the search is. This results in sometimes haphazard diligence with respect to compliance, incomplete responses, and turnaround times measured in weeks and months.

Further, service providers often "pre-litigate" search warrants, returning them without being executed because of some perceived defect in language in the warrant. That is unheard of in other contexts; law enforcement investigators gather the evidence that they feel is responsive to the warrant, and then the defendant has an opportunity to challenge that collection later. The only option to really explore this would be to ask the prosecutor to seek a show cause hearing, and it is difficult to find the time for that when you are looking for a missing child, a dangerous fugitive, or identifying tentacles in an online child porn network. As a result, this practice on the part of service providers goes largely unchallenged. This is almost unheard of outside the digital space: when law enforcement demonstrates probable cause to a neutral magistrate and obtains a search warrant, we decide what evidence to gather and when we gather it, and any aggrieved party has the ability to object later through the courts. By creating a statutory requirement for responsiveness that looks more like response to legal demands in the physical world, this Committee would give law enforcement and industry a benchmark to ensure fairness across the industry, transparency for citizens, and adequate safeguards for public safety.

We have heard service providers cite the high volume of law enforcement requests as a reason for response times that stretch into months, threatening underlying investigations. We have heard they do not have the staff necessary to process the volume of requests quickly. While staffing levels are obviously the prerogative of the company, we understand the difficulty of assigning new resources to an activity that is not a profit center. But the consequences of these decisions in the world of criminal investigations is significant. Further, many of these providers are in the business of finding technological solutions to just this kinds of problem - automating processes to enhance efficiency and accountability and share information effectively. They are well acquainted with monitoring customer service centers and determining adequate staffing levels. The people on the other end of the line when we call providers are often very knowledgeable and helpful, and they can demonstrate significant interest and investment in our cases. I work with a lot of very helpful people in the compliance offices of many service providers who are doing the right thing. In most cases, I do not think the problem is a matter of their willingness, but rather the resource allocation decisions made above their pay grade.

Since providers have little economic incentive to innovate or increase staffing levels in their compliance shops, a reasonable legal requirement for responsiveness may be part of the solution to these problems. Such a solution need not be overly costly or burdensome. Congress can protect citizens' privacy and at the same time ensure that victims of crime see justice done thanks to the persistent work of investigators who have timely and reliable access to evidence. Any reform of ECPA should take this issue into consideration.

Notification provisions may put a significantly greater and more costly administrative burden on law enforcement. 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. 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. In addition, due to the nature of investigations today and the way people create accounts, there is no way to clearly understand - within the timeframes specified in pending ECPA reform legislation - who exactly is to be notified. How much time must investigators spend chasing down parties to notify, rather than working their investigations?

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 about 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 exists in the digital crime scene. Communications records have taken their place alongside physical evidence, biological evidence, testimonial evidence, and 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, and should further ensure that law enforcement does not face greater obstacles to gathering digital evidence that we encounter with other evidence types.

A casual review of transparency data supplied by major service providers will show that law enforcement legal demands affect only a tiny percentage of accounts and a very small number of cases relative to the overall criminal caseload in the United States. For example, the latest Google transparency report covering the last six months of 2014 shows that the company received just under 10,000 "user data requests" from U.S. law enforcement agencies. Facebook reports that it received just over 17,500 law enforcement requests from U.S. agencies during the first six months of 2015. Twitter reports that during the first half of 2015 it received just under 2,500 "account information requests" from U.S. law enforcement agencies. Those sound like big numbers until you consider there are nearly 18,000 law enforcement agencies in the United States, which means that on average, each law enforcement agency made less than one request to Google, around one request to Facebook, and far less than one request to Twitter for user information during the time periods covered by their transparency reports. Obviously some agencies are not making any requests at all, and many agencies with heavy caseloads are making frequent requests. 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 help us identify sexual predators, recover kidnapping victims, and successfully prosecute murderers. 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 who are the boots on the ground. This has led to situations where responses to legitimate law enforcement requests have been delayed, or where the service provider has refused to provide records without process, regardless of the circumstances.

Another Tennessee case comes to mind; once again, my unit was handling the communications component of an AMBER Alert investigation. One of the many leads that we received about someone who might have knowledge of the missing child's location appeared in a post on the site of a social media provider. When we contacted the provider, this was only one in a flood of leads, any one of which could be critical to rescuing the victim. We can't know which one is the key until we receive the evidence we need. That social media provider told us that while they agreed that the situation was an emergency, they were aware that the emergency provision in ECPA was permissive rather than mandatory, and it was their policy never to provide records on an exigent basis; they always wanted legal process (in this case, a search warrant) first. Could we have found the victim sooner, and spared them additional time in the hands of their abductor? We'll never know.

We would also 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.

Any effort to reform ECPA should address the creation and logging of certain types of records. Certain types of widely used electronic communications are not retained by some providers, and the deletion of data can hinder law enforcement investigations. In particular, law enforcement faces challenges with respect to "IP logs" which are records of which computer or other device is linked to a particular communication. Without a statutory requirement for logging and retention of those records, it is possible to make online threats or victimize children with impunity, secure in the knowledge that law enforcement cannot identify the point where the communications were made. I am well aware that retention means a cost for service providers; it is for precisely that reason that voluntary compliance is not likely to work, and a statutory requirement should be considered. I would urge Congress to find a balance that is not overly burdensome to service providers, but that ensures that law enforcement has access to critical evidence for at least some period of time.

Preservation provisions under current law should be revisited to ensure that law enforcement can prevent service providers from notifying customers of the existence of the request. One provision of the bill the committee is considering 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 orders under 2703(f) 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 threat to investigations is clear if these situations are not handled appropriately, and there should be no room for interpretation by service providers in this matter.

Conclusion

Any effort to modify the standard of proof for access to stored content and certain communications records that does not address the concerns outlined above will lengthen law enforcement's investigative timeline, and therefore reduce our effectiveness. 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 move in the digital world, and some of those details make their way into digital crime scenes. Just as there is no question that the people living those lives have an interest in preserving the privacy of that information, there can be no question that some of those devices hold the keys to finding an abducted child, identifying people who trade in images of children being victimized, apprehending a dangerous fugitive, or preventing a terrorist attack.

Our society benefits from an open exchange of ideas on topics critical to the public interest, and we believe that H.R. 699 reflects a largely one-sided debate where concerns of industry and privacy groups are addressed without reflecting the concerns of the law enforcement community. 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 committee to ensure that members of the state and local law enforcement community who are in the trenches doing this work every day - and whose jobs will be significantly impacted by any changes in the law - have their voices heard before finalizing the effort to reform the Electronic Communications Privacy Act.

We must be mindful that any restriction of law enforcement's lawful access to electronic evidence, whether by redefining legal barriers, heightening protections for evidence in the digital world compared to the physical world, 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. We must find a way to preserve ECPA's original intent, to enhance citizens' privacy and to ensure that criminal investigators get evidence they need quickly and reliably when the law says that they can.

Mr. GOODLATTE. Thank you.

Mr. Calabrese, I think maybe I have your pronunciation correct now. Is that right?

Mr. CALABRESE. You actual were right the first time. It's Calabrese, but I'll take it however you give it. Thank you.

Mr. GOODLATTE. Thank you. I'm on a losing streak here, but go ahead.

TESTIMONY OF CHRIS CALABRESE, VICE PRESIDENT, POLICY, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. CALABRESE. Well, thank you, Mr. Chairman, for having me testify. That's the thing we appreciate the most.

Ranking Member Conyers, Members of the Committee, thank you for the opportunity to testify on behalf of the Center for Democracy and Technology. CDT is a nonpartisan advocacy organization dedicated to protecting privacy, free speech, and innovation online. We applaud the Committee for holding a hearing on the Electronic Communications Privacy Act, ECPA, and urge the Committee to speedily approve H.R. 699, the "Email Privacy Act."

When ECPA was passed in 1986, it relied on balancing three policy pillars: Individual privacy, the legitimate needs of law enforcement, and support for innovation. Changes in technology have eroded this balance. The reliance on trusted third parties for long-term storage of our communications have left those communications with limited statutory protections. This void has created legal uncertainty for cloud computing, one of the major business innovations of the 21st Century and one at which U.S. companies excel.

At the same time, information accessible to the government has increased dramatically from emails and text messages to social networking posts and photos. Most if not all, of this information would not have been available in 1986. The technology has changed but the law has not, creating a major loophole for Americans' privacy protections.

In the face of this outdated statute, courts have acted, recognizing in cases like *U.S. v. Warshak* that people have a reasonable expectation of privacy in email and invalidating key parts of ECPA. But that patchwork is not enough on its own. It continues to lag behind technological change and harms smaller businesses that lack an army of lawyers. It also creates uncertainty around new technologies that rely on the use and storage of the contents of communications.

Reform efforts face a concerted assault from civil agencies that seek to gain new powers and blow a huge privacy loophole in the bill. Agencies have blocked reform in spite of the fact that the SEC has confessed to never subpoenaing an ISP post-*Warshak*. No less than FBI Director Comey told this Committee that in regard to ECPA, a change wouldn't have any effect on our practices.

In fact, new civil agency powers would harm the privacy of ordinary citizens. Imagine if the IRS had had these powers back from 2010 to 2012 when they were improperly investigating the tax status of Tea Party organizations. During that investigation, the IRS sent lengthy time-consuming questionnaires seeking information on what members were reading, their Facebook posts, donor lists, and copies of the materials they were disseminating. While the IRS'

targeting of conservative groups was limited to these lengthy questionnaires, their subpoena authority is extremely broad and likely could have been used here.

If the IRS had had the power that the SEC proposal recommends be granted to all Federal agencies, they would have been able to go beyond gathering information directly from the target of the investigation. The IRS would have been able to go to court and enforce an order allowing them to go directly to the ISP and seek the subject's email. While under the SEC proposal, the subject in the investigation would have been able to contest that order in court, civil standards are very low, and it's clear that the IRS had a very expansive idea of the information they could seek. This type of agency overreach is exactly why we can't grant agencies unjustified new authorities.

Support for privacy reform is deep and abiding. More than 100 tech companies, trade associations, and public interest groups have signed onto ECPA reform principles. Signatories include nearly the entire tech industry, span the political spectrum, and represent privacy rights, consumer interests, and free market values.

The Email Privacy Act has more than 300 cosponsors, including a majority of Republicans and Democrats. Post-*Warshak*, a warrant for content has become the status quo. Nonetheless, it is critical for the Committee to approve H.R. 699 in order to cure a constitutional defect in ECPA, protect individual privacy, and assure that new technologies continue to enjoy robust constitutional protections. Thank you.

[The prepared statement of Mr. Calabrese follows:]

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org

Statement of Chris Calabrese
Vice President, Policy
Center for Democracy & Technology

Hearing before the U.S. House Judiciary Committee on H.R. 699, the "Email Privacy Act."

December 1, 2015

Chairman Goodlatte, Ranking Member Conyers, and members of the Committee

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information. We applaud the Committee for holding a hearing on the Electronic Communications Privacy Act (ECPA) and urge the committee to speedily pass H.R.699, the Email Privacy Act.

Every day, whistleblowers reach out to journalists (and members of this Committee), advocates plan protests against government injustice and ordinary citizens complain about their government. All of these activities are crucial to our democracy. They also all rely on our long-held constitutional guarantee of private communications, secure from arbitrary access by the government. This is true whether the communication happens in the form of a letter, a phone call or, increasingly, an email, text message or over a social network. But as our technology has changed, the legal underpinnings that protect our privacy have not always kept up.

The foundational value that ECPA reform seeks to uphold, as embodied by H.R.699, is the right to privacy for the content of our communications, even as technology evolves. In the face of an outdated statute, the courts have stepped in, creating key legal precedents and strong limits on access. But that patchwork is not enough on its own. It continues to lag behind technological change and harms smaller businesses that lack an army of lawyers. Reform efforts also face a concerted assault from civil agencies that seek to use statutory changes as a tool to gain new powers. A recent scandal involving improper investigations by the IRS into the tax exempt status of conservative organizations highlights the danger those new powers could create for Americans' privacy.

The House has consistently sought to solve these problems through strong reform measures and more than 300 members have cosponsored the Email

Privacy Act. CDT continues to believe that a legislative solution – passage of H.R.699 – is the best way to advance a modest but critical privacy protection.

Support for privacy reform is deep and abiding. A majority of Republicans and Democrats in the House support it. More than one hundred technology companies, trade associations, and public interest groups have signed onto ECPA reform principles.[1] Signatories include nearly the entire tech industry, span the political spectrum and represent privacy rights, consumer interests, and free market values. Finally, the public is firmly behind reform. A recent poll shows 86 percent of voters support an update to ECPA.

The Need for Reform

In 1986, when ECPA was written, few Americans owned computers and even fewer used email. Hard drives were small. Service providers offered little storage capacity and the storage they did sell was expensive. The World Wide Web didn't exist. Neither did cloud computing or broadband or social media or smartphones. The little data that was stored was kept on local computers.

Obviously that is not the world we live in today. Decades after the beginning of the Internet Age, we store a vast array of sensitive communications with third parties — emails, text messages, work documents, pictures of our children, and love letters. Under ECPA, they receive widely varying degrees of protection – most of which are inadequate and out of touch with consumer expectations.

These changes in technology – the rise of remote storage and cloud computing, and the digitization of almost all communications – have two main implications for ECPA. First, they create serious inconsistencies in how similar communications are treated and the reasonable expectation of privacy they deserve. Second, they have disrupted the fundamental balance created in ECPA between privacy rights, law enforcement interests and the needs of innovators.

An Inconsistent Law

When trying to understand the conflicting standards and illogical distinctions that plague the current statute, it can be helpful to consider the technological reality at the time of the passage of ECPA.

---

[1] *About the Issue: ECPA Reform*, DIGITAL DUE PROCESS, http://www.digitalDueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

In 1986, Congress created two categories of providers and accorded users of those services different levels of protection. Legislators defined an electronic communications service (ECS) as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[2] It was aimed at protecting the nascent use of email. Today, ECSs typically include any service that allows users to communicate with each other–whether by email, text message, social network or other means. Under ECPA, those communications are protected by a warrant only for the first 180 days after they are sent and are thereafter accessible with a subpoena. That 180-day rule is an outdated reflection of the fact that in 1986 hard drive capacity was incredibly expensive and no one contemplated long-term storage. The assumption was that if a user left an email on a server that long, it was abandoned and merited a lower privacy protection.

The second category of service under ECPA 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."[3] Today, this would likely cover a cloud-based service accessed solely by an individual user, such as a Dropbox account. Under ECPA, RCSs receive only the protection of a subpoena. In 1986, RCSs tended to be major companies handling data for other major companies. As such, records in RCS storage appeared more like business records, and hence lawmakers granted them subpoena protections.

These distinctions make little sense today. Emails and other content are stored indefinitely and data held by RCSs are clearly as private as those by ECSs. It is often hard to glean in which category a particular service belongs. If a user stores a document remotely so she can later edit the document, does it move from RCS to ECS storage when she permits others to edit it as well? It also leads to wildly uneven results. The same communication could be protected by a warrant if stored on a home computer, a subpoena when stored as a draft in an inbox, a Title III super warrant when in transit, a warrant for the first 180 days in an inbox and then a subpoena after that.[4]

Further, this one distinction only scratches the surface of the confusion over ECPA. Even basic questions over what type of stored records ECPA applies to can be confusing, given the limited definition of electronic storage. Nor does the statute contain basic protections like a suppression remedy for illegally obtained

[2] 18 U.S.C. § 2510(15) (2012).
[3] *Id*, at § 2711(2).
[4] 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 (2004).

information or reporting requirements for how often communications are shared with the government.

These problems have not gone unnoticed. Starting in 2007, CDT began working through its Digital Privacy and Security Working Group ("DPSWG") to find common ground on a solution to some of ECPA's problems. In 2010, we announced the formation of the Digital Due Process (DDP) coalition, consisting of nine companies and twelve trade associations, think tanks and advocacy groups. DDP supported four key principles for reforming ECPA – one of which was the "warrant for content" fix at the heart of H.R.699. DDP has blossomed today into a broad coalition of more than a hundred groups and companies, including major technology companies, advocacy organizations from the right and the left and grassroots organizations representing millions of members.[5]

Congress has recognized the need for reform, as well. The Senate Judiciary Committee voted out of committee legislation either identical or similar to H.R.699 in both 2012 and 2013. H.R. 699 is the most cosponsored bill in the House with more than 300 cosponsors including a majority of both the Republican and Democratic caucus.

The federal courts and the tech industry have also attempted to fill the void left by the lack of reform. In 2003, in *Theofel v. Farey-Jones*, the Ninth Circuit clarified confusion in the statute regarding when an email was in electronic storage and rejected the Justice Department's distinction between opened and unopened e-mail.[6] Most significantly, in 2010, in *U.S. v. Warshak*, the Sixth Circuit ruled that people have a reasonable expectation of privacy in email content and that it should only be accessed with a search warrant.[7]

The *Warshak* decision was a watershed. While it technically only applied in the Sixth Circuit, the difficulty in determining where a particular user was located and the persuasiveness of the court's reasoning led most, if not all, major technology companies to adopt a warrant standard for all stored content. Even more significantly, it cast into question the constitutionality of a significant portion of the statute and made the need for reform even more urgent.

---

[5] For a full list, see *Who We Are*, DIGITAL DUE PROCESS, http://digitalddueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163.

[6] Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003).

[7] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

The Balance in ECPA

At the time of its passage, the goal of ECPA was to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement,"[8] and to support the development and use of new types of technologies and services.[9] Congress wanted to encourage the innovation represented by these new technologies and realized that would not be possible if the privacy of users was not protected.[10]

ECPA accomplished that goal by creating a familiar framework – a high level of protection for the content of communication and a lower protection for business records or abandoned communications. Notably, this framework was prescient in recognizing that 3rd parties could and would hold sensitive information that merited warrant protection.

Since this initial balance was struck, we have seen a technological revolution and the result has been a statute that is now much less protective of privacy and hinders innovation.

A short (and probably incomplete) list of the communications content that I store with third parties today includes:

- Work and personal email,
- Text messages,
- More than a decade of photographs,
- Music,
- My passwords to all my online accounts,
- Social networking posts – many of which are shared with very few people,
- Notes – both personal and work,
- Personal contacts,
- My calendar,
- Hundreds of books, and
- Home videos and movies.

The striking thing about this list is how pedestrian it is. Most Americans could create a similar list; some would likely be able to add many more categories. Yet all of this is protected under a legal framework that is dramatically out of date.

---

[8] H.R. REP. No. 99-647, at 19 (1986).
[9] S. REP. No. 99-541, at 5 (1986) (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems").
[10] *Id.*; H.R. REP. No. 99-647, at 19.

Protections are largely reliant on a handful of court decisions and technology companies with strong government access policies.

The need for reform of ECPA to support innovation is equally striking. This Committee is familiar with the importance of cloud computing. Businesses all over the world are looking to cloud-based services for their information management needs in order to save money on equipment and to achieve better computing reliability and data security. Cloud-based services allow companies to expand their computing capacity quickly, which is particularly valuable for start-up businesses and entrepreneurs. Such services give employees the flexibility to share information and collaborate. The global Software-as-a-Service (SaaS) market is expected to reach $106 billion by next year.[11] American companies have been the global leaders in this area, and it has been an engine for U.S.-based innovation, economic growth and job creation.

Currently, ECPA does not provide a solid legal foundation to continue this growth. When businesses contract out to cloud providers, there is a strong argument under ECPA that those cloud providers are offering the services of an RCS and hence the information they store is only protected by a subpoena. Contrast that with the full protection of a warrant offered when someone saves information on her own personal computer. As Fred Humphries, Vice President of U.S. Government Affairs at Microsoft said, "Our goal is simple: the law should treat data stored in the cloud as closely as possible to data that we previously stored in our homes or in our offices."[12]

At the same time, law enforcement's ability to collect information has grown astronomically. It's not just access to the content of communication. Everything we do online – and increasingly offline through our mobile devices – also produces metadata. Our location, with whom we are communicating, our friends and social networks – all of it is accessible to law enforcement under a variety of legal standards, most of which are lower than a warrant backed by probable cause. While increased protections for metadata are not part of H.R.699, it is important to keep this cornucopia of new information in mind when considering any reform effort. The reality is that we currently live in a golden age of surveillance where the government has access to copious amounts of

---

[11] Louis Columbus, *Roundup of Cloud Computing Forecasts and Market Estimates, 2015*, FORBES (Jan. 24, 2015), http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/.

[12] Microsoft Corporate Blogs, *A day of action to demand ECPA reform*, MICROSOFT (Dec. 5, 2013), http://blogs.microsoft.com/on-the-issues/2013/12/05/a-day-of-action-to-demand-ecpa-reform/.

information about all of us. H.R.699 is just a level set in one area, returning privacy protections to the content of communications while we continue to see erosions in many others.[13]

Law enforcement has not denied the need for reform in this area. At a hearing last year, FBI Director James Comey said about ECPA, "There is an outdated distinction. For email, over 180 days, I think, under the 1980s statute is treated as something that you could in theory obtain without a search warrant. We don't treat it that way. We go get a search warrant from a Federal judge no matter how old it is. So a change wouldn't have any effect on our practice."[14] Similarly, in a past hearing on reforming the ECPA, the Department of Justice agreed "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."[15] Given this acknowledgement that a problem exists – and the reality that there is a constitutional infirmity in the statute protecting all stored communications – it is frustrating that some in law enforcement continue to resist commonsense reform.

The Legislation

The Email Privacy Act (H.R.699) does not fix all the problems described above, but it does remedy the constitutional infirmity identified by *Warshak* and provides a strong, consistent and easily administered legal protection for the content of communications.

The key to the protections in H.R.699 can be found in Section 3. It amends ECPA so that the disclosure of the content of email and other electronic communications by an ECS or RCS is subject to one clear legal standard – a search warrant issued based on a showing of probable cause. The provision eliminates the confusing and outdated "180-day" rule. Section 3 also requires

---

[13] For more on the golden age of surveillance, see Peter Swire, *Going Dark or a Golden Age for Surveillance?*, CDT.ORG (Nov. 28, 2011), https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/.

[14] *Oversight of the Federal Bureau of Investigation: Hearing before the H. Comm. on the Judiciary*, 113th Cong. 69 (2014) (statement of the Hon. James B. Comey, Dir., Fed. Bureau of Investigation).

[15] *ECPA Part 1: Lawful Access to Stored Content: Hearing before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 4 (2013) (statement of Elana Tyrangiel, Acting Assistant of Attorney General, Dep't of Justice Office of Legal Policy).

that the government notify the individual within either 3 or 10 days if their information was disclosed.

Section 3 also reaffirms current law to clarify that the government may use an administrative or grand jury subpoena in order to obtain certain kinds of electronic communication records from a service provider, including a customer's name, address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information.

Lastly, the section contains a rule of construction regarding government access to internal corporate email. It states that nothing in the bill precludes the government from using a subpoena to obtain email and other electronic communications directly from a company when the communications are to or from an officer, agent or employee of a company.

Section 4 permits delayed notice under the same standard as current law. A court may extend the delay periods for a period of up to an additional 180 or 90 days at a time (depending on whether an investigation is criminal or civil). Law enforcement may also obtain an order barring providers from disclosing the existence of a warrant.

H.R.699 also grants new authority to assist the government in their investigations. In cases where there has been a delay, Section 4 requires that service providers notify the government in advance when that time period expires and they intend to notify a customer about the warrant. Current law requires no such advance notice. The purpose of this provision is to ensure that the government has an opportunity to protect the integrity of its investigation and, if warranted, to ask a court to delay the notification, before such notice is given. It also doubles the period for which notice to a user of law enforcement access to communications content can be delayed. Finally, it adds civil discovery subpoenas to the list of subpoenas that can be used to compel disclosure of subscriber identifying information, placing all subpoenas on the same footing.

H.R.699 is also noteworthy for what it does not do. It does not impact national security powers under the Foreign Intelligence Surveillance Act – a rule of construction in Section 6 makes this clear. It does not affect the traditional exceptions that allow law enforcement to access communications without a warrant – exigency, consent and the other exceptions found in 18 U.S.C. § 2702. Nor does it interfere with the existing process that allows providers to work with the National Center for Missing and Exploited Children to identify and help prosecute child pornography under 18 U.S.C. § 2258A.

This simple change to the law – treating searches of an individual's inbox the same way we treat searches of her home – is profoundly important to personal privacy and American business while not unduly interfering with law enforcement's ability to protect public safety.

Issues of Special Note

Opponents of H.R.699 have identified three areas of concern – access by civil agencies, the handling of emergencies and notice to subjects of an investigation. I will address each in turn.

Civil Investigation Carve Out

In a letter to the Senate Judiciary Committee in April 2013, the Chair of the Securities and Exchange Commission (SEC) stated that a warrant requirement would block the SEC from obtaining digital content from service providers.[16] The SEC reiterated this desire for new authority to access the content of individuals' emails at a September 2015 hearing before the Senate Judiciary Committee.[17] The SEC is a civil agency and lacks authority to issue warrants, relying instead on subpoenas for investigations. The SEC argued that ECPA reform should allow civil agencies to obtain digital content from service providers without a warrant. However, the SEC's request for new authority is unnecessary and troubling.

The scope of this request is very broad. While the SEC has only requested that all federal civil law enforcement agencies be granted the power to compel emails and other content from service providers,[18] ECPA's provisions have always applied to all government – including state and local agencies. But even if this authority was somehow limited to federal agencies, it would mean that the Internal Revenue Service (IRS), Environmental Protection Agency (EPA), Consumer Financial Protection Bureau (CFPB), and potentially many more agencies would have a new authority to demand a target's emails from service providers without going directly to the target of an investigation.

---

[16] *See* Letter from the Hon. Mary Jo White, Chair, Securities and Exchange Comm'n, to Sen. Patrick Leahy, Chair, Sen. Judiciary Comm. (Apr. 24, 2013), *available at* https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf.

[17] *See Reforming the Electronic Communications Privacy Act: Hearing Before the S. Comm. On the Judiciary*, 114th Cong. (2015) (statement of Andrew Ceresney, Dir., Div. of Enforcement, U.S. Sec. Exch. Comm'n), *available at* http://www.judiciary.senate.gov/imo/media/doc/09-16-15%20Ceresney%20Testimony.pdf.

[18] Letter from the Hon. Mary Jo White, *supra* n. 16, at 3.

An effective and time-honored method to access these types of communications in civil investigations already exists. Civil agencies can already obtain digital content with a subpoena issued directly to the target of the investigation – such as a user who sent or received emails. Civil agencies can enforce these subpoenas on individuals in court, and courts can order the user to disclose the data sought under the subpoena.[19] In addition, ECPA already allows civil agencies to issue preservation orders – without court approval – that direct service providers to prevent deletion of information from a user's account, thereby preventing destruction or alteration of evidence, while a motion to compel is being pursued.[20] ECPA reform would not change any of these existing powers for civil agencies. In reality, what the SEC is seeking is a new authority. Andrew Ceresney, Director of the SEC Division of Enforcement, stated unequivocally at the September Senate hearing that the SEC has never sought content from service providers since *U.S. v. Warshak* was decided in 2010.[21]

Ceresney has also stated incorrectly that the new power the agency seeks will provide a greater level of protection than under a warrant.[22] A warrant is the "gold standard" for privacy protection in the U.S., which is why it is embedded in the Fourth Amendment of our Constitution. The most invasive kind of searches, such as a search of your home or your personal belongings (including your letters), must generally be conducted with a warrant. The warrant itself is very narrow in scope: the government must prove to a judge or magistrate that there is probable cause to believe that specific evidence related to a crime is currently in the specified place to be searched. Other places and items, unless in plain view during the search, cannot be touched.

One of the most troubling parts of the SEC proposal is that it does not specify the standard that must be met before conducting a search, but suggests the subpoena standard is the standard the SEC would want to use if its proposal were implemented.[23] Under this standard, the government would only need to prove that the customer records sought are relevant to an investigation. Because it requires such a low standard of review, the subpoena is by far the easiest

---

[19] *See, e.g.*, FTC v. Sterling Precious Metals, LLC, 2013 U.S. Dist. LEXIS 50976 (S.D. Fla. Apr. 9, 2013).

[20] 18 U.S.C. § 2703(f). Evidence preservation orders can be issued at early stages of an agency's inquiry, even before launching a formal investigation.

[21] *Reforming the Electronic Communications Privacy Act: Hearing Before the S. Comm. On the Judiciary*, 114th Cong. (2015).

[22] *See* Statement of Andrew Ceresney, *supra* n. 17, at 5.

[23] *See id.* Ceresney's testimony proposed a system in which the subscriber or customer would have "the opportunity to challenge" the request for data at a judicial proceeding, where they could raise concerns such as "privilege" or "relevancy."

instrument for the government to use. It is also the broadest in scope, because a large number of communications can be considered "relevant" to an investigation.

This problem is compounded by the fact that the predicate to begin a civil investigation is much broader than a criminal investigation. Simply put, many more actions are violations of civil law versus criminal law. For example, under the SEC's proposal, the government could obtain personal electronic communications relevant to misfiling tax returns or violating the health code. In addition to this problem, subpoenas can also be directed not only at people subject to the investigation, but also to any witnesses with relevant information. Finally, information gathered as part of a civil process could be shared for use in a parallel criminal investigation – creating a major backdoor to the protections in the bill.[24]

The recent scandal involving the IRS's inappropriate investigation of Tea Party organizations provides a vivid example of the dangers of agency overreach. Between 2010 and 2012, the IRS began to specifically target applications for tax-exempt status that came from organizations with names that included words such as "Tea Party," "Patriots," or "9/12".[25] In response to these applications, the IRS sent lengthy, time-consuming questionnaires, requesting that the applicants answer questions such as, "Please provide copies of all your current web pages, including your blog posts. Please provide copies of all your newsletters, bulletins, flyers, newsletters or any other media or literature you have disseminated to your members or others. Please provide copies of stories and articles that have been

---

[24] For example, Form 1662 of the Securities and Exchange Commission, which is designed to be used with all SEC civil subpoenas, expressly states:

> The Commission often makes its files available to other governmental agencies, particularly United States Attorneys and state prosecutors. There is a likelihood that information supplied by you will be made available to such agencies where appropriate. Whether or not the Commission makes its files available to other governmental agencies is, in general, a confidential matter between the Commission and such other governmental agencies.

SECURITIES AND EXCHANGE COMMISSION, SEC 1662 (09-14), http://www.sec.gov/about/forms/sec1662.pdf.

[25] Treasury Inspector General for Tax Administration, "Inappropriate Criteria Were Used to Identify Tax-Exempt Applications for Review," 6 (May 14, 2014), *available at*: https://www.washingtonpost.com/blogs/wonkblog/files/2013/05/201310053fr-revised-redacted-1.pdf.

published about you."[26] Other questionnaires asked that the organizations provide a resume for each of their past and present directors, officers, and key employees.[27] as well as a list of what books their members were reading and printouts of their Facebook posts.[28] Failure to answer these questions resulted in the rejection of the organization's application for tax-exempt status.

Although it appears that the IRS's targeting of conservative groups was limited to these lengthy questionnaires,[29] the IRS probably could have used its administrative subpoena authority, as well, because that authority is extremely broad. I.R.C. § 7602 authorizes the IRS to issue a summons for the purpose of "determining the liability of any person for any internal revenue tax."[30] Such summonses may be issued to an organization for the purpose of determining exempt status or tax liability, upon authorization by the EP/EO key district director.[31] The summons may request any information that "may be relevant" to an investigation.[32] In addition, the IRS may issue such summonses to a wide variety of people (not just the subjects of an investigation) including any other person the examiner "may deem proper."[33]

If the IRS had the power that the SEC proposal recommends be granted to all federal agencies, they would have been able to go beyond gathering information directly from the target of their investigation. The IRS would have been able to go

---

[26] Chris Good, *Weirdest IRS Questions for the Tea Party: Views, Donors, and Etymology*, ABC NEWS (May 14, 2013), http://abcnews.go.com/blogs/politics/2013/05/weirdest-irs-questions-for-the-tea-party-views-donors-and-etymology/.

[27] *Id.*

[28] David Nather, Tarini Parti and Byron Tau, *IRS wants you to share everything*, POLITICO (May 14, 2013), http://www.politico.com/story/2013/05/the-irs-wants-you-to-share-everything-091378.

[29] The IRS investigations may have been limited to questionnaires because a 1993 guidance document found on their website advises that summons authority should only be used when "1) information is vital to the investigation; 2) the taxpayer or third-party summonee is unreasonably refusing to cooperate; and 3) the information cannot be easily obtained from other sources." George Johnson and Marvin Friedlander, "Summons and Enforcement," 1993 EO CPE Text, https://www.irs.gov/pub/irs-tege/eotopicg93.pdf.

[30] 26 U.S.C. § 7602(a).

[31] Johnson and Friedlander, *supra* n. 29, at 3; *see also Church of Spiritual Tech. v. U.S.*, No. 581-88T, slip op. at 21 n.34 (Cl. Ct., reissued June 29, 1992) (finding that the IRS was permitted to summon a former officer of the Church while considering the Church's exemption application).

[32] 26 U.S.C. § 7602(a)(1).

[33] *Id.* at § 7602(a)(2).

to court and enforce an order allowing them to go directly to the Internet Service Provider in order to access relevant email and other information stored in the cloud. While under the proposal the subject of the investigation would have been able to contest that order in court, the reality is that relevance is a very broad standard that is extremely difficult to challenge. In addition, it's clear from the questions they asked conservative groups that the IRS has a very expansive idea of what was proper for them to investigate.

Given the *Warshak* decision, CDT believes the SEC proposal amounts to an unconstitutional solution to a nonexistent problem – one aimed at getting an unprecedented level of access to Americans' email inboxes.

Changing Rules for Emergency Exceptions

Under ECPA, electronic communications providers cannot give content and sensitive user information to the government absent a court order, subpoena or warrant. However, the law does contain an exception so that in an emergency situation involving danger of death or serious bodily harm, the provider may disclose content and user records to law enforcement absent the legal process that would otherwise be required.[34] Because these requests receive no independent judicial oversight, providers have discretion to assess whether the request is proper and should be fulfilled absent the required legal process. As ECPA reform legislation continues to gather strong support, some have called for a new provision that would change this rule to mandate compliance with any emergency request for user data or content. Such a change is unnecessary, and would raise significant privacy and security problems.

Although most emergency requests are appropriate and receive speedy compliance, there are enough instances where requests are deemed improper that misuse of the emergency authority should not be ignored. Providers' authority to evaluate the legitimacy of these requests is a crucial check against this type of abuse. For example, in 2014, Google rejected 94 out of 342 requests.

The government has previously abused its ability to engage in emergency requests. A 2010 Department of Justice Inspector General report stated that the Inspector General "found repeated misuses of [the FBI's] statutory authority to obtain telephone records through NSLs or the ECPA's emergency voluntary

[34] *See* 18 U.S.C. §§ 2702(b)(8), (c)(4).

disclosure provisions."[35] Based on this, the Inspector General report recommended Congress consider "appropriate controls" on the FBI's ability to obtain records in emergency situations. With mandatory compliance and no judicial oversight, such abuses could become more frequent.

Right now, emergency requests are very rare. America's largest Internet and electronic communications companies only receive a small number of requests. For example, Google only received 342 emergency requests[36] and Microsoft only received 475 requests[37] throughout all of 2014. In comparison, Google received 20,280 subpoenas and search warrants and Microsoft received 12,364 similar requests during that same year.

In the event that a provider denies a request for an emergency disclosure without legal process, the government still has options available. Law enforcement can revise its request to obtain content or data if appropriate justification has not been provided. Additionally, government entities may also seek information through ECPA's mandatory disclosure provisions without delay. In all judicial districts, a magistrate is available for after-hours requests that require immediate action, and Rule 41 of the Federal Rules of Criminal Procedure stipulates for telephonic search warrants to be obtained at all hours.

Requiring providers to comply with any emergency request would also endanger data security by interfering with providers' ability to assess the validity of requests. Data thieves regularly attempt to take customer information by posing as law enforcement and demanding that data be provided pursuant to an emergency. Congress criminalized this activity because of the serious threat it poses.[38] Providers must have the capability to ensure that requests are not fraudulent and prevent disclosure of user data to unauthorized third parties. Mandating disclosure in response to all emergency requests and removing discretion to appeal for clarification, additional information, or a more secure method of disclosure would undercut providers' ability to protect users' sensitive information.

---

[35] *See* OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 268 (Jan. 2010), *available at* https://oig.justice.gov/special/s1001r.pdf.
[36] *See Google Transparency Report: Security and Privacy*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US/.
[37] *See Microsoft Law Enforcement Requests Report*, MICROSOFT, https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.
[38] *See* 18 U.S.C. § 1039 (2012).

The current system for disclosure of user information and content pursuant to emergency requests absent a court order works effectively. It protects both public safety and user privacy and security, and should not be changed.

Notice

Americans' email accounts often contain the most sensitive, private aspects of their lives – from purchase orders and health information to love letters and political or religious communications – and often date back years. For today's digital natives, it may end up as a permanent record of their entire lives. A covert search of a citizen's inbox by the government – even when pursuant to a warrant – is one of the most invasive possible. Like a covert search of a person's home, it directly contradicts the values at the heart of the Fourth Amendment, and must only be done out of absolute necessity. That is why notice of an investigation is so crucial.

Without notice, users subject to a search are unable to protect their constitutional rights including the ability to challenge the validity of a warrant. They cannot protect the rights associated with their email such as attorney client privilege. Nor can they assert the other rights allowed to a defendant under the Federal Rules of Criminal Procedure.[39] In addition, notice enables users to correct cases of mistaken identity that may otherwise subject them to a wrongful search.

At the same time, the Email Privacy Act preserves existing exceptions to the notice requirement. Mirroring current law, in H.R.699 a court may grant a request for delayed notification upon finding that notification of the existence of a search could result in a threat to the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing an investigation or unduly delaying a trial. Although these exceptions are important to protect investigations in extraordinary circumstance, notice must be the norm in law enforcement investigations. Without knowledge of an investigation, a defendant is hamstrung in asserting their constitutional rights and accountability is greatly reduced.

Conclusion

We thank the Committee for holding a hearing on this important issue and urge you to act swiftly to mark-up H.R.699, the Email Privacy Act.

[39] FED. R. CRIM. P. 41.

Mr. GOODLATTE. Thank you, Mr. Calabrese.
And Mr. Salgado, welcome.

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

Mr. SALGADO. Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for the opportunity to appear before you today. My name is Richard Salgado. As director——

Mr. GOODLATTE. Mr. Salgado, would you pull your microphone a little closer to you.

Mr. SALGADO. Sure. Thank you. My name is Richard Salgado. I'm director for law enforcement and information security for Google. I oversee the company's compliance with government requests for users' data, including requests made under the Electronic Communications Privacy Act of 1986, otherwise known as ECPA.

In the past, I have worked on ECPA issues as a senior counsel in the computer crime and intellectual property section in the U.S. Department of Justice. Google strongly supports H.R. 699, the "Email Privacy Act," which currently has 304 cosponsors, more than any other bill currently pending in Congress. It's undeniable and it's unsurprising that there is strong interest in aligning ECPA with the Fourth Amendment and users' reasonable expectation of privacy.

The original disclosure rules set out in ECPA back in 1986 were foresighted given the state of technology back then. In 2015, however, those rules no longer make sense. 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 the documents stored in a desk drawer. There is no compelling policy or legal rationale for there to be different rules.

In 2010, the Sixth Circuit opined in *United States v. Warshak* that EPCA violates the Fourth Amendment to the extent it does not require law enforcement to obtain a warrant for email content. In doing so, the Sixth Circuit effectively struck down ECPA's 180-day rule and the distinction between opened and unopened emails as irreconcilable with the protections afforded by the Fourth Amendment.

Warshak is effectively the law of the land today. It's observed by governmental entities and companies like Google and others. In many ways, H.R. 699 is a modest codification of the status quo and implementation of the Sixth Circuit's conclusions in *Warshak*.

Two important developments have occurred since I last testified before the House Judiciary Committee in support of updating ECPA back in March of 2013, both of which have a significant bearing on efforts to update the statute.

First, the Supreme Court issued a landmark decision in Riley versus California where it unanimously held that, generally, officers must obtain a warrant before searching the contents of a cell phone seized incident to arrest.

Chief Justice Roberts noted that a regime with various exceptions and carve outs would "contravene our general preference to provide clear guidance to law enforcement through categorical

rules." To reinforce the constitutional imperative for clear rules in this area, Chief Justice Roberts concluded his opinion with unambiguous direction to law enforcement. He wrote, "The fact that technology allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple, get a warrant."

Notably, this Committee is being asked by some today to jettison precisely the type of categorical rules that the Supreme Court held were imperative in Riley. Doing so would undermine the user's reasonable expectations of privacy and encroach on core privacy protections afforded by the Fourth Amendment. We urge the Committee to reject such pleas.

Second, many States have enacted bright-line rules to bring their State versions of ECPA in line with the Fourth Amendment. Hawaii, Texas, and Maine have all done this. In addition, earlier this year, the California legislature overwhelmingly approved landmark legislation to update California's version of ECPA, referred to as Cal-EPCA. Not only does Cal-EPCA require the government to obtain a warrant before it can compel third-party service providers to disclose content, but it also extends the warrant requirement to communications metadata and data seized that's stored on electronic devices.

States are appropriately recognizing that the Fourth Amendment protections ought to extend to the sensitive data that's stored in the cloud. H.R. 699 represents an overdue update to ECPA that would ensure electronic communications content is treated in a manner commensurate with other papers and effects that are protected by the Fourth Amendment. It's long past time for Congress to pass a clean version of H.R. 699.

Thank you for your time and consideration, and I'd be happy to answer any questions you may have.

[The prepared statement of Mr. Salgado follows:]

Google

Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google Inc.
House Committee on the Judiciary
Hearing on "H.R. 699, the 'Email Privacy Act'"
December 1, 2015

Chairman Goodlatte, Ranking Member Conyers, and members of the Committee, thank you for the opportunity to appear before you this morning to discuss H.R. 699, the Email Privacy Act.

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 (DDP) Coalition, which supports updating ECPA. More than 100 organizations, trade associations, and corporations are DDP members. DDP members span the ideological spectrum, ranging from the American Civil Liberties Union (ACLU) and the the Center for Democracy & Technology (CDT) to Americans for Tax Reform (ATR) and FreedomWorks. The diverse array of organizations, trade associations, and corporations that comprise the Digital Due Process Coalition is a testament to the breadth of support for updating ECPA in the Internet era.

Google strongly supports H.R. 699, the Email Privacy Act, which is sponsored by Representatives Yoder (R-KS) and Polis (D-CO). H.R. 699 currently has 304 cosponsors, more than any other bill that is pending in Congress. It is undeniable that there is strong interest in aligning ECPA with the Fourth Amendment and users' reasonable expectations of privacy.

ECPA Reflects the Pre-Cloud 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 2015 are dramatically different than in 1986.

- 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 2015, 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. As a result of these technological advances, Americans are increasingly relying on third party service providers to store their online content, including videos, family photos, and confidential communications. The expectation is that such service providers can and will provide infinite storage indefinitely.

The distinctions that ECPA made in 1986 were foresighted in light of technology at the time. But in 2015, 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, but it is one that ECPA continues to make, despite widespread agreement that the statute should be updated.

ECPA Must Be Updated

Although the benefits of cloud computing have become more obvious and widespread, the outdated technology assumptions baked into parts of ECPA do not reflect the reasonable expectations of privacy of users. This is an unfortunate and unintended consequence of technological advancement, as Congress passed ECPA in 1986 in order to protect the privacy of users of electronic services in light of innovation. 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.

One of the most complex and baffling set of rules is around compelled disclosure of communications content. 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 most cases). If the email is 180 days old or newer

and unopened, the government will need a search warrant. In its testimony before the House Judiciary Committee in 2013, and again before the Senate Judiciary Committee in September, the Department of Justice (DOJ) acknowledged that there is "no principled basis to treat email less than 180 days old differently than email more than 180 days old." DOJ also recognized in its testimony that the statute should "not accord lesser protection to opened emails than it gives to emails that are unopened."

In 2010, the Sixth Circuit opined in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), that ECPA violates the Fourth Amendment to the extent that it does not require law enforcement to obtain a warrant for email content. In so doing, the Sixth Circuit effectively dispensed with ECPA's 180 day rule and the distinction between opened and unopened emails as irreconcilable with the protections afforded under the Fourth Amendment. Google believes the Sixth Circuit's interpretation in *Warshak* is correct, and we require a search warrant in all instances when law enforcement seeks to compel us to disclose the contents of Gmail accounts and other Google 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 governmental entities seek to compel third party service providers to produce the content of electronic communications.

Warshak is effectively the law of the land today. It is embraced by companies and observed by governmental entities. In many ways, then, H.R. 699 is a modest effort to codify the status quo and implement the Sixth Circuit's conclusion that the Fourth Amendment requires a warrant in all cases where the government seeks to compel a provider to disclose communications content from a company covered under ECPA. Notably, the bill explicitly carves out the acquisition of communications content pursuant to statutes such as the Wiretap Act and the Foreign Intelligence Surveillance Act. H.R. 699 will have no impact, therefore, on the government's efforts to combat terrorism under those authorities. Similarly, because *Warshak* is effectively the law of the land today, codifying a bright-line, warrant-for-content rule will not result in any substantive changes in how terrorism is investigated using ECPA authorities.

The inconsistent, confusing, and uncertain standards that currently exist under ECPA fail to preserve the reasonable privacy expectations of Americans today. Moreover, providers, judges, and law enforcement agencies 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 and confusing compliance hurdles for service providers, ECPA has created an unnecessary disincentive to move to a more efficient, more productive method of computing.

The Supreme Court and Many State Legislatures Recognize the Importance of Affording the Highest Privacy Protections to Electronic Communications

Two important developments have occurred since I last testified before the House Judiciary Committee in support of updating ECPA in March 2013, both of which have a significant bearing on efforts to update ECPA.

First, the Supreme Court issued a landmark decision in *Riley v. California*, 134 S.Ct. 2473 (2014), where it unanimously held that officers must generally obtain a warrant before searching the contents of a cell phone incident to an arrest. Writing for the Court, Chief Justice Roberts rejected the government's invitation to create "various fallback options for permitting warrantless cell phone searches under certain circumstances," noting that a regime with various exceptions and carve-outs "contravenes our general preference to provide clear guidance to law enforcement through categorical rules." To reinforce the constitutional imperative for clear rules in this area, Chief Justice Roberts concluded his opinion with unambiguous direction to law enforcement:

> "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple - get a warrant."

Notably, this Committee is being asked by some today to jettison precisely the type of categorical rules that Justice Roberts sought to revitalize in *Riley*. But doing so would undermine users' reasonable expectations of privacy and encroach upon the core privacy protections afforded by the Fourth Amendment. We urge the Committee to reject such entreaties and to codify the bright-line, warrant-for-content standard that is reflected in H.R. 699.

Second, since the last ECPA hearing held by the House Judiciary Committee, many states have enacted bright line statutes to bring their state law in accord with the Fourth Amendment. Hawaii, Texas, and Maine have all done this. In addition, earlier this year, the California legislature overwhelmingly approved landmark legislation to update California's electronic privacy laws (colloquially referred to as "CalECPA"). Not only does CalECPA require the government to obtain a warrant before it can compel third party services providers to disclose users' communications content, but it also extends the warrant requirement to communications metadata, including location information, as well as data stored on electronic devices.

To be clear, H.R. 699 does not even go this far. It merely preserves and codifies the constitutionally required warrant-for-content standard that has been observed by law enforcement and providers alike for many years now. Even so, and despite overwhelming support in both the

House of Representatives and the Senate, some agencies are continuing to urge Congress to put the brakes on important and long overdue reforms.

Congress Should Reject Proposals That Weaken the Core Privacy Protections in H.R. 699

Civil Government Agency Issue

Some governmental entities have argued that the *Warshak* rule hampers their ability to investigate and enforce civil violations because civil agencies do not have warrant authority and thus lack the ability to obtain content from providers. These governmental entities have proposed amending ECPA so that agencies can ultimately bypass the target of, or even potential witnesses in, civil investigations and issue legal process (on something less than a warrant) to third party service providers covered by ECPA.

It makes little sense, however, to enact a bright-line, warrant-for-content standard while simultaneously creating a new carve-out that would eviscerate that bright-line rule. Congress should eschew proposals that would create a civil agency carve-out for the following reasons.

First and foremost, a civil agency carve-out would contravene *Warshak* and the Fourth Amendment principles that animated the Sixth Circuit's conclusion in that case. Civil government agencies are still government agencies. The power to compel providers to disclose the content of users' communications should be reserved for criminal cases. Congress should be deeply skeptical of efforts to draft around the Fourth Amendment, which is what some governmental entities are asking it to do.

Second, civil agencies have long done their job without such an exception. They can and do directly subpoena the targets of or witnesses in civil investigations to obtain relevant evidence, including emails and other content the targets or witnesses have stored with providers. This is, of course, how civil litigation routinely works; a discovery request is served on a party or witness and the party or witness is expected to produce responsive material in her possession, custody, or control. There is no reason to radically alter our civil litigation system simply because of the advent of cloud computing, which enables litigants to theoretically obtain the same data from service providers like Google. Electronic communication and remote computing service providers are not, nor should they be, discovery agents for governmental entities that are conducting civil litigation.

Third, if targets and witnesses of civil investigations are intransigent or uncooperative, governmental entities have a broad array of tools to compel compliance. Civil agencies can always enforce subpoenas when a person fails to produce responsive documents. If a target or witness subsequently fails to produce responsive material pursuant to a court order to do so, the judge may

impose sanctions, which could include the denial of counter-claims, adverse inferences as a result of the target's intransigence, fines, default judgments, and even jail time.

Fourth, there is no heightened risk of spoliation or destruction of evidence by requiring civil agencies to subpoena the targets of their investigations. To the extent that civil agencies are concerned about spoliation or destruction of evidence, those concerns are exogenous to ECPA reform. If civil agencies believe that targets and witnesses of investigations, or adversaries in litigation altogether, can't be trusted to produce responsive material, that is a problem neither unique to ECPA, nor addressable by compromising the constitutional requirement for clear rules about government access to user communications.

Fifth, civil discovery often brings with it complex and difficult disclosure issues around relevance, attorney-client privilege and other privileges, trade secrets, confidential business information and the like. If served with civil process to disclose a user's content, a provider will be ill suited to raise these objections or assert privileges; that is something the user should do as part of responding to record requests directed to the user. Congress should eschew any legislative change that would put service providers in the untenable position of making these types of critical judgment calls, which have enormous implications for privacy and due process. The risks of a provider turning over privileged or otherwise protected material increases significantly with the volume of material that is sought by a civil agency. If a civil agency seeks three years' worth of email, it is likely, if not a foregone conclusion, that irrelevant and privileged material about a user will be produced.

Sixth, it is important to remember that civil agencies, even pre-*Warshak*, have operated under ECPA, and have never been able to compel production of all content. Despite this, civil agencies prosecute offenses and undertake enforcement actions against violators with regularity. In its 2014 annual report, the SEC notes that it brought a "record number of cutting edge enforcement actions." In that same report, the SEC said that it brought "more cases than ever before", including "a number of first-ever cases that span the securities industry." It did so, as Chairman White testified earlier this year, without issuing subpoenas for content from providers under ECPA.

Seventh, the proposition that civil regulatory agencies should be conferred with powers similar to criminal authorities to intrude into private communications would, if adopted, have serious implications for the privacy interests of users and the broader judicial administration of the statute, with no demonstrated need. In recent testimony before the Senate Judiciary Committee, the Securities and Exchange Commission (SEC) alluded vaguely to a potential statutory expansion of powers whereby civil agencies could compel providers to disclose communications content through some novel and undefined legal process.

The SEC's notion, which it only outlines in the broadest parameters, leaves many questions unanswered. For example, under what standard would the SEC be able to compel third party service providers to disclose the content of users' electronic communications? And how would such a standard comport with the Fourth Amendment, given the significant nature of the intrusion and the lower evidentiary standards and burden(s) of proof in civil cases? Moreover, would the ability to obtain electronic communications content under this new standard exist just for the SEC, or would it apply to any "governmental entity" under ECPA, which by definition includes thousands of state and local governmental entities, as well as other federal governmental entities? In determining which governmental entities are empowered with this new authority, should Congress make value judgments about the worthiness of the missions served by each of these governmental entities? It also raises the question of why, if the agency is able to give notice to the user and give the user an opportunity to respond, as the concept sets out, the agency can't just serve legal process on the user like every other litigant, as is done for other evidence in the possession of witnesses and defendants. The notion raises the specter of providers, large and small, conscripted into serving as civil discovery vendors, unnecessarily placed in the middle of messy and protracted litigation of others. It could also offer the government an irresistible path to circumvent the warrant requirement by using this new civil power for a case that will ultimately turn into a criminal matter.

Finally, although some civil agencies have raised hypothetical concerns that a bright line, warrant-for-content rule would frustrate their investigations, there is no evidence that civil agencies typically encounter such scenarios or that, even if they do, the investigations are hindered. In an April 2013 letter to Senator Leahy, the SEC cited a single example where it ostensibly could not have brought a case but for the ability to serve a subpoena directly on a provider to obtain email content about the target. After examining the record in that case, however, the Center for Democracy and Technology found that it "actually shows that the need for new authority is greatly overstated, if not totally unjustified," and that it "illustrates precisely the risk of indiscriminate production of personal emails that we have warned about."

Emergency Exception

Under current law, service providers *may* disclose the contents of communications or customer records to a governmental entity in an emergency involving danger of death or serious physical injury to any person. Some law enforcement agencies, however, propose *requiring* service providers to disclose the contents of communications and customer information whenever any federal, state, or local governmental entity believes there is an emergency under ECPA.

In November 2013, Google began including information about emergency requests in its bi-annual transparency report covering government demands for user data. Other service providers, including Facebook, Microsoft, and Yahoo, also now include information about emergency requests

in their transparency reports.

This data helps shed light on the volume of emergency requests that service providers receive, which is very low in comparison to the total number of compulsory legal demands that service providers receive under ECPA. In the second half of 2014, for example, Google received 171 emergency requests affecting 272 user accounts in the U.S. That figure represents less than 2% of all compulsory legal demands in the U.S. received by Google. Moreover, Google voluntarily disclosed data in response to 80% of such emergency requests. (By comparison, Google disclosed data in response to 78% of compulsory legal demands in the U.S. in the second half of 2015.) Effectively, what this means is that Google did not disclose user data in response to an emergency request on only 34 occasions in the second half of 2014. Further information about Google's handling of emergency requests appears in the table below.

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

There are many reasons why a service provider may decline to voluntarily disclose the contents of communications or customer records in response to an emergency request.

For example, the service provider may not have any responsive data that pertains to the target of an investigation. For Microsoft, according to its transparency report, this accounts for more than 26% of requests for which no data is provided in the U.S.; Microsoft simply doesn't have any responsive data to provide.

In addition, the government agency may try to use the process where there is no "emergency involving danger of death or serious physical injury to any person". Service providers take seriously their obligation to protect their users' privacy. It unfortunately appears to be the case that some law enforcement officials make emergency disclosure requests because it is easier than getting legal process, with the checks that come with it, even though legal process is available in a timely manner.

8

It's not unusual, when we turn down an emergency request because of the lack of a life or limb emergency, that we receive legal process shortly thereafter. Notably, in 2010, the Inspector General of the Department of Justice, in a report concerning the FBI's use of exigent letters and other informal requests to obtain certain customer records on an emergency basis, concluded that the abuses found made it "critical for the Department and Congress to consider appropriate controls on any use by the FBI of its authority to obtain records voluntarily..."

By granting providers the right to disclose when they believe there is such an emergency, but not an obligation to disclose when the authorities assert there is, we help ensure that law enforcement uses legal process as the preferred means to obtain user data, and the emergency process only in true exigent circumstances.

Delay in securing legal process should not be an issue. In every judicial district, a search warrant is a telephone call away. Rule 41(d)(3) permits a magistrate to respond to a telephonic request for a warrant any time, including after-hours where it is inconvenient to go to court or in an exigent situation where time is of the essence or evidence could be lost. Governmental entities avail themselves of this option and consequently obtain user data in a timely manner when exigent circumstances exist.

Finally, it is somewhat ironic to hear law enforcement agencies express misgivings about statutory authority sought by and granted to the government by the USA PATRIOT Act of 2001. Prior to the PATRIOT Act, the Stored Communications Act had no express carve out for emergency situations at all. The PATRIOT Act actually expanded the ability of government to get stored information, including content, in emergency situations. Congress should decline the request to further expand the ability of the government to compel the production of content without a warrant.

Time Limits

Some law enforcement officials propose imposing rigid time limits for providers to respond to legal process issued under ECPA. Judges, however, routinely prescribe deadlines for compliance that are tailored to the exigencies and gravity of particular cases, as well as the need for the underlying evidence. It is unclear why such a proposal is necessary or why Congress is in a better position to manage the individual dockets of judges that oversee cases. Courts, not legislatures, are better positioned to determine compliance deadlines in particular cases based on the needs of law enforcement and the underlying facts of such cases.

Statutorily prescribing time limits in a manner that is divorced from the context of individual cases would have unintended consequences that likely redound to the detriment of law enforcement.

A code-bound time limit would significantly weaken the flexibility that covered service providers currently have to address emergency requests, diverting their attention instead to the longest outstanding requests, even if there is far less urgency attached to such requests. Service providers that now expedite emergency requests from law enforcement in the absence of a rigid statutory timeframe for production would be constrained to do so in the future if they faced penalties for failing to comply with an arbitrary time limit codified under ECPA. Flexibility, not rigidity, is key for triaging unexpected volume, particularly when it relates to emergency requests.

An artifical and arbitrary time limit for production would also reduce the ability of service providers to verify the validity of legal process. There are more than ten thousand agencies that have subpoena power in the U.S. alone, and it is a challenge to make sure that any particular demand is valid. This is not just a theoretical concern. We do receive fake legal process designed to trick us into releasing user information. Current law enables providers to scrutinize and validate legal process, and, as a result, providers are able to identify fraudulent activity and report it to authorities.

Response rates can be attributable to factors that are beyond the control of service providers. For example, when Google receives legal process that is overbroad, vague, or ambiguous, that will invariably slow our response time. Moreover, a single legal request can ask for information covering multiple products and concern multiple account holders, which obviously increases the time and resources necessary to respond. Finally, law enforcement agencies often demand nondisclosure to users without proper nondisclosure orders. That, too, leads to delay. There is no responsible way to codify a statutory time limit to respond.

Proposals to impose time limits pursuant to ECPA legal process should also consider the significant increase in concomitant demands that service providers receive. Since 2009, government requests for user data issued to Google in criminal matters in the U.S. alone have increased 179%. Such proposals should also account for the explosive growth in demands for location information that wireless carriers and other providers are receiving from law enforcement.

Compelled Consent

Some agencies also recommend that Congress amend the voluntary disclosure provision under 18 U.S.C. 2702(b)(3) to require providers to disclose content with the consent of users. While this proposal may have intuitive surface appeal, there are important practical considerations that militate against adoption.

First, if the government obtains the consent of a user to disclose content, the providers are an unnecessary and inefficient conduit for disclosing this content. As noted above, providers are poorly situated to determine relevance and applicable privileges, even assuming the user has actually

consented. Providers should not be discovery agents for agencies under circumstances where users have consented to providing content. Agencies can obtain content directly from targets or witnesses if they obtain consent.

Second, Congress should be wary of proposals that would presume or deem consent based on unavailability, death, minor status, or other circumstances where users have not provided actual consent. Nor should consent be presumed or deemed given merely because the target or witness of an investigation did not respond to a legal request. As mentioned above, agencies have a broad array of tools in their arsenal in the event that uncooperative or intransigent witnesses fail to respond to legitimate requests for information.

Third, authenticating users and verifying consent is not always simple. Providers "authenticate" their users through the account information provided, and if a user confirms receipt of the authentication request, a provider is entitled to rely on it. That process is time-consuming, labor-intensive and often results in more questions than answers as users "object" to production or ask about the nature of inquiry. If a user doesn't respond, or for example, if a user is locked out of her account, service providers may rely on other factors to authenticate users, some of which may not always be useful proxies for verifying identity. Moreover, even if a user consents to provide content pursuant to legal process, there may be others (including joint account holders) whose consent may be required. But all of this is an unnecessary burden because users should be required in the first instance to comply with their discovery obligations without entangling service providers.

Notice to User

H.R. 699 requires law enforcement agencies to provide notice to a subscriber or customer of a provider within ten business days of receiving communications content pursuant to the issuance of a warrant. Notice is a core privacy protection in H.R. 699 that must be preserved. Notice from the government may be the only way that a user may ever learn of the warrant. Without notice, the user may never have an opportunity to seek relief where the warrant was improperly obtained, where privileges were violated or the disclosure of the user's communications was otherwise improper. Significantly, very similar user notice requirements exist in ECPA currently, and there has been no indication this has caused any problems.

In the physical world, of course, notice by the government of a warrant is direct and palpable at the time of execution. The notice provision in the Email Privacy Act is less exacting on the government, and gives the government time after receiving the communications to give notice. Moreover, there are no statutory rules in the physical world that authorize the government to prohibit comparable third party service providers (e.g. Public Storage) from notifying customers of search warrants served on the storage company for customer property. Seizure of a computer from

the home or workplace containing the same email stored with a provider, for example, would come with direct notice to the property owner who in turn is free under the law to tell anyone that a warrant was executed.

Currently under ECPA, on the other hand, governmental entities may obtain non-disclosure orders that preclude service providers from notifying users of legal demands for a period of up to 90 days, which can be renewed for additional periods of 90 days. The Email Privacy Act imposes a new requirement on providers. Under the bill, any provider that intends to give notice to a user about a legal demand after expiration of a gag order must give advance notice to the government. Although the National Association of Assistant United States Attorneys argues that the notice should be extended by a few days, there is currently no such advance notice requirement on providers and no indication that this has caused any problem. In 2015, it is anachronistic that service providers with hundreds of millions (if not billions) of users are more constrained to notify users of legal demands than comparable service providers in the physical world or individuals or businesses would be if their property were seized directly from them. This makes it all the more critical that the government provide notice to the user.

Notably, H.R. 699 not only allows law enforcement agencies to delay notification to users under ECPA in some cases, but also increases the timeframe for delayed notification from 90 to 180 days in response to concerns raised by law enforcement agencies. Law enforcement agencies sought and secured this particular provision to the bill. Specifically, it allows governmental entities to seek an initial delay of up to 180 days if notification to a user would lead to an adverse result, and governmental entities can seek an extension of this delay for an additional 180 days (with no limitation on additional 180 day renewals) to the extent an adverse result would persist. In light of these generous delay provisions sought by law enforcement to accommodate situations where an adverse result might occur, it is critical to preserve the direct notification provisions that afford users a meaningful opportunity to, for example, challenge warrants that may violate the Fourth Amendment and to petition for return of their seized property.

* * * * *

It is axiomatic that ECPA no longer reflects users' reasonable expectations of privacy and no longer comports with the Fourth Amendment. H.R. 699 represents an overdue update to ECPA that would ensure electronic communications content is treated in a commensurate manner to other papers and effects stored in the home, which are protected by the Fourth Amendment. It is long past time for Congress to pass a clean version of H.R. 699.

Thank you for your time and consideration.

Mr. GOODLATTE. Thank you, Mr. Salgado.
Mr. Rosenzweig, welcome.

TESTIMONY OF PAUL ROSENZWEIG, VISITING FELLOW, THE HERITAGE FOUNDATION, FOUNDER, RED BRANCH CONSULTING

Mr. ROSENZWEIG. Thank you very much, Mr. Chairman, Ranking Member Conyers. I appreciate very much the opportunity to come before you today to testify about the Email Privacy Act and the underlying principles of balancing privacy and law enforcement needs that are inherent here.

As you know, I am a former prosecutor, having spent 12 years in various roles throughout government. I then became a deputy assistant secretary for the Department of Homeland Security with significant responsibility for our counterterrorism efforts, and today I operate a small consulting company, and I serve as a visiting fellow at the Heritage Foundation. From this perspective, I am pleased to acknowledge that everybody on this panel agrees that a warrant requirement for content of email is an appropriate response to changing technology.

It seems to me almost beyond belief that notwithstanding the uniform agreement of that principle, we have been unable to work out the details of how to implement that as a matter of statutory law. To my mind, that principle has its roots not in our agreement here, but rather in the longstanding understanding of the privacy of one's personal papers and effects that goes back to the very foundings of this Nation.

The most famous case of which was the Wilkes versus Wood case. Wilkes was a protestor, much like some of the people in America today, whose papers and effects were the subject of a general warrant. That search by the Crown at that time was one of the most salient effects that drove the Revolutionary movement. Likewise, the Writs of Assistance case, which James Otis famously lost, unfortunately, in Massachusetts, was what John Adams said was the spark that lit the flame of the Revolution.

Today, email are our private papers. The ISPs that transmit my email to you are the equivalent, functional equivalent of the post office, and the cloud storage system that I use to store that information is the functional equivalent of the file cabinet in my office. There is no ground that I can see that is consistent with what the Framers understood our personal privacy and papers to be to exclude that information from the full protection of the warrant.

And I would add that our history of Fourth Amendment understanding has followed the development of technology by consistently applying that same principle. When the Supreme Court was faced with the idea of telephones in the Katz case back in the 1960's, they saw that those types of personal communications ought to be subject to the exact same sorts of constitutional protections. This notwithstanding the fact that of course telephones were unknown to the Founders, and over the dissent of Justice Black who said, you know, history says there are no telephones, if it's not in the Fourth Amendment, it shouldn't be in the Fourth Amendment.

Likewise, as Mr. Salgado has said, we've recently come to understand that the cell phones in our pockets are not just telephones. They are now mini-computers that contain the stuff and substance of everything that we know and understand, so, too, I would submit, with the content of our email communications and our stored data in cloud service providers, whether it's Google, or Microsoft, or Yahoo, or Dropbox, this is where we store our data today.

So what's the debate? What's left? All that I hear that is left is the application of exceptions that are carve outs and restrictions on this general warrant requirement. And to some degree, that has an intellectual appeal to it, doesn't it, because we've had exceptions to the Fourth Amendment for awhile, but I doubt that that's really what the advocates for the exceptions are suggesting, because I certainly have not heard any of them suggest that we should adopt as well the Fourth Amendment suppression rules for when evidence is wrongfully collected in violation of these exception requirements.

The truth is that we've had no—when ECPA was first passed in the 1980's, no exception for an emergency at all. The current statute was added in 2001, post 9/11 at the suggestions of the Department of Justice. So it's kind of passing strange that we would see that exception and expansion of it held out now as a reason to oppose the fundamental changes that are necessary in light of technology.

I would submit to you that the time is ripe for change and the principle is clear. In the normal law enforcement context, police, FBI, and law enforcement officers should have no more access to stored email than they do to our stored private letters. I would urge this Committee to give the bill before you plenary consideration in a markup and move it to the floor for consideration where these issues can be hashed out. And with that, I thank you very much. I look forward to answering your questions.

[The prepared statement of Mr. Rosenzweig follows:]

STATEMENT

Of

Paul Rosenzweig
Visiting Fellow, The Heritage Foundation
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Washington, D.C.

Before the

Committee on the Judiciary
United States House of Representatives

December 1, 2015

The Email Privacy Act

Introduction

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, I thank you for your invitation to appear today and present testimony on the Email Privacy Act, H.R. 699. My name is Paul Rosenzweig and I am the principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice. I am also a senior advisor to The Chertoff Group and a professorial lecturer in law at George Washington University where I teach a course on cybersecurity law and policy. In addition, I serve as a visiting fellow in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.[1] From 2005 to 2009 I served as the deputy assistant secretary for policy in the Department of Homeland Security.

[1]The Heritage Foundation is the most broadly supported think tank in the United States. During 2014, it had more than 500,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2014 operating income came from the following sources:

- Individuals 75%
- Foundations 12%
- Corporations 3%
- Program revenue and other income 10%

Needless to say, my testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Indeed, to be clear, I work extensively in the cybersecurity and tech space and many of my clients are following this debate with great interest. That having been said, today I am testifying as an individual discussing my own independent research. The views expressed are my own. In addition. Inasmuch as I am appearing under my Heritage Foundation affiliation it is important to note that Heritage scholars neither endorse, nor oppose legislation. Our views on the substance of particular proposals should not be read as advocating for or against the adoption of a particular piece of legislation – we write and speak about the underlying polices in question only.

There is, of course, a great deal that can be said about the privacy of email communications and proposals to protect them. In the interests of brevity and to avoid repeating much of what my colleagues on the panel will say, after offering some introductory thoughts, I will make three simple points:

- Proposals to protect by warrant requirement the content of email are consistent with fundamental values held by the Framers and the origins of the Fourth Amendment. I think, frankly, the Founding Fathers would be shocked to learn that this question is even in dispute;
- Some in law enforcement object to the notice requirement that many proposals for reform include – the idea that before (or sometimes after a period of delay) securing an individual's email, that individual should be notified of the execution of the search. But the concept of notice has been an integral part of warrant requirements for over 200 years. There is little reason to expect that law enforcement can't accommodate notice today; and
- Finally, some argue that email privacy reform will harm national security. As a former official in the Department of Homeland Security I yield to no one in my concern for national security. In my judgment, however, properly drafted exceptions can and will easily insulate ECPA reform from this concern.

I will close by offering some thought on the important context within which this debate arises, as I think there is inadequate appreciation of how broad the import is of the questions you are considering.

The top five corporate givers provided The Heritage Foundation with 2% of its 2014 operating income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Introductory Thoughts

The basic question before this Committee is simple: Should the contents of your email messages be protected from law enforcement scrutiny to the same extent as your physical letters sent through the mail?

To ask the question makes the answer seem obvious. Email is today's postal service and the personal contents of your email messages are as private to you as the letters we used to send through the U.S. Post Office.

But even though the answer seems obvious, that is not, as this Committee knows, what the law actually says. At least today, some of the contents of your email (most notably the emails you store on a server, like on a Gmail service or in Dropbox) are not as well-protected. To read your mail in transit with the Post Office, the government generally needs a warrant, issued by a neutral magistrate, and based on probable cause to believe that the search will provide evidence of a crime. To read the content of email messages stored on a server for an extended period, it doesn't need a warrant at all – it can get the content by issuing a subpoena to your cloud service provider. Unlike a warrant, a subpoena is not based on probable cause and it isn't reviewed by a judge before it is issued. In practice, it is issued by a prosecutor, unchecked by a judge, based on any reasonable ground.

The reason for this difference in treatment is more historical than malevolent. The law that protects email – the Electronic Communications and Privacy Act – was written in 1986, when cloud servers were a dream of the future and when nobody could imagine storing email for any length of time because digital storage costs were so high. Indeed, in 1984 it cost more than $100 to store a single megabyte of data. Today, you can buy a 2 terrabyte storage drive for less than $100 – and that makes the assumptions which underlie the ECPA out of date. This coming year we celebrate the 30th anniversary of the law. Indeed many of the staff working for Congress today were not alive when it was passed.

As a result, under current law, as data moves from local storage to the cloud, the government contends that it does not need to go to the owner of the data to get copies of the data. Instead, the government claims that it can go to the cloud provider, demand the data with a subpoena, and prohibit the data owner from being notified. This needs to change: When government agents want ISPs and cloud providers to disclose sensitive data, they should get a warrant from a judge.

The Fourth Amendment

Any discussion of email privacy must, in my view, be grounded in an historical understanding of the Fourth Amendment. Properly construed, I think that early history demonstrates an

overarching concern with the privacy of personal papers and effects. That, after all, is the language of the Amendment and I think that the Founders would be surprised to know that the words "papers and effects" do not cover my personal love emails to my wife, simply because they are written in electronic form rather than with pen and ink.

More to the point, the history of why the Fourth Amendment was adopted stands as a powerful reminder that the security of our personal thoughts and effects lay at the core of the Framers concerns about government overreach. The story is, by now familiar, but it bears repeating. Two seminal cases from pre-revolutionary days shaped our thinking about the proper balance between government scrutiny of the content of our communications and individual privacy intersts.

The first case, of course is *Wilkes v. Wood,* 98 Eng. Rep. 489 (1763). Wilkes was a well known memper of the opposition party in parliament. He published a pamphlet "The North Briton" criticizing the government and accusing King George III of lying. Robert Wood, an agent of the King, possessed of a general warrant, broke into Wilkes house and seized his papers. The warrant named no suspect nor any specific place to be searched. It was a "general warrant." After the fact Wilkes charged Wood with an act of trespass. He argued that a seizure of his papers and personal effects was an intrusion into his most private concerns. Wood defended, of course, on the ground that a general warrant was sufficient to the matter at hand and protected him from liability. A jury found for Wilkes and awarded him 1000 pounds – an astronomical sum in those days. He also recovered 4000 pounds from Lord Halifax, who had issued the original general warrant.

As Professor Akhil Reed Amar of Yale notes, *Wilkes* was the "most famous case in late eiteenthe-century America," one whos "plot and cast of characters were familiary to every schoolboy in America." Its lessons against sweeping warrants and roving government inspections of personal papers were at ehte core of what the Fourth Amendment intended to prohibit.

The other case, of course, was the Writs of Assistance case that arose in the colonies in 1761. Writs of Assistance were general warrants allowing officials to search for smuggled goods anywhere they suspected the goods might exists. James Otis was on the side of the crown when the Writs were issued, but he resigned his post as Advocate-General and took up the case for the Boston merchants who opposed the writs. He argued that the unwarranted search of personal effects was against British law and violated the rights of Englishmen. Otis lost the case, but his argument, and the resulting controversy galvanized the revolutionary movement. Indeed, his argument was witnessed by a young John Adams who said that "the child independence was then and there born, [for] every man of an immense crowded audience appeared to me to go away as I did, ready to take arms against writs of assistance." It is no

exaggeration to say that concern for overly intrusive government behavior and intrusion was a critical ingredient of the thinking of the Founding Fathers.

Nor is the view I've espoused idiosyncratic. To the contrary, at least one Federal court of appeals has reached the very same conclusion. In *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010) the Sixth Circuit considered the very issue that is at the core of the legislative proposal before you – whether a warrant should be required before an ISP is compelled to turn over to the government the contents of a subscriber's email. The answer it gave was an unequivocal "yes."

As the court recognized communication via email is functionally identical to the types of communication known to the Framers -- letters, for example – and to the types of communication more common in the early 20th century like telephone calls. Indeed, the court noted, email today is as pervasive and ubiquitous as those forms of communication used to be and it is equally personal in nature. For that reason the court correctly noted that it would be wildly incongruous to treat email, letters, and telephone calls differently because of the method of delivery. As the Court said: "It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."

Today, internet service providers like Google, Dropbox and Yahoo are the functional equivalent of the post office and their cloud based storage is the functional equivalent of the filing cabinet I still keep in my office. As *Warshak* put it: "It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception."

Indeed, to put the matter bluntly and directly, if I were to have mailed this testimony to the Committee and the staff were to have stored it in a file cabinet in the offices behind this hearing room, the law would (leaving aside the fact that it is Congress we are talking about) require that law enforcement get a warrant to intercept it in transit and either get a warrant or issue a subpoena directly to the recipient – you, Mr. Chairman – to get it otherwise. By contrast, because I sent this testimony in by email (and because I chose to use an ISP to send it) the government can access that same communication by way of subpoena to my service provider without notice to me and without the need to establish any probable cause to believe I've committed a crime.

One can just imagine what John Wilkes and James Otis would have to say about that state of affairs.

Notice

Many proposals, including the Yoder-Polis bill that is presently before this Committee, require that the government provide notice to the subject of the investigation when it receives electronic data about a subscriber from a provider of electronic communications services, like an internet service provider or a cloud data storage system. For law enforcement this notice is required within 10 days; for other government agencies the timeline is 3 days.

Some in law enforcement oppose this notice requirement. They suggest that it might be unworkable and/or that it would give the subjects of investigation advanced notice of the pendency of an inquiry. Neither concern, it seems to me, is at all well founded.

As to unwieldiness, based on my experience as a former prosecutor, notice is the norm; concealment the exception. For example, it is normal practice – and indeed inevitable – that the execution of a search warrant at an individual's home provides notice of an inquiry and that, absent a sealing order from the court, the subject of the investigation will get a copy of the search warrant. The same should be true of intensely personal effects like email correspondence when that data is held in a cloud storage system – just as it would be if hard copy letters were in a file cabinet in the house.

Nor should we persuaded that subjects of an investigation will be tipped off by an inquiry. There is a long-standing set of rules, codified in Section 2705, that allow a court to delay notification to the subject of an investigation if providing the notice would seriously jeopardize the investigation. I see no reason at all why that same rule of general practice – which presently covers such covert activities as bugging a suspects home – would not suffice in this context.

Indeed, the standard used in deciding whether or not to delay notice to the subject of an investigation was added to the law (codifying earlier common law provisions) at the request of the Department of Justice when the Patriot Act was enacted in 2001. It seems passing strange, indeed, that the same standard thought adequate for critical national security counter-terrorism investigations is now criticized as inadequate under the ECPA.

Finally some in law enforcement have raised concerns with the requirement that, at the expiration of a delay in notification, a customer should be advised of "the nature of the law enforcement inquire with reasonable specificity." Again, this text from the proposal before you is nothing new – it is standard language for administrative subpoenas (12 USC § 3405) and other delayed notice requests (e.g. 12 USC § 3409).

One suspects, with some justification, that the suggestion of confusion is overblown and serves more as a makeweight to conceal a broader and more fundamental objection to the proposal. But since generally opposing a warrant for content requirement cannot be politically or legally sustained (at least not after the *Warshak* case) the objections must be couched in different, but less persuasive terms.

National Security

Third, I want to briefly address the idea that proposals to amend the ECPA somehow threaten national security. As an initial matter, I want to register my disagreement with the general idea that anything that enhances investigative power is, *per se*, an improvement in national security. As I said at the outset, my views are strongly conservative and national security is at the core of my professional life. But I can see no basis for saying that the application of traditional Fourth Amendment principles derogates from national security. To the contrary, it enhances it. I could say more on the topic, but I think the best summary was offered by Robert Mueller, the former FBI director under President Bush, in a speech he gave reflecting on the pressures that arose in the wake of 9/11. As Mueller put it so eloquently: ""The rule of law, civil liberties, and civil -rights — these are not our burdens. They are what makes all of us safer and stronger."

More to the point, beyond the thematic, the assertion is simply incorrect. At least as I read it, the proposals before you have a savings clause that explicitly exempts lawful activity under the Foreign Intelligence Surveillance Act. Thus, as I read the proposal, ECPA reform will not affect intelligence investigations and counter-terrorism efforts. The Foreign Intelligence Surveillance Act has its own set of rules for government access to email and documents stored in the "cloud." ECPA reform legislation will not change those rules in any way. To be sure, there may be some edge cases, where the counter-terrorism connection is not sufficiently clear to permit invoking FISA – but I think we should all be comfortable with a default rule that favors civil liberties, rather than government intrusion.

The Broader Context

Before concluding I want to place the ECPA debate in a broader context. In my judgment one of the reasons that this discussion resonates so in Congress today is that it is emblematic of a broader failure of our Legislative and Executive institutions to come to grips with the changing technological reality of our times. Consider some of the other legal and policy challenges arising from a more greatly-interconnected globe-spanning cyber-network. We see:

- authoritarian nations increasingly restricting content on the web and using domestication requirements as a way of both suppressing dissent and protecting their own native corporations against competition;

- the privacy/security dispute dividing natural allies in America and Europe at the expense of our ability to jointly combat mutual threats;
- data localization requirements that degrade the efficiency and effectiveness of cloud architectures; and
- efforts to apply domestic laws with extraterritorial effect, putting internet providers in the untenable position of choosing between competing legal obligations.

To a large degree, our inability to deal with these challenges is fueled by parallel forces resisting the new technological reality – the unwillingness of the executive branch to modify settled behaviors and the inability of the legislative branch to find consensus for action.

As to the former, my colleagues at The Chertoff Group put it this way in a white paper we released earlier this year:

> The future prospects for law enforcement . . . is a time of uncertainty. For now, US law enforcement is still able to take advantage of American unilateralism, grounded in the circumstance that American companies dominate the market and that they can be compelled to assist American investigations. But this form of mandated assistance cannot be sustained in the long run. Even if the legal power to compel American companies to cooperate is sustained, they cannot provide that which they do not possess. A predictable reaction to such a legal régime is that American companies will lose market share because of these demands. They will be increasingly faced with stringent countervailing foreign law demands. Some nations may adopt both domestic storage requirements and, ultimately, domestic corporate preference requirements, both of which will increasingly put data beyond the effective reach of American criminal investigators.

See The Chertoff Group, "Law Enforcement access to Evidence in the Cloud Era," (May 2015). In short, law enforcement's entrenched resistance to technological change – exemplified paradigmatically by their opposition to ECPA reform – is a classic case of valuing short-term gain at the expense of long-term harm. Harm to the American public; harm to the American competitiveness abroad; and, ultimately, harm to law enforcement's own interests.

As to the latter, I find it remarkable that even though there is broad agreement within Congress on the need for ECPA reform (witness the 300+ co-sponsors of the Yoder-Polis bill and the plethora of other bills reforming other aspects of the law) we seem institutionally incapable of responding to changed circumstance. The Email Privacy Act is, or should be, an easy case. If Congress cannot muster the will to see this reform through, we might despair of its ability to deal with other, more complex and complicated questions of law and policy. In the 1960s Congress was able to pass Title III of the Omnibus Crime Control and Safe Streets Act; in the

1970s, intelligence reform under the Foreign Intelligence Surveillance Act; in the 1980s, the ECPA. These were big achievements – notable efforts by this body to deal with significant challenges of technological evolution. Today, I fear, even the most modest of reforms are locked in stasis.

Conclusion

The time is ripe for change and the principle is clear – in the normal law enforcement context, police and FBI officers should have no more access to our stored email than they do to our stored private letters. Technology has changed the way we live. Today everyone stores their email in the cloud. But the law hasn't kept up. That's why Congress needs to modernize the law. Senators and Representatives have introduced bi-partisan bills to update ECPA into the 21st century. Both chambers should give the proposals plenary consideration.

Mr. GOODLATTE. Thank you. And we'll now proceed under the 5-minute rule with questioning of the witnesses, and I'll begin by recognizing myself.

Mr. Salgado, if Congress were to issue a subpoena to Google for the contents of a customer's emails, would that subpoena violate the Fourth Amendment?

Mr. SALGADO. That's a question I would have to look into as to how the Fourth Amendment applies to Congress, so I've not done enough research to be able to answer that with much confidence. I would say that the changes we're talking about today to ECPA would not in any way affect the investigative powers of Congress.

Mr. GOODLATTE. I think it's a very important question, however, because if you can't answer that question from me right now, answer this question. What's the constitutional distinction between congressional and executive subpoenas?

Mr. SALGADO. Again, I'd probably have to investigate that. The Fourth Amendment is what the Fourth Amendment is, so if there is a restriction there that's based on the Constitution, that exists regardless of what we do with ECPA.

Mr. GOODLATTE. If the subpoena issued to Google for the contents of a customer's emails, the customer might be a government employee who is acting outside of the government's servers and email system and is storing data on Google's cloud, what ability would the Congress have to conduct oversight if your finding is that it violates the Fourth Amendment?

Mr. SALGADO. I don't know that it would, but I do note that Congress would have all the authority it does now to direct the subpoena to the user to get the information directly from the user.

Mr. GOODLATTE. We would very much appreciate your taking some time to think about the answer to that question because it's a very important question with regard to how we address this. Because there either is not a violation, in which case the question arises what's the constitutional distinction between congressional and executive subpoenas, or there is a constitutional violation, in which case the Congress' ability to conduct proper oversight of the executive branch is a very significant one.

Mr. SALGADO. I'd be happy to answer the question. I don't think it touches on the question of this particular step, this particular bill, but I'd be very happy to look into that for you.

Mr. GOODLATTE. Thank you.

Mr. Ceresney, critics of a civil mechanism cite to the fact the SEC has not sought to serve a subpoena on a commercial provider in the 5 years since the Sixth Circuit's decision in *U.S. v. Warshak*. You've heard some of those criticisms right here on this panel today.

They say it's not really a problem that needs to be solved because of that fact. Is this true? And if so, why hasn't your agency sought to challenge the warrant only policy adopted by many providers following *Warshak*?

Mr. CERESNEY. So Congressman, the decision was made at the time. I wasn't at the SEC at the time, but after *Warshak*, a decision was made in excess of caution not to issue subpoenas to ISPs without consent of the subscriber. And since I've been at the SEC,

we have held off on doing that in deference to the discussions have have been ongoing in Congress about amending ECPA.

At the same time, we have never felt like *Warshak* precluded us from obtaining email under the Constitution pursuant to a subpoena with notice to the subscriber. *Warshak* dealt with a grand jury subpoena with no notice to a subscriber, and it did not undermine a long line of case law that exists, that holds that where a subscriber or the party you're seeking email from or seeking material from has precompliance review before a court that that satisfies the Fourth Amendment. It is true that we have not done it, but I can tell you there are cases ongoing which——

Mr. GOODLATTE. I know that you haven't done it. I want to know why.

Mr. CERESNEY. Right. And that is because in an excess of caution at the time and in deference to these discussions, you know, in deference to the discussions that have been ongoing before Congress about the decision of what to do to reform ECPA. From our perspective, there are ongoing investigations that would definitely benefit from ISP subpoenas where we have not obtained email from a subscriber that we do know exists, but we're not able to obtain it because we have not been issuing subpoenas to ISPs.

Mr. GOODLATTE. So how has that affected your ability to conduct investigations?

Mr. CERESNEY. I think it has affected our ability to conduct investigations. We issue subpoenas to individuals all the time for their email, and all the time there is instances where those individuals either don't produce——

Mr. GOODLATTE. And before *Warshak*, you would then issue a subpoena to a third-party holder of those emails. Is that correct?

Mr. CERESNEY. That's correct.

Mr. GOODLATTE. And since then, you haven't felt the need to attempt to do that, and have the courts clarify this issue, which now the Congress is being asked to clarify?

Mr. CERESNEY. We have felt the need, Congressman, but we have, in deference to these ongoing discussions in Congress about reforming ECPA, determined not to do that. But we certainly have identified cases where it would have been helpful to do that to our efforts.

Mr. GOODLATTE. All right. Let me ask one more question to Mr. Littlehale. In addition to serving the warrant on the customer, H.R. 699 also requires law enforcement to provide notice to the customer of the nature of the law enforcement inquiry with reasonable specificity.

Is law enforcement required to provide such information to a person when they serve a search warrant on their home? What is the harm if law enforcement is required to inform the subject of investigation of the nature of the law enforcement inquiry with reasonable specificity?

Mr. LITTLEHALE. Mr. Chairman, in traditional search warrant practice on the premises to be to served——

Mr. GOODLATTE. Turn your microphone on, please.

Mr. LITTLEHALE. Sorry, Mr. Chairman. In traditional search warrant practice, the requirement is simply that law enforcement leave

a copy of the warrant and an inventory of items seized on the premises to be searched.

And in the analogy to a service provider, an entity that is in possession of evidence, we serve a copy of the warrant on them, and we give them notice of the fact that we're requiring them to produce the records.

H.R. 699 imposes an additional set of requirements that we actually discuss something about the nature of our investigation that goes beyond what's required in traditional search warrant practice.

Mr. GOODLATTE. Thank you very much. The gentleman from Michigan, Mr. Conyers is recognized for 5 minutes.

Mr. CONYERS. Thank you, Mr. Chairman. Before I begin my questioning, I'd like to ask unanimous consent to introduce a statement from the gentleman from Colorado, Mr. Jared Polis, into the record. He's the lead Democratic Member on this bill, and his views are worth consideration by the Committee. Can I get a unanimous consent request approved?

Mr. GOODLATTE. Without objection, it will be made a part of the record.

[The information referred to follows:]

Prepared Statement of the Honorable Jared Polis, a Representative in Congress from the State of Colorado

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee:

Thank you for convening this important hearing on H.R. 699, the Email Privacy Act. The Email Privacy Act is the most cosponsored bill in Congress awaiting floor action, and the problem it addresses is one of the most pressing constitutional concerns of our modern age: How can we stop the advancement of technology from eroding our fundamental right to privacy?

In the broadest possible terms, the obvious answer is that we need to update our laws. Many of the laws governing the use of the technology Americans most frequently use today were written long before any of that technology existed or was even conceived of. Congress simply cannot purport to protect Americans' constitutional rights while leaving the federal government to enforce laws designed for a world that doesn't exist anymore.

Today, the law governing many of our online privacy rights is the Electronic Communications Privacy Act (ECPA) of 1986. In 1986, for the vast majority of Americans, "electronic communications" meant a phone call placed from a landline. In 1986, Apple had just released the Macintosh Plus—a cutting-edge personal computer that provided users with an entire megabyte of memory. Today, iPhone 6 users walk around with 16,000 times that amount in their pockets. In 1986, the "World Wide Web" was years away from taking off. Today, that term is already a relic of the past.

As a result of Congress's failure to keep up with the pace of technology, every American's email can be subject to warrantless searches thanks to a 29-year-old legal loophole. Under ECPA, the government has the ability to search through any digital communications stored on a third-party server—such as your emails and instant messages—without a warrant, as long as they are more than 180 days old. In 1986, this loophole may have seemed reasonable because individuals simply didn't leave their emails stored on a server for months at a time. That kind of digital storage space just didn't exist, so authorities considered emails not deleted after six months to be abandoned. In 2015, however, consumers routinely store emails digitally for months or even years at a time.

Most Americans have no idea that a law written 29 years ago allows the government to open their old emails without probable cause. And when they find out, they're shocked—because that reality is simply impossible to square with the basic liberties guaranteed in our Constitution. It simply makes no sense that our homes, cars, and mailboxes are protected from unwarranted government searches but the government can sift through our email inboxes with impunity.

Congress has the power to change that. The Email Privacy Act has 304 cosponsors in the House—a bipartisan, veto-proof supermajority of Members of this body—and far-reaching support across all sectors of the economy and across the political spec-

trum, from groups like the Heritage Foundation and the American Civil Liberties Union to tech startups, Fortune 500 companies, and Chambers of Commerce.

There are some federal officials calling for special carve-outs and lower burdens of evidence in order to access Americans' old emails. I urge the committee to resist these efforts to undermine the bill for several reasons.

First, the sheer volume of support for this bill suggests that Americans and their representatives in Congress overwhelmingly support the legislation as written and do not believe electronic correspondence should be subject to a lower standard of evidence than physical documents when it comes to government searches.

Second, the authors of ECPA clearly did not anticipate a future in which Americans have access to nearly unlimited storage space that allows us to store our emails on the cloud in perpetuity. In asking for a special carve-out from warrant requirements, these federal agencies are asking for broad new search authorities that go far beyond the intent of the 1986 legislation and that would significantly undercut the intended reforms of the Email Privacy Act.

Third, the federal officials asking for these broad new authorities have not put forward compelling evidence that the 180-days loophole has served a legitimate law-enforcement purpose.

And finally, it is impossible to square a lower standard of evidence for emails older than 180 days with the Constitution's 4th amendment protections against unreasonable search and seizure. There is simply no constitutional basis for exempting digital correspondence from our privacy laws, and there is no compelling safety or crime-prevention reason for doing so either.

The 180-days loophole is a longstanding problem with a simple, bipartisan, broadly popular, noncontroversial solution at the ready. With 304 cosponsors in the House, the Email Privacy Act is the most-cosponsored bill of the 114th Congress not to receive a floor vote. I urge the Committee to favorably report H.R. 699 so that it can finally get a vote on the House floor, where I am confident it would pass with overwhelming bipartisan support.

Thank you.

Mr. CONYERS. All right. Thank you. Let me begin my questions with Chris Calabrese. I'm trying to find out why this bill is so popular from your point of view. The Email Privacy Act, 304 sponsors, privacy advocates, civil libertarians support it, former prosecutors, Fortune 500 companies, and small businesses across the country. More than 100,000 Americans have signed a petition urging the White House to support this measure. How come?

Mr. CALABRESE. Well, I think that Americans believe very strongly in the values that underpin this Nation, the fundamental idea of privacy and a balance between what government can do and having rules around how they can do it. All this bill does is the very modest step of bringing our privacy protections into the 21st Century, and everybody agrees with that.

A recent poll in the Washington Post said that 86 percent of Americans supported reform. This panel is unified in saying that we need a warrant for email. Now, we have some minor issues around the edges, but honestly, I believe that this is a bill that would pass Congress or pass the House of Representatives by 300 or 400 votes.

It is that popular. It is that common sense. I think we simply need a markup. We can work out some of these issues around the edges, and the American people can get the privacy protections that they want and they need. Thank you.

Mr. CONYERS. Thank you. And also in your testimony you mention that the bill faces a concerted assault from civil agencies that seek to use statutory changes as a tool to gain new powers. Some argue the powers are already on the books. Why do you refer to the SEC's proposal as a request for new powers?

Mr. CALABRESE. I think that if you don't use an authority for 5 years and there is a questionable legal standard about whether you can use it at all, it's new authority. That's simply put. It simply can't be that you have this existing authority and you say it's incredibly valuable but you've held off on using it for 5 years. Either what you're doing in your investigations aren't important, which we all know is not true, or you don't think you have this authority, and to me, there are really no other options, and I think that this is new authority.

Mr. CONYERS. Thank you.

Mr. Rosenzweig, the government often conducts parallel criminal and civil investigations to the same target. What would be the practical consequences if we adopted a warrant standard for email in criminal investigations and some lesser standard for those in civil investigations?

Mr. ROSENZWEIG. There'd be the risk that the exception would swallow the rule. I spent much of my early career prosecuting environmental criminal cases, a regulatory area where the civil regulatory authorities had civil and administrative powers for securing evidence. There was a set of procedures, parallel proceedings procedures, that were internal to the executive branch that governed the circumstances under which those civilly collected evidence could be transferred to the criminal prosecution side for use in a criminal case. Those rules were simply rules of grace at the discretion of the executive branch. They were not statutorily mandated and they were not expressed in any constitutional limit.

There would be at least some risk that in an effort to evade the warrant requirement that was created by reform of ECPA, criminal authorities would solicit the securing of that evidence through civil process under a lesser standard. I do not mean to ascribe ill motivation to anybody in any part of this process. But, nonetheless, the interstitial pressures are very real.

Mr. CONYERS. Let me squeeze in one final question here. The Sixth Circuit in *Warshak* held that, to the extent that the Stored Communications Act permits the use of subpoenas to compel the production of email, the statute is unconstitutional. Given that holding, is the mechanism proposed by the SEC also unconstitutional? Anybody want to try that in addition to you?

Mr. ROSENZWEIG. I think it likely is. It hasn't been tested in court. There is a history of restricting civil authorities for constitutionally protected material. There's also, frankly, some law that points to things called administrative searches that might be seen as a validation of the SEC's position. If I were to judge it, I would probably say—come down against it, but nobody makes a lot of money predicting the Supreme Court.

Mr. CONYERS. Could it withstand the Fourth Amendment challenge in the courts, do you think?

Mr. ROSENZWEIG. I would say no.

Mr. CONYERS. All right. Thank you so much.

Thank you, Mr. Chairman.

Mr. GOODLATTE. Thank you, Mr. Conyers.

The Chair now recognizes the gentleman from Wisconsin, Mr. Sensenbrenner, for 5 minutes.

Mr. SENSENBRENNER. Thank you, Mr. Chairman.

In the *Warshak* case in 2010, the Sixth Circuit ruled the content of America's emails is protected by the Fourth Amendment. I agree with that holding. Since that decision, the SEC has been unable to subpoena email content from service providers.

Now, Mr. Ceresney, I've read your testimony and listened to it. Did you write it in 2009?

Mr. CERESNEY. No. I wrote it——

Mr. SENSENBRENNER. Okay, well, thank you very much.

Now, if the SEC cannot currently subpoena email content from service providers, is it truthful to testify that if H.R. 699 becomes law the SEC will be denied the ability to obtain evidence?

Mr. CERESNEY. I don't agree that we're not able to do it currently. We have refrained from doing it in deference to Congress' ongoing discussions about it.

Mr. SENSENBRENNER. Okay. Well, I guess you kind of ignored the *Warshak* decision on that.

Now, even under ECPA as it was written almost 30 years ago, the SEC could only subpoena email content after it was older than 180 days. Aren't you asking this Committee to expand a legal authority that was found unconstitutional in a more limited form?

Mr. CERESNEY. We are not. I think——

Mr. SENSENBRENNER. Well, then, why aren't you? Because you would like to be able to issue subpoenas on email content that's less than 180 days old.

Mr. CERESNEY. We would defer. If Congress decided that——

Mr. SENSENBRENNER. No. No. No. No. No. No. No. You know, the thing is, is that I think the court has decided and you're not happy with the court decision. What your testimony says is that you'd like to expand something that's already been held unconstitutional.

Mr. CERESNEY. I disagree. *Warshak* was——

Mr. SENSENBRENNER. Well, I disagree with you.

Now, let me ask the whole panel, just to ask yes or no. If Congress gives civil agencies the authority to subpoena email content to service providers, would that law be constitutional? I think Mr. Ceresney has already said yes.

Mr. CERESNEY. Yes.

Mr. SENSENBRENNER. Can I get a yes-or-no answer from the other five panelists?

Mr. COOK. I'd love an opportunity to explain the——

Mr. SENSENBRENNER. No. I'm limited on time.

Mr. COOK. I understand, sir.

Mr. SENSENBRENNER. Yes or no please.

Mr. COOK. My answer is yes, it would be constitutional.

Mr. SENSENBRENNER. Mr. Littlehale?

Mr. LITTLEHALE. Yes, it would be.

Mr. SENSENBRENNER. Mr. Calabrese?

Mr. CALABRESE. I believe no, it would not be.

Mr. SENSENBRENNER. Mr. Salgado?

Mr. SALGADO. I believe no, it would not be.

Mr. SENSENBRENNER. Okay. Mr. Rosenzweig?

Mr. ROSENZWEIG. No. That's what *Warshak* said.

Mr. SENSENBRENNER. Uh-huh.

Now, I think we've heard from Mr. Ceresney. Messrs. Cook and Littlehale, since you believe the law would be constitutional, how

do you square that position with the Sixth Circuit court's holding in *Warshak*?

Mr. COOK. Well, I think the critical distinction is the one that the SEC has already drawn, and that is that the subpoena at issue there was a grand jury subpoena, one issued with no notice to anybody. The Fourth Amendment to the United States Constitution, as we all know, has never imposed a warrant requirement without any exceptions or without any other way to meet the reasonableness clause.

Mr. SENSENBRENNER. Okay. Mr. Littlehale?

Mr. LITTLEHALE. Congressman, I believe that the due process provided by the SEC proposal offers a significant amount of protection, the same sort of protection contemplated by the Fourth Amendment, and I believe that the courts would view that as sufficient protection.

Mr. SENSENBRENNER. Well, you know, the issue is, is that a subpoena—there can't be a motion to quash a subpoena until it's served. So even if there's an immediate motion to quash a subpoena, isn't there the risk of a constitutional violation here?

Mr. CERESNEY. Congressman, there isn't. That's because our subpoenas are not self-executing. If we want to enforce our subpoena, we need to go to a court and compel production.

Mr. SENSENBRENNER. Okay. Well, except that *Warshak* seems to indicate the opposite. Well, you know, the thing is, is that here we're having to balance the fact that apparently the position of law enforcement is that they want to expand what is currently the law. And the position of those who are privacy advocates say the law is the law and codify it.

I think this is a slam dunk for Congress to make a determination, because we already have something that everybody seems to think is okay, you know, except a few people that would like to expand the dragnet.

With that, I'll yield back.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman. And I'm glad that we're having this hearing today. As had been mentioned at the beginning of the hearing, over 300 Members of Congress are sponsoring the legislation. So it hasn't been a close call for most of us.

There is a competing—not a competing bill, a bill that encompasses the provisions in this bill, but also goes to geolocation. And I'm wondering, Mr. Cook, the DOJ recently enacted a policy requiring a warrant before deploying a cell site simulator, like a Stingray, to locate a suspect using their cell phone. Does your association support that policy?

Mr. COOK. The answer to that, of course, is yes. The use of a Stingray or Triggerfish, cell site simulator, under certain circumstances would trigger Fourth Amendment protections. That is to say that either a warrant or one of the exceptions. And there are many occasions when law enforcement uses a Stingray and it does so under the emergency aid or exigent circumstances exception.

Ms. LOFGREN. If you support this absent the exigent circumstance exception, which we're not arguing against, would you consider that a warrant for any means of obtaining real-time

geolocation information should also be favorably supported by your group?

Mr. COOK. I'm not sure I understand.

Ms. LOFGREN. For example, you don't need a Stingray to actually identify where a person is with a cell phone. But the identification issue is the same. So wouldn't that logic extend to that?

Mr. COOK. Well, when law enforcement seeks prospective tracking of a suspect, as was the case in Jones, an ongoing tracking, then the Fourth Amendment is implicated. And I think Jones resolved that for us.

Ms. LOFGREN. I think it did as well. Shouldn't that same logic apply also to historical location information?

Mr. COOK. That's a great question. And of course, as I can tell from your questioning, you're fully familiar with the court struggling with that issue, the fourth and the fifth circuit and other courts divided on that. And so part of the division I think is driven by an understanding of the technology. The technology with respect to some location information is that it's just not as specific as GPS tracking. And with respect to that, the courts have recognized that there's——

Ms. LOFGREN. If I can, I don't want to run out of time. Assuming that the technology issues are resolved, and it's not the U.S. Attorneys Association's job to do that, logically shouldn't the Fourth Amendment apply to historical records as well as prospective records?

Mr. COOK. The other longstanding doctrine, of course, that touches on that is the one that the courts have pointed to, and that is the Smith and Miller third-party records doctrine.

Ms. LOFGREN. Right, which has also been not favorably received recently by the Congress.

Let me turn to you, Mr. Salgado, because we have approached this whole issue from the point of the Fourth Amendment and the Constitution and the right to privacy and the like. But it also has an impact on American business. The most important technology companies in the world are located in the United States. I would like, can you comment on the impact, if any, on American business for a perception in other countries that privacy is not secure if you use an American product?

Mr. SALGADO. Thank you, yes. I certainly can easily burn up the rest of your time with an answer to that question. It is a significant impact on American industry that there's a perception outside of the United States—Europe, it's no secret, certainly holds this perception—that data held by U.S. companies is somehow there for the taking for U.S. Government.

This bill, the Email Privacy Act, is a good step toward getting rid of that misperception, making sure our statutes reflect the true protections that the Fourth Amendment offers.

Ms. LOFGREN. Now, if I can, and you may not have the answer to this, but certainly this is not an issue just for Google, but for Facebook and all the ISPs, and Microsoft has a big case in Ireland right now, and the like. Has anybody added up the dollars at risk to the U.S. economy on this privacy issue?

Mr. SALGADO. You know, that may have been done. I'd need to get back to you with that, it's not on the tip of my tongue, to be able to answer.

Ms. LOFGREN. Okay. That's fair enough. I would like to just mention that the Chief Justice's conclusion in Riley versus California is, "Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple, get a warrant."

How does that decision apply to the legislation that we're considering today, in your judgment?

Mr. SALGADO. I think it illustrates the point that the Supreme Court wants us to have bright rules so that the law enforcement officer in the field knows what to do. And when we're talking about the Fourth Amendment and our right to privacy, we're not messing around with gray areas, that we recognize the significance of this right to Americans, we recognize the significance of the privacy interest, we have clear rules, and the rules should be to default to a warrant.

Ms. LOFGREN. Thank you very much. My time has expired, Mr. Chairman.

Mr. COLLINS [presiding]. The gentlelady's time has expired.

The Chair now recognizes the gentleman from Iowa, Mr. King.

Mr. KING. Thank you, Mr. Chairman.

I thank the witnesses for your testimony.

First, it was mentioned that there's a general agreement among the panel, I believe, and others, that except for a few people who would like to expand the dragnet. I would ask Mr. Cook and Mr. Littlehale, is there anything in this bill that expands the dragnet?

Mr. Cook?

Mr. COOK. Well, I'm troubled by the characterization.

Mr. KING. Well, let me define dragnet so that you don't have to. And that would be is there anything in this bill that expands your ability to do investigations that maybe makes innocent citizens more vulnerable?

Mr. COOK. No, sir. I think that the bill is narrow, in fact, expansively limits in a couple of unprecedented ways law enforcement's ability to do their job.

Mr. KING. That's my understanding of it as well. Mr. Littlehale?

Mr. LITTLEHALE. Yes, Congressman, I share that concern.

Mr. KING. And you would share the characterization with Mr. Cook as well?

Mr. LITTLEHALE. I believe that the bill imposes additional limitations on traditional search warrant practice. And even if the standard of proof governing an additional category of records as contemplated in the bill is given, we will have less authority with respect to those records than we would with records in the physical world, yes.

Mr. KING. I thank both gentlemen. I turn to Mr. Salgado. In thinking about this from a Google perspective, when I or a citizen sign up for an email account, there's a long agreement that's there that I have to confess I have not studied that or have my attorney look that over, but I say, okay I agree. And I sign up for my email. And I'm glad to have the service. And it works really good. Am I in that waiving some protection to privacy in that agreement?

Mr. SALGADO. Well, not with regard to what we're talking about here. The agreements certainly talk about how we use the information and where we might be needing to disclose it in order to provide the service. So it's meant to describe to you, and those who are interested in knowing these things, what's happening. But with regard to this bill and the Fourth Amendment, we will honor search warrants that are served on us in valid legal process.

Mr. KING. Will you honor subpoenas?

Mr. SALGADO. We honor subpoenas but not for content. So we will honor subpoenas for what the statute says we honor subpoenas for. And it's our preference to let users know when we get these requests, unless we are informed by gag order, for example, that we're not able to. So we will honor all of those rules that Congress has set in place and that the Fourth Amendment has established. We also will honor requests to preserve information while law enforcement goes through the effort of getting a search warrant which may take a period of time.

Mr. KING. Are you aware of any ISPs that have a different policy than you're describing here with Google's?

Mr. SALGADO. There may be slight differences in how the product works or the policies are slightly different. But, no, generally I think the sort of pattern I'm describing is one that certainly the larger companies here operate under.

Mr. KING. Then practice is pretty close to the mirror of the act we're discussing, the legislation we're discussing?

Mr. SALGADO. Yes, sir. I think that's right. I'm not aware of providers who are producing content on anything less than a search warrant at this point.

Mr. KING. So I would burn more time on that but I appreciate your response. And I would like to turn to Mr. Rosenzweig because I believe that you gave the clearest definition of modern electronics versus the postal service from that constitutional—the Founders' era. This is still the constitutional era. And I would put it this way, ISP equals post office, emails equal your filing cabinet. Is that an accurate description of yours?

Mr. ROSENZWEIG. ISPs equal the post office, yes. That would be my summary or stored email equals letters in my file, right.

Mr. KING. Okay. Yes. Stored emails. And could I have the right to, if I had an ISP provider that said we want to waive, will you waive your authority, will I waive my constitutional protections and hand that data over to an ISP provider, I could do that willingly, couldn't I, under the constitution and current law?

Mr. ROSENZWEIG. Oh, you could consent to anything. Provided your consent is voluntary and not coerced, you could. You don't, if the police come to your door and say can I get the letters in your file cabinet, you don't have to require a warrant. You could say sure, come on in.

Mr. KING. You're familiar with *California v. Greenwood*?

Mr. ROSENZWEIG. Yes.

Mr. KING. And so the distinction here between *Warshak* and *California v. Greenwood*, which is essentially if you take your garbage out to the curb, it's not protected by any Fourth Amendment right. If I delete my emails, and they're within the custody of an

ISP, and I've waived my right to privacy, that would be open access then to the investigators?

Mr. ROSENZWEIG. I would say no. But I would have to think about that. My sense is that when I delete the email, I'm intending not to throw it to the curb as garbage, but rather to eradicate its existence altogether. If I'm aware of the fact that a copy is kept, maybe. But I don't think I'm aware.

Mr. KING. So it's actually, we're getting where we need to go with this panel, I think is the distinction between *Greenwood* and *Warshak* on what those emails consist of, are they garbage or aren't they, are they access to an investigator by subpoena or by a warrant or aren't they. So I appreciate the panel. This has been clarifying testimony today. And I thank the Chairman. And I yield back the balance of my time.

Mr. COLLINS. At this time, the gentlelady from Washington State, Ms. DelBene, is recognized.

Ms. DELBENE. Thank you, Mr. Chair. And I just want to thank the Chair for holding this hearing and to all of you for taking the time to be here with us today. Mr. Ceresney, do you dispute the continued availability of preservation orders and court interference to enforce administrative subpoenas of targets of SEC investigations should the Email Privacy Act pass?

Mr. CERESNEY. So if the question is whether preservation requirements should be contained in the statute and the ability to obtain from the subscriber, should that also be required.

Ms. DELBENE. Do you think if the Email Privacy Act passes, do you think that you're going to continue to have the availability of preservation orders and court interference to enforce administrative subpoenas?

Mr. CERESNEY. I believe that that is still something that one could obtain under the proposed statute. But what that wouldn't allow us to do is to then obtain those emails from ISPs when the individual doesn't provide them to us.

Ms. DELBENE. So you've argued in your testimony that one problem with the Email Privacy Act would be that it leads targets of investigations to delete emails, thereby destroying evidence. So are you telling this Committee that the Email Privacy Act would be to blame if you don't take the commonsense step of issuing a preservation order on an ISP from day one of an investigation. Is there any reason whatsoever that you wouldn't take that step, that very simple step, which can be done directly by the SEC without a judge's involvement?

Mr. CERESNEY. We would certainly take that step. The problem is the preservation doesn't then allow us to then obtain the email from the ISP. So certainly we would do that, we would try to preserve the email and make sure that it's available. But then the next step, that is obtaining it from the ISP, that would not be available to us.

Ms. DELBENE. So your comment that this would lead people to delete emails doesn't really hold water. If you have a preservation order, the information is going to be saved there.

Mr. CERESNEY. But if the person deleted the email and then we subpoenaed the person, they wouldn't have it. The only person, the

only entity that would have possession, custody, and control of the email would be the ISP and we wouldn't have an avenue——

Ms. DELBENE. If you have a preservation order, then the ISP is going to preserve that information.

Mr. CERESNEY. Yes. But if they preserve it and we can't obtain it——

Ms. DELBENE. I don't know about you, but I use email to keep in touch with my family, my husband, my friends back home in Washington State, all across the country. And I'm sure pretty much everyone in this room and this building would tell a similar story. As email has gone mobile, it's virtually indistinguishable from a phone call or a text message and, no doubt, contains very important details of people's personal lives and stored in the cloud by companies like Mr. Salgado's, and we would all hope to be kept safe from intruders or prying eyes.

I find it highly disturbing in your testimony today that seems to suggest that the SEC views email service providers more like a witness or an informant that you would be able to tap directly for information as opposed to the digital home of intimate communications. So let me ask you this: If the SEC wants a box of documents sitting in a target's home, can you use an administrative subpoena to bring a locksmith to their home to open the door, walk in, and take documents?

Mr. CERESNEY. We cannot. What we——

Ms. DELBENE. Then please explain to us why you think we should give you the ability to do exactly that with a digital equivalent. How that could possibly comport with simple expectations of privacy and due process and without a shred of meaningful evidence from you so far or anyone else that the lack of this authority will have any impact on your ability to carry out investigations whatsoever?

Mr. CERESNEY. We view the ISP as a third-party storage provider, much like an Iron Mountain provider would be for hard copy documents that are kept in a storage facility. And if in the circumstance where hard copy documents are kept in a storage facility, we could go to that storage facility with notice to the person who uses that storage facility and try to obtain those documents via subpoena. And that I think is the analogy that we would draw that would be appropriate in these circumstances.

And from our perspective, we do have instances in the past when we did issue ISP subpoenas where we could show that we obtained significant evidence in investigations for that purpose. As to the last number of years when we haven't used it, we don't know what we have lost. But it's certainly our investigations——

Ms. DELBENE. I want to get your view, Mr. Calabrese, on this in terms of the role of that third-party provider being the home of people's personal communications.

Mr. CALABRESE. Well, it's clearly our digital home. I mean, you would find much more sensitive information about me in the cloud than you honestly would in my house at this point. If you wanted physical documents, they are much more sensitive in my house. The thing I would also like to point out that we haven't really touched upon here is that the standard for accessing information in the civil context is very low. It's mere relevance. It's not a high

standard of probable cause. Also the number of things that a predicate—a civil agency has, sort of simply mis-filling out your taxes, for example, are much greater than the criminal predicates for a warrant. So we're talking about a much lower standard, much greater number of ways that we can access information. That means that we're potentially opening up the cloud to much greater invasion by civil agencies even than we would by criminal agencies. And I think that's exactly backwards.

Ms. DELBENE. And, Mr. Ceresney, if you give me just a couple more seconds, Mr. Chair, you talked about cases. Can you give me the specific names of those cases?

Mr. CERESNEY. We have a number of cases. And we would be happy to provide it to your staff. It includes an accounting fraud case where an email indicated that somebody was using earnings management, an insider trading case where an email contained a tip, a microcap fraud case where the emails showed control of corporation. And just one last thing to answer Mr. Calabrese's point, we would be fine if Congress established a probable cause standard as the standard that we would have to meet. Whatever standard Congress would like to establish for us to have to meet, we are fine meeting that standard. What we need is some mechanism in instances where an individual does not produce to us email, and has deleted it, or otherwise destroyed it——

Ms. DELBENE. And I think we've already discussed that right now. Post-*Warshak*, you have never used that authority. So my time has expired. And I just want to yield back.

Mr. COLLINS. The gentlelady's time has expired. At this time, the gentleman from Texas, Mr. Gohmert, is recognized.

Mr. GOHMERT. Thank you, Mr. Chairman. Thank you to the witnesses for being here. For anyone that can answer, if someone deletes an email that he or she has already sent out, would the ISP be able to retrieve that at some point?

Mr. SALGADO. I would be happy to try to answer that. It may vary from company to company. In most cases, I think it's fair to say that there would be some short period of time between the point of deletion and when the system purges the content that has been deleted. So there would be some period of time. That time period may vary from provider to provider.

Mr. GOHMERT. Couldn't it be retrieved from the person to whom it was sent?

Mr. SALGADO. It certainly could. So there may be many communicants involved in it.

Mr. GOHMERT. Right. The issue there, and I'm not one of the cosponsors at this time, even though I am one of the persons proudest of the work that Kevin Yoder has done in getting this bill to this point. I think it's fabulous. I think it's important. My concern has been, is that we have left a provision at page 10, for example, that allows the governmental entity to apply for a court order so that they can still not inform the individual. And that's fine to my mind if there's a question of endangering the life or physical safety of an individual, like a child that was talked about, flight from prosecution. As a former judge, I've signed all kinds of felony warrants. But I made sure that there was probable cause. And I made

sure there was particularity in the description in the affidavit, as well as in my warrant.

And I felt very comfortable in 2005 and 2006 when the Bush administration was ensuring us we would never use the national security letters for anything unless there was someone who actually had contact with an international terrorist or terrorist organization, those type of things. And then we find out in I think in July of 2007, the IG said there were potentially thousands of abuses where there was basically no case, they just sent them out. And I'm surprised to hear this from me, but in the New York Times, there's a good article by Carla Monyhan talking about Nicholas Merrill, how he fought to disclose the contents of the NSL. And then we also, with the disclosures of Snowden, yes, he committed an act of treason, but he also exposed lies by the last Administration and this Administration.

When I saw the order, the affidavit and order regarding Verizon's disclosures of all of their metadata, I realized we were lied to by both Administrations about what was being sought. We were told that, look, you don't have to worry, there's a FISA court, a confirmed judicial nominee that's a Federal judge, they'll protect the Constitution. There was no particularity at all, just give us everything on everybody you got. And the judge just signed, oh, okay, you want everything? Here's everything. I couldn't believe it.

And so I'm not as comfortable with providing the exception that I'm sure was demanded by governmental entities. And I'm wondering if an excuse of destruction of, or tampering with evidence or intimidation of potential witnesses, enough to get an order saying we can avoid informing whoever sent the email or whoever should have possession of the email, we don't have to inform them if we're concerned they might delete the emails. Really? Well, that would always be a concern. So you could always, always, always get some judge somewhere that would sign off on that order. I know that now after seeing the disclosures by Snowden. So I'm not comfortable that this is really going to be that helpful because of that massive gaping hole.

On page 11, it says that basically the provider would have the burden of notifying the government at the end of the exclusionary notice time. The provider has the burden of notifying the government. The government, okay, my time is about up, so I'm going to notify the subject of the warrant, so that the government can get, there should be no burden on the provider to do that. If the government wants to keep that secret, the government should try to extend it. But I'm not sure that it wouldn't be extended automatically in virtually every case.

Mr. Rosenzweig, you say that we should not—we've always protected a man's documents and we shouldn't change that because it's in a cloud. I would agree. But the ISPs require we check a box that says these documents aren't yours anymore, they're mine. And I'm wondering if maybe we should have some legislation that tells ISPs, you know what, these documents, they really are the property of the person that created them, not the one who holds or provided the safe to put them in.

Mr. COLLINS. The gentleman's time has expired. But the witness may answer.

Mr. GOHMERT. Anybody care to respond?

Mr. ROSENZWEIG. I share, I would respond by saying I share your concern about the delayed notification provisions, especially the destruction of evidence portion of it. I think that other portions, you know, a risk of physical injury and harm, those are very good. I would point out that 2705 was added in the immediate aftermath of 9/11 as a codification of a longstanding common law that had developed in the courts of appeals that had adopted these various rules for when they would delay notification.

So to some degree, you're arguing with something that preexisted 9/11, preexisted ECPA, preexisted—and destruction of evidence has traditionally been one of those possibilities. That may be something that should change. As for control of one's own personal data in the cloud, I think that there are many service providers who offer different degrees of control over your information. And so I generally tend to be comfortable with the idea that there's competition in the marketplace and that if that's something that matters to you, there are service providers who will promise that they take no interest and will not process, will not examine your data. They may be more costly in other ways than service providers who provide you. So I'm kind of a free-marketist on that one.

Mr. GOHMERT. Okay. Thank you very much.

Mr. COLLINS. The gentleman's time has expired. The Chair now recognizes the gentleman, Mr. Cicilline.

Mr. CICILLINE. Thank you, Mr. Chairman. And thank you to our witnesses for sharing your expertise and your diverse perspectives with us today. I believe that all of us assembled here, both those of us on the Committee and our assembled panel of witnesses, recognize that technology often evolves much faster than the law. This, in part, is a testament to the rapid pace of American innovation. But it also presents a gap that must be addressed. And the Email Privacy Act represents an important step forward to closing this gap and preserving privacy protections for Americans. And it's no surprise to me that it's broadly supported by the American people.

I want to begin with you, Mr. Ceresney. In your written testimony, you state if the bill becomes law without modification, the SEC and other civil law enforcement agencies would be denied the ability to obtain critical evidence from ISPs. This phrasing suggests to me that you are engaged in some activity today that would be blocked by this legislation.

And so, my first question is, does the SEC currently use subpoenas to obtain the content of communications from Internet service providers?

Mr. CERESNEY. We do not where we don't have consent of the providers.

Mr. CICILLINE. And why not?

Mr. CERESNEY. As I've said earlier, it's because in an excess of caution and in deference to the discussions that have been ongoing in Congress for a number of years about ECPA reform, we determined to hold off on using that. But it does not mean we do not believe we have the authority under the statute and that it is constitutional to use it.

Mr. CICILLINE. But you do not currently use it?

Mr. CERESNEY. We do not without consent of the subscribers.

Mr. CICILLINE. Your written testimony also acknowledges that the SEC "often conducts investigations in parallel with criminal authorities." If the FBI needs a warrant to obtain my email, but the SEC can obtain my email with something less than probable cause, what prevents the SEC from helping the government to avoid a warrant requirement by sharing my email contents with the FBI?

Mr. CERESNEY. So the first point is whatever standard Congress establishes we're willing to abide by, even if it's probably cause. But, second, when we issue subpoenas——

Mr. CICILLINE. Let me just, so if the standard is probable cause, then your objection is not with the standard, but who makes the determination of probable cause? Because a probable cause finding with a judicial determination is a warrant.

Mr. CERESNEY. No, what we're seeking is authority to achieve a court order with notice to the subscriber, which provides additional protections to a warrant. A warrant is ex parte, and the subscriber doesn't have an ability to object. What we're seeking is an authority to obtain an order from a court with notice to the subscriber. And the subscriber would have the ability to object and provide whatever objections they have, whether they be relevance, whether they be privilege, whatever other objections. That provides additional protections beyond those with the warrant, which is ex parte.

But to answer your question about the criminal authorities, any subpoena or other orders we'd seek would be in advance of our investigation. They would not be at the behest of criminal authorities. We do not issue subpoenas or otherwise seek evidence at the behest of the criminal authorities. We do it to advance our own investigation.

Mr. CICILLINE. Mr. Calabrese, did you want to try that?

Mr. CALABRESE. Yeah, I mean, I think the question that we haven't heard an answer to yet is probable cause of what. Probable cause of a crime in the criminal context is very clear. We know what crimes are. And they're interpreted very tightly. Violations of civil law are much broader. I mean, if I fill out my tax form incorrectly or I state that this was a business expense when maybe it was a vacation, you can say oh, I have probable cause to believe that by going through my emails, I'm going to find that he was on vacation, not on a business trip. So what we really are talking about, no matter what the standard is, it's a much broader access to Americans' content of their communications.

Mr. CICILLINE. And with respect to that, current law provides that the government must show probable cause to obtain the content in an email that has been stored by a provider for 180 days, but can use a lesser process for an email that has been stored for 181 days. Is there consensus that this 180-day rule is inconsistent with how we use emails today? Should it be eliminated? And in addition to that, Mr. Calabrese, in your written testimony you give a good list of the digital content we all store online, emails, text messages, photographs, music, passwords, calendars, and other forms of social networking.

Do these forms of media merit protection under the Fourth Amendment? And is current law adequate to protect any privacy interests in this information?

Mr. CALABRESE. Well, I certainly think that the court in *Warshak* believed that the Fourth Amendment should extend to all these types of contents of communication. My worry is that we don't know what the next new technology is going to look like. We don't know what the next way that we're going to keep our communications private and confidential is. And so we shouldn't be waiting. And ECPA doesn't have a suppression remedy. So these actual determinations don't come up that often. We shouldn't be waiting for 5 or 10 or 15 years for a court to find a strange case that allows them to say we have a reasonable expectation of privacy in communications. We all seem to agree that the content of communications should be protected by the warrant unless Congress says otherwise.

Mr. CICILLINE. Thank you. I yield back.

Mr. COLLINS. The gentleman's time has expired. The Chair recognizes the gentleman from Texas, Mr. Poe.

Mr. POE. I thank the Chairman. I thank all of you all for being here. As my friend Mr. Gohmert was, I used to be a criminal court judge in Texas for 22 years, felony cases, 20,000 cases or more. All that time, constantly I had law enforcement officers come to me with a request for me to sign a search warrant based upon their affidavits. And I signed a lot. And some I did not sign because of the basics of the Fourth Amendment.

The Fourth Amendment makes us different than every other country on Earth because of our history. It's uniquely United States history, goes back to the British who wanted general warrants to kick in doors of warehouses in Boston to see if the American colonists were storing demon rum they hadn't paid taxes on yet. To me, a general warrant is the same as a court order. So we have specific warrants. And like I said, I signed a lot of them.

It makes no sense to me that the right of privacy is protected for 6 months but it's not protected more than 6 months. I send a letter, snail mail. And I put that in an envelope. And I send it off to one of my grandkids somewhere. It floats around in America from post office to post office and who else knows where until it gets to grandson. It's protected. Generally it's protected. It's a form of communication.

When we use emails or store in the cloud, it's a form of communication wherever the cloud may be. So I think it's Congress' responsibility to determine what the expectation of privacy is. It's not, God bless them, Federal judges' responsibility. It's Congress' responsibility to say this is an expectation of privacy for Americans. And when we enter the digital age, I don't buy the argument, well, we're in the digital age, you got to give up some of your constitutional rights so we can have government investigate things.

Whether it's civil investigation, whether it's criminal investigation, I don't buy it. Because the Fourth Amendment gets in the way of that. I think it is one of the most important rights that we have. So it's our duty to set up a standard. Over 300 Members have signed on to Mr. Yoder's bill. It hasn't come up for a vote. Ms. Lofgren and I filed a similar bill in 2013. We want to get a vote on, I want to get a vote on Mr. Yoder's bill. Three hundred and four

Members of Congress agreeing on something? Really? And I think most Members, Republicans and Democrats, see the importance of the privacy.

Mr. Calabrese, let me start with you. I have a lot of questions. And I know I have only 5 minutes. The *Warshak* case, the SEC lost the *Warshak* case. They did not appeal that, did they?

Mr. CALABRESE. No, the case was not appealed.

Mr. POE. It was not appealed. The SEC, the way I get it, the SEC wants a carve-out for civil investigations. The way I see this legislation, it's to protect us from the SEC and the IRS and the EPA. Because without this legislation, they could keep doing what they're doing. Would you like to comment on that, weigh in on that? Civil agencies snooping around in email. And I'm using the word snoop, that's my word.

Mr. CALABRESE. We've already seen agency overreach. We saw it in this Tea Party investigation. There was no question there was improper investigation that was searching for a much broader category of information about people than anyone I think here is comfortable with. The idea of looking at what people are reading, looking at their donor lists as part of a civil investigation into someone's tax status is wrong. And it disturbs me that if someone can have a high—a relevant standard that is so low that we might bring those kind of investigations into play, I think that's a problem. And I think that that's why we need to limit this very powerful authority to warrants that are supervised by judges under probable cause.

Mr. CERESNEY. Judge, may I respond?

Mr. POE. Not yet. You can respond in writing because I have the same question for all six of you. The basis of a search warrant also requires there be notice. Under the current law, let's use the SEC or let's use the IRS, I like to use them better, they can do their investigation, their snooping, and the person being investigated doesn't know about it. Is that correct, Mr. Calabrese?

Mr. CALABRESE. It depends on the circumstances. Sometimes notice is delayed.

Mr. POE. Notice is delayed.

Mr. CALABRESE. Sometimes notice is delayed. Sometimes they do know about it.

Mr. POE. But would you agree that it's part of our fundamental fairness under the Fourth Amendment that there is a search warrant, the search warrant is executed, and that there is a return to the judge of what was seized or not seized, and, eventually, whoever's house was searched or property was searched, they get notice of the results of the search warrant?

Mr. CALABRESE. This is one of the most——

Mr. COLLINS. The gentleman's time has expired. But the witness can answer.

Mr. CALABRESE. This is one of the most invasive things that the U.S. Government or any government can do to its citizens, it can investigate them, make them the subject of law enforcement scrutiny. So, yes, absent some compelling reason not to notify them, I think they absolutely deserve to know that they are the subject of government scrutiny.

Mr. POE. I ask unanimous consent to submit questions for the record, Mr. Chairman.

Mr. COLLINS. You have unanimous consent to submit as many as you like, Judge.

Mr. POE. And we should get the southern rule. If we're from the south, we should be able to talk longer than just 5 minutes.

Mr. COLLINS. Well, we just are better expressing ourselves in our eloquence and slow southern execution.

Mr. POE. Thank you, Mr. Chairman.

Mr. COLLINS. With that, the Chair recognizes the gentlelady from Texas, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. I thank you so very much, Mr. Chairman. And I thank the witnesses. I want to engage in a give and take with Mr. Calabrese, Mr. Salgado, and Mr. Rosenzweig if I might. But let me just ask a pointed question to Mr. Cook. Let me thank all of you for your service. And acknowledge that the *Warshak* case, Mr. Ceresney, I will not attribute your win or loss, I will just take the case as a Sixth Circuit case.

I just want to ask, since that case, the *Warshak* case, Mr. Cook, do you know whether or not the Department of Justice has used anything less than a warrant based on probable cause to compel a third-party provider to produce the contents of a communications? You all adhere to that?

Mr. COOK. Yes.

Ms. JACKSON LEE. All right. That's good. Let me move on then.

Mr. COOK. That was easy. Thank you.

Ms. JACKSON LEE. Thank you. To say that I come to this with a sense of trust of government not to sense that government is unworthy and consistently trying to undermine its citizens. But I am an adherent to the Fourth Amendment and its value and its value with the Founding Fathers. So let me engage the three of you. One, I'm going to go to you, Mr. Rosenzweig, to make it clear that issues dealing with terrorism and any elements thereof are specifically, pointedly, and appropriately excluded under this legislation. Are you comfortable with that?

Mr. ROSENZWEIG. Very much so. Indeed, that's part of the ground for at least my personal view that this legislation is appropriate. Given the post-9/11 changes that have empowered our national security apparatus to protect us in ways that I think are appropriate, it's important to exclude from the coverage of this bill those issues. And I think that's something we can agree on. And the construction provision that is in section 6, I guess it is, of the bill is perfectly appropriate to that end.

Ms. JACKSON LEE. I think it is important to make note of that. I'm on Homeland Security as well. America is obviously on alert. But we've always said since 9/11 that we would not allow fear to instruct and guide our interpretation of the Constitution. I want to go to Mr. Salgado.

Mr. Calabrese, there was a law professor at Yale Law School with the same name. Do you have any——

Mr. CALABRESE. Sadly, I don't.

Ms. JACKSON LEE. I had his class. So you'll be favored by your very name. But let me engage both of you in the question of the value and the sanctity of the Fourth Amendment and whether or

not in this interpretation of this bill, which I understand so many of us are on the bill, but 100,000 petitions were sent to the White House to support it, whether it is obstructionist in terms of preventing law enforcement from doing their job. Can you all just engage? Maybe Mr. Calabrese will start and Mr. Salgado will finish.

Mr. CALABRESE. Sure. I don't believe that it is obstructionist. You know, we're codifying what amounts to existing practice and existing protections under the Fourth Amendment. We're also saying that you should have notice when someone does a search of your most private electronic home. And to be clear, unlike a physical warrant where you get that notice immediately, we're actually delaying notice for 10 days here so that law enforcement has got a head start.

Ms. JACKSON LEE. Absolutely.

Mr. CALABRESE. And then we're allowing a gag provision which says that you, in important circumstances, you'll never get that notice. I think these are all pretty basic protections for anyone. And, honestly, if there are issues around the edges, I'm not sure that there are, but if there are, I think that's why we have markups, so that we can bring these issues forward, we can take votes on whether there's anything here that we should be concerned about, and then we can get this bill to the floor.

Ms. JACKSON LEE. Thank you. Mr. Salgado, let me say that I too served as a judge and did a lot of PC warrants for police officers. And I think this should be a comfort. I had a responsibility to the police officer but also to the citizens, to be able to inquire what the basis of this warrant was. And that layer was placed in my hands.

I think the American people place their protection in our collective hands. What do you think? What is your perspective on that? And maybe, Mr. Ceresney, you might want to answer that you are not hindered by the present Sixth Circuit interpretation. But go ahead, Mr. Salgado.

Mr. SALGADO. Yeah, I agree with that completely. The role of the neutral and detached magistrate in American jurisprudence is a significant one. It's something that really sets America apart from a lot of countries, and gives us a layer of protection to make sure that well-meaning but perhaps poor judgment in some cases is overridden by the cooler judgment of a magistrate who doesn't have a particular interest in a case. It's significant for Fourth Amendment, it's no accident that that is the standard for valid warrants.

Ms. JACKSON LEE. Quickly. Thank you. Mr. Ceresney, do you want to comment on that as Mr. Yoder sits in the room on pins and needles wondering how we're going to treat his bill?

Mr. COLLINS. The gentlelady's time has expired. But the gentleman can answer.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Mr. CERESNEY. I couldn't agree more that it is important to have a role for a judge in this situation to provide objective views on the matter. And that's why the order that we are proposing would be before a judge with notice to the subscriber. And the subscriber would be able to bring before that judge whatever objections they have to our seeking the email.

And that is actually the remedy that we are seeking in this case. We would try to obtain that email from the subscriber. If we

couldn't, then we would go before a judge and try to obtain the order. And the judge would be the objective factfinder to determine whether we've met the standard.

Ms. JACKSON LEE. Mr. Chairman, I like this bill. But I'm willing to listen to the gentlemen. But I like our bill before us. And I look forward to it going to markup. I yield back.

Mr. COLLINS. Thank you. The gentlelady's time has expired. The Chair now recognizes the gentleman from Pennsylvania, Mr. Marino.

Mr. MARINO. Thank you, Chairman. Good afternoon, gentlemen. My question here is going to be directed to Mr. Rosenzweig and Mr. Salgado in that order. Please speak to the trends of users moving to encrypted services, often hosted overseas in order to seek privacy, and how this might make us less safe than if we had a clear framework in place. Do you understand my question?

Mr. ROSENZWEIG. I do understand your question. I think to begin the answer, obviously, the encryption discussion is slightly different than the one we're having now about the lawful access to content. What I would say about the encryption discussion is that it is essentially a reflection of the exact same impulse, which is that people are seeing increasingly the lack of privacy in their personal effects and papers in their—I like the idea of a digital home, their electronic home. And to the extent that this Congress does not take steps to protect that privacy by law, encryption is essentially citizens engaging in self help and protecting themselves with their own capabilities.

I would say that, from my perspective, encryption is an idea. It's a mathematical proof. It's not suppressible. So if we do not regularize access through things like the proposal before you that will provide comfort to citizens, they're going to engage even more, I think, in self help.

Mr. MARINO. Thank you. Mr. Salgado?

Mr. SALGADO. I agree completely with that statement. And I think to the point in your question about the movement of users to services overseas, I think that's a natural consequence of the misimpression that U.S. Government has such easy access to the data providers. And it's not true. And this bill will help make it clear. And it will help prevent the fleeing of users to other services based on this misperception.

Mr. MARINO. Thank you. Mr. Cook and Mr. Littlehale, I have 18 years of law enforcement behind me, prosecution, State and Federal level. And as far as I'm concerned, what I've seen here since I've been in Congress, and this is only my third term, the less Federal Government in my life, the better.

Basically what NSA has done, what the IRS, and there are many more that we could get into, the overreaching and what I think is criminality that has taken place in these agencies. But being a law enforcement guy, and I've prosecuted many child abuse cases and pornography cases, if the two of you can quickly tell me what the obstacle is to you and how we can fix that. Because I know in some investigations that I had, I didn't want the person who was looking at and transferring and uploading and downloading child pornography to know at this point of my investigation that he was the target or she was the target. Could you please respond?

Mr. COOK. Yes, sir. And I'm concerned that we've lost sight of that issue and the exigent or emergency aid exception issue, so if I could just begin with that. The concern that we have is many of these investigations, whether it's child pornography or any other type of investigation, many fraud investigations involve dozens, sometimes hundreds or thousands sometimes in child pornography cases of targets. For us to get the content and then have to let the target of the investigation know is a new discovery requirement that puts the targets, whether it's terrorism or otherwise, on notice that we're looking at them. It's unprecedented, I've said that, unprecedented in our law.

Mr. MARINO. What is the change that we can make? And Mr. Littlehale, you go, and then collectively tell me what the changes are that you would like to see.

Mr. LITTLEHALE. Thank you, Congressman. If all we were interested in is extending and leveling the playing field for the 180-day rule and content, this bill would be a page long. The notice provisions that you're talking about, along with the additional protections that the bill provides, are one of the great reasons that we're concerned about it. While I certainly think that we would like to have a conversation, I think those are a little bit more than issues around the edges.

I mean, the body of our concern about the bill is that when we get a warrant, we want it to mean something. That's true on the earlier point with respect to encryption. You know, if I serve a search warrant on somebody, I want to have access to that evidence. And in many instances now, I don't. Well, I want to find that evidence in other places. And if it's denied to me because of delays or because of burdensome notice provisions, those slow me down. They make me less effective as an investigator. And I believe that this Committee should undertake a robust review of what this bill is going to do to the——

Mr. MARINO. My time has run out. Would the two of you please put in writing and get it to me what you think could be a remedy for this, and anyone else who wants to address that as well.

Listen, I am just as much a Fourth Amendment advocate as I am putting these people behind bars. And I wish I—no one should have to look at the photos of the kids that I've looked at and you've seen over the years and question as to why we need to have some delay before letting that person know that they're going to be arrested. I yield back. Thank you.

Mr. COLLINS. The gentleman's time has expired. The Chair now recognizes the gentleman from New York, Mr. Jeffries.

Mr. JEFFRIES. I thank the distinguished Chair. And I thank the witnesses for your presence here today.

I want to follow up on that discussion from my good friend from the great State of—the Commonwealth of Pennsylvania. Mr. Cook, I know you've expressed concerns as it relates to the notice requirement. And I think in your testimony you refer to the provisions as a red alert tool that could notify an individual that he or she is under investigation. Is that right?

Mr. COOK. That is correct.

Mr. JEFFRIES. And if you could just kind of walk me through a series of responses as it relates to the particular concern that

you've got with the notice provision. Because it's my understanding that section 4 permits up to 10 days of delayed notice. Is that right?

Mr. COOK. That's correct.

Mr. JEFFRIES. And is it your view that the 10 days is inadequate?

Mr. COOK. So I think it's important for me to point out that in our discussions already, we have drawn parallels with the Fourth Amendment as it applies in other contexts. And everybody seems in agreement that that's the goal, is to make the bill parallel Fourth Amendment protections.

But this bill does more than that. And here's why. For example, if you have terrorists working out of an apartment, a third-party's apartment, and there is evidence in that apartment, we get a search warrant, search that apartment, there's no obligation for us to tell the terrorists that we've gotten evidence out of that apartment that can be used against them.

Mr. JEFFRIES. Right. But this bill doesn't necessarily impose that obligation. It's a default provision, but there are steps that the government can take under exigent circumstances. I wouldn't think that it would be sound public policy to create a law that simply applies in the instance of the terrorist context where this is a country of 300-plus million people that values their privacy rights, so there has got to be an appropriate balance between the legitimate ability of law enforcement to help keep us safe and to prosecute wrongdoers to the full extent of the law, and the civil rights and civil liberties of American citizens. Is that correct?

Mr. COOK. As an email user, I could not agree more, but I think that the Fourth Amendment has already reached that balance because in the analogy that I've given you, when we search that third-party's home or service provider, that homeowner or service provider is within their rights to contact whomever they want to notify them.

There has never been an obligation for the government to figure out who the evidence is going to be used against and to notify them. That's why I say this is unique in the law, and I've never seen it before.

Mr. JEFFRIES. Now, as it relates to sort of the 10 days delay, if the government concludes that additional delay is warranted, this bill, correct, provides for a court to make that determination that the notice can be delayed indefinitely. Is that right?

Mr. COOK. Not indefinitely. There's a 180-day limitation, and then there's a recurring obligation to reach back to the court.

Mr. JEFFRIES. Right, but after that 180-day period expires, the government can go back to the court and request another 180-day delay. Is that correct?

Mr. COOK. That is correct. There are narrow limitations on it. For example, one of the limitations is that if we can show that there would be harm to another individual, but there are many times when the harm could be to a community rather than an individual, and I wish I could report to you that all judges are reasonable and will always, in the right circumstances, limit that new constant—or this new statutory notice rule, but the truth is that that just isn't how it works, and expanding these obligations on the government will come with great risk in serious cases.

Mr. JEFFRIES. But there are times that an Article III judge can reasonably, or a magistrate that's not an Article III judge, but an Article III judge or magistrate could reasonably disagree with the government as it relates to privacy protections and potential overreach. Is that correct?

Mr. COOK. Of course. Of course it is, and there are times when that will—that this agreement will result in notification to—under this newly created rule, to targets of criminal investigations and alert them to allow them to flee or otherwise destroy evidence or otherwise engage in bad behavior.

Mr. JEFFRIES. Mr. Calabrese, could you speak to the adequacy of this notice requirement in your view?

Mr. CALABRESE. I believe it's a very strong notice requirement and constitutionally appropriate with a very strong delay procedure. One of the things I'm struggling with a little bit is, we're talking about a circumstance where I am going before the judge and getting a search warrant. At that same time, I may get a delay of that search warrant, so we're not talking about some kind of separate process where I've got to go through an additional burden.

When I get the warrant, I can also make the case that I must delay notice. That can happen for 180 days. Before a provider or anyone else, you know, notifies the subject, they have to tell the government that they are going to do that, giving the government an ability to go back to the court and say, you know what, the reasons for our delay have not ended and we need to expand it. I mean, I think it's a very reasonable, very balanced approach that supports a fundamental constitutional value, one of notice that's embedded in the Fourth Amendment.

Mr. JEFFRIES. Thank you. I yield back.

Mr. COLLINS. The gentleman's time has expired. At this time, the Chair recognizes the gentleman from Texas, Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Mr. Chairman. As a former U.S. attorney, I always appreciate and listen to concerns expressed by law enforcement whenever Congress proposes changes to a law that may impact your ability to do your job because you're the folks that are working so hard to keep us safe, and I want to certainly make sure you have the tools and resources and capability necessary to do that effectively.

That being said, I also strongly believe that in an increasingly connected, complex, digital society, our laws have to be modernized to make sure they reflect the current technological landscape. As our technology is evolving, this extremely personal information is being stored on our computers, on our smartphones, on our Fitbits, where we travel, what we eat, what we read, where we shop, who we communicate with, all highly personal information, and so we've got to make sure we've got robust protections in place for that.

I certainly don't believe that the Fourth Amendment protections that we all hold so dear and the needs of law enforcement are mutually exclusive. And I appreciate all the witnesses being here today to have a thoughtful discussion about that.

Mr. Ceresney, I want to start with you because, from my perspective, it seems like that the SEC has been the most vocal civilian agency in expressing concerns about modifying ECPA, but the SEC doesn't appear to have served a subpoena on a commercial provider

in 5 years since the *Warshak* decision. And despite that, the SEC's annual report last year, 2014, touted a record year, cutting edge enforcement actions, more cases than ever before, a number of first ever cases that span the securities industry.

And I know that Chairman White has testified that the SEC isn't issuing subpoenas to third-party service providers for content. So given the record number of cases, enforcement actions, and first ever cases brought by the SEC, all done without encroaching on Fourth Amendment rights of Americans, why is the SEC asking Congress to give it the authority to get content on something less than a warrant?

Mr. CERESNEY. Well, we certainly have been successful, we think, in enforcing the securities laws, but that does not mean that there aren't cases that we would benefit tremendously from emails that we would be able to obtain from ISPs. And I guess the point that I would assert is that the Fourth Amendment is not violated by what we are proposing, which would be an order before a judge, which a judge could issue, with notice to the subscriber after the subscriber has the opportunity to raise whatever objections they have under a standard that Congress would establish. And from our perspective, that does comply with the Fourth Amendment, and it also balances privacy protections because you would have an objective factfinder reviewing the situation and determining whether it's appropriate for us to obtain emails in that circumstance.

And I can tell you that there are ongoing investigations now, which we have refrained from seeking those emails from ISPs, which would definitely benefit from such emails.

Mr. RATCLIFFE. When you say what you are proposing, I mean, how have you been proposing it?

Mr. CERESNEY. We've had ongoing discussions with Members of Congress about these issues for the last couple of years.

Mr. RATCLIFFE. Okay. Well, because, you know, from my perspective, it seems like you've been altering your behavior for the last few years in response to this opinion rather than coming to a committee of jurisdiction, at least from my perspective. I know that when FBI has a problem, they come and let us know what it is and how we can fix it.

Mr. CERESNEY. We've been having ongoing discussions with the staff of both Judiciary Senate and House Judiciary throughout this period, certainly since I've been at the SEC, which is over——

Mr. RATCLIFFE. That's fair enough. Thanks for that.

Mr. Salgado, in your testimony, paraphrasing here a little bit, but essentially you seem to be saying that H.R. 699 is really just a codification of the status quo under *Warshak*. Is that right?

Mr. SALGADO. That's accurate, yes.

Mr. RATCLIFFE. Okay. You don't think that H.R. 699 goes beyond the holding in *Warshak*?

Mr. SALGADO. I don't think it does. I'm happy to hear suggestions, but my review of *Warshak* and the bill suggests that they're very consistent.

Mr. RATCLIFFE. Mr. Calabrese, you agree with that?

Mr. CALABRESE. I do.

Mr. RATCLIFFE. Mr. Rosenzweig.

Mr. ROSENZWEIG. I think I do. I haven't done—I haven't checked precisely, though.

Mr. RATCLIFFE. Okay. I'm going to yield. My time is about to expire, so I'm going to yield back the balance of my time. Thank you all for being here.

Mr. COLLINS. The gentleman yields back. Now the Chair recognizes himself for questions.

Mr. Salgado, there has been an issue, and we brought this up here in this emergency issue of provisions, emergency disclosure mechanisms, and Mr. Littlehale, actually, in his written testimony, that the primary emergency disclosure mechanism currently in law are voluntary. He also mentions that companies are often—and this is his words—unable or unwilling to respond to law enforcement's lawful demands in a timely manner.

Now, I think we all would agree true emergencies are there, and as a son of a Georgia State trooper, there's not going to be anybody that would deny the need from a law enforcement perspective. However, it seems to be implying that there's something missing here. So we did a little bit of research in our office and with others, and based on the concerns we saw, that publishing Google's transparency report, based on that report, which we have looked at, it says Google received 171 emergency disclosure requests and provided at least some data in response to 80 percent of emergency disclosure requests.

One, I think, for most people to understand it, we've looked into it, but I'd like to hear your answer. To better understand that, can you explain why Google responded to only 80 percent of these requests, break down those numbers for us, and why couldn't the response rate be 100 percent, given what has been heard from Mr. Littlehale here.

Mr. SALGADO. Sure. I'd be happy to. I think the statistic you're referring to is in our transparency report.

Mr. COLLINS. Yes.

Mr. SALGADO. We've been publishing that number for a while here so that policymakers and others can get an idea of what this work is like. The number is actually relatively low, 171 compared to the type of legal process we get.

The 80 percent represents lots of different situations where the emergency doesn't justify the disclosure. Often, the case is that the identifier that's given to us in the emergency request doesn't actually go back to any real account. So there are some services out there where you can create an account using a Google or any email address, and it's not verified that there is such an address. They may use that account to threaten a school shooting or engage in other some violent activity.

The authorities quite legitimately will come to Google and ask us for information about this account that was used to create the account that made the threat. We look in our system, and there is no such account, so the response back is we have no data to produce in response to this otherwise legitimate emergency request. That gets counted as a nondisclosure, and that adds into the 20 percent where there was not a disclosure. There was no responsive data.

That's probably the most common situation in that 20 percent. There may be other situations where the request is coming in and the emergency is over, that the investigation is now actually about a historical crime, there is no ongoing threat of loss of life or serious physical injury, which means it's inappropriate to be using that authority to get the information.

And we are able to, at that point, say this doesn't look like an ongoing emergency, we can preserve the information, and when you come back to us with the legal process, we can promptly disclose.

Mr. COLLINS. Okay. And just real quickly, but you went on with your answer long enough to bring up a question. Are you making that determination if the emergency situation is still ongoing?

Mr. SALGADO. That's right. The statute——

Mr. COLLINS. Not the law enforcement agency offering?

Mr. SALGADO. The statute says that we are allowed to disclose if we have a good faith belief that there's an emergency.

Mr. COLLINS. Okay. Mr. Littlehale, when you testified before House Judiciary Committee in 2013 about the emergency disclosure issue, you said that some providers make a decision never to provide records in the absence of legal process, no matter the circumstance.

Can you identify the service providers that have a policy of categorically rejecting emergency requests in the absence of compulsory legal process? If not, why?

Mr. LITTLEHALE. Congressman, as I stated in response to the question at the time, I have made the decision not to identify, in the examples that I give, specific providers because I don't want to highlight a vulnerability in a public forum. There may come a time when we do have to disclose that.

Mr. COLLINS. Well, I tell you what. I would like to request you can submit that in a nonpublic forum, but I'm really concerned here that we're making a categorical statement without categorical proof.

Mr. LITTLEHALE. Well, I can certainly say anecdotally that the agents——

Mr. COLLINS. No, I want to know—you made a direct statement.

Mr. LITTLEHALE [continuing]. That I work with have been told that by providers.

Mr. COLLINS. Mr. Littlehale, you made a direct statement. It wasn't anecdotally. I didn't start off by saying, "Anecdotally, providers make a decision never." You said in your testimony, providers make a decision never to provide records in the absence of legal process, no matter the circumstance, and that's a very direct statement against the business practices of Internet providers.

Is it true? Is it not true? Do you have evidence? Or do you not have evidence?

Mr. LITTLEHALE. I have been told that by providers, yes.

Mr. COLLINS. But you don't have evidence. You made a statement that is not grounded, except anything and anecdotally.

Mr. LITTLEHALE. Well, I'd say I would suggest that I do have evidence. I have been told that by providers.

Mr. COLLINS. Well, I was told that there was a Santa Claus, but I found out real quickly there wasn't. I mean, I'm trying to figure out——

Mr. LITTLEHALE. Congressman, I would suggest that that's evidence. If you choose not to believe me, then I suppose I can't help you with that, but I have been told and agents that work for me have been told that in some cases.

Mr. COLLINS. I'll just let that one sit.

Mr. Ceresney, during an exchange with Senator Leahy in a Senate hearing on this topic, you said that with regard to phone calls, you're not seeking authority, the criminal—authority that criminal authorities have that civil agencies do not, but in seeking to get access to emails without a warrant, you're essentially seeking something more than the authority, the criminal authorities have. Isn't that contradictory?

Mr. CERESNEY. I don't think we're seeking more authority than the criminal authorities have.

Mr. COLLINS. So what are you seeking?

Mr. CERESNEY. I'm sorry?

Mr. COLLINS. Then what are you seeking? I'll give you a chance to clarify that.

Mr. CERESNEY. Sure. What we're seeking is the ability to obtain emails after we try to obtain them from an individual subscriber by going to a court and obtaining a court order with notice to the subscriber and allowing the subscriber to raise whatever objections they have before the court.

Mr. COLLINS. Well, I think it's—and like I said, it's interesting that some of the testimony that's been given here, and I think, you know, it's very concerning from some issues of anecdotal evidence and real evidence and discussion, especially on the SEC side, when you're, you know, giving the—you know, your own report saying you're doing more than you've ever done here, yet without this, by choice or decision, however you're wanting to do it.

Mr. Calabrese, one last question for you, as my time is now over. But in dissent from the FTC request of civil agency carve out, FTC Commissioner Brill wrote, "I am not convinced that this authority is necessary to maintain the commission's effectiveness as a law enforcement agency now or in cases that we can presently foresee. On the other hand, I am concerned that the judicial mechanism for civil law enforcement agencies to obtain content from ECPA providers could entrench authority that have potential to lead invasions of individual privacy, and under some circumstances, may be unconstitutional in practice."

Could you speak very briefly. Do you agree or disagree with his concern?

Mr. CALABRESE. I do worry that we will create an unconstitutional or incredibly reckless carve out for civil agencies. And my hope is that we continue to push H.R. 699 forward as is to a markup and we can vote and get it to the floor. Thank you.

Mr. COLLINS. Well, I appreciate it. In looking around and seeing how it's just me and the distinguished Ranking Member, this concludes today's hearing. I'd like to thank all the witnesses for attending. Without objection, all Members have 5 legislative days to submit additional written questions for the witnesses or additional materials for the record.

And with that, this hearing is adjourned.

[Whereupon, at 12:28 p.m., the Committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Doug Collins, a Representative in Congress from the State of Georgia, and Member, Committee on the Judiciary

Mr. Chairman, thank you for holding today's hearing on H.R. 699, the Email Privacy Act. I appreciate the chance to discuss this important legislation and hear from the witnesses. I hope that today's hearing is just the first step towards Committee mark-up and consideration of H.R. 699.

H.R. 699 was introduced by my friend from Kansas, Rep. Kevin Yoder. I am a cosponsor and strong supporter of the Email Privacy Act. If enacted, the bill would update the Electronic Communications Privacy Act to better reflect advances in technology and to ensure that Americans' electronic communications are protected from unwarranted government intrusion.

As of today this legislation has 305 cosponsors, earning it the distinction of being the most supported piece of legislation in the House that has not yet received consideration on the House Floor. Twenty-eight of these cosponsors serve on the House Judiciary Committee. The majority of each party has cosponsored the legislation. It is not often that you see this type of overwhelming bipartisan support for legislation, but the numbers speak for themselves that this issue is one that deserves and demands consideration.

I understand that certain Members may have concerns with specific provisions of the legislation. While I support the legislation in its current form, I think the best way to address these concerns is through a markup of the legislation, where amendments can be discussed and democratically considered. No one is served by this legislation languishing in legislative limbo.

Law enforcement needs clarity. Internet service providers need laws that accurately reflect their technological advances. And most importantly, the American people need and deserve privacy protections guaranteed to them by the Fourth Amendment of the United States Constitution.

It is past time that our digital privacy laws were updated to reflect today's technology and communications climate. The Electronic Communications Privacy Act (ECPA) was written in 1986, and intended to balance the interests of preserving citizens' privacy rights while protecting legitimate law enforcement needs. While the principles behind the law are still critically important and it remains a hallmark of privacy protections for communications, in practice many parts of the law simply have not kept up with the world as it is today. ECPA—and in particular the Stored Communications Act (SCA) provision of the law—must be amended to reflect the realities of the digital era in which we live.

The Email Privacy Act takes critical steps to update ECPA so that Americans' Fourth Amendment rights are better protected and so that citizens' can communicate on the internet free from unwarranted government snooping.

The bill eliminates the outdated "180 day" standard from current law. Current law under ECPA does not require law enforcement to obtain a warrant to access the content of emails or other forms of online communication—such as documents stored on a cloud service—if they are more than 180 days old. For messages over

180 days old, only a subpoena—rather than a warrant—is required for access. While this distinction may have made sense when storage space on personal computers was extremely limited and emails were still a fledging and rarely used form of communication, it certainly does make sense today. Americans deserve the same strong Fourth Amendment protections whether their emails are a day old or several months old. The Email Privacy Act addresses this issue by instituting a requirement that law enforcement obtains a search warrant before accessing the content of Americans' private emails and online communications.

H.R. 699 would essentially codify a decision issued by the Sixth Circuit Court of Appeals in 2010 in *United States v. Warshak* while clarifying additional privacy protections. In *Warshak* the Court held that the government's accessing of 27,000 emails directly from a suspect's internet service provider (ISP) with a subpoena and an ex parte order was unlawful under the Fourth Amendment. Specifically, the Sixth Circuit said that subscribers have "a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'" and "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." [1]

In light of *Warshak* and the Email Privacy Act, the Securities and Exchange Commission (SEC) and other civil agencies have sought exemptions from the warrant requirement, arguing instead that it should be allowed to retain subpoena powers. The SEC maintains that subpoena authority is critical for their investigations, but that statement has been called in question by SEC Chair Mary Jo White's admission that the SEC has not used subpoena authority post-*Warshak*.

The Federal Trade Commission (FTC) has made similar claims that it should be subject to a warrant exemption when seeking content from ISPs. However, Commissioner Brill went so far as to file a dissent to the FTC's request for a carve out. Commissioner Brill stated, "I am not convinced that this authority is necessary to maintain the Commission's effectiveness as a law enforcement agency now or in cases that we can presently foresee. On the other hand, I am concerned that a judicial mechanism for civil law enforcement agencies to obtain content from ECPA providers could entrench authority that have the potential to lead to invasions of individuals' privacy and, under some circumstances, maybe unconstitutional in practice."

I share Commissioner Brill's concerns. Absent much more compelling evidence from civil investigative agencies, I do not believe that these agencies should be allowed to pry into Americans' personal lives based solely on subpoena authority. This kind of change could fundamentally harm the important steps taken in H.R. 699 to better protect Americans' rights to have their online communications protected.

Let me make clear that I believe it is critical law enforcement has the tools they need to prevent and fight crime. My father was a Georgia State Trooper, so I was instilled with respect and admiration for our men and women in uniform from a young age. I believe that in true emergencies, law enforcement needs to be able to access information quickly. I believe there are potentially legitimate reasons that law enforcement would seek the content of an individual's online communication. However, I do not believe that we should create so many carve-outs and exceptions to the law that the purpose of the legislation is lost. We must carefully balance the needs of law enforcement with the rights of Americans.

The Email Privacy Act updates ECPA to restore that balance and bring our privacy laws into today's world. I look forward to hearing from our witnesses, and I hope that today is a step closer towards passage of H.R. 699.

Thank you Mr. Chairman, I yield back.

---

[1] *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010).

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary

Thank you, Mr. Chairman. Let me extend my thanks to you and Ranking Member Conyers for working together in a spirit of bipartisanship to convene this important hearing on H.R. 699, the "Email Privacy Act."

The Fourth Amendment to the United States Constitution states:

- *"The 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, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

The Fourth Amendment originally enforced the notion that "each man's home is his castle", secure from unreasonable searches and seizures of property by the government.

The authors of the Constitution had good cause to work to establish protections against government overreach, which they themselves experienced.

In our history we can understand the seriousness with which the Founding Fathers viewed government authority to search private citizens' correspondence or communications.

The British authorities used writs of assistance, a form of general warrant, which permitted house-to-house searches.

These orders generally failed to allege any illegal activity and were not approved by a judge.

John Adams credited these practices as being "the spark in which originated the American Revolution."

As a direct result the founders of this nation drafted the Fourth Amendment to the Constitution of the United States.

However, beginning with the 1967, Supreme Court decision in *Katz v. United States* (establishing the "reasonable expectation of privacy" test) held that what a person knowingly exposes to the public, even in a home or office, is not subject to Fourth Amendment protection.

This holding began the move to establish what has become known as the Third Party Doctrine—such that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed to him by Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third part will not be betrayed.

The Third Party Doctrine was expanded in two key Supreme Court decisions in mid- to late 1970s: *U.S. v. Miller,* 425 U.S. 435 (1976) (holding that one does not have a constitutionally protected privacy interest in personal records held by a bank), and *Smith v. Maryland,* 442 U.S. 735 (1979) (holding that the installation and use of the pen register was not a "search" and thus no warrant was required).

These integral cases came before the Internet and long before the use of Cloud based computing services, but their impact are still felt today.

The Modern Communication Age

In possibly the first survey of its kind, in 1983, the polling firm Louis Harris & Associates asked U.S. adults if they had a personal computer at home and, if so, if they used it to transmit information over telephone lines.

Just 10% of adults surveyed said they had a home computer and, of those, 14% said they used a modem to send and receive information.

The resulting estimate was that 1.4% of U.S. adults used the internet in 1983.

In 2014, the Pew Center for American life found that eight in ten U.S. adults (81%) say they use laptop and desktop computers.

Further, 90% of adults in the United States own a smartphone, providing them with instant access to email services.

While the 1986 enactment of the Electronic Communications Privacy Act (ECPA) (which sought to govern how law enforcement agencies and private parties may access electronic communications, was meant to be forward looking as technologies began to rapidly advance), and various lower court decisions such as the 2010 Sixth Circuit case *U.S. v. Warshak,* 631 F.3d 266 (6th Cir. 2010), (which held that subscribers have a reasonable expectation of privacy in the content of electronic communications and that the government must obtain a warrant to access email stored by a third party), have attempted to clarify and govern electronic storage on third party servers, constitutional and legislative privacy safeguards for electronic communica-

tions and other forms of developing digital media are wholly inadequate for modern times.

The advent of Cloud Commuting services has only further broadened the question of third parties and communications due to the storage of not only emails, but digital photos, video, audio, electronic books, music preferences, political views, religious beliefs or the lack thereof.

Smart devices in use by tens of millions of Americans allow for the collection, and retention of much more information—and that retention is outside of the control of the email user.

The use of email as a primary means of communication is not limited to individuals, but obviously extends to businesses.

The number of worldwide email accounts continues to grow from over 4.1 billion accounts in 2014 to over 5.2 billion accounts by the end of 2018.

The total number of worldwide email users, including both business and consumer users, is also increasing from over 2.5 billion in 2014 to over 2.8 billion in 2018.

Email remains the most pervasive form of communication in the business world, while other technologies such as social networking, instant messaging (IM), mobile IM, and others are also taking hold, email remains the most ubiquitous form of business communication.

H.R. 699 a Step in the Right Direction

H.R. 699, The Email Privacy Act will amend the 29-year-old Electronic Communications Privacy Act to prevent the government from accessing private electronic communications without a warrant.

Specifically, the Email Privacy Act will prohibit a provider of remote computing service or electronic communication service (including email communications) to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions.

H.R. 699 will revise provisions under which the government may require a provider to disclose the contents of such communications.

The bill further clarifies the Electronic Communication Privacy Act of 1986 by eliminating the different requirements applicable under current law such how communications would be treated if they are:

o stored for fewer than, or more than, 180 days by an electronic communication service; or

o held by an electronic communication service as opposed to a remote computing service.

Importantly, this bill requires the government to obtain a warrant from a court before requiring providers to disclose the content of such communications regardless of how long the communication has been held in electronic storage by an electronic communication service, or whether the information is sought from an electronic communication service or a remote computing service.

FBI Director Comey, has testified that the current practice of the FBI is to obtain a warrant for e-mail communications, and that this bill would not change their current practices.

Moreover, this bill would not change any of the existing exceptions in the Electronic Communication Privacy Act that allow emergency requests for assistance to be processed in a timely manner.

The bill does require a law enforcement agency, within 10 days after receiving the contents of a customer's communication, or a governmental entity, within 3 days, to provide a customer whose communications were disclosed by the provider a copy of the warrant and a notice that such information was requested by, and supplied to, the government entity.

It further allows the government to request delays of such notifications.

H.R. 699 is an important measure that directs the Comptroller General to report to Congress regarding disclosures of customer communications and records under provisions: (1) as in effect before the enactment of this Act, and (2) as amended by this Act.

The Constitution of the United States is alive and well in the 21st Century, and this bill through overwhelming bipartisan support is making strides to make sure that citizens are secure in their digital records and effects.

Again, thank you for holding this important hearing and I look forward to the testimony of our distinguished panel of witnesses.

Thank you. I yield back the remainder of my time.

Hearing: H.R. 699, THE "EMAIL PRIVACY ACT"

2141 Rayburn House Office Building

Dec 01 2015

10:00AM

Full Committee

By Direction of the Chairman

Testimony of Congressman Kevin Yoder (KS-03)

Chairman Goodlatte, Ranking Member Conyers, and distinguished members of the House Judiciary Committee, I thank you for the opportunity to testify today speaking on behalf of my bill, H.R. 699, the Email Privacy Act. I would especially like to thank the majority of members of this committee who are cosponsors of this legislation: Reps. Sensenbrenner, Smith, Chabot, Franks, Jordan, Poe, Chaffetz, Marino, Gowdy, Labrador, Farenthold, Collins, Walters, Ratcliffe, Bishop, Nadler, Jackson Lee, Cohen, Johnson, Chu, Deutch, Gutierrez, Bass, Richmond, DelBene, Jeffries, and Cicilline.

This legislation is one of the most broadly bipartisan bills of the 114th Congress, unifying a supermajority of the House of Representatives spanning the entire political spectrum. More than 300 Members of Congress from both parties agree that H.R. 699 should become law to ensure that Americans' privacy rights are protected and American technology companies remain at the forefront of innovation throughout the world. Furthermore, a broad bipartisan coalition of advocates, companies, and our constituents support this legislation.

As many of you know, digital privacy reform was recently the topic of a Senate Judiciary Committee hearing, where my bill's companion legislation has been offered by Senator Mike Lee and Ranking Member Patrick Leahy. I commend the two Senate lead sponsors, as well as Judiciary Committee Chairman Chuck Grassley for his work to advance this legislation in the Senate.

The Electronic Communications Privacy Act, or ECPA as its known, is a law that was written and passed in 1986. It currently allows any federal agent to gain access to our email content or other data stored in the cloud without a warrant so long as that content is at least 180 days old. While the authors of this legislation should be commended for their efforts to set reasonable guidelines for the time, by today's standards this is shameful. Contents held in our emails most certainly deserve the same constitutional protections as the contents of our paper documents.

In 1986, we were two years removed from the release of the first Macintosh computer. The average hard disk drive stored less than 1% of what a typical hand-held phone holds today. Twenty-nine years ago, when you were finished with an email – if you even used email – you deleted it. Nothing was stored more than six months, which is why the standards codified in

ECPA made sense. Even by 1995, the earliest date we could find polling data and nearly ten years after the passage of ECPA, only 9% of American adults used the Internet.

However, the problem we now face is technology has changed more in the 29 years since ECPA was passed than in the prior 210 put together. Today, most Americans carry around in our pockets or purses supercomputers that contain more processing power and storage than computers the size of the Judiciary Hearing Room did in 1986.

Although some may not want to admit, these are sacred devices. They hold anything from our most private moments with family to romantic communications to confidential banking information. Many of us now keep our most precious photos of our children and grandchildren on these devices instead of in a scrapbook. They guide us when we travel and they keep us on schedule. They connect us with the world around us.

But because we are bound by standards authored in 1986, federal law allows the government to completely disregard their sacrosanct contents. Because Congress has failed to update this law, the government is free to trample on the Fourth Amendment protections afforded to every American.

Not only do I believe this to be true, along with more than 300 of my House colleagues, but the United States Court of Appeals for the Sixth Circuit also agreed in *U.S. v. Warshak* in 2010 when it ruled government agents violated Steven Warshak's privacy rights when they compelled a third-party server to produce contents of his emails without first obtaining a warrant. The Administration chose not to appeal the case to the Supreme Court then, yet maintains the need to keep ECPA in place today.

Along with Congress and the courts, the American people overwhelmingly agree with our position. In a poll released on Monday, 77% of responders agreed that the government should have to obtain a warrant to search email content. Furthermore, when participants had the basics of ECPA explained to them, 86% agreed the law must be updated. However, until recently the Internal Revenue Service printed in its handbook that Americans do not "have a reasonable expectation of privacy" in their email. I would assert that statement contains the closest thing you will find to the Administration's position on ECPA reform, which is squarely outside the mainstream on this issue and a major reason why we need to pass my bill.

The Email Privacy Act would update and fix the severely outdated portions of the United States Code codified by ECPA to reflect current technology and practice. We must value the constitutional guidance handed down by our forefathers in the Fourth Amendment over a law written 29 years ago. As I have said before, passing the Email Privacy Act would be a reflection on the genius of our forefathers more so than a criticism of lawmakers three decades ago.

Today, you will hear testimony from officials from the Securities and Exchange Commission and other government agencies who will attempt to argue essentially what the IRS handbook stated in writing – that Americans do not have a reasonable expectation of privacy in their digital communications stored on a third-party server or in the cloud. In an attempt to make their investigations less burdensome, they will assert the need to subpoena documents from a third-

party provider of your email account like Google rather than you – the individual. On the contrary, if you held the same contents printed on a piece of paper in a desk inside your home, they would subpoena you directly during an investigation – not IKEA, who manufactured your desk. They are defending an indefensible double standard.

What's worse, even while they will testify to that effect here today, these agencies have admitted in prior testimony that because of the *Warshak* decision, their agents do not currently invoke ECPA to gain access to email contents. Specifically important to note because of today's panel, SEC Chairwoman Mary Jo White testified before the Appropriations Committee in in April that she has not invoked ECPA for email contents since she took over as chair of the SEC. Ultimately, this means the Email Privacy Act would codify existing practice.

Finally, as a thought experiment, I ask the members of this committee to imagine someone walking into this room right now and picking up your cell phone without your permission. Imagine that person beginning to read through the content on your device. When you try to stop them, they assure you that they will only read content more than six months old. Would that ease your mind?

Maybe it would ease your mind if that person was an employee of the IRS?

If it doesn't, I urge you take swift, decisive action to update this long overdue law. I look forward to the Judiciary Committee scheduling a markup of my legislation so Congress may send my bill to the President's desk. While legislative activity in the Senate shows promise, this effort really is by a mandate directly from the people. That's why the People's House must lead the charge.

Chairman Goodlatte, Ranking Members Conyers, and members of the Committee, I thank you for your time and your careful consideration today.

BRAD R. WENSTRUP
2ND DISTRICT, OHIO

COMMITTEE ON ARMED SERVICES

COMMITTEE ON VETERANS' AFFAIRS
CHAIRMAN, SUBCOMMITTEE ON ECONOMIC OPPORTUNITY

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

www.Wenstrup.House.Gov

Congress of the United States
House of Representatives

1318 LONGWORTH BUILDING
WASHINGTON, D.C. 20515
(202) 225-3164

7954 BEECHMONT AVENUE
SUITE 200
CINCINNATI, OHIO 45255
(513) 474-7777

120 NORTH MAIN STREET
PEEBLES, OHIO 45660
(513) 605-1380

4350 AICHOLTZ ROAD
CINCINNATI, OHIO 45245
(513) 605-1388

November 30, 2015

Chairman Bob Goodlatte
House Judiciary Commitee
2138 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Goodlatte,

I write today to share a concern regarding the limits of the Stored Communications Act that has been brought to my attention by law enforcement in my district.

In late January 2015, there were multiple instances of shots fired at the Great American Tower in downtown Cincinnati. In order to catch the party or parties responsible, the Cincinnati Police Department (CPD) issued subpoenas for the cell phone and text records from the surrounding cell towers. Regrettably, subpoenas to some of the larger telecommunications companies were not answered in a prompt manner, and CPD has been unable to apprehend any suspects.

Unfortunately, I understand this example is not unique. Police departments across the country report frustration with delayed responses to criminal subpoenas for records from telecommunications companies. Given the often fast-paced nature of criminal activity, a slow response to these important data requests means too many crimes are going unsolved.

I understand that the Judiciary Committee is undergoing a thorough review and update of the Electronic Communications Privacy Act (ECPA). As access to private communications records is governed by Title II of ECPA, I ask the Committee to explore ways in which we can improve the process so that criminal subpoenas for communications records are responded to in a timelier fashion.

Thank you for your consideration.

Sincerely,

Brad R. Wenstrup

Brad Wenstrup
U.S. Representative

○