

Calendar No. 556

112TH CONGRESS }
2d Session }

SENATE

{ REPORT
{ 112-258

VIDEO PRIVACY PROTECTION ACT AMENDMENTS ACT OF 2012

DECEMBER 20, 2012.—Ordered to be printed

Mr. LEAHY, from the Committee on the Judiciary,
submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 2471]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to which was referred the bill (H.R. 2471) to amend section 2710 of title 18, United States Code, to clarify that a video tape service provider may obtain a consumer's informed, written consent on an ongoing basis and that consent may be obtained through the Internet, having considered the same, reports favorably thereon, with an amendment and an amendment to the title and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Background and Purpose of the Bill	2
II. History of the Bill and Committee Consideration	5
III. Section-by-Section Summary of the Bill	8
IV. Congressional Budget Office Cost Estimate	10
V. Regulatory Impact Evaluation	12
VI. Conclusion	12
VII. Additional Views of Senators Grassley, Sessions and Coburn	13
VIII. Changes to Existing Law Made by the Bill, as Reported	21

I. BACKGROUND AND PURPOSE OF THE BILL

A. THE VIDEO PRIVACY PROTECTION ACT AMENDMENTS

The Video Privacy Protection Act of 1988 (“VPPA”) prohibits video service providers from disclosing personally identifiable information except in certain, limited circumstances. As a general rule, personally identifiable information may be disclosed only with the prior written consent of the individual. The impetus for enacting the VPPA occurred when a weekly newspaper in Washington, DC, published a profile of Judge Robert H. Bork based on the titles of 146 films his family had rented from a video store.¹ At the time, the Senate Judiciary Committee was conducting hearings on Judge Bork’s nomination to the Supreme Court. Members of the Judiciary Committee denounced the disclosure.²

The VPPA prohibits unauthorized disclosure of personally identifiable information that links a customer or patron to particular materials or services. Individuals may bring a civil action for damages in the event of an unauthorized disclosure.³ The VPPA does permit the disclosure of personally identifiable information under appropriate and clearly defined circumstances. For example, the VPPA allows for disclosure of personally identifiable information concerning a consumer pursuant to a court order or “with the informed, written consent of the consumer given at the time the disclosure is sought.”⁴ The VPPA does not limit the rights of consumers or patrons under State or local law.

At the time of the VPPA’s enactment, consumers rented movies from video stores. The method that Americans used to watch videos in 1988—the VHS cassette tape—is now obsolete. In its place, the Internet has revolutionized the way that American consumers rent and watch movies and television programs. Today, so-called “on-demand” cable services and Internet streaming services allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.

The Internet has similarly revolutionized how Americans share information. In the 1980s, when individuals wished to recommend a movie to a friend, the individual would likely call the friend on the telephone. In the 1990s, an email would likely be sent. Today, many Americans post their opinions and recommendations on social networking sites, like Facebook and Twitter.

The VPPA authorizes video tape service providers to share customer information with the “informed, written consent of the consumer at the time the disclosure is sought.”⁵ This consent must be obtained from the consumer each time the provider wishes to disclose that information. But, similar restrictions do not apply to disclosures of consumer information relating to book or music preferences. For example, Americans share information about the books that they read and the music that they listen to via social media sites, using services such as Spotify or the Washington Post’s social sharing app. However, the VPPA requires written consent to disclose information related to video rentals and purchases

¹“The Bork Tapes,” *The City Paper*, Sept. 25–Oct. 1, 1987, at page 1.

²See, S. Rep. No. 100–599, at pages 5–6 (1988).

³See, 18 U.S.C. §2710(c).

⁴See, 18 U.S.C. §2710(b)(2).

⁵*Id.* at 2710(b)(2)(B).

every time a disclosure is sought. That requirement creates obstacles for American consumers to share information about their video preferences through social media sites on an ongoing basis.

The bill addresses this limitation by amending the VPPA to allow consumers to provide their informed, written consent to disclose video viewing information—if they wish—one time in advance. This update to the law will allow American consumers to continuously share their movie or television preferences through social media sites. The legislation retains the privacy protections already in the law which requires that consumers “opt-in” to the sharing of their video viewing information. The bill similarly retains the requirement in current law that consumers provide informed written consent.

In addition, the bill provides that consumers may “opt-in” to the information sharing on an ongoing basis for a period of up to two years at a time, and they may “opt-out” of the information sharing at any time.

Lastly, the bill requires that the opportunity for a consumer to withdraw consent to the disclosure of video viewing information must be presented in a clear and conspicuous manner. The Committee intends that the language in Section 102 of the bill requires a video tape service provider to provide one of two opportunities for the consumer to withdraw consent: on a case-by-case (i.e., per title) basis, or to withdraw consent for ongoing disclosures. It is not the intent of the Committee to specify where on a website, or in what form, the opportunity to withdraw consent should be provided.

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS

The Electronic Communications Privacy Act (“ECPA”) amended Title III of the Omnibus Crime Control and Safe Streets Act to protect against the unauthorized interception of electronic communications. When Senator Leahy introduced the ECPA with Senator Mathias on June 19, 1986, he said that: “The Electronic Communications Privacy Act provides standards by which law enforcement agencies may obtain access to both electronic communications and the records of an electronic communications system. These provisions are designed to protect legitimate law enforcement needs while minimizing intrusions on the privacy of system users as well as the business needs of electronic communications system providers.”⁶ For almost three decades, the ECPA has been the premier privacy law protecting Americans from unauthorized Government intrusions into their private electronic communications.

The Electronic Communications Privacy Act requires that the Government obtain a court order, based upon probable cause, in order to intercept wireless and data communications. The law also requires that the Government obtain a search warrant in order to compel a third-party service provider to disclose the content of email, or other electronic communications, that the provider maintains in electronic storage. However, this search warrant requirement for email applies only if the email is 180 days old or less. Under the ECPA, an email is presumed to be abandoned after 180 days and the law allows the Government to compel the disclosure of older email with either a subpoena or a court order that is

⁶ See Cong. Rec., June 19, 1986 at page S 7993.

issued upon a finding that there are specific and articulable facts demonstrating that the information sought is relevant to a criminal investigation. The ECPA also allows the Government to use a subpoena or court order to compel disclosure of documents—regardless of their age—that a user stores in the Internet “cloud.”⁷

At the time that Congress enacted the ECPA, Congress assumed that most Americans would periodically access their email accounts and download any emails that they wished to read, and that third-party service providers would subsequently delete any email stored on their servers. In fact, Congress believed that the most extended period of time that a service provider might store an email would be for six months. But, after almost three decades, new technologies—such as the Internet, social networking sites and cloud computing—have changed how Americans use and store email today. Storing documents and other information electronically has become much less expensive and mobile technologies permit users to access stored documents wherever the user chooses to access the Internet. Yet, the digital privacy protections that the Congress put in place by enacting ECPA have not kept pace with these changes.

In March 2010, a diverse coalition of privacy and civil liberties advocates, major technology companies, think tanks, and academics wrote to Chairman Leahy to urge the Committee to begin work on reforming the Electronic Communications Privacy Act to reflect the realities of the digital age. The aptly named “Digital Due Process” coalition argued that the ECPA has been out-paced by changes in technology and the growth of email as a primary means of communicating. The Committee held the first of several hearings and briefings on ECPA reform in September 2010.

On January 11, 2011, Chairman Leahy announced that his legislative agenda for the 112th Congress would include legislation to update the Electronic Communications Privacy Act to better protect Americans’ digital privacy. In April 2011, the Committee held a second hearing on the ECPA reform effort that focused specifically on the perspectives of the Departments of Justice and Commerce on proposed updates to the law.⁸ On May 11, 2011, Chairman Leahy introduced the Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, legislation that would, among other things, update the ECPA to require a search warrant for the Government to access the contents of any email obtained from a third-party service provider. On September 20, 2012, Chairman Leahy offered this portion of his ECPA reform bill as an amendment in the nature of a substitute to H.R. 2471. The Committee favorably reported this legislation on November 29, 2012. The reforms in the bill seek to carefully balance the privacy expectations of American citizens, the legitimate needs of law enforcement agencies and the interests of the American technology sector.

The Committee recognizes that most Americans regularly use email in their professional and personal lives for confidential communications of a personal or business nature. The Committee also recognizes that there is growing uncertainty about the constitutionality of the provisions in ECPA that allow the Government to

⁷ See 18 U.S.C. §2703(d).

⁸ Although the Obama administration did not take an official position on the legislative proposals to update the ECPA, the Committee received technical comments and feedback on these proposals from the Departments of Justice and Commerce and other affected federal agencies.

obtain certain email content without a search warrant.⁹ The absence of clear legal standards for access to electronic communications content not only endangers privacy rights, but also endangers the admissibility of evidence in criminal and other legal proceedings. Accordingly, the Committee has determined that the law must be updated to keep pace with the advances in technology, to ensure the continued vitality of the Fourth Amendment protections for email and other electronic communications content.

The ECPA reforms in the bill have bipartisan support on the Committee, as well as the support of a broad coalition of privacy, civil liberties, civil rights and technology organizations from across the political spectrum. The organizations and individuals below support the principles embodied in the legislation:

Technology Industry and Trade Associations: Adobe, AOL, eBay, Facebook, IBM, LinkedIn, Microsoft, Netflix, Symantec, Verizon, Business Software Alliance, Computer and Communications Industry Association, Newspaper Association of America, Software & Information Industry Alliance, and TechAmerica.

Privacy, civil liberties and civil rights communities: American Civil Liberties Union, Americans for Tax Reform, American Library Association, Center for Constitutional Rights, Center for Democracy & Technology, Competitive Enterprise Institute, The Constitution Project, Electronic Frontier Foundation, The Leadership Conference on Civil and Human Rights, Liberty Coalition, Mexican American Legal Defense and Educational Fund, Muslim Legal Fund of America, NAACP, National Association of Criminal Defense Lawyers, National Hispanic Media Coalition, National Urban League, and TechFreedom.

Law Enforcement Community: Zachary W. Carter, U.S. Attorney, Eastern District of New York (1993–1999); W. Thomas Dillard, Assistant U.S. Attorney, Eastern District of Tennessee (1967–1976, 1978–1983), U.S. Attorney, Northern District of Florida (1983–1986); Saul A. Green, U.S. Attorney, Eastern District of Michigan (1994–2001); Rodger A. Heaton, U.S. Attorney, Central District of Illinois (2005–2009); A. Melvin McDonald, U.S. Attorney, District of Arizona (1981–1985); Jerome F. O’Neill, U.S. Attorney, District of Vermont (1981), First Assistant U.S. Attorney, District of Vermont (1975–1981); Stephen M. Orlofsky, U.S. District Judge, District of New Jersey (1996–2003); U.S. Magistrate Judge, District of New Jersey (1976–1980); and Ron Woods, U.S. Attorney, Southern District of Texas (1990–1993).

II. HISTORY OF THE BILL AND COMMITTEE CONSIDERATION

A. INTRODUCTION OF THE BILL

On July 8, 2011, Representative Goodlatte introduced H.R. 2471—a bill to amend the Video Privacy Protection Act, Title 18, United States Code, Section 2710, to clarify that a video tape service provider may obtain a consumer’s informed, written consent to disclose video viewing information to a third party on an ongoing

⁹In 2010, the Court of Appeals for the Sixth Circuit held that use of a subpoena or court order under Section 2703 of ECPA to obtain the contents of emails violated the Fourth Amendment’s prohibition against warrantless searches. See *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). As a result, today, a different legal standard applies for obtaining email content for cases arising in the Sixth Circuit.

basis and that such consent may be obtained through the Internet. The House Committee on the Judiciary favorably reported H.R. 2471 with amendments on December 2, 2011. On December 6, 2011, the House of Representatives passed the bill by a vote of 306 to 116. The bill was referred to the Senate Committee on the Judiciary on December 7, 2011.

B. COMMITTEE CONSIDERATION

Chairman Leahy placed H.R. 2471 on the Committee's executive business agenda on September 13, 2012. The Committee considered this legislation on September 20, 2012, and November 29, 2012.

The Committee has held three hearings related to H.R. 2471. On September 22, 2010, the Judiciary Committee held a hearing entitled, "The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age." The hearing examined several gaps in this digital privacy law that have resulted from changes in technology. The witnesses for this hearing were: Cameron F. Kerry, General Counsel, United States Department of Commerce; James A. Baker, Associate Deputy Attorney General, United States Department of Justice; James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology; Brad Smith, General Counsel and Senior Vice President, Legal and Corporate Affairs, Microsoft Corporation; and Jamil N. Jaffer, Attorney, Washington, D.C. During this hearing, Senator Leahy called for Congress to work on bipartisan legislation to update the ECPA to meet the privacy demands of the digital age.

On April 6, 2011, the Judiciary Committee held a hearing entitled, "The Electronic Communications Privacy Act: Government Perspectives on Privacy in the Digital Age." This hearing examined potential updates to the Electronic Communications Privacy Act to address inconsistencies in that law, changes in technology, and new threats to privacy and cybersecurity. The witnesses for this hearing were: Cameron Kerry, General Counsel, United States Department of Commerce, and James Baker, Associate Deputy Attorney General, United States Department of Justice.

On January 31, 2012, the Judiciary Committee's Subcommittee on Privacy, Technology and the Law held a hearing on "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century." Senator Franken chaired this hearing. The purpose of this hearing was to examine possible updates to the Video Privacy Protection Act. The witnesses for this hearing were: Representative Mel Watt (D-NC); David Hyman, General Counsel, Netflix, Inc.; Professor William McGeeveran, University of Minnesota Law School; Marc Rotenberg, Executive Director, Electronic Privacy Information Center (EPIC); and Christopher Wolf, Director, Privacy and Information Management Group, Hogan Lovells, LLP.

On September 20, 2012, Chairman Leahy offered an amendment in the nature of a substitute for H.R. 2471, which the Committee adopted by consent. The substitute bill made several changes to the bill to enhance privacy, including adding a requirement to the bill that consumer consent to share video viewing information be a clear and conspicuous "opt-out" option. Accordingly, a video tape service provider must give consumers either a clear and straightforward opportunity to withdraw from all ongoing disclosures or a clear and straightforward opportunity to withdraw from ongoing

disclosures on a case-by-case basis. The “case-by-case” option is intended to allow consumers to opt out of the sharing of information relating to the viewing of individual movies or television series.

The Chairman’s amendment also added several provisions to strengthen privacy protections in the Electronic Communications Privacy Act of 1986. Specifically, the amendment amends Title 18, United States Code, Section 2702 to prohibit an electronic communication or remote computing service provider from voluntarily disclosing the contents of its customer’s email or other electronic communications to the Government. The amendment also amends ECPA so that the disclosure of the content of email and other electronic communications by an electronic communication or remote computing service provider to the Government is subject to one clear legal standard—a search warrant issued based on a showing of probable cause. In addition, the amendment requires that the Government notify the individual whose account was disclosed, and provide that individual with a copy of the search warrant and other details about the information obtained. Such notice must be provided within three business days of the Government’s receipt of the communications if the Government entity requesting the information is a law enforcement agency, unless the notice is delayed pursuant to a court order.

On November 29, 2012, the Committee resumed consideration of the substitute bill. Several amendments to the bill were offered:

First, Chairman Leahy offered a manager’s amendment to the bill to address several issues raised by the law enforcement community. The amendment made the following changes to the bill: (1) adds a rule of construction provision to the bill to clarify that the bill does not intend to apply the Electronic Communications Privacy Act’s warrant requirement to the Wiretap Act, the Foreign Intelligence Surveillance Act, or any other provision of Federal law; (2) extends the time period during which the Government must give notice from three days to 10 business days; (3) extends the time period during which the Government may seek a court order to delay notice under the bill from 90 days to 180 days; (3) extends the time period during which the Government may seek a court order to preclude a service provider from notifying a customer about a Government request for communications from 90 days to 180 days; (4) adds a requirement that service providers notify the Government of their intent to inform a customer about a request for electronic communications content at least three business days before such notice is given; and (5) adds civil discovery subpoenas to the list of subpoenas that the Government may use to obtain routing information and other non-content information under Section 2703(c) of ECPA. The Committee adopted the amendment by voice vote.

Second, Chairman Leahy offered a technical amendment to modify the title of the bill, which the Committee also adopted by voice vote.

Third, Senator Lee offered an amendment on behalf of himself and Senator Cornyn to retain the original three-day notice requirement in the bill and 90-day delayed notification periods in the bill for government entities other than law enforcement agencies. The Committee adopted the amendment by voice vote.

Fourth, Senator Feinstein offered an amendment to the video privacy title of the bill that requires that the time period during which a consumer may give ongoing consent to the disclosure of video viewing information shall not exceed a period of two years. The Committee adopted the amendment by voice vote.

Lastly, Senator Grassley offered an amendment to create an exception to the warrant requirement for electronic communications content that is stored for more than 180 days in an electronic storage system in cases involving child abduction or kidnapping, child pornography, or violent crimes against women. The Committee rejected the amendment by roll call vote. The vote record is as follows:

Tally: 7 Yeas, 11 Nays

Yeas (7): Grassley (R-IA), Hatch (R-UT), Kyl (R-AZ), Sessions (D-AL), Cornyn (R-TX), Graham (R-SC), and Coburn (R-OK).

Nays (11): Leahy (D-VT), Kohl (D-WI), Feinstein (D-CA), Schumer (D-NY), Durbin (D-IL), Whitehouse (D-RI), Klobuchar (D-MN), Franken (D-MN), Coons (D-DE), Blumenthal (D-CT) and Lee (R-UT).

The Committee then voted to report the bill, as amended, favorably to the Senate by voice vote. Senator Sessions (R-AL) requested that his vote be recorded as no.

III. SECTION-BY-SECTION SUMMARY OF THE BILL

TITLE I—VIDEO PRIVACY PROTECTION

Section 101. Short Title

This section designates the title as the “Video Privacy Protection Act Amendments Act of 2012.”

Section 102—Video Privacy Protection Act Amendment

Section 102 amends Title 18, United States Codes, Section 2710(b)(2) to clarify that video tape service providers may obtain a customer’s informed, written consent to share video viewing information on an ongoing basis and that such consent may be obtained via the Internet. The provision also makes clear that the decision to share video viewing information must be at the consumer’s election (i.e. “opt in”). Moreover, the provision includes a requirement that video service providers provide their customers, in a clear and conspicuous manner, with the opportunity to withdraw the consent given to share video viewing information at any time.

In addition, the provision limits the amount of time that a consumer’s ongoing consent to share video viewing information remains valid. Section 102 requires that the length of time during which advance consent will remain valid shall not exceed two years.

TITLE II—ELECTRONIC COMMUNICATIONS PRIVACY

Section 201. Short Title

This section designates the title as the “Electronic Communications Privacy Act Amendments Act of 2012.”

Section 202. Confidentiality of Electronic Communications

Section 202 amends Title 18, United States Code, Section 2702 (the Electronic Communications Privacy Act or “ECPA”) to prohibit an electronic communication or remote computing service provider from voluntarily disclosing the contents of its customer’s email or other electronic communications to the Government. There are limited exceptions to this prohibition under current law, including customer consent, and disclosure to law enforcement to address criminal activity.

Section 203. Elimination of 180-Day Rule; Search Warrant Requirement for Content; Required Disclosure of Customer Records

Section 203 amends the ECPA so that the disclosure of the content of email and other electronic communications by an electronic communications or remote computing service provider to the Government 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 that calls for different legal standards for the Government to obtain email content, depending upon the email’s age and whether the email has been opened. The provision also requires that the Government notify the individual whose account was disclosed, and provide that individual with a copy of the search warrant and other details about the information obtained. Such notice must be provided within ten business days of a law enforcement agencies receipt of the communications, unless the notice is delayed pursuant to Section 204 of the bill.

Section 203 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 customer name, address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information.

At the request of the Department of Justice and the Federal Trade Commission, Section 203 also contains a provision that adds civil discovery subpoenas to the types of subpoenas that may be used under existing law (administrative subpoena authorized by Federal or State law, Federal or State grand jury subpoena and trial subpoena) to obtain routing and other non-content information from a third-party provider.

Section 204. Delayed Notice

Section 204 amends section 2705 of the ECPA to provide that the Government may seek a court order to delay notifying an individual of the fact that the Government has accessed the contents of the individual’s electronic communications for up to 180 days, if the requesting government entity is a law enforcement agency, and for up to 90 days, if the requesting government entity is a civil or administrative enforcement agency. A court may extend the delay periods for a period of up to an additional 180 or 90 days at a time, respectively.

Section 204 also establishes a 180-day time limit on the period that the Government could preclude a service provider from informing its customer about the disclosure of electronic communica-

tions information to the Government. If the government entity is a civil or administrative enforcement agency, the applicable time period for preclusion of notice is 90 days. These time periods may also be extended by a court for up to an additional 180 or 90 days at a time, respectively.

Lastly, Section 205 requires that service providers notify the government of their intent to inform a customer or subscriber of the fact that the provider has disclosed the individual's electronic communications information to the Government at least three business days before the provider gives such notice to the customer or subscriber. 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.

Section 205. Rule of Construction

Section 205 provides that the search warrant requirement for electronic communications content contained in Section 203 of the bill does not apply to any other Federal criminal or national security laws, including Title III of the Omnibus Crime Control and Safe Streets Act of 1986 (commonly known as the "Wiretap Act") and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq. (commonly known as "FISA")).

IV. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The Committee sets forth, with respect to the bill, H.R. 2471, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

DECEMBER 18, 2012.

Hon. PATRICK J. LEAHY,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2471, an act to amend section 2710 of title 18, United States Code, to clarify that a video tape service provider may obtain a consumer's informed, written consent on an ongoing basis and that consent may be obtained through the Internet.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz (for federal costs), who can be reached at 226-2860, Elizabeth Cove Delisle (for the impact on state, local, and tribal governments), who can be reached at 225-3220, and Paige Piper/Bach (for the impact on the private sector), who can be reached at 226-2940.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 2471—An act to amend section 2710 of title 18, United States Code, to clarify that a video tape service provider may obtain a consumer’s informed, written consent on an ongoing basis and that consent may be obtained through the Internet

Current law permits businesses that rent, sell, or deliver audio visual materials to disclose personal information about customers to other persons if the customer grants written consent. H.R. 2471 would clarify that such consent may be given by such customers through the use of the Internet. The act also would make several other changes to current law relating to the privacy of personal electronic communications. CBO estimates that implementing H.R. 2471 would have no significant cost to the federal government. Enacting the legislation would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

H.R. 2471 would impose intergovernmental mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by changing the procedures that government agencies must follow when they obtain electronic communications. Because the changes would result in minimal additional spending, CBO estimates that the costs of the intergovernmental mandates would be small and would not exceed the threshold established in UMRA (\$74 million in 2013, adjusted annually for inflation).

H.R. 2471 would impose private-sector mandates, as defined in UMRA, on providers of video tape services and other entities. Title I would require such providers to use “distinct and separate” forms when obtaining consent to disclose a consumer’s personally identifiable information. At the same time, the act would benefit providers and other entities by allowing them to obtain consent via the Internet, in advance, and only once until consent is withdrawn. Current law requires written consent each time disclosure of a consumer’s personally identifiable information is sought.

In addition, title II would require providers of video tape services and other entities to inform the government of their intent to notify a customer or subscriber of the fact that the provider has disclosed information about the individual’s electronic communication activities to the government, no later than three business days prior to providing such notice.

Based on information from industry sources, CBO estimates that there would be no significant net costs to comply with the mandate; thus, any costs would fall well below the annual threshold established in UMRA for private-sector mandates (\$146 million in 2012, adjusted annually for inflation).

On October 25, 2011, CBO transmitted a cost estimate for H.R. 2471 as ordered reported by the House Committee on the Judiciary on October 13, 2011. CBO estimates that implementing that version of the legislation also would have no significant cost to the federal government.

The CBO staff contacts for this estimate are Mark Grabowicz (for federal costs), Elizabeth Cove Delisle (for the impact on state, local, and tribal governments), and Paige Piper/Bach (for the impact on the private sector). The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

V. REGULATORY IMPACT EVALUATION

In compliance with Rule XXVI of the Standing Rules of the Senate, the Committee finds that no significant regulatory impact will result from the enactment of H.R. 2471.

VI. CONCLUSION

The bill, as amended, H.R. 2471, provides greatly needed updates to our Federal digital privacy laws. The bill carefully balances the need to protect Americans' privacy rights in cyberspace, with the legitimate needs of law enforcement and the interests of the American technology sector. Given the many advances in technology and new threats to privacy, the passage and enactment of these important privacy updates is long overdue.

VII. ADDITIONAL VIEWS

ADDITIONAL VIEWS FROM SENATORS GRASSLEY, SESSIONS, AND COBURN

Although we voted to report the bill, we write to express concerns with portions of the Video Privacy Protection Act Amendments Act of 2012 (VPPA) that were contained in Chairman Leahy's manager's amendment to H.R. 2471 adopted at the Committee's Executive Business Meeting. Our concern focuses specifically on the amendments that relate to the Electronic Communications Privacy Act of 1986 (ECPA). We agree that ECPA reform is necessary to update the law to match advances in technology. Having said that, we agree with those on both sides of the Committee that expressed concerns at the mark-up with the current draft that we can craft the bill in a way that increases email privacy but also protects law enforcement agencies' ability to obtain information in order to investigate serious crimes, such as child abduction and domestic violence, as well as civil regulatory agencies' ability to investigate wrongdoing. This version does not strike the proper balance, but it is the start of an important discussion.

However, we must now state for the record what we believe is the right path to take before the full Senate can act on this issue. First, we are troubled by the piecemeal approach taken by the Chairman. The Committee should take a more comprehensive approach to updating the laws involving electronic communications and data, and fully address the many concerns that have been raised by the law enforcement, technology, and privacy communities. Second, the Chairman's amendment is flawed because it increases burdens on law enforcement officers seeking access to often critical evidence, especially in time-sensitive cases. Third, and finally, the Chairman's amendment removes a valuable tool from civil regulatory agencies, which rely on administrative subpoenas to obtain email communications when investigating insider trading, accounting fraud, and false or misleading statements made by companies about their financial situations. While we support the goal of harmonizing and updating ECPA, failure to address these important issues and strike the proper balance will prevent this legislation from becoming law.

Current Law

ECPA was enacted in 1986 as a result of advancements in wireless communication technology and was designed to provide modern rules for government access to electronic communications and related data. It was designed to balance the public's privacy inter-

ests with law enforcement’s need to access electronic communication information for investigative purposes.¹

ECPA created a spectrum of legal standards depending on the level of privacy interest in the information sought by the government. For example, under one part of the law, a government entity may require a provider of electronic communication services to disclose the contents of a wire or electronic communication that is in electronic storage for 180 days or less pursuant to a criminal search warrant.² For communications stored with a third party for more than 180 days, however, the statute authorizes a lower legal burden.³ A government entity can require a provider of electronic communication services to disclose the contents of the communications either by search warrant (without notice to the subscriber or customer), or by administrative, grand jury, or trial subpoena, or a Section 2703(d) court order if notice is first provided to the subscriber or customer.⁴ The basis for the “180 day rule” is that if the emails are stored by a third party service provider, for more than six months, one’s expectation of privacy in the content of these communications diminishes, and these records are considered more akin to third party business records than real-time communications. As a result, law enforcement investigators have been able to use quicker and more efficient methods of legal process (i.e. subpoena or 2703(d) order) to obtain these older emails and related records.

The ability to use a subpoena or a court order has allowed law enforcement officials to gather older email content information quickly in cases where time is of the essence and probable cause may not yet have been developed. Under the Chairman’s amendment, however, criminal investigators would not be able to obtain email information in criminal investigations until they have developed probable cause and could obtain a search warrant.

Additionally, these same tools have permitted federal regulatory agencies like the Securities and Exchange Commission, the Food and Drug Administration, the Consumer Product Safety Commission, and the Federal Trade Commission, etc., to gather important information by administrative subpoenas and carry out their enforcement responsibilities over important industries. But the Chairman’s amendment eliminates these administrative subpoenas and, because civil investigators have no criminal search warrant authority, they therefore will no longer be able to obtain email information. Civil regulators would then have no ability to compel the disclosure of email content from third party Internet service providers. As a result, the Chairman’s amendment calls into question whether civil regulatory agencies can even undertake the types of investigations Congress has authorized and empowered them to undertake.

ECPA Reform Requires a More Comprehensive Review

As an initial matter, in conducting a review of the laws relating to electronic communications and related documents, we agree that

¹ S. Rep. No. 99–541, pt. 3, at 5 (1986) (noting that, when ECPA was first adopted, the Senate Judiciary Committee believed that it “represent[ed] a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies”).

² 18 U.S.C. § 2703 (a) (2006).

³ 18 U.S.C. § 2703 (a) (2006).

⁴ 18 U.S.C. § 2703 (b) (2006).

work needs to be done to ensure that our laws are up to date and do not negatively impact business innovation and development. We also need to address legitimate privacy concerns. It is equally important, however, to hear from the law enforcement community to ensure that we do not limit their ability to obtain information necessary to catch criminals and terrorists who use electronic communications to further their crimes. ECPA has specific definitions and has come to be interpreted by courts in particular ways; therefore, any amendment requires careful consideration to ensure that we do not create loopholes that make it harder for law enforcement to do their jobs and allow criminals and terrorists to operate with impunity.

This amendment appears to upset the important balance between privacy and public safety without consideration of the concerns raised by current law enforcement officials. In fact, at the last hearing on this matter—held nearly two years ago—the only law enforcement input came from a representative of the Department of Justice who offered no official position because none had been cleared by the current Administration.⁵ When this bill was first scheduled for mark-up in September 2012, representatives from the Major Cities Chiefs of Police Association, Major Counties Sheriffs' Association, Association of State Criminal Investigative Agencies, National Sheriffs' Association, National Narcotic Officers' Associations' Coalition, and National District Attorneys' Association all co-signed a letter “strongly urging the Committee to reconsider acting on the ECPA reform proposal until a comprehensive review of its impact on law review investigations is conducted.”⁶ These law enforcement groups also expressed substantive concerns that the Chairman’s amendment would increase the burden on law enforcement and delay investigations.⁷ Additionally, the Federal Bureau of Investigations Agents Association wrote that “many key stakeholders have not had a chance to fully vet the amendment,” and that urged the Chairman to work with law enforcement to “revise provisions that potentially undermine our ability to protect this Nation, the Constitution, and our citizens.”⁸ We attach these letters to these Additional Views as part of the record.

Our first responders—the brave men and women serving in law enforcement who are on the front lines protecting our communities—need to have a seat at the table and be able to contribute to the ECPA dialogue in a meaningful way. We need to understand what the impact to law enforcement investigations will be before passage of this bill. Regrettably, the Chairman has not made input from state and local law enforcement a priority.

The Amendment May Adversely Affect Criminal Investigations

Law enforcement representatives have raised concerns with the Chairman’s amendment that it would increase the legal standard

⁵The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary, 112th Cong. 7 (2011) (answer by James Baker, Associate Deputy Attorney General, U.S. Dep’t of Justice).

⁶Letter from the MCCPA, MCSA, NSA, ASCIA, NNOAC, and NDAA to U.S. Senate Judiciary Committee Chairman Leahy & Ranking Member Grassley, 2 (September 18, 2012) (attached in appendix).

⁷Id. at 2–3.

⁸Letter from FBIAA to U.S. Senate Judiciary Committee Chairman Leahy, 1 (September 19, 2012) (attached in appendix).

to require a criminal search warrant for the content of all email communications regardless of the length of time they have been in electronic storage. They argue that increasing the legal burdens will hinder and delay criminal investigations.⁹ Criminal search warrants require a showing of probable cause to believe that a crime has been committed and that evidence of that crime will be located in the place to be searched. This can be a challenging standard, especially in cases where time is of the essence.

For example, in the early stages of a child abduction case where time is of the essence, the facts are usually not fully known. Investigators often cannot establish probable cause to search a missing child's email account—or a similar account such as Facebook or Twitter—because it is not clear that a kidnapping has occurred or that evidence of that crime will be found in the child's email account. However, under current law, investigators have been able to access the contents of a child's email account by using grand jury subpoenas or court orders, thereby identifying valuable investigative leads and even perpetrators who may have been communicating with the child.

Under the Chairman's amendment, however, investigators have no way to compel the disclosure of this vital information and are left at the mercy of parental consent or voluntary disclosure by service providers. While neither of these scenarios requires a warrant, they are both highly problematic for other reasons. Investigators would encounter issues with parental consent when a child's parents are unavailable because they are dead or missing, or unwilling to consent when they are targets of the investigation.

Voluntary disclosure by service providers is likewise unreliable, because the Chairman's amendment does not provide a tool for law enforcement to compel disclosure. In Section 2702(b) of Title 18, United States Code, service providers are permitted to voluntarily disclose email content information to law enforcement officials if the provider, *in good faith*, believes that an emergency involving danger of death or serious physical injury to any person requires the disclosure without delay of the communication. But, even if an emergency arises and time is of the essence, the Chairman's amendment *does not require* a service provider to disclose important information to law enforcement investigators. Early in an investigation, when any information as to the location of the child and identity of the kidnappers is absolutely critical, a provider may be reluctant to voluntarily disclose information without a warrant for a number of reasons. These might include a fear of litigation for disclosing a customer's information without a warrant, declining to accept law enforcement's assertion that there are enough facts to justify an emergency, implementing a policy of always requiring a search warrant, and many other possible impediments to the rapid recovery of the child.

This question was raised at the Committee mark-up of the Chairman's amendment as to whether the traditional "exigent circumstances" to the Fourth Amendment would be sufficient to permit investigators to seize the electronic communication information

⁹Id. at 2; Letter from the MCCA, et al, to Chairman Leahy & Ranking Member Grassley, supra note 6, at 2-3.

without a warrant. Despite assurances from supporters of the bill that the traditional exigent circumstances exception would apply in the event this bill becomes law, this is not a settled issue by any means.

As a threshold matter, courts across the country disagree as to whether the contents of email stored in the hands of a third party service provider trigger privacy protection under the Fourth Amendment. Some courts have held that emails are analogous to a mailed letter, and that an individual's reasonable expectation of privacy ends upon delivery of the letter or the transmission of the email to the recipient.¹⁰ Other courts have reached a different conclusion, holding that a subscriber enjoys a reasonable expectation of privacy in the content of emails that are stored or sent and received through a third-party internet service provider.¹¹ Unfortunately, the Committee never held a hearing, heard witnesses or reviewed evidence, or even had the opportunity to debate this important question. Had the Committee fully vetted this bill, perhaps we would have greater clarity on this question.

But even assuming *arguendo* that the Fourth Amendment exceptions apply, the exigent circumstances exception would not be helpful under the Chairman's amendment because often law enforcement officials will be forced to seek the active cooperation of service providers. For example, if investigators believe it is necessary to search a storage locker and exigent circumstances exist, then the exception permits them to simply search the locker and seize the contents. In contrast, investigators do not possess the capability to seize an email account without the assistance of the third party service provider, even if exigent circumstances exist. Therefore, despite the exigent circumstances exception, investigators are still at the mercy of the service providers.

One problem with the exigent circumstances exception in the ECPA context is that it leaves the determination of an "emergency" solely in the hands of a service provider instead of the law enforcement professional. Law enforcement investigators, who have the training and experience in such matters, should be making the determination as to what constitutes an emergency situation—not an untrained employee of a service provider. An emergency exception that allows law enforcement professionals to determine the existence of an emergency and requires service providers to disclose the requested information is a potential fix that might help address

¹⁰ See, e.g., *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (holding that, like letter-writers whose expectation of privacy ends upon delivery of the letter, individuals may not possess a legitimate expectation of privacy "in transmissions over the Internet or e-mail that have already arrived at the recipient"); *United States v. Dupree*, 781 F.Supp.2d 115, 159 (E.D.N.Y.2011) (finding that defendants could "not claim a legitimate expectation of privacy in emails that they gave [an employee] permission to access and view"); *State v. Hinton*, 280 P.3d 476, 482 (Wash. App. 2012) (ruling that the defendant's expectation of privacy in a text message terminated upon the message's delivery to the recipient). Furthermore, the Supreme Court has held that the Fourth Amendment did not prevent the government from reviewing electronic pager messages of its employees. *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010).

¹¹ See, e.g., *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial [internet service provider]'"); *United States v. Forrester*, 512 F.3d 500, 509–11 (9th Cir. 2008) (finding that a customer does not have a legitimate expectation of privacy in the email addresses attached to transmitted messages or the internet protocol addresses visited on a home computer because that information is voluntarily conveyed to the service provider, but distinguishing between addresses and the content of messages, noting that "the contents may deserve Fourth Amendment protection, but the address and size of the package do not").

some law enforcement concerns and might help recalibrate ECPA so that there is better balance between privacy and public safety.

We have a related concern as to whether Congress should be looking at setting time limits to ensure timely compliance with the search warrants. By raising all content requests to a search warrant standard, the Chairman's amendment would delegate authority to every state, local, and federal judge to manage requests for email content. This is important because, traditionally, search warrants do not operate like subpoenas, where recipients are typically given up to 14 days to respond. Instead, search warrants usually require immediate processing and prompt reporting back to the judge. However, law enforcement officials have advised us that third-party service providers do not always provide prompt compliance. Additionally, because the statute is silent on this matter, courts often create their own time limits. We should consider whether uniform time limits for compliance with the search warrant are appropriate and seek to avoid the confusion inherent with third-party compliance wrought by the variable time limits set by the different federal and state courts issuing these warrants.

Civil Investigations Could Be Adversely Affected

As noted above, under the Chairman's amendment, agencies with civil regulatory authority will no longer be able to compel access to older email content because the amendment removes the administrative subpoena as a tool to obtain email communications. The Chairman's amendment permits criminal search warrants as the sole legal vehicle to compel disclosure of email content. Without criminal search warrant authority, these civil federal agencies reported to us that the amendment will negatively impact their investigations.

For example, the Securities and Exchange Commission (SEC) relies on email communications to help determine a person's intent, agreements and conspiracies to defraud, and patterns of illegal conduct when investigating allegations of insider trading, accounting fraud, and providing false or misleading information about securities and the companies that issue them. In providing technical assistance to the Ranking Member in evaluating the bill, the SEC advised that this legislation would significantly impact the SEC's enforcement of the securities laws—including insider trading.

The SEC recently filed a civil case against two individuals that alleges that over a period of years they engaged in a scheme to artificially inflate the financial results of a publicly owned retailer by engaging in a series of fraudulent financial transactions. During the investigation, the SEC obtained an email using an ECPA-authorized subpoena showing that one of the defendants sent an email describing the publicly owned company's commitment to buy certain products and services at inflated prices. The email stated "the fake credits that were negotiated with" the company were being used "to hit certain quarterly numbers." This evidence was particularly important because the defendants were sophisticated and had cleverly and carefully concealed their scheme. The SEC subpoenaed the Internet Service Provider (ISP) because an individual in the case had failed to produce an email from one his personal email accounts in response to a subpoena issued to him al-

most a year earlier. SEC investigators confronted the defendant with the email obtained from the ISP. The defendant then produced his personal email, including this inculpatory one. This example demonstrates how important the administrative subpoena is in the civil regulatory context; indeed, it can be the difference between enforcing the laws and watching helplessly as crafty fraudsters escape liability and accountability for their crimes.

The SEC has also advised us that investigative administrative subpoenas for email from ISPs are highly valuable in other situations, such as: (1) when investigators are attempting to locate stolen assets of victimized investors, (2) where the target of an investigation lives outside the United States, and (3) where the target of an investigation claims to have deleted all of their emails, has a damaged hard drive, or simply withholds the evidence.

The administrative subpoena is a vital tool for other federal civil enforcement agencies as well. The Food and Drug Administration also uses administrative subpoenas to review email communications to investigate allegations regarding violations of food and drug safety laws. The Consumer Product Safety Commission and the Federal Trade Commission use email communications to investigate allegations of fraud, deception, and unfair business practices in the marketplace. The Commodities and Futures Trading Commission (CFTC) relies on email communications to investigate fraud, manipulation, and abusive trading practices in the marketplace. Through effective oversight, the CFTC enables the futures markets to serve the important function of providing a means for price discovery and offsetting price risk.

Additionally, the Department of Justice (Department), in providing technical advice on the amendment, indicated that the Chairman's amendment would negatively impact civil cases brought by the Department. Notably, they provided an example where the Civil Rights Division uses administrative subpoenas to retrieve text and email messages, as well as social media, in cases involving sexual or racial harassment of employees, tenants, and students. For example, when the Department sues to prevent harassment, the conduct often occurs over a long period of time and may be targeted at multiple victims. Department lawyers are sometimes confronted with loss of evidence because victims delete messages that contain disturbing sexual or racist content or because a significant period of time has passed since they received the messages.

Evidence is also lost because harassers intentionally delete evidence of their conduct. Messages that contain harassing or abusive racist and sexual content are highly relevant in these cases and are typically discoverable through current ECPA procedures. When the Department is unable to obtain these messages directly from victims or harassers, they need the ability to serve civil discovery subpoenas directly on third party providers to obtain evidence of racial and sexual harassment. While the Chairman's amendment permits civil discovery subpoenas for non-content electronic information, it does not include a tool for the Civil Rights Division to compel the disclosure of the content of email information from the third party service provider. Therefore, under the amendment, much of this evidence currently used to enforce safe and appropriate work- and

study-places would be lost and victims of harassment would be left vulnerable to their harassers.

Conclusion

We agree that ECPA reform is needed to address the dramatic advances to technology over the last three decades. We disagree, however, with the current hurried process and the piecemeal version reported by the Committee. Thus far, the process has lacked transparency, ignored the very valid concerns of the law enforcement community, and proceeded in a fragmented fashion. ECPA reform requires a comprehensive approach that strikes the proper balance between privacy and public safety. Going forward, we trust that the Committee will address the concerns described above and that meaningful ECPA reform can be achieved.

CHARLES E. GRASSLEY.

JEFF SESSIONS.

TOM COBURN.

VIII. CHANGES TO EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by H.R. 2471, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

18 U.S.C. 2710—WRONGFUL DISCLOSURE OF VIDEO TAPE RENTAL OR SALE RECORDS

(a) DEFINITIONS.—For purposes of this section—

(1) the term “consumer” means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term “ordinary course of business” means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term “personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term “video tape service provider” means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) VIDEO TAPE RENTAL AND SALE RECORDS.—

(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer—

(A) to the consumer;

(B) **to any person with the informed, written consent of the consumer given at the time the disclosure is sought;** *to any person with the informed, written consent (including through an electronic means using the Internet) of the consumer that—*

(i) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;

(ii) at the election of the consumer—

(I) is given at time the disclosure is sought; or

(II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and

(iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to

withdraw for ongoing disclosures, at the consumer's election;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if—

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) CIVIL ACTION.—

(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award—

(A) actual damages but not less than liquidated damages in an amount of \$2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

- (D) such other preliminary and equitable relief as the court determines to be appropriate.
- (3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.
- (4) No liability shall result from lawful disclosure permitted by this section.
- (d) **PERSONALLY IDENTIFIABLE INFORMATION.**—Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.
- (e) **DESTRUCTION OF OLD RECORDS.**—A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.
- (f) **PREEMPTION.**—The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

18 U.S.C. 2702—VOLUNTARY DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS

- (a) **PROHIBITIONS.**—Except as provided in subsection (b) or (c)—
- (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
- (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
- (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
- (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
- (3) **[a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.]** *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 commu-*

nication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such service.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime;

or

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

18 USC § 2703—REQUIRED DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS

[(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to 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) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

[(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—

[(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

[(A) without required notice to the subscriber or customer, 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) by a court of competent jurisdiction; or

[(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

[(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

[(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

[(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

[(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic

transmission from), a subscriber or customer of such remote computing service; and

[(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

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

[(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when 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) by a court of competent jurisdiction;

[(B) obtains a court order for such disclosure under subsection (d) of this section;

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

[(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 such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

[(E) seeks information under paragraph (2).

[(2) A provider of electronic communication service or remote computing service shall 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 utilized;

[(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 to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

[(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.]

(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 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 clause (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 pertaining 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 subpoena, 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.

(d) REQUIREMENTS FOR COURT ORDER.—[A court order for disclosure under subsection (b) or (c)] A court order for disclosure under subsection (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that [the contents of a wire or electronic communication, or] the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

18 USC § 2705—DELAYED NOTICE

[(a) DELAY OF NOTIFICATION.—

[(1) A governmental entity acting under section 2703(b) of this title may—

- [(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or
- [(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.
- [(2) An adverse result for the purposes of paragraph (1) of this subsection is—
- [(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) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).
- [(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.
- [(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—
- [(A) states with reasonable specificity the nature of the law enforcement inquiry; and
- [(B) informs such customer or subscriber—
- [(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
- [(ii) that notification of such customer or subscriber was delayed;
- [(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and
- [(iv) which provision of this chapter allowed such delay.
- [(6) As used in this subsection, the term “supervisory official” means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating

agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

[(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

- [(1) endangering the life or physical safety of an individual;
- [(2) flight from prosecution;
- [(3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- [(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.]

(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(a) 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 1 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 1 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 communications service or remote computing service shall notify the governmental entity that obtained the contents of a communication or information or records under section 2703 of the intent of the provider of electronic communications 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.

