Calendar No. 66

113TH CONGRESS
1st Session

SENATE

REPORT
113–34

ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS ACT OF 2013

MAY 16, 2013.—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 S. 607]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to which was referred the bill (S. 607), a bill to improve the provisions relating to the privacy of electronic communications, having considered the same, reports favorably thereon, with an amendment, and recommends that the bill, as amended, do pass.

CONTENTS

I. BACKGROUND AND PURPOSE OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS ACT OF 2013

A. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS

The Electronic Communications Privacy Act ("ECPA") amended the Omnibus Crime Control and Safe Streets Act to protect against the unauthorized interception of electronic communications. When Senator Leahy introduced ECPA with Senator Mathias on June 19, 1986, he said: "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."[1] For almost three decades, 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 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 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."[2]

At the time that Congress enacted ECPA more than 25 years ago, 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. 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. 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

[1] *See* Cong. Rec., June 19, 1986 at page S7993.
[2] *See* 18 U.S.C. § 2703(d).

reforming the Electronic Communications Privacy Act to reflect the realities of the digital age. The aptly named "Digital Due Process" coalition argued that 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 ECPA reform effort that focused specifically on the perspectives of the Departments of Justice and Commerce on proposed updates to the law.[3] 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 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.

Reform of the Electronic Communications Privacy Act remained a top legislative priority for the Committee during the 113th Congress. On March 18, 2013, Chairman Leahy and Senator Mike Lee introduced the Electronic Communications Privacy Act Amendments Act of 2013, S. 607. The legislation establishes a uniform search warrant requirement for the Government to compel the disclosure of all email content when email is stored with a third-party service provider. This bipartisan privacy legislation seeks 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 legislation is substantially identical to ECPA reform proposal the Senate Judiciary Committee favorably reported in November 2012.

The Committee recognizes that most Americans regularly use email in their professional and personal lives for confidential communications of a business or personal nature. The Committee also recognizes that there is growing uncertainty about the constitutionality of the provisions in ECPA that allow the Government to obtain certain email content without a search warrant.[4] The absence of a clear legal standard 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 in order to ensure the continued vitality of the Fourth Amendment protections for email and other electronic communications content.

The reforms in the bill will better safeguard the privacy of email and other electronic communications while allowing law enforce-

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

[4] In 2010, the United States 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. S*ee United States* v. *Warshak,* 631 F.3d 266, 288 (6th Cir. 2010).

ment to carry out its important mission. The bill contains several important provisions to ensure that the reforms to ECPA do not hinder law enforcement. First, the bill preserves the exceptions to the warrant requirement under existing law. For example under current law, the Government does not need a warrant in an emergency situation involving danger of death or serious physical injury, or when a crime is being committed.[5] Second, to protect the integrity of ongoing investigations, the bill adds a new notice requirement to the law that requires service providers to notify the Government of their intent to inform a customer about a disclosure of electronic communications information at least three business days before giving such notice.

In addition, the bill does not alter the legal authorities that the Government currently uses to obtain electronic communications content in national security matters. Specifically, the bill provides that the search warrant requirement does not apply to 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 (commonly known as "FISA")). The Committee does not intend for the bill to alter other existing statutory authorities pursuant to which the Federal Government collects electronic communications and related information, including surveillance and other intelligence authorities. Accordingly, the bill does not preclude any other legal authorities that permit the acquisition by the United States Government of the contents of wire or electronic communications, or other records or information of a subscriber or customer of any electronic communications service or remote computing service, pursuant to other lawful authorities, including in Title 18 (*e.g.,* chapters 119, 121 or 206), Title 50 (*e.g.,* the Foreign Intelligence Surveillance Act of 1978, as amended), or any other provision of Federal law.

The bill also includes several provisions to help civil enforcement agencies, such as the Federal Trade Commission and the Securities and Exchange Commission, investigate corporate wrongdoing and protect consumers. Section 3 of the bill adds civil discovery subpoenas to the existing tools that the Government may use to obtain non-content information under ECPA. Section 3 of the bill also makes clear that the Government may employ administrative, civil discovery and grand jury subpoena to obtain corporate email and other electronic communications directly from a corporate entity, when such communications are contained on an internal email system.

In addition, the bill preserves the legal tools in existing law for civil enforcement agencies to obtain electronic communications information. For example, the bill preserves the ability for civil enforcement agencies to issue subpoenas to a service provider to compel the disclosure of email account information (*i.e.* non-content information). The bill also preserves the ability of such agencies to compel the target of a civil enforcement investigation to produce electronic communications content information to the Government, including electronic communications content information that is stored with a third party service provider. Lastly, to address con-

[5] *See* 18 U.S.C. 2702(b).

cerns about the potential destruction of evidence, the bill preserves the tools in current law that allow the Government, including civil enforcement agencies, to require a service provider to preserve any evidence in its possession to included stored email content.[6]

The objections to the bill raised in the additional view are misguided and belied by a plain reading of the bill and current law. First, the additional views incorrectly suggest that the bill may adversely impact criminal investigations. As discussed above, current law provides numerous exceptions to the warrant requirement in ECPA to accommodate emergencies, child exploitation matters and other criminal activity.[7] The bill preserves all of these exceptions. The additional views also acknowledge that the well-established exigent circumstances exception to the warrant requirement provides a separate legal ground for the Government to obtain electronic communications information without a warrant in time sensitive situations.[8] The authors provide no support to substantiate their claim that these longstanding authorities are inadequate.

The additional views also incorrectly suggest that the bill would adversely impact the important work of the Securities Exchange Commission and other civil enforcement agencies. As discussed above, under current law, civil enforcement agencies can use subpoenas to among other things—(1) compel the disclosure of stored communications from the targets of their investigations, (2) obtain crucial customer records from service providers and (3) require third-party service providers to preserve any electronic communications information sought by the Government. Contrary to the assertion in the additional views, the bill does not eliminate administrative subpoenas. In fact, the bill augments the subpoena authority of civil agencies by permitting these agencies, for the first time, to use civil discovery subpoenas to obtain records under ECPA. Moreover, creating a broad statutory exception to the warrant requirement for civil enforcement matters would eviscerate the important privacy protections in the bill and in current law. Such an exception would apply to all kinds of civil agencies at the Federal, State and local level, including the Internal Revenues Service. Such an exception could also circumvent the warrant requirement in the bill, by permitting the Government to use information obtained under the civil exception in a related criminal matter. The Securities and Exchange Commission and numerous other civil enforcement agencies have successfully performed their duties by relying upon the civil tools already in the law to acquire stored email content for decades, while complying with the existing warrant requirement in the law for emails that are less than 180 days old. There is no reason to believe that this would not continue to be the case with a uniform warrant requirement for all electronic communications content.[9]

---

[6] *See* 18 U.S.C. 2703(f).

[7] *See* 18 U.S.C. 2702(b)(6), (7) and (8).

[8] *See, e.g., Kentucky* v. *King,* 563 U.S._____ (2011) (exception to warrant requirement applies when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.)

[9] To the extent that the Securities and Exchange Commission requires additional legal authorities to compel the disclosure of information, such authorities should be considered when Congress reviews the laws enacted to govern how that agency investigates and enforces civil regulatory matters. *See, e.g.,* Section 19(c) of the Securities Act of 1934 (15 U.S.C. 77(a), *et seq.*); Section 21(b) of the Securities and Exchange Act (15 U.S.C. 78a, *et seq.*); Section 209(b) of the

Continued

Lastly, the additional reviews raise the prospect of adding a statutory time limit to the bill. There is universal agreement on the Committee that service providers should provide timely responses to requests from law enforcement when proper legal process has been obtained. The Committee believes that the courts, which have familiarity with the specific facts and circumstances of particular investigation, are in the best position to address such timeliness issues.[10] Therefore, the bill appropriately recognizes the longstanding practice of leaving such case-by-case decisions to the courts.[11]

The carefully balanced ECPA reforms in the bill have bipartisan support on the Committee, as well as the support of a broad coalition of more than 100 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, the Chamber of Commerce, eBay, Facebook, IBM, LinkedIn, Microsoft, 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 Heritage 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: William K. Sessions, Former Director of the Federal Bureau of Investigation (1987–1993); 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).

Investment Advisers Act (15 U.S.C. 80b–1, *et seq.*); and Section 42(b) of the Investment Company Act (15 U.S.C 80a–1, *et seq.*).

[10] A statutory time limit imposed by Congress could be very harmful to law enforcement, because such a requirement could cause communications service providers make disclosures to the Government based upon a "first come, first served" basis, without regards to the specific facts and needs of law enforcement in particular case.

[11] The additional views also propose that the Committee examine other reforms to ECPA, including clarifying the legal standard for law enforcement to access geolocation information. In May 2011, Chairman Leahy introduced legislation to update ECPA to address geolocation information and other electronic privacy issues. The Committee held two hearings on these forms and the Committee will continue to work on these issues.

II. History of the Bill and Committee Consideration

A. INTRODUCTION OF THE BILL

On March 18, 2013, Senators Leahy and Lee introduced S. 607—the Electronic Communications Privacy Act Amendments Act of 2013.

B. COMMITTEE CONSIDERATION

Chairman Leahy placed S. 607 on the Committee's executive business agenda on April 18, 2013. The Committee considered and favorably reported this legislation on April 25, 2013.

The Committee has held two hearings related to S. 607. 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 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.

In addition, on November 29, 2012, the Committee considered and favorably reported legislation substantially similar to S. 607 as part of H.R. 2471, the Video Privacy Protection Act Amendments Act of 2012.

On April 25, 2013, the Senate Judiciary Committee favorably reported S. 607 with the following two amendments:

First, Chairman Leahy offered a technical amendment to the bill to make technical corrections to the rule of construction language in the bill at the request of the Department of Justice. The changes further clarify that the bill does not apply to, or alter, any other Federal criminal or national security laws that authorize the United States Government to collect, or acquire, wire or electronic communications—or related records—including the surveillance and other intelligence authorities contained in the Wiretap Act (Chapter 119 of Title 18) and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, *et seq.*). The Committee unanimously adopted the amendment by voice vote.

Second, Senator Grassley offered an amendment to require that the Comptroller General of the United States conduct a study and report to Congress by September 30, 2015 on how ECPA is cur-

rently being applied, including the extent to which law enforcement is relying upon section 2703 of ECPA to obtain information in criminal matters, and how the law will be affected by the new warrant requirement in the bill. The Committee unanimously adopted the amendment by voice vote.

The Committee then voted to report the Electronic Communications Privacy Act Amendments Act of 2013, as amended, favorably to the Senate by voice vote.

III. Section-by-Section Summary of the Bill

The Leahy-Lee Electronic Communications Privacy Act Amendments Act would update the privacy protections for Americans' email and other electronic communications for the digital age. The Electronic Communications Privacy Act (ECPA) is one of the nation's premier digital privacy laws. After three decades, ECPA has become outdated by vast technological advances and changing law enforcement missions since the law's initial enactment. The bill would update this law to improve the privacy protections for electronic communications information that is stored or maintained by third-party service providers. The bill maintains the careful balance that Congress struck when it first enacted the law—to continue to protect and promote consumer privacy interests, law enforcement needs, and American innovation in the digital age.

Section 1. Short title

This section designates the Act as the Electronic Communications Privacy Act Amendments Act of 2013.

Section 2. Confidentiality of electronic communications

Section 2 amends Title 18, United States Code, Section 2702 (the Electronic Communications Privacy Act or "ECPA") to prohibit an electronic communications or remote computing service provider from voluntarily disclosing the contents of its customers' 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 3. Elimination of 180-day rule; Search warrant requirement for content; Required disclosure of customer records

Section 3 amends 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 for a law enforcement agency, and three business days for other agencies, of a Government entity's receipt of the communications unless the notice is delayed pursuant to Section 4 of the bill.

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 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 3 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.

Lastly, the section contains a rule of construction regarding Government access to internal corporate email that makes clear that nothing in the bill precludes the Government from using a subpoena to obtain email and other electronic communications content obtained from an intended recipient or original sender, or to obtain such communications directly from a company when the communications are to or from an officer, agent or employee of a company and the company is acting as an electronic communications service provider for its own internal email system.

Section 4. Delayed notice

Section 4 amends section 2705 of 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 4 also establishes a time limit on the period that the Government could preclude a service provider from informing its customer about the disclosure of electronic communications 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. The time period for preclusion may extend up to 180 days if the requesting Government entity is a law enforcement agency. These time periods may also be extended by a court for up to an additional 90 or 180 days at a time, respectively.

Lastly, Section 4 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 5. Evaluation by the Government Accountability Office

Section 5 requires that the Comptroller General of the United States submit a report to Congress by September 30, 2015, that evaluates, among other things, during the five years prior to the effective date of the amendments in the bill—(1) how often law enforcement relied upon section 2703 of ECPA to requests electronic communications content information; (2) the average length of time needed for service providers to comply with such requests; (3) the number of times a warrant was used for such requests; and (4) the number of times law enforcement requested delayed notification pursuant to section 2705 of ECPA. Section 5 also requires that the Comptroller General—(1) the effects of the new warrant requirement contained in the bill on the courts; (2) conduct a survey to determine the average length of time required to respond to requests for information; and (3) determine whether the new warrant requirement in the bill resulted in an increase in the use of the emergency exception to the warrant requirement in section 2702(b)(8) of ECPA.

Section 6. Rule of construction

Section 6 provides that the search warrant requirement for electronic communications content contained in Section 3 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, S. 607, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

MAY 16, 2013.

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 S. 607, the Electronic Communications Privacy Act Amendments Act of 2013.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

S. 607—Electronic Communications Privacy Act Amendments of 2013

S. 607 would amend the Electronic Communications Privacy Act of 1986 (Public Law 99–508) to make several changes to the current laws relating to the privacy of personal electronic communications. The bill also would require the Government Accountability Office (GAO) to prepare a report, by the end of fiscal year 2015,

on service providers' disclosure of customer communications to law enforcement agencies.

Based on the cost of similar activities, CBO estimates that it would cost $1 million to $2 million from appropriated funds over the 2014–2015 period for GAO to prepare the report required by the bill. CBO estimates that other provisions of the bill 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.

S. 607 would impose intergovernmental mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by changing the procedures that governmental 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 ($75 million in 2013, adjusted annually for inflation).

S. 607 also would impose a private-sector mandate by requiring providers of electronic communications and remote computing services to inform the government before they notify a customer or subscriber that they have disclosed information to the government. Based on information from industry sources, CBO estimates that the cost of the mandate would fall well below the annual threshold established in UMRA for private-sector mandates ($150 million in 2013, adjusted annually for inflation).

The CBO staff contacts for this estimate are Mark Grabowicz and Matthew Pickford (for federal costs), Elizabeth Cove Delisle (for the impact on state, local, and tribal governments), and Marin Burnett (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 S. 607.

VI. Conclusion

The bill, as amended, S. 607, 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 AND SESSIONS

AMENDMENTS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ARE NECESSARY BUT SHOULD ALSO ADDRESS THE IMPACT ON LAW ENFORCEMENT, THE COURTS, AND CIVIL REGULATORY AGENCIES

In the 112th Congress, we voted to report virtually the same version of this bill because we believe that the Electronic Communications Privacy Act of 1986 ("ECPA") needs to be updated to match advances in technology. However, we also stated that the bill needed work to better protect email privacy without hampering law enforcement agencies' ability to obtain information in order to investigate serious crimes, as well as civil regulatory agencies' ability to investigate wrongdoing. We expressed concern that the bill did not strike the proper balance, but it was the start of an important discussion. We believe that these changes are important to continue the carefully crafted balance between protecting privacy and providing needed tools to law enforcement.

We find ourselves in the same position in this Congress. We reiterate that the Committee should work to ensure that this balance is continued as we update ECPA for decades to come. First, the Committee should consider whether a more comprehensive approach to updating the laws involving electronic communications and data is warranted. This would include looking to advances in technology for location information in addition to the content of communications. It would also assist in addressing the concerns that have been raised by the law enforcement, technology, and privacy communities. Second, the bill should address the ability of law enforcement to obtain access to critical evidence, especially in time-sensitive emergency cases. Third, and finally, more consideration is needed with regard to the bill's removal of 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.

We appreciate that members on the Committee share these concerns and spoke up at the Committee mark-up to highlight the need for modifications to the current bill. Additionally, we welcome the views of the well-respected Chairwoman of the Securities and Exchange Commission, Mary Jo White. While we support the goal of harmonizing and updating ECPA, failure to address these important issues and strike the proper balance will be detrimental to not just the law enforcement and civil regulatory agencies seeking to obtain necessary information, but to the American people, busi-

nesses, and the court system and may require future action from Congress to update other parts of ECPA.

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 interests 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 current 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" has been 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 therefore treated 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 the content contained in these older emails and related records.[5]

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. However, under the bill 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 en-

---

[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).

[5] On March 19, 2013, while testifying before the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, Acting Assistant Attorney General Elana Tyrangiel testified that the Department of Justice no longer supports differentiating between emails kept in storage for less than 180 days and emails stored for over 180 days. She did not indicate, however, whether the Department had solicited input from the thousands of state and local law enforcement professionals on the front lines prior to offering a view that could adversely impact the course of their investigations.

forcement responsibilities over important industries. But this bill eliminates these administrative subpoenas. Therefore, since civil investigators have no criminal search warrant authority, they would no longer be able to obtain the contents of emails unless a target of an investigation or a charged defendant graciously provides the incriminating email containing the "smoking gun." Civil regulators would then have no ability to compel the disclosure of email content from third party Internet service providers. As a result, the bill raises concerns over civil regulatory agencies' ability to 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 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 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 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.

Demonstrating the need for a comprehensive review, the bill is silent regarding the use of ECPA to obtain data regarding location information data. Increasingly, judges across the country are examining whether ECPA allows law enforcement to obtain location information data obtained from a handheld device or from cellular site towers. The Committee on the Judiciary in the House of Representatives recently held a hearing to address this exact question.[6] This hearing examined the different legal tools law enforcement utilizes to obtain stored, prospective, or real-time geolocation information. Specifically, the hearing focused on the different statutes employed to obtain this information, including the use of ECPA, 2703(d) orders, pen registers, and combinations of these various authorities.[7] The testimony at the hearing discussed the need for Congress to bring clarity to ECPA and companion statutes to address the splits among the various federal courts as part of any ECPA reform effort. This bill does not include such endeavors and as a result, does not examine ECPA in a comprehensive manner. The Committee should follow the lead of the House Judiciary Committee and examine these important issues to ensure that the proper balance is struck with regard to all aspects of ECPA, including geolocation.

The amendment may adversely affect criminal investigations

Law enforcement representatives have raised concerns that increasing the legal standard to require a criminal search warrant

[6] *See* The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance Before the H. Comm. on the Judiciary, 113th Cong. (April 25, 2013).
[7] *Id.* (Statement of Mark Eckenwiler, Senior Counsel, Perkins Coie LLP).

for the content of all email communications regardless of the length of time they have been in electronic storage will hinder and delay criminal investigations.[8] 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 bill, 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 bill does not address the current standard in Section 2702(b) of Title 18, United States Code on emergency disclosures. This section merely requires service providers 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 bill *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.

Some members of the Committee have stated that the traditional "exigent circumstances" to the Fourth Amendment would be sufficient to permit investigators to seize the electronic communication information without a warrant. Despite assurances from supporters of the bill that the traditional exigent circumstances exception

[8] *Id.* at 2; Letter from the MCCPA, et al., to Chairman Leahy & Ranking Member Grassley, *supra* note 7, at 2–3.

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.[9] 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.[10] Unfortunately, the Committee never held a hearing, heard witnesses or reviewed evidence, or even had the opportunity to debate this important question.

But even assuming *arguendo* that traditional Fourth Amendment exceptions apply, the exigent circumstances exception to the warrant requirement would not be helpful in obtaining email content because the bill leaves law enforcement officials at the mercy of the service providers, even in an emergency. 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 some law enforcement concerns and might help recalibrate ECPA so that there is better balance between privacy and public safety.

Finally, 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 bill 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.

---

[9] *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).

[10] *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").

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 bill, 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 bill 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, Securities and Exchange Commission Chairwoman Mary Jo White recently sent a letter to the Committee outlining her concerns that the SEC will be unable to obtain critical emails necessary to investigate civil securities fraud statutes. Specifically, she wrote that the legislation, in its current form, could have an impact on the Commission's "ability to protect investors and to assist victims of securities fraud." [11]

Chairman White's letter also argues that the proposed "workarounds" that have been suggested would be inadequate. For example, some argue that the solution is to simply obtain emails from the targets of the investigation.[12] Chairman White argues that often time these individuals delete relevant emails or otherwise fail to provide them despite obtaining a subpoena.[13] As a result, the Chairman White fears that this could embolden non-compliance with subpoenas by targets of investigations.[14]

Additionally, Chairman White argues against those who say the SEC could simply work with the Justice Department to obtain a warrant.[15] She notes that, "the Commission cannot request that the DOJ apply for a search warrant on the SEC's behalf." Further, she adds that the vast majority of cases investigated by the SEC are not criminal and therefore would be outside the scope of ability to obtain a warrant—effectively limiting enforcement.[16]

To remedy this, Chairman White advocates for an amendment to allow a judicial standard for civil matters akin to a criminal search warrant.[17] This is an idea worth considering as we move forward. It would still require a ruling from a judge of a competent jurisdiction, similar to what we will allow for criminal cases under this bill, while retaining the protections provided in this bill.

The 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

---

[11] Letter from SEC to U.S. Senate Judiciary Committee Chairman Leahy (April 24, 2013) (attached in appendix).
[12] *Id.* at 2–3.
[13] *Id.*
[14] *Id.*
[15] *Id.* at 2.
[16] *Id.*
[17] *Id.* at 3.

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 alleging 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 of his personal email account in response to a subpoena issued to him almost 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.

Conclusion

We agree that ECPA reform is needed to address the dramatic advances to technology over the last three decades. We have concerns, however, with the version reported by the Committee. There are very valid concerns raised by the law enforcement community

and civil regulatory agencies and those concerns should be addressed. ECPA is an important privacy law and advances in technology warrant an update. However, in addition to the changes made for content in this bill, ECPA reform should address some of these other concerns raised to ensure we have 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 so that ECPA reform can be achieved.

CHARLES E. GRASSLEY.
JEFF SESSIONS.

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 S. 607, 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 USC § 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 communication 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.

(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.

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.

○