Congressional Research Service
Informing the legislative debate since 1914

Reform of the Electronic Communications Privacy Act (ECPA)

Richard M. Thompson II
Legislative Attorney

Jared P. Cole
Legislative Attorney

May 15, 2015

Congressional Research Service
7-5700
www.crs.gov
R44036

CRS REPORT
Prepared for Members and
Committees of Congress

c11173008

Summary

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to both protect the privacy of an individual's electronic communications and provide the government with a lawful means for accessing these communications if sufficient process is followed. Although passed at the infancy of the Internet, the Stored Communications Act (SCA), which is part of ECPA, has been interpreted over the years to cover the content of emails, private Facebook messages, YouTube videos, and so-called metadata, or non-content information, connected to our Internet transactions (e.g., websites visited, to/from and time/date stamps on emails).

The scope of the SCA is determined largely by the entities to which it applies, "electronic communication service" (ECS) providers and "remote computing service" (RCS) providers, both terms of art defined in the statute. It does not apply to government access of records directly from the target of an investigation. The SCA has two core components. First, it creates a broad bar against service providers voluntarily disclosing a customer's communications to the government or others, subject to various exceptions, and second, it establishes procedures under which the government can require a provider to disclose customers' communications or records. As to government access, ECPA utilizes a tiered system with different levels of evidence required depending on whether the provider is an ECS or RCS, whether the data sought is content or non-content, whether the email has been opened, and whether advance notice has been given to the customer.

In recent years, ECPA has faced increased criticism from both the tech and privacy communities that it has outlived its usefulness in the digital era and does not provide adequate privacy safeguards for individuals' electronic communications. In light of these concerns, various reform bills have been introduced in the past several Congresses, with three major reform bills pending in the 114th Congress. The Electronic Communications Privacy Act Amendments Act of 2015 (S. 356, H.R. 283) and the Email Privacy Act (H.R. 699), almost identical in text, would, among other things, place both ECS and RCS providers under the same legal requirement; eliminate the current 180-day rule found in the SCA and require a warrant for emails no matter how long they have been stored or whether they have been opened; and remove the reliance on the definition of "electronic storage," which has confused the lower courts. Additionally, the Online Communications and Geolocation Privacy Act (H.R. 656) would make similar changes to the SCA.

Some federal agencies, most prominently the Securities and Exchange Commission (SEC), that currently rely on their subpoena authority to access electronic communications, have argued that these bills would stymie their ability to conduct investigations as they have no legal authority to obtain a warrant. In response to this concern, both the Email Privacy Act and the ECPA Amendments Act include a rule of construction providing that nothing in these bills should be read to preclude the SEC or any other federal agency from seeking these records directly from the target of the investigation, rather than the target's service provider.

Finally, there has been ongoing litigation in the lower federal courts as to ECPA's extraterritorial reach. The Law Enforcement Access to Data Stored Abroad (LEADS) Act (S. 512, H.R. 1174) would require third-party service providers to disclose the contents of U.S persons' electronic communications held overseas upon issuance of a warrant based on probable cause.

Contents

Contacts

Introduction

In 1986, when introducing the Electronic Communications Privacy Act (ECPA), Senator Patrick Leahy observed that the nation's then-existing electronic communications privacy laws were "hopelessly out of date."[1] The Senate Judiciary Committee agreed that the law had "not kept pace with the development of communication and computer technology ... [n]or [had] it kept pace with changes in the structure of the telecommunications industry."[2] Later that year, Congress enacted ECPA, which, at over 25 years old, remains the primary law governing government and private actor access to our stored online communications. It governs, for instance, when the government can demand that Google turn over our emails, when social media sites like Facebook must provide our private posts, when video-sharing sites like YouTube must provide our stored videos, and when our cell phone companies have to turn over cell location information.

In recent years, ECPA has faced increased criticism from both the tech and privacy communities that it has outlived its usefulness in the digital era and does not provide adequate privacy safeguards for individuals' electronic communications. In light of these concerns, various reform bills have been introduced in the past several Congresses, with three major reform bills pending in the 114th Congress. The Electronic Communications Privacy Act Amendments Act of 2015 (S. 356) and the Email Privacy Act (H.R. 699), almost identical in text, would, among other things, place both ECSs and RCSs under the same legal requirement; eliminate the current 180-day rule found in the Stored Communications Act (SCA) and require a warrant for emails no matter how long they have been stored or whether they have been opened; and eliminate the reliance on the definition of "electronic storage," which has confused the lower courts. Additionally, the Online Communications and Geolocation Privacy Act (H.R. 656) would make similar changes to the SCA.[3]

Some federal agencies, most prominently the Securities and Exchange Commission (SEC), that currently rely on their subpoena authority to access electronic communications, have argued that these bills would stymie their ability to conduct investigations as they lack legal authority to obtain a warrant. In response to this concern, both the Email Privacy Act and the ECPA Amendments Act include a rule of construction providing that nothing in these bills should be read to preclude the SEC or any other federal agency from seeking these records directly from the target of the investigation, rather than the target's third- party service provider.

Finally, there has been ongoing litigation in the lower federal courts as to ECPA's extraterritorial reach. The Law Enforcement Access to DATA Stored Abroad (LEADS) Act would require third-party service providers to disclose the contents of U.S persons' electronic communications held overseas upon issuance of a warrant based on probable cause.[4]

This report provides an overview of ECPA reform. It will first outline the background and history of the legal environment prior to ECPA and the problem precipitating ECPA's passage. It will then survey the current legal framework for accessing electronic communications and other non-

[1] 132 Cong. Rec. 14608 (1986).

[2] S. Rept. 99-541, at 2.

[3] H.R. 656, 114th Cong. (2015).

[4] S. 512, 114th Cong. (2015); H.R. 1174, 114th Cong. (2015).

content information from providers, and describe specific types of data accessible under ECPA. Finally, it will explore the various bills that would amend ECPA, including selected legal issues raised by these measures.

Background of ECPA

Before passage of ECPA in 1986, government access to private electronic communications was governed primarily by the Fourth Amendment and the federal wiretap law. In 1967, the Supreme Court issued two landmark Fourth Amendment cases. In *Katz v. United States*, the Court held that the Fourth Amendment's prohibition against "unreasonable searches and seizures" entitles individuals to a reasonable expectation of privacy in their private communications.[5] In *Berger v. New York*, the Court struck down a New York wiretap law that failed to include adequate safeguards for the privacy interests of those whose communications were being "tapped."[6]

One year later, in an effort to regulate wiretapping while also giving law enforcement a lawful means for intercepting telephone conversations, Congress enacted the "Wiretap Act" as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[7] Title III prohibits the unauthorized interception and disclosure of wire or oral communications, while simultaneously providing a procedure for law enforcement to conduct such interceptions upon judicial approval.[8] However, Title III only covered the "aural" interception of wire or oral communications—the interception of actual sounds—that are interpreted by hearing, and not sight.[9] This left largely unregulated the transfer of digital communications.[10]

This legal uncertainty as to whether new digital forms of communication would be covered by Title III or other federal law prompted the introduction of the original version of ECPA in 1985.[11] Foreshadowing arguments made by proponents of ECPA reform today, the Senate Judiciary Committee observed at the time that this gap in coverage could stifle American technological innovation, expose law enforcement to liability, allow the erosion of American privacy rights, and jeopardize the admissibility of probative evidence in criminal prosecutions.[12] One year later Congress enacted ECPA.[13]

---

[5] *See* U.S. CONST. amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); Katz v. United States, 389 U.S. 347, 359 (1967).

[6] Berger v. New York, 388 U.S. 41, 63-64 (1967).

[7] Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, 801, 82 Stat. 197, 212.

[8] See 18 U.S.C. § 2511.

[9] *See* United States v. New York Telephone Co., 434 U.S. 159, 166-67 (1977); United States v. Seidlitz, 589 F.2d 152, 157 (4th Cir. 1978) ("The words 'aural acquisition' literally translated mean to come into possession through the sense of hearing.") (quoting Webster's Third New International Dictionary, 1967 ed.)).

[10] *See* OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 46 (1985).

[11] *Id.* at 21.

[12] S. Rept. 99-541, at 5.

[13] Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1868.

ECPA's Framework

ECPA contains three main titles. Title I updated the Wiretap Act to include not only the interception of oral and wire communications, but also electronic communications.[14] Title III created new rules regulating the use of a pen register, a device that allows users to capture the routing information associated with communications, such as telephone numbers dialed or the to/from address in an email.[15] Title II added Chapter 121 to the *United States Code* entitled "Stored Wire and Electronic Communications and Transactional Records Access," commonly referred to as the Stored Communications Act (SCA).[16] As technology has developed, law enforcement has relied less frequently on real-time interception authorized under the Wiretap Act, and has instead relied on its authority under the SCA—accessing stored electronic communications, such as emails directly from a service provider.[17] This shift explains why reform of ECPA has centered almost entirely on the SCA.

The scope of the SCA is determined largely by the entities to which it applies. First, it does not apply to personal users, but only to providers of an "electronic communication service" (ECS) and a "remote computing service" (RCS).[18] A provider of ECS allows its customers "to send or receive wire or electronic communications."[19] A provider of RCS provides "computer storage or processing services by means of an electronic communication system."[20] Although these definitions can be confusing in the abstract, they make more sense when applied.

The SCA has two core components: (1) a broad prohibition against providers voluntarily sharing customers' communications with the government or others, subject to certain enumerated exceptions,[21] and (2) procedures permitting the government to require the disclosure of customers' communications or records.[22]

As to the first component, under 18 U.S.C. § 2702(a)(1), a provider of ECS to the public "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage."[23] The importance of the definition of "electronic storage" will be discussed below.[24]

Section 2702(a)(2) provides that a provider of RCS to the public shall not knowingly disclose the contents of a communication which is carried or maintained by that service.[25] There are two other conditions that must be met in order for a communication to remain protected under subsection (a)(2). First, the communication must be maintained "on behalf of, and received by means of

[14] 100 Stat. 1848.

[15] 100 Stat. 1868.

[16] 100 Stat. 1860.

[17] *See* Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 394 (2014).

[18] *See* 18 U.S.C. § 2702(a)(1)-(2).

[19] 18 U.S.C. § 2510(15).

[20] *Id.* § 2711(2).

[21] *Id.* § 2702.

[22] *Id.* § 2703.

[23] *Id.* § 2702(a)(1).

[24] *See infra* note 35 and accompanying text.

[25] *Id.* § 2702(a)(2).

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."[26] Second, the communication must be maintained "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."[27] Although there appears to be little case law interpreting this second condition, it would appear that an RCS which is permitted to access the contents of a communication for purposes other than storage or computer processing—for example, advertising—would not be subject to the prohibition on disclosing the contents of communications.[28] In essence, it acts as an additional exception to nondisclosure.

Section 2702(a)(3) prohibits a provider of ECS or RCS to the public from disclosing a "record or other information pertaining to a subscriber to or customer of such service (not including the contents of a communication covered by paragraph (1) or (2)) to any governmental entity."[29] Note that this rule, which concerns non-content or "metadata," does not apply to nongovernmental, private entities. This permits companies to share non-content information with other private entities, insofar as the SCA is concerned. There may be other federal or state laws prohibiting disclosures of particular classes of information.[30]

Section 2702(b) provides exceptions to the *permissible* disclosure of the *content* of communications covered by the prohibitions in subsection (a), including to an addressee or intended recipient of a communication, as authorized under Section 2703; as may be necessary incident to the rendition of the service or the protection of the rights of property of the provider of that service; or 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.[31] Section 2702(c) provides similar exceptions for the disclosure of *non-content* information, including as authorized under Section 2703; with the lawful consent of the customer or subscriber; and to any person other than a governmental entity.[32]

The second major component of the SCA is the rules concerning *required* disclosure of customer communications and records. Section 2703 sets up a tiered system with different standards that apply depending on whether an ECS or RCS is holding the record, whether the data sought is content or non-content, whether the email has been opened, and whether advanced notice has been given to the customer. An interesting aspect of this tiered system is that the government may use greater process when lesser process would satisfy the statute—for instance, the government may use a warrant when a subpoena would suffice.[33]

---

[26] *Id.* § 2702(a)(2)(A).

[27] *Id.* § 2702(a)(2)(B).

[28] *See* Juror Number One v. Superior Court, 206 Cal. App. 4th 854 (2012).

[29] *Id.* § 2702(a)(3).

[30] *See, e.g.*, Right to Financial Privacy Act, 12 U.S.C. § 3401; Video Privacy Protection Act, 18 U.S.C. § 2710; Family Educational Rights and Privacy Act of 1978, 20 U.S.C. § 1232g.

[31] *Id.* § 2702(b).

[32] *Id.* § 2702(c).

[33] Orin K. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1220 (2004).

At the highest level, Section 2703(a) requires the government to obtain a warrant if it seeks access to the *content* of a communication from an ECS provider that has been in "electronic storage" for 180 days or less.[34] Moving down a tier, if the communication has been stored for longer than 180 days, or if it is being "held or maintained" by an RCS "solely for the purpose of providing storage or computer processing services," the government can use a subpoena or a court order under Section 2703(d) so long as notice is provided to the customer at some point.[35] Section 2703(d) orders require the applicant to prove "specific and articulable facts, showing that there are reasonable grounds to believe that the contents of a[n] ... electronic communication ... are relevant and material to an ongoing criminal investigation."[36]

While Section 2703 facially permits government access to the contents of emails stored more than 180 days or those no longer in electronic storage, a 2010 ruling from the Sixth Circuit Court of Appeals calls into question the constitutional validity of this provision. In *United States v. Warshak*, the government accessed 27,000 emails directly from the suspect's ISP with a subpoena under Section 2703(b) and an ex parte order under Section 2703(d).[37] The Sixth Circuit held that such access was unlawful under the Fourth Amendment as subscribers enjoy "a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'" and "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[38]

In addition to the content of communications, the SCA permits access to non-content information with a warrant, but the government may also use a subpoena or a Section 2703(d) order without having to provide the customer notice.[39] To access basic subscriber information, including the customer's name, address, phone number, length of service, and means of payment (including bank account numbers), the government may follow the more stringent requirements for obtaining a warrant or a Section 2703(d) order, but can also use an administrative subpoena, which requires no prior authorization by a judicial officer.[40]

With forced government disclosures under Section 2703, much hinges on whether a communication is held in "electronic storage."[41] "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[42] Emails that are pending delivery or have not been opened are considered to be in "temporary, immediate storage," thus,

---

[34] 18 U.S.C. § 2703(a).

[35] Section 2705, Title 18, permits delayed customer notice under some circumstances.

[36] *Id.* § 2703(d). A §2703(d) order is similar to the *Terry* rule applied to law enforcement stop and frisks, which requires less than probable cause to believe a crime has been committed, but more than a mere hunch. Terry v. Ohio, 392 U.S. 1, 21 (1968).

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

[38] *Id.* at 288.

[39] 18 U.S.C. § 2703(c). Non-content information such as the to/from line in emails is generally not protected under the Fourth Amendment. *See* United States v. Forrester, 521 F.3d 500, 509 (9th Cir. 2007).

[40] 18 U.S.C. § 2703(c).

[41] *See* 18 U.S.C. § 2703(a) ("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.... ") (emphasis added).

[42] 18 U.S.C. § 2510(17).

are considered in "electronic storage."[43] Once emails are opened, however, they are no longer in "temporary, intermediate storage."[44]

Lower federal courts have taken different approaches in determining whether opened emails could be considered stored for "backup purposes" as provided in subsection (B). Some courts have held that opened emails can *never* fall within the definition of "electronic storage," as the term "backup protection" in subsection (B) was only intended to cover the protection of communications in the event the email system crashed before transmission was complete.[45] The district court in *United States v. Weaver* provided a more nuanced analysis when addressing whether opened emails left solely on a Hotmail account, a "web-based email system[]," could nonetheless be considered stored for "backup purposes."[46] The district court observed that because the emails were never downloaded by the user, but instead were solely stored on Microsoft's servers, Microsoft could not be considered as storing them for backup purposes.[47] Instead, Microsoft was "maintaining the messages 'solely for the purpose of providing storage or computer processing services to such subscriber or customer.'" In contrast, the Ninth Circuit Court of Appeals held in *Theofel v. Farey-Jones* that emails left on a service provider's server after users downloaded them through their workplace email program could be considered stored for "backup purposes."[48] The rationale was that the email left on the server after delivery provided a "second copy" in case the customer needed to download it again. However, the court noted that "prior access" to the emails was "irrelevant," and that the appropriate inquiry is whether "the underlying message has expired in the normal course."[49] This seemingly fact-intensive inquiry has been called into question as "quite implausible and hard to square with the statutory text."[50] In any event, several of the major ECPA reform proposals would expand ECPA's reach and rely less on the definition of "electronic storage" for determining which statutory safeguards would apply.[51]

The lower federal courts have held that the SCA applies to the disclosure of various electronic communications and associated data, including

- Emails[52]
- Text messages[53]

[43] Fraser v. Nationwise Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Penn. 2001) ("It is clear that the Stored Communications Act covers a message that is stored in intermediate storage temporarily, after the message is sent by the sender, but before it is retrieved by the intended recipient."); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511-12 (2001).

[44] *See In re DoubleClick Inc.*, 154 F. Supp. 2d at 512.

[45] *Fraser*, 135 F. Supp. 2d at 636; Lazette v. Kulmatycki, 949 F. Supp. 2d 748 (2013).

[46] United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009).

[47] *Id.* at 772.

[48] Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003).

[49] *Theofel*, 359 F. 3d at 1076.

[50] Kerr, supra note 29, at 1217.

[51] *Compare* 18 U.S.C. § 2703 ("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*.... "), *with* S. 356, § 3, H.R. 699, § 3, S. 512, § 3, H.R. 1174, § 3 ("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.... ").

[52] *See Theofel*, 359 F. 3d at 1077.

- Social media private messages, wall postings, and comments[54]
- Private YouTube videos[55]
- Historical cell site location information[56]

While access to these various categories of electronic data is subject to the SCA, the protections accorded to each differs depending on how long the data has been stored, whether the communication has been accessed by the user, and whether the data is considered content or non-content. For instance, in *Quon v. Arch Wireless Operating Co., Inc.*, the Ninth Circuit held that the provider of text messaging services was operating as an ECS and that text messages stored by the company were in "electronic storage."[57] Under this reading, a warrant would be required to access text messages stored 180 days or less, and lesser process would be required if the messages were stored longer than 180 days. On the other hand, in *Viacom Intern. v. YouTube Inc.*, YouTube was considered an RCS with respect to private videos stored on its site, and therefore would be subject to the lower "specific and articulable facts" standard found in Section 2703(d).[58] To a certain extent, the various ECPA reform bills attempt to eliminate some of these distinctions and would generally require a warrant to access any electronic communications.

Finally, ECPA outlines when the government must provide notice to customers when their communications have been disclosed to the government. If the government seeks the contents of an electronic communication stored by an ECS, notice must be provided as required under Federal Rule of Criminal Procedure 41.[59] If the government seeks access to the contents of electronic communications from an RCS under a Section 2703(d) order or an administrative subpoena, prior notice must be given to the customer. Additionally, the government can seek delayed notice under 18 U.S.C. § 2705.[60]

(...continued)

[53] *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 901 (9th Cir. 2008).

[54] *See* Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 980, 989 (C.D. Cal. 2010).

[55] *See* Viacom Intern. Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

[56] *See*, *e.g.*, *In re* Application of the United States of America for Historical Cell Site Data, 724 F. 3d 600 (5th Cir. 2013); United States v. Davis, No. 12-12928 (11th Cir. May 5, 2015). There is a split in the lower courts whether the SCA combined with the pen register/trap trace statute (18 U.S.C. § 3123) permits access to *prospective or real-time* cell site information without a probable cause warrant. *Compare In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) (rejecting hybrid theory), *with In re*: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006) (accepting hybrid theory). There also appears to be a split in the lower courts whether the government can access so-called "cell tower dumps" under § 2703(d). A cell tower dump request is one in which the government does not seek access to data associated with a particular cell phone number, but rather access to data associated with *all* cell activity recorded by particular cell towers. *Compare In re* Application for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 678 (S.D. Tex. 2013) (rejecting access to cell tower dumps under § 2703(d), *with* In the Matter of Application for Cell Tower Records Under 18 U.S.C. § 2703(d), No. H-15-136M, 2015 WL 1022018, *4 (S.D. Tex. March 9, 2015) (permitting access to cell tower dumps for ten minute period under § 2703(d)).

[57] *See Quon*, 529 F.3d at 902, *rev'd on Fourth Amendment grounds* Quon v. City of Ontario, 560 U.S. 746 (2010).

[58] *See Viacom Intern. Inc.*, 253 F.R.D. at 264.

[59] 18 U.S.C. § 2703(a).

[60] 18 U.S.C. § 2705.

ECPA Reform Legislation

In recent years, ECPA has faced increased criticism from both the tech and privacy communities that it has outlived its usefulness in the digital era and does not provide adequate privacy safeguards for individuals' electronic communications. In March 2010, a group of tech companies, privacy advocates, and academics urged Senator Leahy, then-chairman of the Senate Judiciary Committee, to introduce legislation to bring federal electronic communications privacy laws into the digital era.[61] In light of these and other concerns, ECPA reform has seen increased legislative attention in the past few Congresses.

In May 2011, Senator Leahy filed the Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011), which would have, among other things, required law enforcement to obtain a warrant before accessing the content of any electronic communication, no matter how long it had been stored or whether it had been retrieved by the recipient.[62] The following year, Senator Leahy offered this part of his ECPA bill as an amendment to a video privacy protection bill (H.R. 2471) that was being reported out of the Senate Judiciary Committee.[63] These provisions were ultimately removed from the bill and were never enacted. Representative Yoder's Email Privacy Act (H.R. 1852), introduced in the 113th Congress and nearly identical to Senator Leahy's reform bill, obtained a majority of the members of the House as co-sponsors (272), but was not acted on by the full House.[64] In the spring of 2013, the Senate Judiciary Committee favorably reported Senators Leahy and Lee's ECPA Amendments Act of 2013 (S. 607) to the full Senate, but it was never taken up by the full body. The ECPA Amendments Act of 2015 (S. 356, H.R. 283)[65] and the Email Privacy Act (H.R. 699)[66] were re-introduced in the 114th Congress. Similar to the past Congress, the Email Privacy Act has obtained a majority of the members of the House as co-sponsors (261). The Online Communication and Geolocation Protection Act, which would make similar amendments to ECPA, was introduced in the 113th (H.R. 983)[67] and 114th (H.R. 656)[68] Congresses. A competing bill, the Law Enforcement Access to Data Stored Abroad (LEADS) Act (S. 512, H.R. 1174), which covers, among other things, the extraterritorial reach of ECPA warrants, was first introduced in the 113th Congress[69] and has been re-introduced in the 114th Congress.[70]

[61] S.Rept. 113-64, 2-3 (2013); *see* Digital Due Process, http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

[62] *See* S. 1011, 112th Cong. (1st Sess. 2011).

[63] H.R. 2471, 112th Cong. (2011).

[64] H.R. 1852, 113th Cong. (2013).

[65] S. 356, 114th Cong. (2015).

[66] H.R. 699, 114th Cong. (2015).

[67] H.R. 983, 113th Cong. (2013).

[68] H.R. 656, 114th Cong. (2015).

[69] S. 2871, 114th Cong. (2014).

[70] S. 512, 114th Cong. (2015); H.R. 1174, 114th Cong. (2015).

ECPA Amendments Act of 2015 (S. 356, H.R. 283) and the Email Privacy Act (H.R. 699)

Section 2 of S. 356, H.R. 283, and H.R. 699 would amend Section 2702(a)(3) of ECPA to provide that both an ECS and an RCS would be prohibited from voluntarily disclosing to a governmental entity the content of any communication and any non-content information such as subscriber information or other communications metadata. This blanket prohibition is subject to various exceptions under existing law, including required disclosure to the government under Section 2703.[71]

Section 3 of these bills contains three major reforms to accessing the *content* of communications under ECPA. First, it would place both an ECS and RCS under the same legal requirements. Second, they would eliminate the current 180-day rule found in Section 2703(a). Again, under Section 2703(a) as currently written, emails stored for 180 days or less are subject to the warrant requirement, while emails either opened or stored for more than 180 days are subject to less stringent process.[72] These bills would eliminate this temporal requirement; thus, access to emails would require a warrant no matter how long they have been stored. Third, this section would remove the interpretive difficulty of determining whether a particular communication is in "electronic storage." Recall that federal courts have disagreed whether an opened email was being held in "electronic storage."[73] This bill expands the scope of protection to include not only messages in "electronic storage," but also those "stored, held, or maintained by the provider." This would appear to bring any opened emails under the warrant umbrella.

As under existing law, the government would be authorized to access *non-content* information, described as a "record or other information pertaining to a subscriber or customer," with a warrant, a Section 2703(d) order, consent of the subscriber, or upon a formal written request if the crime being investigated is telemarketing fraud. The government would be authorized to access basic subscriber information—such as name, address, local and long distance telephone records, and means and source of payment—with a warrant, a Section 2703(d) order, or with lesser process such as a federal or state administrative subpoena, a grand jury, a trial, or a civil discovery subpoena. The authorization to use a *civil discovery* subpoena is the only new authority that this subsection would add to current law.

These bills would also alter when notice must be provided to a customer whose communications are disclosed to the government. Under the current system, customers need not be notified when the government uses a warrant to access the content of their communications from an ECS. To require the disclosure of an email that has been opened or stored for more than 180 days, the government can use lesser process than a warrant, but must provide notice to the customer. Under the proposed legislation, the government would be required to provide the customer notice if it accesses the contents of electronic communication from either an RCS or an ECS no matter if it has been stored for more than 180 days or has been opened. If the government entity accessing the information is law enforcement, it would have 10 days to give notice; all other governmental entities would have 3 days. These bills also include a provision permitting applicants for a

[71] *See supra* notes 31-32 and accompanying text.

[72] *See* "ECPA Framework," *supra* p. 3.

[73] *Compare* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 634 (E.D. Pa. 2001), *with* United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009).

disclosure order to request that notification be delayed. If the government entity accessing the information is law enforcement, it can request a delay of not more than 180 days; all other governmental entities can request a delay of not more than 90 days.

Online Communication and Geolocation Protection Act (H.R. 656)

Like the Email Privacy Act and the ECPA Amendments Act, the Online Communication and Geolocation Protection Act (H.R. 656) would eliminate the different legal treatment given to information held by an RCS and ECS; would eliminate the 180-day rule provided under current law; and would expand the scope from communications held in "electronic storage," to those "stored, held, or maintained by that service."[74] There are, however, differences between the other reform bills and H.R. 656. First, H.R. 656 would require that any governmental entity receiving the contents of a communication provide notice to the customer within three days of receiving such information. The Email Privacy Act and ECPA Amendments Act, on the other hand, give a law enforcement agency 10 days and any other governmental entity 3 days to provide notice. (Note that delayed notice would still be permitted under Section 2705.) Second, unlike the other reform bills, H.R. 656 would not extend access to non-content information under Section 2703(c) with a civil discovery subpoena. Third, H.R. 656 does not include a "rule of construction" that is included in the other reform bills,[75] that states that nothing in the bills should be construed to prohibit the government from seeking electronic communication records directly from a target of an investigation as opposed to a service provider.

Administrative Subpoenas

While the various ECPA reform bills discussed above appear to enjoy broad support among tech, civil liberty, and government constituencies,[76] some federal agencies have argued that passage of these bills would significantly curtail their ability to conduct investigations. In an apparent effort to assuage these concerns, the Email Privacy Act, the ECPA Amendments Act, and the LEADS Act include a "rule of construction" noting that these agencies can still seek electronic communications directly from the target of their investigation.

Currently, many federal agencies possess subpoena authority which allows them to compel the production of documents from providers without prior approval of a court.[77] Pursuant to Section

[74] H.R. 656, 114th Cong. (2015).

[75] *See infra* note 91 and accompanying text.

[76] *See*, *e.g.*, Letter to Senate Judiciary Committee from Coalition of Companies and Organizations (January 22, 2015), *available at* https://cdt.org/insight/letter-to-senate-judiciary-committee-in-support-of-ecpa-amendments-act/; BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, EXECUTIVE OFFICE OF THE PRESIDENT 66 (2014) ("Congress should amend ECPA to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world—including by removing archaic distinctions between email left unread or over a certain age."); *ECPA Part 1: Lawful Access to Stored Content: Hearing Before the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 4 (2013) (statement of Elana Tyrangiel, Acting Assistant Attorney General, Office of Legal Policy) ("Many have noted—and we agree—that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.").

[77] *See* Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and (continued...)

2703(b), federal agencies have issued subpoenas to service providers to obtain subscriber information about individuals, including their names, telephone numbers, email addresses, and physical addresses,[78] and have indicated that they have used this authority to obtain the content of emails held by service providers for more than 180 days.[79]

Administrative subpoenas are subject to a lower evidentiary standard than the probable cause threshold required to obtain a warrant.[80] Courts reviewing such subpoenas, whether in response to a motion to quash the subpoena or at the behest of the agency seeking to enforce the subpoena in court, do so under the Fourth Amendment's general protection against unreasonableness.[81] The Supreme Court has explained that in order for such subpoenas to be upheld: (1) the investigation must be for a legitimate purpose, (2) the materials sought must be relevant to the purpose, (3) the agency must not already possess the information, and (4) the agency must have followed the proper procedural steps.[82] The Court has also indicated that information sought must be "reasonably relevant" to the investigation,[83] and "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[84] The relevancy standard is a relatively low evidentiary threshold. In the grand jury context, the Court has observed that a subpoena will be quashed on relevancy grounds only when a court finds that there is "no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject" of the investigation.[85]

Generally, federal district courts have a duty to enforce proper subpoenas and may not restrict their scope unless they are "plainly incompetent or irrelevant to any lawful administrative purpose."[86] The Supreme Court has made clear that agencies are not required by the Constitution to notify the target of an investigation when subpoenaing information from third parties.[87] In response to a subpoena, a target may raise privileges to protect information from disclosure, such as the attorney-client and work-product privileges.[88]

All of the major ECPA reform bills would require a warrant to obtain the contents of electronic communications held by service providers, whether held for more or less than 180 days. One

---

(...continued)

Entities, U.S. Dep't of Justice, Office of Legal Policy.

[78] *See, e.g.*, United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010).

[79] *See* Letter from Mary Jo White, SEC Commissioner, to Senator Patrick J. Leahy, Chairman of the Senate Judiciary Committee (April 24, 2013).

[80] *See* United States v. Powell, 379 U.S. 48, 57-58 (1964); U.S. CONST. amend. IV.

[81] *See* Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946) ("The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable."); Doe v. United States, 253 F.3d 256, 263 (6th Cir. 2001); *In re* Subpoena Duces Tecum, 228 F.3d 341, 347 (4th Cir. 2000).

[82] *See* United States v. Powell, 379 U.S. 48, 57-58 (1964). *But see* United States v. Bell, 564 F.2d 953, 959 (Temp. Emer. Ct. App. 1977) (requiring only the first two factors in approving an administrative subpoena).

[83] U.S. v. Morton Salt, 338 U.S. 632, 652 (1950).

[84] See v. City of Seattle, 387 U.S. 541, 544 (1967).

[85] United States v. R. Enterprises, 498 U.S. 292, 301 (1992).

[86] Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943).

[87] *See* S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741-42 (1984).

[88] *See, e.g.*, N.L.R.B. v. Interbake Foods, LLC, 637 F.3d 492, 499 (4th Cir. 2011); Director, Office of Thrift Supervision v. Vinson & Elkins, LLP, 124 F.3d 1304, 1306–07 (D.C.Cir. 1997); NLRB v. Harvey, 349 F.2d 900, 907 (4th Cir. 1965).

result of this provision would be that administrative subpoenas—subject to a lower standard of proof than warrants—would no longer be sufficient to compel service providers to produce the contents of electronic communications. However, because most federal agencies—other than the Department of Justice (DOJ)—do not possess independent authority to seek a warrant from a magistrate judge,[89] such legislation would appear to preclude agencies conducting an investigation to obtain the contents of electronic communications held by service providers directly from the provider itself. Instead, in order to do so, agencies would presumably need to rely on the DOJ to seek a warrant, whose authority is limited to doing so in criminal investigations.[90]

However, the Email Privacy Act, the ECPA Amendments Act, and the LEADS Act specify a "rule of construction" which clarifies that agencies may use subpoenas to obtain the contents of electronic communications from an "originator, addressee, or intended recipient."[91] While agencies thus could not use a subpoena to obtain the contents of electronic communications directly from service providers, they may still do so from the individuals who sent or received certain messages. In addition, the rule of construction makes clear that administrative agencies may seek the contents of electronic communications from corporations where the emails are from officers or employees of the corporation and the corporation is serving "as an electronic communications service provider for its own internal email system."[92] So, if Company X provided in-house email services to its employees, the government could seek those communications directly from the company under the SCA.

Legislation requiring a warrant to access the contents of electronic communications held by service providers appears to codify the requirements announced by the U.S. Court of Appeals for the Sixth Circuit in *U.S. v Warshak*.[93] In that case, the DOJ obtained a subpoena under Section 2703(b) compelling the target of a criminal investigation's ISP to turn over the contents of his emails to the government.[94] The Sixth Circuit held that because subscribers have a reasonable expectation of privacy in the content of email "stored with, or sent or received through, a commercial ISP," the government must obtain a warrant based on probable cause to access them.[95]

Nevertheless, at least one federal agency has claimed that the new warrant requirement contained in the reform bills would unduly restrict its investigative authority. The Securities and Exchange Commission (SEC), in a letter to the Senate Judiciary Committee, noted that the targets of agency

---

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

[90] Id. Alternatively, if the agency issued a subpoena directly to an individual compelling the disclosure of the contents of electronic communications held by a service provider, a court might find that those contents were nonetheless within the individual's control and compel their production. *Cf.* Flagg v. City of Detroit, 252 F.R.D. 346, 359 (E.D. Mich. 2008) (finding that text messages held by a service provider were within the defendant's control for the purposes of Federal Rule of Procedure 34 and were subject to disclosure consistent with the SCA); Mintz v. Mark Bartelstein & Associates, Inc., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) ("Because Plaintiff is the 'originator' of his text messages, he may request copies of these messages from AT&T consistent with the SCA. See 18 U.S.C. § 2702(b)(2).").

[91] H.R. 699, § 3, 114th Cong. (2015) ; S. 356, § 3, 114th Cong,; H.R. 283, § 3, 114th Cong. (2015); S. 512, § 3, 114th Cong. (2015); H.R. 1174, § 3, 114th Cong. (2015).

[92] S.Rept. 113-34, at 9 (2013).

[93] 631 F.3d 266, 288 (6th Cir. 2010).

[94] *Id*. at 283.

[95] *Id*. at 288 (quoting Warshak v. United States, 490 F.3d 455, 472 (6th Cir. 2007), reh'g en banc granted, opinion vacated (Oct. 9, 2007)).

investigations do not always "retain copies of their incriminating communications or may choose not to provide the e-mails in response to Commission subpoenas."[96] Accordingly, the letter argued, the SEC has historically relied on authority under Section 2703(b) to obtain the contents of electronic communications from service providers during its investigations. The legislation would foreclose the SEC from doing so in the future, thereby weakening its investigative authority. The letter argued that if the individuals under investigation know that the SEC cannot go directly to the service providers to obtain the contents of emails, then those individuals will be less likely to be forthcoming in response to subpoenas issued directly to them. The letter concluded by suggesting that the legislation be amended by inserting a provision that would allow a federal civil agency to seek the contents of electronic communications from service providers subject to a standard similar to that governing the issuance of criminal search warrants.

However, various civil liberties groups pushed back against this position. In a letter to the SEC, a collection of privacy advocates questioned the necessity of obtaining the contents of electronic communications directly from service providers.[97] First, the letter argued that the agency had not done so since the Sixth Circuit Court of Appeals' 2010 decision in *Warshak*, and had rarely done so prior to that case. Second, the letter pointed to alternative methods of obtaining the contents of email, such as seeking to enforce a subpoena directly on the individual who is the target of an investigation in federal court. In addition, the letter argued that the authority sought by the SEC could lead to abuse. Information obtained via subpoena could be shared with the DOJ in a parallel criminal investigation, thus avoiding the warrant requirement. And the attorney-client privilege could be violated in the collection of personal emails if the target of such a subpoena was not permitted to filter the emails for privileged material. The letter proposed its own amendment to potential legislation, which would clarify that administrative agencies could use subpoenas to require individuals to obtain and disclose information held by a third party.

Law Enforcement Access to Data Stored Abroad Act (LEADS Act) (S. 512, H.R. 1174).

Like the Email Privacy Act, the ECPA Amendments Act, and the Online Communication and Geolocation Privacy Act, the Law Enforcement Access to Data Stored Abroad Act (LEADS Act) would require a warrant based on probable cause to obtain the contents of communications from both an ECS and RCS and eliminate the 180-day rule.[98] In fact, the LEADS Act would provide all the other amendments to ECPA contained in both the Email Privacy Act and the ECPA Amendments Act (e.g., notice requirements, the "rule of construction," and authority to use civil discovery subpoenas for non-content information).

In addition to these changes, the LEADS Act would authorize the government to obtain the contents of electronic communications regardless of where those contents are stored if the account holder is a U.S. person.[99] This perceived need to extend ECPA's reach extraterritorially

[96] Letter from Mary Jo White, Chair of the Securities and Exchange Commission, to Senator Patrick J. Leahy, Chair of the Senate Judiciary Committee (April 24, 2013).

[97] Letter from American Civil Liberties Union, et al., to Mary Jo White, Chair of the Securities and Exchange Commission (April 9, 2014).

[98] *See* Law Enforcement Access to Data Stored Abroad Act, H.R. 1174, 114th Cong. (2015); Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).

[99] *Id*. at § 3.

has been prompted, in part, by two facets of the Internet. The first is the fact that service providers can store customer data in fragmented form in multiple locations including overseas.[100] The second is that data is not always stored in the same country as the user.[101]

The LEADS Act would partially address an issue currently being litigated in federal court—whether, under ECPA, the government can compel third-party service providers to produce the contents of electronic communications held overseas. In a pending case in the U.S. Court of Appeals for the Second Circuit, the United States sought and received a warrant from a federal magistrate judge under Section 2703(a) of ECPA for the contents of emails and subscriber information for an email account operated by Microsoft Corporation.[102] Microsoft complied with the portion of the warrant seeking non-content information, which was stored on servers located inside the United States. However, Microsoft determined that the content information sought by the warrant was located in servers hosted in Dublin, Ireland and moved to quash that aspect of the warrant. In its challenge, Microsoft argued that because federal courts generally lack authority to issue warrants for the search and seizure of items located outside of the United States, the warrant issued here was therefore unauthorized.[103] The magistrate judge—and, subsequently, the district court judge—rejected this argument and upheld the warrant.[104] The court reasoned that Section 2703(a) warrants were not traditional warrants but hybrids, with aspects similar to both subpoenas and traditional warrants. In contrast to traditional warrants, subpoenas require the disclosure of information within a recipient's control, regardless of location (even if overseas). In addition, when executing Section 2703(a) warrants, government officials do not view any information until it arrives in the United States, so no extraterritorial search occurs

While resolution of this question, at least in the Second Circuit, awaits the court's decision, the LEADS Act would at least partially clarify the government's authority in this area. The act would require third-party service providers to disclose the contents of U.S. persons' electronic communications held overseas upon issuance of a warrant based on probable cause.[105] However, the legislation contains an exception: courts issuing such warrants shall modify or vacate the warrant if, upon a motion by the service provider, the court finds that disclosure would force the service provider to violate the laws of a foreign country.[106] Given the variety of legal privacy regimes in other countries and the relative ease with which major service providers can relocate and store data around the world, it is unclear precisely how these provisions of the LEADS Act would affect email privacy.

In addition, while the bill specifically authorizes the government to compel the disclosure of the contents of communications held by third-party service providers overseas if the account holder is a U.S. person, it is silent as to non-U.S. persons.[107] Were the LEADS Act to pass into law, this

[100] *See* Kerr, *supra* note 17, at 408.

[101] *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 469 (S.D.N.Y. 2014).

[102] *Id.* at 477.

[103] *Id*. at 470.

[104] *Id*. at 477; *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624, at *1 (S.D.N.Y. Aug. 29, 2014) ("On July 31, 2014, the Court heard oral argument on those objections and affirmed Judge Francis's ruling by issuing the July 31 Order on the record.").

[105] Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. § 3(a)(2) (2015).

[106] *Id*.

[107] *Id*.

omission raises the question whether the government is barred from issuing a warrant or a subpoena to require a service provider to disclose the contents of communications of non-U.S. persons held overseas. For example, assuming law enforcement was investigating criminal activity involving a U.S. person in concert with a non-U.S. person visiting the country—would the government be permitted to compel the disclosure of the emails held overseas of the U.S. person, but not the non-U.S. person?

One interpretation of this omission is that the broad privacy protections contained in Section 2702 would bar providers from disclosing the contents of communications of non-U.S. persons held overseas, and because Section 2703, under existing law or as amended by the LEADS act, does not specifically authorize the government to obtain a warrant compelling a service provider that stores information overseas to disclose them, the government is precluded under Section 2702 from obtaining them. Relying on the canon of statutory interpretation *expressio unius est exclusio alterius* ("expressing one item of an associated group or series excludes another left unmentioned"),[108] it might be argued that the LEADS Act's express inclusion of U.S. persons could be interpreted to mean that the communications of non-U.S. persons were not intended to fall within the reach of this new rule.

However, an alternative view would be that while the LEADS Act appears to lack any *authorization* for the government to obtain a warrant to compel the disclosure of the contents of communications of non-U.S. persons held overseas, the privacy protections of Section 2702 are simply inapplicable to such contents and do not bar the government from seeking them by other means. The "presumption against extraterritorial application" of U.S. law teaches that if a statute "gives no clear indication of an extraterritorial application, it has none."[109] And even "when a statute provides for some extraterritorial application, the presumption ... operates to limit that provision to its terms."[110] If one considers an ECPA warrant compelling a service provider to disclose the contents of communications held overseas to authorize a law enforcement seizure abroad, rather than simply directing an entity to act within the United States—a question currently under litigation in the Second Circuit Court of Appeals[111]—then the presumption against extraterritorial application of U.S. law would presumably apply. In that case, the statute must clearly indicate that the privacy protections of Section 2702 apply abroad. Failing that, the relevant provisions of Section 2702 would not protect the contents of communications of non-U.S. persons held abroad, and the government could conceivably rely on alternative authorities to compel disclosure, such as a traditional subpoena.[112] This issue, as well as other interpretive questions raised by ECPA reform, would likely have to be resolved through litigation.

[108] Chevron U.S.A. Inc. v. Echazabal, 536 U.S. 73 (2002) (quoting United States v. Vonn, 535 U.S. 55, 65 (2002)).

[109] Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010). However, another rule of construction, derived from *United States v. Bowman*, 260 U.S. 94 (1922), teaches that Congress "need not expressly provide for extraterritorial application of a criminal statute if the nature of the offense is such that it may be inferred." United States v. MacAllister, 160 F.3d 1304, 1307-08 (11th Cir. 1998).

[110] *Id*. at 265.

[111] *See* Brief for Appellant, In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. (2d Cir. Dec. 8, 2014).

[112] Whether a traditional subpoena could be used to compel service providers to disclose the contents of emails of non-U.S. persons held by the provider overseas is beyond the scope of this report.

Author Contact Information

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

Jared P. Cole
Legislative Attorney
jpcole@crs.loc.gov, 7-6350