NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
17 N.C. J.L. & TECH. ON. 185 (2016)

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: DOES THE ACT LET THE GOVERNMENT SNOOP THROUGH YOUR EMAILS AND WILL IT CONTINUE?

Brittany Brattain*

The Securities and Exchange Commission ("SEC") is an enforcement powerhouse that has historically relied on the 1986 Electronic Communications Privacy Act ("ECPA") to collect electronic communications directly from Internet Service Providers ("ISPs") with a subpoena. The ECPA shields recent or unopened electronic communications from government eyes, but treats all others as abandoned and thus subject to warrantless government search and seizure. In 2015, Congress introduced the Email Privacy Act to align the ECPA with current technologies and their pervasive role in society by requiring a warrant before the government may access any emails from ISPs. The SEC seeks a civil agency exemption. This Recent Development argues that the SEC's proposed exemption must fail because the bill's warrant requirement will respect the Fourth Amendment's preference for bright-line rules without inhibiting investigations.

I. INTRODUCTION

"As the target of an [sic] SEC investigation, I know that the SEC has a broad array of tools at their disposal to obtain information directly from targets,"[1] said billionaire investor Mark Cuban.[2] The SEC was designed to "protect investors, maintain fair,

* J.D. Candidate, University of North Carolina School of Law, 2017. The author would like to thank the NC JOLT staff and editors for their thoughtful feedback and encouragement, particularly Maria Moore, Charlotte Davis, Chelsea Weiermiller, and Collette Corser.

[1] Eric Hal Schwartz, *The Big One: Mark Cuban Wants the SEC to Stay Out of His Email*, DCINNO, (Dec. 14, 2015, 12:00 PM), http://dcinno.streetwise.co/2015/12/04/mark-cuban-wants-congress-ecpa-bill-to-stop-sec-email-searc/.

[2] FORBES, *The World's Billionaires*, http://www.forbes.com/profile/mark-cuban/ (last visited March 21, 2016).

orderly, and efficient markets, and facilitate capital formation."[3] One branch of the SEC, the Division of Enforcement, is the agency's law enforcement arm which investigates and prosecutes securities law violations.[4] Historically, the SEC has relied on a 1986 law, the ECPA, to investigate alleged securities law violations by compelling internet service providers ("ISPs") to disclose their subscribers' private electronic communications.[5] However, the SEC's historic electronic investigative techniques are now coming under scrutiny by Congress.[6]

The recent scrutiny arises as Congress asserts a bipartisan effort to reform the ECPA to reflect new technologies.[7] At the time Congress created and passed the ECPA, the Internet was just sixteen years old[8] and the World Wide Web did not yet exist.[9]

---

[3] U.S. SEC. & EXCH. COMM'N, *What We Do*, https://www.sec.gov/News/Article/Detail/Article/1356125787012 (last visited March 21, 2016).

[4] U.S. SEC. & EXCH. COMM'N, *How Investigations Work*, https://www.sec.gov/News/Article/Detail/Article/1356125787012 (last visited March 21, 2016). The Commission has the authority to bring proceedings in federal court or initiate an administrative action, where appropriate. *Id.*

[5] *See* United States v. Warshak, 532 F.3d 521, 523 (6th Cir. 2008); Warshak v. United States, 631 F.3d 266, 288 (6th Cir. 2011).

[6] *See* U.S. SENATE, *Senate Committee on the Judiciary Questions for the Record from Senator Grassley To: Andrew Ceresney Director, Division of Enforcement U.S. Sec. & Exch. Comm'n.*, https://www.judiciary.senate.gov/download/ceresney-responses-to-questions-for-the-record [hereinafter Ceresney Responses].

[7] HOUSE OF REPRESENTATIVES JUDICIARY COMMITTEE, *House Judiciary Committee Announces Hearing on Electronic Communications Privacy Act,* (Nov. 24, 2015), http://judiciary.house.gov/index.cfm/press-releases?ID=7B80AA0E-CB80-4AD0-9FF7-467488B49B40 [hereinafter *Committee Announces Hearing*].

[8] The Internet came to life in 1969, prompted by researchers and scientists who desired to share information and computers remotely. By 1971, the Internet grew into an electronic post office where individuals exchanged all types of written information. Mark Ward, *Celebrating 40 Years of the Net*, BBC NEWS (October 29, 2009, 9:25 PM), http://news.bbc.co.uk/2/hi/technology/8331253.stm. For additional information on the formation of the Internet, see RAND CORP., *Paul Baran and the Origins of the Internet,* http://www.rand.org/about/history/baran.html (last visited March 21, 2016).

Congress structured the ECPA based on specific assumptions regarding how technologies worked in the 1980s and how individuals interacted with such technologies during that time.[10] As technology has grown and changed over the years, the logic underlying the ECPA is no longer fully accurate, and Congress aims to correct these flaws by enacting the Email Privacy Act.[11]

The Email Privacy Act applies greater protections to a user's electronic communications by demanding that the government obtain a warrant before it gains the power to compel a third-party service provider to disclose a user's private information.[12] This legislation significantly heightens the protections afforded to electronic communications by requiring the government to obtain a warrant based on probable cause and approved by a neutral magistrate, as opposed to the current law, which allows the government to compel information with merely a subpoena and appropriate notice to the subject of the investigation.[13] In reaction to these magnified protections, the SEC claims that a warrant requirement would impede its investigations.[14] Accordingly, the Commission is pushing for a civil agency exemption, which would allow the SEC (and all civil agencies) to search and seize electronic communications with only an administrative subpoena.[15]

---

[9] The World Wide Web is made up of many linked documents. This part of the Internet is viewable only with a special program, called a browser. STUDENT DICTIONARY UPPER INTERMEDIATE LEVEL 980 (2d ed. 2016).

[10] *See* H.R. REP. NO. 99-647, at 22-23 (1986).

[11] *See* H.R. 699, 114th Cong. (2015), Currently filing through Committees in the House is a bill called the Email Privacy Act, which is identical to a bill moving through Committees in the Senate called the Electronic Communications Privacy Amendment Act of 2015; *see* S. 356, 114th Cong. (2015).

[12] *See* H.R. 699.

[13] *See* 18 U.S.C. § 2703 (2010), *see also* H.R. 699.

[14] U.S. SEC. & EXCH. COMM'N, *Testimony on Updating the Electronic Communications Privacy Act,* (Dec. 1, 2015), https://www.sec.gov/news/testimony/testimony-ceresney-12015.html.

[15] "H.R. 699 would require government entities to procure a criminal warrant when they seek the content of emails and other electronic communications from ISPs. Because the SEC and other civil law enforcement agencies cannot obtain criminal warrants, we would effectively not be able to gather evidence,

This Recent Development argues that the SEC's proposed civil agency exemption to the Email Privacy Act should fail because it would blur the line between criminal and civil law enforcement investigation, deter the use of American technology, and ignore the importance of electronic communication and storage in today's world. Part II provides background on the ECPA. Part III discusses the Email Privacy Act and the Commission's proposed civil exemption to the bill. Part IV argues for the passage of the Email Privacy Act without a civil agency exemption. Part V concludes.

II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AND ITS HISTORY

In response to perceived gaps in federal privacy protection afforded to electronic communications, Congress passed the Electronic Communications Privacy Act ("ECPA")[16] in 1986 to balance individual privacy and law enforcement needs.[17] As a result of rapid technological advances in computing and telecommunication in the 1980s, individuals and corporations have enjoyed unparalleled access to new technologies for processing and storing data and communicating with others.[18] With these advances, "Americans . . . lost the ability to lock away a great deal of personal and business information."[19] Technology outpaced judicial interpretations[20] of the Fourth Amendment and privacy statutes in effect at the time.[21] This section explores the

---

including communications such as emails, directly from an ISP, regardless of the circumstances. Thus, if the bill becomes law without modifications, the SEC and other civil law enforcement agencies would be denied the ability to obtain critical evidence . . ." *Id.*

[16] *See* S. REP. NO. 99-541, at 1, *reprinted in* 1986 U.S.C.C.A.N. at 3555 ("[This] bill . . . update[s] and clarif[ies] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

[17] *See id.* at 1 *reprinted in* 1986 U.S.C.C.A.N. at 3555; s*ee also* Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[18] *See id.* at 2-3, *reprinted in* 1986 U.S.C.C.A.N. at 3556-57.

[19] *Id.* at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3557.

[20] *See* H.R. REP. NO. 99-647, 1, 22 (1986).

[21] *See* S. REP. NO. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3560.

background and history surrounding the ECPA, and provides an explanation of the relevant parts of the Act.

An individual's right to privacy is protected by the Fourth Amendment and federal statutes.[22] In 1986, the Fourth Amendment offered weak protection to electronic communications and few courts had yet applied the Fourth Amendment to digital technologies.[23] Although the Fourth Amendment protects "persons, houses, papers, and effects"[24] in the real world, these protections do not readily transfer to Americans' "virtual homes"[25] for three important reasons.[26] First, the third-party doctrine formulated by the U.S. Supreme Court holds that Fourth Amendment protections

---

[22] "The Framers addressed the subject of personal privacy directly in the Fourth Amendment." Fisher v. United States, 425 U.S. 391, 400 (1976). Statutes that provide privacy protections include the Electronic Communications Privacy Act and the Privacy Act of 1974. *See* 18 U.S.C. §§ 2510 *et seq.* 5 U.S.C. § 552a. (2010). Ten state constitutions protect citizens' right to privacy including: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. National Conference of State Legislatures, *Privacy Protections in State Constitutions,* http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (last visited March 21, 2016). *See e.g.,* ALASKA CONST. art. I § 22 "The right of the people to privacy is recognized and shall not be infringed." *See* ARIZ. CONST. art. II § 8, "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." *See* LA. CONST. art. I § 5 "Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy."

[23] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004).

[24] U.S. CONST. amend. IV.

[25] The "virtual home" is a term used to describe the private information that individuals store with network service providers that offer remote storage capabilities and those that transmit information across the internet from one use to another. In the virtual home individuals store private information including bank records, personal and business calendars, steps walked, calories consumed, as well as family photos.

[26] *See* Kerr *supra*, note 23 at 1210–12, *see also* S. REP. NO. 99-541, 1, 1-4, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555–58 (characterizing the statutory and constitutional protections given to electronic information as "weak, ambiguous, or non-existent" and noting that "electronic mail remains legally as well as technically vulnerable to unauthorized surveillance").

are extinguished when private information is shared with a third party.[27] This doctrine limits Fourth Amendment protections for electronic communications because users transmit and store electronic communications through the use of ISPs.[28] The third-party doctrine holds that when users reveal their private information to ISPs, even if such information is only intended for transmission or secure storage, the user forfeits any Fourth Amendment protection of that information.[29]

Second, the Fourth Amendment regulates government actors, and individuals acting as agents of the government, but not private actors.[30] ISPs are private actors, [31] and thus can search and seize

---

[27] *See e.g.*, Lopez v. United States, 373 U.S. 427, 439–40 (1963), (ruling that an individual had no reasonable expectation of privacy that the Fourth Amendment protects in a recorded conversation with a government agent posing as a friend); Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding no reasonable expectation of privacy in the wrongdoings revealed to a friend); United States v. White, 401 U.S. 745, 752–53 (1971) (plurality opinion) (refusing to extend Fourth Amendment protections to information recorded and transmitted to the police by a wrongdoer's "trusted accomplice"); United States v. Miller, 425 U.S. 435, 441–43 (1976) (applying the third party doctrine to financial records disclosed to banks even when the information was disclosed for a limited purpose with the expectation that the bank would not share it with others); Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (determining that Smith held no reasonable expectation of privacy in the phone numbers that he dialed when he conveyed those numbers to the telephone company); *Cf.* Riley v. California, 573 U.S. ___, ___ (2014) (slip opinion at 28) (protecting cell phone data under the Fourth Amendment even when the information was shared with third party cell phone carrier).

[28] *See* S. REP. NO. 99-541, at 3 *reprinted in* 1986 U.S.C.C.A.N. at 3557; *see also,* Kerr, *supra* note 23, at 1210.

[29] *See* Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001) (finding no Fourth Amendment protections in non-content information disclosed to ISPs). *See also* Kerr, *supra* note 23, at 1210.

[30] United States v. Ford, 765 F.2d 1088, 1090 (11th Cir.1985) (holding that a search by a private person does not implicate the Fourth Amendment unless the individual acts as an instrument or agent of the government.)*; see also* CORNELL UNIV. L. SCH., *Fourth Amendment: An Overview*, available at: https://www.law.cornell.edu/wex/fourth_amendment (last visited March 21, 2016) (describing the Fourth Amendment as regulating unreasonable governmental intrusion but not private intrusion).

their users' information, even if the information is protected by the Fourth Amendment, and reveal information to the government without implicating the Fourth Amendment. The Fourth Amendment gives "no protection to the wrongdoer whose trusted accomplice [or ISP] is or becomes a police agent."[32]

Third, the Fourth Amendment empowers the government to use a grand jury subpoena to induce private parties to release Fourth Amendment protected information.[33] When retrieving electronic communications, the government does not personally search or seize the electronic files; instead, the Government uses a grand jury subpoena to force the ISP to release information relevant to the investigation.[34] The government can obtain a grand jury subpoena based on reasonableness, a standard less stringent than probable cause.[35] In this way, the Fourth Amendment allows the government to obtain a user's electronic communication without a warrant or probable cause. However, a private actor compelled to disclose information by a grand jury subpoena is protected by the Fourth Amendment's reasonableness requirement and can challenge the subpoena in court as unreasonable.[36]

---

[31] Examples of ISPs include UUNET, Qwest, Sprint, AT&T, and GTE. All of these companies are private businesses that offer services for a fee and are unaffiliated with the U.S. federal government. *See Internet Service Provider (ISP)* GALE ENCYCLOPEDIA OF E-COMMERCE (2002), http://www.encyclopedia.com/topic/Internet_service_provider.aspx (last visited March 21, 2016).

[32] United States v. White, 401 U.S. 745, 752 (1971).

[33] *In re Subpoena Duces Tecum*, 228 F.3d 341, 347–49 (4th Cir. 2000) (implementing Fourth Amendment protections when the government used a subpoena that mandated disclosure of private papers by requiring the government to show reasonableness in the scope, relevancy, and burden of the subpoena). *See also* American Civil Liberties Union v. Clapper, 785 F.3d 787, 814–15 (2d Cir. 2015).

[34] SEC uses a subpoena to compel others to provide documents and testimony. U.S. SEC. & EXCH. COMM'N, *How Investigations Work,* https://www.sec.gov/News/Article/Detail/Article/1356125787012.

[35] *In re Subpoena Duces Tecum*, 228 F.3d at 347 (differentiating the basis needed for a warrant, which is probable cause under the Fourth Amendment, and a subpoena, which is reasonableness under the Fourth Amendment).

[36] *Id; see also* Hale v Henkel, 201 U.S. 43, 76 (1906) (applying Fourth Amendment protections against unreasonable subpoenas to corporations).

Collectively, these Fourth Amendment principles have left electronic communications held by third parties out in the open for the government to find.

Three key federal statutes, collectively referred to as the ECPA, protect individuals' privacy on the Internet,[37] the ECPA is comprised of the Wiretap Act,[38] the Stored Communications Act ("SCA"),[39] and the Pen Register Act,[40] which protect individuals' oral and written wire and electronic communications from third party interference and regulate government surveillance of those data while in transmission and storage.[41] Congress now moves to amend portions of the ECPA, specifically SCA, to recalibrate the balance struck between privacy interests and law enforcement interests tangled up in the SCA. Thus, a brief explanation of the current Act is necessary.[42] In this section, Part A will discuss the technological assumptions upon which the SCA is based and the types of ISPs covered under the SCA. Part B of this section examines the privacy protections afforded to different types of

---

[37] *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986). The ECPA is codified in various portions of chapter 18 of the United States Code, 18 U.S.C. § 1367, §§ 2510-22, §§ 2701-12, §§ 3121–27.

[38] 18 U.S.C. §§ 2510–22 (2010). The Wiretap Act prohibits the interception of any wire, oral, or electronic communication while the communication is in transit.

[39] *Id.* at §§ 2701–12. The Stored Communications Act regulates access to stored electronic communications. The Act is discussed in further detail in Part II A and B, *infra.*

[40] *Id.* at §§ 1367, 3121–27. The Pen Register Act limits the installation and use of pen registers and trap and trace devices which collect transactions information about the communication as defined in *Id.* § 3127(3)(4). The Pen Register Act is not a part of Congress's ECPA Amendment Bills and thus is beyond the scope of this Recent Development. For more information on this statute, *see* ORIN S. KERR, COMPUTER CRIME LAW, 618–32 (3d ed. 2012).

[41] Together the Wiretap Act and the Stored Communications Act provide these protections, specifically, 18 U.S.C. § 2511 prohibits the interception of wire, oral, or electronic communications during transmission, and *Id.* § 2701 prohibits unauthorized access to a facility that provides electronic communications services or stores electronic communications.

[42] Two bills amending the Stored Communications Act, one portion of the ECPA, circulated through committees in the House and Senate in 2015 and early 2016. The bills are identical in language.

communications and the burdens that the government must meet in order to compel information from ISPs.

A. Structure of the Stored Communications Act

The SCA, one part of the ECPA, protects the privacy of electronic communications by providing customers and subscribers with statutory rights and remedies that limit access to information.[43] Specifically, the SCA regulates retrospective surveillance[44] (surveillance of stored communications)[45] of emails and messages held by specific types of ISPs.[46] The SCA protects the privacy of electronic communications through § 2703, which prescribes different thresholds of proof that the government must meet to compel a provider to disclose various types of

---

[43] The SCA prohibits unauthorized access of a "facility through which an electronic communication service is provided . . . ; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." *Id.* § 2701. Violators face fines and imprisonment up to ten years. *Id.*

[44] The following example from Kerr, differentiates retrospective surveillance from prospective surveillance:

Wiretapping a telephone provides the classic example of prospective surveillance. When the FBI wiretaps a telephone line, it seeks to listen to the contents of *future conversations*. In the case of retrospective surveillance, in contrast, the government seeks to access stored records of *past communications*. The use of O.J. Simpson's telephone records in his murder trial furnishes a well-known example. The Los Angeles Police Department obtained Simpson's phone records to show that Simpson had made several suspicious calls the night of his wife's murder. This example illustrates retrospective surveillance . . . ; the police used the phone company's stored business records relating to *past communications* to try to prove Simpson's guilt. (emphasis added).

Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't,* 97 NW. U. L. REV. 606, 616 (2003).

[45] *See* 18 U.S.C. § 2701 (2010); *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 (2004) (describing the form of surveillance governed by the SCA).

[46] *See* 18 U.S.C. §§ 2510(15), 2711(2) (2010) (defining the two types of Internet service providers covered under the SCA: providers of electronic communication services, and providers of remote computer storage). The covered ISPs are described in more detail later in this section.

communications.[47] Section 2702 defines when an ISP can voluntarily disclose communications to the Government.[48] Finally, the SCA imposes harsh penalties and imprisonment for up to ten years upon any person who violates the statute.[49]

Congress formulated privacy protections in the SCA based on specific assumptions regarding the way that computer-to-computer communications worked in the 1980s.[50] These concepts influenced the scope of the SCA with regard to which types of ISPs were covered and which types of communications were shielded most faithfully from government surveillance. The first assumption that informed the SCA was the way in which service providers transmitted communications and processed data.[51] At that time, business and individuals used computers for information processing and storage.[52] In the process of sending and receiving electronic data, such as emails, providers of electronic communication services developed a system that created and stored copies of the information at least until the intended recipient downloaded the content.[53] Although storage sometimes lasted for as long as three months.[54] This system of copying and storing electronic information warded against system failures that would otherwise wipe out electronic data.[55]

In processing, data businesses sent company records to providers of remote computer services for advanced analysis, and service providers retained copies of these customer files for long

---

[47] *See id*. § 2703.
[48] *See id*. § 2702.
[49] *See id*. § 2701(b).
[50] *See* H.R. REP. NO. 99-647, 1, 22–23 (1986) (describing data transmissions, electronic mail, and remote computing services as the technologies were understood in 1986 when the ECPA passed).
[51] *See* S. REP. NO. 99-541, 1, 3 *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.
[52] *See id.*
[53] *See id.*, H.R. REP. NO. 99-647, 1, 22 (1986).
[54] *See* S. REP. NO. 99-541, at 3 *reprinted in* 1986 U.S.C.C.A.N. at 3557, *see also* H.R. REP. NO. 99-647, at 22.
[55] *See* S. REP. NO. 99-541, at 3 *reprinted in* 1986 U.S.C.C.A.N. at 3557, *see also* H.R. REP. NO. 99-647, at 22.

periods of time.[56] For example, before Microsoft Excel, Lotus 123, and similar computer programs, businesses (or individuals with need) hired remote computing services to perform advanced analytics on data to determine things such as customer trends or projected gross earnings.[57] The next assumption applied to providers of remote computer services that stored bulk amounts of data for individuals and businesses. In the 1980s, users sought out electronic storage providers and paid for remote electronic storage space where business records and other files would live.[58]

Operating under these assumptions, Congress constructed the SCA to protect electronic communications held by two types of public ISPs: providers of electronic communications service ("ECS") and providers of remote computing service ("RCS").[59] Under the SCA, a provider of ECS is one that enables users to send and receive wire or electronic communications,[60] while a provider of RCS is one that offers long-term electronic storage or computerized information processing to the public.[61] A provider's status as an ECS or a RCS depends on the provider's function in connection with the specific copy of a particular communication.[62] This means that one provider may serve as both an ECS and a RCS for one communication. For example, Google and Yahoo act as an ECS when providing email services during which communications are transmitted and held for only short periods in short term storage.[63] These companies also perform as a RCS when providing customers with long-term storage through applications such as

---

[56] *See* S. REP. NO. 99-541, at 3 *reprinted in* 1986 U.S.C.C.A.N. at 3557.
[57] *See id.*
[58] *See id.*
[59] *See* 18 U.S.C. §§ 2510(15)–2711(2). An "electronic communication service" is defined as a "service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* at § 2510(15). A "remote computing service" is defined as a provider that offers to the public "computer storage or processing services." *Id.* at § 2711(2).
[60] *Id.* at § 2510(15).
[61] *Id.* at § 2711(2).
[62] *See* Kerr, *supra* note 23, at 1216.
[63] *See* S. REP. NO. 99-541, 1, 14 *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

Google Drive[64] and Dropbox.[65] In addition, platforms like Salesforce.com that produce statistics from customer information uploaded to the site are RCSs,[66] and Microsoft acts as a RCS through its One Drive application, which offers storage of electronic files.[67]

All other types of ISPs, most commonly those that do not provide services to the public, fall beyond the scope of the SCA and instead rely on the privacy protections embedded in the Fourth Amendment.[68] Unprotected ISPs are the most common because they include government email accounts to which individuals may direct inquiries, corporate email accounts from which colleagues brainstorm business ideas and to which individuals submit job applications, and university email accounts through which students and professors generally communicate.

The key to determining when a provider acts as an ECS, a RCS, or neither is to consider whether the copy in question is "incident to transmission,"[69] a backup copy of a communication incident to transmission, or a copy in remote storage.[70] For example, when users send information from a Gmail account, Google acts as a provider of ECS during transmission.[71] Google continues to act as a provider of ECS while the email is unopened.

---

[64] *See* GOOGLE, *Google Drive*, https://www.google.com/drive/ (last visited March 21, 2016).

[65] *See* Wired Media, *Rather than recreate Google Drive, Yahoo integrates Dropbox into Mail,* ARS TECHNICA, (Apr. 12, 2013, 7:15 PM), http://arstechnica.com/information-technology/2013/04/rather-than-recreate-google-drive-yahoo-integrates-dropbox-into-mail/.

[66] *See* SALESFORCE, *Products*, https://www.salesforce.com/ (last visited March 21, 2016).

[67] *See* MICROSOFT, *OneDrive*, https://onedrive.live.com/about/en-us/ (last visited March 21, 2016).

[68] *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998); *see also* Kerr, *supra* note 23, at 1226.

[69] 18 U.S.C. § 2510(7) (showing that electronic storage is synonymous with incident to transmission); *see* H.R. NO. 99-647, at 38 (defining incident to transmission as "any temporary intermediate storage of a communication" and any backup copy).

[70] 18 U.S.C. § 2510(7); H.R. NO. 99-647, at 38.

[71] This example is adapted from Kerr, *supra* note 23, at 1216.

The SCA categorizes unopened emails as data incident to transmission.[72] After opening emails,[73] recipients may delete the messages or leave them in their inboxes. With regards to the opened emails in the inbox, Google becomes a provider of RCS because Google transmitted the email to its final destination, the recipient's eyes, and is now holding the message for long-term storage.[74] When users take screenshots of emails or download emails to their personal computer hard drives, Google no longer acts as an ECS or a RCS with regard to the copy of the email on its users' personal computers.

However, a circuit split has developed concerning whether an opened email is incident to transmission and thus connected to a provider of ECS, or in remote storage, and thus connected to a provider of RCS. The Ninth Circuit holds that an ISP acts as an ECS to the email until the ISP and the user no longer need the email.[75] The Ninth Circuit finds the opened/unopened distinction irrelevant because the opened email can be a backup copy of the message that is "incident to transmission."[76] As a result, the Ninth Circuit classifies Google as a provider of ECS for a longer period of time, with the duration lasting for as long as the ISP or user reasonably believes that they may need to access the file in the

[72] H.R. NO. 99-647, at 64–65 (classifying an opened email stored on a server as long-term storage provided by a RCS); *see* Kerr, *supra* note 23, at 1216.

[73] A circuit split has emerged with regards to whether or not an opened email is protected under the ECPA, which is discussed below. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004) (classifying opened emails as data in short-term storage and protected by the highest standards under the SCA); *see* KLA-Tencor Corp. v. Murphy, 717 F. Supp. 2d 895, 904 (N.D. Cal. 2010) (applying *Theofel)*; *c.f.* United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (finding *Theofel* "unpersuasive"); *c.f.* United States v. Warshak, 631 F.3d 266, 291 (6th Cir. 2010) (calling the Ninth Circuit's classification in *Theofel* "implausible").

[74] H.R. NO. 99-647, at 64–65 (delineating long-term storage as any storage that goes beyond the email's delivery).

[75] Theofel, 359 F.3d at 1076.

[76] *See id.* at 1077 (determining that opening an email does not change the character of the communication or the relationship between the ISP and the communication).

future.[77] These classifications are critical because they determine the privacy protections available for the communication.

B. Privacy Protections that Limit Government Access under the Stored Communications Act

The SCA provides Fourth Amendment-like protections to electronic communications through § 2703, which governs how and when the government can compel an ISP to divulge electronic communications.[78] The designation as a provider of ECS or RCS plays a crucial role in the implementation of § 2703 because the government can compel information in different ways and times depending on whether the communication is held by a provider of ECS or RCS.[79]

Specifically, § 2703 imposes distinct standards that the government must meet to compel ISPs to disclose different types of communications.[80] The highest protections go to the providers of ECSs.[81] The Government must obtain a search warrant, based on probable cause, to compel a provider of ECS to release the contents of communications held for 180 days or less.[82] However, for information held by a provider of ECS *for more than 180 days* or for information retained by a provider of RCS, the Government may compel the provider to disclose the communications three different ways: search warrant based on probable cause,[83] a

---

[77] *See id.* at 1076 (extending the duration of "incident to transmission" for as long as ISP or user may need to download the communication from the ISP's server).

[78] 18 U.S.C. § 2703.

[79] *See id.* § 2703(a)–(b).

[80] *See id.* The rules in § 2703 govern content and non-content information. Content information "includes any information concerning the substance, purport, or meaning of that communication," while non-content information includes data such as transactional record and account logs. 18 U.S.C. § 2510(8); *see also* U.S. Dep't of Justice, Searching and Seizing Computers Obtaining Electronic Evidence in Criminal Investigations, 130 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

[81] *See* 18 U.S.C. § 2703(a).

[82] *See id.* at § 2703(a).

[83] *See id.* at § 2703(b)(1)(B).

subpoena with notice to the ECS's customer,[84] or a court order with notice to the customer of the provider of ECS.[85] To obtain a list of basic subscriber information, the government needs only a subpoena (without notice to the subscriber) to compel the ISP to provide the subscriber's name, address, local and long distance telephone connection records, or records of session times and durations, length of service and types of services utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service including any credit card or bank account number.[86]

An example can help to explain these rules. Suppose for example, that law enforcement approaches Google with a warrant based on probable cause. With this authority, the government can obtain anything specifically identified in the warrant that Google holds, including opened or unopened emails, no matter what type of provider holds the data and no matter how long the data have been stored. If the government approaches Google with a subpoena with notice to the customer, the government can compel Google to disclose basic subscriber information, from a provider of RCS the government can compel opened emails and other stored data, from a provider of ECS the government can compel emails in storage for more than 180 days. If the government approaches Google with a subpoena *without notice to the customer*, the government can only compel basic subscriber information, which includes the subscriber's name, IP address, and the source of payment for services. This example illustrates the ways that the government can compel the same types of information through various methods, while also demonstrating the limitations of the subpoena with notice compared to the wide reach of a warrant.

To obtain a warrant, the government must show probable cause for its belief that evidence of a crime is present in the place to be

[84] *See id.* at § 2703(b)(1)(B)(i).
[85] *See id.* at § 2703(b)(1)(B)(ii).
[86] *See id.* at § 2703(c)(2).

searched.[87] A subpoena may be obtained in a civil or criminal investigation; the notable difference between the two appears when a court becomes involved.[88] During criminal investigations, the government may obtain a court-issued subpoena by showing that the request is not "unreasonable or oppressive."[89] To meet these standards, courts have required the government to show that the subpoenaed information is evidentiary and relevant, that the evidence cannot reasonably be obtained in other ways, and that the government requested the subpoena in good faith, rather than as a fishing expedition.[90] During civil investigations, subpoenas are issued without any action by the court.[91] An agency or attorney[92] issuing a subpoena must still show that the subpoenaed information is relevant to a claim or defense in the case.[93] With the power of a warrant or subpoena, the government can compel information from an ISP, even when the ISP is not involved in the litigation.[94] However, Congress has limited the many powers that

---

[87] Illinois v. Gates, 462 U.S. 213, 214 (1983) (examining when a confidential informant's tip meets the standard of probable cause for the issuance of a warrant); CORNELL UNIV. L. SCH., *Probable Cause*, https://www.law.cornell.edu/wex/probable_cause#footnoteref1_q2zy1wf (last visited March 21, 2016).

[88] *See* FED. R. CIV. P. 45(a)(3) (authorizing licensed attorneys to issue and sign civil subpoenas without involving the court); *cf.* FED. R. CIV. P. 45(a)(3) (requiring the court to authorize and approve a subpoena during a criminal investigation).

[89] FED. R. CRIM. P. 17(c)(1).

[90] United States v. Nixon, 418 U.S. 683, 700 (1974).

[91] *See* FED. R. CIV. P. 45(a)(3) (assigning the clerk of the court and attorneys authorized to practice in the district with the power to issue and sign civil subpoenas); *see also* CAB v. Hermann, 353 U.S. 322, 323 (1957) (giving government agencies the absolute right to issue administrative subpoenas).

[92] FED. R. CIV. P. 45(a)(3), "Subdivision (a)(3) specifies that an attorney authorized to practice in that court may issue a subpoena, which is consistent with current practice."; FED. R. CIV. P. 45, Notes of Advisory Committee on Rules—2013 Amendment; *see also* § 2453 Form and Issuance of a Subpoena, 9A FED. PRAC. & PROC. CIV. § 2453 (3d ed.).

[93] FED. R. CIV. P. 45(3); *see* S. REP. NO. 99-541, at 39; *see also,* § 2459 Subpoena for the Production of Documents and Things—Quashing or Modifying a Subpoena, 9A FED. PRAC. & PROC. CIV. § 2459 (3d ed.)

[94] *See generally* FED. R. CIV. P. 45 (compelling testimony, documents, and tangible items from third parties unaffiliated with the litigation).

would enable agencies and attorneys to enforce their own subpoenas.[95] Thus, failure to comply with a subpoena can only be corrected by a court order.[96] In addition to the burden of proof that the government must meet under § 2703, the SCA provides individuals with the opportunity to quash the subpoena by showing that the subpoena is unreasonable in time, scope, or burden.[97] The burden of showing unreasonableness falls on the individual moving to quash.[98]

III. EMAIL PRIVACY ACT AND THE SEC'S PROPOSED CIVIL EXEMPTION

The Email Privacy Act, a bill in the House with bipartisan support,[99] aims to recalibrate the ECPA in light of the highly advanced technologies of today, which are vastly different from those available when the ECPA was first passed in 1986.[100] The Email Privacy Act aims to clarify the law in § 2703[101] that governs

---

[95] *See* United States v. Bisceglia, 420 U.S. 141, 151 (1975) (protecting individuals from arbitrary government subpoena power by placing the court between the government and the individual subpoenaed).

[96] *See* United States v. Vivian, 217 F.2d 882, 883 (7th Cir. 1955) (requiring a separate court hearing before holding a subpoenaed individual in contempt for noncompliance).

[97] 18 U.S.C. § 2703(d) (2010); *see also* S. REP. NO. 99-541, at 39.

[98] S*ee id.* at § 2459 Subpoena for the Production of Documents and Things—Quashing or Modifying a Subpoena, 9A Fed. Prac. & P. Civ. § 2459 (3d ed.)

[99] *See* Sophia Cope, *Senate Judiciary Committee Finally Focuses on ECPA Reform*, ELEC. FRONTIER FOUND. (Sept. 14, 2015), https://www.eff.org/deeplinks/2015/09/senate-judiciary-committee-finally-focuses-ecpa-reform (declaring the President's support for ECPA reforms); *see also* BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, EXEC. OFFICE OF THE PRESIDENT (May 1, 2014) https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (last visited Jan. 17, 2016).

[100] The World Wide Web did not exist at the time that the ECPA was passed. The World Wide Web further blurs the distinction between providers of ECS and RCS because today many websites process information sent to them which could qualify them as a RCS, however, legislative history indicates that a data processing service included under the RCS label covered outsourced data processing. *See* S. REP. No. 99-541, 1, 3, reprinted in 1986 U.S.C.C.A.N. 3555, 3557; *see also Committee Announces Hearing*, *supra* note 7.

[101] 18 U.S.C. § 2703.

when and how the Government may compel ISPs to disclose a subscriber's private communications and data.[102] In reaction to the Email Privacy Act, the SEC has pushed back arguing that the legislation will hinder the Commission's enforcement efforts.[103] This section focuses on the ECPA amendment, subsection A discusses the assumptions that inform the E-Privacy Act and the heightened protections that Congress proposes for various types of electronic communications. Subsection B goes through the SEC's proposed civil exemption and demonstrates how the agency's proposed exemption rests on the old assumptions of the 1986 ECPA.

A. ECPA Reform: The E-Privacy Act

Many things have changed since the ECPA passed in 1986, but two critical changes specifically underlie the need for ECPA reform: technological advances and the changing judicial interpretation of the ECPA.[104] Today, agencies are uncertain of what simple words mean in the ECPA and are unclear on what the statute empowers agencies to do.[105] The Email Privacy Act provides clarity regarding the protections given to various types of electronic communications, and attunes the balance between privacy interests and law enforcement needs in this new technological era.[106]

---

[102] *See Committee Announces Hearing*, *supra* note 7.

[103] *See* Andrew Ceresney, *Testimony on Updating the Electronic Communications Privacy Act*, U.S. SEC. & EXCH. COMM'N (Sept. 16, 2015), https://www.sec.gov/news/testimony/testimony-electronic-communications-privacy-act.html.

[104] *See Committee Announces Hearing*, *supra* note 7; *see also* Warshak v. United States, 631 F.3d at 266; *see also* Theofel v. Farey-Jones, 359 F.3d 1066.

[105] *See* Letter from Mary Jo White, Chair, SEC, to Sen. Patrick Leahy, Chair, Sen. Judiciary Comm. (Apr. 24, 2013), at 3, https://www.cdt.org/files/file/SEC%20ECPA%20Letter.pdf [hereinafter Mary Jo White Letter] (describing how the SEC has not used its § 2703(b) subpoena power since the Sixth Circuit decided Warshak, and suggesting that the Commission is concerned or confused over its ability to use a power that the ECPA granted to it).

[106] DIGITAL DUE PROCESS, *ECPA Reform: Why Now?,* www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-

The enumerated goals of the Email Privacy Act include (1) providing consistency so that electronic communications and data are protected in the same way without regard to the technology used to communicate or store these data; (2) protecting privacy while preserving methods of civil and criminal investigation; and (3) providing clarity to the government, the public, and service providers regarding their obligations and rights during government investigations.[107] For example, the opened/unopened distinction that exists everywhere but the Ninth Circuit[108] complicates issues when the government approaches an ISP with a subpoena with notice to the subscriber.[109] Under judicial interpretation, this form of process would be sufficient in a North Carolina federal court,[110] but may not be in a California federal court.[111]

Specifically, the ECPA reform bills provide consistency[112] by protecting an individual's virtual home in the same way that the law protects an individual's real home. The amendments would create a single standard—a warrant[113]—for retrieving the contents

---

8e02000C296BA163 (last visited Jan. 17, 2016); *see also Committee Announces Hearing*, *supra* note 7.

[107] H.R. 699, 114th Cong. (2015); *see* Chairman Bob Goodlatte, Statement of Judiciary Committee Chairman Bob Goodlatte Full Committee Hearing on H.R. 699, The Email Privacy Act, JUD. CMTE. U.S. HOUSE OF REPRESENTATIVES, http://judiciary.house.gov/index.cfm/press-releases?id=AD96D145-2264-495B-87A4-BA7506EF3B66 (last visited Jan. 17, 2016).

[108] *See* Part II B. *infra.*

[109] *See infra*, note 73.

[110] 28 U.S.C. §§ 41, 81–131 (2010) (classifying North Carolina to be included in the Fourth Circuit of the Federal District Courts).

[111] *Id*. (classifying California to be included in the Ninth Circuit of the Federal District Courts); *see also* Theofel, 359 F. 3d at 1077 (changing the traditional understanding of the process required to compel an ISP to disclose an opened email).

[112] Furthermore, these reform amendments provide a standard that consistently applies across all investigative agencies, including federal, state, and local agencies. H.R. 699; H.R. 283, 114th Cong. (2015-2016).

[113] Under the ECPA Amendments, a court-approved search warrant is required for any investigation into the content of electronic communications and records. However, a subpoena satisfies civil investigations when the agency wishes to collect only the "name, address, local and long distance telephone connection records, or records of session times and durations, length of service

of electronic communications, no matter how old the records are, whether the emails have been opened, or where the records are stored.[114] A consistent warrant requirement across files of all ages would account for new technology, including massive cloud computing and archived files. The cloud offers virtually unlimited data storage, which prompts users to retain emails and files for a longer period of time. As a result of this file hoarding, a much larger number of files fall outside of warrant protection under the 1986 version of the ECPA.[115] The proposed updates to the ECPA take into account the need and ability to store electronic information for longer periods, as they provide the same protection to older emails and files of all ages.[116] In the cloud, individuals intentionally store a large amount of information.[117] However, because ISPs frequently archive information, these data can get stored in the cloud without an individual's knowledge or intent, and thus people could potentially be exposed to warrantless

---

(including start date) and types of service used, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service of a subscriber or customer of such service." H.R. 699 §3 (c), 114th Cong. (2015).

[114] "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 . . . ." H.R. 699 (a). In contrast to the current law, "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 . . . . A governmental entity may require the disclosure by a provider of electronic communications services of the content 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" with an administrative subpoena. 18 U.S.C. § 2703(a)-(b).

[115] *See* 18 U.S.C. § 2703 (exempting information stored with providers of RCS from the warrant requirement).

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

[117] *See* Sebastian Anthony, *How big is the cloud?* EXTREME TECH (May 23, 2012, 10:48 am) http://www.extremetech.com/computing/129183-how-big-is-the-cloud.

searches through no fault of their own. When information is archived, individuals have no control over what is stored and what is deleted.[118] The ECPA amendments consider how electronic information storage has evolved over time and provide Americans with protections that match this millennium's ever-growing technologies.

The amendments maintain the ECPA's goal of balancing law enforcement needs with Americans' right to be free from government intrusion in their inboxes. Although the ECPA reform amendments prohibit enforcement agencies from accessing the content of electronic files without a warrant, these entities will still have the power to use subpoenas to access and collect transactional information needed for civil investigations, such as names, addresses, time stamps, services provided, and payment information.[119] Legislators provided a carve-out that made a court-issued subpoena[120] the standard for the government to access internal corporate emails between officers, agents, and employees.[121] Congress also kept warrant exceptions for emergencies involving danger of death or serious physical injury.[122] In most circumstances, the government must notify customers of its investigations with service of process and inform customers when any of their information was accessed or obtained during a subpoena-powered investigation.[123] To balance the needs of law enforcement, the government may, upon approval of the court, delay notification for no more than 180 days.[124] This strikes an appropriate balance because it requires a neutral magistrate to determine if delay of notification is appropriate. Furthermore, the

---

[118] HOW TO GEEK, *How to Recover or Permanently Delete Files from the Cloud,* http://www.howtogeek.com/212601/how-to-recover-or-permanently-delete-files-from-the-cloud/ (last visited March 21, 2016).

[119] H.R. 699; H.R. 283, 114th Cong. (2015).

[120] This is still stronger than the 1986 version of the ECPA, which allowed a member or appointee of the SEC to issue a subpoena, whereas the Amendment requires a court to do so. *See* 18 U.S.C. § 2703; *see also* H.R. 699.

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

[122] 18 U.S.C. § 2258A (2010); 18 U.S.C § 2702(b) (2010).

[123] *See supra* note 73 and accompanying text.

[124] H.R. 699 § 4(a)(1)–(4).

delay is limited to instances when there is reason to believe that notification would endanger the investigation of life or limb.[125]

Reform also provides clarity and protection to service providers. The amendments define the exact information that a service provider must disclose when an investigating agency serves a subpoena[126] and makes it illegal for a provider of n ECS or RCS to disclose the contents of any records under its control unless the investigating governmental agency presents a warrant.[127] These clear-cut and definitive rules give customers confidence in the privacy and security of their electronic information. Today, the cost of physical storage facilities is expensive and organizing paper files is cumbersome and time-consuming. The cloud offers a cheaper alternative and provides search and find features to locate needed files quickly. The clear-cut rules of the ECPA amendments will provide peace-of-mind and allow businesses to select the most cost-efficient and productive form of mass storage—the cloud. Furthermore, these amendments protect the longevity of the American technology sector by dissipating customers' fears that their information may be susceptible to a warrantless government search.

The progress that Congress has made in creating the E-mail Privacy Act is threatened by the SEC's proposed civil exemptions. As you will read in the next subsection, the SEC's proposed exemption relies on old assumptions regarding the way that technology works and the way that individuals and businesses interact with computer technologies.

B. Proposed SEC Exemptions to ECPA Reform

In response to the first wave of ECPA reform bills, the Chair of the SEC proposed that the Commission be exempt from the

---

[125] *See id.*

[126] *See supra* note 86 and accompanying text (describing the information that is accessible under the power of a subpoena in civil investigations).

[127] H.R. 699, 114th Cong. (2015); H.R. 283, 114th Cong. (2015); S. 356, 114th Cong. (2015).

warrant requirement to obtain electronic information.[128] This exemption would grant to federal civil law enforcement agencies the power to induce service providers to provide electronic records and files without a warrant.[129] This proposed exemption would authorize the SEC and other federal civil agencies, including the EPA and the IRS, to collect information from an ISP without going directly to the individual under investigation. The SEC claims that it needs this authority because electronic communications often provide critical evidence establishing the "timing, knowledge, relationships in certain cases, or awareness that certain statements to investors were false or misleading."[130] The Commission points out that obstinate defendants and geographical boundaries pose issues to the agency's investigations:

> In certain instances, the person whose emails are sought will respond to our request. But in other instances, the subpoena recipient may have erased emails, tendered only some emails, asserted damaged hardware, or refused to respond – unsurprisingly, individuals who violate the law are often reluctant to produce to the government evidence of their own misconduct. In still other instances, email account holders cannot be subpoenaed because they are beyond our jurisdiction.[131]

The SEC fights against the Email Privacy Act's warrant requirement because the SEC, as a civil agency, cannot obtain a criminal warrant.[132] The Commission notes that its ability to seek information directly from the ISP is critical for three reasons. First, it provides the Commission with authority that encourages targets to deliver information themselves.[133] Targets are more likely to comply with subpoena orders when the Commission can threaten alternative ways to obtain the information, such as going to the ISP to get the information.[134] However, if the agency lost these

---

[128] Mary Jo White Letter, *supra* note 105. The request was made again during a September 2015 hearing before the Senate Judiciary Committee. *Reforming the Electronic Communication Privacy Act: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement from Ceresney, *supra* note 103).

[129] Mary Jo White Letter, *supra* note 105.

[130] Ceresney, *supra* note 103.

[131] Mary Jo White Letter, *supra* note 105.

[132] *Id.*

[133] *Id.*

[134] *Id.*

alternative routes to collect information, targets would be more likely to destroy incriminating information and less likely to comply with subpoenas because they would understand that if the SEC is unable to get the information from them, it will be unable to collect the information from anyone else.

Second, the Commission argues that the power to seek information from ISPs is critical in times when the targeted subscriber has deleted emails, damaged hardware, or fled to a jurisdiction where a subpoena has no authority.[135] ISPs maintain extensive backup copies of files; thus by going to the ISP to compel information, the SEC will have a full and complete record from which to draw evidence.[136] An ISP's backup system is critical to this argument because it provides the Commission with the most thorough, and complete information. After compelling information from the ISP, the SEC knows that it has evidence that is untampered with and void of any gaps. Without the power to compel information from the ISP some information like deleted emails or corrupted files will be inaccessible. Thus, the SEC may be left with an incomplete record to fuel its investigation and prosecution.

Third, the SEC argues that the Commission's power to compel ISPs to disclose information prevents the cat and mouse chase.[137] This could happen if the Commission reissues subpoenas for the jurisdiction to which the target fled.[138] This chase would waste the SEC's time and money and lead to ineffective and inefficient securities law enforcement.

Instead of a warrant, the SEC proposes legislation "that would (1) require civil law enforcement agencies to attempt, where possible, to seek electronic communications directly from a subscriber before seeking them from an ISP; and (2) should seeking them from an ISP be necessary, give the subscriber or

---

[135] *Id.*
[136] *Id.*
[137] Mary Jo White Letter, *supra* note 105; Ceresney, *supra* note 103.
[138] Mary Jo White Letter, *supra* note 105; Ceresney, *supra* note 103.

customer the opportunity to challenge the request in a judicial proceeding."[139]

The second prong of the SEC's proposal would purportedly offer *more protections*[140] than a warrant because it gives individuals an opportunity to challenge search requests, an option unavailable under a warrant. While the SEC's desire to give every person a voice is noble, it would not work out as suggested in practice because the plaintiff, the SEC, selects the venue of the court. Thus, the courthouse where the defendant would need to appear in order to contest the SEC's search request would likely be far from home, making it difficult or impossible to afford the trip.[141] Furthermore, the SEC's proposal overlooks the fact that an overwhelming majority of searches are conducted without warrants and are based upon the consent of the targeted individual.[142] One study suggested that as many as 98% of warrantless searches are conducted by consent.[143] Statistics show that people often consent to searches even when there is no real threat of a legal search; thus, if people consent to searches after verbal requests, it is highly unlikely that an individual facing a formal order authorizing a search would protest the order or the Commission's right to search. This is especially true given the SEC's strong enforcement reputation,[144] which enhances its authority and domination over its investigatory targets. Looking past the natural tendency to obey authority, the SEC's second prong poses an even bigger issue

---

[139] Ceresney, *supra* note 103.

[140] *See id.*

[141] FED. R. CIV. P. 1391.

[142] *See, e.g.*, RICHARD VAN DUIZEND ET AL., THE SEARCH WARRANT PROCESS 68–69 (1984).

[143] *Id.* at 19. Quoting a police detective as follows: "Actually, there are a lot of warrants that are not sought because of the hassle . . . . I don't think you can forgo a case because of the hassle of a search warrant, but you can . . . work some other method. If I can get consent [to search], I'm gonna do it." *Id.* This detective suggested that as many as 98% of the searches were by consent. *Id.*

[144] *See* Hazel Bradford, *SEC Management Enforcement Unit Evolves into Respected Watchdog,* PENSIONS & INVESTMENTS (Nov. 30. 2015), http://www.pionline.com/article/20151130/PRINT/311309984/sec-management-enforcement-unit-evolves-into-respected-watchdog.

because it provides no standard of proof that the SEC must meet before making a search request.[145] The Email Privacy Act reform is intended to put digital and paper effects on the same playing field. The SEC's proposal does not accomplish this object, as it provides no standards that the agency must follow in order to compel an ISP to disclose an individual's electronic communications.

The SEC's proposal implements process to protect the privacy rights of individuals by forcing agencies to approach the target of the investigation first. However, it falls short in that it still allows the agency to gather information from an ISP without a showing of probable cause.[146]

IV. THE EMAIL PRIVACY ACT SHOULD PASS WITHOUT THE SEC'S PROPOSED AGENCY EXEMPTION

The Email Privacy Act should pass without the SEC's proposed civil agency exemption because the amendments will not inhibit the SEC's enforcement power while following the court's preference for a Fourth Amendment bright-line rule.

A. The Commission's Powers to Gather and Collect Evidence in Civil Investigations

As a civil law enforcement agency, the SEC has never had the power to obtain a warrant.[147] Instead, the SEC has relied on subpoenas to investigate alleged violations. The ECPA-reform-bills change how the government may obtain the contents of electronic communications; however, these changes would not inhibit the SEC's ability to investigate civil crimes due to Congress's carve-out for corporate emails sent among insiders and

---

[145] *See* Ceresney, *supra* note 103 (providing no standard that the government must satisfy before compelling ISP to disclose information).

[146] *See id.* The SEC's proposal requires reasonable suspicion rather than probable cause, which is the standard required for a warrant. *Id.*

[147] Civil agencies can obtain court-ordered subpoenas but not warrants. *See* Mike Masnick, *SEC is a Due Process Nightmare*, TECHDIRT (Apr. 7, 2014 2:30 PM), https://www.techdirt.com/articles/20140404/22161026807/sec-is-due-process-nightmare-searches-emails-without-warrant-refuses-to-share-exculpatory-evidence.shtml.

employees.[148] Furthermore, the SEC has relied solely on subpoenas served directly on individuals since 2010, with impressive enforcement rates and outcomes.[149] A court-issued subpoena is adequate for the government to access internal corporate emails sent between officers, agents, and employees, and it provides a warrant exception for emergencies involving danger of death or serious physical injury. Furthermore, this bill empowers the government to delay notification to individuals whose information has been obtained; however, the delay requires court approval and cannot be extended beyond 180 days.

The corporate email carve-out[150] would enable the SEC to continue its civil investigations as usual. Under the corporate email carve-out, the Email Privacy Act affords less protection to employee emails sent from corporate accounts than to individual emails sent from personal accounts.[151] Under this exception, agencies seeking an employee's emails sent from a corporate email account may get permission to search from the corporation instead of getting consent directly from the employee.[152] Here, Congress finds the potential for shared responsibility to justify the alternative route to consent.[153] Given that the SEC primarily regulates corporate insiders, this exclusion will allow the agency unfettered access to corporate emails, which are typically treasure troves for insider trading investigations.[154]

During civil investigations, emails and other electronic files can be effectively obtained through the use of subpoenas issued directly to individuals either being investigated or who have sent or received the emails being sought.[155] Any civil law enforcement

---

[148] *See* H.R. 699, 114th Cong. (2015).
[149] *Id.*
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*
[154] L. Hilton Foster, *Insider Trading Investigations*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/about/offices/oia/oia_enforce/foster.pdf.
[155] The SEC's proposal aims to authorize the agency to serve third-party ISPs, rather than individuals under investigation. The ECPA reform bills will not

agency, including the SEC, can enforce these subpoenas by having a court demand that the user disclose the requested data.[156] Furthermore, the ECPA (in its current state and under the reform bills) provides the SEC and other civil enforcement agencies with the power to issue preservation orders to prevent an individual from destroying evidence while a court-approved subpoena is sought.[157] The SEC will retain these powers under the ECPA reform amendments.

The SEC has not sought content from ISPs since 2010,[158] when the Sixth Circuit declared that the government must have a warrant before secretly searching and seizing emails stored by a third-party ISP.[159] Even without this investigative tool, the SEC has been a dominating force in American civil law enforcement, with 755 total enforcement actions in 2014,[160] as compared to a total of 664 enforcement actions in 2009,[161] the last full calendar year that the SEC compelled information directly from ISPs[162] Between 2009 and 2014, nearly every category of SEC enforcement action has increased.[163] The only category that decreased, Issuer Reporting

---

affect the SEC's power to serve the individuals under investigation in order to obtain their records.

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

[157] 18 U.S.C. § 2703(f) (2012).

[158] *Reforming the Electronic Communication Privacy Act: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (2015).

[159] United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2011).

[160] *Year-by-Year SEC Enforcement Statistics*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/news/newsroom/images/enfstats.pdf.

[161] Comparing 2014 to any year between 2005 and 2009, there has been an increase in enforcement actions brought by the SEC, even though it lost an "important investigative tool." *Id.* Also, comparing any year between 2010 and 2014 will show the same upward trend (for example, when comparing 2012 to 2006 the total enforcement action in 2012 is greater than the total enforcement actions in 2006). *Id.*

[162] *Id.*

[163] Specified corporate insiders are required to submit periodic reports to the SEC concerning security purchases and other relevant information to help the agency defend against insider trading. *See* U.S. SEC. & EXCH. COMM'N, *Edgar Filer Manual Vol. II* (Aug. 15, 2015), https://www.sec.gov/info/edgar/forms/edgform.pdf.

and Disclosure, involves the failure of corporations to file information in a timely manner with the SEC.[164] This category is not affected by the agency's ability to investigate corporations' internal files because these filings are made directly to the SEC.[165] In these investigations, the SEC will have the filing in hand, which is all of the information needed to prosecute the violation. If the SEC does not possess the filing, this indicates that the corporation failed to file, but the SEC does not need to investigate corporate files to discover this. It only need investigate its own files, which it has plenary power to do. In spite of the SEC's lost investigative tool, it appears that the agency does not need a loophole around serving the target of its investigations in order to effectively enforce its civil laws.

B. Fourth Amendment's Preference for Bright-Line Rules

The Supreme Court fights to make bright-line rules for police officers who are fighting crimes,[166] so too should the legislature develop bright-line rules for investigators searching for evidence within an individual's virtual home.

Bright-line rules provide straightforward guidelines that law enforcement officers and investigators can apply in a split second.[167] The Supreme Court has favored these rules based on practical concerns that police officers and investigators need to act quickly to fight crime.[168] Specifically, in *Dunaway v. New York*, the Supreme Court described a Fourth Amendment bright-line rule as "essential to guide police officers, who have only limited time and expertise . . . ."[169] Again, in *New York v. Belton*, the Court rejected

---

[164] *See id.*

[165] *See id.*

[166] *See* Riley v. Cal., 573 U.S. ____, (2014) (slip opinion); Michigan v. Summers, 452 U.S. 692 (1981); Dunaway v. N.Y., 442 U.S. 200 (1979); Robinson v. U.S., 414 U.S. 218 (1973).

[167] *See Riley*, 573 U.S. ____; *Summers*, 452 U.S. 692; *Dunaway*, 442 U.S. 200; *Robinson*, 414 U.S. 218.

[168] *See Riley*, 573 U.S. ____(slip opinion at 28); *Summers*, 452 U.S. at 704; *Dunaway*, 442 U.S. at 214; *Robinson*, 414 U.S. at 258.

[169] *Dunaway*, 442 U.S. at 213–14.

balancing tests for the Fourth Amendment and instead demanded categorical rules:[170]

> A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions, may be the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be "literally impossible of application by the officer in the field.[171]

Later, in *Robinson v. United States*, the Court reaffirmed its belief in a bright-line test by rejecting case-by-case analysis for Fourth Amendment scrutiny.[172] Recently, the demand for a bright-line rule has been applied to electronic content in *Riley v. California*.[173]

In *Riley*, the police stopped a gang member for driving with expired registration tags.[174] During the stop, police gained lawful authority to impound Riley's car and conducted a full and legal vehicle search.[175] Through the lawful vehicle search, the police uncovered two illegally possessed weapons for which they arrested Riley.[176] Incident to arrest, police took Riley's smart phone[177] and later searched the phone's contents, which contained pictures and videos that identified Riley as a gang member and linked him to a previously unsolved murder.[178] On review, the Supreme Court announced a bright-line rule for cell phone searches: "[o]ur answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[179] The Court based its bright-line rule on the fact that

---

[170] *Summers*, 452 U.S. at 705 n. 19.
[171] New York v. Belton, 453 U.S. 454, 458 (1981).
[172] *Robinson*, 414 U.S. at 235.
[173] *Riley*, 573 U.S. ____.
[174] *Riley*, 573 U.S. at ___, (slip opinion at 1).
[175] *Id.* at ___, (slip opinion at 2).
[176] *Id.* at ___, (slip opinion at 2).
[177] The court described Riley's phone as: "a 'smart phone,' a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity." *Id.*
[178] *Id*.
[179] *Id.* at ___ (slip opinion at 28). In addition, the court refused to adopt a test that would require lower courts to determine on a case-by-case basis when electronic records were comparable to physical records. *See id.* at 25.

technology now allows an individual to carry enormous amounts of private information in virtual form that vastly exceeds the amount of information that one could carry in physical form.[180] The Court deemed the amount and type of information contained in a cell phone to be worthy of the highest degree of Fourth Amendment protections: the warrant.[181]

The Email Privacy Act tracks the structure and substance of the *Riley* opinion and should therefore overcome challenges in the courts. The Act provides investigators with a simple standard that they must meet in order to compel an ISP to disclose electronic information.[182] The Act requires a warrant[183] just like the Court did in *Riley*.[184] The bright-line rule in the Email Privacy Act stands in sharp contrast to the 1986 ECPA,[185] which mandates different forms of process for various types of electronic information; however, differentiating between a provider of RCS and ECS is no simple task, as the provider status changes over time.[186] During investigations, law enforcement officers do not have the "time or expertise" to tease out what type of process is needed for specific types of communication.[187]

Under the current ECPA regime, investigators tasked with compelling electronic data from an ISP must consider and weigh various facts including if the information is stored, how the information is stored, where the information is stored, when the information is stored, and when the information was stored.[188] An investigator contemplating these questions may not have the resources to determine if information is in storage or whether the

---

[180] *Id.* at ___ (slip opinion at 25).
[181] *Id.* at ___ (slip opinion at 28).
[182] *See* H.R. 699, 114 Cong. (2015).
[183] *See id.*
[184] Riley, 573 U.S. at ___ (slip opinion at 28).
[185] *See* H.R. 699; *see also* 18 U.S.C. § 2703.
[186] *See supra* Part II.
[187] Dunaway v. New York, 442 U.S. 200, 213–14 (1979); *see* 18 U.S.C. § 2703.
[188] The answers to these questions determine the type of process that the Government must satisfy before legally compelling an ISP to disclose a user's private information. *See* 18 U.S.C. § 2703.

information exists as a backup file.[189] Investigators may not be able to determine when a user stored information with the provider in question. Investigators are faced with so many questions that they may not act at all. These questions render the ECPA, in its current form, in violation of the court's bright-line rule underscoring Fourth Amendment protection.[190] While violation of a preference is not fatal, it does violate the Congressional intent of the 1986 Congress that passed the ECPA to provide Fourth Amendment-like protections to electronic communications.[191]

These bright rules are vital to the accurate execution of the law during high-stress, time-crunched, crime-fighting, and evidence-gathering situations.[192] The SEC demonstrated its expectation of confusion in the field when it instructed investigators to see the Office of Chief Counsel for any ECPA matters.[193] The SEC understood that the technicalities of the ECPA's compulsion rules are too much for laypersons to understand and think through in the spur of the moment, like an investigator may need to do. The current state of the ECPA, with its exceptions and hard-to-find answers, has halted certain law enforcement techniques for fear of an unintentional violation that will irreparably harm the Commission's reputation.[194]

The Email Privacy Reform Act provides uniform, standardized bright-line rules that provide much needed clarity for law enforcement so that investigators can return to their jobs of ferreting out crime, rather than attempting to ferret out legislative intent.

---

[189] Under the ECPA, stored files are protected by the subpoena, which offers the least amount of process, whereas backup files are protected by the warrant requirement. *See id*.

[190] *See e.g.*, New York v. Belton, 453 U.S. 454, 454 (1981).

[191] *See* S. REP. NO. 99-541, at 2.

[192] *See, e.g.*, Riley v. California, 573 U.S. ____, (2014) (slip opinion); Michigan v. Summers, 452 U.S. 692 (1981); *Dunaway*, 442 U.S. 200; Robinson v. United States, 414 U.S. 218 (1973).

[193] U.S. SEC. & EXCH. COMM'N, *Enforcement Manual*, Office of Chief Counsel (June 4, 2015).

[194] *See* Ceresney, *supra* note 103; *see also* Mary Jo White Letter, *supra* note 105.

V. CONCLUSION

The Email Privacy Act provides a clear and cogent standard to govern investigators ferreting out crime. It greatly improves upon the 1986 ECPA by updating the technological assumptions that underlie the law, clarifying and rewriting rules created by common law interpretations of the ECPA's standards to modern technology, and providing a clear bright-line rule that law enforcement can execute quickly and systematically.[195] These improvements cannot be fulfilled unless the Email Privacy Act passes without the SEC's proposed exemption.

The SEC and Congress both agree that the ECPA needs updating in order to keep up with current technology and to clear up conflicting common law rules.[196] However, tension results when one looks at the different ways that the SEC and Congress plan to reform the outdated law. While Congress wants a complete overhaul of the 1986 version, the SEC proposes an overhaul for criminal investigations but suggests a civil exemption for its own agency and other civil agencies, like the IRS and EPA.[197] The SEC's proposed exemption will protect the agency's investigatory power while providing additional protections to individuals by way of additional process.[198] For the last ten years, the SEC has not sought information directly from an ISP, out of deference to a Congress that, for years, has been grappling with ECPA reform.[199] In those ten years of "limited powers" the SEC's enforcement results have increased in the number of individuals prosecuted, and the amount of money collected from civil violations.[200] Statistics

---

[195] *See* H.R. 699, 114th Cong. (2015).

[196] *See* U.S. SEC. & EXCH. COMM'N, *Testimony on Updating the Electronic Communications Privacy Act,* (Dec. 1, 2015), https://www.sec.gov/news/testimony/testimony-ceresney-12015.html; *see also* Ceresney Responses, *supra* note 6.

[197] U.S. SEC. & EXCH. COMM'N, *Testimony on Updating the Electronic Communications Privacy Act,* (Dec. 1, 2015), https://www.sec.gov/news/testimony/testimony-ceresney-12015.html.

[198] *See id.*

[199] *Id.*

[200] *Year-by-Year SEC Enforcement Statistics*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/news/newsroom/images/enfstats.pdf.

show that the SEC does not need to compel an ISP to protect the dignity of securities and the securities market.[201] The additional process that the SEC proposes in its plan empowers individuals who are targets of SEC investigations to contest the SEC's subpoena and the information sought.[202] However, individuals must contribute massive amounts of time and money to assert such procedural protections in court.[203] The time and money required makes these individual procedural protections non-existent, or at least out of reach for most individuals.

Given society's abundant reliance on electronic technologies for personal, and business matters, the ECPA reform has been a long time coming and must develop a law with strong protections. The breadth and force of these protections is paramount because the Fourth Amendment, which protects Americans from unreasonable search and seizure by the government, does not protect electronic information in the same way that it protects tangible items.[204] Thus, the American people can only rely on Congress for shelter and Congress must deliver and deliver in a fashion that is meaningful and responsive to the demands of current technology in both form and function. The delivery that Congress must make is the passage of the Email Privacy Act which protects individuals in criminal *and* civil investigations through a warrant requirement.[205] In the words of the Supreme Court, "[Congress's] answer to the question of what police must do before searching a[n] [electronic communications] is accordingly simple—get a warrant."[206]

---

[201] *See id.*

[202] Ceresney Responses, *supra* note 6.

[203] *Id.*

[204] S. REP. NO. 99-541, at 1, *reprinted in* 1986 U.S.C.C.A.N. at 3555 ("[This] bill . . . update[s] and clarif[ies] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."); *see also* 18 U.S.C. §§ 2510 *supra* note 22.

[205] *See* H.R. 699, 114th Cong. (2015).

[206] Riley v. California, 573 U.S. at ___, (slip opinion at 28). In addition, the court refused to adopt a test that would require lower courts to determine on a case-by-case basis when electronic records were comparable to physical records. *See id.* at 25.