Cloud Computing: Constitutional and Statutory Privacy Protections

(name redacted)
Legislative Attorney

March 22, 2013

Congressional Research Service
7-....
www.crs.gov
R43015

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Cloud computing is fast becoming an integral part of how we communicate with one another, buy music, share photos, conduct business, pay our bills, shop, and bank. Many of the activities that once occurred solely in the physical world, including communications with one another, are increasingly moving to the digital world. What was once a letter to a friend is now a Facebook message; a call to a loved one is now a Skype chat; a private meeting with a business partner is now a video conference call. In short, the cloud is revolutionizing not only how we compute, but also how we live. Where individuals once locked personal or business papers solely in a desk drawer or filing cabinet, they now also store them on someone else's computer.

In short, cloud computing is a web-based service that allows users to access anything from e-mail to social media on a third-party computer. For instance, Gmail and Yahoo are cloud-based email services that allow users to access and store emails that are saved on each respective service's computer, rather than on the individual's computer. As more communications are facilitated through these cloud-based programs, it is no surprise that government and law enforcement would seek to access this stored information to conduct criminal investigations, prevent cyber threats, and thwart terrorist attacks, among other purposes. This prompts the following questions: (1) What legal protections are in place for information shared and stored in the cloud? (2) What legal process must the government follow to obtain this information? and (3) How do these rules differ from those applied in the physical world?

Protections of communications in the physical world flow from the Fourth Amendment and various federal statutes such as the Electronic Communications Privacy Act of 1986 (ECPA), which includes the Stored Communications Act (SCA). Under the Fourth Amendment, government officials are generally prohibited from accessing an individual's communication, such as tapping into a telephone call or opening a postal letter, without first obtaining judicial approval. In the digital world, courts have by and large required law enforcement to acquire a warrant before accessing the contents of electronic communications, but have permitted law enforcement to access non-content information such as routing data with lesser process. These cases do not seem to distinguish between cloud-based and traditional forms of Internet services.

Federal courts have applied the SCA to various electronic communications including e-mails, messages sent on social networking sites like Facebook and MySpace, and movies posted on video-sharing sites like YouTube. The process for obtaining these communications under the SCA depends on how long the information has been stored with the service provider and how the provider is classified under the SCA. The relatively few cases dealing with cloud computing have required lesser legal process for accessing electronic communications sent via cloud-based services than traditional forms of Internet computing.

In light of this rapidly changing technology, there have been several legislative proposals to augment the Fourth Amendment's protections for digital communications and update existing statutory protections like the SCA for information shared and stored in the cloud.

Contents

Contacts

Introduction

Although it is difficult to provide a precise definition of "cloud computing," it is generally described as web-based services that allow users to access anything from e-mail to social media to banking to more complex programs like business computing.[1] Traditionally, users would download software and manipulate data on their own computer, while in the cloud, this activity occurs over the Internet on a third-party computer. Many e-mail services like Gmail and Hotmail operate using cloud computing, as do music programs like Grooveshark and Pandora, and social media sites like Facebook and Twitter.[2] Likewise, many smartphone applications employ cloud computing that permits users to store and access large amounts of data. Cloud storage is also on the rise, with an estimated 500 million users by year end, and 1.3 billion users by 2017.[3] Cloud storage services like DropBox, Google Drive, and SkyDrive by Microsoft allow users to store their information on the computer of a third-party and access it from any platform with Internet access.[4]

As cloud computing becomes integrated into our daily lives, a host of personal information (e.g., private communications, financial data, photographs, etc.) will be stored on a server owned by a third party. This raises privacy and security issues, including when and how government may access this information as part of a criminal or other type of investigation. This report first describes cloud computing and how it differs from traditional computing. It then describes how the Fourth Amendment and federal electronic privacy statutes apply to communications in the physical world, to Internet communications generally, and specifically to the cloud. Finally, this report surveys recent legislation and other various proposals designed to update the existing statutory framework.

Privacy for Communications in the Physical World

Because many traditional activities are increasingly being transferred online, it is vital to first understand what privacy protections apply in the physical world before turning to possible protections in the cloud. The Fourth Amendment and federal communication statutes provide the core privacy protections in the physical world.

---

[1] Jonathan Strickland, *How Cloud Computing Works*, HOW STUFF WORKS (October 15, 2012), http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm/printable. The National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." NAT'L INST. STANDARDS & TECH., THE NIST DEFINITION OF CLOUD COMPUTING, Spec. Pub. 800-145, at 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] Rivka Tadjer, *What is Cloud Computing?*, PC MAGAZINE (November 18, 2010), http://www.pcmag.com/article2/0,2817,2372165,00.asp.

[3] Jagdish Rebello, *Consumers Aggressively Migrate Data to Cloud Storage in the First Half of 2012*, IHS iSUPPLI (October 15, 2012), http://www.isuppli.com/Mobile-and-Wireless-Communications/News/Pages/Consumers-Aggressively-Migrate-Data-to-Cloud-Storage-in-First-Half-of-2012.aspx.

[4] Jonathan Strickland, *How Cloud Computing Works*, HOW STUFF WORKS (October 15, 2012), *available at* http://computer.howstuffworks.com/cloud-computing/cloud-storage.htm.

The Fourth Amendment provides, in relevant part, that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]"[5] The primary purpose of the Fourth Amendment is to ensure the privacy of the citizenry and to prevent arbitrary government intrusion into their lives. To determine if the Fourth Amendment applies in a given case, a court tests whether the government activities constitute a *search*. The modern formulation for determining whether certain conduct is a search under the Fourth Amendment derives from Justice Harlan's concurrence in *Katz v. United States*.[6] This test asks "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[7] What is *reasonable* in a given case—the yardstick for all Fourth Amendment analyses—can depend greatly on the facts of the case.[8] However, there are certain lines of cases that provide baseline rules for the protection of communications in the physical world.

The closest analog to an e-mail in the physical world is the postal letter. In 1878, the Supreme Court was asked to rule in *Ex parte Jackson* whether Congress had the constitutional authority to exclude certain obscene material from the U.S. postal system.[9] In discussing the nature of protecting the postal system, the Court observed that

> Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[10]

The Court in *Ex parte Jackson* relied on a content/non-content distinction to find that the inside of the letter (the content) was protected, while the routing information on the outside (non-content) was not subject to similar Fourth Amendment restrictions.

Of more recent vintage, the Court observed in *United States v. Jacobsen* that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."[11] The free flow of mail, however, is not absolute. In *United States v. Leeuwen*, the Court held that government officials may detain packages for a brief period of time without a warrant to confirm

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

[6] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[7] *Id.*

[8] Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'").

[9] *Ex parte* Jackson, 96 U.S. 727 (1877).

[10] *Id.* at 733.

[11] United States v. Jacobsen, 466 U.S. 109, 115 (1984).

the suspicious nature of the package.[12] Additionally, under federal regulations postal workers can record the outside, routing information on letters sent, a technique known as a mail cover, to gather evidence regarding the commission of a crime.[13] These same regulations, however, prohibit postal employees from opening the mail, unless one of the limited exceptions applies.[14]

Like the contents of letters, the contents of a conversation—the words spoken either in person or through a device such as a cell phone or land-line phone—are generally protected under various constitutional and federal statutory provisions. In *United States v. Katz*, the Court held that the contents of an individual's conversation are protected under the Fourth Amendment, even when spoken in a public telephone booth.[15] The Court remarked that an individual who makes a telephone call from a closed telephone booth "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[16] Congress augmented *Katz* in Title III of the Omnibus Crime Control and Safe Streets Act of 1968[17] as amended by the Electronic Communications Privacy Act of 1986 (ECPA),[18] establishing significant restrictions on surreptitious interception of private communications. Commonly referred to as the Wiretap Act, Title III prohibits the intentional interception of telephone, face-to-face, and electronic communications using a mechanical or other device, unless one of several exceptions applies, such as consent of one of the parties to the conversation, or a judicially authorized warrant based upon probable cause.[19]

Although accessing the contents of a telephone communication generally requires a probable cause warrant, access to telephone routing information, including the numbers dialed, requires lesser process. In *Smith v. Maryland*, the Court applied the third-party doctrine to the telephone numbers a person dials to place a call.[20] The third-party doctrine provides that information a person voluntarily conveys to another person is generally not protected by the Fourth Amendment.[21] The Court observed in *Smith* that when the defendant used his phone, he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [he] assumed the risk

[12] United States v. Leeuwen, 397 U.S. 249, 253 (1970) ("No interest protected by the Fourth Amendment was invaded by forwarding the packages the following day rather than the day when they were deposited. The significant Fourth Amendment interest was in the privacy of this first-class mail; and that privacy was not disturbed or invaded until the approval of the magistrate was obtained.").

[13] 39 C.F.R. §233.3(a). Several federal circuit courts have upheld the mail cover practice under the Fourth Amendment. See United States v. Choate, 576 F.2d 165 (9th Cir. 1978); United States v. Huie, 593 F.2d 14 (5th Cir. 1979).

[14] 39 C.F.R. §233.3(g) ("No person in the Postal Service except those employed for that purpose in dead-mail offices, may open, or inspect the contents of, or permit the opening or inspection of sealed mail without a federal search warrant, even though it may contain criminal or otherwise nonmailable matter, or furnish evidence of the commission of a crime, or the violation of a postal statute.").

[15] Katz v. United States, 389 U.S. 347, 359 (1967).

[16] *Id.* at 352.

[17] Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, §801, 82 Stat. 197, 211.

[18] Electronic Communications Privacy Act of 1986, P.L. 99-508, §101, 100 Stat. 1848, 1848.

[19] 18 U.S.C. §2511(1). *See generally* CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by (name redacted) and (name redacted).

[20] Smith v. Maryland, 442 U.S. 735 (1979).

[21] The same theory applies when one party to a conversation records or discloses it. United States v. White, 401 U.S. 745 (1971).

that the company would reveal to police the numbers he dialed."[22] Seven years later, Congress included in ECPA a prohibition against the use of pen registers and trap and trace devices (which can record the incoming and outgoing telephone numbers from a certain customer), unless the government obtained a court order certifying that the information to be obtained is "relevant to an ongoing criminal investigation."[23]

Another crucial form of communication in the modern world that is increasingly moving to the cloud is the transfer of business records. In *United States v. Miller*, the Court applied the third-party doctrine to hold that a bank customer has no legitimate expectation of privacy in banking documents such as checks and deposit slips transferred to a bank in the ordinary course of business.[24] There, the Court observed that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government. … This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[25] In reaction to *Miller*, Congress enacted the Right to Financial Privacy Act, creating a statutory protection for these financial documents.[26]

Privacy for Communications on the Internet

Although the jurisprudence of Internet privacy is in its infancy, the current body of case law sheds light on how the Fourth Amendment and federal statutes apply to the cloud. When applying the Fourth Amendment, it appears that courts have not distinguished between traditional forms of Internet communication and cloud-based communication; the same rules apply to each. However, when applying the Stored Communications Act, cloud computing such as web-based e-mails or messaging through social network sites has not received the robust privacy protections accorded to traditional e-mail services.

Fourth Amendment

For the most part, courts have applied the Fourth Amendment to Internet communications by analogy to the physical world.[27] Like the traditional cases, the outcomes of the Internet cases have hinged on whether the information sought by the government was considered "content" or "non-content."[28] Generally, the courts have held that access to Internet communications that constitute the content of the communication is a search for which a warrant is required. By contrast, access to information that reveals only non-content information such as routing information—including

[22] *Id.* at 744.

[23] 18 U.S.C. §3123(a)(1).

[24] United States v. Miller, 425 U.S. 435, 443 (1976).

[25] *Id.*

[26] Right to Financial Privacy Act of 1978, P.L. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §§3401-3422).

[27] *See* David A. Couillard, *Defogging the Cloud: Applying the Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2219 (2009).

[28] *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1029 (2010).

an Internet Protocol address (IP address) or the to/from address in an e-mail—has been subjected to lesser legal process.

In 2007, the Ninth Circuit Court of Appeals held in *Forrester v. United States* that the government's access to the "non-content" information transferred as part of an Internet communication—such as the to/from address line in an e-mail—did not constitute a search under the Fourth Amendment.[29] In that case, several defendants were allegedly manufacturing ecstasy in violation of federal drug laws. During its investigation, the government sought to intercept defendant Dennis Alba's Internet and e-mail activity. The government received a court order to install a "mirror port" at Alba's Internet service provider, which enabled the government to learn the to/from addresses of his e-mails, the IP addresses of the websites he visited, and the total volume of information sent to or from his account. At trial, Alba claimed that this evidence was obtained in violation of his Fourth Amendment right to be free from unreasonable searches and seizures. In denying Alba's claim, the Ninth Circuit relied on two lines of Fourth Amendment cases. First, the court analogized this routing information to the telephone numbers dialed in the third-party case, *Smith v. Maryland*.[30] Like the defendant in *Smith* who should have expected the numbers he dialed would be revealed to the carrier that would place his call, "e-mail and internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by the service provider for the specific purpose of directing and routing of information."[31] Second, the panel likened the addressing information of electronic communications to the outside address information on physical mail, which is generally not protected under the Fourth Amendment.[32] Because e-mails contain similar addressing information, the court concluded that they are not entitled to Fourth Amendment safeguards.

Like *Forrester*, the Third Circuit Court of Appeals in *United States v. Christie* held that individuals do not have a reasonable expectation of privacy in their IP addresses.[33] This case originated when the FBI acquired the IP addresses of computer users who were accessing child pornography websites. The FBI then requested the names of the users linked to these IP addresses from their ISP. Again, applying the third-party doctrine, the court held that "no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs. IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers."[34]

[29] United States v. Forrester, 512 F.3d 500, 509 (9th Cir. 2007).

[30] Smith v. Maryland, 442 U.S. 735 (1979).

[31] *Forrester*, 512 F.3d at 510.

[32] *See Ex Parte* Jackson, 96 U.S. 727, 732 (1878).

[33] United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010).

[34] *Christie*, 624 F.3d at 574 (internal quotation marks omitted). Court have also held that individuals do not have a reasonable expectation of privacy in their subscriber information. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) ("We conclude that plaintiffs in these cases lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators."); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) ("[The defendant] can point to no evidence that he had a subjective expectation of privacy in his internet and phone 'subscriber information'—i.e., his name, e-mail address, telephone number, and physical address—which the Government obtained through the administrative subpoenas. Bynum voluntarily conveyed all this information to his internet and phone companies. In so doing, [the defendant] 'assumed the risk that th[os]e compan[ies] would reveal [that information] to police.'"); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (same).

Although the panel in *Forrester* concluded that outside address information that is visible to a third-party carrier is not subject to Fourth Amendment protection, it commented in passing that "the *contents* may deserve Fourth Amendment protection" and that certain surveillance techniques may "breach the line between mere addressing and more content-rich information."[35]

In 2010, the Sixth Circuit Court of Appeals in *United States v. Warshak* recognized this difference between content and non-content information, holding that the content of e-mail communications is protected under the Fourth Amendment.[36] There, Warshak was being investigated for a scheme to defraud customers of his company. The government sought and obtained permission from Warshak's ISP to preserve the contents of Warshak's e-mails, and eventually the government was permitted access to approximately 27,000 e-mails. Warshak then moved to suppress this access as forbidden under the Fourth Amendment absent a warrant. The Sixth Circuit held that the contents of the e-mails were protected under the Fourth Amendment. Like the Ninth Circuit decision, the ruling in *Warshak* compared e-mails to physical mail, observing that "[g]iven the fundamental similarities between e-mail and traditional forms of communication, it would defy common sense to afford e-mails lesser Fourth Amendment protection."[37] The panel noted the importance of e-mail as an "indispensable part" of modern society.[38] The panel held that "if government agents compel an ISP to surrender the contents of a subscriber's e-mails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception."[39]

Thus, while slim, this body of case law applying the Fourth Amendment to Internet communications seems to establish several rules. First, for government officials to access the contents of e-mails or other electronic communications, they must obtain a warrant based upon probable cause absent a warrant exception. Second, if the government seeks non-content information such as subscriber information, the to/from line on an e-mail, or the IP addresses of websites visited, a subpoena will generally suffice. Additionally, it does not appear that these courts consider the nature of the e-mail service provided, whether cloud-based or the traditional client-based e-mail, as part of their Fourth Amendment analysis. It would seem that these same rules apply to both types of services.

Stored Communications Act (SCA)

In the early 1980s, Congress voiced concern that electronic communications were not accorded the same privacy as analogous communications in the physical world. The Senate Judiciary Committee observed in 1986 that "[p]rivacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances."[40] Likewise, the House Judiciary Committee noted other problems with unclear legal standards relating to access to electronic communications.[41] The House Committee feared that unclear legal standards would discourage

[35] *Forrester*, 512 F.3d at 511 (emphasis added).

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

[37] *Id.* at 286 ("E-mail is the technological scion of tangible mail, and it plays an indispensable part in the Information Age.... As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise.")

[38] *Id.*

[39] *Id.*

[40] S.Rept. 99-541, at 5 (1986).

[41] H.Rept. 99-647, at 19 (1986).

potential customers from using this new technology. The House Committee was also concerned that police officers who were conducting investigations may face liability or that evidence obtained may not be admissible in a criminal prosecution.[42] In light of these concerns, Congress overhauled federal communication privacy laws in 1986 as part of the Electronic Communications Privacy Act of 1986 (ECPA).[43] The Stored Communications Act (SCA), enacted as Title II of ECPA, was designed to regulate the access and dissemination of electronic communications stored on computers. The SCA has two core components: (1) the procedures the government must follow to compel disclosure of stored communications;[44] and (2) the situations in which a service provider may voluntarily share a customer's communications.[45]

Scope of the SCA

The SCA covers providers of two types of public services: an "electronic communication service," or ECS, and a "remote computing service," or RCS. An ECS provider is any service which allows its customers to "send or receive wire or electronic communications."[46] An ECS provider is prohibited from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service[,]" subject to certain exceptions.[47] "Electronic storage" is in turn defined as information that is stored (1) incidental to the transmission of that communication, or (2) for backup purposes.[48] An RCS provider is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system[.]" An RCS is prohibited, also subject to certain exceptions, from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service."[49]

Required Disclosure of Communications

Section 2703 of the SCA sets forth the procedures the government must follow to gain access to electronic communications, such as e-mails, from an ECS or RCS provider. Section 2703 is tiered—the more content-rich the information sought, the higher the level of evidentiary proof the government must proffer.

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.[50] The same procedure is available for communications stored for *more* than 180 days from an ECS provider or from an RCS provider (no matter how long the communication is stored with it), but there are two other alternatives. If the government provides

[42] *Id.*

[43] Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1848.

[44] 18 U.S.C. §2703.

[45] 18 U.S.C. §2702.

[46] 18 U.S.C. §2510(15).

[47] 18 U.S.C. §2702(a)(1).

[48] "Electronic storage" means "(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." 18 U.S.C. §2510(17).

[49] 18 U.S.C. §2702(a)(2).

[50] 18 U.S.C. §2703(a).

notice to the customer, it can access these older communications with a subpoena or a court order under Section 2703(d).[51] These 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."[52]

In addition to the content of communications, the SCA permits access to non-content information with a warrant, but the government may use a subpoena or a Section 2703(d) order without having to provide the customer notice.[53] To access 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.[54]

Voluntary Disclosure of Communications

Section 2702 establishes when a service provider may voluntarily disclose the content of communications and customer information to another entity. This section applies only to service providers to the "public";[55] thus, nonpublic providers can turn over these documents without any process required.[56] For public providers, the contents of a communication may not be divulged unless one of the eight exceptions in Section 2702(b) applies, which include consent of one of the parties to the communication; as a necessary incident to the rendition of services; in connection with a missing child; inadvertently obtained and pertains to the commission of a crime; or if there is imminent risk of death or serious physical injury to any person.[57] A public provider may release customers' records or other non-content information if it meets one of the six exceptions provided in Section 2702(c), which include consent of the subscriber; as a necessary incident to the rendition of services; and in connection with a missing child.[58]

[51] Under exigent circumstances, notice of court ordered disclosure may be delayed. 18 U.S.C. §2705.

[52] 18 U.S.C. §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).

[53] 18 U.S.C. §2703(c).

[54] 18 U.S.C. §2703(c).

[55] 18 U.S.C. §2702(a)(1).

[56] Universities that provide e-mail to their students and faculty and companies that provide e-mails to their employees do not constitute "public providers" under the SCA. *See* Andersen Constulting LLP v. UOP, 991 F. Supp. 1041, 1042-43 (N.D. Ill. 1998); Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1226 (2004).

[57] 18 U.S.C. §2702(b).

[58] 18 U.S.C. §2702(c).

Application of the SCA

E-mails

It is clear from the text of the SCA that government access to the content of *unopened* e-mails stored for 180 days or less by an electronic communication service requires a warrant.[59] It is also clear that opened or unopened e-mails stored for more than 180 days may be accessed with a subpoena or a Section 2703(d) order, so long as the government provides notice to the subscriber.[60] However, there is a split in the courts as to whether an *opened* e-mail stored 180 days or less is in "electronic storage" under the SCA. The practical result of this definitional breakdown is that police must get a warrant if the communication is in electronic storage, but need only use a subpoena if not. One of the substantial points of departure is how these divided courts view the difference between traditional forms of e-mail such as client-based services and web-based e-mails that rely on cloud technology.

In *Theofel v. Farey-Jones* before the Ninth Circuit Court of Appeals, the defendant Farey-Jones subpoenaed the plaintiffs' ISP provider NetGate for access to "[a]ll copies of e-mails sent or received by anyone" within the plaintiff's company.[61] NetGate provided some, but not all of the e-mails. The plaintiffs sued Farey-Jones under, among other statutes, Section 2701 of the Stored Communications Act, for unlawful access to their e-mail communications. The crux of this issue was whether the e-mails were in "electronic storage" under the SCA.[62] Again, "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.... "[63] If they were in electronic storage, the subpoena used would be insufficient to access the e-mails. The court held that these e-mails were for backup purposes under subsection (B), and observed:

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again-if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.[64]

The Ninth Circuit concluded that "where the underlying message has expired in the normal course, any copy is no longer performing any backup function."[65] *Theofel*'s holding appears to apply when the user downloads a message on his computer and the ISP keeps a copy of the e-mail for "backup protection." However, it is uncertain whether a future court would apply this rule to cloud computing where the only copy of the message is left on the service provider's computer.

---

[59] 18 U.S.C. §2703(a).

[60] 18 U.S.C. §2703(a), (b). Recall that under exigent circumstances, notice of court ordered disclosure may be delayed. 18 U.S.C. §2705.

[61] Theofel v. Farey-Jones, 359 F.3d 1066, 1071 (9th Cir. 2003).

[62] *Id.* at 1075.

[63] 18 U.S.C. §2510(17).

[64] *Theofel*, 359 F.3d at 1075.

[65] *Id.* at 1070.

In passing, the Ninth Circuit noted that "[a] remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes."[66] The court seems to be stating that this rule would not apply to some e-mail providers—possibly cloud providers. One observer has suggested that this dicta in *Theofel* evidences that e-mails stored in the cloud would not be stored for backup purposes, and thus, would not be subject to the more stringent warrant requirement.[67]

The District Court for the Central District of Illinois picked up on this distinction in *United States v. Weaver,* where it had to apply the SCA to a cloud-based e-mail system. There, the government sought e-mails from Justin Weaver's Microsoft Hotmail account as part of its child pornography investigation.[68] The government executed a subpoena to Microsoft seeking any opened or sent e-mail from Weaver's account. Microsoft produced some e-mails to the government, but failed to produce e-mails that had already been opened and those that had been stored for fewer than 181 days. The court had to determine whether these e-mails were in "electronic storage" under Section 2703(a), as defined in Section 2510(17), or "storage" under Section 2703(b)(2).[69] If they were in "electronic storage" then the government should have produced a warrant to access them; if they were not, the subpoena would suffice.

Noting that the e-mails sought by the government were those already opened, the court concluded that they were not in "temporary, intermediate storage" under subsection (A) of Section 2510(17). Turning to subsection (B), the court had to determine if they were being stored for "backup protection." Reviewing the nature of web-based e-mail, which relies on cloud technology, the court observed that "Hotmail users can access their e-mail over the web from any computer, and they do not automatically download their messages to their own computers as non-web-based e-mail service users do. Instead, if Hotmail users save a message, they generally leave it on the Hotmail server and return to Hotmail via the web to access it on subsequent occasions."[70] The court went to say that the result may differ if the "users opt to connect an e-mail program, such as Microsoft Outlook" to their e-mail accounts and download messages to their own computers. However, the court concluded that if someone uses a pure cloud-based e-mail system, those e-mails cannot be stored for "backup purposes" under subsection (B) as they would be the only copy of the e-mails. Once the user opened the e-mail and left it on the Hotmail account, Microsoft was "maintaining the messages 'solely for the purpose of providing storage or computer processing services to such subscriber or customer.'"[71] This made Microsoft an RCS, rather than an ECS provider. Thus, the e-mails were subject only to the subpoena requirement.

Social Networking

In *Crispin v. Christian Audigier, Inc.*, the United States District Court for the Central District of California was asked whether messages sent through private messaging services or through posting on user-created profile pages on social networking sites Facebook and MySpace are

[66] *Id.* at 1077.

[67] Illana R. Katana, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 634-35 (2011).

[68] United States v. Weaver, 636 F. Supp. 2d 769, 769-70 (C.D. Ill. 2009).

[69] 18 U.S.C. §2703(a), (b)(2).

[70] *Weaver*, 636 F. Supp. 2d at 772.

[71] *Id.* (citing 18 U.S.C. §2703(b)(2)).

covered under the SCA.[72] *Crispin* arose as part of discovery requests in private litigation, when defendant Christian Audigier served subpoenas on Facebook and MySpace for access to communications between the plaintiff and a third party. The plaintiff moved to quash the subpoenas, arguing that Facebook and MySpace were prohibited from disclosing the communication under Section 2702(a)(1) of the SCA.[73]

As to the private messages sent on these social networking sites, the court relied on *Weaver* and the dicta in *Theofel* to hold that when messages are opened and retained on the site, Facebook and MySpace operate as RCS providers, and the messages are subject only to the subpoena requirement.[74]

The court next turned to the "wall postings" on Facebook and the MySpace comments page, which permit users to post messages on another user's profile space. The court first analogized these comment pages to the traditional electronic bulletin board services (BBS). A BBS is a website that permits users to post messages on a "board" for the general public to view. Precedent and legislative history established that these bulletin boards were covered under the SCA.[75] However, to be entitled to protection under the SCA, access to messages posted on these sites must be restricted in some meaningful way from the public at large.[76] Facebook and MySpace, the court reasoned, provide a similar function: they permit users to post messages on other users' "walls" so long as they have authorization to do so.[77] Although these social networking sites were considered ECSs, the court still had to determine whether the information had been in "electronic storage" under the SCA. The court concluded that messages that had not been retrieved fell within the first definition of electronic storage—that is, that they were being temporarily stored "incidental to transmission." However, because Crispin had already accessed the messages, they fell within the second electronic storage pathway—stored for backup purposes.[78] Ultimately, the Court remanded the case to the magistrate judge to determine if "either the general public had access to plaintiff's Facebook and MySpace comments, or access was limited to a few."[79] If the latter, the communications would fall under the SCA's protections and the subpoena would be quashed.

YouTube Videos

In *Viacom Intern. Inc. v. YouTube Inc.*, the federal district court for the Southern District of New York had to determine whether access to YouTube videos was governed by the SCA.[80] There, Viacom claimed that videos posted on Google's video-sharing website YouTube violated federal

[72] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[73] *Id.* at 969.

[74] *Id.* at 987.

[75] *Id.* at 981 (quoting United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) ("Thus, the SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system.")).

[76] Citing the Senate Judiciary Committee report issued during congressional consideration of the SCA, the court noted that "to access a communication in such a *public* system is not a violation of the Act, since the general public has been 'authorized' to do so by the facility provider." *Id.* at 981 (citing S.Rept. 99-541, at 36 (1986)).

[77] *Id.* at 981-82.

[78] *Id.* at 989.

[79] *Id.* at 991.

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

copyright law. Viacom requested certain videos from Google as part of its discovery requests. The court first concluded, with little discussion, that Google was an RCS provider under the SCA.[81] It then moved on to the question of whether the SCA permitted such disclosure. Viacom argued that users who posted videos on YouTube have authorized disclosure of those videos under Section 2702(b)(3), which allows the provider to "divulge the contents of a communication ... with the lawful consent of ... the subscriber."[82] The court rejected this argument, observing that, although YouTube's Terms of Use and Privacy Policy provides a disclaimer that any video posted in the public areas of the site may be divulged, none of the provisions in that user agreement "can be fairly construed as a grant of permission from users to reveal to plaintiffs the videos they have designated as private and chosen to share only with specified recipients."[83] Thus, the court held the SCA did not permit Viacom access to those videos that had been marked private by the user who posted them.[84] The court, however, permitted Viacom access to non-content data such as "the number of times each video has been viewed on YouTube.com or made accessible on a third-party website through an 'embedded' link to the video."[85]

Differences in Privacy Protections in the Physical World, Traditional Computing, and Cloud Computing

In summary, there are many similarities between searches in the physical and digital worlds. For instance, for law enforcement to access the contents of a postal letter, it must first obtain a warrant based upon probable cause, but routing information on the outside of the letter does not receive the same protection.[86] This distinction also applies to telephone calls, where law enforcement cannot surreptitiously record the content of one's conversation, but can access the numbers dialed with lesser process.[87] The limited number of courts reviewing this issue under the Fourth Amendment have applied this same content/non-content distinction to electronic communications such as e-mails. To access the content of an e-mail, law enforcement generally must obtain a warrant. To obtain the routing information, such as an IP address or the to/from address of an e-mail, a subpoena will usually suffice.

However, there are also differences between searches in the physical world and the Internet. For example, under the SCA, the government can access the contents of e-mails stored for more than 180 days, and in some circuits, e-mails that have been opened no matter how long they are stored, with a subpoena and notice to the customer. This is a clear difference from the physical world, as the government cannot access one's private physical letters, no matter how long they are stored, without a warrant. Also, in many instances, evidence obtained by an illegal search in the physical world is not admissible in a criminal prosecution under the exclusionary rule. Under the SCA,

[81] *Id.* at 264.

[82] 18 U.S.C. §2702(b)(3).

[83] *YouTube Inc.*, 253 F.R.D. at 265.

[84] *Id.*

[85] *Id.*

[86] *See supra* note 11-14 and accompanying text.

[87] *See supra* note 20-23 and accompanying text.

however, there is no suppression remedy; thus, even evidence unlawfully obtained may be admitted into evidence at trial.[88] In any event, if applicable, the Fourth Amendment provides a baseline threshold which the SCA cannot lessen. [89]

Additionally, the few courts that applied the SCA to e-mail and other Internet communications seem to have created a dividing line between traditional forms of Internet computing and cloud-based computing. For instance, under the Ninth Circuit's approach in *Theofel*, traditional e-mail services are covered under the SCA's more stringent warrant requirement, whereas the cloud-based e-mails in *Weaver* were subject to the lesser subpoena requirement. In *Viacom Intern. Inc.*, Youtube was considered an RCS provider thus also subjecting posted videos to the subpoena requirement. It remains to be seen whether future courts will apply this distinction between cloud-based and traditional forms of electronic communications.

Proposed Changes to the Current Statutory Framework

Several courts, commentators, and government officials alike have called for an overhaul of ECPA, though disagreement may exist as to how to balance the competing interests of the government, the communications industry, and the individual. Senator Patrick J. Leahy, chairman of the Senate Judiciary Committee, observed at a committee hearing that while ECPA is a useful tool for government officials, it is "hampered by conflicting standards that cause confusion for law enforcement, the business community, and American consumers alike."[90] He further observed that "a single e-mail could be subject to as many as four different levels of privacy protections under ECPA, depending on where it is stored and when it is sent."[91] Several observers have also opined on perceived flaws in the SCA: "It is more complicated than it needs to be. It has sections that are redundant and merely confusing. The absence of a statutory suppression remedy has created significant uncertainty about how the statute works. The SCA also offers surprisingly low privacy protections when the government seeks to compel the contents other than unretrieved communications held pending transmission for 180 days or less."[92] The Department of Justice has also called for changes to ECPA, but has cautioned against the implementation of a heightened standard for accessing electronic communications:

---

[88] United States v. Meriwether, 917 F.2d 955, 960 ("The ECPA does not provide an independent statutory remedy of suppression for interceptions of electronic communications.").

[89] There has been some discussion whether permitting access to the content of e-mails with a subpoena or process less than a probable cause warrant is constitutional under the Fourth Amendment. *See* Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 393 (2009). The Sixth Circuit, in an as-applied challenge to the SCA in *United States v. Warshak* held:

> The government may not compel a commercial ISP to turn over the contents of a subscriber's e-mails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's e-mails. Moreover, to the extent that the SCA purports to permit the government to obtain such e-mails warrantlessly, the SCA is unconstitutional.

[90] *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age, Hearing Before the Sen. Comm. on the Judiciary* 2 (April 6, 2011) (statement of Sen. Patrick J. Leahy) [hereinafter ECPA Hearing].

[91] *Id.* at 2.

[92] Kerr, *supra* note 56, at 1243.

> Congress may wish to consider that raising the standard for obtaining information under ECPA may substantially slow criminal and national security investigations. In general, it takes longer for law enforcement to prepare a 2703(d) order application than a subpoena, and it takes longer to obtain a search warrant than a 2703(d) order. In a wide range of investigations, including terrorism, violent crimes, and child exploitation, speed is often judged to be essential.[93]

Legislation has been introduced in the 112th and 113th Congresses, and various measures have been proposed by other entities, to overhaul ECPA.

Recent Legislative Proposals

Recent legislative proposals introduced in the 112th and 113th Congresses aim to clarify and strengthen the requirements for accessing an individual's electronic communications under the SCA. [94] Although the language in each bill differs, several of the provisions in each bill relating to the SCA have the same substantive effect. These bills would

- require a government entity to obtain a warrant based upon probable cause to retrieve the content of information from both providers of electronic communication services and remote computing services;
- eliminate the 180-day rule currently contained in Section 2703(a), so that communications stored for 180 days or 181 days would be treated the same;
- amend Section 2703(a) to not only cover communications in "electronic storage" but also those that are being "held or maintained" by that service;
- require the government to notify the customer of any search conducted under the SCA within three days, including a copy of the warrant, unless delayed notice is permitted under Section 2705; and
- eliminate the ability of providers to voluntarily share content and subscriber information with a government entity unless one of the Section 2702(b) exceptions applies.

Additionally, H.R. 6399 from the 112th Congress would have also

- created a statutory suppression remedy for violations of the SCA;[95]

---

[93] ECPA Hearing, *supra* note 90, at 5 (statement of James Baker, Associate Deputy Attorney General).

[94] There were three bills introduced in the 112th Congress: the Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong., 1st Sess. (2011), filed by Senator Patrick J. Leahy, the ECPA 2.0 Act of 2012, H.R. 6529, 112th Cong., 2d Sess. (2012), filed by Representative Zoe Lofgren, and the Electronic Communications Privacy Act Modernization Act of 2012, H.R. 6399, 112th Cong., 2d Sess. (2012), filed by Representatives Jerrod L. Nadler and John Conyers, Jr. In the 113th Congress, Rep. Lofgren re-introduced her measure, which is now entitled the Online Communication s and Geolocation Protection Act, H.R. 983, 113th Cong., 1st Sess. (2013).

[95] This suppression remedy would be similar to the exclusionary rule under the Fourth Amendment. In the Fourth Amendment context, evidence unlawfully obtained in violation of its prohibition against unreasonable searches and seizures cannot be admitted in a criminal prosecution against the defendant whose rights were violated. Mapp v. Ohio, 367 U.S. 643, 655 (1961). This is known as the exclusionary rule. The Supreme Court has held that the primary purpose of the exclusionary rule is its deterrent effect:

> [T]he rule's prime purpose is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures: "The rule is

(continued...)

- required the Administrative Office of the United States Courts to report annually to Congress on how many orders or warrants were sought and issued concerning the contents of electronic communications; and
- required a provider to report annually to the Administrative Office of the United States Courts the number of legal demands it has received from federal, state, and local law enforcement agencies, and the number of accounts about which information was disclosed. The providers can receive compensation for the costs of compiling these records.

Other Proposals

Uniformity and Technology Neutrality

Although each of the legislative proposals above would apply the same rules to both ECS and RCS providers, it is not clear that this approach would sufficiently capture all of the various communications that occur in the cloud. As some observers have pointed out, sites such as eBay, which permit users to buy and sell items online, are probably not ECS providers, as they do not provide users the ability to send or receive communications on the Internet.[96] And it has been argued that the site is not an RCS provider, as it does not provide "processing service" for its users, although he notes this debate is ambiguous at best as this term is neither defined by statute nor construed in any case. Thus, even if Congress applies the same rules to both ECS and RCS providers, some cloud services such as eBay might still not be covered. Congress could either draft language specifically covering cloud services, or draft a broad definition for the class of entities that would come within the SCA's ambit, preferably aiming for technology neutrality.

Another observer offered the following language, which intends to rescind the 180-day rule, apply the same rules to all service providers, and provide protections even if a message has been received or downloaded by the user:

> A governmental entity may only require a provider of communications services to disclose the contents of a wire or electronic communication, if transmitted or stored electronically, only upon the issuance of a warrant by a court of competent jurisdiction, whether or not the provider stores the communication after receipt by the user, and regardless of whether the communication remains on the server after receipt or is downloaded to the user's device.[97]

(...continued)

> calculated to prevent, not to repair. Its purpose is to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it.

United States v. Calandra, 414 U.S. 338, 347 (1974) (quoting Linkletter v. Walker, 381 U.S. 618, 637 (1965)).

[96] The legislative history asserts that "[e]xisting telephone companies and electronic mail companies" are examples of electronic communication services. S. Rpt. 99-541, at 14. In *Crowley v. CyberSource Corp.*, the court held that Amazon.com, an on-line retailer, was not an electronic communication service, even though communications could be sent to and from its site. Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001).

[97] Kattan, *supra* note 67, at 654

Consent Provisions

Currently, there is an exception under ECPA for interceptions made with prior consent of one of the parties to the communication.[98] However, ECPA does not define "consent." For instance, does clicking on a user agreement when one signs up for Gmail or Hotmail suffice as consent for these providers to access the content of one's e-mails and share them with the government? One commentator has suggested that the consent requirement should be clarified:

> Notably, an e-mail service might scan the contents of customers' e-mail messages for content that suggests an interest in certain products and may provide that information to behavioral advertising agencies that create consumer databases and feed online ads on behalf of their clients. Under ECPA, those service providers have violated the law if they have not obtained user consent for those practices. Unfortunately, ECPA's failure to define consent leaves users and service providers without guidance on this point. Is a consumer's decision to use a monitored e-mail service, after being given an opportunity to read a privacy policy, sufficient to indicate consent? Or should explicit opt-in consent, pursuant to conspicuous notice, be required?[99]

As an example of this opt-in regime, as part of the Driver's Privacy Protection Act, Congress required state motor vehicle departments to receive the express consent of individuals before sharing certain personal information.[100] A similar approach could be implemented with ECPA.

Conclusion

The Supreme Court once remarked that when an individual "puts something in his filing cabinet, in his desk drawer, or in his pocket, he has the right to know it will be secure from an unreasonable search or an unreasonable seizure."[101] Does this proposition hold true today when people turn to digital desk drawers, digital filing cabinets, and digital pockets? For the most part, many of the protections that apply to the physical world have been transferred to the digital world. In the physical world the contents of letters, telephone calls, and other forms of communication are generally protected by the Fourth Amendment's prohibition against unreasonable searches and seizures. The limited number of courts reviewing the question have held that the content of Internet communications are similarly protected from government searches under the Fourth Amendment. These protections may be supplemented by the SCA, which accords varying degrees of privacy safeguards to both public and private intrusions, depending on how long the communication has been stored and how the provider of the network service is classified under its complicated definitions. Additionally, courts have occasionally applied lesser degrees of protection to communications sent and received through cloud-based services than with traditional forms of Internet communications, based on the manner the information is stored by each, and how such storage is defined under the SCA. Recent legislative proposals would apply the same rules to communications in the physical and digital worlds and between traditional computing and cloud computing.

---

[98] 18 U.S.C. §2511(2)(d).

[99] Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 159 (2011).

[100] 18 U.S.C. §2721.

[101] Hoffa v. United States, 385 U.S. 293, 301 (1966).

Author Contact Information

(name redacted)

Legislative Attorney
[redacted]@crs.loc.gov, 7-....