Notre Dame Law Review

Volume 86
Issue 5 *Symposium: Creativity and the Law*

Article 15

9-1-2011

# Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing

Hien Timothy M. Nguyen

# CLOUD COVER: PRIVACY PROTECTIONS AND THE STORED COMMUNICATIONS ACT IN THE AGE OF CLOUD COMPUTING

*Hien Timothy M. Nguyen**

## INTRODUCTION

Internet technology has completely revolutionized the way people interact, how companies transact business, and the type and amount of information that is available to the public. From its beginnings as a forum for users to transmit messages to the emergence of social networking and media services, each stage of development has transformed the way we live. Cloud computing has been heralded as the next stage in this evolution, with the potential to transform how both individual users and companies use computers and the Internet. Yet, what is cloud computing and what are the privacy implications for its users?

Cloud computing concerns "both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services."[1] The basis of "the cloud is a collection of [interconnected] computers and servers that are publicly accessible via the Internet."[2] Individual users connect to the cloud from their own computing devices, over the Internet, and "the cloud is seen as a single application, device, or document."[3] The hardware in the cloud, which is the collection of computers and serv-

* Candidate for Juris Doctor, Notre Dame Law School, 2012; B.A., Political Science, University of California, Santa Barbara, 2008. Many thanks to Professor Patricia Bellia, the Notre Dame Law Review, and Wendy Tran for their helpful comments and careful edits on this Note. I would also like to thank Christine Chiang for her support and encouragement throughout law school. Finally, I would like to thank my family, Ruc, Kim, Elizabeth, and Danielle, for their unceasing love and support.

1 Michael Armbrust et al., *Above the Clouds: A Berkeley View of Cloud Computing*, UC BERKELEY RELIABLE ADAPTIVE DISTRIBUTED SYSTEMS LAB., 1 (Feb. 10, 2009), www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

2 MICHAEL MILLER, CLOUD COMPUTING 16 (2009).

3 *See id.*

ers, is invisible to the end user.[4] For example, a cloud service such as Google Docs allows me to create documents from my home by logging into Google's website. I, or other authorized users, can then edit that same document while at school, at the airport, or at the library. If someone steals my laptop or if its hard drive crashes, I will still have a copy on the cloud service (and perhaps multiple backups of older versions). Similar services exist for users to purchase computing power[5] or storage space[6] that is accessible on any computer. In the case of computing power, a user developing an application would save on physical space, avoid the cost of buying, maintaining, and operating the servers, and benefit from scalability.

As with most technological advancements, the law is often slow to catch up. While users might have an expectation that the files or applications they store on the cloud are private, the reality is that they may not have as much privacy as they would like to believe.[7] The architecture of the Internet and the way cloud computing services operate means that courts are unlikely to apply Fourth Amendment protections. The current federal statutory framework governing stored electronic communications, the Stored Communications Act[8] (SCA) remains frozen in a 1980s conception of electronic communi-

4 *See id.*

5 *See, e.g.*, *Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2 (last visited Sept. 6, 2011); *Google App Engine*, GOOGLE, http://code.google.com/appengine (last visited Sept. 6, 2011); *Windows Azure*, MICROSOFT CORP., http://www.microsoft.com/windowsazure (last visited Sept. 6, 2011).

6 *See, e.g.*, DROPBOX, http://www.dropbox.com (last visited Sept. 6, 2011); SUGARSYNC, https://www.sugarsync.com (last visited Sept. 6, 2011).

7 Some notable statements have been made with regards to the lack of privacy one can expect on the Internet. *See, e.g.*, Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, THE GUARDIAN (Jan. 11, 2010), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy (reciting Facebook founder Mark Zuckerberg's comment that privacy is "something that has evolved over time" and that "[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people"); Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED NEWS (Jan. 26, 1999), http://www.wired.com/politics/law/news/1999/01/17538 (reciting the comment of Sun Microsystems's CEO Scott McNealy that "[y]ou have zero privacy anyway. . . . Get over it."); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON 1–3 (2004) (discussing "digital dossiers," or collections of detailed information about individuals based on their online activities). However, in the case of many cloud computing services, the privacy expectation lies in the *content* of the data stored or transmitted through the cloud. This is similar to how one might retain an expectation of privacy in a rental locker, but not necessarily the *record* that one has a locker with a particular service. *See infra* notes 37, 107–08 and accompanying text.

8 18 U.S.C. §§ 2701–2712 (2006).

cations. It is a confusing statute[9] that the courts have interpreted in an inconsistent and unclear manner.[10]

This Note argues that the Stored Communications Act and its privacy protections are inadequate in the modern age of cloud computing, especially where users of cloud services might naturally have an expectation of such protection. The Internet has proven itself to be a driving force for economic and technological growth, and cloud computing promises to be the next step in its evolution. However, one legal obstacle to the widespread adoption of cloud computing technologies, especially among corporate users, is that the current legal framework offers inadequate privacy protections. As a result, I propose several amendments to the SCA to bring it up to date with modern technology. In Part I, this Note examines the current state of legal protections for online privacy. I start with the Fourth Amendment and explain how, as it is currently interpreted, Fourth Amendment protections are unlikely to apply to Internet communications because of the third-party doctrine, which holds that users do not have a reasonable expectation of privacy for information disclosed to third parties. Then, I consider the Stored Communications Act, which was Congress's attempt to fill the void of privacy protections for stored electronic communications. In Part II, I discuss the advancements in technology since the SCA, especially the trend towards increased use of cloud computing services. In Part III, I address why the SCA may not be applicable to many of these cloud services. Finally, in Part IV, I discuss expectations of privacy in the cloud and why Congress ought to enhance the SCA's privacy protections. I also propose three modifications to the SCA to achieve this aim of greater privacy protections in the cloud computing age. I will argue that Congress should eliminate the distinction between electronic communications services and remote computing services, that the statute should include a suppression remedy, and that Congress should clarify the

9 *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain a confusing and uncertain area of the law.").

10 *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (finding that an e-mail acquired from post-transmission storage was in "electronic storage," because the ISP saved it for purposes of "backup protection"), *with In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (stating that an e-mail is only in electronic storage "incident to [its] transmission" and only until downloaded), *and* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633–34, 636 (E.D. Pa. 2001) (finding that "backup protection" includes only temporary backup storage pending delivery and thus an e-mail acquired from post-transmission storage was not in electronic storage).

limits of voluntary disclosures. I justify these changes based on the privacy interest that users retain in their use of cloud services.

## I. LEGAL PROTECTIONS FOR ONLINE PRIVACY

The right to privacy has been described as "the most comprehensive of rights and the right most valued by civilized men."[11] However, conceptualizing this right has been a "contested endeavor."[12] Some scholars contend that protection of privacy promotes individual autonomy and is essential to deliberative democracy,[13] while others argue for privacy based on economic efficiency.[14] One scholar, Ken Gormley, identified four major approaches to privacy: (1) Roscoe Pound and Paul Freund's view that privacy was "an expression of one's *personality* or *personhood*, focusing upon the right of the individual to define his or her essence as a human being";[15] (2) scholarship like Louis Henkin's marking of privacy "within the boundaries of *autonomy*—the moral freedom of the individual to engage in his or her own thoughts, actions and decisions";[16] (3) scholarship such as Alan Westin and Charles Fried's understanding of privacy "in terms of citizens' ability to *regulate information* about themselves, and thus control their relationships with other human beings, such that individuals have the right to decide 'when, how, and to what extent information about them is communicated to others'";[17] and (4) the view of scholars like Ruth Gavison who have "taken a more noncommittal, mix-and-match approach, breaking down privacy into two or three essential compo-

11 Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

12 Danielle Keats Citron & Leslie Meltzer Henry, *Visionary Pragmatism and the Value of Privacy in the Twenty-First Century*, 108 MICH. L. REV. 1107, 1107 (2010); *see also* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978) ("The concept of 'privacy' is elusive and ill defined.").

13 *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–28 (2000) (contending that informational privacy promotes individual autonomy, which comports with values of individual dignity and equality, promotes diversity of speech and behavior, and is essential to participation in a democratic society); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651–53 (1999) (arguing that strong information privacy rules are necessary for deliberative democracy and individual self-determination, which would be limited if widespread and secret surveillance were the norm); *see also* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 388–91 (2008) (arguing that intellectual privacy, or the protection of records of our intellectual activities, is essential to First Amendment free thought and expression).

14 *See* Posner, *supra* note 12, at 404.

15 Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1337.

16 *Id.*

17 *Id.* at 1337–38 (quoting ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)).

nents," such as "secrecy, anonymity and solitude"[18] or "repose, sanctuary and intimate decision."[19]

With these often intertwined understandings[20] in mind, the rapid development of new technologies—particularly in the area of the Internet—has presented many new and unforeseen challenges for the protection of privacy,[21] especially since there is a tension in information privacy law between privacy and security.[22] The proliferation of new technologies also brings with it more elaborate record-keeping systems that can reveal the most intimate details of a person's life.[23] Yet, new ways of conducting business and social interactions on the Internet also allow for additional threats to citizens and the State. Security involves society's interest in protecting against these threats, which often includes monitoring and information-gathering activities.[24] These activities also often pose a serious threat to citizens' privacy, because of the vast amount of information that they can reveal.[25] Much of privacy law seeks to provide some sort of balance between these competing interests. This Part examines the primary constitutional mechanism for protecting privacy, the Fourth Amendment, as well as the relevant statute for protecting one's privacy in stored electronic communications—the Stored Communications Act.

### *A. The Fourth Amendment and Its Limits*

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against

18 *Id.* at 1338 (quoting Ruth Gavison, *Privacy*, 89 YALE L.J. 421, 433 (1980)).

19 *Id.* (quoting Gary L. Bostwick, Comment, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 CALIF. L. REV. 1447, 1447 (1976)).

20 *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 19 (1997).

21 *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 1 (2d ed. 2009).

22 *See id.* at 77.

23 The extensive records of an individual, which Daniel Solove termed "digital dossiers," and the "horde of aggregated bits of information [can be] combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002).

24 *See* SOLOVE & SCHWARTZ, *supra* note 21, at 77.

25 *Cf. id.* ("Throughout the twentieth century, technology provided the government significantly greater ability to probe into the private lives of individuals."). As the Sixth Circuit noted, "[b]y obtaining access to someone's email, government agents gain the ability to peer deeply into his activities" because everything from lovers' exchanges to business plans are exchanged over e-mail, providing for "an account of its owner's life." United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).

unreasonable searches and seizures, shall not be violated."[26] The Supreme Court has recognized that "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[27] Although this has been interpreted to allow for strong protections for a person in his or her physical home,[28] the architecture of the Internet and the way users create, store, and access information on their computers means that Fourth Amendment protections for Internet communications are either unclear or may not exist at all.[29] A typical Internet user does not have a physical "home" or any truly private space on the Internet, but rather different types of accounts with different service providers that are used to store information.[30] These accounts consist of data that is stored on remote servers and the user's private information is sent to private third parties through their remote computers.[31]

With this in mind, the biggest difficulty in applying current Fourth Amendment doctrine to Internet communications is the courts' narrow interpretation of the Fourth Amendment's reasonable expectation of privacy test in communication networks.[32] Because an individual does not have a reasonable expectation of privacy in information revealed to third parties,[33] and since the architecture of the Internet necessitates data transfers to third-party servers, courts have traditionally been reluctant to find that Internet users retain a reasonable expectation of privacy in information they send over the

26 U.S. CONST. amend. IV.

27 Schmerber v. California, 384 U.S. 757, 767 (1966).

28 *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).

29 *See In re* United States, 665 F. Supp. 2d 1210, 1213 (D. Or. 2009) ("This feature of the Internet has profound implications for how the Fourth Amendment protects Internet communications—if it protects them at all. The law here remains unclear and commentators have noted that there are several reasons that the Fourth Amendment's privacy protections for the home may not apply to our 'virtual homes' online."); 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, 1209–10 (2004).

30 *See* Kerr, *supra* note 29, at 1209–10.

31 *See id.*

32 *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 627 (2003).

33 *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he 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.").

Internet.[34] Furthermore, "the Fourth Amendment does not apply to a search or seizure . . . effected by a private party on his own initiative . . . [unless] the private party acted as an instrument or agent of the Government."[35] As most Internet communications services are private actors, there would be no Fourth Amendment protection when a provider searches its own servers for a user's data and discloses it to the government or a third party.[36] Thus, although the Fourth Amendment provides citizens with strong protections from government intrusion into physical spaces, its protections are much more limited in the context of cyber spaces on the Internet.[37]

---

34 *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333–36 (6th Cir. 2001) (finding that there was no expectation of privacy in materials intended for publication or public posting, in e-mail that had already reached its recipient, and in non-content subscriber information disclosed to a user's Internet service provider); *In re United States*, 665 F. Supp. 2d at 1224 (using the third-party doctrine to find that since the defendants voluntarily, by their acquiescence to the ISP's privacy policy, conveyed to the ISPs and exposed to the ISP's employees the contents of their e-mails, there was no Fourth Amendment violation). *But see* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (finding that Fourth Amendment protection applied to contents of e-mail communications, because individuals maintain reasonable expectations of privacy in e-mails). The recent *Warshak* decision highlights the changes in our understanding of technology, its role in our lives, and how the SCA protects privacy. The court analogized an e-mail to a letter or phone call, and the commercial ISP as "the functional equivalent of a post office or a telephone company." *Id.* at 286. Since Fourth Amendment protections apply to letters passing through the post office or telephone calls, the court concluded that the police could not seize the contents of Warshak's e-mail with merely a subpoena. *Id.* at 288.

35 *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (citing United States v. Jacobsen, 466 U.S. 109, 113–14 (1984); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).

36 *See, e.g.*, United States v. Richardson, 607 F.3d 357 (4th Cir. 2010) (finding that the defendant was not entitled to Fourth Amendment protections when AOL, an Internet service provider with whom the defendant had an e-mail account, reported the defendant's use of its e-mail services to transmit child pornography); United States v. Jarrett, 338 F.3d 339, 346–47 (4th Cir. 2003) (finding that an anonymous hacker who performed a search on the defendant's computer was a private actor and not acting as a government agent, and thus there was no Fourth Amendment violation).

37 This is not without controversy, as noted above at note 29, because some courts have suggested that users do retain a reasonable expectation of privacy in their e-mail. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not."); United States v. Cioffi, 668 F. Supp. 2d 385, 390 n.7 (E.D.N.Y. 2009) ("One preliminary matter is *not* in question: The government does not dispute that [the defendant] had a reasonable expectation

### *B. The Stored Communications Act*

To address the uncertainty in the area of the Internet and electronic communications, Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act.[38] By passing the SCA, Congress hoped to encourage the development and use of new and emerging methods of communication through protecting citizens' privacy expectations.[39] The SCA (1) limits the government's ability to compel providers to disclose information that they are storing and (2) limits the provider's ability to disclose information to both governmental and non-governmental entities voluntarily.[40] It does this by differentiating between two broad categories of providers: (1) electronic communications services (ECS) and (2) remote computing services (RCS). The level of privacy protection afforded to a stored communication differs based on which category the communication provider falls in (for that communication), and in some instances, how long the communication has been stored.

---

of privacy in the contents of his personal email account."). Some scholars also advocate application of the Fourth Amendment to the Internet. *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 125 (contending that e-mail users generally retain a reasonable expectation of privacy in the e-mails stored on their ISPs' computers). Professor Patricia Bellia points out that the situation of an electronic communications service provider is more similar to the telephone company in *Katz v. United States*, 389 U.S. 347 (1967), where there was a reasonable expectation of privacy in using a phone booth, than *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), where one lacks an expectation of privacy in one's bank records or the telephone number one dials. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403–06 (2004). In *Miller* and *Smith*, the information was conveyed so that the third party could do something with that information, such as provide banking services or put through a telephone call. *See id.* at 1403. In the case of an electronic communications service provider, the contents of the communications are not necessary or relevant for the service provider to transmit the communication. *See id.* Furthermore, as in *Katz*, even though the provider might have the technical ability to "listen" in to the contents, the user still expects the communications to be private. *See id.* at 1405.

38 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.); S. REP. No. 99-541, at 1–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555–57.

39 *See* S. REP. No. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

40 *See* 18 U.S.C. § 2702 (2006) (stating the statute's provisions for a provider's voluntary disclosures); *id.* § 2703 (stating the statute's provisions for the government's ability to compel a provider's disclosure).

### 1. Electronic Communications Services

In the technology world of 1986, electronic communications services mainly dealt with data transmissions and electronic mail.[41] The SCA defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[42] The statute also distinguishes between those communications that are in "electronic storage" and those that are not. Electronic storage is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission . . . [and] any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[43]

As for what is required of the government to compel disclosure, § 2703(a) requires presenting a search warrant if the provider has held the communication in "electronic storage" for 180 days or less.[44] If the communication has been held for more than 180 days (or is held by an RCS), then § 2703(b) allows for the government to compel disclosure with less than notice to the subscriber and a search warrant.[45] The government can use a search warrant without notice to the subscriber, or can present the provider with an administrative or grand jury subpoena and provide notice to the subscriber, or can secure a court order under § 2703(d) of the statute.[46] A "2703(d) order is not equivalent to a search warrant"[47] and may be issued if the government can demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[48] If the information sought is the subscriber's identifying information, such as his or her name, addresses (physical, e-mail, or IP), or phone number, then only a subpoena is required.[49] Alternatively, a service provider can voluntarily

---

41 *See* H.R. REP. No. 99-647, at 21–23 (1986).

42 18 U.S.C. § 2510(15). An "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id.* § 2510(12).

43 *Id.* § 2510(17).

44 *Id.* § 2703(a).

45 *Id.* § 2703(b).

46 *Id.*

47 Bellia, *supra* note 37, at 1417.

48 18 U.S.C. § 2703(d).

49 *Id.* § 2703(c)(2). An Internet Protocol (IP) address is the "numerical address by which a location in the Internet is identified." *Glossary*, INTERNET CORP. FOR

disclose the subscriber's identifying information to any non-governmental entity.[50] When it comes to voluntary disclosures of data, the SCA only allows a public service provider (one that offers its services to the public) to disclose the data if it meets one of the exceptions in § 2702(b).[51] However, if the service provider is private (one that does not provide services to the general public), then it is not bound by the disclosure limitations of the SCA.[52]

For purposes of ECS classification, electronic storage covers (1) temporary and intermediate storage of a communication incidental to the transmission and (2) storage for backup protection of the communication. If a user has not retrieved a communication, then it is in electronic storage, because "its storage by the service provider is 'temporary,' 'intermediate,' and 'incidental' to its transmission."[53] If the service provider retains copies of the unopened communication in the event of a service disruption, that would also qualify as being in electronic storage.[54] The cases become more problematic where the communication has been opened, but retained by the service provider on the user's behalf.[55]

Courts have differed in their interpretation of what "electronic storage" includes.[56] The Ninth Circuit's approach in *Theofel v. Farey-Jones*[57] claims that an Internet service provider's copy of the message functions as a "backup" for the user (as opposed to "backup" only including temporary backup storage pending delivery).[58] However, some scholars have claimed that the Ninth Circuit's reasoning is "strained"[59] and "relies on the assumption that users download emails from an ISP's server to their own computers."[60] Although that is how many e-mail systems work (such as in a work or university environment), many other e-mail systems are "web-based" and "remote."[61] These e-mail systems function similarly to many cloud computing ser-

---

ASSIGNED NAMES AND NUMBERS (Aug. 13, 2010), http://www.icann.org/en/general/glossary.htm.

50 18 U.S.C. § 2702(c)(6).

51 *Id.* § 2702(a).

52 *Id.*

53 Bellia, *supra* note 37, at 1417.

54 *See id.*

55 *See id.*

56 *See supra* note 10 and accompanying text.

57 359 F.3d 1066 (9th Cir. 2004).

58 *Id.* at 1075.

59 *See* Bellia, *supra* note 37, at 1419; Kerr, *supra* note 29, at 1217–18.

60 *See* United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).

61 *Id.* (citing Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 917 (W.D. Wis. 2002)). Web-based e-mail, where the e-mails are stored on the cloud, can

vices, in that they are accessible over the web from any computer and do not automatically download the messages or data to the user's own computer.[62] A user may view the message on the website, save it on the remote server, and re-access it later on the remote server.[63] As *Theofel* notes, "[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."[64] Thus, even under the Ninth Circuit approach, it is very unlikely that data stored on cloud computing services will have the benefit of warrant protection.

### 2. Remote Computing Services

Congress intended the SCA's category of remote computing services to cover outsourced computer processing and data storage.[65] In the era in which Congress enacted the SCA, users would outsource data storage and large amounts of computer processing to remote servers.[66] As these remote computing services were third-party services that would need a copy of the user's data, they raised privacy concerns over the handling of such data.[67] In addition to meeting the definition that a provider offers to the *public* "computer storage or processing services by means of an electronic communications system,"[68] a provider must also satisfy some other requirements. The

---

include some more popular types of e-mail services, such as Gmail, Hotmail, or Yahoo! Mail.

62 *See id.*

63 *See id.*

64 *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004).

65 The Senate Report on the SCA noted that:

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

S. REP. No. 99-541, at 10–11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564–65.

66 *See id.* at 3, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

67 *See id.*

68 18 U.S.C. § 2711(2) (2006).

data must be received electronically from the customer[69] and the content must be "carried or maintained" by the service provider "solely for the purpose of providing storage or computer processing services" to the customer.[70] Furthermore, the provider cannot be authorized to "access the [customer's] content[ ] . . . for purposes of providing any services other than storage or computer processing."[71] Communications stored under the remote computing services category receive less protection than those that qualify as held under electronic communications services. Communications can be compelled by a subpoena with notice, a § 2703(d) order with notice, or a search warrant.[72]

## II. THE CLOUD COMPUTING CONTEXT

The concept of outsourcing computing processes and storing data on remote servers is not new, but advancements in technology have made it a more viable option for users.[73] The emergence of personal computing in the 1980s meant that there was a focus on the individual computer. Thus, software programs ran individually on each computer and documents were stored on the computer on which they were created.[74] Networking quickly developed as a way for corporate users to share files, exchange messages, and backup valuable data.[75] By the early 1990s, the Internet emerged[76] and since then has grown exponentially into a global platform that facilitates much of the world's social, economic, and political activity. With more people than ever connected to the Internet, its technologies play a vital role in the day-to-day lives of many people.

In recent years, the proliferation of broadband Internet connections has enabled the development of new technologies that take advantage of such connections, such as cloud computing. The National Institute of Standards and Technology defines three basic types of cloud computing services: (1) Cloud Software as a Service

69 *See id.* §§ 2702(a)(2)(A), 2703(b)(2)(A).

70 *See id.* §§ 2702(a)(2)(B), 2703(b)(2)(B).

71 *Id.* § 2702(a)(2)(B).

72 *Id.* § 2703.

73 *See* Armbrust, *supra* note 1, at 2 ("*Cloud Computing* is a new term for a long-held dream of computing as a utility, which has recently emerged as a commercial reality." (footnote omitted)).

74 *Cf.* MILLER, *supra* note 2, at 18 (touting the benefit of cloud computing arising from its holding multiple copies of documents, rather than simple storage on the creator's hard drive).

75 *See* PAUL E. CERUZZI, A HISTORY OF MODERN COMPUTING, 292–95 (2d ed. 2003).

76 *See id.* at 295–96.

(SaaS), (2) Cloud Platform as a Service (PaaS), and (3) Cloud Infrastructure as a Service (IaaS).[77] SaaS involves the "capability provided to the consumer . . . to use the provider's applications running on a cloud infrastructure."[78] This can range from productivity applications such as word processing, spreadsheet, and presentation programs[79] to entertainment hubs (video and music)[80] and video conferencing systems.[81] PaaS involves the "capability provided to the consumer . . . to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider."[82] PaaS providers furnish "the entire application environment including hardware, operating system, and application platform,"[83] so that IT organizations or aspiring developers can quickly create and manage applications. An example of this is Microsoft's Windows Azure, which "provide[s] the functionality to build applications that span from consumer Web to enterprise scenarios."[84] Finally, IaaS involves the "capability provided to the consumer . . . to provision processing, storage, networks, and other fundamental computing resources."[85] Instead of a complete platform, IaaS providers supply only the necessary resources that organizations require. An example might be Netflix, an established online video rental service, moving its existing Internet technology to the cloud via Amazon Web Services.[86]

---

77 *See* Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. OF STANDARDS & TECH (Oct. 7, 2009), http://csrc.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

78 *Id.*

79 *See, e.g.*, *Microsoft Office Web Apps*, MICROSOFT CORP., http://office.microsoft.com/en-us/web-apps (last visited Sept. 6, 2011).

80 *See, e.g.*, *Qriocity*, SONY NETWORK ENT. INT'L, http://www.qriocity.com/us/en (last visited Sept. 6, 2011); *Watch Instantly*, NETFLIX, https://www.netflix.com/BrowseGenres/Watch_Instantly/gev (last visited Sept. 6, 2011). These services often advertise their ability to let users select from a large library of music or videos at any given time, from anywhere the user may be.

81 *See, e.g.*, *Cisco Collaboration Cloud*, CISCO, http://www.cisco.com/en/US/prod/ps10352/collaboration_cloud.html (last visited Sept. 6, 2011) (advertising its "Consistent Availability," "Scalable Architecture," and "Built-In Outage Protection").

82 Mell & Grance, *supra* note 77.

83 Drue Reeves, *Microsoft Windows Azure, Demystified*, CIO (Dec. 4, 2008), http://www.cio.com/article/468413/Microsoft_Windows_Azure_Demystified.

84 *Microsoft Windows Azure*, MICROSOFT CORP., http://www.microsoft.com/windowsazure/faq (last visited Sept. 6, 2011).

85 Mell & Grance, *supra* note 77.

86 Brad Stone & Ashlee Vance, *'Cloud' Computing Casts a Spell*, N.Y. TIMES, April 19, 2010, at B1.

Cloud computing has been heralded as being potentially transformative for the way individuals use and interact over the Internet. Cloud computing allows a user to access his or her data from *any* computer and facilitates collaboration among multiple users.[87] Unlike traditional networking, where a user could only access data if he or she was logged on to the particular network, cloud computing allows access from anywhere over an Internet connection.[88] Furthermore, users can benefit from not having to install additional resource intensive applications on their computers (aside from a web browser) in order to access cloud services.[89] For example, a person who needs to create a document might choose to do so on Google Docs or Microsoft Office Web instead of installing word processing software on the computer.

In the corporate environment, cloud computing also provides many benefits. Cloud computing provides scalability, which can be especially beneficial to emerging companies. Rather than being forced to invest in equipment,[90] software, and personnel to maintain the systems, companies can purchase computing power and storage space from a cloud provider.[91] Cloud computing provides for flexible "*usage-based pricing*,"[92] because the "hours" purchased through cloud computing "can be distributed non-uniformly in time (e.g., use 100 server-hours today and no server-hours tomorrow"[93] and the company will only have to pay for the hours it uses.[94] In the event of a business slowdown, where a company needs to scale down its resource usage, cloud computing might reduce or even eliminate the financial loss of having under-utilized equipment.[95] If a business needs to scale up its resource usage, cloud computing allows it to add resources quickly, with very short lead-time of minutes or hours (instead of days or weeks to procure the physical equipment), which allows the matching of

87 *See* MILLER, *supra* note 2, at 12.

88 *See id.* at 8–9.

89 *See* David S. Barnhill, Note, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 640–41 (2010).

90 Armbrust et al., *supra* note 1, at 10 ("[T]he absence of up-front capital expense allows capital to be redirected to core business investment.").

91 *See* Bruce Gain, *Cloud Computing of the Future*, 32 PROCESSOR, Feb. 26, 2010, at 14, *available at* http://www.processor.com/editorial/article.asp?article=articles/P3205/23p05/23p05/23p05.asp; Eric Knorr & Galen Gruman, *What Cloud Computing Really Means*, INFOWORLD (April 7, 2008), http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031.

92 Armbrust et al., *supra* note 1, at 10.

93 *Id.*

94 *Id.*

95 *See id.* at 12.

resources to workload much more closely.[96] For example, an Internet retailer might be extremely busy during the holidays, but far less busy during the rest of the year. Cloud computing allows for the retailer to purchase additional resources during the holiday season to accommodate the rush of traffic, without having to purchase and maintain underutilized systems during the rest of the year.[97] This prevents wasted resources during the rest of the year, and reduces the risk of accidentally turning away customers during a spike in sales.[98] Finally, businesses might save because the cloud provider can pass on some of the savings they get from their economy-of-scale buying power for computing hardware and software.[99]

Yet, there are many privacy implications that come along with the vast benefits of cloud computing. Having data on the servers of a cloud service provider instead of your own means that if the provider's servers are compromised, then your data could potentially also be compromised.[100] A cloud service provider might retain the right to disclose information to another party.[101] The "terms of service" of cloud providers might also vary from provider to provider, leading users to potentially rely on privacy protections that may exist with one provider, but not another. The growing trend towards cloud computing usage means that more and more people will be storing their data on remote servers (which will likely be outside Fourth Amendment protections, as currently understood).

---

96 *Id.*

97 *See id.* at 10–11.

98 *See id.*

99 *See id.* at 12.

100 This issue has been termed "reputation fate-sharing," where although cloud users might "benefit from a concentration of security expertise at major cloud providers . . . a single subverter can disrupt *many* users." YANPEI CHEN ET AL., UNIV. CAL. BERKELEY, WHAT'S NEW ABOUT CLOUD COMPUTING SECURITY? 4 (2010), *available at* http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf. As an example, Chen, et al., notes an April 2009 FBI raid on two Texas data centers that belonged to Core IP Networks, as part of a general criminal investigation into a company that previously purchased Core IP services. *Id.* at 5; *see also* Robert McMillan, *FBI Raids Dallas Internet Service Provider Core IP*, PC WORLD, (April 3, 2009), http://www.pcworld.com/article/162584/fbi_raids_dallas_internet_service_provider_core_ip.html (reporting on the event). There, FBI agents seized shared equipment, which caused non-related businesses using the same datacenters disruptions or even complete closure. CHEN ET AL., *supra* at 5. An affected customer that was not the subject of the FBI investigation, but whose equipment was affected, applied for a temporary restraining order, which was denied. *Id.*

101 *See, e.g.*, *Terms of Use*, AMAZON WEB SERVICES, http://aws.amazon.com/terms ("AWS reserves the right to refuse service, terminate accounts, remove or edit content in its sole discretion.") (last updated Feb. 8, 2011).

Furthermore, it is unlikely that cloud computing services will have the benefits of the additional protections that come with being an electronic communications service. Cloud computing services do not provide the *ability* to access the Internet, but they provide services that *utilize* the Internet. Courts have found that in the case of the Internet, it is the ISP and the telecommunications companies that fall into the category of electronic communications service providers, because they provide the ability to send or receive electronic communications.[102] As cloud computing users cannot use cloud services without an existing Internet connection, this suggests that at least SaaS and PaaS providers are unlikely to be classified as ECS providers. IaaS providers might be more arguably classified as ECS providers, depending on their function.

Cloud computing promises to be the future of Internet technology, with increasing numbers of people and businesses using cloud services to store and process data every day. How much the law protects privacy is a key concern for most of these users. Yet, the limitations of the SCA, a statute that was written nearly twenty-five years ago and is used to address technologies that were not even imagined at the time, mean that as cloud computing services become more and more ubiquitous, peoples' privacy expectations may not line up with the law's protections.

## III. LIMITATIONS OF THE SCA IN THE CLOUD COMPUTING CONTEXT

As forward-thinking as the SCA was for its time, it is not currently without short-comings. First, the SCA's ECS/RCS distinction seems particularly anachronistic in the age of cloud computing. The number of people who use the Internet has increased exponentially[103] and

102 *See* Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) ("The ECPA definition of 'electronic communications service' clearly includes internet service providers such as America Online, as well as telecommunications companies whose cables and phone lines carry internet traffic."); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 508, 511 n.20 (S.D.N.Y. 2001). *DoubleClick* involved a website, which the court noted were the "users" of the "electronic communication service" of Internet access. Id. at 508–09.

103 In 1986, when Congress passed the statute, the primary users of e-mail and the Internet were businesses, with very few individuals having Internet access at home. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1560 (2004); *see also* DIV. OF SCI. RES. STUDIES, NAT'L SCI. FOUND., THE APPLICATION AND IMPLICATIONS OF INFORMATION TECHNOLOGIES IN THE HOME (2010), *available at* http://www.nsf.gov/statistics/nsf01313/pdf/socio.pdf (noting that in 1994, the earliest year for which data were available, only two percent of households had Internet access). In 2009, seventy-five million households, or 63.5% of Americans, had broadband

new types of technologies have emerged that fundamentally change the way people use the Internet. The justification often given for Congress creating a distinction between ECS and RCS is that "by 'renting' computer storage space with a remote computing service, a customer places himself in the same situation as one who gives business records to an accountant or attorney."[104]

Yet, this analogy is erroneous given the way Internet communications systems work.[105] Although a third party holds the content of the communications, the user still retains an expectation of privacy. The user does not expect the third party to use the content to facilitate any intended transaction, unlike a person handing over financial statements to an accountant. In the case of most cloud computing services, the third party is acting merely as a "rental locker" where the user can store his or her data in a private and secure location on the Internet or a "package carrier" for the user's data. Conversely, at issue in *United States v. Miller*[106] were *records*, not the *contents* of private communications. Professor Patricia Bellia notes that "nothing in *Miller* suggests that the category [of business records] is all-encompassing—that one lacks an expectation of privacy in anything in the hands of a third party,"[107] which was also the position adopted by the Sixth Circuit in *United States v. Warshak*.[108] Moreover, the Supreme Court has recognized that letters and sealed packages are "as fully guarded from examination . . . as if they were retained by the parties forwarding them in their own domiciles."[109] It has also recognized that when someone maintains personal property on a third party's premises, he or she retains a reasonable expectation of privacy, even if that third party has the right to access the property for some purposes.[110] Since

---

Internet at home. *See* U.S. CENSUS BUREAU, CURRENT POPULATION SURVEY, (2009), *available at* http://www.census.gov/population/socdemo/computer/2009/tab01.xls.

104 CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING § 7:48 (3d ed. 2007).

105 *See supra* notes 34 and 37.

106 425 U.S. 435 (1976).

107 Bellia & Freiwald, *supra* note 37, at 148.

108 631 F.3d 266, 287 (6th Cir. 2010).

109 *Ex parte* Jackson, 96 U.S. 727, 733 (1877); *see also* United States v. Thomas, No. 88-6341, 1989 WL 72926, at *2 (6th Cir. July 5, 1989) (per curiam) (finding that bank customers have an expectation of privacy in the contents of their safe deposit boxes, such that a warrant is required for the government to access the contents).

110 *See, e.g.*, Stoner v. California, 376 U.S. 483, 489 (1964) (holding that searching a hotel room without a warrant violated the Fourth Amendment, even though hotel personnel might enter the room to perform their duties); Chapman v. United States, 365 U.S. 610, 616–18 (1961) (holding that searching a house of a tenant, without a warrant, in absence of the tenant but with the consent of the landlord, violated the

most cloud computing providers provide services that are more similar to these last two functions than that of an accountant receiving financial statements, the SCA's privacy protections are inadequate given the user's privacy interest.

Another major limitation in the SCA is that it does not provide for a suppression remedy.[111] This is problematic for several reasons. First, this means that the government's failure to comply with the SCA does not avail the defendant of any substantive remedy (unless a court concludes that the violation rises to the level of a Fourth Amendment violation).[112] Without a proper remedy, the government can get away with less than adequate procedure.[113] Additionally, the defendant would not have a remedy against a service provider, because the service provider would simply be complying with a court order, the validity of which it would have no reason to question,[114] and would be protected under § 2707(e)'s good faith exception.[115] Second, the lack of a suppression remedy means that few defendants have any incentive to challenge the government's surveillance practices.[116] Without an incentive to challenge the government's practices under

---

Fourth Amendment, even though the landlord had the authority to enter the premises); Garcia v. Dykstra, 260 F. App'x 887, 893 (6th Cir. 2008) (finding a reasonable expectation of privacy in a leased storage unit).

111 *See, e.g.*, United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (finding that the SCA specifically allows for only civil damages and criminal punishment for violations, and that Congress did not intend for suppression to be an option for a defendant), *aff'd* 106 F. App'x 688 (10th Cir. 2004); *see also* SOLOVE & SCHWARTZ, *supra* note 21, at 145 ("The SCA does not provide for an exclusionary rule."). *But see* McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998) ("While the government makes much of the fact that § 2703(c)(1)(B) does not provide a cause of action against the government, it is elementary that information obtained improperly can be suppressed where an individual's rights have been violated.").

112 *See* FISHMAN & MCKENNA, *supra* note 104, § 7:51.

113 *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1285 (2004) ("Even if the police violate the Act blatantly, they can still use surveillance evidence obtained from such misconduct against a defendant in a criminal trial."); *see also* United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) (holding that since "Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act," a defendant's motion to suppression information was denied, even though the government conceded the invalidity of the subpoena used to obtain the information), *aff'd* 225 F.3d 656 (4th Cir. 2000).

114 *See* FISHMAN & MCKENNA, *supra* note 104, at § 7:51 (citing United States v. Kennedy, 81 F. Supp. 2d 1103, 1109–10 (D. Kan. 2000)).

115 18 U.S.C. § 2707(e) (2006).

116 *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 824 (2003).

the SCA, relatively few cases apply this particular statute.[117] This results in a statute with a reputation for being poorly understood, because there are fewer judicial opinions that fully analyze the contours of the statute.

Finally, the SCA's privacy protections are limited because of the way the statute deals with voluntary disclosures under § 2702 as opposed to compelled disclosure under § 2703. Voluntary disclosures are particularly important in the context of the Internet and law enforcement, because the majority of the action takes place between law enforcement and the Internet service providers. In many situations, however, there is a "gray zone" where potential liability for service providers disclosing information to the government might be unclear.[118] Orin Kerr gives two examples of how this might occur:

> A police officer contacts an ISP system administrator and explains that he is investigating a child molestation case. The officer asks the system administrator if he is interested in helping out the police by voluntarily disclosing certain files. Wishing to be a good citizen, the system administrator agrees and turns over files to the agent. Is this a case of "compelled" disclosure or "voluntary" disclosure? Alternatively, imagine that a system administrator contacts the FBI and wants to disclose files but then asks for a subpoena just to make sure there was some sort of documentation of the disclosure. The FBI agent agrees, forwards a subpoena to the system administrator, and then accepts the files. Does the presence of the subpoena turn what was a voluntarily disclosure into a compelled disclosure?[119]

In the first instance, the government solicited a disclosure, yet it is unclear whether the ISP's compliance was voluntary or if the system administrator was compelled by believing that the disclosure was essential. In the second instance, it is unclear whether the system administrator was actually "compelled" to disclose the information, because he or she came to the government official intending to disclose, notwithstanding the formality of the subpoena. Kerr suggests that the answers to these questions "depend on what standard courts eventually adopt to distinguish between compelled and voluntary disclosure." [120] A narrow definition of "compelled" disclosure would mean that the ISP's disclosure was not required, because it could have refused the police request. This would undermine the SCA's privacy protections and create the potential for government abuse, because "[i]f a provider is unaware that it has the obligation to require legal

117 *Id.* at 823–24.

118 *See* Kerr, *supra* note 29, at 1224.

119 *See id.* at 1224–25.

120 *Id.* at 1225.

process 'officials could request records in the hopes that the ISP simply will comply.'"[121] The absence of a suppression remedy means that "'there is no incentive for the government not to try this method,' particularly in situations where officers 'suspect that a warrant or subpoena will not be granted.'"[122]

Given that twenty-five years have passed since Congress first enacted the SCA, not all of its provisions have held up well over time. The development of technology and our understanding of the legal implications of new technologies have changed as such technology use becomes more widespread. The SCA's RCS/ECS distinction is anachronistic in the modern age of cloud computing, where cloud providers do not act like an accountant receiving business records, but more like a rental locker or a package carrier. The lack of a suppression remedy and the voluntary disclosure exception also contribute to the SCA's overall ineffectiveness at protecting users' privacy interests. Today, the proliferation of technology into the lives of millions of people means that the need for Congress to amend the SCA is more urgent than ever.

## IV. REWRITING THE SCA FOR THE MODERN COMPUTING AGE

Calls for Congress to amend the SCA are not new.[123] With the explosion of cloud computing and Web 2.0 services in the past few years however, it has become even more urgent and necessary for Congress to bring the SCA into the twenty-first century. The aim of my proposals is not to provide greater protection for stored electronic communications than in other areas, but to bring that protection to a level approaching that of Fourth Amendment protections. Thus, the proposals recognize the important interests of law enforcement in fighting crime and are modestly tailored such that they do not unduly burden government officials. The proposals seek to bring privacy protections in line with constitutional privacy doctrine, and would not affect legitimate emergency disclosures or publicly disclosed informa-

121 *See* Seth Rosenbloom, Note, *Crying Wolf in the Digital Age: Voluntary Disclosure Under the Stored Communications Act*, 39 COLUM. HUM. RTS. L. REV. 529, 546 (2008) (quoting Vanessa Hwang, Note, *Cable Modems and Privacy in the New Millennium*, 32 COLUM. HUM. RTS. L. REV. 727, 763 (2001)).

122 *Id.*

123 *See, e.g., Electronic Communications Privacy Act Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) (statement of Marc J. Zwillinger, Professor, Georgetown University Law Center); Bellia, *supra* note 37, at 1436; Kerr, *supra* note 29, at 1233–43; DIGITAL DUE PROCESS COALITION, http://www.digitaldueprocess.org (last visited Sept. 6, 2011).

tion[124] where the user retains no reasonable expectation of privacy. The ability of the government to successfully investigate, prosecute, and obtain verdicts against criminals in non-Internet related areas indicates that the Fourth Amendment's restrictions on governmental action has not severely handicapped law enforcement's attempts to fight crime. Meanwhile, the privacy protections have greatly benefitted citizens in terms of law enforcement accountability and checking governmental power.

In this section, I will first address some justifications for the strengthening of privacy. Next, I propose three modifications to the SCA that will help clarify and bolster the privacy protections of the SCA in the age of cloud computing.

### *A. Why Strengthen Privacy?*

As noted above in Part I in the various approaches to conceptualizing privacy, privacy can be a good in and of itself, as well as play an important role in a democratic society. Julie Cohen notes that information privacy promotes inventiveness and entrepreneurialship, reinforces the existing social fabric, and plays a role in defining our collective vision of information technologies within society.[125] Neil Richards puts forth a theory of intellectual privacy grounded in the First Amendment, arguing that the safeguarding of our records of intellectual activity is important to First Amendment values of free thought and expression.[126] A particularly important justification for strengthening privacy is an economic-based justification, especially given the Internet's importance as a forum for facilitating economic activity. One distinct impediment to widespread adoption of cloud computing at the corporate level is doubt about the level of security cloud computing can provide for sensitive data.[127] While the law cannot create technological security, it can allow for a more robust framework that protects the privacy interests and expectations of data owners. Stronger privacy protections for the cloud computing data of

124 Examples of publicly disclosed information might be status updates on Facebook, blog postings on a publicly accessible site, or photo uploads on a cloud site with the public-sharing feature activated.

125 *See* Cohen, *supra* note 13, at 1427–28.

126 *See* Richards, *supra* note 13, at 389.

127 *See, e.g.*, Gain, *supra* note 91 ("IT managers of 750- to 1,000-user enterprises are generally extremely cautious about handing over critical and sensitive data to a third party on a platform as vaguely defined as 'the cloud.' Indeed, the main impediment to cloud computing's adoption that will likely remain an issue in the long term is the high standard of security and reliability providers must offer to meet security, regulatory, and even data-ownership concerns.").

corporate users will, in turn, create positive economic effects that accompany the facilitation of commerce. Companies that can be assured their sensitive corporate data will be protected in the hands of cloud service providers are more likely to take advantage of the benefits of operating on the Internet and using cloud computing services to expand their business.

Another justification for strengthening privacy protections might be because of shortcomings of a market-based approach to privacy protections. Although some scholars contend "that the market is functioning optimally and is already adequately accounting for privacy concerns"[128] with "market incentives for companies to keep their data secret"[129] (i.e., companies can change their privacy policies due to publicized outcry or backlash), there are also limitations to relying solely on the market-based approach. First, contract law is limited in that it only protects the privacy of the parties to the contract and not invasions by third parties outside of the contract.[130] Second, unequal bargaining power between the parties means that most users do not bargain over or choose services based on different companies' privacy policies (nor would they usually be able to bargain over privacy terms, which are generally offered on a "take it or leave it" basis).[131] Companies' privacy policies tend to be "little more than 'notices' about a company's policies rather than a contract," allow companies to change the policy without the customer being able to prevent such changes, and often lack binding enforcement mechanisms.[132] These factors combine to make it "difficult for consumers to bargain with [companies] about their privacy because they lack expertise in privacy issues and because it takes substantial time and effort."[133] Yet, a

128 *See* SOLOVE, *supra* note 7, at 79. Solove notes that proponents of this view argue that "[t]he fact that privacy is not afforded much protection demonstrates that people value other things more than privacy—such as efficient and convenient transactions." *Id.* at 81.

129 *Id.* at 80.

130 *See id.* at 81.

131 *See id.* at 82. There is usually some variation in the way certain service providers treat privacy. *See, e.g.*, Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, January 20, 2006, at A1, *available at* http://www.nytimes.com/2006/01/20/technology/20google.html (noting that while Google was refusing to comply with a government subpoena to turn over search engine records on the grounds that it was overly broad, three of its competitors (America Online, Yahoo!, and MSN) complied with the subpoenas). Yet, it is unclear whether consumers choose providers based on privacy as a criterion or if other factors such as ease of use and popularity are more important.

132 *See* SOLOVE, *supra* note 7, at 82–83.

133 *Id.* at 84.

majority of Internet users maintain that they are concerned about their online privacy.[134]

Although direct governmental intrusion into citizens' private life is an often-cited fear, there is also a strong probability for non-governmental actors to affect individuals' privacy greatly.[135] Enormous databases of information exist in the hands of private companies that detail consumers' searching and purchasing habits, as well as individuals' demographic, educational, and work information.[136] Due to this vast amount of information on individuals, governmental actors often formally or informally solicit information from private companies holding such information. In these informal situations, the possibility arises that governmental actors can circumvent the SCA's formal procedures for disclosure either by appealing to the companies' desire to help law enforcement or by claiming an emergency without certifying it as such. Thus, private companies can wield enormous power in the Internet setting, which is one of the reasons why amending the SCA is preferable to waiting for judicial rulemaking to adapt the Fourth Amendment to new technologies. While a Fourth Amendment protection for cloud-based technologies might prevent unreasonable government interferences with individual privacy, it would not protect against interferences by private parties. Additionally, legislative

134 *See Results from June 4–7 Nationwide Poll*, ZOGBY INT'L, 1 (June 7, 2010), http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf. This poll indicated that 87% of adults surveyed nationwide are "concerned with the security of their personal information on the Internet" and 80% of adults are "concerned with companies recording their online habits and using the data to generate profit through advertising." *Id.* Whether this "concern" manifests itself in market choice seems uncertain, given the proliferation of ad-supported services. Additionally, 79% of the adults surveyed believed that law enforcement should have to get a warrant, like the one required to wiretap phone conversations, to track where a user goes on the Internet, versus 12% who say they do not; 88% believe consumers should enjoy "similar legal privacy protections online as they have offline"; and 49% believe government regulators should play a larger role in protecting online consumer privacy, while more than a third (36%) do not. *Id.*

135 *See* Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media*, 72 GEO. WASH. L. REV. 1503, 1504–05 (2004).

136 *See* SOLOVE, *supra* note 7, at 3–4. The notion that "Google knows more about you than your mother," is apparent in the fact that that we are willing to search for topics that we might not want to discuss with our family or friends. *See* Robert L. Mitchell, *What Google Knows About You*, COMPUTERWORLD, (May 11, 2009), http://www.computerworld.com/s/article/337791/What_Google_Knows_About_You. This might be partially due to the mistaken belief that there is a layer of anonymity between the Internet and our real selves. *See* Brian Kane & Brett T. Delange, *A Tale of Two Internets: Web 2.0 Slices, Dices, and Is Privacy Resistant*, 45 IDAHO L. REV. 317, 332 (2009).

rulemaking can be faster[137] and more flexible[138] in light of the rapid development of ever-changing technologies.

### *B. Proposed Modifications to the SCA*

#### 1. Remove the RCS/ECS Distinction and Require Warrants as a General Rule

While the SCA was forward-looking in many ways, its conception of electronic communications technologies remains stuck in the 1980s. Its distinction between ECS and RCS has become unwieldy and has led to confusion and misapplication of the statute. The different levels of protection depending on what function the Internet service is performing at a given time belies the original purpose of the SCA, which was to provide protection in an area where the courts were unclear in their application of Fourth Amendment privacy protections (yet where most people would have a reasonable expectation of privacy).[139] This expectation of privacy, however, is not one that should change according to the different stages in the lifecycle of an e-mail or stored document. When a person sends an e-mail to another person, he or she has the same expectation of privacy when composing the e-mail, when clicking send, and when the other person receives the e-mail, much as that person would have the same expectation of privacy on a document he or she composes and stores locally on a home computer. Thus, my first proposed modification would be to remove the distinction between ECS and RCS and require the government to show probable cause for a search warrant, as the Fourth Amendment requires, before it can compel disclosure of stored electronic informa-

137 *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 869 (2004) ("Years may pass before a court considers how the Fourth Amendment regulates use of a new technology; many more years may pass before the issue is resolved definitively. By the time the courts decide how a technology should be regulated, however, the factual record of the case may be outdated, reflecting older technology rather than more recent developments.").

138 *See id.* at 871 ("Legislatures can experiment with different rules and make frequent amendments; they can place restrictions on both public and private actors; and they can even 'sunset' rules so that they apply only for a particular period of time. The courts cannot." (footnotes omitted)).

139 For an outline of the different standards a single e-mail might face at different points in its life cycle, see *Electronic Communications Privacy Act Reform Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. App'x A, (2010) (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology), *available at* http://judiciary.house.gov/hearings/pdf/Dempsey100505.pdf.

tion. Having this as the general rule, with specific exceptions allowing for lesser standards (such as in the case of emergencies), would greatly simplify the statute, while allowing law enforcement to do its job.[140]

Although some might argue that requiring warrants might impede law enforcement activities, there are still several important benefits to having a warrant requirement, especially given the "technological and regulatory reach of government intrusions that exists today."[141] First, warrants "aim[ ] to prevent searches from turning into 'fishing expeditions.'"[142] The Framers' experience with writs of assistance and general warrants (which did not require specific individuals or specific places to be searched) that "resulted in 'sweeping searches and seizures without any evidentiary basis'"[143] and "'ransacking' and seizure of the personal papers of political dissidents, authors, and printers of seditious libel"[144] led to the inclusion of the warrant clause. Thus, warrants must describe with "particular[ity] . . . the place to be searched, and the persons or things to be seized."[145] Second, the warrant requirement enforces the separation of powers and prevents the "excessive exercises of executive power."[146] Since warrants compel law enforcement officials to justify their exercises of power,[147] this provides a structural check against abuses by such officials. At the same time, warrants "do not constitute an absolute bar to the activities of law enforcement," but "merely ensure that law enforcement officials focus on particular individuals and that they are given adequate independent oversight."[148]

Why then is the current statutory regime insufficient? By allowing the government to compel disclosure with only a subpoena or a § 2703(d) court order, the statute's privacy protections are far lower than that of the Fourth Amendment. According to Daniel

---

140 *See* Solove, *supra* note 113, at 1299.

141 Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1804 (1994).

142 SOLOVE, *supra* note 7, at 192 (citing Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. 107, 115 (1986) ("The spirit and letter of the fourth amendment counseled against the belief that Congress intended to authorize a 'fishing expedition' into private papers on the possibility that they might disclose a crime.")).

143 *Id.* at 193 (quoting Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 82 (1988)).

144 *Id.* (quoting DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 38 (1979)).

145 U.S. CONST. amend. IV.

146 Solove, *supra* note 113, at 1299.

147 Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 17 (1991).

148 Solove, *supra* note 113, at 1300.

Solove, "[u]nlike warrants, subpoenas do not require probable cause and can be issued without judicial approval."[149] William Stuntz notes that "while searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable."[150] Prosecutors can issue subpoenas instead of neutral judicial officers and prosecutors can use grand jury subpoenas to obtain third-party records.[151] Grand jury subpoenas are "'presumed to be reasonable' and may only be quashed if 'there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury investigation.'"[152] Thus, the burden on the government to provide relevant information is far lower, because "[n]o showing of probable cause or reasonable suspicion is necessary, and courts measure relevance and burden with a heavy thumb on the government's side of the scales."[153]

Court orders under § 2703(d) of the SCA also require less than a search warrant. The relevant provision calls for: "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[154] Since the standard only requires that the information is "relevant and material" to the investigation, law enforcement officials can get away with a lot more than if the standard was probable cause. As with subpoenas, the problem with court orders is that they "supply the judiciary with greatly attenuated oversight powers."[155] The judge's job is to "merely determine whether producing records is overly burdensome" (in the case of subpoenas) or whether the "records are 'relevant' to a criminal investigation, a

149 SOLOVE, *supra* note 7, at 202.

150 William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 857–58 (2001) (footnote omitted).

151 SOLOVE, *supra* note 7, at 202. The SCA requires "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena" served by the government entity. 18 U.S.C. § 2703(a)(1)(B)(i) (2006). This has been interpreted to exclude pre-trial discovery subpoenas. *See* F.T.C. v. Netscape Comms. Corp., 196 F.R.D. 559, 560–61 (N.D. Cal. 2000).

152 SOLOVE, *supra* note 7, at 202–03 (quoting United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991)).

153 William J. Stunz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1038 (1995).

154 18 U.S.C. § 2703(d).

155 SOLOVE, *supra* note 7, at 203.

much weaker standard [than probable cause]."[156] Instead of being an impartial decision-maker that gets to determine whether to grant a warrant, the judiciary's involvement with subpoenas and court orders "amounts to little more than a rubber stamp of judicial legitimacy."[157] With the scales tipped in favor of law enforcement, the potential is greater for officials to engage in "fishing expeditions" and the delicate balance that prevents "excesses" is upset.

2. Add a Statutory Suppression Remedy

A second possible change is for Congress to incorporate a statutory suppression remedy into the SCA. This would likely deter abuses of the statute by law enforcement officials.[158] The SCA's lack of a suppression remedy is unlike Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[159] the primary federal statute that governs the interception of wire and oral communications, or the Fourth Amendment, which provides for suppression if government action violates the statute.[160] As Justice Holmes noted, the Fourth Amendment would be simply a "form of words" without the exclusionary rule.[161] This differentiation between *interception* of *wire and oral* communication and retrieval of *stored electronic* communications is unnecessary. The same privacy interests are at stake concerning unreasonable searches and seizures, and there is the same potential danger of law enforcement officials' misconduct exists.

Furthermore, as Orin Kerr argues, adding an exclusionary remedy would "benefit both civil libertarian and law enforcement interests alike."[162] For civil libertarian interests, "a suppression remedy would considerably increase judicial scrutiny of the government's Internet surveillance practices in criminal cases," which would "clarify the rules that the government must follow, serving the public interest of greater

156 *Id.*

157 *Id.*

158 The Fourth Amendment's suppression remedy is said to "protect[ ] innocent people by eliminating the incentive to search and seize unreasonably." Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1266 (1983). Loewy notes that it does this so long as the law enforcement officer's goals are to secure a conviction. *Id.* at 1266 n.169. If the officer is seeking to harass a subject, the exclusionary rule would not help protect that subject against the harassment. *Id.*

159 18 U.S.C. § 2515.

160 *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961); Bellia, *supra* note 37, at 1436.

161 Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920).

162 Kerr, *supra* note 116, at 807–08.

transparency."[163] It would do this by giving defendants the option to challenge government action in criminal cases. For law enforcement interests, a suppression remedy would allow prosecutors to have "greater control over the types of cases the courts decided, enjoy more sympathetic facts, and have a better opportunity to explain and defend law enforcement interests before the courts."[164] Thus, "[t]he statutory law of Internet surveillance would become more like the Fourth Amendment law: a source of vital and enforceable rights that every criminal defendant can invoke, governed by relatively clear standards that by and large respect law enforcement needs and attempt to strike a balance between those needs and privacy interests."[165]

3. Clarify the Scope of Voluntary Disclosures

Finally, Congress can enhance privacy interests by clarifying the scope of voluntary disclosures under a standard that sufficiently protects customers. As an effect of the limited remedies available to those who have been harmed by SCA violations, the lack of judicial opinions on the SCA means that the provisions for when a disclosure is voluntary and when it is compelled is not fully fleshed out. In seeking these clarifications and changes, I use Fourth Amendment doctrine as the standard for where the SCA should be.

I propose that if a cloud service provider voluntarily discloses information because of misrepresentations or because of (illegitimate) government coercion, then it should not be liable for such a disclosure. Yet, there may still be instances where a service provider might be liable for a voluntary disclosure, even if there was government encouragement. For example, if there was no legal process and the service provider voluntarily disclosed information in a non-emergency situation (or other situations to be defined statutorily), the provider would be liable for a violation. In assessing the voluntariness of the disclosure, a court should look at whether the provider discloses the information under a good faith belief that it was compelled. Thus, in a situation where there is a court order or warrant "for show" (where the service provider came to the government seeking to disclose the information to begin with), such legal process should not absolve the service provider of liability.

The other side of liability for compelled disclosures involves the government. Here, the SCA should seek to model its standard such that it is in line with Fourth Amendment standards for third parties

163 *Id.* at 807.
164 *Id.* at 807–08.
165 *Id.* at 808.

acting as agents on behalf of the government. If the government complies with the provisions in § 2703, then it should not be liable for any SCA violations. On the other hand, if the government acted in such a way as to cause the service provider to be its agent, then the government should be liable for violation of the SCA. While Fourth Amendment doctrine has not settled on the "appropriate inquiry to be performed in determining whether involvement of the police transforms a private individual into an agent or instrument of the police,"[166] any modification to the SCA should try to settle on a particular type of test, in the interests of clarity and consistency.

## CONCLUSION

The Stored Communications Act has been noted as a "remarkable achievement"[167] and "forward-looking"[168] for being able to adapt its Fourth Amendment-like protections to emerging technologies, especially in light of the fact that it was enacted in 1986. Yet, technology has developed so much in the past twenty-five years that it has outpaced the Act. The Internet has grown exponentially in those years and is now an integral and pervasive part of millions of peoples' lives. Countless industries, both Internet-based and non-Internet-based, rely on and benefit from using the Internet as a market, a ser-

166 Georgia v. Randolph, 547 U.S. 103, 148 n.2 (2006) (Thomas, J., dissenting). *United States v. Pervaz*, 118 F.3d 1, 5–6 (1st Cir. 1997), considers the various approaches of the Circuits. The Sixth Circuit, in *United States v. Lambert*, 771 F.2d 83 (6th Cir. 1985), uses a narrow standard for agency action: "First, the police must have instigated, encouraged or participated in the search. Second, the individual must have engaged in the search with the intent of assisting the police in their investigative efforts." *Id.* at 89. (citing United States v. Coleman, 628 F.2d 961, 965 (6th Cir. 1980)). The Ninth Circuit's standard is looser, holding that "two of the critical factors in the 'instrument or agent' analysis are: (1) the government's knowledge and acquiescence, and (2) the intent of the party performing the search," *Pervaz*, 118 F.3d at 5–6 (citing United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981)) and that the "Fourth Amendment will not apply when the private party was acting for a reason that is independent of such a governmental purpose," *id.* at 6 (citing United States v. Attson, 900 F.2d 1427, 1433 (9th Cir. 1990)). Finally, the Tenth Circuit requires that the government must "affirmatively encourage or instigate the private action," which is determined by "the totality of the circumstances." *Id.* (citing United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996)). The First Circuit in *Pervaz* ended up concluding that "any specific 'standard' or 'test' [was] likely to be oversimplified or too general to be of help, and that all of the factors mentioned by the other circuits may be pertinent in different circumstances." *Id.*

167 *See* Kerr, *supra* note 29, at 1243.

168 *See* J. BECKWITH BURR, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986: PRINCIPLES FOR REFORM 1 (2010), *available at* http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

vice, or a forum. It is against this backdrop that the emergence of cloud computing technology takes place. The SCA's protections for cloud computing will have enormous implications for the privacy rights of millions of people. Cloud computing has the potential to transform the way people interact and how companies run their businesses. Thus, it is important that Congress update the SCA to bring it up to date with modern technologies so that the same privacy protections that exist for other forms of storage and communications exist in the cloud.