Georgia State University Law Review

Volume 28
Issue 2 *Winter 2012*

Article 6

3-14-2012

Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, Or Both?

Derek Constantine

CLOUD COMPUTING: THE NEXT GREAT TECHNOLOGICAL INNOVATION, THE DEATH OF ONLINE PRIVACY, OR BOTH?

Derek Constantine*

INTRODUCTION

Google Docs[1] is a service used by individuals and, in its Google Apps[2] form, by businesses and educators.[3] Google Docs allows a user to log on to his Google account on any computer and create text documents, spreadsheets, and a variety of other documents while saving everything remotely—allowing that same user to log off one computer, log on to another computer, and continue to work on the same document.[4] Additionally, multiple users can access and edit the same document in Google Docs at the same time to facilitate collaborative work.[5] The use of Google Docs is increasing, with Google claiming to have over two million users.[6] Google Docs is a form of what is generically referred to as cloud computing—online services that provide "the ability to run applications and store data on a service provider's computers over the Internet, rather than on a person's desktop computer."[7] With the growth of online storage and

---

*J.D./M.B.A. Candidate, 2013, Georgia State University College of Law. Thanks to Professor Russell Covey and everyone involved with the Georgia State Law Review for their valuable feedback and suggestions, and thanks to my wife Sarah for her love and encouragement.

1. *Docs*, GOOGLE, http://docs.google.com/ (last visited May 26, 2011).
2. *Apps for Business*, GOOGLE, http://www.google.com/apps/ (last visited May 26, 2011).
3. *See generally About Google Apps*, GOOGLE, http://docs.google.com/support/bin/answer.py?hl=en-uk&answer=60982 (last visited May 26, 2011) (detailing the differences between Apps and Docs).
4. *Online, Free Spreadsheets from Google*, GOOGLE, http://www.google.com/google-d-s/spreadsheets/ (last visited May 26, 2011) [hereinafter *Free Spreadsheets*]; *Online, Free Word Processing with Google Documents*, GOOGLE, http://www.google.com/google-d-s/documents/ (last visited May 26, 2011) [hereinafter *Free Word Processing*]; *What's New in Google Docs?*, GOOGLE, http://www.google.com/google-d-s/whatsnew.html (last visited May 26, 2011).
5. *What's New in Google Docs?*, *supra* note 4.
6. *Office Politics: Microsoft Bids to Keep Its Grip on Corporate Computing Against Google's Challenge*, ECONOMIST (May 13, 2010), http://www.economist.com/node/16113333.
7. William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1199 (2010).

computing services by companies such as Microsoft and Google,[8] now more than ever any person with a basic computer and an Internet connection can store files remotely,[9] borrow processing capabilities,[10] write documents,[11] work on spreadsheets,[12] or create presentations[13]—all through convenient, simple, and often free online services.[14] Given the low cost and ease of use, cloud computing seems like an attractive option to consumers who are cost-conscious but still want the newest software and services.[15] And yet, despite the optimism around cloud computing, many businesses and individuals have been slow to adopt the new services.[16] Companies and individuals have expressed concerns about privacy—including concerns about the government's apparent ability to search and seize files stored in the cloud without Fourth Amendment restraint—as a major reason for the lack of cloud computing adoption.[17]

---

8. Brad Stone & Ashlee Vance, *"Cloud" Computing Casts a Spell*, N.Y. TIMES, Apr. 19, 2010, at B1 ("[C]loud providers are trying to bring these [cloud] services to the more conservative and lucrative world of large corporations."); *Clash of the Clouds: The Launch of Windows 7 Marks the End of an Era in Computing—and the Beginning of an Epic Battle Between Microsoft, Google, Apple and Others*, ECONOMIST, Oct. 17, 2009, at 80, *available at* http://www.economist.com/node/14637206.

9. *MobileMe*, APPLE, http://www.apple.com/mobileme/ (last visited May 26, 2011) (on file with Georgia State University Law Review). MobileMe service is now closed to new subscribers and will transition to Apple iCloud, which provides similar services. *ICloud*, APPLE, http://www.apple.com/icloud/ (last visited Oct. 19, 2011).

10. *Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON.COM, http://aws.amazon.com/ec2/ (last visited May 26, 2011); *Amazon Web Services: Terms of Use*, AMAZON.COM, http://aws.amazon.com/terms/ (last visited May 26, 2011). *See generally Clouds Under the Hammer: Processing Capacity is Becoming a Tradable Commodity*, ECONOMIST, Mar. 11, 2010, at 69 (discussing the evolution of the commoditization of processing power).

11. *Free Word Processing*, *supra* note 4.

12. *Free Spreadsheets*, *supra* note 4.

13. *Free, Embeddable Presentations from Google*, GOOGLE, http://www.google.com/google-d-s/presentations/ (last visited May 26, 2011).

14. *Docs*, *supra* note 1 ("It's easy to get started and it's free!").

15. *Battle of the Clouds: The Fight to Dominate Cloud Computing Will Increase Competition and Innovation*, ECONOMIST, Oct. 15, 2009, at 16, *available at* http://www.economist.com/node/14644393; Stone & Vance, *supra* note 8, at B1 ("In Amazon's model, businesses pay only for the computing cycles they use. Customers eliminate the upfront cost of computer hardware and can then buy more time on Amazon's data center as needed."). *See generally* THOMAS L. FRIEDMAN, HOT, FLAT, AND CROWDED: WHY WE NEED A GREEN REVOLUTION—AND HOW IT CAN RENEW AMERICA 232–33 (2008) (describing vision for the "job of the future" in which the individual will stay home and log onto her company's system where she will access her files, run programs, and perform her job entirely remotely).

16. *Cloudy with a Chance of Rain: Few Companies Are Ready to Accept Cloud Computing*, ECONOMIST (Mar. 5, 2010), http://www.economist.com/node/15640793.

17. *Id.*; *see* discussion *infra* Part I.A.; *see also* Stone & Vance, *supra* note 8, at B1 ("[Companies] fear that their confidential information could be vulnerable on another company's system, out of their

A close examination of the terms of the service agreement that apply to Google's services may surprise some users.[18] Google acknowledges that users retain any "copyright and any other rights [users] already hold in Content which [users] submit, post or display on or through" its services. It further states, however, that "[b]y submitting, posting or displaying the content [users] give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which [users] submit, post or display on or through" Google's services.[19] Considering the expansive nature of the terms of Google's general service agreement and assuming consumers actually read the agreement rather than blindly clicking "agree," users may wonder what level of privacy their files will have if uploaded or sent through one of Google's services.

What privacy rights apply to electronic and online files is an issue that courts are struggling to develop[20] and that the United States Supreme Court has only recently and very cursorily addressed.[21] The controlling legislation on privacy rights related to online activities such as email and cloud computing activities is the Stored Communications Act (SCA),[22] part of the Electronic

---

control."); Jonathan Zittrain, *Lost in the Cloud*, N.Y. TIMES, July 20, 2009, at A19 ("[T]he federal government has been able to demand some details of your online activities from service providers—and not to tell you about it."); *Fuzzy Maths: In a Few Short Years, Google Has Turned from a Simple and Popular Company into a Complicated and Controversial One*, ECONOMIST, May 13, 2006, at 79, *available at* http://www.economist.com/node/6911096 ("[P]rivacy advocates voiced concerns over [Google's] practice of placing advertisements in contextually related e-mail messages on its webmail service.").

18. *Google Terms of Service*, GOOGLE, http://www.google.com/accounts/TOS (last visited May 26, 2011); *see also Google Docs: Additional Terms of Service*, GOOGLE, http://www.google.com/google-d-s/intl/en/addlterms.html (last visited Aug. 3, 2011).

19. *Google Terms of Service*, *supra* note 18.

20. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 910 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (finding employees had a reasonable expectation of privacy with their text messages).

21. City of Ontario v. Quon, 130 S. Ct. 2619, 2628, 2633 (2010) (holding that employer's search of employee's text message did not violate the Fourth Amendment and, assuming arguendo for the sake of dismissing the case on other grounds, that the employee had a reasonable expectation of privacy in his text messages).

22. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2711 (2006)).

Communications Privacy Act of 1986.[23] Given that the SCA was enacted in the 1980s, courts have struggled to apply it to the Internet,[24] and legal scholars have attempted to understand and interpret the Act's application.[25] In addition to the lingering questions over the applicability of the SCA, there are questions as to whether the Fourth Amendment applies to Internet environments[26] and, if it does, how it applies.[27] The Ninth Circuit recently commented, "The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question."[28]

Part I of this Note will provide a brief historical background on the development and current state of both the SCA and the Fourth Amendment.[29] Part II of this Note will examine the applicability of the SCA to online environments and specifically to files uploaded to cloud computing environments.[30] Part II will then examine the Fourth Amendment and analyze whether it can be effectively applied to

---

23. *Id.*

24. Quon v. Arch Wireless Operating Co., 529 F.3d at 900 (discussing whether a wireless phone provider was an Electronic Communication Service under the Stored Communications Act and whether employees had a reasonable expectation of privacy with their text messages); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010) (finding private messaging and web mail services constitute Electronic Communication Services under the Stored Communications Act).

25. 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, 1209–13 (2004); Scott Ness, *The Anonymous Poster: How to Protect Internet Users' Privacy and Prevent Abuse*, 2010 DUKE L. & TECH. REV. 8, ¶6 (2010); Evan E. North, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1307 (2010); Jennifer Heidt White, *Text Message Monitoring After* Quon v. Arch Wireless*: What Private Employers Need to Know About the Stored Communications Act and an Employee's Right to Privacy*, 5 SHIDLER J.L. COM. & TECH. 19, para. 3 (2009), *available at* http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/433/vol5_no4_art19.pdf?sequence=1; *see* Robison, *supra* note 7, at 1196.

26. State v. Bellar, 217 P.3d 1094, 1110–11 (Or. Ct. App. 2009) ("Nor are a person's privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another. Again, in a practical sense, our social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the 'cloud,' on servers owned by internet service providers. . . . I suspect that most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone else.").

27. David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2206 (2009); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007 (2010).

28. Quon v. Arch Wireless Operating Co., 529 F.3d at 904.

29. *See* discussion *infra* Part I.

30. *See* discussion *infra* Part II.A.

cloud computing environments and provide privacy protection to users from "unreasonable searches and seizures"[31] by the government.[32] Finally, Part III will recommend that the SCA should apply to both webmail services and cloud computing environments and that the Fourth Amendment's protection should be digitized and applied to the cloud computing environment, providing adequate privacy rights to people in "the Internet age."[33]

I. DEVELOPMENT OF THE SCA AND THE FOURTH AMENDMENT

A. The Current State of the Stored Communications Act

The SCA is the primary legislation controlling privacy rights related to online activities such as email and general cloud computing activities.[34] Congress recognized the importance of the growing computer industry in the 1980s and put into place legislation dealing with privacy rights related to the networking activities occurring at that time.[35] The SCA distinguishes between two types of electronic services—Electronic Communication Services (ECS)[36] and Remote Computing Services (RCS).[37] For the SCA to control the fate of an electronic message or file, the service provider that hosts the message or file must be considered an Electronic Communication Services provider or a Remote Computing Services provider under the SCA.[38] So the ultimate fate of any electronic message or file under the SCA

31. U.S. CONST. amend. IV.
32. *See* discussion *infra* Part II.B.
33. Quon v. Arch Wireless Operating Co., 529 F.3d at 904; *see infra* Part III.
34. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2711 (2006)).
35. *Id. See generally* Kerr, *supra* note 25.
36. 18 U.S.C. § 2702(a)(1) (2006) ("[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . . ."). *See generally* Robison, *supra* note 7, at 1205–14.
37. § 2702(a)(2) ("[A] person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . ."). *See generally* Robison, *supra* note 7, at 1205–14.
38. § 2702(a).

is determined much more by the classification of the service provider that hosts the message or file than by the message or file itself.[39]

1. Electronic Communication Service

For a message to fall under the language of the Electronic Communication Service section of the SCA, the Electronic Communication Service provider must provide "the ability to send or receive wire or electronic communications."[40] In addition, the message must be "in electronic storage."[41] Electronic storage under the SCA is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"[42] or "any storage of such communication by an electronic communication service for purposes of backup protection."[43] Although the language may seem complex, the essential characteristic of a message qualifying for ECS protection is that it must either be held by the provider only temporarily during transmission itself or be held by the provider for "backup protection."[44]

With the increase in Gmail and other webmail services, providers' large storage limits allow users to store a message on the provider's server rather than download it to the user's computer.[45] It is unclear whether the stored message will actually qualify as a communication under the ECS language. The message is not temporarily held by the provider "incidental to the electronic transmission thereof,"[46] since the message is left permanently on the provider's server until the user deletes it. Although users may claim a message is left on the provider's server as "backup protection,"[47] courts may not agree,

39. *Id.*
40. 18 U.S.C. § 2510(15) (2006).
41. § 2702(a)(1).
42. § 2510(17)(A).
43. § 2510(17)(B).
44. *Id.*
45. *Gmail: Your Storage Limit*, GOOGLE, http://mail.google.com/support/bin/answer.py?answer=6558 (last visited Aug. 3, 2011) ("Gmail offers more than 7 GB of free storage for your messages and attachments . . . .").
46. 18 U.S.C. § 2510(17)(A).
47. § 2510(17)(B).

since there is only one copy of the message—it is not being backed up from anywhere else.[48] The message only exists on the provider's server.[49] Given those considerations, the status of an email message sent from or to a webmail address is unclear, with courts often in complete disagreement as to how such messages should be categorized.[50]

Under the SCA, the Government must get a warrant to retrieve a message that has been in storage for 180 days or less and that is being held by a provider that qualifies as an Electronic Communication Service provider.[51] A subpoena or a court order, rather than a warrant, can be enough for a message that has been in storage for more than 180 days with prior notice to the subscriber or customer.[52] So for a message that has been held in storage for less than 180 days, the status of a service provider can have significant consequences on how easily the Government can obtain a message under the ECS language.

2. Remote Computing Service

To be considered a Remote Computing Service provider, a company must provide "computer storage or processing services by

---

48. *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (finding emails that have been opened are not in temporary storage incidental to transmission and are not in electronic storage so the government does not need a warrant to obtain copies of the emails); *See Gmail: Your Storage Limit*, *supra* note 45.

49. *Gmail: Your Storage Limit*, *supra* note 45.

50. Courts have addressed the question of whether the Stored Communications Act applies to emails far more frequently than they have addressed other cloud computing services and, while unopened email messages are generally recognized as messages in electronic storage, courts often directly contradict one another regarding opened email messages. *See Weaver*, 636 F. Supp. 2d at 773. *But see* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004) (finding opened emails kept on a server are considered to be kept for backup purposes since the language of the Stored Communications Act "does not distinguish between intermediate and post-transmission storage"); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010) (finding private messaging and web mail constitute communications under the Electronic Communication Services language, and social networking sites are Electronic Communication Services); Jennings v. Jennings, 697 S.E.2d 671, 677–78 (S.C. Ct. App. 2010), *reh'g denied*, 2010 S.C. App. LEXIS 176 (S.C. Ct. App. Aug. 27, 2010) (holding that opened emails are stored for backup protection and, thus, qualify as communication under the Electronic Communication Service language if they are left on the server merely "in the event that the user needs to retrieve [the messages] again").

51. 18 U.S.C. § 2703(a) (2006 & Supp. 2009).

52. *Id.*; 18 U.S.C. § 2703(a)–(b) (2006 & Supp. 2009).

means of an electronic communications system."[53] The SCA considers an electronic communications system to be a facility "for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[54] The content of an electronic file held by a Remote Computing Service provider may only fit within the SCA if the file is maintained "solely for the purpose of providing storage or computer processing services to [a] subscriber or customer."[55]

Given the complexities in a cloud computing environment, providers may not meet these requirements since the language of the SCA is dated and cryptic.[56] As with Electronic Communication Services, the courts have embraced a broad array of interpretations of the RCS language.[57]

Even if courts consider a provider to be a Remote Computing Service, a government entity can entirely avoid having to get a warrant to retrieve an electronic file under the RCS language,[58] unlike the language found under the ECS requiring a warrant for messages that are less than 180 days old.[59] With prior notice to the subscriber or customer, a government entity can either obtain a court order by offering "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" or by obtaining a subpoena for disclosure.[60] So even if a cloud computing

53. 18 U.S.C. § 2711(2) (2006).
54. 18 U.S.C. § 2510(14) (2006).
55. 18 U.S.C. § 2702(a)(2) (2006).
56. *See* Kerr, *supra* note 25, at 1214–15.
57. Viacom Int'l, Inc. v. Youtube, Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (finding Youtube qualified as a Remote Computing Service because the court considered Youtube's access to be connected to its provision of storage services); *see also* Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (finding that "the archive maintained by [the service provider] constitutes 'computer storage,' and that the company's maintenance of this archive on behalf of the City is a 'remote computing service' as defined under the SCA").
58. 18 U.S.C. § 2703(b)(1)(B) (2006).
59. 18 U.S.C. § 2703(a) (2006 & Supp. 2009).
60. 18 U.S.C. § 2703(d) (2006); 18 U.S.C. § 2703(b)(1)(B)(i) (2006).

service is considered a Remote Computing Service under the SCA, little privacy protection is extended to the consumer.

B. The Current State of the Fourth Amendment

In addition to the SCA, the Fourth Amendment may influence privacy rights online.[61] The Fourth Amendment provides people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[62] and goes on to specify that warrants should only be issued "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[63] The expression that a person has a "reasonable expectation of privacy" was first introduced in *Katz v. United States*,[64] where the Court found that a reasonable expectation of privacy exists when two requirements are met: "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.'"[65] The Court in *Katz* further specified that "the Fourth Amendment protects people, not places."[66] Given the Court's focus on the individual's right to privacy rather than merely the setting in which the individual finds herself,[67] later courts have been willing to interpret broadly the Fourth Amendment's simple statement extending protection to "persons, houses, papers, and effects."[68] The idea of a reasonable expectation

61. *See* discussion *infra* Part I.B.

62. U.S. CONST. amend. IV.

63. *Id.*

64. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) ("[A]n enclosed telephone booth is an area where . . . a person has a constitutionally protected reasonable expectation of privacy . . . .").

65. *Id.* at 361.

66. *Id.* at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citations omitted)); *see also* United States v. Ross, 456 U.S. 798, 822–23 (1982) ("[T]he Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view. But the protection afforded by the Amendment varies in different settings." (citing Robbins v. California, 453 U.S. 420, 427 (1981))).

67. *Katz*, 389 U.S. at 351.

68. U.S. CONST. amend. IV. *See* Bond v. United States, 529 U.S. 334, 335 (2000); Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 351 (8th Cir. 2004); United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983).

of privacy has been applied to a variety of new areas as the interpretation of the Fourth Amendment has evolved.[69]

The concept of a reasonable expectation of privacy has been applied to searches of computers, with courts often focusing on whether a party has been explicitly informed that his computer is subject to searches.[70] Courts are somewhat divided when applying the reasonable expectation considerations to wireless and online services such as email accounts. They have often directly contradicted each other at the fundamental level of whether or not they should start their analysis under the assumption that an individual has a reasonable expectation of privacy regarding online communication.[71]

---

69. *Bond*, 529 U.S. at 335 (finding law enforcement's physical manipulation of a person's carry-on bag was a violation of the Fourth Amendment); *Katz*, 389 U.S. at 352 ("No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment."); *Doe*, 380 F.3d at 351 (finding school policy of conducting random searches of backpacks and purses violated the Fourth Amendment); *Freire*, 710 F.2d at 1519 (finding Fourth Amendment privacy rights in a briefcase by stating that "[f]ew places outside one's home justify a greater expectation of privacy than does the briefcase.").

70. Maes v. Folberg, 504 F. Supp. 2d 339, 347 (N.D. Ill. 2007) (finding employee "had an expectation of privacy in her laptop computer" because there were no policies or practices in place that eliminated the employee's reasonable expectation); s*ee also* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (finding employee had no reasonable expectation of privacy in his work computer because his employer "had announced that it could inspect the laptops that it furnished for the use of its employees," but there could be a right of privacy in employer-owned equipment under the Fourth Amendment as long as it was reasonable).

71. *Compare* United States v. Valdivieso Rodriguez, 532 F. Supp. 2d 332, 339 (D.P.R. 2007) (stating that "an expectation of privacy has generally not been found to exist with regard to subscriber information provided by service users to their internet service providers, records on individuals' internet usage or as to communications made on an internet website" while courts have also been hesitant to find "a reasonable expectation of privacy to exist in e-mail or electronic chat-room communications"), *and* United States v. Charbonneau, 979 F. Supp. 1177, 1184–85 (S.D. Ohio 1997) (finding that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant" until such time as the recipient of the message "forwards the e-mail to a third party," at which time the message does "not enjoy the same reasonable expectations of privacy" (quoting United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996))), *with* City of Ontario v. Quon, 130 S. Ct. 2619, 2628, 2633 (2010) (holding that employer's search of employee's text messages was reasonable since employer's stated policy allowed employer to monitor all network activity and assuming arguendo that employee had a reasonable expectation of privacy in his text messages but not ruling on the issue), *and* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 910 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (finding employees had a reasonable expectation of privacy with their text messages), *and* State v. Bellar, 217 P.3d 1094, 1107 (Or. Ct. App. 2009) (stating that "defendant did not . . . lose his protected privacy interest in the data stored on the hard drive of his computer and that the privacy interest continued after the data was transferred").

The Ninth Circuit held in *Quon v. Arch Wireless Operating Co.* that an employee had a reasonable expectation of privacy in the text messages they sent and received.[72] However, the United States Supreme Court in *City of Ontario v. Quon* reversed that decision in light of the employer's stated policy permitting it to access employee text messages.[73] The Court in *City of Ontario v. Quon* did not directly address the reasonable expectation of privacy of the employee, merely assuming arguendo that the employee had a reasonable expectation.[74] By focusing on a party's expectation of privacy and society's recognition that the expectation is reasonable, the Court returned to its views expressed in *Katz*.[75]

II. ATTEMPTING APPLICATION OF THE FOURTH AMENDMENT AND THE SCA WHILE CONSIDERING THE PROBLEM OF THE THIRD PARTY DOCTRINE

A. Applying the Fourth Amendment

Applying the Fourth Amendment to any cloud computing environment engenders great confusion.[76] Despite this lack of clarity, several recent decisions apply the Fourth Amendment to various networked and wireless situations, showing courts' willingness to provide Fourth Amendment protection to cloud computing environments.[77] In *State v. Bellar*, the court commented that the "social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the 'cloud'" and that "most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone

72. Quon v. Arch Wireless Operating Co., 529 F.3d at 910.

73. City of Ontario v. Quon, 130 S. Ct. at 2628, 2633 (holding that employer's search of employee's text messages was reasonable since employer's stated policy allowed employer to monitor all network activity).

74. *Id.*

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

76. *See* discussion *supra* Part I.B.

77. Quon v. Arch Wireless Operating Co., 529 F.3d at 910 (finding employees had a reasonable expectation of privacy with their text messages); State v. Bellar, 217 P.3d 1094, 1107 (Or. Ct. App. 2009) ("[D]efendant did not . . . lose his protected privacy interest in the data stored on the hard drive of his computer and that the privacy interest continued after the data was transferred.").

else."[78] In *Quon v. Arch Wireless Operating Co.*, the court stressed the importance of an employee having both "a reasonable expectation of privacy in the item seized or the area searched" and "demonstrat[ing] that the search was unreasonable" to show there was a Fourth Amendment violation.[79] Before *Quon v. Arch Wireless Operating Co.* was reversed, the court held that there was a reasonable expectation of privacy on the part of the employee as to the content of his text messages.[80]

In reversing *Quon v. Arch Wireless Operating Co.*, the United States Supreme Court unfortunately chose not to address the reasonable expectation of privacy issue, leaving confusion in its wake.[81] However, given the ever increasing importance of online environments, lower courts have followed the Supreme Court's

---

78. *Bellar*, 217 P.3d at 1110, 1111 ("Nor are a person's privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another.").

79. The court acknowledged that it was facing a new issue and set a threshold question to be answered. Quon v. Arch Wireless Operating Co., 529 F.3d at 904 (stating that "[t]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question" and asking "the threshold question: Do users of text messaging services . . . have a reasonable expectation of privacy in their text messages stored on the service provider's network?").

80. The court makes a distinction between the "outside" of a text message—the information required to send a text message—and the "inside" of a text message—the content of the message itself. Quon v. Arch Wireless Operating Co., 529 F.3d at 905 ("As with letters and e-mails, it is not reasonable to expect privacy in the information used to 'address' a text message . . . . However, users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider.").

81. The Court acknowledged the importance of the issue but expressed concern in making too broad a ruling before the Court properly understood the potential implications a ruling could have:

> Before turning to the reasonableness of the search, it is instructive to note the parties' disagreement over whether Quon had a reasonable expectation of privacy.
>
> . . . .
>
> . . . Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.
>
> . . . .
>
> A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted.

City of Ontario, v. Quon, 130 S. Ct. 2619, 2629–30 (2010). The Court ultimately reversed on the grounds that the search was motivated by legitimate, employment-related concerns and the policy in place was that pager messages were available for review, which allowed the court to reverse while assuming arguendo that the employee had a reasonable expectation of privacy without actually addressing the issue. *Id.* at 2629–30 ("The record does establish that [the employer], at the outset, made it clear that pager messages were not considered private. The [employer]'s Computer Policy stated that '[u]sers should have no expectation of privacy or confidentiality when using' [employer] computers.").

decision in *Katz v. United States* by applying the Fourth Amendment to the individual rather than the situation[82] and interpreting the Fourth Amendment's reasonable expectation of privacy to apply to networked, online, or wireless situations.[83]

B. Applying the SCA

Given the often directly contradictory court decisions,[84] it is very difficult for practitioners to anticipate the outcome of cases involving electronic messages or electronic files. Despite these disparate holdings, two recent cases concerning electronic messages provide a broader interpretation of the Electronic Communications Services language and thus, more protection to users of cloud computing services.[85] In *Jennings v. Jennings*, the court addressed the ongoing controversy as to whether an opened email message left on the service provider's server is left for "backup protection."[86] The court, holding that such messages are left for backup protection, commented that "one of the purposes of storing a backup copy of an email message on an ISP's server after it has been opened is so that the message is available in the event that the user needs to retrieve it again."[87] In *Crispin v. Christian Audigier, Inc.*, the court found that a webmail service provider and two social networking sites were Electronic Communication Service providers.[88] These holdings show

82. Katz v. United States, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places.").

83. Quon v. Arch Wireless Operating Co., 529 F.3d at 905; Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); *Bellar*, 217 P.3d at 1107.

84. *See* discussion *supra* Part I.A.

85. *Crispin*, 717 F. Supp. 2d at 987; Jennings v. Jennings, 697 S.E.2d 671, 677–78 (S.C. Ct. App. 2010), *reh'g denied*, 2010 S.C. App. LEXIS 176 (S.C. Ct. App. Aug. 27, 2010).

86. 18 U.S.C. § 2510(17)(B) (2006); *Jennings*, 697 S.E.2d at 677–78.

87. *Jennings*, 697 S.E.2d at 677–78 ("In the present case, the previously opened emails were stored on Yahoo's servers so that, if necessary, [the user] could access them again. Accordingly, we hold that the emails in question were stored 'for purposes of backup protection.'").

88. *Crispin*, 717 F. Supp. 2d at 981–82 ("There . . . is no basis for distinguishing between Media Temple's webmail and Facebook's and MySpace's private messaging, on the one hand, and traditional web-based email on the other. As a consequence, the court concludes that each of Media Temple, Facebook, and MySpace is an ECS provider."). *But see* Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 656 (N.Y. Sup. Ct. 2010) (holding that plaintiff had no reasonable expectation of privacy in social networking sites, "as neither Facebook nor MySpace guarantee complete privacy").

that, despite previous courts' decisions to the contrary,[89] the debate over interpreting the ECS language is swaying in the direction of providing greater protection to electronic messages. The court in *Crispin* also took a very broad interpretation of the RCS language and found the three sites to be Remote Computing Service providers.[90] This holding suggests that courts are willing to qualify such service providers under the SCA language.[91]

Interpreting the SCA remains difficult given the lack of precedent and continuity across jurisdictions.[92] If the Ninth Circuit's recent interpretation in *Quon v. Arch Wireless Operating Co.* of Fourth Amendment protections to electronic communications is at all suggestive of an interest in increased Fourth Amendment protections online,[93] courts may need to broaden their interpretations of the SCA. They may need to apply the SCA to a more diverse group of service providers to prevent the SCA from providing less protection to electronic communications and files than the Fourth Amendment will provide.[94]

---

89. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (holding that the Electronic Communication Service language "is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an email service stores a message until the addressee downloads it. The statute's language explicitly refers to 'temporary, intermediate' storage" and further stating that the Electronic Communication Service language "only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it").

90. *Crispin*, 717 F. Supp. 2d at 987 ("As respects messages that have been opened and retained by Crispin, . . . [Facebook, MySpace, and Media Temple] operate as RCS providers providing storage services . . . .").

91. *Id.* ("[U]nder the reasoning of . . . Flagg, . . . the three entities operate as RCS providers providing storage services . . . ."); Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (finding that "the archive maintained by [the service provider] constitutes 'computer storage,' and that the company's maintenance of this archive on behalf of the City is a 'remote computing service' as defined under the SCA").

92. *Compare Crispin*, 717 F. Supp. 2d at 981–82, *with Romano*, 907 N.Y.S.2d at 656.

93. Despite the United States Supreme Court's reversal of *Quon v. Arch Wireless Operating Co.* in *City of Ontario v. Quon* on other grounds, the Ninth Circuit agreed with the lower court in holding that an employee had a reasonable expectation of privacy. City of Ontario v. Quon, 130 S. Ct. 2619, 2633 (2010); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 910 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010); Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1141 (C.D. Cal. 2006).

94. The concern is that if courts interpret the SCA narrowly and only allow it to apply to a minimum number of service providers while, at the same time, courts interpret the Fourth Amendment broadly and allow it to apply to a variety of online environments, the SCA may prove to be unconstitutional when

C. Third Party Doctrine May Control

No matter how a court decides to apply the SCA and the Fourth Amendment in a cloud computing context, application of the Third Party Doctrine may ultimately be the deciding factor in a case involving cloud computing. The Third Party Doctrine, recognized in a concurrence in *Katz v. United States*,[95] asserts that a party's free exchange of information with a third party essentially destroys the reasonable expectation of privacy upon which much of the Fourth Amendment's protection is based.[96] The Third Party Doctrine has been applied to a number of Fourth Amendment cases[97] based on the sentiment expressed in *Katz* that it is reasonable for an individual to assume that any party with whom he or she shares any information is "recording [the information] or transmitting it to another."[98] In *Smith v. Maryland*,[99] the Court held that a person did not have a reasonable expectation of privacy in the numbers he or she dialed into a phone since the numbers had to be shared with the phone company to

---

courts encounter a situation in which the Fourth Amendment protects a certain file or message while the SCA, due to its narrow interpretation, provides little or no protection to the service provider—and thus to the file or message. *See* discussion *supra* Part II.B (detailing the recent rulings regarding a reasonable expectation of electronic privacy); discussion *infra* Part III.B.2.

95. Katz v. United States, 389 U.S. 347, 363 (1967) (White, J., concurring)("When one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable (or law-abiding) associates. It is but a logical and reasonable extension of this principle that a man take the risk that his hearer, free to memorize what he hears for later verbatim repetitions, is instead recording it or transmitting it to another." (citation omitted)).

96. *Id.* at 360 (Harlan, J., concurring).

97. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that a phone number dialed by the petitioner was not protected by a Fourth Amendment reasonable expectation of privacy because the phone number was shared with the phone company and concluding that the court has "consistently . . . held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that copies of checks and other bank records kept by a bank do not receive Fourth Amendment protection under the reasoning that the "Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . 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"). *See generally, e.g.*, Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966). For a more recent reference to the Third Party Doctrine, consider *United States v. Charbonneau*. United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997) (finding there is a reasonable expectation of privacy until the recipient of the message "forwards the e-mail to a third party").

98. *Katz*, at 363 (White, J., concurring).

99. *Smith*, 442 U.S. at 743.

complete the call.[100] In *United States v. Miller*, copies of an individual's business documents possessed by a bank were not afforded Fourth Amendment protection because the documents had been voluntarily shared with the bank.[101]

Considering the service agreements used by a variety of cloud computing service providers, many individuals have argued that the Third Party Doctrine will foreclose the possibility of Fourth Amendment protection against the government accessing a party's files in a cloud computing environment.[102] A broad range of service agreements exist, but the majority fall into three general categories:[103] (1) an all-inclusive access agreement allowing the provider significant access and control over uploaded files,[104] (2) a generic, general access agreement allowing the provider access primarily to monitor for objectionable content,[105] and (3) an overtly limited access agreement allowing the provider little to no access to a

---

100. *Id.* at 742 ("[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.").

101. *Miller*, 425 U.S. at 442 (holding that respondent's "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business" has "no legitimate 'expectation of privacy'").

102. *See* Robison, *supra* note 7, at 1226–28; Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

103. *See* Robison, *supra* note 7, at 1215.

104. *E.g.*, *Google Terms of Service*, *supra* note 18 ("By submitting, posting or displaying the content [users] give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which [users] submit, post or display on or through [Google's services].").

105. *E.g.*, *Amazon Web Services: Terms of Use*, *supra* note 10 (stating that Amazon "reserves the right (but not the obligation) to remove or edit such content, but does not regularly review posted content," and "has the right but not the obligation to monitor and edit or remove any activity or content"); *ICloud Terms and Conditions*, APPLE, http://www.apple.com/legal/icloud/en/terms.html (last visited Oct. 19, 2011) ("Apple reserves the right at all times to determine whether Content is appropriate and in compliance with this Agreement, and may pre-screen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable."); *MobileMe Terms of Service*, APPLE, http://www.apple.com/legal/mobileme/en/terms.html (last visited May 26, 2011) (on file with Georgia State University Law Review) ("Apple reserves the right at all times to determine whether Content is appropriate and in compliance with these TOS, and may pre-screen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of these TOS or is otherwise objectionable."); *Yahoo! Terms of Service*, YAHOO!, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last visited May 26, 2011) ("Yahoo! and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo! Services.").

user's files.[106] Many providers make it clear in their service agreements that they may access and monitor users' activities and files.[107] Some users may argue that they still have a reasonable expectation of privacy in their files since many service providers are very specific in stating what they may or may not do with a user's files.[108] But the Court in *United States v. Miller* stated that there was no expectation of privacy "even if . . . 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."[109] Comparing this language to the language in many service agreements—such as Amazon's agreement giving it "the right but not the obligation to monitor and edit or remove any activity or content"[110]—it is reasonable that the Third Party Doctrine will prevent the application of Fourth Amendment protection against certain service providers.

This argument does have its weak points, though. First, some service agreements go out of their way to assure users that the provider will not view the user's files.[111] In that context, the Third Party Doctrine would likely not apply, and courts would be forced to use multiple methods of interpreting the Fourth Amendment for the cloud computing environment. Second, the Court raised concerns in *Smith v. Maryland* that the supposed voluntary choice the plaintiff made to share the phone number he dialed with the phone company was not actually voluntary.[112] Justice Marshall's dissent in *Smith*

---

106. *E.g.*, *Privacy: Decho Corporation Privacy Policy*, MOZY, http://mozy.com/privacy (last visited May 26, 2011) (online file backup service provided at Mozy.com states in its privacy policy that Decho "will not view the files that [users] backup using [Decho's service]").

107. *See supra* notes 104–105.

108. *E.g.*, *Amazon Web Services: Terms of Use*, *supra* note 10 (Amazon "reserves the right . . . to remove or edit . . . content").

109. United States v. Miller, 425 U.S. 435, 443 (1976).

110. *Amazon Web Services: Terms of Use*, *supra* note 10.

111. *See supra* note 106.

112. Smith v. Maryland, 42 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." (citation omitted)).

expressed concern that a person had no choice but to either accept potential surveillance or not use a phone—considered to be "a personal or professional necessity."[113]

Similarly, individuals may also end up with no choice but to use cloud computing environments as more and more businesses and individuals embrace them,[114] since the majority of service agreements allow some form of access to a user's files by the service provider.[115] If service agreements continue to embrace the notion of accessing user's files, users of cloud computing services may find themselves with no alternative other than to assume the risk of storing information on cloud computing sites with no expectation of privacy.

III. THE FUTURE OF CLOUD COMPUTING: HOW PRIVACY RIGHTS SHOULD APPLY ONLINE

A. Several Current Recommendations Exist

While the courts have been slowly addressing the issue of how much privacy should be given to online files and emails, practitioners and academics have put forward a variety of solutions, including: the virtual container approach, the content/no content approach, and the loss of privacy online approach.[116] As discussed below, these solutions are inadequate or incomplete, and courts and Congress should instead: (1) apply the Fourth Amendment to online environments using a virtual container approach that focuses on the use of a username and password to prevent public access to the container, (2) interpret the ECS language broadly to find webmail service providers to be Electronic Communication Service providers, (3) amend the RCS language to include a warrant requirement similar to that found in the ECS language, and (4) allow the Third Party Doctrine to eliminate a Fourth Amendment claim for any all-

113. *Id.*
114. Stone & Vance, *supra* note 8, at B1; *Office Politics*, *supra* note 6.
115. *See supra* notes 104–105.
116. *See* discussion *infra* Part III.A.1–3.

inclusive access agreements while preventing the Third Party Doctrine from eliminating a Fourth Amendment claim for generic, general access agreements or overtly limited access agreements.

1. A Virtual Container That Conceals its Contents

Throughout the evolution of the Fourth Amendment, courts have applied its protection to situations involving containers that conceal their contents from the general public, such as briefcases, backpacks, and the home.[117] Courts have distinguished containers that effectively conceal their contents from the general public from those that reveal their contents.[118] A suggested solution to the question of how to apply the Fourth Amendment to an online environment is to look at the online world as analogous to the physical world and focus on the concept of virtual containers.[119] A virtual container in the cloud computing context would be a folder or email account hosted on a remote server.[120] A court would then focus on whether that virtual container effectively concealed its contents from the outside world and, if the contents were effectively concealed, the Fourth Amendment would provide the same level of protection that any other concealed container would receive.[121] Effective concealment of a virtual container's contents would be shown through the use of a username and password, electronic encryption, or some other form of protection that prevents the general public from accessing the virtual container or its contents.[122]

---

117. Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 351 (8th Cir. 2004) (holding that searches of backpacks and purses violated the Fourth Amendment); United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983) (finding Fourth Amendment privacy rights in a briefcase).

118. United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005) (holding that a gun case that was labeled "gun guard" did not maintain a reasonable expectation of privacy because the label clearly revealed the contents of the container, with the court stating that "[a]lthough a person generally has an expectation of privacy in items he places in a closed container, some containers so betray their contents as to abrogate any such expectation").

119. *See* Couillard, *supra* note 27, at 2233–37.

120. *See id.* at 2233–34.

121. United States v. D'Andrea, 497 F. Supp. 2d 117, 122 n.16 (D. Mass. 2007), *rev'd*, 648 F.3d 1 (1st Cir. 2011) ("A website, like a computer file, is properly analogized to a file cabinet or other physical containers in which records can be stored."); Couillard, *supra* note 27, at 2236.

122. *See* Couillard, *supra* note 27, at 2236.

Although the virtual container solution seems like a reasonable approach in most contexts, the use of electronic encryption on uploaded files does not fit well with an analogy to containers in the non-virtual world.[123] When addressing methods of concealing data in the non-virtual world, courts have focused on whether police have legal access to the data itself while assuming that, if the police have such access, they are free to attempt to decode or reconstruct the data.[124] Claiming an electronic file uploaded to a particular site should receive Fourth Amendment protection if encrypted but not providing protection to the same file uploaded to the same site if unencrypted makes little sense. Courts should focus on the virtual container the file is stored in rather than the encryption applied to the file itself.

2. Content/Non-Content

An interesting distinction has been made between items in electronic communications that qualify as content versus non-content.[125] Non-content items are electronic tags that are required to send, receive, and identify messages.[126] In an email, the non-content

---

123. *See id.* at 2234 (arguing that encryption should be recognized as a form of concealment that will invoke Fourth Amendment protection while acknowledging that "an encrypted letter sealed in an envelope would be covered by the Fourth Amendment, but the legal basis for its protection would be the envelope, not the encryption"); Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 506 (2001) (arguing that merely encrypting or encoding data cannot ensure Fourth Amendment protection and "the decryption of ciphertext cannot violate a reasonable expectation of privacy").

124. *See* United States v. Longoria, 177 F.3d 1179, 1183 (10th Cir. 1999) (holding that defendant's Fourth Amendment rights were not violated when defendant was recorded speaking of illegal activities in Spanish even though he specifically used Spanish to prevent individuals he was standing with, who were not in on the illegal activities, from understanding his statements); United States v. Scott, 975 F.2d 927, 930 (1st Cir. 1992) (holding that the government did not violate defendant's Fourth Amendment rights when the government seized and reconstructed shredded tax records that defendant shredded in an attempt to conceal records from the government); United States v. Rubinstein, No. 09-20611-CR, 2010 WL 2723186, at *11–12 (S.D. Fla. June 24, 2010) (recommending that evidence recovered from a desktop with a warrant not be suppressed despite the government's delay in examining the computer while expressing no concern that investigators attempted to decrypt an encrypted drive found on the computer). For a further discussion of encryption technologies and issues, see Kerr, *supra* note 123, at 506, and Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 391–96 (2010).

125. *See* Kerr, *supra* note 27, at 1019–23.

126. *See id.* at 1019–20.

would likely be considered the "To" and "From" fields in the message.[127] Content, on the other hand, would be the text of an electronic communication—the actual message itself.[128] This distinction is compared to postal letters in the non-virtual world.[129] The outside of letters and packages can be inspected without any concern over violating the sender's Fourth Amendment rights—similar in nature to inspecting the "To" and "From" fields in an electronic communication.[130] The inside of the letter cannot be opened and inspected without proper Fourth Amendment permission—similar again to the subject line and the text of an electronic communication.[131]

This distinction between content and non-content works well for many different forms of electronic communication, but it becomes less useful when applied to documents stored online. What is the content or the non-content of an electronic document? Possibly the title of the electronic file would be considered non-content while the text of the document itself would be the content. The challenge with that division is that the file name may well reveal the subject of the document. In a warrantless review of an email or a postal letter, however, the authorities should not review the subject line of an email or the subject matter of a postal letter.[132]

Recognizing the difficulty of applying a content/non-content distinction to online documents, one approach is to apply a

127. *See id.*
128. *Id.*
129. *Id.*
130. 39 C.F.R. § 233.11 (2010); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("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 . . . . Whilst in the mail, they can only be opened and examined under like warrant . . . ."); Kerr, *supra* note 27, at 1019–20.
131. 39 C.F.R. § 233.11 (2010) (stating that even if postal workers suspect a piece of mail is dangerous to people or property, the workers must screen the package "without opening mail that is sealed against inspection or revealing the contents of correspondence within mail that is sealed against inspection"); *Jackson*, 96 U.S. at 733 ("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."); Kerr, *supra* note 27, at 1019–20.
132. 39 C.F.R. § 233.11 (2010); Kerr, *supra* note 27, at 1030. Even postal regulation blatantly recognizes the importance of protecting the content of correspondence. 39 C.F.R. § 233.11 (2010) (stating that workers screen packages "without . . . revealing the contents of correspondence within mail that is sealed against inspection").

content/non-content approach to electronic communications and apply a different approach to documents stored in the cloud.[133] However, this approach would force courts and practitioners to use two different methods to analyze the available Fourth Amendment protection to an individual's cloud computing account. With the ever-expanding list of companies that provide both online document storage and email services—such as Apple or Google—it makes more sense to develop one method to apply to all online cloud computing activities.[134]

3. Loss of Privacy Online

Despite the possible applications of the Fourth Amendment and the SCA to today's online environment, there is an argument for simply embracing the idea that individuals should have little to no online privacy. The cofounder of Sun Microsystems, Scott McNealy, is now infamous for his blunt statement, "You have zero [online] privacy anyway. Get over it."[135] Given the SCA's limiting language and a lack of clear understanding as to what law applies to online files if the SCA does not, it is reasonable to believe that online privacy may not currently exist.[136]

Although individuals and companies may be wise to operate under this assumption until online privacy is more clearly understood, allowing an ongoing general lack of online privacy is a significant mistake. Cloud computing environments have enormous potential, not only through saving money and providing greater convenience, but also through additional benefits like far less energy consumption

---

133. Kerr, *supra* note 27, at 1019–20, 1029 (arguing primarily for the application of content/non-content distinctions to electronic communications).

134. *ICloud: Calendar, Mail, and Contacts*, APPLE, http://www.apple.com/icloud/features/calendar-mail-contacts.html (last visited Oct. 19, 2011); *ICloud: Documents in the Cloud*, APPLE, http://www.apple.com/icloud/features/documents.html (last visited Oct. 19, 2011); *MobileMe Features*, APPLE, http://www.apple.com/mobileme/features/ (last visited May 26, 2011) (on file with Georgia State University Law Review) ("MobileMe keeps your mail, contacts, and calendar information in the cloud . . . ."); *Products*, GOOGLE, http://www.google.com/intl/en/options/ (last visited May 26, 2011).

135. Eric Cohen, *Privatization of American Morality*, L.A. TIMES, Mar. 18, 2001, at M1; Robison, *supra* note 7, at 1195.

136. *See* discussion *supra* Part I.A; Robison, *supra* note 7, at 1239.

per household and, thus, a greener world.[137] Scaring individuals and companies away from cloud computing by limiting the Fourth Amendment's application to online environments and narrowly reading the SCA language would severely constrict the benefits of cloud computing.

B. An All Encompassing Approach

An effective solution for managing cloud computing and privacy concerns online must address three different elements: (1) the application of the Fourth Amendment to cloud computing environments, (2) how the SCA will apply to cloud computing situations not contemplated when the SCA was initially created, and (3) how service agreements and the Third Party Doctrine will influence the application of both the Fourth Amendment and the SCA.

1. The Fourth Amendment Online

Courts should apply the Fourth Amendment to online environments using a virtual container approach. The virtual container approach requires a username and password. Several courts have already applied the Fourth Amendment to online environments.[138] Throughout the history of the Fourth Amendment, courts have stressed the importance of applying the Fourth Amendment to "people, not places."[139] It is important to recognize that, as cloud computing becomes more prevalent, people will continue to upload more and more of their personal documents to the cloud. Courts should focus on a person's Fourth Amendment rights rather than on the fact that a person may store her personal files in a new location. The court in *United States v. Freire* reasoned that briefcases carry such close, personal items—such as "address books,

137. FRIEDMAN, *supra* note 15, at 232–33 (detailing how, by using a machine called a Sun Ray terminal at home to log on to the cloud, the user can conserve significant energy by not using a traditional PC).

138. *See* discussion *supra* Part I.B.

139. Katz v. United States, 389 U.S. 347, 351 (1967).

personal calendar/diaries, [and] correspondence"—that they warrant Fourth Amendment protection.[140] Cloud computing embraces all of these functions.[141] If an individual mailed a postal letter or printed a document at home and carried it in her briefcase to work, both the letter and the document would receive Fourth Amendment protection.[142] It makes little sense to claim that if instead of mailing a letter she sent an email, and if instead of printing a document she uploaded the document to the cloud and retrieved it when she arrived at work, neither of her documents would be protected by the Fourth Amendment.[143]

Certainly not all online files should be protected. If an individual uploads a file to a public site, accessible by anyone, that individual has exposed the file to the public, and no protection should be extended to the file. Although the Court in *Katz* specified that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[144] While the Court clearly recognized the importance of protecting personal files, the Court also used the language "may be" rather than "is." Drawing a distinction as to which files should receive constitutional protection in a cloud computing environment is a complicated process. Courts should embrace the concept of the virtual container, but focus on the container itself rather than the file uploaded to the cloud.[145]

Essential to extending constitutional protection to online environments is the idea of a virtual container that conceals its contents through the use of a username and password, showing the individual's attempt to preserve her privacy.[146] MobileMe's service

140. United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983); Couillard, *supra* note 27, at 2210–11.

141. *ICloud: Calendar, Mail, and Contacts*, APPLE, http://www.apple.com/icloud/features/calendar-mail-contacts.html (last visited Oct. 19, 2011); *MobileMe Features*, APPLE, http://www.apple.com/mobileme/features/ (last visited May 26, 2011) (on file with Georgia State University Law Review) ("MobileMe keeps your mail, contacts, and calendar information in the cloud . . . ."). *See* discussion *supra* Introduction.

142. Couillard, *supra* note 27, at 2238.

143. *Id.*

144. *Katz*, 389 U.S. at 351.

145. *See* discussion *supra* Part III.A.1.

146. *See* United States v. Ross, 456 U.S. 798, 822–23 (1982) ("[T]he Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view.").

provides a helpful distinction between online files that should receive Fourth Amendment protection and online files that should not.[147] A user of MobileMe's service has two different virtual containers: a private folder and a public folder.[148] The private folder is accessible to only those particular individuals that have the user's username and password, while the public folder is accessible to anyone who has the web address.[149] Much like a briefcase, backpack, or postal package, the private, password-protected virtual container effectively conceals its contents from the general public and should receive constitutional protection through the user's Fourth Amendment rights. The public folder, on the other hand, reveals its contents to whoever has the web address and should receive no constitutional protection.[150] This virtual container understanding should be applied to all cloud computing environments, extending Fourth Amendment protection to webmail services or any other cloud computing services that conceal the contents of an online container behind a username and password. If, on the other hand, the contents of a container are visible to anyone with knowledge of the container's online location, Fourth Amendment protection should not be extended.

2. The SCA's Future

In addition to applying the Fourth Amendment to the cloud computing environment, the SCA must be read broadly to prevent the Act from being found unconstitutional. Courts should interpret the ECS language broadly to find webmail service providers to be Electronic Communication Service providers. The flexible interpretations in both *Crispin v. Christian Audigier, Inc*. and *Jennings v. Jennings*, where the courts found webmail providers and

147. *MobileMe's iDisk Features*, APPLE, http://www.apple.com/mobileme/features/idisk.html (last visited May 26, 2011) (on file with Georgia State University Law Review).

148. *Id.*

149. *Id.*

150. While the default setting allows anyone with the web address to access files in the public folder, there is an option to password protect the public folder to limit general, public access to it. For simplicity's sake, MobileMe's iDisk service will be analyzed assuming the service retains its default setting. *MobileMe: How to Password-Protect Shared Files in your iDisk*, APPLE, http://support.apple.com/kb/HT2127 (last visited Oct. 19, 2011).

social networking sites to be Electronic Communication Service providers, should guide future courts in applying the ECS language.[151] A strict interpretation of the SCA may lead courts to find a webmail service provider does not qualify as an Electronic Communication Service and thus find the SCA does not require that same provider to demand a warrant from the government to search and seize webmail.[152] This interpretation would have contradictory results: while the user would have Fourth Amendment rights in his webmail service, the SCA would not force his webmail service provider to require a warrant for a governmental search. This contradiction could potentially threaten the constitutionality of the ECS portion of the SCA. Thus, an interpretation of the ECS language allowing webmail service providers to qualify as Electronic Communication Service providers is essential.

The Legislature should amend the RCS language to include a warrant requirement similar to that found in the ECS language. Simply requiring a subpoena or a court order should not be enough. Even the broad interpretation of the RCS language found in *Crispin* should not prevent it from being found unconstitutional.[153] If a court qualifies a cloud computing provider as a Remote Computing Service provider, a warrant is not necessarily required for a government agency to search and seize online documents.[154] The Act will be in direct conflict with the application of the Fourth Amendment to cloud computing environments through the virtual container method. On the one hand, the Fourth Amendment would require the government to get a warrant to search any files stored in a virtual container protected by a username and password. On the other hand, the RCS language would not require a warrant and instead, merely require a subpoena or a court order to access the files even if a court did find

151. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); Jennings v. Jennings, 697 S.E.2d 671, 676 (S.C. Ct. App. 2010), *reh'g denied*, 2010 S.C. App. LEXIS 176 (S.C. Ct. App. Aug. 27, 2010).

152. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001); discussion *supra* Part II.A.

153. *Crispin*, 717 F. Supp. 2d at 987.

154. *See* discussion *supra* Part I.A.2.

that a service provider qualified as a Remote Computing Service.[155] Given this contradiction, the RCS language must be amended. It should incorporate a warrant requirement similar to that found in the ECS section of the SCA, which requires a warrant to access files stored in a password-protected virtual container.

3. Service Agreements and the Third Party Doctrine

Courts should allow the Third Party Doctrine to eliminate a Fourth Amendment claim with any all-inclusive access agreements while preventing the Third Party Doctrine from eliminating a Fourth Amendment claim with generic, general access agreements or overtly limited access agreements.[156] While the initial presumption by courts should be that the Fourth Amendment applies to cloud computing environments, the service agreements of cloud computing providers will have an enormous influence on whether Fourth Amendment rights will ultimately require warrants for government searches of an individual's cloud computing files. Of the three standard types of agreements, two are relatively easy to address.[157] The all-inclusive agreement, embraced by companies such as Google, that allows significant access and control over uploaded files to the service provider should be recognized as a user voluntarily sharing information with a third party and, thus, eliminate the user's reasonable expectation of privacy.[158] The lack of a reasonable expectation of privacy on the user's part should then eliminate the user's Fourth Amendment protections as to the cloud computing

155. *See* discussion *supra* Part I.A.2.

156. It is worth noting that users may not actually read the access agreements—commonly in the form of click-wrap or click-through agreements requiring users to click a button labeled 'Agree' before they proceed—when they sign up for cloud computing services. The question of whether a user will be held to an access agreement that he did not read is a valid question, but it is outside the scope of this Note. This Note assumes that access agreements between a user and a service provider are valid. For further discussions on the enforceability of click-wrap or click-through agreements, see Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 577–78 (2007); Lucille M. Ponte, *Getting a Bad Rap? Unconscionability in Clickwrap Dispute Resolution Clauses and a Proposal for Improving the Quality of These Online Consumer "Products"*, 26 OHIO ST. J. ON DISP. RESOL. 119, 120 (2011); Ty Tasker & Daryn Pakcyk, *Cyber-Surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 ALB. L.J. SCI. & TECH. 79, 85–86 (2008).

157. *See* discussion *supra* Part II.C.

158. *E.g.*, *Google Terms of Service*, *supra* note 18.

files. Agreements that are overtly limited and allow the provider little to no access to a user's files should not qualify as a user voluntarily sharing information with a third party and, thus, should allow a user to reasonably expect privacy. [159] This reasonable expectation should translate into an extension of the user's Fourth Amendment rights to her online files.

Applying the Third Party Doctrine to a generic, general access agreement that allows the provider general access primarily to monitor for objectionable content is not as straightforward.[160] Although providers do have access to a user's files, that access is distinguishable and far more limited than access given to providers with all-inclusive access agreements.[161] The agreement allows providers to generally monitor the files uploaded by a user but does not suggest a continuous, intrusive monitoring by the provider. The distinction between constant monitoring and more general monitoring is similar to a distinction made by the court in *United States v. Maynard*, examining a scenario in the non-virtual world.[162] The court in *Maynard* found that police violated a driver's reasonable expectation of privacy in his movements when they attached a GPS tracking device to his car without a warrant and tracked his every move for a month.[163] While the court acknowledged that an individual does not generally have a reasonable expectation of privacy when he moves about in public, the court distinguished an individual merely moving about for a short time in public and police tracking his every move for a month.[164]

---

159. *E.g.*, *Privacy: Decho Corporation Privacy Policy*, *supra* note 107.

160. *E.g.*, *Amazon Web Services: Terms of Use*, *supra* note 10; *ICloud Terms and Conditions, supra* note 106; *MobileMe Terms of Service*, *supra* note 106; *Yahoo! Terms of Service*, *supra* note 106.

161. *Compare Google Terms of Service*, *supra* note 18, *with ICloud Terms and Conditions, supra* note 106, *and MobileMe Terms of Service*, *supra* note 106.

162. United States v. Maynard, 615 F.3d 544, 558, 563, 568 (D.C. Cir. 2010).

163. *Id.* at 558 (noting that the use of the GPS device allowed the police to discover "the totality and pattern of [the defendant's] movements from place to place to place").

164. *Id.* ("[U]nlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. . . . [T]he whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more . . . than does the sum of its parts.").

The distinction drawn by the court in *Maynard* is important when considering the application of the Third Party Doctrine to cloud computing environments. Under a generic monitoring service agreement providing general access, a user should have a reasonable expectation of privacy since the provider does not explicitly state that it will review each file uploaded by the user. The provider instead will perform only occasional monitoring functions. This situation is distinguishable from *Smith v. Maryland* where the phone numbers an individual dialed had to be shared with the phone company to complete every single call.[165] This situation is also distinguishable from *United States v. Miller* where the documents a customer shared with the bank were each individually reviewed by the bank's employees "in the ordinary course of business."[166]

If a provider with a generic, general access agreement begins to closely monitor a user's activity or turns files over to the government without requiring a warrant, the user's reasonable expectation of privacy and Fourth Amendment rights should be considered violated pursuant to *Maynard*. There is a significant difference between sporadically viewing and continuously monitoring or claiming a license to every file that is uploaded. Unless the service agreement specifically states that every file is reviewed by or licensed to the provider—as in the all-inclusive service agreements or a traditional Third Party Doctrine case—a user should reasonably expect privacy in her cloud computing documents. To ensure users understand what is at stake, the wording of an all-inclusive access agreement should explicitly state that a user's Fourth Amendment rights in any documents uploaded to the cloud are lost if the user agrees to the all-inclusive access agreement.

CONCLUSION

Concerns over what privacy rights exist for online documents have left many individuals and companies questioning the wisdom of

165. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
166. United States v. Miller, 425 U.S. 435, 442 (1976).

embracing cloud computing.[167] Given the potential advantages that cloud computing services offer, courts should clarify the privacy rights given to cloud computing environments. The Fourth Amendment should apply to online environments, and courts should adopt a virtual container model that recognizes the distinctions between a username and password protected container and a container available to the general public.[168] The Electronic Communication Service language of the SCA should be interpreted broadly to avoid conflicting with the Fourth Amendment, while the Remote Computing Services language of the SCA should be found unconstitutional given its conflict with the Fourth Amendment—no matter what interpretation is applied.[169] The Remote Computing Services language should then be amended to include a warrant requirement.[170] While the Third Party Doctrine should also be applied to the cloud computing environment, it should be applied narrowly—only to those service agreements that grant service providers all-inclusive access to a user's files.[171] Courts should give users as much online privacy protection as possible to ensure individuals and companies will readily embrace cloud computing and the benefits it can provide.

167. *See* discussion *supra* Introduction.
168. *See* discussion *supra* Part III.B.1.
169. *See* discussion *supra* Part III.B.2.
170. *See* discussion *supra* Part III.B.2.
171. *See* discussion *supra* Part III.B.3.