Santa Clara University
School of Law

Santa Clara Law Review

Volume 55 | Number 2 Article 6

10-7-2015

Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud

Christina Raquel

BLUE SKIES AHEAD: CLEARING THE AIR FOR INFORMATION PRIVACY IN THE CLOUD

Christina Raquel*

TABLE OF CONTENTS

---

* Managing Editor, SANTA CLARA LAW REVIEW, Volume 55; J.D. Candidate, May 2015, Santa Clara School of Law; B.A., Political Science, University of Southern California, 2012. I would like to thank the Volume 55 Editorial Board of the SANTA CLARA LAW REVIEW for their dedication and countless hours of hard work, and Professor Allen S. Hammond for his assistance and encouragement. I owe my biggest thanks to my dear family and friends for their never ending love and support.

INTRODUCTION

Are you twenty-eight years old, feel encumbered by the past, and find yourself unable to achieve your initial promise? Do you think it's about time to get your head in the cloud? "Yes," replied the Stored Communications Act.[1] Four years before the introduction of the World Wide Web, Congress passed the Stored Communications Act ("SCA") as part of the Electronic Communications Privacy Act ("ECPA") in 1986 to govern access to electronically stored communications.[2] Premised on the 1980's computer technology, the SCA represented a remarkably progressive statutory framework that established privacy safeguards for emerging technologies.[3]

Outdated and disjointed nearly three decades later, the SCA finds itself struggling to maintain applicability and legitimacy amidst the recent thunderstorm of technological innovation. Today, the SCA provides a tangled web of "Fourth Amendment-like privacy protections, regulating the relationship between government investigators and [Internet] service providers in possession of users' private information."[4]

Today's Americans, more forward thinking than ever before, have their heads in the cloud. The cloud represents a

1. *See* 18 U.S.C. §§ 2701–11 (2000 & Supp. I 2001).

2. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

3. *See* Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 351 (2009).

4. 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, 1212 (2004) [hereinafter Kerr, *SCA User's Guide*].

transformative computing model where users share or store their information on remote servers owned or operated by third parties.[5] Files once confined to one's home are now readily accessible in his or her respective virtual home with the simple tap of a finger on any Internet-connected device.[6]

As society increasingly turns away from the personal computing model, the recent proliferation of cloud computing engenders considerable uncertainty as to the SCA's scope of privacy protections to communications stored in the cloud.[7] The SCA's inability to guarantee constitutional privacy protections in the current technological landscape—unanticipated by Congress in 1986—will undermine consumer and corporate trust, and consequently, stifle technological innovation.

It is crucial for Congress to look at clouds from both sides now, because the SCA really doesn't consider clouds at all.[8] This Comment argues that the existing statutory framework inadequately protects cloud users and propositions Congress to amend the SCA so as to not marginalize individuals who migrate their data from their in-home filing cabinets to their digital lockers in the cloud. The SCA should ensure parity between content stored physically and electronically.

Parts I through V provide the foundation for this discussion by exploring the cloud and the applicable constitutional and statutory doctrines. Together, Parts VI and VII demonstrate that the SCA's archaic framework has created a fragmented set of privacy protections that leave cloud-computing platforms outside the statute's protection. Finally, Part VIII proposes statutory amendments that adequately reflect the existing technological landscape while providing flexibility for emerging technologies as they become relevant. Having argued that data in the cloud should receive

---

5. Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality From Cloud Computing* (Nov. 4, 2009), http://www.world privacyforum.org/pdflWPFCloud PrivacyReport.pdf.

6. *How Cloud Computing Works,* HOWSTUFFWORKS.COM http://computer. howstuffworks. com/cloud-computing/cloud-computing.htm (last visited Oct. 20, 2013).

7. *See e.g.*, Ilana R. Kattan, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 619 (2011) (explaining that the personal computing model is a model "in which users access, store, and manage their data and processing locally on their own PCs.").

8. JONI MITCHELL, BOTH SIDES NOW (Reprise 1969).

protection comparable to their tangible equivalents, Part VIII advocates for "tech neutrality," where, regardless of future developments in communication technology, the presence and application of the Electronic Communications Privacy Act remain constant.[9]

I. CLOUD COMPUTING PLATFORMS

Cloud computing represents a dynamic technological and computational advance. With about 69% of United States Internet users currently utilizing cloud-based platforms and with $241 billon industry forecasts by 2020, experts project cloud computing to revolutionize "how businesses function, how cities are planned, and how people carry out their work."[10] This section will detail the technological landscape that facilitated the cloud's evolution, define cloud computing and its variations, and explain how individuals utilize the cloud.

A. Technological Landscape & Evolution

While the cloud computing paradigm recently gained traction as a trendy and widespread infrastructure, its underlying concepts are derivative of 1960s technologies: mainframe and personal computing models.[11] Firms—recognizing the then-inordinate costs to acquire, maintain, and operate mainframe computers—essentially acted as landlords and allowed users to "operate on slices of a central server's time and resources."[12] This technological real estate market quickly dissipated during the following two decades with the advent of the fairly inexpensive minicomputer.[13] In the 1990s, Application Service Providers ("ASPs") quickly emerged as industry leaders, providing standardized, fully provisioned, and fully maintained

9. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1016 (2010) [hereinafter Kerr, *Fourth Amendment to the Internet*].

10. Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 356 (2013).

11. *See* John Soma et al., *Chasing the Clouds Without Getting Drenched: A Call for Fair Practices in Cloud Computing Services*, 16 J. TECH. L. & POL'Y 193, 196 (2011).

12. *Id.*

13. ANDY MULHOLLAND ET AL., ENTERPRISE CLOUD COMPUTING: A STRATEGY GUIDE FOR BUSINESS AND TECHNOLOGY LEADERS 15 (2010).

applications accessible over Internet-connected personal computers.[14] Just as quickly as the ASPs dissipated alongside the rubble of the dot-com bust, the arrival of virtualization technologies, ubiquitous Internet deployment, commoditizing of hardware, and software standardization set the stage for shared-services computing's comeback performance.[15]

B. Defining the Cloud

In the midst of an August 2006 address at the Search Engine Strategies Conference, Google, Inc. CEO Eric Schmidt gave wind to the term, "cloud computing," by referring to software applications hosted on remote servers.[16] The cloud is a collection of interconnected computers and servers publically accessible via the Internet.[17] In network diagrams—comprised of servers, client PCs, switches, routers, and the Internet—the cloud icon represents the overarching element that allows the network to function.[18] Consisting of networks, remote web-based applications, and remote data storage, cloud computing essentially represents a metaphor for the Internet.[19]

Despite significant efforts to define cloud computing, its existing definitions vary and will likely be refined when the paradigm becomes better understood.[20] The National Institute of Standards & Technology ("NIST") defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable

---

14. *Id.*

15. *See* Soma et al., *supra* note 11, at 196–97; *see also*, Soma et al., *supra* note 11, at n.11 ("'Virtualization' is a method of running multiple independent virtual operating systems on a single physical computer."); *see generally* Soma et al., *supra* note 11 (explaining that "Commoditizing of hardware" is the mass production and ease of access as well as the identical nature of hardware).

16. *See* Jacob M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet*, 23 GEO. MASON U. CIV. RTS. L.J. 255, 258 (2013).

17. *See id.* at 258–59.

18. *See* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1626 (2013).

19. *See* ANTHONY T. VELTE ET AL., CLOUD COMPUTING: A PRACTICAL APPROACH 3–4 (2010); *see also* 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, 360–61 (2010).

20. William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 BUS. LAW. 237, 237 (2010).

computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[21] To simplify NIST's definition, cloud computing is "a different way for people to use their computers."[22]

C. Using the Cloud

While computer users of earlier decades needed to maintain specialized software on their hard drives to accomplish various tasks, the cloud securely delivers that sophisticated technology as a virtual platform on the Internet at the physical access-point on an as-needed basis.[23] Located in data centers around the world, thousands of computers handle data processing and storage for millions of users.[24] Users enjoy anywhere access to their files and applications once they move their content to the cloud.[25]

Clouds take on several different structures and functions depending on the varying needs of the end-users, provider's framework, and service exchange.[26] Organizations deploy clouds in two predominant ways: (1) privately on the organization's infrastructure, or (2) publically over the Internet as a fee-based, advertiser-supported service.[27] While private cloud users encounter similar risks as public cloud users, the public cloud is the foremost concern for policy makers and industry leaders.[28]

The industry generally partitions public clouds into three

---

21. PETER MELL & TIMOTHY GRANCE, NAT'L. INST. OF STANDARDS AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2 (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

22. Small, *supra* note 16, at 259.

23. *See* Kesan et al., *supra* note 10, at 355.

24. *See* Soghoian, *supra* note 19, at 364.

25. *See* Darlene Bedley, *A Look at the Proposed Electronic Communications Privacy Act Amendments Act of 2011: Where Is Smart Grid Technology, and How Does Inevitable Discovery Apply?*, 36 NOVA L. REV. 521, 524 (2012).

26. *See* Jenna Gerber, *Head Out of the Clouds: What the United States May Learn from the European Union's Treatment of Data in the Cloud*, 23 IND. INT'L & COMP. L. REV. 245, 247 (2013).

27. *See* Timothy D. Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 283, 287 (2010).

28. *See* Brad Smith, *Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud*, MICROSOFT (Oct. 20, 2013, 8:45 PM), https://www.microsoft.com/en-us/news/press/2010/jan10/1-20brookingspr.aspx (Senior Vice President and General Counsel).

service models based on the distinct capabilities offered to the consumer: (1) Software-as-a-Service ("SaaS"), (2) Platform-as-a-Service ("PaaS"), and (3) Infrastructure-as-a-Service ("IaaS").[29] SaaS involves the "capability provided to the consumer . . . to use the provider's applications running on a cloud infrastructure."[30] 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."[31] IaaS involves the "capability provided to the consumer . . . to provision processing, storage, networks, and other fundamental computing resources . . . IaaS providers supply only the necessary resources that organizations require."[32]

Businesses and users migrate their content to the cloud, as its delivery model provides alluring advantages to both service providers and end-users alike.[33] Service providers benefit from their enhanced ability to readily deny or terminate access to troublesome users, heighten security, and guard sensitive intellectual property and technology.[34] When software is delivered via the Internet, unauthorized copying is virtually nonexistent.[35] Where users are unable to host the tools on their own servers, and where cloud products' computation and coding remain tightly held on the given provider's servers, cloud providers do not encounter the infamous and illegal network-sharing of expensive and essential technology such as Microsoft Office, Adobe

29. *See* Gerber, *supra* note 26, at 247.

30. Hien Timothy M. Nguyen, *Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing*, 86 NOTRE DAME L. REV. 2189, 2201 (2011) (ranging from productivity applications such as word processing to entertainment hubs providing video and music).

31. *See, e.g.*, *id.* (discussing how Microsoft's Windows Azure provides the function to build applications spanning from consumer Web to enterprise scenarios).

32. *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the Sen. Comm. on the Judiciary*, 111th Cong. 113 (2010) (statement of The Computer & Communications Industry Association) ("IaaS offers full-service virtual information stacks designed to replace a company's entire server room and network through virtualization technology."); *see also*, Ngyuen, *supra* note 30, at 2201 (discussing how Netflix is moving its existing Internet technology to the cloud via Amazon Web Services).

33. *See* Soma et al., *supra* note 11, at 201.

34. Soghoian, *supra* note 19, at 364.

35. *Id.*

Photoshop, and the like.[36] Similarly, trade secrets, such as algorithms, that exist for such programs and applications are considerably less accessible by competitors, as reverse engineering is exceptionally difficult.[37]

Many cloud computing applications and services are consumer-oriented.[38] End-users enjoy either free or inexpensive technologies, offering many of the same, basic features found on their desktop counterparts, and more.[39] By sharing resources across numerous users, cloud platforms significantly enhance users' abilities to work collaboratively.[40] End-users benefit from the cloud's data preservation and overwhelming accessibility: users may access applications and data from any device, anywhere in the world, provided they have some sort of Internet connection.[41] As applications run directly from the cloud, cloud computing provides a simple solution to computer memory and storage capacity issues.[42] Alongside eliminating hard drive capacity issues, cloud computing similarly eliminates hard drive failure concerns.[43] Cloud services regularly back up files on multiple servers, giving users solace in that their files will never be lost.[44]

The cloud's abundant benefits are not without risk. Migrating data to the cloud necessarily suggests that users relinquish some dominion over that data.[45] The ominous rain cloud that looms over this innovative paradigm is privacy, or the lack thereof. While the right to privacy represents "the most comprehensive of rights and the right most valued by civilized men,"[46] conceptualizing this right in the cloud is a perplexing endeavor.

Uncertainty as to privacy in the cloud should give pause to users, providers, legislators, and judges alike. While no

---

36. *Id.*
37. *Id.* at 365.
38. *See id.* at 356–66.
39. *See* Tina Cheng, *A Cloudy Forecast: Divergence in the Cloud Computing Laws of the United States, European Union, and China*, 41 GA. J. INT'L & COMP. L. 481, 484–85 (2013).
40. *See* Martin, *supra* note 27, at 297.
41. *See* Kesan et al., *supra* note 10, at 362.
42. Cheng, *supra* note 39, at 484.
43. *See* Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29, 29–30 (2010).
44. Cheng, *supra* note 39, at 484.
45. *See* Martin, *supra* note 27, at 300.
46. Olmstead v. United States, 277 U.S. 438, 478 (1928).

law expressly addresses privacy in the cloud, a cursory glance at United States privacy law—both constitutional and statutory—lends credence to the principle of safeguarding user-privacy in the cloud.[47]

II. THE FOURTH AMENDMENT

The Fourth Amendment, applicable to federal, state, and local investigators,[48] serves as the primary regulator of law enforcement conduct in the course of physical-world criminal investigations.[49] It provides, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."[50] The Fourth Amendment requires that the government submit a particular description of the places to be searched and the things to be seized.[51] While an all-encompassing reasonableness standard provides the Fourth Amendment with procedural legitimacy,[52] the Supreme Court administers the amendment's goal by creating exacting standards that proscribe what law enforcement can do, when, and under what circumstances.[53]

The Supreme Court recognized that "[t]he overriding function of the Fourth Amendment is to protect the personal privacy and dignity against unwarranted intrusion by the state."[54] "It is not the breaking of his doors, and the

47. *See generally* U.S. CONST. amend. IV; *see also* 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. §§ 2701–10 (2006)).

48. *See* Mapp v. Ohio, 367 U.S. 643, 670 (1961) (holding that the exclusionary rule of the Fourth Amendment applies to the states through the Fourteenth Amendment).

49. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law,* 54 HASTINGS L.J. 805, 810 (2003) [hereinafter Kerr, *Lifting the Fog*].

50. U.S. CONST. amend. IV.

51. U.S. CONST. amend. IV; *see also* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (describing the particularity required in a warrant for the places to be searched); *see also* Andresen v. Maryland, 427 U.S. 463, 474 (1976) (describing the permissible breadth of warranted seizures).

52. *See* Illinois v. McArthur, 531 U.S. 326, 330 (2001) (noting that the Fourth Amendment's "central requirement is one of reasonableness.").

53. *See* Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1164 (1998).

54. *See* Schmerber v. California, 384 U.S. 757, 767 (1966) (finding no Fourth Amendment violation where a police officer directed a physician to draw a blood

rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property."[55]

A. The Reasonable Expectation of Privacy

Notwithstanding the apparently extensive protection offered by the Fourth Amendment, not all government action that uncovers probative evidence constitutes a "search" within the Fourth Amendment context.[56] Accordingly, the Fourth Amendment does not guard against all searches in all areas.[57]

Katz v. United States[58] denotes the Court's modern era privacy doctrine.[59] *Katz* arose when government agents, without a search warrant, attached a listening device to the exterior of a public phone booth—from which Katz made a call—in order to eavesdrop on the defendant's telephone conversation.[60] In finding the contents of the phone conversation protected by the Fourth Amendment, the Court emphasized that what a person seeks to maintain as private, even in an area accessible to the public, is sacrosanct under the Fourth Amendment.[61]

Justice Harlan, concurring in judgment, canonized the penumbral privacy doctrine: the reasonable expectation of privacy.[62] Under his twofold adage, an individual has a reasonable expectation of privacy where: (1) the individual demonstrates a subjective expectation of privacy, and (2) where the expectation is objectively reasonable, i.e. "one that society is prepared to recognize" as such.[63] The courts have since embraced Justice Harlan's two-fold approach to assess

---

sample from a drunk driving suspect).

55. Boyd v. United States, 116 U.S. 616, 630 (1886) (holding that compelling a criminal defendant to produce incriminating documents constitutes a Fourth Amendment search).

56. *See* Scolnik, *supra* note 3, at 353 (citing an example from Illinois v. Caballes, 543 U.S. 405, 408-09 (2005) where a drug-detecting dog's sniff did not constitute a search).

57. *See id.*

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

59. *See* Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes As E-Mails Get Dusty*, 88 B.U.L. REV. 1043, 1047 (2008).

60. *See Katz*, 389 U.S. at 349.

61. *See id.* at 353.

62. *See id.* at 360 (Harlan, J., concurring).

63. *Id.* at 361.

the scope of Fourth Amendment protections.[64]

B. The Third Party Doctrine

While the Fourth Amendment may protect individuals from unreasonable searches of items he or she maintains as private, the Court somewhat undermined the initial promise of *Katz* when propounding subsequent doctrines.[65] The Court developed the third party doctrine, which functions as a coherent guideline in defining the reasonableness of an individual's expectation of privacy.[66]

Under the third party doctrine, an individual relinquishes his or her reasonable expectation of privacy when he or she knowingly reveals private information to another person, effectively assuming the risk that the other person will reveal the once-private information to the government.[67] If the third party willingly conveys that information to such authorities, the government may then use the once private material against the individual.[68]

Couch v. United States[69] demarcates the Court's first encounter with the third party doctrine jurisprudence. Couch argued that the Fourth Amendment protected documents that the IRS subpoenaed from her accountant.[70] The Court held that an individual could not assert a Fourth Amendment challenge to preclude the government from subpoenaing tax records in her accountant's possession.[71] Since an accountant necessarily reviews and hands over a client's documents when filing a tax return, Couch—by divesting such records to her accountant—relinquished her reasonable expectation of privacy in those documents.[72]

Expanding *Couch*, the Court in *United States v. Miller*[73] found that a bank customer retained no reasonable expectation of privacy in the financial documents he

64. *See* Scolnik, *supra* note 3, at 353.

65. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1577 (2004).

66. *See* Small, *supra* note 16, at 262.

67. *See* Oza, *supra* note 59, at 1047.

68. *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984).

69. Couch v. United States, 409 U.S. 322 (1973).

70. *See* Small, *supra* note 16, at 264.

71. *See Couch*, 409 U.S. at 336.

72. *See* Small, *supra* note 16, at 264.

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

"voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[74] Despite Miller's subjective expectation of privacy, an objective expectation could not exist with regard to the checks, deposit slips, and financial statements freely disclosed to the bank and its employees, as "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government."[75]

The Court then applied the third party doctrine to electronic communications in *Smith v. Maryland*.[76] Without a search warrant, the police installed a pen register at the company's central office as a surveillance technique to record numbers dialed from defendant Smith's line.[77] While Smith asserted a Fourth Amendment challenge to the search and seizure of the telephone number he dialed, the Court inferred that, because customers received itemized bills listing the long-distance calls they made, "telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[78]

Absent statutory guidance, the courts would be left to determine the breadth of the third party doctrine with respect to electronic communications through case law, which would invariably lead to inconsistencies.[79] The case law regarding the Fourth Amendment's application to Internet communications remains remarkably sparse and, unfortunately for users, the existing case law does little to safeguard their digital documents that are increasingly being stored on remote third-party servers.[80] As such, Congress, as opposed to the courts, has the appropriate faculties and institutional advantage to forage the complex technological landscape and accordingly develop a statutory scheme to which the courts will defer.[81]

---

74. *Id.*
75. *Id.* at 443.
76. Smith v. Maryland, 442 U.S. 735 (1979).
77. *See id.* at 742–43.
78. *Id.*
79. *See* Small, *supra* note 16, at 262.
80. *See* Soghoian, *supra* note 19, at 390.
81. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies:*

III. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

The Electronic Communications Privacy Act of 1986 ("ECPA") represents a Congressional endeavor to prevent the Fourth Amendment's third party doctrine from compromising the privacy interests of electronic communications stored by third parties.[82] The ECPA is one of the nation's premier digital privacy laws.[83] While the Fourth Amendment applies exclusively to government intrusions, Congress, recognizing that private parties pose a serious threat to Internet privacy, defined the scenarios in which an individual may reasonably maintain an expectation of privacy with regard to his or her electronic communications.[84]

In the mid-1980s, consensus was reached among members of Congress, the telecommunications industry, and the computing industry that the nation's developing technologies were significantly out of tune with their respective federal surveillance law and privacy safeguards.[85] The House Committee on the Judiciary and the Senate Committee on Governmental Affairs ascertained the urgency for updating legal protections for electronic communications.[86] Chairman of the Senate Judiciary Committee, Patrick Leahy, stated that the "[then-] existing law [was] 'hopelessly out of date.'"[87] An expert testifying at the House Committee hearing said it was "reasonable to assume that during the 1990's[,] electronic mail will become a regular and important part of the communications mix that a substantial number of Americans use."[88]

Reservations as to the ambiguity between privacy

Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 801, 838 (2004) [hereinafter Kerr, *Constitutional Myths*].

82. *See* Oza, *supra* note 59, at 1054.

83. *See* Gerber, *supra* note 26, at 257.

84. *See* Kerr, *Constitutional Myths*, *supra* note 81, at 872.

85. *See Hearing Before the Subcomm. on Patents, Copyrights, and Trademarks, Electronic Communication Privacy of the Senate Comm. on the Judiciary,* 99th Cong. 130–31 (1985) (prepared statement of Jerry J. Berman, on behalf of the American Civil Liberties Union ("ACLU")).

86. S. REP. 99-541, 2 (1986).

87. *Id.*

88. *See Hearing Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice,* 99th Cong. 20 (1985) (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association, accompanied by Michael F. Cavanagh, Executive Director, Electronic Mail Association).

protections and law enforcement access standards with respect to electronic communications prompted the committees to ask the Office of Technology Assessment to evaluate threats posed by unregulated intrusions into electronically transmitted communications.[89] The 1985 study determined that "legal protections for electronic mail [were] 'weak, ambiguous, or non-existent,' and that 'electronic mail remain[ed] legally as well as technically vulnerable to unauthorized surveillance.'"[90]

Congress amended the Omnibus Crime Control and Safe Streets Act of 1968[91] and consequently modernized the legislation, expanding its scope to a new category of electronic communications.[92] Through the Electronic Communications Privacy Act, Congress ultimately extended then-existing wire and oral communication protections to the new electronic communications.[93]

The ECPA consists of three federal statutes: (1) the Wiretap Act,[94] (2) the Stored Communications Act ("SCA"),[95] and (3) the Pen Register Statute.[96] The Fifth Circuit evaluated the interaction between the ECPA and the SCA as follows:

> Congress' use of the word 'transfer' in the definition of 'electronic communication,' and its omission in that definition of the phrase 'any electronic storage of such communication' (part of the definition of 'wire communication') reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'[97]

---

89. *See* S. REP., *supra* note 86, at 5.

90. *See id.* at 4.

91. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968). This statute represented the primary federal statute governing wire and oral communication interceptions. *See* Nguyen *supra* note 30, at 2215.

92. *See* Nicholas Matlach, *Who Let the Katz Out? How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles in Katz v. United States Will Fix It*, 18 COMMLAW CONSPECTUS 421, 442 (2010).

93. *See* S. REP., *supra* note 86, at 2, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

94. 18 U.S.C. §§ 2510–22.

95. 18 U.S.C. §§ 2701–10.

96. 18 U.S.C. §§ 3121–27.

97. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994).

This interplay evinced a standard: the ECPA governs a communication transitioning between the source and the destination, while the SCA governs the communication once it reaches its destination.[98] Accordingly, the Stored Communications Act is the principal legislation controlling online privacy rights, including e-mail and cloud computing.[99]

IV. THE STORED COMMUNICATIONS ACT

The way in which the Internet functions seemingly frustrates arguments for robust Fourth Amendment protection in remotely stored files under the current doctrine.[100] The 1986 *Senate ECPA Report* recognized that a communication "subject to control by a third party computer operator" might, similar to the bank records in *Miller*, "be subject to no constitutional privacy protection."[101] In conjunction with changes in communications technology and content-proliferation, Congress enacted new privacy measures through the SCA.[102] Congress acknowledged "[f]or the person or business whose records are involved, the privacy or proprietary interest in that information should not change" solely because the information is maintained and stored by a service provider as opposed to one's person or one's business premises.[103] By statutorily codifying end-users' privacy rights for their stored account information held by third party network service providers, the SCA addresses the inherent imbalances between the Fourth Amendment and the Internet's function.[104]

The SCA safeguards Fourth-Amendment privacy-like rights by supervising the interplay between service providers (who possess and maintain users' private information) and government investigators.[105] Chapter 121 of the United States Code is comprised of two principal sections: Section 2702 (voluntary disclosure of customer communications or

98. *See* Matlach, *supra* note 92, at 448.

99. *See* Derek Constantine, *Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, or Both?*, 28 GA. ST. U. L. REV. 499, 503 (2012).

100. *See* Kerr, *Lifting the Fog*, *supra* note 49, at 806.

101. *See* S. REP., *supra* note 86, at 3.

102. *See* Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 607 (2007).

103. *See* S. REP., *supra* note 86, at 3.

104. *See* Kerr, *SCA User's Guide*, *supra* note 4, at 1212.

105. *Id.*

records) and Section 2703 (compelled disclosure of customer communications or records).[106] For purposes of understanding relevant terminology, the discussion of Section 2703 will precede the Section 2702 discussion.

A. Section 2703: Compelled Governmental Access

This section intricately sets forth the circumstances whereby service providers must disclose customer communications and information to government entities. Section 2703 provides three mechanisms by which the government compels disclosure: (1) search warrant, (2) court order, or (3) subpoena.[107]

A search warrant requires the government to comply with the Fourth Amendment's probable cause requirement: given the totality of the circumstances, the government must establish, at a minimum, a fair probability that the defendant committed the crime.[108] The other procedural mechanisms by their very nature fall short of the Fourth Amendment safeguards.

The court order mandates that the government provide "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."[109] Use of a Section 2703(d) court order typically requires prior notice to the affected customer or subscriber.[110] This standard represents an intermediate level that is lower than the search warrant's probable cause but more exacting than the reasonable relevance standard required for subpoenas.[111]

The third and most lenient standard is for a subpoena issued upon a showing of "reasonable relevance."[112] Under this standard, the government need only show that the information it seeks bears reasonable relevance to a criminal

106. *See* 18 U.S.C. §§ 2701–03.

107. *See id.* § 2703(a)–(b).

108. *See* Kattan, *supra* note 7, at 630 (noting that the warrant does not require certainty).

109. 18 U.S.C. § 2703(d).

110. *Id.* § 2705.

111. *See* Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages*, 32 HASTINGS COMM. & ENT L.J. 365, 375 (2010).

112. *See* Kattan, supra note 7, at 631.

investigation.[113]

Under Section 2703, the point at which a governmental entity must obtain a search warrant supported by probable cause, or a less exacting form of process in order to compel disclosure of electronically stored communications, relies exclusively upon three distinctions: (1) content communication information and non-content communication information,[114] (2) Electronic Communications Service ("ECS") and Remote Computing Service ("RCS"),[115] and (3) communications stored with an ECS for 180 days or less and communications stored with an ECS for over 180 days.[116] These fundamental distinctions yield varying levels of protection for electronically stored information.[117]

1. The Content-Non-Content Dichotomy

Here, the rules are the same for both ECS and RCS providers.[118] Name and e-mail address of the recipient, for example, constitute non-content under the SCA.[119] A warrant is never required where the government compels access to non-content information.[120] Where the government seeks access to the "contents" of electronic communications—"information concerning the substance, purport, or meaning of that communication"—maintained in "electronic storage," however, the government may be required to obtain a search warrant consistent with its corresponding Fourth Amendment requirements.[121]

2. Electronic Storage

The ECPA defines electronic storage as "any temporary, intermediate storage of a wire or electronic communication

113. *Id.*
114. *See* 18 U.S.C. § 2703(a).
115. *See id.* § 2703(a)–(b).
116. *See id.* § 2703(c)(1).
117. *Id.* at 142.
118. *See* Kerr, *SCA User's Guide*, *supra* note 4, at 1219.
119. *See* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 142 (2011) (the ECPA defines content as any information that assists with routing or addressing of a communications, identifies the time of the communication, or conveys information about a subscriber other than the contents of the subscriber falls outside of the content category).
120. *See id.*
121. *See* 18 U.S.C. § 2510(8); *see also* 18 U.S.C. § 2510(17); *see generally* 18 U.S.C. § 2703; *see* Kennedy, *supra* note 119, at 141.

incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communications service for purposes of backup protection of such communication."[122]

While the ECPA provides a fairly straightforward definition of "electronic storage," it has been the subject of much debate in practice. The confusion exists between delivered and opened e-mails and those that remain in post-transmission storage on the provider's facilities. A federal judge found the ECPA did not protect e-mails where such e-mails remained stored after the recipient opened them.[123] They were in neither "temporary, immediate storage" nor "backup storage."[124] While the U.S. Department of Justice prefers this position, the Ninth Circuit took the opposite view and found e-mails protected by the ECPA, as post-transmission storage served as a backup function.[125]

3. The ECS-RCS Dichotomy

The SCA defines an ECS as "any service which provides users thereof the ability to send or receive wire or electronic communications."[126] The SCA defines RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system."[127] Where ECS-maintained communications must remain in "electronic storage" to receive any protections under the statute, RCS-maintained contents receive their corresponding protections where (1) it is held or maintained on its customer's behalf,[128] and where (2) the provider is authorized to access the communication's contents only to provide such storage or services.[129]

The ease with which the government can obtain an ECS

---

122. *Id.* § 2510(17).

123. *See* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635 (E.D. Pa. 2001).

124. *Id.*

125. Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2003).

126. 18 U.S.C. § 2510(15).

127. *Id.* § 2711(2) (defining "electronic communications system" as "any wire, radio, electromagnetic, photo-optical or photoelectric facilitates for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.").

128. *See id.* § 2703(b)(2)(A).

129. *See id.* § 2703(b)(2)(B).

maintained communication depends exclusively on its time in "electronic storage." While the SCA mandates that the government procure a search warrant for contents stored for 180 days or less, access to the same exact contents stored for over 180 days is less onerous as it may be obtained with the less exacting Section 2703(d) court order or subpoena.[130] The SCA provides limited procedural safeguards to ECS communications stored for over 180 days and all RCS contents alike.[131] Accordingly, the government may compel RCS providers to disclose contents by merely proffering a court order or subpoena.

B. Section 2702: Voluntary Disclosures

The Fourth Amendment neither limits the ability of private actors to voluntary disclose communications to the government, nor prevents service providers from releasing the contents of customer communications and information to other private parties.[132] While Congress enacted Section 2702 of the ECPA to remedy the Fourth Amendment's shortcoming and to provide guidance as to when disclosure of particular communications and records is permitted, it did so through a seemingly incoherent compilation of categories, definitions, rules, and exceptions.[133]

1. Non-Content Requests

Public providers may disclose non-content information, without restriction, to any person other than a governmental entity.[134] On the other hand, such content may only be disclosed to governmental entities where exceptions—such as service of process by the governmental entity—apply.[135] Non-public providers may voluntarily disclose non-content to any private or governmental entity, but may be required to

130. *See id.* § 2703(b)(1).

131. *See id.* § 2703(a)–(b).

132. *See* Kennedy, *supra* note 119, at 137; *see also* United States v. Katz, 389 U.S. 347, 351 (1967); and *see* United States v. Richardson, 607 F.3d 357, 364 (2010).

133. *See* 18 U.S.C. § 2702(b)(1)–(8).

134. *See id.* § 2703(c)(2) (Contents is defined in the ECPA: "[W]hen used with respect to any wire, oral, or electronic communication, [contents] include any information concerning the substance, purport, or meaning of that communication.").

135. *See id.* § 2702(c)(6); *see also* § 2703(c)(1).

produce such material upon service of process.[136]

2. Content Requests to a Public ECS Provider

ECS providers who offer services to the public may not divulge the contents of a communications to a private party unless the enumerated exceptions apply.[137] Even in the event of civil litigation with corresponding civil subpoenas demanding such contents, the Section 2702 exceptions would be inapplicable, requiring the service provider to maintain the customer contents as private.[138] Essentially, absent statutory exception or user consent, the provider must refuse the private party's request.

The circumstances differ where the government seeks production of customer communications and records. Voluntary disclosure to the government is not permitted; however, Section 2702 permits disclosure authorized by Section 2703.[139] Accordingly compliance with governmental request for disclosure is allowed where the government procures a search warrant, subpoena, or court order.[140]

3. Content Requests to a Non-Public ECS Provider

As Section 2702 omits statutory obligations with respect

---

136. *See id.* §§ 2702(c)(1), (4), (6), 2703(c)(1). *See also* Kennedy, *supra* note 119, at 140 ("A public ECS or RCS provider may disclose non-content customer information to any non–governmental entity. Disclosures of such information to governmental entities may be made only where an exception—such as consent of a party or subscriber or service of process by the governmental entity—applies . . . . A non–public ECS or RCS provider may disclose non–content customer information to any private or governmental entity but may be compelled to do so only upon service of process.").

137. *See id.* § 2702(b)–(c) (detailing the exceptions for communications and customer records, respectively: delivery to intended recipients of those communications and other lawful purposes "necessarily incident to the rendition of the services or to the protection of rights or property of the provider of that service," or "with the lawful consent of the originator or an addressee or intended recipient of such communication.").

138. *See id.* Kennedy, *supra,* note 119, at 139 n.57 ("neither subpart's exceptions covers subpoenas brought by nongovernmental litigants.").

139. *See id.* § 2702(b)–(c).

140. 18 U.S.C. §§ 2702(b)(2), 2703(a)–(d). *See also*, Kennedy, *supra* note 119, at 140 ("A public ECS or RCS provider may disclose the contents of a communication stored on its service to a governmental or non-governmental entity only where an exception—such as the consent of a party or subscriber or service of process by a governmental entity—applies . . . . A non–public ECS or RCS provider may voluntarily disclose the contents of a communication stored on its service to a private or governmental entity but may be *compelled* to do so only upon service of process.").

to private networks and other entities that do not hold themselves out to serve the public, such providers may freely disclose contents to a private third party, subject to contractual privacy assurances the provider has given its users.[141]

Since the non-public service provider is not subject to Section 2702, such providers are not required to adhere to Section 2703 when dealing with a governmental entity.[142] While it can freely disclose content to the government, the government cannot compel it to do so unless the government complies with disclosure mechanisms enumerated in Section 2703.[143]

V. ECPA AMENDMENTS ACT OF 2013

In September 2010, the Senate Committee on the Judiciary held its first hearing on ECPA reform, acknowledging that the ECPA represents legislation passed when most of today's technological pioneers were toddlers or young children.[144] On March 19, 2013, Senator Patrick Leahy introduced the Electronic Communications Amendments Act of 2013 ("2013 Amendments Act").[145] Accompanied by bipartisan support, the Senate Committee on the Judiciary unanimously voted the ECPA Amendments Act of 2013 to move onto the full Senate for a vote on April 25, 2013.[146]

The bill aims to amend several provisions of the ECPA.[147] Notably, the bill—as introduced—would generally prohibit both ECS and RCS providers from voluntarily disclosing its

---

141. *See id.* § 2702. *See* Kennedy, *supra* note 119, at 139.

142. *See id.* 18 U.S.C. § 2073(c). *See* Kennedy, *supra* note 119, at 139 ("non-public service provider[s] . . . [are] not required to apply the exception permitting disclosures that are authorized by 2703 when [they] deal with a governmental entity.").

143. *See id.* § 2703. Kennedy, *supra* note 119, at 139 ("[communications], whether held on a public or private service, enjoy the privacy interests recognized by section 2703 when it imposes constraints on governmental access.").

144. *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary,* 112th Cong. 1 (2011) (statement of Sen. Patrick J. Leahy).

145. Electronic Communications Privacy Amendments Act of 2013, S. 607, 113th Cong. (2013) (as reported by S. Comm. on the Judiciary, Apr. 25, 2013).

146. *Senate Judiciary Panel Votes to Require Warrants for Police E-mail Searches*, DIGITAL DUE PROCESS (Apr. 25, 2013), http://digitalddueprocess.org/index.cfm?objectid=7BAE62D0–B112–11E2–98D7000C296BA163.

147. S. 607 §§ 2, 3 (2013).

customers' electronic communications contents to governmental entities.[148] While it would still retain the ECS-RCS distinctions, it would adopt a uniform search warrant standard for production of customer electronic communications held in "electronic storage with or otherwise stored, held, or maintained by the provider."[149] The government must also promptly notify the customer whose content has been accessed via a third-party service provider, and consequently provide that user with a copy of the warrant and related information.[150] Finally, the bill would eliminate the rule that allows the government to obtain e-mails in electronic storage after 180 days.[151]

VI. LEGAL IMPLICATIONS OF CLOUD COMPUTING

In theory, ECPA serves as a useful government tool; however, in its current state it is "hampered by conflicting standards that cause confusion for law enforcement, the business community, and American consumers alike."[152] The Senate Judiciary Committee observed in 1986 that "[p]rivacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances."[153] While increasingly more American households have access to broadband Internet, and while nearly 70 percent of Americans utilize Internet webmail, store data online, or use online software programs, the SCA has been largely unmodified to reflect these shifts.[154] At the time Congress adopted the ECPA, there was no World Wide Web, and Mark Zuckerberg, who would grow to start Facebook, was merely

148. *Id.* § 3(a) ("A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains a warrant.")..

149. *Id.* § 3(a).

150. *Statement Of Senator Patrick Leahy on Committee Consideration Of The Electronic Communications Privacy Act Amendments Act of 2013,* DIGITAL DUE PROCESS (Apr. 25, 2013), http://digitaldueprocess.org/index.cfm?objectid=8808E3B0-ADC6-11E2-98D7000C296BA163.

151. *See* S. 607 § 3 (2013).

152. *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 2 (2011) (statement of Sen. Patrick J. Leahy).

153. S. REP., *supra* note 86, at 5.

154. *See* Scolnik, *supra* note 3, at 378.

two years old.[155] Now, the law regulating Facebook is almost as old its founder.[156]

Notable legal implications emanate from the SCA's narrow scope. Section 2703 provides the government with the unique occasion to circumvent long established privacy rights. It does not function as a catch-all statute that safeguards all stored Internet communications; rather, it is narrowly tailored to provide a set of Fourth Amendment-like protections to a very specific class of Internet communications.[157] The ECS-RCS distinction does not capture all providers; as such, many cloud computing services either fluctuate between an ECS and RCS status or completely fall outside the SCA's purview.[158] Classifying cloud services as ECS, RCS, or neither impacts what rights the user has with respect to his or her data. Unfortunately for cloud users who fall outside the SCA's narrow scope, the courts' jurisprudence on the Fourth Amendment governs the privacy of their communications, and the existing case law under the third party doctrine does little to protect papers and documents increasingly stored in the cloud.[159]

While the 1986 ECPA stands as one of our nation's premiere privacy laws, it is painfully outdated.[160] In the years since the ECPA's enactment, technology has seen a dramatic, and arguably disruptive development as far as services available to electronic communications users.[161] As technology has fundamentally changed the way we store and use information since 1986, the existing ECPA represents a very apparent disconnect between privacy expectations and statutory protections.[162] There is no comprehensive federal legislation that sets statutory minimum requirements safeguarding users' privacy and personal data in the cloud.[163] As such, the cloud threatens to undermine and delegitimize

155. Gerber, *supra* note 26, at 256.
156. *Id.*
157. *See* Kerr, *SCA User's Guide*, *supra* note 4, at 1214.
158. *See* William J. Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1209 (2010).
159. *See* Soghoian, *supra* note 19, at 390.
160. *See* Gerber, *supra* note 26, at 257.
161. *See* Kennedy, *supra* note 119, at 145.
162. *See* Mulligan, *supra* note 65, at 1572.
163. Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 443 (2013).

the regulatory approaches to information privacy in the United States.[164]

This disconnect spawned an uproar among various organizations, congressmen, companies, and Americans alike. The ECPA Amendments Act of 2013 is certainly well-received by the 1986 ECPA-critics; however, similar issues arising under the 1986 ECPA may likely manifest themselves in the 2013 Amendments Act, should Congress enact the proposed bill. To varying extents, both the ECPA and the 2013 Amendment Act reflect the pre-Internet computing landscape seen by the 1980s.[165] As the ways we communicate in the cloud computing arena place a tremendous strain on the 1986 statutory dichotomies, the proposed amendments, while a considerable improvement from their predecessor, will continue to stifle cloud computing's ability to achieve its future promise.

VII. CLOUD COMPUTING UNDER THE 1986 ECPA & THE ECPA AMENDMENTS ACT OF 2013

As the past twenty-eight years since the ECPA's enactment have seen numerous dramatic and statutorily disruptive developments in technology and electronic communications,[166] this analysis will proceed by discussing the predominant flaws under the existing 1986 ECPA framework in the cloud computing arena, and then assess whether the ECPA Amendments Act of 2013 has the ability to remedy its predecessor's shortcoming.

This analysis will discuss four issues with respect to cloud computing, the existing legal framework, and the potential framework in light of the proposed amendments: (A) the definition of electronic storage, (B) the ECS-RCS distinction, (C) the corresponding 180-day rule for ECS communications, and (D) a doctrinal approach to the cloud under the Fourth Amendment.

A. The Uncertain "Electronic Storage" Definition

The SCA complicates the already muddled boundary of cloud-storage searches.[167] The SCA protects the

164. *See* Schwartz, *supra* note 18, at 1646.
165. *See* Scolnik, *supra* note 3.
166. *See* Kennedy, *supra* note 119, at 145.
167. *See* Mark Wilson, *Castle in the Cloud: Modernizing Constitutional*

communication provided the ECS provider maintains the communication in "electronic storage."[168]

The Department of Justice approach to "electronic storage" recognizes limited protection for electronic communications accessed by its recipient, not maintained in "electronic storage" by an ECS.[169] Conversely, in finding that e-mails were "stored" by an ECS service within the meaning of the SCA, the Ninth Circuit determined that the second clause of the "electronic storage" definition applied to data only where it is stored for backup purposes.[170] In dicta, the Ninth Circuit left open the inquiry as to whether "[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."[171]

By leaving this inquiry open, the Ninth Circuit essentially described the cloud-computing quandary: individuals use the cloud for numerous purposes, including, but not limited to, backing up information.[172] Under this interpretation, such use of cloud services falls outside the purview of the SCA, as the data was not stored *exclusively* for "backup purposes."[173] Files stored on Google Docs and the like illustrate this dilemma. Files stored on these servers are not necessarily stored for "backup purposes" and therefore are not in "electronic storage," since the contents are "constantly updated as the software, installed on a user's computer or smart phone, monitors the local file for changes and updates the server's copy as necessary."[174]

As the Senate Judiciary Committee left this portion of the SCA untouched, the varying approaches to the "electronic storage" provision with respect to cloud computing necessarily mean that communications sent and maintained

---

Protections for Cloud-Stored Data on Mobile Devices, 43 GOLDEN GATE U. L. REV. 261, 276 (2013).

168. *See* 18 U.S.C. § 2701(a)(2).

169. *See* Kattan, *supra* note 7, at 636 & n.155.

170. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (2003) (reasoning the intent to store data for such purposes must be the *motivating* purpose for storage and not merely another possible reason for storage; therefore, the mere possibility that a copy could serve as a backup does not constitute electronic storage under the SCA).

171. *Id.* at 1077.

172. *See* Wilson, *supra* note 167, at 278.

173. *Id.* (footnote omitted).

174. *Id.* (footnote omitted).

in the cloud will vary and drift outside the statutory purview of ECS-provider protection.[175]

B. The ECS-RCS Distinction

A cloud user's constitutionally mandated privacy is predicated on the characterization of the cloud service provider and the particular content stored in that cloud under the ECPA's complicated ECS-RCS analytical framework, which no longer bears any technological significance today.[176] This distinction becomes increasingly problematic where cloud services cannot be characterized as ECS or RCS, since contents of electronic communications falling outside these technical definitions "can [be] disclose[d] or use[d] with impunity."[177]

The justification proffered by Congress in drawing 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."[178]

The inconsistent burdens of proof imposed on the government with respect to electronic communications—particularly RCS—made sense when memory was scarce.[179] Service providers could assume that intended e-mail recipients effectively abandoned his or her e-mails after 180 days.[180] Likewise, the ECPA's disparate treatment for information stored on businesses' own computers—as opposed to a remote vendor—did not carry with it such dramatic implications as it does today.[181] Congress' justification is now inaccurate given the way in which Internet communication systems function.[182]

The extent to which communications sent through cloud-

---

175. *See* Kattan, *supra* note 7, at 636.

176. *Id.* at 655; *see e.g.*, n.312 (citing 18 U.S.C. § 2703(a) which requires a search warrant to compel ECS providers to disclose communications in "electronic storage" for 180 days or less and describes the tripartite standard that applies to compel RCS providers).

177. *See* Wesley Coll. v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997) (citing 18 U.S.C. § 2702(a).

178. *See* Nguyen, *supra* note 30, at 2205 (footnote omitted).

179. *See* Kennedy, *supra* note 119, at 145–46 (footnote omitted).

180. *See* Kerr, *SCA User's Guide*, *supra* note 4, at 1234.

181. *See* Julie J. McMurry, *Privacy in the Information Age: The Need for Clarity in the ECPA*, 78 WASH. U. L.Q. 597, 617 (2000).

182. *See* Nguyen, *supra* note 30, at 2205 (footnote omitted).

based servers receive search warrant protection remains unclear as various cloud-based system-services present increasingly difficult cases. As these cloud computing services tend to fall short of the SCA's twin requirements for ECS communications, they do not enjoy the heightened protections afforded to ECS communications.[183] Where ECS-qualifying services must provide users with "the ability to send or receive . . . electronic communications," many of today's cloud services are programmed for purposes other than communication and lack any sending or receiving functionality.[184] Moreover, as "electronic storage" is a term of art, cloud services fail to satisfy its narrow definition.[185] Contrary to the SCA's requirement that the electronic storage exist as temporary and incidental to service, numerous cloud services offer users considerable storage capacity to facilitate long-term data retention.[186] Furthermore, many cloud providers offer their storage service together with applications designed to access and deploy that data through remote computers.[187] As cloud users' content, with the very narrow exceptional e-mail category, is stored inconsistent with the twin ECS provider and "electronic storage requirements," the heightened ECS protections are poorly suited for the cloud.[188]

The existing RCS definition leaves its scope somewhat unclear.[189] The SCA defines RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system."[190] While computer storage is a relatively clear concept today, the question as to what constitutes a "processing service" posits a more trivial question especially with the invention of the World Wide Web.[191] The legislative history indicates that such services

183. *See* Robison, *supra* note 158, at 1209 (quoting 18 U.S.C. § 2510(15)).
184. *See id.*
185. *See id.*
186. *See, e.g.*, Gmail Help: Archiving Mail, http://https://support.google.com/mail/answer/6576?hl=en (last visited Oct. 12, 2013) (noting that Gmail's archive function "removes messages from your inbox . . . but keeps them in your account so that you can always find them later.").
187. *See, e.g.*, Google Docs, https://www.google.com/docs/about/ (last visited Feb. 10, 2015) (discussing its multiple applications for creating and editing docs, presentations, and spreadsheets).
188. *See* Robison, *supra* note 158, at 1209–10.
189. *See* Kerr, *SCA User's Guide*, *supra* note 4, at 1229.
190. 18 U.S.C. § 2711(2) (2012).
191. *See* Kerr, *SCA User's Guide*, *supra* note 4, at 1229–30.

refer to outsourcing functions.[192] To the extent computer networks existed in 1986, they predominately operated over proprietary facilities, not over systems controlled by third-party vendors.[193] Remote data processing did not yet exist as a means by which electronic communication and information was exchanged; rather, it was a method by which multiple users shared mainframe computers.[194]

While the ECS characterization almost entirely excludes cloud services from its protection, a quick glance at the SCA's RCS requirements leaves cloud users with false hope by initially availing their respective cloud provider to an RCS-qualifying status.[195] Most cloud providers offer—as the qualifying RCS providers must—public computer storage or processing services over a network. Relying on the seemingly short analysis, some courts have applied the RCS provisions to cloud computing services, ostensibly consistent with legal scholars' opinions and the SCA's legislative history.

While on its face, cloud computing satisfies the RCS requirements, the analysis used to reach this conclusion is inherently flawed: it neglects to account for the remaining requirements.[196] There are five remaining prerequisites that must be satisfied to qualify as an RCS provider.[197] It is commonplace for many cloud providers to adopt models that disregard the final two requirements, precluding an RCS qualification.

Consider the fairly recent social networking phenomenon. How should the site fall within the narrow SCA classifications where it stores and processes profile information (RCS-like), yet where it also permits communication among users (ECS-like)?[198]

---

192. *See id.*

193. *See* Kennedy, *supra* note 119, at 145.

194. *See* Mulligan, *supra* note 65, at 1560–61.

195. *See* Robison, *supra* note 158, at 1211.

196. *See* 18 U.S.C. § 2703(b) (2012).

197. *See id.* While the cloud services ordinarily satisfy the requirements that the data (1) contain "content," (2) be "carried or maintained . . . on behalf of . . . a subscriber or customer," and (3) have been electronically transmitted to the provider, the SCA also mandates (4) that the customer-data be transmitted to the cloud provider "solely for the purpose of providing storage or computer processing services," but that the cloud provider (5) "not [be] authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."

198. *See* Kattan, *supra* note 7, at 637–40 (discussing the narrow ECS-RCS application to Gmail).

Also consider how cloud services are profitable if they provide their services free of charge. These providers often rely on some advertising revenue to fund their operations. While advertising does not violate the SCA's requirements per se, numerous cloud providers provide targeted advertising opportunities where advertisers utilize targeted marketing campaigns that reach specific audiences by accessing the user's website-visits. This business model necessarily requires access to content, in contravention with the SCA's "solely for the purposes of storage" mandate.[199] Where customers authorize access to their data for such advertising services in exchange for free access to the cloud services, the SCA will not apply and the data will be subject to disclosure.[200]

The implications of such classifications are sweeping, as RCS contents are never protected by a probable-cause standard.[201] While the SCA fails to recognize this dichotomy, proprietary and confidential records stored within an RCS can be as sensitive and valuable as e-mails stored with an ECS.[202] These distinctions neither conform to the reasonable expectation of Americans nor serve the public interest.

While the Senate committee's bill eliminates the tiered standards for ECS and RCS communications, it does not entirely remove the ECS-RCS terminology. This can prove fatal because the approach still relies on definitions of obsolete technology where these distinctions no longer matter.[203] Even under the proposed legislation, some cloud services can slip through the cracks and escape the ECPA's protections in general.

C. The ECS 180-Day Distinction

Cloud computing platforms allow users to store e-mails on providers' servers for increasing periods of time and sometimes indefinitely.[204] In 2004, for example, Gmail provided users with one gigabyte of free storage.[205] Now, almost a decade later, Gmail users enjoy fifteen gigabytes of

199. *See* Robison, *supra* note 158, at 1213.
200. *Id.*
201. *See* 18 U.S.C. § 2703(b).
202. *See* Kennedy, *supra* note 119, at 151.
203. *See* Cheng, *supra* note 39, at 495.
204. *See* Scolnik, *supra* note 3, at 378.
205. *See id.*

free storage.[206] In spite of the seemingly infinite amount of free storage, the existing standard is still wedged in the crevices of 1986 technology. In setting forth two varying levels of protection for e-mails on third party servers, existing users essentially surrender their reasonable expectation of privacy—and consequently their Fourth Amendment protection—between day 179 and 181.[207] Where e-mails are stored on servers for 180 days or less, the government must fully comply with the Fourth Amendment by providing a search warrant supported by probable cause. On the other hand, the government need only meet a Section 2703(d) standard—specific articulable facts—or a subpoena standard—reasonable relevance—to access e-mails stored on the server for over 180 days.[208]

While the existing law circumvents the Fourth Amendment in the 48-hour period between day 179 and 181, the technological circumstances have not always been as such. The rationale for these distinctions are based in large part on 1986-era technology and the expectations those limitations created.[209] When Congress enacted the ECPA in 1986, e-mail service providers could not maintain customers' e-mails on their servers for extended periods of time, as the storage capacity was significantly limited.[210] "Most—if not all—electronic communication systems (such as electronic mail systems), however, only ke[pt] copies of messages for a few months."[211] Beyond that point, storage bore more resemblance to business records maintained by a third party.[212]

As the ECPA's drafters gave customers a weak and arguably nonexistent expectation of privacy in the contents of their message, they likely assumed that any e-mails stored for over 180 days had never been retrieved.[213] In 1986, ISPs stored user e-mails to the extent it was deemed necessary, i.e., until the user logged in and downloaded their mail.[214]

---

206. *See id.* at 378.
207. *See* Oza, *supra* note 59, at 1057.
208. *See* Kennedy, *supra* note 119, at 143.
209. *See id.*
210. *See* Oza, *supra* note 59, at 1072.
211. H.R. REP. NO. 99-647, at 68 (1986).
212. *Id.*
213. *See* Kennedy, *supra* note 119, at 143.
214. *See ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the*

The reality of this statutory scheme is that customers who store their e-mails on their computer indefinitely are protected by a warrant requirement, yet users who access their e-mails in the cloud may not receive such protections, depending on the contents' time in storage.[215] It is also ironic that:

> [T]he e-mails or private messages that are both the most important and the most private are the older messages that you have read through several times and have intentionally decided to save . . . . By contrast, the unopened e-mails in your inbox are likely to be commercial solicitations that you have not yet had time to delete."[216]

This irony demonstrates that the SCA, as applied to e-mail, is unconstitutional. The judiciary has been sluggish in recognizing Fourth Amendment protections for electronic information that would otherwise receive constitutional protection but-for its electronic character.[217] *United States v. Ferguson*[218] properly applied Section 2703 and Section 2705 while concurrently undermining traditional Fourth Amendment protections. During an investigation in *Ferguson*, the government discovered that Ferguson maintained accounts with both Yahoo! Mail and MSN Hotmail and successfully submitted a request to a magistrate to compel both services to produce all e-mails maintained in their storage for over 180 days.[219] Given the ECPA's 180-day requirement, e-mails held in storage for over 180 days were turned over without a warrant.[220] Had Ferguson used a desktop application such as Microsoft Outlook with POP settings, they would have been unreachable by the ECPA and would not have been turned over to the government without a search warrant.[221]

Comm. on the Judiciary H.R., 111th Cong. 2 (2010) [hereinafter *ECPA Reform and the Revolution in Cloud Computing*] (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation).

215. *See* Kennedy, *supra* note 119, at 143–44.

216. *ECPA Reform and the Revolution in Cloud Computing*, *supra* note 214, at 123 (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP).

217. *See* Wilson, *supra* note 167, at 273.

218. United States v. Ferguson, 508 F. Supp. 2d 7 (D.D.C. 2007).

219. *Id.* at 8.

220. *See* Oza, *supra* note 59, at 1061.

221. *See Ferguson*, 508 F. Supp. 2d at 8.

Recently in *United States v. Warshak*,[222] the Sixth Circuit recognized a Fourth Amendment right for e-mails stored within an ISP. There, the United States procured 27,000 of Warshak's e-mails utilizing an administrative subpoena pursuant to the SCA that ultimately led to Warshak's mail and bank fraud convictions.[223] The Sixth Circuit found that while Warshak had privacy protections under the Fourth Amendment, the government's reliance on the SCA precluded reversing Warshak's conviction.[224] Nevertheless, the court held "to the extent that the SCA purports to permit the government to obtain such e-mails warrantlessly, the SCA is unconstitutional."[225]

Together, *Ferguson* and *Warshak* represent the very disconnect between the ECPA and modern technology. The balance struck by Congress in 1986 falls severely out of alignment in light of the advent of cloud computing and increased online storage capacities. This distinction merely puts an increasing amount of user data within law enforcement's reach, requiring lower, and arguably unconstitutional, burdens of proof.[226] Federal statutory protection for e-mails should not depend on how the users choose to store their e-mail.[227]

Acknowledging that distinguishing privacy protections based on a stored-content's age bears no logic in light of today's cloud computing capabilities, the Senate Judiciary Committee struck the 180-day requirement in the ECPA Amendments Act of 2013.[228] Under the proposed bill, users who opt to leave their e-mails in the cloud do not suffer a decrease in privacy protections.[229] This legislation would not discriminate against those utilizing the cloud paradigm; as such, users' data would remain confidential and could only be accessed with due process of law.[230]

---

222. United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010).
223. *Id.* at 282.
224. *Id.* at 274.
225. *Id.* at 288.
226. *See* ECPA Reform and the Revolution in Cloud Computing, *supra* note 214, at 25.
227. *See id.* at 120.
228. *See* Electronic Communications Privacy Amendments Act of 2013, S. 607, 113th Cong. §§ 2–3 (2013).
229. *See* ECPA Reform and the Revolution in Cloud Computing, *supra* note 214, at 29.
230. *Id.* at 40.

D. The Fourth Amendment Application to the Cloud

Applying the Fourth Amendment to any cloud service proliferates confusion. *Smith*, *Miller*, and *Couch* establish that the third party doctrine precludes some legitimate privacy expectation where the third party is a business.[231] The implications that arise from the Fourth Amendment's caveat is that where a user transmits electronic communications over a third party's server, the government may approach the third party to produce documents, all while remaining consistent with the Fourth Amendment's reasonable expectation of privacy.[232]

Notwithstanding the third party doctrine, several recent decisions involving the Fourth Amendment protection in the cloud arena manifest the lower courts' willingness to extend Fourth Amendment protection to the cloud.[233] In *Quon v. Arch Wireless Operating Co.*, the court emphasized the importance of an employee's reasonable expectation of privacy with respect to the item seized or the area searched.[234]

Although the United States Supreme Court reversed—leaving unaddressed the reasonable expectation of privacy issue—the lower courts seemingly demonstrate their deference for the increasing importance of online environments by applying the Fourth Amendment to the individual, irrespective of the situation.[235] Moreover, the current Fourth Amendment framework does not necessarily preclude the courts from continuing to apply this methodology to the cloud. *Miller* and *Smith* do not control the cloud issue specifically. Storing one's data on a third-party server is not analogous to conducting business with a bank, and an IP address is not comparable to a telephone number.[236]

---

231. *See* Small, *supra* note 16, at 269.

232. *See* Constantine, *supra* note 99, at 513–16.

233. *See* Quon v. Arch Wireless 529 F.3d 892, 910 (2010) (finding that employees maintain a reasonable expectation of privacy with their text messages); *see also* State v. Bellar, 217 P.3d 1094, 1107 (Or. Ct. App. 2009) ("[D]efendant did not relinquish his privacy interest in the data stored on his computer's hard drive and that privacy interest continued after the data was transferred.").

234. *See Quon*, 529 F.3d at 904. The United States Supreme Court reversed but neglected to address the reasonable expectation of privacy issue.

235. *See* Katz v. United States, 389 U.S. 347, 351 (1976).

236. *See* R. Bruce Wells, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, 12 U. PA. J. CONST. L. 223, 237 (2009).

Despite this emerging judicial pattern, the courts should not be expected to traverse the intricate technological landscapes. Given that Congress has the benefit of overwhelming industry input, statutory guidance will yield more accurate and exacting standards. Accordingly, the initial reform in the cloud-computing arena must originate in the legislature.

VIII. CLEARING THE AIR: HOW TO MAKE WAY FOR THE CLOUD

While the Senate Judiciary Committee passed the ECPA Amendments Act of 2013 with overwhelming accord, there is no guarantee that Congress will enact the legislation, considering they failed to pass similar amendments in 2011.[237] The ECPA Amendments Act of 2013 is certainly a step in the right direction; however, as the aforementioned analysis indicates, it does not offer adequate remedies for the existing cloud-privacy concerns.

Limiting the Fourth Amendment's application to the online environment and narrowly construing the SCA language would severely constrict the benefits offered by cloud computing and undermine individuals' and companies' trust in the technology.[238] One of the primary advantages that the United States would gain in adopting new cloud-computing laws would be a coherent legal framework that replaces the archaic and fragmented statutory schemes that currently govern.[239] The ECPA should undergo a comprehensive amendment process that provides fluid emerging technologies the same protections as their existing equivalents. In doing so, however, Congress must achieve a balance between protecting user-privacy rights and avoiding unduly cumbersome provisions that restrict the free flow of data that is the essence of cloud computing.[240] An effective solution must underscore using and strengthening the existing legal frameworks under both the Fourth Amendment and the ECPA, as well as using these foundations to oversee the doctrines' application to the cloud paradigm and emerging

237. *See* Kennedy, *supra* note 119, at 156.
238. *See* Constantine, *supra* note 99, at 524.
239. *See* Gerber, *supra* note 26, at 275.
240. *See id.* at 273.

technologies.[241]

While industry leaders overwhelmingly advocate for reform that includes increased privacy, law critics favor private sector accommodations over legislative approaches.[242] Such critics argue that proposed privacy regulations interfere with the private relationship between ISPs and their customers, disrupt the free-market for electronic communications service, and reason that "protecting privacy imposes real costs."[243] Although critics express their discomfort with government interference in the consumer-industry relationship, this arguably narrow view neglects to address the significant costs imposed by the cloud's weak privacy protections. The cloud's appeal is its innovative technology and overwhelming flexibility.[244] Inadequate privacy protection, particularly in the cloud's early stage, will not only moot its flexibility, but will also impede innovation. Excessive government accessibility to the cloud is imprudent, as consumer and industry trust in cloud computing cannot be undermined.[245] Addressing the current shortcomings of cloud privacy legislation necessarily requires entrusting the entities with the appropriate faculties to remedy the statutory deficiencies.[246]

As the ECPA Amendments Act of 2013 and the analysis above indicate, the 180-day ECS distinction and the lowered protection for RCS communications serve no legitimate purpose. The 180-day distinction and corresponding tiered standards for ECS communications essentially eviscerate one of the cloud's premiere advantages: increased capacity.[247] Similarly, the lowered protection afforded to RCS communications is arguably unconstitutional.

In conjunction with removing the 180-day rule and tiered privacy standards for different communications, Congress should also eliminate the SCA's ECS-RCS distinction and

---

241. *See* Carol M. Celestine, "*Cloudy" Skies, Bright Futures? In Defense of A Private Regulatory Scheme for Policing Cloud Computing*, U. ILL. J.L. TECH. & POL'Y, SPRING 2013, at 141, 158.

242. *See* Katherine A. Oyama, *E-Mail Privacy After United States v. Councilman: Legislative Options for Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 525 (2006).

243. Fred H. Cate, PRIVACY IN THE INFORMATION AGE 102 (1997).

244. *See* Celestine, *supra* note 241, at 158.

245. *See* King & Raja, *supra* note 163, at 470.

246. *See* Celestine, *supra* note 241, at 159–60, 164.

247. *See* Kattan, *supra* note 7, at 642.

provide a unified technology and transmission neutral definition. "Tech neutrality" is a concept where, regardless of future developments in communication technology, the presence and application of the ECPA remain constant.[248] This type of approach would provide equitable protection to current and future technology alike.[249] A "tech neutral" definition in place of the ECS-RCS terminology should read to apply for all content, transmitted under any Internet medium, whether stored or otherwise maintained for any length of time.[250] Under this framework, user data stored and processed in the cloud would receive the same level of protection regardless of the platform or business model used to generate, communicate, or store the data.[251]

A. Proposed Amendment for Definitions Under the SCA

The proposed amendments for definitions would involve eliminating electronic communication service and remote computing serviced definitions and replacing them with a unified definition under the term "Internet Communication Service." The amendment would also revise the definition of "electronic storage." The amendments would read as follows:

§ 2510(15) Internet Communication Service

(A) any service which provides users, customers, or subscribers with ability to send, receive, store, or otherwise maintain wire or electronic communications.

§ 2510(17) "Electronic Storage"

(A) any wire or electronic communication that is stored electronically or otherwise held, stored, or maintained by the Internet Communication Service for any purpose of such communication.

B. Proposed Amendment for Disclosures Under the SCA

The proposed amendments for the voluntary and compelled disclosures incorporate the above amended terminology, abolish the 180-day distinction, and require a search warrant supported by probable cause for all content.

---

248. *See* Kerr, *Fourth Amendment to the Internet*, *supra* note 9, at 1016.

249. *See* Cheng, *supra* note 39, at 504.

250. *See* Christopher R. Brennan, *Katz Cradle: Holding on to Fourth Amendment Parity in an Age of Evolving Electronic Communication*, 53 WM. & MARY L. REV. 1797, 1822 (2012).

251. *See ECPA Reform and the Revolution in Cloud Computing*, *supra* note 214, at 41.

The amendments would read as follows:

§ 2702: Voluntary Disclosure

(a) Prohibitions. Except as provided in subsection (b) or (c),

(1) an Internet Communication Service or its agent shall not knowingly divulge to any person or entity either the contents or records of that communication information pertaining to a user, customer of or subscriber to such service.

§ 2703: Compelled Disclosure

(a) Contents of an Internet Communication Service in electronic storage. A governmental entity may require disclosure by a provider of Internet Communication Service of the contents of a wire or electronic communication in its electronic storage only if the governmental entity obtains a warrant issued according to the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction directing the disclosure.

CONCLUSION: BLUE SKIES AHEAD

While the ECPA is nearly thirty years old, it functioned as a progressive and enlightening statutory framework in the years immediately following its enactment.[252] This past decade's dramatic technological innovations have wreaked havoc through the ECPA to the extent that it is inflexible and no longer sustainable. Congress must promote innovation in the cloud arena, and the only way to accomplish that objective is to accommodate the past decade's technological leaps. The law should be concerned exclusively with personal data, regardless of user-choice as to storage or other data maintenance.[253]

It is crucial that Congress develop a clear understanding with respect to the existing murky categories and distinctions. In doing so, Congress should conform to user-and-industry-reasonable expectations of privacy. In effect, the above-amended statutes would not provide cloud users preferential treatment; rather, it would provide equal process under the law.[254] These proposed revisions do not foreclose

252. *See* Kennedy, *supra* note 119, at 161.

253. *See* Schwartz, *supra* note 18, at 1654.

254. *See ECPA Reform and the Revolution in Cloud Computing*, *supra* note 214, at 110.

flexibility from its framework. It fosters the ability to innovate, protects consumer interests, and at the same time equips law enforcement personnel with coherent standards necessary to carry out their legitimate needs in the new technological era.

By making the ECPA "tech neutral," Congress can send a message to individuals, companies, and global governments that they can safely use current cloud platforms and future platforms without compromising their users' data privacy.