Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act

WILLIAM JEREMY ROBISON*

TABLE OF CONTENTS

INTRODUCTION .......................................... 1196

I. CLOUD COMPUTING: AN EMERGING DEFINITION ................. 1197
   A. A BRIEF HISTORY OF COMPUTER NETWORKING ............... 1197
   B. THE ERA OF CLOUD COMPUTING ........................ 1199

II. ORIGINS AND OPERATION OF THE STORED COMMUNICATIONS ACT ... 1204
   A. ELECTRONIC COMMUNICATION SERVICES .................. 1205
   B. REMOTE COMPUTING SERVICES ........................ 1206
   C. PRIVACY PROTECTIONS .............................. 1207

III. CLOUD COMPUTING AS AN ELECTRONIC COMMUNICATION SERVICE ... 1209

IV. CLOUD COMPUTING AS A REMOTE COMPUTING SERVICE .......... 1212
   A. APPLICATION OF THE STATUTORY LANGUAGE ............... 1212
   B. AN EXAMINATION OF EXISTING CLOUD PROVIDERS .......... 1214
   C. EXISTING JUDICIAL PRECEDENTS ........................ 1218
   D. INTERPRETING TERMS OF SERVICE AGREEMENTS ............. 1220
   E. IMPLICATIONS FOR CLOUD COMPUTING USERS .............. 1222

V. CAN THIS BE WHAT CONGRESS INTENDED? .................. 1223
   A. COMPETITION AND FREE MARKET DETERMINATIONS ........... 1224
   B. CODIFYING THE FOURTH AMENDMENT .................... 1226

VI. WILL CLOUD COMPUTING BE A TIPPING POINT FOR ONLINE PRIVACY? .............................. 1232

* Georgetown Law, J.D. expected 2010; University of California, San Diego, B.A. 1999. © 2010, William Jeremy Robison. I would like to thank Professors Elizabeth Banker, Marc Zwillinger, and Michael Songer for their assistance with early drafts of this Note. I am also indebted to Andrew March, Erin Langley, and the staff of The Georgetown Law Journal for their insightful feedback.

1195
INTRODUCTION

Scott McNealy, the Chairman and former CEO of Sun Microsystems, caused an uproar in 1999 when he dismissed online privacy concerns and proclaimed, “You have zero privacy anyway. Get over it.”1 Was he right? Within the realm of cloud computing, he may have been uncomfortably close to the truth. The Stored Communications Act (SCA),2 a component of the broader Electronic Communications Privacy Act (ECPA),3 is the primary federal source of online privacy protections, but it is more than twenty years old. Despite the rapid evolution of computer and networking technology since the SCA’s adoption, its language has remained surprisingly static. The resulting task of adapting the Act’s language to modern technology has fallen largely upon the courts. In coming years, however, the courts will face their most difficult task yet in determining how cloud computing fits within the SCA’s complex framework.

This Note ultimately concludes that the advertising supported business model embraced by many cloud computing providers will not qualify for the SCA’s privacy protections. In exchange for “free” cloud computing services, customers are authorizing service providers to access their data to tailor contextual and targeted advertising. This quid pro quo violates the SCA’s requirements and many customers will find that their expectations of privacy were illusory. Consequently, a cloud provider’s terms of service agreement may be the only privacy protections applicable to its customers.

Subsequently, this Note explores whether the lack of privacy protections for cloud computing is consistent with Congress’s intent in adopting the SCA and whether it will be a catalyst for expanding privacy measures in the future. In response, Part V explores the SCA’s legislative history and argues that the modern form of cloud computing is incompatible with the concerns and Fourth Amendment principles that motivated Congress’s adoption of the Act. Part VI further examines potential judicial, legislative, and societal forces that could prompt revisions to the SCA, but concludes that the lack of privacy protections

---

in cloud computing is unlikely to be addressed anytime soon.

I. CLOUD COMPUTING: AN EMERGING DEFINITION

A. A BRIEF HISTORY OF COMPUTER NETWORKING

The law cannot keep up with the pace of change in computer networking. By the time legislatures or courts figure out how to deal with a new product or service, the technology has already progressed. It is, therefore, useful to learn the state of technology at the time Congress enacted a law or the Judiciary issued a legal opinion to clarify the logic and principles that girded its decision. This is particularly true of the Stored Communications Act, which Congress structured around on the state of technology in 1986. To understand the Act, and recent innovations to which it might apply, a quick tour of some computer history is necessary.

Early computer technology was prohibitively expensive for all but the largest businesses and organizations. In 1965, IBM offered to rent its early mainframe computers for $50,000–$80,000 per month because few customers could afford their $2.2 million–$3.5 million price tag.4 By 1970, the rental cost of increasingly sophisticated IBM mainframes grew to $190,000–$270,000 per month and the purchase price exceeded $12 million.5 The few entities that could afford a mainframe, including the Department of Defense, the Internal Revenue Service (IRS), and the National Aeronautics and Space Administration (NASA), shared its processing power and data storage with the entire organization.6 The mainframe was a centralized resource that employees could access through lab-coat wearing specialists in their IT department or by using a “dumb” computer terminal that existed only as a gateway to the mainframe’s functionality.7

By the early 1980s, new advances diminished reliance on mainframes. Increasingly powerful personal computers allowed individual users to install applications and store data on their own equipment, rather than using a shared mainframe computer.8 The development of operating systems, such as Microsoft’s MS-DOS and Apple’s Macintosh interface, also made computers more friendly to the average user.9 By 1984, personal computer sales eclipsed those of large corporate mainframes in the $22 billion computer industry.10

9. See Ceruzzi, supra note 6, at 269–76.
As computing decentralized, networking quickly developed. Users needed something more efficient than a large floppy disk to send a file created on their computer to a colleague. In corporate environments, users interconnected through a private, internal network to reach the company’s e-mail server or communicate with co-workers. Many personal users began subscribing to self-contained networks, such as Prodigy, CompuServe, and America Online. Subscribers typically paid based on the amount of time they were connected to the network; unlike today’s Internet users, few could afford to spend hours casually exploring the provider’s network. After connecting to the network via a modem, users could download or send e-mail, post messages on a “bulletin board” service, or access information. It was on the cusp of this phase, with computer networking in its infancy, that Congress adopted the Stored Communications Act in 1986.

A new disruptive technology soon changed the course of networking. The World Wide Web arrived in 1990 and allowed the integration of individual networks via the Internet. The introduction of the web browser, such as Netscape Navigator in 1994, made it even easier for users to access and explore the content available through the Internet. Internet usage exploded and by 1997 more than fifty-six million Americans had Internet access at home, work, or school.

The Internet’s capabilities continue to expand rapidly with the addition of new technologies and enormous infrastructure investment. Providers, such as Hulu (video content), the iTunes store (music and video content), and Skype (telephone and videoconferencing services), are now capitalizing on these enhancements to offer new Internet-based services. These services are possible, in part, due to the growing availability of high-speed Internet access; in April 2009, sixty-three percent of adults in the United States had a broadband

11. See Ceruzzi, supra note 6, at 291–95.
13. See Jeffrey A. Tannenbaum, Speed, Cost and Cachet Aid Growth of Electronic Mail, Wall St. J., July 27, 1988, at 29 (“In May 1987, for example, CompuServe dropped its hourly rate for certain fast-transmission users to $12.50, from $19.50 evenings and $22.50 during the day.”).
16. See Carr, supra note 8, at 17; Ceruzzi, supra note 6, at 295–304.
17. See Abbate, supra note 14, at 217; Carr, supra note 8, at 17.
Internet connection in their home. Mobile Internet access, through devices such as the iPhone, is also spreading rapidly and extending the Internet’s reach beyond the home and workplace. These changes have made the Internet a ubiquitous part of our daily lives.

B. THE ERA OF CLOUD COMPUTING

The increasing functionality of the Internet is decreasing the role of the personal computer. This shift is being led by the growth of “cloud computing”—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. Service providers operate a group of computer servers that are connected to each other and function as a single “cloud” of resources. The cloud is configured to divide the tasks of running applications and storing data into small chunks and to distribute them among the servers’ aggregate resources. Providers recognize that this is difficult for the average user to understand and market the service as “cloud computing” to help strip away the complexity.

Many Internet users have experienced cloud computing, but fail to recognize or understand the technology making it possible. For example, most computer users are familiar with the operation of word processing programs, such as Microsoft Word. The program runs on the user’s computer and the resulting documents are saved on the computer’s hard drive. In contrast, cloud computing...

---

21. See Tom Wright, Poorer Nations Go Online on Cellphones, Wall St. J., Dec. 5, 2008, at B4. Mobile Internet access also has the potential to extend service into areas where fixed-line infrastructure is lacking or prohibitively expensive. Id.
22. See Miller, supra note 7, at 13–15.
23. See, e.g., Rearden LLC v. Rearden Commerce, 597 F. Supp. 2d 1006, 1021 (N.D. Cal. 2009) (finding that cloud computing is “a term used to describe a software-as-a-service (SAAS) platform for the online delivery of products and services”); FTC Complaint of Electronic Privacy Information Center at 4, In re Google, Inc. & Cloud Computing Servs. (Mar. 17, 2009) (“Cloud Computing Services are an emerging network architecture by which data and applications reside on third party servers, managed by private firms, that provide remote access through web-based devices.”), available at http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf; Robert Gellman, World Privacy Forum, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing 4 (2009) (“[C]loud computing involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections.”) (emphasis omitted); Posting of Bob Boorstin to Google Public Policy Blog, What policymakers should know about “cloud computing,” http://googlepublicpolicy.blogspot.com/2009/03/what-policymakers-should-know-about.html (Mar. 20, 2009, 10:35 EST) (defining cloud computing as “the movement of computer applications and data storage from the desktop to remote servers”).

For some large organizations, the development of a private cloud may be a cost-effective means of serving the entity’s computing needs. See Michael Armbrust et al., Univ. of Cal. at Berkeley, Above the Clouds: A Berkeley View of Cloud Computing 1 (2009) (differentiating between public and private cloud computing). However, for purposes of this Note, the analysis will focus on public clouds intended to serve third parties.
allows a user to complete the same task on the Internet. An Internet user can access a word processing application, such as Google Documents, that resides on a service provider’s computers and save the completed document on the provider’s server to access later. The user’s computer is irrelevant in this process. This structure closely resembles the early mainframe computing model; instead of a “dumb terminal” designed solely to access a mainframe’s resources, the personal computer is beginning to serve as a “dumb terminal” to access cloud computing’s resources via the Internet.

The increasing importance of cloud computing is underscored by the intense competition it is creating within the technology industry. Many of the industry’s largest players are moving aggressively to capitalize on the growing popularity of cloud computing and capture market share. In the midst of this competitive chaos, participants are organizing into opposing factions to promote different standards and operating principles to guide the development of cloud computing. The industry cannot even agree on the meaning of the term “cloud computing.” These battles have Internet forums and media outlets buzzing with anticipation about the potential for a period of open warfare within the industry.

Cloud computing promises to overcome the inefficiencies created when everyone has their own computer—a “dispersed computing” structure. For the last several decades, computer companies focused their efforts on building faster processors and higher capacity storage devices. Despite the extra capacity this created, three problems inherent in a dispersed computing structure have not been resolved. First, computer purchasers must buy more processing power and storage capacity than they currently need to anticipate future growth or rare moments of peak demand. Until that day comes, if it ever does, that expensive capacity will remain idle and unproductive. Second, the assembly and maintenance of computer equipment and applications requires users to develop techno-

---

24. See Carr, supra note 8, at 17 (“Instead of relying on data and software that reside inside our computers, inscribed on our private hard drives, we increasingly tap into data and software that stream through the public Internet.”).


26. Armbrust et al., supra note 23, at 3 (noting the industry-wide disagreement about the exact meaning of “cloud computing”); Cloud Computing: Clash of the Clouds, ECONOMIST, Oct. 17, 2009, at 80, 80–82 (same). In October 2009, the National Institute of Standards and Technology (NIST) released another proposed definition of cloud computing—its fifteenth draft of the proposal—providing, in part, that: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Peter Mell & Tim Grance, Nat’l Inst. of Standards and Tech., The NIST Definition of Cloud Computing (15th version 2009).

27. See Cloud Computing: Clash of the Clouds, supra note 26, at 80–82 (noting that Apple, Google, and Microsoft are “preparing for battle” over cloud computing).

28. See Carr, supra note 8, at 55–56 (noting studies of corporate data centers showing that only 25%–50% of storage capacity and less than 25% of processing power are being used); Nicholas G. Carr, The End of Corporate Computing, MIT SLOAN MGMT. REV., Spring 2005, at 67, 70 (estimating
logical expertise. This is a costly and time consuming endeavor that distracts organizations and individuals from other activities in which they offer specialized knowledge or abilities. Finally, dispersed computing lacks the redundancy necessary to protect valuable data and overcome equipment failures. Everyone has an unfortunate tale of a hard drive failure that resulted in hours, weeks, or years of lost effort and memories. While this is a painful event for a person, it can be disastrous for a business. When a calamity or technology failure strikes, essential data is lost and workforces are idled—unless redundant storage or processing power is available to remedy the problem.

Advances in computer and networking technology have also surmounted many of the limitations that encouraged the initial development of a dispersed computing model. Network capacity and transmission speeds presented the largest roadblocks to cloud computing in earlier years. Users need a fast Internet connection to upload or retrieve large quantities of data or interact with a server-based application in real-time. Until recently, though, the unavailability or expense of broadband Internet access limited many users to relatively slow dial-up connections. The widespread deployment of fiber optics, high-speed DSL, and cable broadband services during the last decade overcame this problem across much of the nation and most American households now have access to high-speed Internet. Additionally, the software and hardware required to share computing resources among multiple users advanced rapidly. Cloud providers must be able to divide users’ tasks among CPUs, allocate...
storage capacity efficiently, and safeguard users’ transmissions and stored data. These challenges are now being met with innovative solutions, including multicore processing technology, grid-computing infrastructure, and improved data center architecture.37

While computer science created the ability to provide cloud computing, other factors were creating the demand. Escaping the endless cycle of buying and installing “upgrades” required by technology vendors is among cloud computing’s most attractive features.38 By withdrawing support for previous hardware and software versions, technology companies essentially force users to buy their latest products.39 Yet, these upgrades can be difficult and costly to install and any new features they include offer little benefit to many users.40 Additionally, as people and organizations shift their data to a digital environment, the constraints of the personal computer are becoming more visible and less acceptable. A major limitation is people’s need to interact with their applications or data while outside the home or office.41 Colleagues also struggle to collaborate on projects when content is trapped inside a personal computer.42 A common frustration is the inability to jointly review or edit a document or presentation with other users. A personal computer user may need to distribute the file via e-mail and manually synthesize the comments and edits received back from reviewers.43

Cloud computing helps users circumvent these difficulties by making the personal computer largely irrelevant.44 A cloud user only needs to have a device connected to a cloud provider—a laptop, smartphone, or shared public computer will suffice.45 Both the application and data are stored in the cloud, allowing the cloud provider to install upgrades and complete the maintenance for all of its users simultaneously.46 The cloud user can focus on the desired

37. See Carr, supra note 8, at 64–68 (discussing Google’s proprietary development of many of these technological advances); Miller, supra note 7, at 12–13.


39. See David H. Freedman, Upgrade Madness, Inc. Mag., Feb. 2006, at 65, 66 (“Upgrades are an enormous source of revenue for the software industry, and most vendors aren’t above engaging in some form of stick-waving with customers who won’t jump for the carrot. The big stick in this regard is the threat to retire older versions—declare them officially obsolete and withdraw support.”).

40. Id. at 65–66.

41. See Miller, supra note 7, at 27.

42. Id. at 14–15.

43. Id. at 75, 148–50.

44. See Cloud Computing: Clash of the Clouds, supra note 26, at 80 (noting that cloud computing renders personal computing devices and their operating systems less important).

45. The minimal processing and storage needs of a device needed primarily to access cloud applications is driving the growth of a new generation of less powerful and cheaper computers, commonly referred to as “netbooks.” See Randall Stross, The PC Doesn’t Have To Be an Anchor, N.Y. Times, Apr. 19, 2009, at BU-4; Clive Thompson, The Netbook Effect, Wired, Mar. 2009, at 60, 62.

46. See Freedman, supra note 39, at 66.
task, rather than the infrastructure or technology making it all possible.

Widespread consumer embrace of early cloud computing offerings suggests that a meaningful shift is underway, rather than a passing fad. Webmail—e-mail services offered by a cloud provider through an Internet-based user interface—was among the first cloud computing services offered to the public.47 This form of cloud computing—known within the computer industry as “Software as a Service”48—moved e-mail from desktop applications, such as Microsoft Outlook, to Internet-based e-mail applications running on cloud providers’ servers.49 Webmail offered users several improvements over its desktop predecessors, such as remote access from any Internet-enabled device. The public quickly embraced webmail services and millions have since established e-mail accounts with cloud providers such as Hotmail, Yahoo! Mail, and Gmail.50 Webmail’s popularity led to the rapid development of other cloud-based applications, including calendars, contact management, word processing, and digital photo applications.51 Many desktop application publishers recognize this trend and are changing their programs to operate in a cloud-based configuration.52

Recent developments in cloud computing will further decentralize control over the applications and services hosted on a cloud provider’s infrastructure. Many providers are shifting away from designing their own applications (the “Software as a Service” model) and instead opening up their systems to third-party developers who create applications that run on the cloud provider’s platform (the “Platform as a Service” model).53 This cloud computing model allows programmers to develop new applications or create “mashups” that combine the capabilities of multiple cloud applications.54 Opening the cloud

47. See Ceruzzi, supra note 6, at 318–19. Webmail has also given courts their first exposure to the cloud computing environment. See, e.g., United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (examining the Fourth Amendment issues relating to the seizure of e-mail from a Yahoo! webmail account).
48. See Miller, supra note 7, at 40–41.
49. See id. at 52.
platform to third-party programmers is likely to rapidly increase the pace of development and functionality. Additionally, some cloud providers are selling raw computer resources, including processing power and data storage, as a type of utility service (the “Hardware as a Service” model). These providers are offering their services with usage-based rates that mirror the pricing structure used by electric utilities. This business model is expanding rapidly as users and providers realize its benefits. For consumers, these services provide access to reliable and easily expandable computing resources for much less effort and cost than would be required to buy and maintain the hardware themselves. Meanwhile, providers recognize the opportunity to profit from their large reservoirs of unused processing and storage capacity.

Cloud computing, through its applications, platforms, and services, is already affecting the ways that people and businesses interact with and use computers and the Internet. The viability of the technology and its growing acceptance by consumers and service providers offer powerful evidence that a lasting technological and societal shift is underway. As a result, courts will need to determine how existing laws may or may not protect electronic communications and content in this new computing model.

II. ORIGINS AND OPERATION OF THE STORED COMMUNICATIONS ACT

The Stored Communications Act is best understood by considering its operation and purpose in light of the technology that existed in 1986. The Act is not

55. Professor Zittrain attributes much of the success of personal computers and the Internet to their role as “generative technologies” that allowed experimentation and innovation by third parties. See Zittrain, supra note 12, at 1980–94, 2039–40. In a more recent example of this phenomenon, Apple opened the iPhone to third-party software developers, and users downloaded more than three billion applications from its App Store within eighteen months. Press Release, Apple Inc., Apple's App Store Downloads Top Three Billion (Jan. 5, 2010), available at http://www.apple.com/pr/library/2010/01/05 appstore.html. Apple’s competitors are now scrambling to open up their own platforms. See Jenna Wortham, Apps Boom as Companies Seek a Place on Your Phone, N.Y. TIMES, June 8, 2009, at B4 (noting that “Apple showed that new apps sell phones” and others are seeking to replicate its App Store model).

56. See Carr, supra note 8, at 85–103 (analogizing cloud computing to the decentralization of electricity production and the growth of modern utilities at the turn of the century); Miller, supra note 7, at 41–42.


58. See Michael Fitzgerald, Cloud Computing: So You Don’t Have To Stand Still, N.Y. TIMES, May 25, 2008, at BU-4 (discussing the benefits of using Amazon Web Services for a small Internet-based business that unexpectedly generated more than 750,000 customers in three days).

59. See, e.g., Amazon: Lifting the Bonnet, ECONOMIST, Oct. 7, 2006, at 91 (“In order to cope with the Christmas rush, Amazon has far more computing capacity than it needs for most of the year. As much as 90% of it is idle at times. Renting out pieces of that network to other businesses, such as SmugMug, an online photo site that uses the S3 service, is a way to get extra return on Amazon’s $2 billion investment in technology.”).
built around clear principles that are intended to easily accommodate future changes in technology; instead, Congress chose to draft a complex statute based on the operation of early computer networks. To apply the Act to modern computing, courts need to begin by extracting operating principles from a tangled legal framework. Fortunately, several sources can guide an inquiry into congressional intent. First, the legislative history of the Stored Communications Act, as represented in committee reports and transcripts of hearings from the House of Representatives and Senate, offers extensive background into the technology and problems that prompted the need for the legislation.60 Second, Congress notes its explicit reliance on a report from the Office of Technology Assessment (OTA) prepared in 1985 to review the potential threats to civil liberties resulting from new or emerging technologies.61 Finally, the language and structure of the Act offers some clues into Congress’s approach to privacy in computer networks.

The first step in deciphering the Stored Communications Act is to recognize the two primary uses of computer networks that Congress sought to regulate: (1) electronic communication services (ECS) designed to handle “data transmissions and electronic mail” and (2) remote computing services (RCS) intended to provide outsourced computer processing and data storage.62 Congress decided to build the Act around these two categories and apply differing privacy protections to each.63 Any analysis under the Act must begin by classifying the data in question within one of these categories.64

A. ELECTRONIC COMMUNICATION SERVICES

Congress explored the category of electronic communication services, designed to transmit information and data between users, primarily through the lens of early electronic mail systems.65 At the time, e-mail operated through a fragmented delivery system in which communications were slowly transmitted between the computer servers operated by e-mail providers.66 Each provider’s servers would temporarily store an e-mail until transmitting it along to its next waypoint. After an e-mail reached its destination, the recipient would use a

64. See infra Parts III–IV for an application of the Act’s ECS and RCS categories to cloud computing services.
66. See S. Rep. No. 99-541, at 8; Tannenbaum, supra note 13, at 29 (noting that an e-mail user in 1988 paid forty cents per message, which typically reached its recipient within twenty minutes). The OTA report noted there were at least five stages in the transmission and storage of an e-mail. OTA Report, supra note 61, at 48–50.
dial-up modem to connect to her e-mail provider and download the message to her computer; alternatively, some providers would conveniently “put the messages onto paper and then deposit it in the normal postal system.”

Elected officials struggled to understand this new technology and relied on analogies to the more familiar postal service. However, important differences limited the analogy’s value. For example, the House report on the Act specifically noted that e-mail differs from traditional postal mail in that the service provider “may technically have access to the contents of the message and many retain copies of transmissions.”

The fragmented e-mail system used in the mid-1980s is embodied in the Stored Communications Act’s provisions governing electronic communication services (ECS). A service provider needs to satisfy two requirements for communications stored on its system to receive the ECS privacy protections offered by the Act. First, the service provider must offer users “the ability to send or receive . . . electronic communications.” Electronic communications is broadly defined to mean nearly any form or style of communication, including “signs, signals, writings, images, sounds, data or intelligence of any nature.” Second, the service provider must hold the electronic communication in “electronic storage.” This requirement is commonly misunderstood because the statutory definition of “electronic storage” is much narrower than its name suggests. The Act limits “electronic storage” to mean (1) “temporary, intermediate storage . . . incidental to the electronic transmission” of the communication and (2) copies made by the service provider for “backup protection.” This rather odd definition is better understood in light of the e-mail delivery system in place at the time, which required multiple service providers to store communications briefly before forwarding them on to their next destination or while awaiting download by the recipient.

B. REMOTE COMPUTING SERVICES

Congress created a second category covering “remote computing services” to address third-party service providers that offered “sophisticated and convenient computing services to subscribers and customers from remote facilities.” Buying a lot of processing or storage capacity was prohibitively expensive for many organizations in 1986. Outsourcing these functions to a service provider, however, created economies of scale that offered a sustainable cost structure for

68. H.R. REP. No. 99-647, at 22 & n.34.
70. Id. § 2510(15).
71. Id. § 2510(13).
72. Id. § 2510(17).
73. See Kerr, supra note 2, 1213–14; see also supra notes 65–68 and accompanying text.
the new technology. The Senate report about the Stored Communications Act notes that “[i]n the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data in-house on the user’s own computer or on someone else’s equipment.” A company or organization that decided to outsource its computing needs would transmit its data for processing either to a third-party service provider’s personnel or directly transfer it to the provider’s remote computer. At the time of the Act’s adoption, outsourced computing was a service marketed to “businesses of all sizes—hospitals, banks and many others,” rather than individual consumers.

Congress included the category of remote computing services (RCS) in the Stored Communications Act to ensure the privacy of data outsourced to these third-party service providers. A service provider must meet strict requirements to qualify as an RCS and enjoy the benefit of privacy protections for its customers’ data. First, the provider must offer “computer storage or processing services” to the public through an electronic communications system. Second, the data must be received electronically from the customer. Third, the content must be “carried or maintained” by the service provider “solely for the purpose of providing storage or computer processing services” to the customer. Finally, the provider cannot be “authorized to access the [customer’s] content for purposes of providing any services other than storage or computer processing.” The requirements for RCS precisely describe the nature of the commercial relationship that existed at the time of the Act’s adoption between the outsourced computing providers and their business clientele.

C. PRIVACY PROTECTIONS

If a computing service qualifies as an electronic communication service (ECS), the Act provides two levels of privacy protection depending on whether disclosure of the communication is voluntary or compelled by the government.

75. Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties and the Admin. of Justice of the H. Comm. on the Judiciary, 99th Cong. 84–85, 89 (1986) [hereinafter ECPA Hearings] (statement of Michael P. Nugent, Chairman, Comm. on Computer Systems and Communications Privacy, ADAPSO); see also Carr, supra note 8, at 52 (noting that “a typical IBM mainframe was about $30,000 a month in the mid-1960s”); Patricia L. Bellia, The Memory Gap in Surveillance Law, 75 U. Chi. L. Rev. 137, 142–44 (2008) (discussing the decline in storage pricing over the past five decades).
77. Id.
78. Id. at 10. Not until 1990—more than four years after the SCA’s adoption—did the first provider begin offering Internet access to consumers. Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1572 (2004).
80. Id. §§ 2510(14), 2711(2).
81. Id. §§ 2702(a)(2)(A), 2703(b)(2)(A).
82. Id. §§ 2702(a)(2)(B), 2703(b)(2)(B).
83. Id.
84. See Kerr, supra note 2, at 1213–14; see also supra notes 74–78 and accompanying text.
Under the first tier, an ECS provider may voluntarily disclose a user’s communication if one of eight conditions is satisfied, such as when the communication’s sender or recipient consents or when necessary for “the protection of the rights or property of the provider.” A second tier imposes much greater restrictions when the government seeks compelled disclosure from the ECS provider. In these instances, a search warrant is required if the communication has been in “electronic storage” on the provider’s service for 180 days or less. After 180 days, the government may use an alternate legal process with a lower causal threshold.

Data stored by a remote computing service (RCS) is subject to the same two-tiered approach, but receives fewer privacy protections than communications held by an ECS. An RCS provider may voluntarily disclose a customer’s data in compliance with one of the same eight statutory exceptions applicable to an ECS provider. However, the second tier protections against compelled disclosure by the government are more limited. Data stored in an RCS for any duration may be accessed by the government through a § 2703(d) order requiring only “reasonable grounds to believe” the data is “relevant and material to an ongoing criminal investigation.”

In both an ECS and RCS, personal identifying information about the user, such as her name, physical or e-mail addresses, and IP address, is entitled to little protection. A service provider can voluntarily disclose the user’s personal identifying information to any non-governmental entity or provide it directly to the government upon receipt of an administrative subpoena.

Among the Act’s most significant, although unstated, privacy protections is the ability to prevent a third party from using a subpoena in a civil case to get a user’s stored communications or data directly from an ECS or RCS provider. Courts interpret the absence of a provision in the Act for compelled third-party disclosure to be an intentional omission reflecting Congress’s desire to protect users’ data, in the possession of a third-party provider, from the reach of private

---

85. 18 U.S.C. § 2702(b)(3), (5).
86. The protections offer surprisingly little recourse for criminal defendants because of the lack of a suppression remedy for evidence gathered in violation of the Stored Communications Act’s (SCA) requirements. See United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (holding that Congress did not provide a suppression remedy for evidence gathered in violation of the SCA). Some observers have suggested that the lack of a meaningful incentive for criminal defendants to challenge detrimental court decisions explains the seemingly modest amount of case law surrounding the SCA’s application. See Orin S. Kerr, Lifting the “Fog” of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law, 54 HASTINGS L.J. 805, 841 (2003) (arguing for the creation of a suppression remedy to further doctrinal development of the SCA).
87. 18 U.S.C. § 2703(a).
88. Id. § 2703(b).
89. 18 U.S.C. § 2702(b).
90. 18 U.S.C. § 2703(d). The Act also requires that the government provide the customer with notice of the compelled disclosure, but notification may be delayed with a court’s permission. Id. § 2705 (2000 & Supp. I 2009).
91. 18 U.S.C. § 2702(c)(6).
92. Id. § 2703(c)(2)(A).
litigants. Without this blanket immunity from subpoena in civil cases, a user’s entire portfolio of stored communications and data might be fair game for an adversary. An important limitation to this privacy safeguard is the Act’s allowance for a service provider to voluntarily share a user’s personal identifying information with a non-governmental entity. Consequently, an ECS or RCS provider is only limited by its contractual relationship with the user in deciding whether to respond for requests, via subpoena or otherwise, for a user’s personal identifying information.

III. CLOUD COMPUTING AS AN ELECTRONIC COMMUNICATION SERVICE

Many cloud computing services fail to qualify for the heightened privacy protections provided to electronic communication services (ECS) in the Stored Communications Act. One of the Act’s twin requirements is that an ECS give users “the ability to send or receive . . . electronic communications.” Yet, many of today’s popular cloud computing services are designed for purposes other than communication, such as word processing or digital photo storage, and lack any “send or receive” capability.

Cloud services further violate the second condition for an ECS requiring that communications be held in “electronic storage.” As discussed previously, electronic storage is a term of art within the SCA that is limited to (1) storage of a “temporary [and] intermediate” nature that is “incidental to the electronic transmission” of the communication or (2) storage of the communication by the ECS provider to provide backup protection. But cloud services satisfy neither of these definitions. Contrary to the requirement that storage be temporary and incidental to the service, many cloud providers offer their customers generous...
storage capacity to enable long-term data retention. As an example, the Google Documents service offers its customers the ability to store 5000 documents and presentations, in addition to 1000 spreadsheets—far more than any customer may need for temporary purposes. Furthermore, the supplemental services that cloud providers offer clarify their intent to serve as a final repository for their customers’ data, rather than a source of backup protection. For instance, many cloud providers offer their data storage services alongside applications designed to manipulate that data or mobile applications for accessing that data through remote computers. Because users’ content is not being stored by the ECS provider within the SCA’s narrow definition of electronic storage, the ECS protections are inapplicable.

Webmail services are an exceptional category of cloud services that may qualify as an ECS. These cloud services offer customers the ability to “send or receive” e-mail and, therefore, satisfy the first prong of the ECS requirements. The further requirement that communications be in “electronic storage” is more problematic, but expansive court interpretations provide some relief. Every circuit to consider the issue agrees that unopened e-mail remains in electronic storage for 180 days because it is being held temporarily until the recipient reads or retrieves it. The vast majority of unopened e-mail stored by a webmail service will, therefore, qualify as a electronic communication held by an ECS and receive the Act’s privacy protections.

After an e-mail is opened, however, the analysis becomes more complicated. Many courts hold that an electronic communication is complete the moment it is opened or downloaded by its intended recipient. These courts reason that, upon completing the journey to the recipient, the e-mail converts immediately into plain data that the user can store or delete. Once viewed or downloaded though, the e-mail is no longer considered an “electronic communication” and the service provider is no longer an ECS with respect to that e-mail.

In these circuits, the loss of ECS protection is not the end of the story. The same provider can act in both an ECS and RCS capacity, and the services it
provides must be considered individually to determine which standard is applicable in a given situation. Therefore, the possibility remains that a cloud provider might be acting as a remote computing service when storing the opened e-mail for its customer. Congress foresaw a similar situation within the legislative history of the Act:

Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by [the RCS provisions of] section 2702(a)(2).

A split among federal courts now complicates this otherwise straightforward analysis, but may provide greater protections for some webmail customers. In *Theofel v. Farey-Jones*, the Ninth Circuit held that an opened e-mail remains in “electronic storage” and, therefore, the communication continues to be protected by the Act’s ECS provisions while it remains in storage with the provider. The *Theofel* decision embraces the novel theory that customers are storing opened e-mail on the provider’s server as a form of backup protection—one of the two permissible definitions of “electronic storage.” The Ninth Circuit recently reaffirmed its holding in *Theofel*, but the decision continues to receive substantial judicial and academic criticism. Although the Ninth Circuit’s position may be unpopular, the critical mass of technology companies

105. Kerr, *supra* note 2, at 1215.
107. 341 F.3d 978 (9th Cir. 2003), amended by 359 F.3d 1066, 1075–76 (9th Cir. 2004) (refusing to distinguish between intermediate and post-transmission e-mail storage in defining ECS).
108. See *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 902 (9th Cir. 2008), *reh’g en banc denied*, 554 F.3d 769 (9th Cir. 2009), *cert. granted sub nom. City of Ontario v. Quon*, 78 U.S.L.W. 3359 (U.S. Dec. 14, 2009) (No. 08-1332). *Quon* involved the privacy of text messages sent by a City of Ontario police officer using an employer-issued text-messaging pager. *Id.* at 895. The Court contacted Arch Wireless, its service provider for the pagers, and asked for copies of the text messages sent by Sergeant Quon after he exceeded his monthly allocation several times. *Id.* at 897–98. The transcripts revealed inappropriate personal messages, allegedly in violation of the City’s policy, and resulted in an Internal Affairs investigation. *Id.* at 898. The Ninth Circuit held that Arch Wireless was an ECS and, by releasing his messages to the City, it violated Sergeant Quon’s rights under the SCA. *Id.* at 903. The court further held that the search of the archived text messages violated Quon’s Fourth Amendment rights. *Id.* at 910. The Supreme Court recently granted certiorari in *Quon*, but it does not appear that the SCA-related issues will be considered. City of Ontario v. Quon, 78 U.S.L.W. 3359 (U.S. Dec. 14, 2009) (No. 08-1332). Instead, the Court will only consider the issues surrounding the Fourth Amendment privacy rights of government employees in the workplace. See Petition for a Writ of Certiorari at i, City of Ontario v. Quon, No. 08-1332, 2009 WL 1155423 (Apr. 27, 2009).
located within the Circuit causes this reading of the Act’s requirements for webmail to be applied in many cases.111

IV. CLOUD COMPUTING AS A REMOTE COMPUTING SERVICE

A. APPLICATION OF THE STATUTORY LANGUAGE

At first glance the Stored Communications Act’s requirements for a remote computing service (RCS) offer false hope that they will apply to cloud computing services. The RCS provisions in the Act would seem to be an intuitive fit for cloud computing because Congress originally added them to address outsourced computer processing and data storage.112 In many ways, cloud computing is a reversion to and expansion of this practice.113 The Act’s language also offers some initial appeal for cloud computing. To qualify as an RCS, the cloud service must publicly offer “computer storage or processing services” over a network.114 Most cloud providers offer both of these services via the Internet and would appear to satisfy this requirement. Some courts, relying on this short analysis, have applied the RCS provisions to cloud computing services,115 with alleged support from the Act’s legislative history116 and the concurrence of legal scholars.117

This analysis of cloud computing is flawed though because it fails to account for the Act’s remaining requirements. Besides the types of services that may be provided, an RCS must satisfy five other prerequisites. As an initial matter, the data must (1) contain “content[ ],” (2) be “carried or maintained . . . on behalf

110. See, e.g., Kerr, supra note 2, at 1217 (remarking that “the Ninth Circuit’s analysis in Theofel is quite implausible and hard to square with the statutory text”); Marc J. Zwillinger & Christian S. Genetski, Criminal Discovery of Internet Communications Under the Stored Communications Act: It’s Not A Level Playing Field, 97 J. CRIM. L. & CRIMINOLOGY 569, 580 (2007) (noting that “the Theofel court’s analysis is somewhat tortured”).

111. See Zwillinger & Genetski, supra note 110, at 581; see also SEARCHING AND SEIZING COMPUTERS, supra note 104, at 123 (“Unfortunately . . . there is now a split between two interpretations of ‘electronic storage’—a traditional narrow interpretation and an expansive interpretation supplied by the Ninth Circuit. . . . As a practical matter, federal law enforcement within the Ninth Circuit is bound by the Ninth Circuit’s decision in Theofel, but law enforcement elsewhere may continue to apply the traditional interpretation of ‘electronic storage.’”).

112. See supra section II.B.

113. See Bellia, supra note 75, at 145.


116. See H.R. REP. NO. 99-647, at 65 (1986) (noting that opened electronic mail stored on the provider’s server may fall within the RCS provisions).

117. See, e.g., Kerr, supra note 2, at 1216 (citing COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § III.B (2002)).
of . . . a subscriber or customer,” and (3) have been electronically transmitted to
the provider.\textsuperscript{118} A cloud service will ordinarily satisfy these requirements. However, the final two requirements to be an RCS necessitate closer scrutiny. The Act demands that the customer’s data be transmitted to the cloud provider “solely for the purpose of providing storage or computer processing ser-
vices.”\textsuperscript{119} Finally, it insists that the cloud provider “not [be] authorized to access
the contents of any such communications for purposes of providing any services
other than storage or computer processing.”\textsuperscript{120}

Cloud providers commonly embrace a business model that leaves the final
two requirements unsatisfied and, as a result, they will not qualify as an RCS.
Many cloud providers rely extensively on advertising revenue, rather than fees
from customers, to fund their offerings.\textsuperscript{121} Although advertising does not violate
the Act’s requirements, a subset of cloud providers have sought a competitive
advantage, against other advertising platforms, by providing contextual or
targeted advertising opportunities. In these systems, advertisers no longer pay to
reach every visitor to a particular website or advertising network. Instead,
contextual advertising allows a marketing campaign to target a specific audi-
ence based on the content a website visitor is accessing.\textsuperscript{122} For example, a
widget retailer can use the Google AdWords system to buy a keyword, such as
“widget,” and ensure that its advertising appears whenever a website visitor
browses content related to widgets on a website participating in the Google
AdSense program.\textsuperscript{123} This marketing mechanism is particularly effective be-
because it allows advertisers to appear at the moment a potential customer may be
most receptive.\textsuperscript{124}

Contextual advertising requires access to content though, which violates the
Stored Communications Act’s requirements. Cloud users often authorize a
provider to access their stored data—through implied or explicit consent to the
provider’s terms of service agreement and privacy policy—as a condition of

\textsuperscript{119} Id. § 2702(a)(2)(B).
\textsuperscript{120} Id. (emphasis added).
\textsuperscript{121} See Chris Anderson, Free! Why $0.00 is the Future of Business, WIRED, Mar. 2008, at 140; see also The End of the Free Lunch—Again, ECONOMIST, Mar. 21, 2009, at 16 (noting the widespread use of
the advertising-based business model among web service providers and its limitations).
\textsuperscript{122} See Rescuecom Corp. v. Google Inc., 562 F.3d 123, 125–26 (2d Cir. 2009) (discussing the
operation of the Google AdWords contextual advertising system).
\textsuperscript{123} See Google Content Network, http://www.google.com/adwords/contentnetwork/audience.html
(last visited Feb. 12, 2010).
\textsuperscript{124} See, e.g., Jonathan Lemonnier, Contextual Targeting Boosts Loyal Following, ADVERTISING AGE, Apr. 14, 2008, at 7 (discussing a contextual advertising case study showing a 19% increase in brand
recall versus non-targeted advertising); Yahoo! Customized Advertising FAQ, http://info.yahoo.com/
relevantads/faq/ (last visited Feb. 12, 2010) (“Customization features are designed to bring you the
news, weather, or other content you want, and to help you find what you are looking for more
efficiently. We apply this principle to advertising, believing that relevant ads will be more useful.”).
using a cloud computing service. By sharing their data with the cloud provider, users make possible the advertising services that pay for the costs associated with providing the cloud service—a model familiar to radio listeners and television viewers who have long accepted commercials embedded in programming to offset some or all of its cost. In essence, a customer’s privacy is the true cost of “free” cloud computing services.

But a customer’s willingness to share her data for advertising purposes has privacy implications well beyond the relationship with the cloud provider. The Act’s RCS privacy protections require that “storage or computer processing” be the sole reason that a customer transmits her data to the cloud provider. When data is also shared with the cloud provider to facilitate contextual advertising, this requirement is not satisfied. The Act further requires that the cloud provider only be authorized to access the customer’s data to provide the processing or storage service. However, by agreeing to share her data with the cloud provider for contextual advertising purposes, this additional requirement is unfulfilled. The applicability of the RCS provisions in the Stored Communications Act will, therefore, always require examining the cloud provider’s terms of service agreement and privacy policy. If a customer authorizes access to her data for the provision of contextual or targeted advertising services, the Act will not apply and the data will be at risk of disclosure to the government or another third party.

B. AN EXAMINATION OF EXISTING CLOUD PROVIDERS

Analyzing the existing terms of service agreements and privacy policies in use by large cloud providers offers insight into the types of data sharing provisions that courts are likely to encounter. Terms of service agreements and privacy policies are omnipresent and nearly every large company relies on them to regulate the use of its website and to disclose its data handling practices. Both documents are contracts that define the relationship between website

125. See infra section IV.B. These website contractual agreements also use other titles, including “terms of use” and “statement of rights and responsibilities.” This Note uses “terms of service” in reference to all such agreements.

126. See, e.g., Evernote Terms of Service § 10 (July 9, 2009), http://www.evernote.com/about/tos/ (noting the existence of a quid pro quo by requiring users to “agree that Evernote may present advertising in connection with the Service in consideration for the rights granted you to access and use the Service”); Google Terms of Service § 17.1 (Apr. 16, 2007), http://www.google.com/accounts/TOS (“Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.”).


128. See Suhong Li & Chen Zhang, An Analysis of Online Privacy Policies of Fortune 100 Companies, in Online Consumer Protection: Theories of Human Relativism 269, 277 (Kuanchin
operators, including cloud providers, and their visitors. Despite knowing that people rarely read them, courts often bind website visitors to these agreements. Yet, few cloud providers likely anticipate or understand the broader significance these agreements have for their customers’ privacy under the Stored Communications Act.

Terms of service agreements and privacy policies in use by several major cloud providers offer varying degrees of authority to access a customer’s data. The agreements can generally be classified into three categories: (1) explicit authority to access a customer’s data for marketing purposes, (2) vague authority to potentially access a customer’s data for purposes beyond the primary services, and (3) explicit prohibitions against accessing a customer’s data for any purpose other than providing a specific service. Each type of agreement is likely to lead to a different conclusion under the Act’s remote computing services standard and requires a unique analysis.

The least protective agreements empower cloud providers to access a customer’s data for many purposes, including advertising. Google, one of the largest cloud providers, uses such agreements extensively. Google’s advertising system relies on customers’ data, among other variables, to provide targeted marketing opportunities for advertisers. To facilitate this service, Google uses a master terms of service (“ToS”) agreement and a master privacy policy that apply to all of its cloud services, supplemented by smaller sub-agreements with provisions unique to each service.

The master ToS agreement states that “Google reserves the right . . . to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any [Google] Service.” With regard to the Gmail service, Google is overt with respect to its use of this authorization for marketing purposes; the Google Privacy Center informs customers that “[t]he Gmail filtering system also scans for keywords in users’ e-mails which are then used to match and serve ads. When a user opens an e-mail message, computers scan the text and then instantaneously display relevant information that is matched to the text of the message.”

---

129. See, e.g., United States v. Drew, 259 F.R.D. 449, 462 & n.22 (C.D. Cal. 2009) (surveying cases in which courts enforced website agreements); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000) (holding that a website user assented to the terms of service by using the provider’s service). But see Jason Isaac Miller, Note, “Don’t Be Evil”: Gmail’s Relevant Text Advertisements Violate Google’s Own Motto and Your E-Mail Privacy Rights, 33 Hofstra L. Rev. 1607, 1632–35 (2005) (arguing that website visitors should not be bound to the Terms of Use agreement for Google’s Gmail service because it “provides a flawed registration process that robs prospective users of the opportunity to give informed consent and manifest their agreement”).


131. Google Terms of Service, supra note 126, § 8.3.

Furthermore, the master ToS agreement requires customers to agree that “[b]y submitting, posting or displaying the content you 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 you submit, post or display on or through, [Google’s] Services.”133 Google, therefore, not only reserves the right to access a customer’s data for any purpose, but also to disclose it publicly.134

Sometimes Google’s ToS agreements can even reach beyond a customer’s own data and into the content of a third party. For example, website owners can use Google’s popular AdSense marketing platform to earn money by displaying contextual advertising on their website.135 Of course, Google needs to know what type of content is appearing on the website to allow it to deliver properly targeted advertising. To secure this access, Google’s ToS agreement for the AdSense service authorizes it to “access, index and cache” the customer’s website.136 While a website owner might willingly expose her own content to Google, she must also be mindful of her customers’ data that is stored or displayed on the website. Thus, website owners participating in the AdSense program need to ensure they have authorization to share their own customers’ data with Google for advertising purposes.137

It is unfair to single out Google as having a particularly expansive agreement because many other cloud providers are similarly up-front about their intention to access customers’ data for advertising purposes. Evernote, a cloud provider offering customers an online repository for documents, images, and other content, states that its services “may be supported by advertising revenue” and “display advertisements . . . [that] may be targeted to Content subject matter.”138 In order for Evernote to provide this targeted advertising, an express quid pro quo is written into its ToS agreement requiring customers to “agree that Evernote may present advertising in connection with the Service in consider-

133. Google Terms of Service, supra note 126, § 11.1.
134. Id. § 11.2 (“You agree that this license includes a right for Google to make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services.”).
136. Google AdSense Online Standard Terms and Conditions § 16 (Feb. 25, 2008), http://www.google.com/adsense/terms (“You grant Google the right to access, index and cache the Property(ies), or any portion thereof, including by automated means including Web spiders or crawlers.”); see also Bradley v. Google, Inc., No. C 06-05289(WHA), 2006 WL 3798134, at *1 (N.D. Cal. Dec. 22, 2006) (finding that Google AdSense “ads were tailored to the host website’s content”).
138. Evernote Terms of Service, supra note 126, § 10.
ation for the rights granted [customers] to access and use the Service.”139 Epernicus, another cloud provider of social networking services, requires users to grant it an unrestricted license to access and use users’ content “for any purpose, commercial, advertising, or otherwise.”140

Other cloud providers use a terms of service agreement and privacy policy that occupy an ambiguous middle ground. The ToS agreements in use by these providers reserve the right to access a customer’s data, but offer little guidance as to when or how that authority might be used. Several popular cloud providers, including Amazon Web Services and YouTube, use agreements with such indeterminate language.141 Some of these providers, however, offer non-binding guidance about their intended use of that authority. For example, Yahoo! reserves the right to “pre-screen” content on its service,142 but, at least for its webmail service, explains in its privacy policy that “Yahoo!’s practice is not to use the content of messages stored in your Yahoo! Mail account for marketing purposes.”143

A final group of cloud providers rely on ToS agreements that offer customers an explicit promise not to access their data. Some providers, such as Remember the Milk, a cloud provider offering a task management application, disavow any authority to access a customer’s data stored on its service.144 Mozy, a cloud provider offering automated back-up storage for consumers, tries to assure customers about the privacy of their content by plainly asserting, “We will not view the files that you backup using the Service.”145 Interestingly, rather than following Mozy’s approach and offering a general promise not to access customers’ data, many cloud providers elect to go even further and also specifically disclaim the ability to access content for advertising purposes.146

139. Id.
141. See Amazon Web Services Terms of Use (Sept. 22, 2008), http://aws.amazon.com/terms/ (“AWS has the right but not the obligation to monitor and edit or remove any activity or content.”); YouTube Terms of Service § 6.C, http://www.youtube.com/t/terms (last visited Dec. 21, 2009) (“BY submitting User Submissions to YouTube, you hereby grant YouTube a worldwide, non-exclusive, royalty-free, sublicensable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the User Submissions in connection with the YouTube Website . . . .”).
142. Yahoo! Terms of Service § 6 (Nov. 24, 2008), http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (“You acknowledge that . . . 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.”).
144. Remember the Milk Terms of Use § 5, http://www.rememberthemilk.com/help/terms.rtm (last visited Dec. 21, 2009) (“We will not use any of your content for any purpose except to provide you with the Service.”).
146. See, e.g., Zoho Terms of Service (Sept. 7, 2009), http://www.zoho.com/terms.html (“We respect your right to ownership of content created or stored by you. You own the content created or stored by you. Unless specifically permitted by you, your use of the Services does not grant Zoho the license to
C. EXISTING JUDICIAL PRECEDENTS

Before analyzing how these differing terms of service agreements and privacy policies will be applied under the Stored Communications Act, it is helpful to survey the Act’s existing jurisprudence. Courts have considered the precise contours of the Act’s remote computing service (RCS) provisions in surprisingly few cases. For many years, outsourced computing services declined in popularity and the RCS provisions came to be viewed as antiquated and irrelevant. However, two recent cases demonstrate that technology evolves in surprising ways and new computing services, including cloud computing, will reinvigorate the RCS privacy protections.

In *Flagg v. City of Detroit*, the defendants argued that the RCS provisions applied to stored text messages. Because the Act does not allow an RCS provider to disclose a customer’s data to an opposing party in civil litigation, the defendants sought to qualify the text messaging service as an RCS to prevent the service provider from divulging their messages. While the court conceded that there is not a discovery mechanism for data stored in a qualifying RCS, it held that the text messaging service failed to satisfy the requirements to be a remote computing service. The court noted that the Act requires that an RCS provider not be “authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.” In a strict interpretation of this requirement, the court held that the text messaging service provider was authorized to access a customer’s messages to provide the additional “service of retrieval” for stored text messages. Consequently, the stored text messages were not protected by the RCS privacy protections and their production during civil litigation was appropriate. The court proceeded to determine that, even if the text messages were being stored on an RCS, two of the eight exceptions allowing their disclosure would apply.

The *Flagg* court’s interpretation of the requirements for an RCS cautions that many cloud computing users will not enjoy the Stored Communications Act’s privacy protections. Any cloud service necessarily requires the “service of retrieval” for using applications or data stored with the cloud provider. Based on

---


149. Id. at 347.

150. Id. at 358–59 (quoting 18 U.S.C. § 2702(a)(2) (2006)).

151. Id. at 359.

152. Specifically, the court held that retrieving the text messages and sharing them with the customer might be viewed as “necessarily incident to the rendition of the [storage] service” and, thus, disclosure would be permissible under the exception available in § 2702(b)(5). Id. at 359 (quoting 18 U.S.C. § 2702(b)(5)). Additionally, the court held that the particular facts of the case would support disclosure, under § 2702(b)(3), based on the consent of the customer or sender. Id. at 359–66.
the interpretation applied in *Flagg*, this “service” would universally disqualify cloud providers and their customers from seeking refuge from disclosure under the Act. However, there are several reasons to believe that this reading of the Act’s requirements is unduly harsh. Most importantly, it would seemingly invalidate Congress’s allowance for an RCS to provide computer storage, which requires the ability to later retrieve customers’ stored data. The *Flagg* court’s opinion includes multiple alternate holdings and suggests that it too was unsure about the soundness of this argument. Regardless of its precise holding, the court’s approach to interpreting the RCS provisions in the Act may prove more informative. *Flagg* suggests, at a minimum, that future courts will strictly interpret and rigidly impose the Act’s RCS provisions and are unlikely to offer leniency when a cloud provider is allowed to access customers’ data for advertising or other purposes not explicitly authorized in the Act.

In *Viacom International Inc. v. YouTube Inc.*[^153] a district court interpreted the remote computing service provisions within the context of a cloud provider’s video sharing service.[^154] The court held that YouTube qualified as an RCS when storing private videos and other user content on its cloud service.[^154] In a brief footnote, the opinion notes that YouTube was authorized by its terms of service agreement to “access and delete potentially infringing private videos.”[^155] The court determined that this authorization was permissible under the Act because it occurred “in connection with [YouTube]’s provision of alleged storage services”—presumably a reference to the exception allowing cloud providers to access a customer’s data when it is “necessarily incident to the rendition of the service.”[^156] The court relied almost exclusively on an analysis of YouTube’s terms of service agreement to reject an additional argument that customers’ videos should be disclosed under the SCA’s consent exception.[^157] After dissecting the ToS agreement, the court determined it did not offer a user’s implied consent to divulge private videos to unauthorized third parties.

*Viacom* provides valuable guidance on the interaction between the RCS provisions and a non-webmail cloud service. The court’s extensive reliance on YouTube’s terms of service agreement shows the increasingly important role these contracts are serving to define the legal rights of cloud providers and their customers—well beyond the scope of their contractual relationship with each other. *Viacom* also follows *Flagg*’s approach of narrowly reading the scope of the “solely for storage or computer processing” requirement for an RCS. In both cases, the courts questioned whether any actions by the service provider, even slightly different from its primary storage function, could disqualify the customer’s data from the Act’s privacy protections. The courts in *Flagg* and *Viacom* hesitated to allow basic functions, such as retrieval or screening for unlawful

[^154]: *Id.* at 264.
[^155]: *Id.* at 264 n.8.
[^156]: *Id.*
[^157]: *Id.* at 264–65 & nn.9–11.
content, to come within the RCS provisions, which suggests a court would almost certainly reject instances where a cloud provider is authorized to access a user’s content for advertising or other tangential purposes.

D. INTERPRETING TERMS OF SERVICE AGREEMENTS

The judicial precedents interpreting the remote computing service (RCS) provisions, although limited, offer valuable guidance in determining how courts are likely to apply the Act’s requirements to cloud providers.

The two categories of terms of service (ToS) agreements and privacy policies on the ends of the spectrum offer relatively straightforward analyses. The category of protective agreements that expressly limit or disclaim the cloud provider’s authority to access a customer’s data for any secondary purposes, including advertising, is the most likely to qualify under the Act. Because these cloud providers are confining their access to the underlying “storage or computer processing” services, the Act’s plain language is satisfied. Therefore, these cloud services will likely survive scrutiny under the RCS provisions and their customers will benefit from the Act’s privacy protections.

On the other end of the spectrum, cloud providers who expressly rely on content for contextual or targeted advertising will fail to satisfy either of the twin requirements for an RCS. Specifically, by authorizing access to their data for advertising purposes, customers are offering their content for a purpose other than “storage or computer processing” in two ways. First, a cloud provider’s marketing program is a means to generate revenue and offer its services profitably. A customer’s willingness to make her content available for use in this program is part of a quid pro quo in which the customer receives “free” cloud services in exchange. Sharing one’s data with the cloud provider’s advertising program to offset any direct costs is thus a secondary purpose and contravenes the Act’s requirement that the customer’s data be transmitted to the cloud provider “solely for the purpose of providing storage or computer processing.”

Second, the targeted advertising may itself represent a direct service to the customer, despite its parallel financial benefit to the cloud provider. The tremendous revenue generated through online marketing, especially pay-per-click advertising, shows that Internet users rely on advertising to identify and explore offerings that interest them. Consumers appear to value a service that

158. By one estimate, $21–$25 billion in advertising is already sold annually to support “free” online services to consumers. See Anderson, supra note 127, at 165.
matches advertisements to their specific interests, by considering their stored content and other personal data, and guiding them to relevant products and services among the Internet’s seemingly infinite offerings.161 Ultimately, contextual advertising is problematic under the Act whether it is considered as a cost-offsetting service for the cloud service’s customer or as a separate service for exploring a consumer’s unique interests. In either scenario, the user’s content is being used for a secondary purpose, beyond simply “storage or computer processing,” and the Act’s privacy protections would not apply.

A more difficult analysis awaits when the cloud provider reserves authority to access a customer’s data in its ToS agreement, but offers limited guidance about its exercise of that power. When read in the context of the ToS agreement, many providers appear to be reserving authority to access customers’ data to proactively remove harmful or offensive content. A cloud provider is understandably concerned about the potential legal liability or harm to its goodwill that may result when its cloud service is used to store objectionable materials.162 Such a defensive purpose arguably falls within the Act’s exception allowing RCS providers to divulge content to protect its “rights or property.”163 However, the desire to preventively identify and remove these undesirable materials logically compels the provider’s need for a universal license to access all of a customer’s data. A more tailored authorization to access only objectionable content would essentially preclude advance screening because it creates circularity: whether specific content would be objectionable could not be known until after it was accessed. However, the difficulty with being authorized to access all of a customer’s data is that its exercise depends on the business practices and trustworthiness of the cloud provider. The same provision that allows access to a customer’s data to identify harmful material could also justify access for advertising purposes. To understand whether a cloud provider is authorized and intending to access a customer’s data for purposes other than “storage or computer processing,” a court would need to delve into each cloud provider’s operations and practices.

This uncertainty will likely result in courts refusing to apply the RCS’s privacy protections to cloud providers with ambiguous ToS agreements. There are several reasons why this is so. First, courts have no incentive to undertake the difficult task of speculating about how each cloud provider intends to use its


162. See Yahoo! Inc. v. La Ligue Contre Le Racisme Et L’Antisémitisme, 433 F.3d 1199 (9th Cir. 2006).

163. 18 U.S.C. § 2702(b)(5) (2006). Arguably, the mere authorization to access content to screen for objectionable material is not within the requirement that an RCS provider only provide “storage and computer processing” functions. However, this argument requires a narrow reading of these two authorized purposes, and at least one court has rejected such an interpretation. See Lukowski v. County of Seneca, No. 08-CV-6098, 2009 WL 467075, at *11–12 (W.D.N.Y. Feb. 24, 2009).
authority to access customers’ data. Even if the cloud provider’s prior use of that authorization could be determined, the court will have no way to figure out how the cloud provider might use it in the future.\textsuperscript{164} Second, a cloud provider has alternate mechanisms available, other than an authorization to access all of a customer’s data, to safeguard its systems, limit its legal liability, or protect its reputation. Instead, aggressive enforcement of the customer conduct requirements in its ToS agreement, coupled with responsive review of complaints about offensive or illegal content, could fulfill each of these objectives.\textsuperscript{165} Either of these protective measures could happen under a ToS agreement limiting the cloud provider’s access to “storage or computer processing” purposes or those exceptional uses authorized by the Act, including the “protection of the rights or property of the provider.”\textsuperscript{166} When courts encounter an expansive authorization to access customers’ data in a ToS agreement, the availability of other mechanisms should raise judicial concern about the true purpose it was included. Consequently, courts have little reason to favorably interpret assumptions about a cloud provider’s ambiguous authority to access a customer’s data in a ToS agreement and would likely disqualify its cloud services from the RCS privacy protections.

E. IMPLICATIONS FOR CLOUD COMPUTING USERS

As this analysis shows, the privacy protections that a cloud user will be entitled to under the Stored Communications Act will ultimately be determined by the cloud provider’s terms of service (ToS) agreement and privacy policy.\textsuperscript{167} When the ToS agreement allows the cloud provider to rely on the customer’s data to provide contextual advertising, the cloud service will not qualify as a remote computing service (RCS). Similarly, when the cloud provider reserves a general right to access a customer’s data without specifying the limits of that authority, the cloud service is also unlikely to qualify as an RCS. Only when a cloud provider expressly limits its access to a customer’s data for the purposes of providing computer storage or processing functions will the customer benefit from the Act’s RCS provisions, including the protection from compelled disclosure by the government and civil litigants.\textsuperscript{168}

\textsuperscript{164} Courts are generally unwilling to engage in speculation about future applications of existing practices or policies by a party to the litigation. \textit{See, e.g.}, City of L.A. v. Lyons, 461 U.S. 95, 109–10 (1983) (refusing to speculate about a police department’s future application of a chokehold policy).


\textsuperscript{166} 18 U.S.C. § 2702(b)(5).

\textsuperscript{167} However, irrespective of these agreements, webmail may receive the heightened ECS privacy protections in the Ninth Circuit and some districts within the Sixth Circuit because of those jurisdictions’ controversial views about the classification of opened webmail. \textit{See supra} notes 107–11 and accompanying text.

\textsuperscript{168} \textit{See supra} section II.C.
The ramifications of being excluded from the Stored Communications Act’s privacy protections are potentially significant for a customer. First, the government will have few restrictions on its ability to compel disclosure of a customer’s data. A user might try to resist by claiming a Fourth Amendment privacy right, but a similar defense has not prevailed in past cases involving e-mail. These precedents suggest that courts would be unlikely to extend constitutional protections into the realm of cloud computing. Second, only the contractual promises made in the cloud provider’s ToS agreement and privacy policy limit its ability to disclose a customer’s data to a third party. Unfortunately for customers, these protections are usually weak or nonexistent. Consequently, a cloud provider will have complete discretion in deciding whether to respond to requests, via subpoena or otherwise, for its customer’s data and personal identifying information. This would include disclosure to opposing parties in civil litigation that would otherwise be precluded entirely if the Act applied. Therefore, cloud computing users should carefully scrutinize these documents to understand the degree of resistance a cloud provider may be obligated to offer if their data is sought by the government or other third party.

V. CAN THIS BE WHAT CONGRESS INTENDED?

Not every cloud computing service will qualify for the Stored Communications Act’s (SCA) privacy protections. Rather than viewing this as a failure of the Act’s language to adapt to modern technology, this result is consistent with Congress’s desire to limit the scope of the Act’s protections. The SCA includes, for example, several prerequisites before a user’s content in a remote computing


170. See, e.g., Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), vacated, 532 F.3d 521 (6th Cir. 2008) (en banc) (vacating an earlier opinion holding that a Fourth Amendment privacy right exists in stored e-mail); United States v. Rodriguez, 532 F. Supp. 2d 332, 339–40 (D.P.R. 2007) (holding that there is no expectation of privacy in Internet transmissions or e-mail that has arrived at its recipient); United States v. Charbonneau, 979 F. Supp. 1177, 1184–85 (S.D. Ohio 1997) (holding that there is no expectation of privacy after an e-mail is received by its intended recipient, distributed widely, or sent to an undercover agent). The Government has argued that even if a Fourth Amendment privacy right does exist, the terms of service agreements used by many service providers would still authorize the disclosure of a customer’s e-mail to law enforcement. See Final Reply Brief for Defendant-Appellant United States of America at 13–18, Warshak, 490 F.3d 455, vacated, 532 F.3d 521 (No. 06–4092), 2007 WL 2085416.

171. See infra section VI.A.

172. See supra section IV.B.


174. See supra notes 93–95 and accompanying text.
service (RCS) receives the Act’s privacy protections. These requirements are a deliberate attempt by Congress to limit the Act’s reach, and when they are not satisfied, as is the case for many cloud providers, the Act’s protections are lost. Many cloud services are not within the Act’s coverage for the same reasons that Congress intended some computing services to lie beyond the Act’s reach in 1986. The legislative history and language of the Act clarify that Congress had two purposes in adopting the SCA: eliminating privacy concerns that might harm the development of new technology and applying the privacy principles that developed in Fourth Amendment jurisprudence to computer networks. To accomplish these goals, Congress made compromises and adaptations based on the unique characteristics of computer networks. But the Act’s final formulation plainly reflects a congressional desire for a narrowly tailored solution that would not apply to every computing service.

A. COMPETITION AND FREE MARKET DETERMINATIONS

Congress recognized early on that privacy considerations might limit the utilization of efficient, outsourced computing services. The Subcommittee on Courts, Civil Liberties, and the Administration of Justice explored these concerns in detail during its consideration of the Stored Communications Act. At one point during the hearings, an exchange occurred between committee members and P. Michael Nugent, who testified for Electronic Data Systems Corporation (EDS) and an industry group of RCS providers. Nugent opened his testimony with an overview of the need for the Act to protect privacy for both the RCS providers and their users:

We firmly believe, and it is a problem that is going to be growing as we go through the information age, that our customers should not lose their privacy rights and communication when relying on third party providers of data processing and data transmission services. The results of that, of course, are, we may lose business, so that’s why we’re here.

[I]f we do not accord or deal with these very basic [privacy] concerns, we may not get the business. Often, the hardware, the software, the technology, is as important to the customer as privacy protection; put it the other way, privacy protection is as important as the service that we perform. So, therefore, we believe that our customers shouldn’t lose their rights when they go outside for data processing and data transmission services as they must in this day and age.

175. See ECPA Hearings, supra note 75.
176. EDS, until being acquired in May 2008 by Hewlett-Packard, remained among the largest cloud computing providers, primarily serving large business and institutional users, with over one million cloud applications hosted on its infrastructure. See EDS Application Servs., Transform and Modernize Your Applications 7 (Dec. 2008), http://h10134.www1.hp.com/services/apps/downloads/apps_services_overview.pdf.
177. ECPA Hearings, supra note 75, at 76.
In a later follow-up question, Representative Boucher reinforced this message with a leading question, asking, “And so the absence of that protection creates a disincentive for individuals to use the new technology; would you agree with that?” After their legislative hearings, both the House and Senate Committees expressed their intent to address RCS clients’ privacy concerns in the SCA.

Congress wanted to deal with these privacy issues for two reasons. First, privacy concerns threatened the burgeoning RCS industry. Nugent emphasized this point in his prepared written statement to the House Subcommittee, arguing that the absence of RCS privacy protections may encourage construction of private networks among large companies or force smaller companies to choose between privacy and the competitive advantages offered by the new technology. Second, Congress believed ECS and RCS providers were competing at a disadvantage with other forms of communication, including the postal system and telephone networks. Congress frequently noted that computer networks were analogous to telephones and first-class mail, both of which enjoyed significant statutory or constitutional privacy protections. Indeed, the anomalous absence of privacy protections when a computer is used “in lieu of, or side-by-side with” these protected services provided much of the momentum for the Act’s introduction. At its core, the Act reflected Congress’s concern that the varying privacy protections offered to different mediums for transmitting or processing information might influence market forces in determining the viability of the new technology.

Neither of Congress’s concerns about ensuring a level playing field or fostering the growth of new technologies is implicated when applying the Act to cloud computing. Unlike the RCS providers that lobbied for the Act’s adoption, cloud providers have access to a statutory scheme that allows them to address customers’ privacy concerns. Of course, cloud providers may also choose to

---

178. Id. at 90.
179. See H.R. Rep. No. 99-647, at 19 (1986) (commenting that the questionable privacy protections available to users of computer networks “may unnecessarily discourage potential customers [from] using such systems”); id. at 65–66 (“This provision reflects the rapidly growing importance of information storage and processing to the Nation’s commerce. Today, the subject matter of commerce increasingly is information in electronic form and the processing of information itself has become a major industry. The secure storage of electronic information has thus become as important to the commercial system as the protection of paper records.”); S. Rep. No. 99-541, at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3559 (noting that the uncertain privacy protections “may unnecessarily discourage potential customers from using innovative communications systems” or “discourage American businesses from developing new . . . forms of telecommunications and computer technology”).
180. See ECPA Hearings, supra note 75, at 81 (“[O]nly those companies who were large enough and financially able to afford to maintain and operate their own private networks would be able to protect their privacy interests, and there would be a definite disincentive to the use of commercial systems, which is definitely not in the national interest.”).
182. See id.
183. See O’Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 87 (Ct. App. 2006) (“[A] fundamental purpose of the SCA is to lessen the disparities between the protections given to established modes of private communication and those accorded new communications media.”).
adopt a business model that opts out of the Act’s protections in exchange for the opportunity to access a customer’s data for advertising purposes. Whether users’ preference for more privacy will place the opt-out cloud providers at a competitive disadvantage will ultimately be decided by market forces—just as Congress intended.\textsuperscript{184} Whatever the result, it will not be the result of inequities in the federal legal regime.

\section*{B. CODIFYING THE FOURTH AMENDMENT}

After shifting its Fourth Amendment jurisprudence to a “reasonable expectation of privacy” framework in \textit{Katz v. United States},\textsuperscript{185} the Supreme Court decided a series of cases reiterating that the Fourth Amendment does not typically protect the privacy of information that is disclosed to a third party.\textsuperscript{186} These decisions caused concern that constitutional privacy protections may be lacking for computer networks and, particularly, remote computing services that were developing rapidly in the 1980s.\textsuperscript{187} In \textit{United States v. Miller}, for instance, the Court refused to apply the Fourth Amendment’s protections to copies of checks and deposit slips held by the defendant’s banks.\textsuperscript{188} Similarly, in \textit{Smith v. Maryland}, the Court held that a telephone number dialed from the defendant’s home was not within the Fourth Amendment’s scope.\textsuperscript{189} The Court reasoned in both cases that a person cannot have a reasonable expectation of privacy in information that is disclosed to a third party, such as a bank or telephone company.\textsuperscript{190} Computer networks necessarily involve a third-party service provider and the application of the third-party disclosure doctrine adopted in \textit{Miller} and \textit{Smith} suggested that the Fourth Amendment would not protect computer

\begin{flushright}
\textsuperscript{184} See infra note 262.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{187} See, e.g., Neil M. Richards, Essay, \textit{The Information Privacy Law Project}, 94 GEO L.J. 1087, 1117–19 (2006) (reviewing \textsc{Daniel J. Solove}, \textsc{The Digital Person: Privacy and Technology in the Information Age} (2004)) (noting that the result of the third-party disclosure cases is that “virtually all [electronic records] will remain unprotected by the Fourth Amendment”).
\end{flushright}

\begin{flushright}
\textsuperscript{188} \textit{Miller}, 425 U.S. at 440–43.
\end{flushright}

\begin{flushright}
\textsuperscript{189} \textit{Smith}, 442 U.S. at 742–46.
\end{flushright}

\begin{flushright}
\textsuperscript{190} Id. at 743 (“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. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.”); \textit{Miller}, 425 U.S. at 443 (“This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).
\end{flushright}
networks. Congress adopted the Stored Communications Act to respond to this perceived constitutional void. Congress relied extensively on existing Fourth Amendment jurisprudence to draft the Act’s electronic communications service (ECS) and remote computing service (RCS) privacy protections. For instance, Congress imposed a bright-line rule eliminating the warrant requirement for unopened communications stored by an ECS provider after 180 days—paralleling the Fourth Amendment concepts of abandonment and relinquishment of privacy interests. In § 2702(b)(8), Congress provided an exception allowing a provider to divulge a customer’s data when a “good faith” belief exists that “death or serious physical injury to any person requires disclosure.” This exception closely tracks both the principle and language of the exigent circumstances exception to the Fourth Amendment’s warrant requirement. The Court’s case law allowing a person to waive her privacy interests by consent is incorporated explicitly in § 2702(b)(3) and § 2703(c)(1)(C). The incorporation of these legal principles shows the extent to which Congress relied upon and codified the existing jurisprudence of the Fourth Amendment.

The unique characteristics of computer networks required Congress to alter the application of some Fourth Amendment principles. Certain of these modifications provide stronger privacy protections than the Fourth Amendment offers in comparable contexts. One notable area of strengthening occurred through the limitations placed upon the private search doctrine. The Court has long recognized the Fourth Amendment to be a constraint solely upon government actors; this leaves non-governmental actors free to invade the privacy of others on their own accord and share the evidentiary fruits of those invasions with the govern-

191. See S. REP. NO. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 (“Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.” (citing United States v. Miller, 425 U.S. 435 (1976))).


193. See, e.g., Abel v. United States, 362 U.S. 217, 241 (1960) (“There can be nothing unlawful in the Government’s appropriation of . . . abandoned property.”); cf. United States v. Thomas, 451 F.3d 543, 545–46 (8th Cir. 2006) (holding that the defendant abandoned his mail after failing to retrieve it from a rented postal box for one year and, therefore, destroyed any Fourth Amendment property interest in the mail).


195. See, e.g., Mincey v. Arizona, 437 U.S. 385, 392 (1978) (“The need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency.” (quoting Wayne v. United States, 318 F.2d 205, 212 (D.C. Cir. 1963))).

196. Compare 18 U.S.C. § 2702(b)(3), and 18 U.S.C. § 2703(c)(1)(C), with Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (“It is equally well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent.”).
But in § 2702(b)(7), Congress dramatically narrowed the opportunity for voluntary disclosure by computer network providers. Rather than the limitless cooperation allowed by the private search doctrine in the physical world, a computer network provider can only share users’ communications and data with the government when it relates to the commission of a crime and is discovered inadvertently. However, the third-party disclosure doctrine (reaffirmed in Miller and Smith), which initially motivated the Act’s adoption, presented Congress with its most difficult problem. Congress needed to determine when the third-party disclosure doctrine should yield, in whole or part, to allow computer network users to enjoy a protected sphere of privacy despite sharing their content with a third-party provider. The resulting legislative solution to this dilemma accounts for much of the Act’s complexity.

Congress found a helpful roadmap in the doctrinal approaches to privacy previously applied to the postal service and telephone system. Both communication mediums presented the same underlying conflict between Fourth Amendment principles and evolving societal expectations of privacy; in each case, the Judiciary—and ultimately Congress—decided that privacy should be protected under limited circumstances. Two factors defined the scope of the privacy interest: necessity and expectations. Courts recognized the necessity of using the postal service and telephone system for communication and commerce in modern society and the lack of practical alternatives for people wanting greater privacy. Additionally, courts considered users’ expectation that a mailed parcel or telephone conversation would not actually be exposed to a service provider during its transmission. Congress evaluated these same two criteria to guide its adaptation of the third-party disclosure doctrine for electronic communications and remote computing services.

197. See, e.g., United States v. Jacobsen, 466 U.S. 109, 113 (1984) (holding that the Fourth Amendment “proscribes only governmental action,” and does not apply to searches conducted by private individuals); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (“[T]he Fourth Amendment’s] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies . . . .”).


199. See supra notes 186–92 and accompanying text.

200. See H.R. REP. NO. 99-647, at 22 (1986) (noting the House committee’s belief that e-mail “combines features of the telephone and regular first class mail” and discussing three differences between these communication mediums that influenced the SCA’s development).

201. See Susan Freiwald, First Principles of Communications Privacy, 2007 STAN. TECH. L. REV. 3, ¶ 29 (arguing that the Katz decision depended “on the overriding importance of the telephone” and that “any other result would be destructive of society’s ability to communicate”); see also infra notes 205, 212.


203. See S. REP. NO. 99-541, at 2–3, 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 (discussing the importance of new communications and computer networking technology to individuals and commerce); id. at 5 (noting the statutory privacy protections for first-class mail and telephone calls, but
Since *Ex Parte Jackson* in 1877, the Court recognized a Fourth Amendment right to keep private the content of letters and sealed packages transmitted through the U.S. Postal Service. The Court understood that use of the mail system was no longer a voluntary decision that signaled a user’s willingness to share materials with a third-party service provider. Instead, the mail system had become a necessary aspect of modern life for interpersonal communication and commerce. The Court did not, however, provide complete privacy for letters and packages; a right to privacy remained intact only for the internal part of a letter or package that the sender sought to conceal. For example, newspapers and other open mailings exposed to the plain view of postal employees are not entitled to the Fourth Amendment’s privacy protections. Similarly, courts held that users expect the postal service to see the writings on the external part of a sealed parcel and there is no reasonable expectation of privacy in the information.

Telephone communications presented a similar privacy dilemma because they are transmitted over the telephone company’s infrastructure. When first confronted in 1928 with the issue of privacy in telephone conversations, the Court took a firm stance in *Olmstead v. United States* and held that the absence of a statute protecting privacy in computer networks, despite each of these communication mediums being used interchangeably by consumers and businesses.

204. See, e.g., *Ex Parte Jackson*, 96 U.S. 727, 732–33 (1877) (holding that Fourth Amendment protections apply to the internal contents of letters and sealed packages in the possession of the U.S. Postal Service). Although many of the postal service privacy cases were decided before *Katz* and the third-party disclosure cases that followed, their reasoning continues to be upheld after these shifts in Fourth Amendment jurisprudence. See, e.g., *United States v. Van Leeuwen*, 397 U.S. 249, 251–53 (1970) (noting the continued Fourth Amendment interest in the privacy of the contents of first-class mail after *Katz*); *United States v. Choate*, 576 F.2d 165, 174–80 (9th Cir. 1978) (applying the Court’s post-*Katz* framework and affirming prior case law holding that there is no Fourth Amendment privacy interest in the information appearing on the external parts of an envelope or package); see also Kerr, * supra* note 192, at 824 & n.126 (arguing that *Katz* actually caused little change in the Court’s previous approach to the Fourth Amendment).

205. See, e.g., *United States ex rel. Milwaukee Social Democratic Pub. Co. v. Burleson*, 255 U.S. 407, 437–38 (1921) (Holmes, J., dissenting) (noting that use of the second-class mail was essential for a newspaper publisher to remain in business); *Ex Parte Jackson*, 96 U.S. at 733 (noting that access to the mail or other modes of transportation was necessary to circulate a publication).

206. *Ex Parte Jackson*, 96 U.S. at 733 (“Letters and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.”).

207. *Id.* at 732–33 (“[A] distinction is to be made between different kinds of mail matter, [between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined.”)."

208. See, e.g., *United States v. Huie*, 593 F.2d 14, 15 (5th Cir. 1979); *Choate*, 576 F.2d at 174–80 (holding that there was no Fourth Amendment privacy interest in the information on the outside of a mailed package “because the information would foreseeably be available to postal employees and others looking at the outside of the mail”).

government’s wiretap on the defendant’s home telephone did not implicate a Fourth Amendment privacy interest. However, the ubiquity of telephone services by the 1960s caused the Court to reconsider its position and in *Katz* the Court found a valid Fourth Amendment privacy interest in a conversation over a public payphone. The technology had reached a societal tipping point and transitioned from a convenience to a modern-day necessity. Accordingly, the courts modified the Fourth Amendment’s scope to accommodate this change. Following the doctrinal path of the earlier mail cases, courts relied on a caller’s reasonable expectations to define the scope of privacy given to telephone communications. Consequently, courts found a Fourth Amendment privacy interest in the content of a telephone conversation but declined to extend privacy protections to the telephone number dialed to initiate the conversation.

Congress applied a looser analysis of the necessity and expectation factors in drafting the Stored Communications Act than courts had demanded for mail or telephone communications. When Congress adopted the Act in 1986, electronic communication systems had not become a necessity to the same degree that drove the Judiciary to enlarge privacy protections for mail and telephone services. Similarly, remote computing services were growing in popularity at the time of the Act’s adoption, but they were not necessary for businesses to compete effectively or survive. Congress’s willingness to construct privacy protections for computer networks—with the expectation that the requisite necessity would develop later—was a departure from the judicial practice of extending safeguards only after a service matured. Rather than anticipating the success of computer networks, Congress’s early embrace of the new technology may have become a self-fulfilling prophecy that catalyzed its widespread adoption. Ultimately, Congress’s decision to preemptively extend privacy protections to computer networks and outsourced computing services represented a more ambitious approach to privacy than the Court’s cautious “wait and see” attitude toward the postal service and telephone calls.

Congress adopted a more cautious approach in aligning the Act’s privacy protections with the privacy expectations of computer network users. The Act

---

211. 389 U.S. at 352–53.
212. *See id.* at 352 (“To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”).
213. *See id.* at 352–53.
214. *See Smith v. Maryland, 442 U.S. 735, 743 (1979).*
217. As Professor Kerr argues, there are many benefits to a statutory approach to privacy protections, including the development of policies on an ex ante basis and the ability to receive input and feedback from experts. Kerr, *supra* note 192, at 867–70, 875–82.
reflects a tiered compromise, creating a spectrum of privacy protections that apply to different types of information. The strongest protections were reserved for electronic communication services (ECS), such as e-mail, in § 2702(a)(1) and § 2703(a). Because ECS operates similarly to mail and telephone communications—both of which receive the full benefit of the Fourth Amendment under existing constitutional law—Congress reasoned that users would rightfully expect similar treatment for their e-mail communications.\textsuperscript{218} To the contrary, personal identification data that a network user voluntarily shares with a service provider receive the weakest protections under § 2702(c) and § 2703(c).

The remote computing service (RCS) functionality of computer networks, however, caused Congress to develop a mid-level tier offering a modest degree of privacy protections. Congress recognized that some user content is transmitted over a computer network to a service provider with the intent to store or process that data, rather than communicate it. Although the service provider’s servers hold the user’s content, she may not expect that it would be exposed to prying eyes.\textsuperscript{219} This unusual arrangement presented Congress with a situation in which analogies to existing precedents in the physical world broke down. Comparisons to sealed letters provided an awkward comparison at best because of the intangible nature of digital information. Prior privacy approaches to facilities that rent storage units also offered limited assistance because customers in those facilities could secure their possessions and deny access to the storage provider. Because the user shared the content with the service provider, the high level of protection given to ECS was unjustified, but in Congress’s view some degree of privacy was appropriate. The RCS category was therefore created to provide a limited set of privacy protections when a user has an actual, reasonable expectation that the service provider will not view her stored content.\textsuperscript{220}

Despite Congress’s liberalization of privacy protections in the SCA, many cloud providers rely on a business model that will run astray of the limitations in the Act. Congress did not express an unlimited tolerance for interaction between RCS providers and their customers; rather, Congress sought to preserve at least a modicum of privacy when users expect to maintain it. For instance, Congress specifically recognized that users’ privacy expectations remained intact when RCS providers stored or processed users’ data without


\textsuperscript{219} Encryption may ultimately remedy this problem in computer networks and, more specifically, in cloud computing. See Kerr, supra note 192, at 866 & n.389; Stephen J. Dubner, Bruce Schneier Blazes Through Your Questions, N.Y. Times, Dec. 4, 2007, http://freakonomics.blogs.nytimes.com/2007/12/04/bruce-schneier-blazes-through-your-questions/. However, the current lack of readily available encryption options for consumers and the inability of many cloud providers to support encryption limit their utility for constraining a cloud provider’s access to a user’s content.

\textsuperscript{220} With regard to the relationship between an RCS provider and a user’s content, the SCA requires that the content be in the provider’s possession “solely for the purpose of providing storage or computer processing” and that access to the content “not [be] authorized . . . for purposes of providing any [other] services.” 18 U.S.C. § 2702(a)(2)(B) (2006).
peering into its contents. But terms of service agreements empowering a cloud provider with far-reaching authority to access stored content, for marketing or other purposes, eliminate the user’s expectation of privacy that Congress considered critical. Thus, excluding many cloud computing services from the protections of the SCA is entirely consistent with Congress’s intent to limit the Act’s scope.

VI. WILL CLOUD COMPUTING BE A TIPPING POINT FOR ONLINE PRIVACY?

As most Americans move their personal content into the cloud, a corresponding increase in privacy protections seems appropriate. There are, however, significant obstacles to expanding privacy rights for cloud computing that widespread adoption alone cannot overcome. These judicial, legislative, and societal impediments make it unlikely that an enlargement of the Stored Communications Act or the protective scope of the Fourth Amendment will necessarily follow.

A. JUDICIAL OBSTACLES

The trajectory of Fourth Amendment jurisprudence suggests that courts are unlikely to enhance privacy protections for cloud computing users. Courts only rarely serve as the initial impetus for expanding privacy protections; when they do, it is typically through cautious extension of the Fourth Amendment,221 in response to societal or technological changes.222 Yet, since the 1960s, the Supreme Court has applied an even narrower view of the Fourth Amendment’s protections and the applicability of its remedies.223 The Court has focused its recent Fourth Amendment efforts on reexamining the costs and benefits of excluding evidence gathered in violation of the Fourth Amendment224 and limiting the range of situations that invoke the Fourth Amendment’s protections.225 Given the current state of its Fourth Amendment jurisprudence, it seems unlikely that the Court will drastically expand the scope of privacy protections for Internet users—after failing to accept an Internet-related privacy

221. See Kerr, supra note 192, at 807 (“[C]ourts rarely accept claims to Fourth Amendment protection in new technologies that do not involve interference with property rights, and have rejected broad claims to privacy in developing technologies with surprising consistency.”).
223. See, e.g., Thomas Y. Davies, Correcting Search-and-Seizure History: Now-Forgotten Common-Law Warrantless Arrest Standards and the Original Understanding of "Due Process Of Law," 77 Miss. L.J. 1, 218–19 (2007) (“[A]lthough the Supreme Court resurrected search-and-seizure rights in the form of the Fourth Amendment during the early part of the twentieth century, the Justices have subsequently dismantled the substance of those rights, especially during the last four decades.”).
case for more than two decades. Not only would this significantly change the dimensions of the Fourth Amendment’s scope, it would likely require reassessing core privacy principles, such as the third-party disclosure doctrine, that would have repercussions beyond the digital world.

Without meaningful guidance from the Supreme Court, lower courts are in disarray with respect to privacy interests in computer networks. Federal courts cannot reach consensus on the privacy protections applicable to e-mail; for instance, a circuit split currently exists over the categorization of e-mail within the Stored Communications Act. Courts have also struggled to determine if the Fourth Amendment protects e-mail. In *Warshak v. United States*, the Sixth Circuit held that the Fourth Amendment protected a person’s e-mail from government searches and seizures, only to retract the opinion a short time later in an en banc decision that avoided the issue. In *United States v. Maxwell*, an earlier case heard by the Court of Appeals for the Armed Forces, the Fourth Amendment was also held to apply to e-mail, but other courts have discounted its precedential value. These cases reflect the degree of uncertainty among lower courts about how the SCA and Fourth Amendment apply to e-mail—making it unlikely that they can proceed anytime soon to the thornier issues surrounding communications and stored data in cloud services.

Judicial modification of online privacy protections is further complicated by the Act’s existence. Despite the eloquence of the two-prong test developed in *Katz v. United States*, “the phrase ‘reasonable expectation of privacy’ is essentially a legal fiction that masks a normative inquiry into whether a particular law enforcement technique should be regulated by the Fourth Amendment.” The SCA, however, reflects Congress’s own normative judgment about the appropriate degree to which a person’s privacy interests should be protected in an online environment. The lack of a contrary societal or judicial consensus with respect to online privacy issues further suggests that Congress’s solution might be the best of the imperfect options available. At the very least,

---

226. See, e.g., Kerr, supra note 192, at 831 (arguing that “courts generally do not engage in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies”); Richards, supra note 187, at 1118 (“Moreover, the Court has been loath as a general matter to read the protections of the Fourth Amendment broadly in the context of new technologies.”). But see Mulligan, supra note 78, at 1595–96 (“With respect to files on third-party servers, the case law supporting reasonable expectations of privacy in rented physical spaces and in computers and files stored on them, turned over for repair, suggest that electronically stored personal files on an RCS would fall within the zone of privacy protected by the Fourth Amendment.”).

227. See supra notes 107–11 and accompanying text.

228. 490 F.3d 455 (6th Cir. 2007), vacated, 532 F.3d 521 (6th Cir. 2008) (en banc).


231. 389 U.S. 347, 361 (Harlan, J., concurring).

there is nothing to suggest that Congress’s view departs from societal norms so spectacularly that it contradicts constitutional privacy principles. Consequently, there is little basis upon which the Court might render the SCA unconstitutional—either directly or implicitly—and be tempted to substitute Congress’s balancing act with its own normative inquiry under the guise of Fourth Amendment jurisprudence.

B. LEGISLATIVE OBSTACLES

Congress has expanded privacy protections several times when the use of a new technology was not addressed by the courts or was held to be unprotected. Indeed, some of Congress’s broadest expansions of privacy protections have followed the Court’s unwillingness to do so.233 After Olmstead v. United States, in which the Court held that the Fourth Amendment did not apply to telephone communications,234 Congress responded by proscribing wiretapping in the Communications Act of 1934.235 Similarly, Congress adopted the Pen Register Act236 to respond to Smith v. Maryland, which held that the Fourth Amendment did not extend to telephone numbers processed by a telephone company’s automated routers.237 In other instances, such as the provisions covering remote computing services in the Stored Communications Act, Congress has injected new privacy protections before the courts have had an opportunity to consider them.238

Although Congress has historically favored the enlargement of privacy protections, it is unlikely to lead the fight to expand online privacy. Congressional inertia can be overcome when the right combination of variables intersect, including political momentum and societal demand.239 Two main obstacles currently prevent these variables from aligning for online privacy issues. First, the SCA itself impedes the adoption of new privacy measures by shrinking the gap between the existing and ideal degree of privacy protections that Congress might want. Second, recent congressional actions are reducing the sphere of

233. Kerr, supra note 192, at 857 (“[S]ince the 1960s Congress rather than the courts has shown the most serious interest in protecting privacy from new technologies.”). Professor Kerr argues that “legislatures often are better situated than courts to protect privacy in new technologies” because of their ability to respond to technological changes more rapidly, gather additional information, and consider the context of the technology’s application and future development. Id. at 806–08, 888.
234. 277 U.S. 438, 466 (1928).
238. See H.R. Rep. No. 99-647, at 23 (1986) (“[R]emote computing services are still relatively new, and there is no case law directly on point.”); see also Anuj C. Desai, Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy, 60 Stan. L. Rev. 553, 577 (2007) (arguing that Ex Parte Jackson merely constitutionalized the privacy protections that the Continental Congress adopted for the U.S. mail system in 1792).
239. See William N. Eskridge, Jr., Dynamic Statutory Interpretation 151–52 (1994).
individual privacy, especially after the September 11, 2001 terrorist attacks, rather than seeking its expansion.\textsuperscript{240}

The SCA limits the political value of tackling online privacy issues and, therefore, obstructs efforts to adopt stronger protections. Congress has a limited capacity to pursue new legislation and it is hard to get its finite attention focused on a particular issue. Consequently, seeking incremental change in a previously legislated subject area is particularly difficult.\textsuperscript{241} The SCA already provides some quantum of privacy in online communications and content, but as society embraces new technologies, including cloud computing, the balance that the Act struck more than two decades ago may no longer be appropriate. But aligning the SCA’s provisions with current mainstream views about online privacy would not require dramatic changes that would generate substantial public attention. Instead, such an effort would likely involve making incremental enhancements to the Act’s structure, clarifying issues of judicial dispute, or modernizing statutory language.\textsuperscript{242} Because of the limited political return such modest changes would offer, politicians have few incentives to advocate for them.

The SCA also influences societal expectations about online privacy and thus minimizes the political pressure for change. Societal forces can cause both Congress and the courts to revisit privacy protections. Within the judicial realm, the Court held in \textit{Katz v. United States} that privacy issues under the Fourth Amendment focus on whether society is prepared to recognize an expectation of privacy under certain circumstances as being reasonable.\textsuperscript{243} This approach makes it difficult for privacy advocates to advance their interests because of the circularity in using societal expectations to define new legal protections for individual privacy when those expectations are influenced by existing legal protections.\textsuperscript{244} In the same circular manner, the SCA’s privacy standards subtly influence societal norms when they are reflected in media reports, judicial

\begin{footnotesize}
\begin{enumerate}
\item See, e.g., Mulligan, supra note 78, at 1596–98.
\item Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring) (“[T]here is a twofold requirement, 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.’”).
\item See Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) (recognizing that government action influences expectations of privacy). The circularity is indirect though, and courts suggest that statutes do not reflect a per se threshold of societal expectations. See United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999), aff’d, 225 F.3d 656 (4th Cir. 2000) (unpublished table opinion) (“Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of ‘reasonably objective’ for Fourth Amendment purposes.”).
\end{enumerate}
\end{footnotesize}
decisions, and terms of service agreements.\textsuperscript{245} In the legislative realm, the lack of a significant disparity between societal privacy expectations and the SCA's existing protections minimizes the political pressure to bring about change. Political action is motivated when constituencies expand and engage their members to generate enough momentum to attract attention.\textsuperscript{246} Yet, privacy issues attract a limited natural constituency and building a large coalition of interested online users to generate political change is difficult\textsuperscript{247}—particularly when the SCA's existing statutory scheme continues to define and reinforce societal norms about online privacy.

Even if there is societal demand for greater online privacy protections, elected officials and judges need to recognize that a shift in expectations has happened. However, the demographics of Congress and the Judiciary make it unlikely that their members are well-positioned to determine society’s expectations, especially about emerging technologies. Younger people are much more likely to embrace cloud computing services,\textsuperscript{248} but the average age of senators\textsuperscript{249} and House members\textsuperscript{250}—as well as the Justices\textsuperscript{251} on the Court—reflects a notable generational gap from this core user population. Advocates for enhanced online privacy measures will have to bridge this divide and ensure that elected officials and judges understand the technology and its implications for individual privacy before they can secure their assistance in changing the status quo.

\textsuperscript{245. United States v. Drew}, 259 F.R.D. 449 (C.D. Cal. 2009), offers a timely example of this phenomenon. Few people are likely familiar with the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (Supp. 2009), used to convict Drew, yet the resulting guilty verdict and media reports powerfully communicated to society the seriousness of violating a website’s terms of service agreement under federal law. See, e.g., Jennifer Steinhauer, Woman Found Guilty in Web Fraud Tied to Suicide, N.Y. TIMES, Nov. 27, 2008, at A25. After the jury’s verdict, the district court concluded that a “CFAA misdemeanor violation . . . [for] the conscious violation of a website’s terms of service runs afoul of the void-for-vagueness doctrine” and reversed her conviction. \textit{Id.} at 464. But the court suggested that the CFAA's civil penalties or felony provisions might still be permissible for such violations. \textit{Id.} at 464–67.

\textsuperscript{246. See, e.g., Anthony Downs, Up and Down with Ecology—The “Issue-Attention Cycle,” PUB. INT., Summer 1972, at 38, 38–41 (proposing a five-stage process through which public attention is focused on an issue and political action results).}

\textsuperscript{247. See Lew McCready, What Was Privacy?, HARV. BUS. REV., Oct. 2008, at 123, 126 (“[S]omeone will always have to speak for privacy, because it doesn’t naturally rise to the top of most consideration sets, whether in government or in the private sector.”).}

\textsuperscript{248. Compared to Internet users over sixty-five years old, Internet users under thirty years old are twice as likely to use cloud computing applications, nearly three times more likely to use webmail and online file storage, and seven times more likely to store personal videos online. HORRIGAN, supra note 50, at 5. These differences are further magnified when Internet utilization rates among the differing age groups are factored into account. \textit{Id.}}

\textsuperscript{249. In the 111th Congress, the average age of a senator was 63.1 years—an increase of more than three years since the 109th Congress. MILDRED AMER & JENNIFER E. MANNING, CONGRESSIONAL RESEARCH SERV., MEMBERSHIP OF THE 111TH CONGRESS: A PROFILE 1 (2008).}

\textsuperscript{250. In the 111th Congress, the average age of a representative was 57 years—an increase of almost two years since the 109th Congress. \textit{Id.}}

\textsuperscript{251. At the beginning of the Court’s 2009 Term, the average age of the nine Justices was 67.9 years. See \textit{THE JUSTICES OF THE SUPREME COURT} (2009), http://www.supremecourtus.gov/about/biographiescurrent.pdf.}
C. SOCIETAL OBSTACLES

A final obstacle to strengthening online privacy protections is the changing societal attitude toward online privacy. Younger generations have much less concern about online privacy than older generations. This divergence is partially attributable to the different ways that each generation uses the Internet. Older users generally rely on the Internet for transactional encounters, such as gathering information from websites, exchanging direct communications via e-mail, managing personal finances, and purchasing goods. In contrast, younger users are more likely to embrace the Internet’s interconnectedness and convenience by participating in social networking, sharing digital content, and using cloud services.

The generational differences in Internet usage are shifting societal calculations about the value of online privacy. Privacy involves a tradeoff with other competing values, such as cost, convenience, efficiency, and networking. The widespread use of cloud computing services by younger generations is driven extensively by these latter values. Popular social networking sites, such as Facebook and MySpace, necessarily involve the public (or semi-public) sharing of personal information and content with a network of other users. For users of these services, the value of networking and communicating with others outweighs the intangible costs to their personal privacy. Older Internet users

252. See A Special Report on Social Networking: Privacy 2.0, ECONOMIST, Jan. 30, 2010, at 12, 12–13 (hereinafter Privacy 2.0] (summarizing recent comments by Mark Zuckerberg, the Chief Executive Officer of Facebook, arguing “that social norms ha[ve] shifted and that people ha[ve] become willing to share information about themselves more widely”).


255. See id. at 3; JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 231 (2008) (“People [born after 1985] routinely set up pages on social networking sites—in the United States, more than 85 percent of university students are said to have an entry on Facebook—and they impart reams of photographs, views, and status reports about their lives, updated to the minute.”).

256. See FRED H. CATE, PRIVACY IN THE INFORMATION AGE 102 (1997) (arguing that privacy conflicts with important values, including “society’s interest in free expression, preventing and punishing crime, protection of private property, and the efficient operation of government”).

257. See Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Cal. App. 2009) (noting that an individual had no reasonable expectation of privacy when she posted material on MySpace, even if she “expected a limited audience,” because the material is “opened . . . to the public at large” and the “potential audience was vast”).

have fewer incentives to bargain away their privacy. When sending personal communications or transacting business on the Internet, fears about identity theft and confidentiality place a premium on protecting personal information. Furthermore, older users may have a better appreciation for privacy’s benefits and the consequences that might follow from allowing too much personal information to circulate in the digital realm.  

Expecting to receive something for “free” from cloud providers is also reducing users’ privacy expectations. One sign of this change is users’ growing comfort, especially among younger users, with cloud providers analyzing the content of websites they visit in order to deliver targeted advertising. From a market-based perspective, the frequency with which Internet users of all ages are willing to expose their online activities or exchange their personal data for free services and content suggests that they assign a low market value to their privacy. Additionally, if people truly want greater privacy protections, one would expect cloud providers to compete to offer consumers better protections; instead, new users continue streaming toward Google and other cloud providers to partake in their advertising-sponsored offerings.

The generational gap in privacy expectations and embrace of free services from cloud providers suggest little opportunity to generate societal momentum for greater online privacy protections. Younger generations are less concerned with personal privacy than older generations and are likely to carry those views forward as they gradually assume society’s reins in the future. The expanding business model of exchanging privacy for free access to cloud providers’ offerings will also continue to reduce the perceived market price of individual privacy. Thus, the likelihood for building a societal consensus about the need for heightened online privacy protections is gradually slipping away.

and for good reason—the reality is that most of us, most of the time, really don’t care. Or, rather, if accessing useful services or getting work done more efficiently requires some privacy concessions, we gladly concede.

259. See Palfray & Gasser, supra note 253, at 63–64 (arguing that parents and teachers should educate younger generations about the potential long-term consequences of posting their intimate personal details on the Internet).

260. See Anderson, supra note 121, at 194 (describing the increasing availability of free digital services and the business model for such services).

261. See Privacy 2.0, supra note 252, at 13 (“Most people who use Facebook and other social networks seem prepared to accept the idea of targeted advertising as the price of getting free access to the service.”); Harris Interactive, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles, http://www.harrisinteractive.com/harris_poll/index.asp?PID=894 (last visited Feb. 12, 2010) (finding that 49% of eighteen-to thirty-one-year olds are comfortable with cloud providers using their online activity to display contextual advertising or content, while just 31% of Internet users over the age of sixty-two approved).

262. See Reihan Salam, Good Guys Don’t Make Billions, SLATE, Feb. 26, 2008, http://www.slate.com/id/2185113/ (“The vision of immaculate capitalism, in which no one gets screwed and everyone gets awesome, free stuff, is as old as capitalism itself. The trouble is that filthy lucre needs to change hands at some point, or else capitalism goes kaput.”). But see Steven Hetcher, Changing the Social Meaning of Privacy in Cyberspace, 15 Harv. J.L. & Tech. 149, 174 (2001) (“[D]ue to the efforts of norm proselytizers and norm entrepreneurs, the demand for privacy among consumers has surged.”).
CONCLUSION

The business model embraced by many cloud computing providers is incompatible with the requirements of the Stored Communications Act. A provider’s authorization to access a customer’s data, for the provision of contextual advertising or other purposes, will likely disqualify that customer from receiving the Act’s privacy protections. As a result, courts will need to carefully scrutinize a cloud provider’s terms of service agreement and privacy policy to determine the degree to which it is authorized to access customers’ data. A brief analysis of the agreements currently used by Google and several other cloud providers confirms that many users will ultimately discover they are outside the boundaries of the SCA and their data is vulnerable to disclosure.\textsuperscript{263} Although unsettling, this result is consistent with Congress’s doctrinal approach in drafting the Act to limit its protections to certain contexts. Yet, despite the growing popularity of cloud computing services, there appears to be little opportunity for judicial or legislative relief in the near future. Professor Kerr notes that “there are many problems of Internet privacy that the SCA does not address.”\textsuperscript{264} It appears that cloud computing is one of them.

\textsuperscript{263} See supra section IV.B.

\textsuperscript{264} Kerr, supra note 2, at 1214.