TXTS R SAFE 4 2DAY: *QUON V. ARCH WIRELESS* AND THE FOURTH AMENDMENT APPLIED TO TEXT MESSAGES

Alyssa H. DaCunha[*]

INTRODUCTION

Since its birth in 1992,[1] the text message has become a part of life for over 270 million Americans.[2] It is how they vote for their American Idols,[3] remind their political constituents to vote,[4] send their friends and relatives holiday greetings,[5] order pizzas,[6] and learn about their travel delays.[7] In one month alone, U.S. cell phone users send 110 billion text messages,[8] and Americans now send more text messages than they make phone calls.[9] In August 2008, in a move that certified the text message's mainstream legiti-

[*] George Mason University School of Law, Juris Doctor Candidate, May 2010; Editor-in-Chief, GEORGE MASON LAW REVIEW, 2009-2010; George Washington University, B.A. International Affairs, *summa cum laude*, Jan. 2006. I would like to thank Professor Neomi Rao for her insight and assistance with this Note, and Phillip DaCunha for his constant patience and support.

[1] Victoria Shannon, *15 Years of Text Messages, a 'Cultural Phenomenon'*, N.Y. TIMES, Dec. 5, 2007.

[2] *See* CTIA—THE WIRELESS ASSOCIATION, WIRELESS QUICK FACTS, YEAR END FIGURES [hereinafter CTIA YEAR END FIGURES], http://www.ctia.org/advocacy/research/index.cfm/AID/10323 (last visited Aug. 11, 2009) (reporting that 270.3 million Americans have cell phones as of December 2008); JOHN HORRIGAN, PEW INTERNET & AMERICAN LIFE PROJECT, MOBILE ACCESS TO DATA & INFORMATION 2 (March 2008), http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Mobile .Data.Access.pdf.pdf (indicating that 58 percent of Americans with cell phones have sent or received a text message); *see also* Philip L. Gordon, *Text Messaging in the Workplace Poses New Challenges for U.S. Employers and Global Businesses with U.S. Operations*, 7 Privacy & Sec. L. Rep. (BNA) 1483 (Oct. 13, 2008) ("Describing the recent growth of text messaging in the United States as explosive would be an understatement.").

[3] AmericanIdol.com, Frequently Asked Questions, http://www.americanidol.com/faq/ (last visited Sept. 5, 2009).

[4] Garrett M. Graff, Op-Ed., *Text the Vote*, N.Y. TIMES, Aug. 12, 2008, at A21.

[5] Shannon, *supra* note 1.

[6] PapaJohns.com, SMS Ordering, http://www.papajohns.com/sms/index.shtm (last visited Sept. 5, 2009).

[7] Shannon, *supra* note 1.

[8] CTIA YEAR END FIGURES, *supra* note 2.

[9] Marguerite Reardon, *Americans Text More Than They Talk*, CNET NEWS, Sept. 22, 2008, http://news.cnet.com/8301-1035_3-10048257-94.html.

macy, the Democratic nominee for president announced his running-mate via an early-morning text message to supporters.[10]

Because text messages have assumed a place of prominence in modern personal communications, they are an increasingly integral part of law enforcement surveillance.[11] When courts are called upon to examine the propriety of a given search or surveillance, they are faced with a maze of case law interpreting both precedent and statutory protections in a variety of ways.[12] The Fourth Amendment, the traditional guardian of homes, papers, and persons, defines the contours of proper searches and seizures.[13] However, a series of cases in the 1970s created an exception to Fourth Amendment protections for papers turned over to a third party. Under the third-party disclosure exception, law enforcement does not execute a search for Fourth Amendment purposes where the expectation of privacy in papers has already been diminished by disclosure to an outside party.[14]

In the realm of electronic communications,[15] the third-party disclosure rule has interesting implications: all correspondence and files must pass through a third-party network provider to reach the recipient, and copies of the communications are stored indefinitely on the provider's servers.[16] Thus, the technology required to send text messages raises a question as to whether the files have been "disclosed" to a third party. If the disclosure exception applies, an individual has no reasonable expectation of privacy in

---

10 Adam Nagourney & Jeff Zeleny, *Obama Chooses Biden as Running Mate*, N.Y. TIMES, Aug. 23, 2008, at A1.

11 *See, e.g.*, United States v. Jackson, No. 07-0035, 2007 U.S. Dist. LEXIS 80120 (D.D.C. Oct. 30, 2007). In *Jackson*, the defendant was convicted of wire fraud and allegedly text messaged a friend to ask him to vouch for a letter the defendant submitted under his name to the court as part of her sentencing hearings. *Id.* at *2, *3-4. Law enforcement sought copies of the contents of her texts in order to investigate her improper contact with a witness. *Id.* at *4.

12 *See infra* Part I.C.

13 U.S. CONST. amend. IV. Note that the Fourth Amendment only limits state action and does not apply to the actions of private citizens or organizations. *See generally* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE 77 (8th ed. 2007).

14 *See infra* Part I.B.1.

15 A note regarding methodology is appropriate here. While this Note addresses a recent development in search and seizure law as it relates to text-messaging, much of the scholarly support for the Note comes from cases and articles addressing other forms of electronic communications, most notably e-mail. Due to the practical differences between e-mail and texts, developments in search and seizure law will affect different segments of the population depending on whether the development affects e-mail or texts. *See infra* notes 35-40 and accompanying text (discussing why the ubiquity and inexpensiveness of cell phones make text messages available to a broader range of the population). However, there are no material differences between the underlying technologies that are sufficiently substantive to change the legal analysis. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472) (explaining why the analysis for e-mails and text messages is substantively identical). Thus, while this Note will focus primarily on text messages, its analysis applies equally to e-mails and other electronic communications that rely on network transmission.

16 *See infra* Part I.A.

the text messages and law enforcement will not violate the Fourth Amendment by obtaining and reading the communications through internet surveillance.[17] Faced with this open question with regard to e-mails, Congress enacted the Stored Communications Act ("SCA") in 1986 to protect electronic communications by requiring the government to comply with certain procedures before obtaining the communications.[18] Unfortunately, by codifying the early 1980s state of network technology, Congress created a statute that proved difficult for courts to apply as new technologies arose, and no coherent body of case law has emerged to guide courts in applying the statute.

Until recently, all circuits to consider the issue had concluded that electronic communications were not constitutionally protected from internet surveillance.[19] However, the Ninth Circuit set a new course in its 2008 decision in *Quon v. Arch Wireless*.[20] Basing its decision on both statutory and constitutional grounds, the Ninth Circuit held that the plaintiff had a reasonable expectation of privacy in his text messages.[21] The Court then applied a stringent test to determine the reasonableness of the search[22] and interpreted the Fourth Amendment to grant broad privacy protections to text messages.[23] In so doing, it split with all other circuits that have examined the issue, none of which have used the Constitution as a source of protection for electronic communications obtained through surveillance.[24] By

---

17 This Note uses the term "internet surveillance" to refer to any means by which the government accesses the contents of electronic communications that travel through computer networks. This is the term commonly used in scholarly literature despite being a misnomer in two aspects. First, this surveillance may target electronic communications that travel in networks other than the internet, such as cellular communications networks; and second, law enforcement may obtain communications through methods that are not traditionally considered "surveillance," such as relying upon legal process in compelling production of the communications from service providers, rather than surreptitiously gaining access to them without the knowledge of their owner. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1381 (2004).

18 18 U.S.C. §§ 2701-2712 (1986). The statute is referred to in various ways: it comprises Title II of the Electronic Communications Privacy Act ("ECPA"), so commentators sometimes refer to the statute as either Title II or, more generally, as the ECPA. *See, e.g.*, William R. Corbett, *Awaking Rip Van Winkle: Has the National Labor Relations Act Reached a Turning Point?*, 9 NEV. L.J. 247, 258 (2009). This Note refers to the statute's specific name ("SCA" or "the statute").

19 *See infra* Part I.C.3.

20 529 F.3d 892, 905 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

21 *Id.* at 909.

22 *Id.* at 908 ("[I]f less intrusive methods [for the search] were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the government's legitimate purposes . . . the search would be unreasonable . . . ." (quoting Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1336 (9th Cir. 1987))).

23 *Id.*

24 *See* Warshak v. United States, 532 F.3d 521, 526-27 (6th Cir. 2008) (vacating a previous Sixth Circuit decision that had found e-mails protected by the Constitution); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005) ("[A]n

holding that individuals have a reasonable expectation of privacy in their text messages and applying a reasonableness inquiry that adequately weighted the privacy interests of the individual, the Ninth Circuit in *Quon* forged a path towards constitutional protections for text messages and illustrated the inadequacy of the SCA.

This Note examines both the constitutional and statutory protections for text messages and argues that the current statutory protections are weak, outdated, and violate the Fourth Amendment by allowing law enforcement to search personal electronic communications with fewer procedural protections than are required for traditional forms of communication such as the telephone and postal mail. The interplay between the SCA and the Constitution is a topic that has received little attention from scholars, but is of critical importance to courts faced with this issue with increasing frequency.[25] Part I of this Note explains the basic technology at issue, the significant facets of Fourth Amendment protection, and the SCA. It also reviews the interpretation of the statute by various courts and examines the discrepancies in their holdings. Part II examines the Ninth Circuit's holding in *Quon v. Arch Wireless*. Part III analyzes the significance of *Quon* and argues that, despite lapses in the Ninth Circuit's reasoning under the statute, its decision on the constitutional issues properly restores the Fourth Amendment to the forefront of protecting modern personal electronic communications. Part IV gives a practical guide for applying the Ninth Circuit's approach and concludes by identifying several outstanding questions.

I. BACKGROUND

A. *What is a Text Message?*

In December 1992, engineer Neil Papworth made history by typing the words "Merry Christmas" on his computer keyboard and sending his holi-

individual sending an e-mail loses 'a legitimate expectation of privacy . . . .'" (quoting Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001))); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers . . . . [T]hey may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient."); United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002). The Fifth Circuit examined the issue of constitutional protections for text messages within the context of a search incident to arrest and determined that an individual has an expectation of privacy within that context; the Fifth Circuit has yet to determine whether constitutional protections apply to text messages accessed through internet surveillance. *See* United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007); *see infra* Part I.B.3 (reviewing those circuits that have addressed the issue).

25 Bellia, *supra* note 17, at 1379 (noting that "[b]ecause the scholarship largely ignores statutory issues, or the interplay between the statutory and constitutional issues, courts do not receive needed guidance for applying the surveillance statutes").

day greeting to a fellow engineer's cell phone.[26] It would be several more years before standard cell phones would have the capacity to send and receive alphabet characters and before cell phone companies adapted their billing programs to offer text-messaging to their customers.[27] However, by 2000, U.S. wireless subscribers were sending an average of 14.4 million text messages per month, a figure that has continued to grow steadily.[28]

A text message, or short message service ("SMS"), allows a user to send a message consisting of a maximum of 160 characters from a cell phone or computer to another cell phone.[29] When a wireless user presses "send" on a text message, the message is transmitted to the wireless network, which stores the message in a centralized location and forwards the message to a cell phone tower for transmission to the recipient's cell phone.[30] The network provider retains a copy of the text message indefinitely, allowing messages to be sent even when the recipient's phone is turned off or out of range.[31] After delivery, the network provider retains the message in an archived form as a service to the user in case of data loss or the loss or breakage of a phone.[32]

Although the text message's swift rise to ubiquity surprised many,[33] its popularity can be explained by four key factors. First, several characteristics of the text make it remarkably convenient. Text messages can be sent and received from any location and do not require access to technology other than a cell phone, making it an extremely mobile form of communication.[34] Second, the prevalence of cell phones allows a broad range of the population easy access to the technology needed to send and receive text messages. Unlike e-mail, the hardware needed to send a text message is inexpensive; pre-paid cell phones may be purchased for under $40 at many

---

26 Shannon, *supra* note 1.

27 *Id.*

28 CTIA YEAR END FIGURES, *supra* note 2. By December 2005, Americans were sending 9.8 billion text messages per month, and the most recent figures indicate that Americans now send over 110 billion text messages per month. *Id.*

29 HowStuffWorks.com, How SMS Works, http://communication.howstuffworks.com/sms.htm (last visited Sept. 6, 2009); *see also* Yuki Noguchi, *Life and Romance in 160 Characters or Less*, WASH. POST, Dec. 29, 2005.

30 HowStuffWorks.com, *supra* note 29.

31 HowStuffWorks.com, SMS Advantages, http://communication.howstuffworks.com/sms1.htm (last visited Aug. 21, 2009).

32 The length of time that a message is stored varies by provider. *See* Jacob Leibenluft, *Do Text Messages Live Forever?*, SLATE, May 1, 2008, http://www.slate.com/id/2190382 (explaining that AT&T Wireless keeps text messages for forty-eight hours, whereas Sprint keeps them for two weeks).

33 Shannon, *supra* note 1 ("[F]ew people in telecommunications believed at the time that it would take off as a communications medium of its own.").

34 Donna Reid & Fraser Reid, *Insights into the Social and Psychological Effects of SMS Text Messaging* at 1 (Feb. 2004), http://www.160characters.org/documents/SocialEffectsOfTextMessaging.pdf.

drugstores.[35] Thus, individuals without home computers or consistent internet access are still able to send text messages for a minimal capital outlay.[36] Third, text messages are an ideal platform for a variety of popular and profitable cell phone applications such as games, travel alerts, stock market updates, shopping, weather alerts, traffic updates, promotional endeavors, and driving directions,[37] and are a cost-effective method of increasing voter turn-out.[38] Finally, network providers have an incentive to encourage communication through text messages, as texts utilize higher frequency bandwidths that are unsuitable for voice communication and serve little other functional purpose.[39] Accordingly, most wireless providers charge only a low monthly fee for an unlimited number of text messages.[40] The negligible marginal cost of sending a text contributes to its status as one of the cheapest methods of communication. As a result of their ease of use, accessibility, and low cost to both users and providers, text messages have assumed a prominent role in modern personal communications.

B. *Constitutional Protections for Communications: The Fourth Amendment*

1. Creation and Development of Fourth Amendment Protections

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

---

35 This amount is based on a visit to three drugstores in the Northern Virginia area between September 10, 2008 and October 29, 2008.

36 This is largely attributable to the price difference between home computers and cell phones; the lower price of cell phones allows more individuals access to cellular technology as opposed to internet technology. A Pew Research Center study published in June 2008 revealed that 83 percent of adult Americans have cell phones (and thus have the capacity to send text messages), whereas only 77 percent of adult Americans have home computers, and 6 percent of that group does not have internet access. THE PEW RESEARCH CENTER FOR PEOPLE & THE PRESS, BIENNIAL MEDIA CONSUMPTION SURVEY Question 94A (Apr. 2008), http://people-press.org/questions/?qid=1714987&pid; THE PEW RESEARCH CENTER FOR PEOPLE & THE PRESS, BIENNIAL MEDIA CONSUMPTION SURVEY Question 93A (Apr. 2008), http://people-press.org/questions/?qid=1714986&pid.

37 HowStuffWorks.com, *supra* note 32; Shannon, *supra* note 1.

38 Graff, *supra* note 4, at A21.

39 *See* Tom Clements, *SMS—Short but Sweet*, SUN DEVELOPERS NETWORK, Feb. 2003, http://developers.sun.com/mobility/midp/articles/sms; *see also* Reardon, *supra* note 9 ("[I]n the U.S. texting is proving to be a cash cow for carriers.").

40 These data are based on research conducted on October 19, 2008, for zip code 22043 (Falls Church, Va.) at the websites for Verizon Wireless, Sprint Wireless, and AT&T Wireless.

> probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[41]

The structure of the Amendment reflects the Framers' view that the people's interests were best served by a government of distinct branches that checked each other's power.[42] The requirement that the executive branch obtain a warrant by demonstrating probable cause to an objective judge or magistrate creates a check on the executive branch's power and protects the privacy of the public.[43]

One of the first cases to challenge the boundaries of the Fourth Amendment was *Ex parte Jackson*[44] in 1878, in which the Supreme Court examined the constitutional protections on private papers in transit through

---

41 U.S. CONST. amend. IV. The creation of the Fourth Amendment was the product of deep-seated colonial frustration over abusive search privileges under both the English common law and American colonial governments. *See generally* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT OF THE UNITED STATES CONSTITUTION (1937); ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT (2006). At English common law, the sheriff had the right to enter a suspect's home and search his home, person, and papers, provided that the King was a party to the case and the sheriff first knocked and announced his presence. *Semanyne's Case*, (1604) 77 Eng. Rep. 194, 195 (K.B.) ("[T]he house of everyone is to him as his (*a*) castle and fortress, as well for his defence against injury and violence, as for his repose . . . ."). Blackstone, writing to address the practice of excise officers obtaining general warrants to search the homes of tax-payers, decried "the frauds that might be committed . . . unless strict watch is kept," 1 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 308 (Univ. of Chi. Press 2002) (1765), and in 1763, the House of Lords denounced general warrants as "contrary to the fundamental principles of the constitution." Wilkes v. Wood, (1763) 98 Eng. Rep. 489, 499 (K.B.). However, even as general warrants were being restricted in England, their use flourished in the fledgling colonial governments. Despite the outrage caused by the general warrants, they were omitted from the long list of grievances included in the Declaration of Independence. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1(a) (4th ed. 2004) [hereinafter LAFAVE, SEARCH AND SEIZURE]. The need for protection from unreasonable searches was a point of contention at the ratification debates on the Constitution, however, and James Madison led an effort to add a bill of rights to the Constitution. *Id.* Madison supplied the first draft of the Fourth Amendment, motivated by a desire to limit the use of general warrants, ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS: A REFERENCE GUIDE TO THE UNITED STATES CONSTITUTION 9 (2003), but stated the right so broadly as to significantly expand upon that modest intent. In distinctively American fashion, the Fourth Amendment's drafters portrayed it as a return to historic rights, but in reality asserted broad new rights fitting for a new democracy built on the foundation of popular sovereignty. William B. Cuddihy & B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 WM. & MARY Q. 372, 400 (1980).

42 Specifically, the Framers reasoned that government structure, rather than mere language, should restrict the government's power. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1126 (2002). As James Madison noted, "experience has taught mankind the necessity of auxiliary precautions," THE FEDERALIST No. 51 (James Madison), and the Framers ensured that the people would be protected from unreasonable search and seizure not simply by "parchment barriers," but by the insertion of a neutral magistrate to the search process. Solove, *supra*.

43 Solove, *supra* note 42, at 1126-27.

44 96 U.S. 727 (1877).

the postal system.[45] The invention of the self-sealing envelope (as opposed to wax-sealed) had enhanced an individual's ability to prevent others from viewing his personal papers in transit, and led the Court to expand its definition of property in which owners had a constitutional protection.[46] The Court held that "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[47]

The emerging technologies of the twentieth century posed a challenge to the Court's traditional property-based understanding of Fourth Amendment protections. In *Olmstead v. United States*,[48] the Court confronted the question of whether wiretapping a phone line constituted an unreasonable search under the Fourth Amendment.[49] Struggling to apply a property-oriented protection to a wire-based communication, the Court concluded that the Fourth Amendment did not protect against wiretapping accomplished without any physical trespass.[50] However, in *Berger v. New York*,[51] the Court reexamined the constitutionality of wire-tapping and *sub silentio* overruled its decision in *Olmstead*. [52] In *Berger*, law enforcement complied with a New York statute that required merely a showing of "reasonable ground to believe that evidence of crime may be thus obtained" in order to receive an ex parte order to wiretap the defendant's home phone.[53] The Court held that the language of the statute was overly broad and allowed "a trespassory intrusion into a constitutionally protected area."[54]

The Court refined its *Berger* decision six months later in *Katz v. United States*,[55] the case widely regarded as establishing the modern approach to Fourth Amendment inquiries.[56] Agents from the Federal Bureau of Investigation ("FBI") recorded phone calls that the defendant made from

---

45 *Id.* at 732-33.

46 *Id.*; *see also* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 10 (2005) ("Sealed letters and packages carry with them the privacy accorded the premises from which they originated; violating that privacy is a trespass which must be authorized by a warrant.").

47 *Jackson*, 96 U.S. at 733. This case is frequently cited for the proposition that one who entrusts papers to a bailee still retains constitutional protections for the papers. ORIN S. KERR, COMPUTER CRIME LAW 408 (2006).

48 277 U.S. 438 (1928).

49 *Id.* at 455.

50 *Id.* at 466. Justice Brandeis wrote a strongly-worded dissent, first invoking Justice Marshall's famous words that "it is a constitution we are expounding," *id.* at 472 (Brandeis, J., dissenting) (quoting McCulloch v. Maryland, 17 U.S. 316, 407 (1819)), and noting that the Fourth Amendment "must have a similar capacity of adaptation to a changing world." *Id.*

51 388 U.S. 41 (1967).

52 *See id.* at 64 (Douglas, J., concurring).

53 *Id.* at 43, n.1, 45 (majority opinion).

54 *Id.* at 44.

55 389 U.S. 347 (1967).

56 *See, e.g.*, Peter P. Swire, Katz *is Dead. Long Live* Katz., 102 MICH. L. REV. 904, 904 (2004).

a public phone booth and introduced these recordings into evidence.[57] The parties disputed whether the phone booth occupied by the defendant was a "constitutionally protected area" that was protected under *Berger*,[58] but the Court rejected this formulation of the issue and stated instead that "the Fourth Amendment protects people, not places. . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[59] Justice Harlan, in his concurrence, articulated the two-prong test now widely used to determine the reasonableness of a search: "[F]irst 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.'"[60] By abandoning the traditional property-based conception of searches,[61] the Court interpreted the Fourth Amendment to protect communications accomplished through new technologies.

No sooner had the Court created a new privacy-based standard than it began to carve out exceptions for information disclosed to third parties. First, in *United States v. White*,[62] the Court held that a defendant did not have a reasonable expectation of privacy in information given to a government informant.[63] The Court distinguished *Katz* by noting that it did not "indicate in any way that a defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police."[64] Second, in *Couch v. United States*,[65] the Court held that a defendant did not have a reasonable expectation of privacy in business records that she disclosed to her accountant.[66] The Court noted that the documents were entrusted to the accountant

---

57 *Katz*, 389 U.S. at 348.

58 *Id.* at 351.

59 *Id.*

60 *Id.* at 361 (Harlan, J., concurring); *see* SALTZBURG & CAPRA, *supra* note 13, at 41 (noting that "*Katz* has been read to set forth a two-pronged test for determining whether government conduct constitutes a search").

61 *Katz*, 389 U.S. at 352 (holding that "[t]he premise that property interests control the right of the Government to search and seize has been discredited" (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)) (internal quotation marks omitted)). *See also* Swire, *supra* note 56, at 906. However, for an alternative view arguing that *Katz* had very little effect on the historic right-to-exclude interpretation of the Fourth Amendment, see Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807 (2004) ("The *Katz* 'reasonable expectation of privacy' test has proven more a revolution on paper than in practice; *Katz* has had a surprisingly limited effect on the largely property-based contours of traditional Fourth Amendment law.").

62 401 U.S. 745 (1971).

63 *Id.* at 749.

64 *Id.*

65 409 U.S. 322 (1973).

66 *Id.* at 335-36. The Court examined the Fourth Amendment claim briefly, noting that the defendant's Fourth Amendment claim merged with her Fifth Amendment claim and did not warrant separate

for the purpose of reviewing the contents and filing a tax return, thus establishing that the defendant was aware that the contents would be seen by another.[67]

The Court merged the reasoning behind these two exceptions in its decision in *United States v. Miller*,[68] in which the Court considered whether an individual had a reasonable expectation of privacy in bank records.[69] The Court cited both *Couch* and *White* in concluding that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[70] Even if the individual subjectively expected confidential treatment of the information conveyed to the third party, the Court stated that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . ."[71]

The Court applied the same analysis in *Smith v. Maryland*[72] and determined that the warrantless use of a pen register device to capture the numbers dialed from a telephone did not constitute a search under the Fourth Amendment.[73] Basing its decision on the established exception to privacy protections for information voluntarily conveyed to third parties, the Court ruled that the defendant did not have an objectively reasonable expectation of privacy in the phone numbers he transmitted to the phone company when dialing.[74] The Court distinguished the facts of this case from those of *Katz* by noting that the pen register device captured only the numbers dialed, rather than the "contents" of the communication.[75] Together, *Smith* and *Miller* are commonly referred to as the "business records cases" and stand for the proposition that information voluntarily disclosed to a third party will not receive Fourth Amendment protection.[76]

---

analysis. *Id.* at 325, n.6. Later, however, the Court proceeded to answer the question of whether the defendant had a reasonable expectation of privacy in the documents. *Id*. at 335-36.

67 *Id.* at 335.

68 425 U.S. 435 (1976). *See also* Bellia, *supra* note 17, at 1400 (recognizing the Court's synthesis of *Couch* and *White* in its decision in *Miller*).

69 *Miller*, 425 U.S. at 436-37.

70 *Id.* at 443. The Court further articulated its reasoning, stating that "[t]he checks are not confidential communications . . . . All of the documents obtained . . . contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442.

71 *Id.* at 443.

72 442 U.S. 735 (1979).

73 *Id.* at 742.

74 *Id.* at 743-44, 745.

75 *Id.* at 741.

76 *See, e.g.*, Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1562 (2004).

2. Remedies for Improper Searches under the Fourth Amendment

Individuals whose Fourth Amendment rights are violated by unconstitutional law enforcement searches may move to suppress the evidence at trial.[77] The ability to suppress improperly obtained evidence serves three key purposes.[78] First, it deters law enforcement from conducting unreasonable searches and seizures.[79] Law enforcement officers, knowing that any evidence seized in the absence of proper procedure will be suppressed at trial, are motivated to comply with warrant requirements to ensure the validity of the seized evidence.[80] Second, the rule preserves judicial integrity by ensuring that the judiciary does not participate in undermining the Constitution that it is duty-bound to uphold.[81] Third, it preserves popular trust in the Constitution and the government generally, and ensures that no individual is convicted on the basis of illegally-seized evidence.[82]

3. The Fourth Amendment Applied to Electronic Communications

Courts have grappled with how to apply the Fourth Amendment to forms of technology that inherently require disclosure to third parties.[83] As

---

77 Civil remedies are also available, but most litigants challenging law enforcement action are more concerned with avoiding incarceration than seeking monetary damages, and thus only seek to suppress the evidence from use at trial. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 812 (2003) [hereinafter Kerr, *Lifting the "Fog" of Internet Surveillance*].

78 LAFAVE, SEARCH AND SEIZURE, *supra* note 41, § 1.1(f). Note, however, that the Supreme Court recently addressed the exclusionary rule in *Herring v. United States*, 129 S. Ct. 695 (2009), and determined that the legal and policy reasons underlying the continued use of the exclusionary rule will not outweigh the individual's privacy interest in all cases. *See id.* at 698, 700-02 (noting that suppression will not be automatic). Rather, the appropriate inquiry (as articulated in *Herring*) requires balancing the gravity of the official misconduct and the benefits from deterrence against the cost of refusing to admit the evidence. *Id.* at 700-02. Thus, "when police mistakes are the result of negligence . . . rather than systemic error or reckless disregard of constitutional requirements," the marginal benefit of deterrence does not outweigh the social cost of excluding the evidence, and the exclusionary rule will not apply. *Id.* at 704.

79 *See* Mapp v. Ohio, 367 U.S. 643, 648 (1961) ("This Court has ever since required of federal law officers a strict adherence to that command which this Court has held to be a clear, specific, and constitutionally required—even if judically implied—deterrent safeguard without insistence upon which the Fourth Amendment would have been reduced to 'a form of words.'" (quoting Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920))); LAFAVE, SEARCH AND SEIZURE, *supra* note 41.

80 Adam Liptak, *Justices Weigh the Value of a Rule that Limits Evidence*, N.Y. TIMES, Oct. 7, 2008, at A18.

81 LAFAVE, SEARCH AND SEIZURE, *supra* note 41.

82 *Id.*

83 This difficulty is partially due to the structure of previous statutes dealing with wiretapping and surveillance during transmission. The SCA was adopted as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, *see infra* Part I.C, which

the Supreme Court has not yet addressed the issue of an individual's reasonable expectation of privacy in electronic communications disclosed to a network provider, courts look to cases addressing other forms of communication for guidance.[84] Before the Ninth Circuit decided *Quon*, all circuits to address the issue had declined to use the Fourth Amendment as a source of protection for the contents of electronic communications.[85] However, despite reaching similar conclusions, the lack of clear guidance is apparent in the ambivalence expressed in their decisions.[86]

The Second and Sixth Circuits followed *Miller* and *Smith* to conclude that the Constitution does not guarantee protection for the contents of electronic files sent through a network provider due to the disclosure to a third party.[87] The Eighth, Tenth, and Eleventh Circuits addressed the issue in

---

included far more stringent requirements than the Fourth Amendment would impose. *See* Michael Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 4 (1983). Congress intended the courts to play the leading role in enforcing Title III, and it was designed to incorporate a strong judicial role. *Id.* at 44. Conversely, the SCA was drafted with different priorities and requires less process than would be required under the Constitution. *See infra* note 130 and accompanying text. Thus, while courts have long been called upon to apply the stringent requirements of Title III, they have only recently been called upon to apply the Fourth Amendment to similar types of communications.

84 *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472) (referring to previous cases dealing with e-mail in order to guide the inquiry for text messages).

85 Courts and commentators are nearly unanimous in their view that so-called "non-content records," such as phone numbers dialed and subscriber information, are not protected by the Fourth Amendment. This exception derives from the Supreme Court's ruling in *Smith v. Maryland*, 442 U.S. 735 (1979), which has been applied to electronic communications to reach the conclusion that the Fourth Amendment does not protect internet protocol ("IP") addresses, e-mail addresses, and routing information. *See supra* notes 72-76 and accompanying text. *See also* United States v. Forrester, 512 F.3d 500, 510 (9th Cir.), *cert. denied sub nom.* Alba v. United States, 129 S. Ct. 249 (2008) (concluding that the government surveillance techniques were "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*" and holding that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to . . . Internet service providers for the specific purpose of directing the routing of information"); 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.4(a) (3d ed. 2007) [hereinafter LAFAVE, CRIMINAL PROCEDURE] (explaining that there is "an emerging framework suggesting that contents of Internet communications ordinarily receive Fourth Amendment protection while non-content Internet communications do not"). This distinction is reflected in the SCA, which requires minimal process for law enforcement to obtain this information. *See infra* note 125 and accompanying text. This Note only analyzes the question of constitutional protections for the contents of electronic communications.

86 *See, e.g.*, Warshak v. United States, 532 F.3d 521, 526 (6th Cir. 2008) (noting that "uncertainty looms large in a debate about the expectations of privacy").

87 United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (noting individuals might not have "an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient" and that users "lose a legitimate expectation of privacy in an e-mail that ha[s] already reached its recipient" (citing Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001))); *Warshak*, 532 F.3d at 526-27

dicta and unpublished opinions and drew similar conclusions.[88] But although the courts reached similar conclusions, the circuits diverged in their reasoning, and their decisions expressed confusion as to how to best answer the constitutional inquiry.[89] Constitutional protection for stored electronic communications remains an open question in the courts today.[90]

C. *The Stored Communications Act*

1. Background to Statutory Protections

The statutory restrictions on internet surveillance have their roots in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[91] which protects wire and oral communications from interception during transmission and allows law enforcement to conduct surveillance only in limited circumstances.[92] Passage of Title III preceded an era of rapid evolution in electronic communications, however, and by 1986 nascent computer functionality had given rise to new forms of communications which were susceptible to interception during storage rather than transmission.[93]

(stating that the reasonableness of an individual's privacy interest in her e-mails "may well shift over time" and depends on the nature of the internet-service agreement).

88 United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) ("While it is clear to this court that Congress intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation of privacy derives from the Constitution."); United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008) (noting that an individual who uses peer-to-peer networks cannot have a privacy expectation in the subscriber information contained on his computer); United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005) (holding that an individual does not have a reasonable expectation in either e-mails that have reached the recipient or text messages). Additionally, the Fifth Circuit held in *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007), that individuals have a reasonable expectation of privacy in text messages, but its decision was made in the context of a search conducted incident to arrest rather than electronic surveillance. *Id.* at 259. In *Finley*, police conducted a direct search of the defendant's cell phone and text messages while arresting him. *Id.* at 254. The Fifth Circuit analogized the search of the phone to a lawful search incident to arrest of a closed container on an arrestee's person, and held that the warrantless search did not violate the Fourth Amendment. *Id.* at 259-60. Thus, while the Fifth Circuit held that text messages are constitutionally protected, its decision applies only to the limited context of searches incident to arrest, and the Fifth Circuit has not yet addressed the issue of protections for text messages obtained through internet surveillance.

89 *See, e.g.*, *Warshak*, 532 F.3d at 526-27.

90 Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

91 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801-804, 82 Stat. 211 (1968) (current version at 18 U.S.C. §§ 2510-2522 (1986)).

92 Bellia, *supra* note 17, at 1389.

93 Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213-14 (2004) [hereinafter Kerr, *A User's Guide to the Stored Communications Act*].

By the early to mid-1980s, businesses were beginning to utilize computer technology, but they generally outsourced computing tasks to third-party processors capable of handling large quantities of data.[94] Commercial internet service providers ("ISPs") and personal e-mail providers had yet to appear on the horizon,[95] but the emerging forms of electronic communications shared a common characteristic: all required the services of an electronic intermediary.[96] Due to the "business records" exception to Fourth Amendment protections for documents relinquished to third parties, businesses felt a growing concern over the uncertainty of protections for their records and private data.[97] Newspapers ominously warned of "tremendous holes in communications privacy."[98] While the question of whether the Constitution would protect stored electronic files was unresolved, it was clear that no statutory protections existed for the files as Title III only protected communications during transmission.[99]

Congress, concerned that the growing uncertainty would "discourage American businesses from developing new innovative forms of telecommunications and computer technology,"[100] solicited advisory reports on the Fourth Amendment status of electronic communications from the Department of Justice ("DOJ") and another government agency, the Office of Technology Assessment ("OTA").[101] The DOJ reported that

> Fourth Amendment warrant requirements are inapplicable to this type of document since there is no reasonable expectation of privacy associated with it. This is a well accepted principle of law relating to documents in the possession of third persons and we know of no sound legal or policy reason why it should not apply to these types of documents.[102]

In contrast, the OTA noted that under *United States v. Miller*, an individual might not be able to challenge a service provider's disclosure of communications, but stressed that "although these are not 'papers' in the traditional sense, they are arguably the computer-age equivalent."[103] The best analogy,

---

94 *Id.*

95 Mulligan, *supra* note 76, at 1561 (noting that "[e]-mail links to commercial mail carriers, such as MCI Mail and Compuserve, would not be available until 1989").

96 See Kerr, *A User's Guide to the Stored Communications Act*, supra note 93.

97 Mulligan, *supra* note 76, at 1559.

98 Stuart Taylor Jr., *Leahy Hopes to Close Gaps in Wiretap Laws*, N.Y. TIMES, Sept. 13, 1984, at A19.

99 Mulligan, *supra* note 76, at 1562.

100 S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

101 *Id.* at 4, 1986 U.S.C.C.A.N. at 3558.

102 Mulligan, *supra* note 76, at 1582-83 (quoting *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. 234 (1986) (statement of James Knapp, Deputy Assistant Att'y Gen., Criminal Div.)).

103 Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties 48 (1985), *available at* http://www.princeton.edu/~ota/disk2/1985/

the OTA argued, was first-class postal mail, and it asserted that individuals likely had a reasonable Fourth Amendment expectation of privacy in electronic communications.[104]

Congress adopted the position advanced by the DOJ and chose to legislate based on the assumption that electronic communications lacked Fourth Amendment protections.[105] In order to grant some measure of protection to electronic communications, it amended Title III by passing the Electronic Communications Privacy Act ("ECPA").[106] The ECPA consists of the SCA, the Wiretap Act, and the Pen Register statute.[107] The Pen Register statute and Wiretap Act govern surveillance of electronic communications during transmission, while the SCA protects electronic communications during storage on the network provider's servers.[108] Because text message surveillance occurs while the text is in storage after transmission, rather than during transmission, it receives protection under the SCA rather than the Wiretap Act or Pen Register statute.

2. The Text of the Statute

The SCA operates to protect text messages stored by network operators in two ways.[109] First, 18 U.S.C. § 2701 limits the government's ability to compel the service provider to disclose the contents of the stored communication.[110] Second, 18 U.S.C. § 2702 limits voluntary disclosure of electronic communications by the service provider, stating that, except in limited circumstances:

> (1) a person or entity providing an *electronic communication service* to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing *remote computing service* to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service (A) on behalf of, and received by

8509/8509.PDF.

104 *Id.* at 48-49.

105 Mulligan, *supra* note 76, at 1583.

106 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522); *see also* Bellia, *supra* note 17, at 1391.

107 Electronic Communications Privacy Act of 1986, §§ 101-111, 201-202, 301-303.

108 Mulligan, *supra* note 76, at 1565. Note that text messages can be stored both before and after transmission, and what law enforcement must do to lawfully obtain the messages under the SCA depends in part on the point in time at which law enforcement seeks to obtain the messages. *See infra* Part II.C.2.

109 LAFAVE, CRIMINAL PROCEDURE, *supra* note 85, § 4.8(a).

110 Section 201 of the SCA, 18 U.S.C. § 2701, creates civil liability for any person or entity that "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a) (1986).

> means of electronic transmission from . . . a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer . . . .[111]

The crux of the statute is the division between the two kinds of services contemplated by the statute's drafters: electronic communication services ("ECS") and remote computing services ("RCS").[112] Correctly classifying whether a network operator is acting as an RCS or an ECS is critical for determining what level of protection the text message merits. Whether law enforcement personnel must obtain a warrant before searching stored electronic communications depends on the type of service being offered and, to a lesser degree, the length of time the communications have been stored.[113] This has posed difficulties for courts, as it requires them to fit modern technologies into a framework constructed over twenty years ago.[114]

The first step in the analysis is to determine whether a provider is acting as an ECS or an RCS.[115] The two types of services are loosely correlated to the two primary functions performed by service providers at the time of the statute's passage:[116] first, processing electronic communications such as e-mails and providing temporary storage of the messages incident to trans-

---

111 18 U.S.C. § 2702(a)(1)-(2) (1986) (emphasis added). The statute defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (1986). Relatedly, the statute defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (1986). A "remote computing service" is defined as providing to the public "computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (1986).

112 *See* Kerr, *A User's Guide to the Stored Communications Act*, supra note 93, at 1214.

113 *See* 18 U.S.C. §§ 2701-2711 (1986).

114 The SCA has been periodically amended, most recently by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), but has not been substantively updated since its passage in 1986. *See, e.g.*, Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488, 3498 (1996) (revising 18 U.S.C. § 2701 to omit an unnecessary preposition); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, 202 (2006) (adding to 18 U.S.C. § 2702 a requirement that the DOJ report the number of voluntary disclosures received per year).

115 The prevailing interpretation of the SCA is detailed in the DOJ's search and seizure manual for law enforcement, COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § II(B) (July 2002), http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm [hereinafter SEARCHING AND SEIZING COMPUTERS], and adopted by the leading scholarly treatise on the subject. LAFAVE, CRIMINAL PROCEDURE, *supra* note 85, § 4.8. While courts frequently disagree with this approach, leading to a variety of practical interpretations, the DOJ interpretation remains the starting point for understanding the way the statute operates.

116 Kerr, *A User's Guide to the Stored Communications Act*, supra note 93.

mission[117] and second, storing data files too large to keep on a personal computer and performing data-processing tasks such as those commonly performed today in spreadsheet programs.[118] The ECS category was designed to apply to the former type of service and the RCS to the latter.[119] However, modern communications usually combine both services, and network operators frequently provide both electronic communication services such as e-mail transmission, as well as remote computing services such as long-term storage and archiving.[120] Thus, a network operator cannot be defined as either an RCS or an ECS in the abstract; its classification will depend on the particular characteristics of the service in question.[121]

The second step in determining the applicable protections requires examining how long the message will be in storage. When a message is stored for less than 180 days by an ECS, law enforcement must obtain a traditional search warrant supported by probable cause in order to compel production of the message.[122] Lesser protection is afforded messages stored by an ECS for more than 180 days or any message stored by an RCS; under these circumstances, the SCA does not require a search warrant or probable cause. Instead, under 18 U.S.C. § 2703(d), law enforcement may instead obtain a subpoena or a court order by demonstrating "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[123] The "relevancy" standard for obtaining a court order under § 2703(d) is less stringent than the probable cause standard required to obtain a search warrant and is a far easier burden for law enforcement to meet.[124] Finally, minimal protections are granted to "basic

---

117 *Id.*

118 *Id.*

119 *Id.*

120 LAFAVE, CRIMINAL PROCEDURE, *supra* note 85, § 4.8(d).

121 *Id.* For a detailed hypothetical of how a service provider could simultaneously be both an RCS and an ECS, see SEARCHING AND SEIZING COMPUTERS, *supra* note 115.

122 18 U.S.C. § 2703(c) (1986); *see also* Kerr, *A User's Guide to the Stored Communications Act*, *supra* note 93, at 1218-19. In all cases, law enforcement may obtain copies of electronic communications where the subscriber or customer consents. 18 U.S.C. § 2703(c).

123 18 U.S.C. § 2703(d) (1986).

124 Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 17 (2007). The § 2703(d) order also requires that law enforcement give the target of the search prior notice, but notice may be suspended whenever the court determines that knowledge of the search may cause an "adverse result," such as deleting the messages in question. 18 U.S.C. § 2705(a)(1)-(2) (1986). In practice, the notice requirement has proven to be quite flexible. For example, in *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008), the government obtained a § 2703(d) order after showing that the information sought was relevant to an investigation, but successfully argued that "notice to [the target] 'would seriously jeopardize the investigation'" and received permission to delay notice for ninety days. *Id.* at 524. However, the government delayed giving notice until a year after the issuance of the order, at which time the target had no recourse to prevent or respond to the search. *Id.*

subscriber information," which includes the customer's name, address, billing information, and the types of services utilized.[125]

When law enforcement fails to comply with the requisite process under the SCA, the affected individual may seek civil remedies, but cannot prevent the wrongfully seized evidence from being introduced at trial.[126] Unlike the exclusionary rule applicable to evidence obtained from searches in violation of the Fourth Amendment, the SCA contains no similar provision; evidence obtained from a search in violation of the SCA will not be suppressed.[127] Instead, an individual is vested only with a private right of action for damages.[128]

3. Cases Interpreting the SCA

Confusion abounds regarding application of the SCA. Courts and commentators alike agree on only one aspect of the statute: it is highly technical and difficult to apply.[129] Although the SCA creates neat categories for allocating protections, the categories codify the state of technology as it existed in 1986, which no longer bears much resemblance to current communications technology.[130] Difficulties have arisen in interpreting numerous

---

125 Basic subscriber information includes:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number).

18 U.S.C. § 2703(c)(2) (1986). Compelling the production of subscriber information requires only an administrative subpoena. *Id*.

126 Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 77, at 829.

127 *Id.*; *see also* United States v. Allen, 53 M.J. 402, 409 (C.A.A.F. 2000) (referring to the SCA and noting that "[a]lthough neither a warrant nor a court order was obtained, there is no exclusionary rule relief under [18 U.S.C.] § 2703 . . . [i]f Congress had intended to have the exclusionary rule apply, it would have added a provision" (citations omitted)).

128 Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 77, at 829 (discussing how the lack of a suppression remedy has meant that the statute is only raised in civil, rather than criminal, cases, where "[t]he promise of attorney's fees and the possibility of punitive damages, combined with the added bonus of a federal question to allow the suit to be filed in federal court, creates a strong incentive for potential plaintiffs to push the boundaries of [the statute] in civil cases").

129 *See* Bellia, *supra* note 17, at 1378 ("The laws regulating electronic surveillance generally, and particularly those governing acquisition of electronic evidence . . . are highly technical and poorly understood . . . . Courts struggle with how to apply overlapping and seemingly conflicting statutory provisions . . . ."); *see also* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (noting in a case examining the relationship between the Wiretap Act and the SCA that the statute is "famous (if not infamous) for its lack of clarity").

130 Bellia, *supra* note 17, at 1383 ("The relevant constitutional and statutory categories developed at a time when electronic communications either did not exist or were not widely used, and subsequent technological developments have placed tremendous strain on those categories.").

provisions of the statute, resulting in a lack of judicial consensus on how to apply the SCA.

The Ninth and Third Circuits struggled to determine when a message is in "backup protection" for the purposes of determining liability under 18 U.S.C. § 2701(a). In *Theofel v. Farey-Jones*,[131] the parties to the lawsuit were adversaries in unrelated commercial litigation in which, during the course of discovery, the defendant served the plaintiff's ISP with a facially defective subpoena for the plaintiff's personal e-mails.[132] The ISP, without seeking legal counsel, complied with the subpoena and produced the plaintiff's e-mails.[133] The plaintiff filed suit under the SCA, and following an unfavorable ruling in the district court, appealed to the Ninth Circuit.[134] After determining that an e-mail stored after delivery fell into the category of "storage . . . for purposes of backup protection,"[135] the court reversed the dismissal of the SCA claim.[136] The Ninth Circuit acknowledged that its decision conflicted with the federal government's interpretation of the statute in its amicus curiae brief, but remained undeterred and included a lengthy discussion of the errors it found in the government's analysis.[137]

A district court within the Third Circuit reached a very different conclusion in *Fraser v. Nationwide Mutual Insurance Co.*,[138] where it held that the SCA did not cover stored e-mails.[139] Despite the evident contradiction between the district court's decision and the name of the statute (the Stored Communications Act), the court held that the SCA only protected messages during transmission.[140] When the question reached the Third Circuit on appeal,[141] the court took a different approach than either the district court or the Ninth Circuit and left unresolved the question of whether an e-mail

---

131 359 F.3d 1066 (9th Cir. 2004).

132 *Id.* at 1071.

133 *Id.* (noting that the ISP provided a "'free sample' consisting of 339 [e-mails]").

134 *Id.* at 1072. The defendant argued that the messages "were not in 'electronic storage' and therefore fell outside the [SCA's] coverage." *Id.* at 1075. Because the messages had already been sent or received before the defendant obtained them, neither party asserted that the messages had been accessed during storage incident to transmission. *Id.* at 1071. Thus, the issue facing the Ninth Circuit was whether the messages could be considered to be in electronic storage for purposes of backup protection and therefore within the scope of the SCA. *Id.* at 1075.

135 *Id.* at 1075 (quoting 18 U.S.C. § 2510(17)).

136 *Id.* at 1075, 1079.

137 *Theofel*, 359 F.3d at 1076-77. Commentators later argued that the Ninth Circuit had incorrectly interpreted the SCA. *See* Bellia, *supra* note 17, at 1419 ("The Ninth Circuit's interpretation of the statutory text, however, is awkward . . . . To the extent that the Ninth Circuit's approach suggests that any communication a service provider holds on a user's behalf is in backup protection, then, it relies on a strained reading of the text.").

138 135 F. Supp. 2d 623 (E.D. Pa. 2001), *aff'd in part, remanded in part*, 352 F.3d 107 (3d Cir. 2003) (holding that the statute did not protect messages stored after transmission).

139 *Id.* at 636.

140 *Id.*

141 Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003).

stored after delivery was in backup storage.[142] Noting that neither the statute nor the legislative history defined the term "backup storage," the court declined to define the term itself and instead broadly interpreted one of the SCA's exceptions to exempt all searches by employers acting as service providers.[143] The Third Circuit retreated from the district court's new definition of backup storage, but by exempting employers from all liability under the SCA, it strained the text of the statute and created an extensive new class of individuals and communications entirely lacking in statutory protection.[144]

The Ninth Circuit's perplexing sequence of decisions in *Konop v. Hawaiian Airlines*, interpreting the intersection between the Wiretap Act and the SCA, exemplifies the difficulty in applying the SCA. In *Konop v. Hawaiian Airlines* (*Konop I*),[145] an airline employee maintained a password-protected website which contained postings that criticized the airline and its labor union.[146] An airline officer viewed the unflattering postings and suspended the employee,[147] leading the employee to bring suit alleging improper surveillance under both the Wiretap Act and the SCA.[148] Viewed objectively, both claims lacked merit: the Wiretap Act applies exclusively to real-time surveillance during transmission of a file, and the SCA provision invoked by the plaintiff applies only to files stored prior to delivery, such as unopened e-mails.[149] The Ninth Circuit, however, approached the issue with the objective of making an outdated statute applicable to a technologically-advanced situation[150] and was wary of granting lesser protections under the SCA when Congress had not clearly stated its intent.[151] Relying on student law review articles and tenuous inferences from the legislative history, the Ninth Circuit ignored both its own precedent and persua-

142 *Id.* at 114 (assuming, without deciding, that the e-mail at issue was in backup storage).

143 *Id.* at 114-15.

144 *See id.* at 115.

145 236 F.3d 1035 (9th Cir.), *withdrawn*, 262 F.3d 972 (9th Cir. 2001), *modified*, 302 F.3d 868 (9th Cir. 2002).

146 *Id.* at 1041.

147 *Id.*

148 *Id.*

149 Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 77, at 833-34.

150 *Konop I*, 236 F.3d at 1046 (noting that Congress's intent was to eliminate arbitrary distinctions between different forms of technologies). The court cited a legislative report lamenting the statute's failure to keep pace with the times by not updating distinctions based on technological advancements and concluded that the best way to apply the statute was to update the distinctions based on the new kinds of technology at issue in this case. *Id.*

151 *Id.* at 1045 ("We are wary of attributing subtle purpose and indirection to the language of a statute that appears to have been crafted with little of either. In other instances, where Congress has provided lesser protection for electronic communications, it has done so straightforwardly, and for discernable reasons.").

sive decisions from the Fifth Circuit, holding that the Wiretap Act applied to stored communications as well as those in transmission.[152]

Not only did this decision render the SCA irrelevant by extending Wiretap Act protections to stored communications,[153] it also subjected both communications in transmission and in storage to the more stringent warrant requirements of the Wiretap Act.[154] The Wiretap Act requires the so-called "super search warrant," mandating, among other things, a detailed affidavit submitted to a judge including the offense likely to be committed if law enforcement does not intervene and an explanation of why no other investigatory technique will suffice.[155] Although the case before the Ninth Circuit was a civil case, its decision would have had far-reaching effects in the criminal context by requiring law enforcement to comply with a nearly impossible standard in order to obtain any stored electronic records. This was a far greater burden than Congress intended.[156] After amicus curiae briefs brought the implications of the decision to the Ninth Circuit's attention, it withdrew its opinion and issued a second decision.[157] In *Konop II*,[158] the Ninth Circuit changed the basis of its ruling from the Wiretap Act to the SCA.[159] Still, its decision has been derided by commentators as "dramatically misconstru[ing] the applicable law."[160] The Ninth Circuit's difficulty in applying the SCA demonstrates that the statute is both a complex and outdated method of protecting modern communications.

---

152 *Id.* at 1045-46; *see also* Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 77, at 834.

153 *Konop I*, 236 F.3d at 1048 (calling the SCA a "lesser included offense" of the Wiretap Act).

154 Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 77, at 835.

155 *Id.* at 815, 835. Kerr observes that "the ['super search warrant'] is quite difficult to obtain . . . . [It] is the highest threshold court order in American criminal law." *Id.* at 815. Accordingly, Kerr notes that "[s]ubjecting every kind of access to the 'super search warrant' requirement of the Wiretap Act would have nullified the Stored Communication Act entirely, and brought many if not most Internet crime investigations to a standstill." *Id.* at 835. *See also* 18 U.S.C. § 2518 (1986) (listing the requirements for a "super search warrant").

156 Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 77, at 835 ("Understood as a whole, the internet surveillance laws clearly did not contemplate this.").

157 *Id.* at 835-36.

158 302 F.3d 868 (9th Cir. 2002).

159 *Id.* at 880.

160 *See* Kerr, *Lifting the "Fog" of Internet Surveillance*, *supra* note 77, at 836 (stressing that "[t]he courts did their best in light of what they knew" but were foiled by "the fog of Internet surveillance law and the complex maze of statutes involved").

II. THE NINTH CIRCUIT TAKES A STAND IN *QUON V. ARCH WIRELESS*

A. *Factual Background*

In 2006, the United States District Court for the Central District of California faced the question of the "legal boundaries of an employee's privacy in this interconnected, electronic-communication age, one in which thoughts and ideas that would have been spoken personally and privately in ages past are now instantly text-messaged to friends and family *via* hand-held, computer-assisted electronic devices."[161] Jeff Quon was employed as a sergeant in the City of Ontario Police Department's Special Weapons and Tactics ("SWAT") team.[162] The city issued its SWAT team text-messaging pagers[163] for work-related purposes, along with a written policy precluding employees from using the pagers for personal communications.[164] The city's contract with its wireless provider, Arch Wireless, allowed for a monthly maximum of 25,000 characters per pager, with overage charges applying to each message sent in excess of the limit.[165] If a police officer exceeded the monthly character limit, the City had an informal policy of requiring the officer to pay the overage charges.[166]

The city had a succinct privacy policy for its technological equipment, which stated that "users should have no expectation of privacy or confidentiality when using these resources."[167] Despite the formal privacy policy, the city, through the lieutenant in charge of its electronic equipment, exercised an unwritten policy of not auditing the employees' pagers to ascertain the nature of the text messages as long as overage charges were paid promptly.[168] The chief of police, Chief Scharf, knew of Lieutenant Duke's policy of allowing personal use of the pagers[169] but did not take action to enforce the written policy prohibiting such usage.[170]

---

161 Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1121 (C.D. Cal. 2006), *aff'd in part, rev'd in part*, 529 F.3d 892 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

162 *Id.* at 1123.

163 Text pagers and cell phones utilize the same technology to transmit messages, although the latter form of sending texts has largely superseded the former. *See Quon*, 445 F. Supp. 2d at 1123; *see also* HowStuffWorks.com, *supra* note 29.

164 *Quon*, 445 F. Supp. 2d at 1123.

165 *Id.*

166 *Id.* at 1124.

167 *Id.* at 1123.

168 *Id.* at 1124. Lieutenant Duke attested that he turned a blind eye to employees' personal text communications by informing them that he did not want to know if the overage charges resulted from personal or work-related usage. *Id.*

169 *Id.*

170 *Quon*, 445 F. Supp. 2d at 1125.

Lieutenant Duke tired of Quon's excessive texting and complained to Chief Scharf, who ordered an inquiry into the substance of the messages to determine whether the messages were work-related.[171] The city requested transcripts of Quon's text messages for the previous two months and Arch Wireless complied by producing forty-six pages of text messages.[172] Various members of the police force reviewed Quon's text messages and discovered sexually explicit messages to both Quon's wife and his mistress.[173] Chief Scharf referred the matter to the internal affairs department to conduct a full inquiry into Quon's misconduct and investigate possible liability for failure to pay attention to duty.[174] A sergeant leading a separate corruption investigation requested copies of Quon's text messages to investigate whether Quon played a role in the corruption, although it is unclear whether she in fact received the transcripts.[175] After learning of the intrusion, Quon, along with his wife, mistress, and two other co-workers, filed suit against the city, Arch Wireless, and members of the police force individually, alleging violations of the SCA, the Fourth Amendment, and various state laws.[176]

B. *District Court Decision*

1. Stored Communications Act Claims

The case came before the district court on cross summary judgment motions.[177] The district court began by analyzing the plaintiffs' SCA claims, after noting that in light of "the statute's age, preceding as it did the mass use of the Internet and the world wide web, its framework at times is 'ill-suited to address the mode[rn] forms of communication,' oftentimes requiring courts to 'struggle[] to analyze problems involving mode[rn] technology within the confines of this statutory framework."[178] The district court first determined that the city and its employees could not be held liable for violations of the SCA on the facts presented in this case, as they were not service providers under § 2702, nor did they obtain the messages in the course of a criminal investigation under § 2703.[179] The district court proceeded to examine Arch Wireless's liability and determined that the company's liability would depend on whether it was classified as an RCS or an

171 *Id.*
172 *Id.*
173 *Id.* at 1126.
174 *Id.* at 1127.
175 *Id.*
176 *Quon*, 445 F. Supp. 2d at 1128.
177 *Id.* at 1121.
178 *Id.* at 1128 (quoting Konop v. Haw. Airlines, Inc., 302 F.3d 868**,** 874 (9th Cir. 2002)).
179 *Id.* at 1128-29.

ECS.[180] The statute identifies a defense to liability for an RCS that discloses stored communications to the service subscriber (i.e., the city of Ontario), but does not create any similar defense for an ECS. None of the parties disputed that the city was the service subscriber, but the issue of whether Arch Wireless was an RCS or an ECS was hotly contested.[181]

The district court recognized that the proper inquiry to determine whether Arch was acting as an ECS or RCS involved examining the characteristics of the communication in question.[182] The legislative history illustrated Congress's intent that a single service provider could offer a range of services, causing its classification to depend on the specific characteristics of the service at issue.[183] While the provision of text-messaging services constituted an electronic communication service, the district court found that the long-term storage of those text messages for archival and record-keeping purposes constituted an RCS.[184] Since only the latter service was at issue in this case, the district court held that Arch Wireless was an RCS provider, and thus not liable for disclosing the text messages to the subscriber.[185] Accordingly, the district court granted summary judgment for the defendants on the SCA claims.[186]

2. Fourth Amendment Claims

The district court proceeded to analyze the plaintiffs' Fourth Amendment claims,[187] looking first at whether Quon had a reasonable expectation of privacy in the areas searched and second at the reasonableness of the searches themselves.[188] The district court noted the city's "operational reality" of choosing not to enforce its written privacy policy and instead informally allowing personal use in exchange for payment of the overage charges[189] and held that Quon had a reasonable expectation of privacy in his text messages.[190] The district court therefore found a material issue of fact

180 *Id.* at 1130.

181 *Id.* at 1133.

182 *Quon*, 445 F. Supp. 2d at 1133.

183 *Id.* at 1136.

184 *Id.* at 1137.

185 *Id.* at 1137-38.

186 *Id.* at 1138.

187 *Id.* at 1138-39.

188 *Quon*, 445 F. Supp. 2d at 1139. The court assumed that the plaintiff had a subjective expectation of privacy in his text messages, thus satisfying the first prong of the *Katz* test. *Id.*

189 *Id.* at 1141.

190 *Id.* at 1143-44.

regarding whether the search was reasonable[191] and denied the defendants' motion for summary judgment on the constitutional question.[192]

C. *Ninth Circuit Decision*

1. Stored Communications Act Claims

The plaintiffs appealed the grant of summary judgment for the defendants on their SCA claims to the Ninth Circuit. In examining the district court's ruling, the court agreed that the district court had correctly framed the issue as requiring a determination of whether Arch Wireless was an ECS (in which case it would be liable) or an RCS (resulting in no liability).[193] It disagreed, however, with the district court's analysis under that framework.[194] The Ninth Circuit read the legislative history as creating a rigid dichotomy whereby a service provider would be classified as either an RCS or an ECS in the abstract, based on the primary service provided.[195] In contrast to the district court, which scrutinized the exact nature of the service at issue in the plaintiffs' claims (i.e., archival storage of text messages) and determined that Arch Wireless was an RCS for the purposes of this case, the Ninth Circuit analyzed Arch Wireless's classification by looking only at the primary service Arch provided to the city (i.e., text-messaging).[196]

The court compared text-messaging services to the two types of providers Congress contemplated when it passed the SCA: (1) providers of data communication (ECSs) and (2) providers of data processing and storage (RCSs).[197] The court concluded that data communication provided the closer analogy to text-messaging, and held that Arch Wireless was an ECS.[198] It cited its decision in *Theofel v. Farey-Jones*[199] to bolster its conclusion, stating that Arch Wireless's storage of the text messages was indistin-

---

191 *Id.* at 1146. The Court held that "if the purpose for the audit was to determine if Quon was using his pager to 'play games' and 'waste time,' then the audit was not constitutionally reasonable," but if "the purpose for the audit was to determine the efficacy of the existing character limits to ensure that officers were not paying hidden work-related costs," then there was no constitutional violation. *Id.*

192 *Id.* at 1149.

195 Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

194 *Id.*

195 *Id.* at 900-01.

196 *Id.* at 900.

197 *Id.* at 900-01.

198 *Id.* at 902.

199 359 F.3d 1066 (9th Cir. 2004).

guishable from the *Theofel* service provider's back-up storage of e-mails.[200] The court found that its classification of the *Theofel* service provider as an ECS thus compelled the conclusion that Arch Wireless was also an ECS.[201] The court held that by disclosing Quon's text messages to the city, Arch Wireless had violated the SCA and directed judgment for the plaintiffs on the SCA claim.[202]

2. Fourth Amendment Claims

After the district court denied summary judgment on the constitutional question,[203] a jury trial resulted in a verdict for defendants on the constitutional question. The plaintiffs appealed the Fourth Amendment issue to the Ninth Circuit.[204] After first observing that "[t]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question," the court explored the "new frontier in Fourth Amendment jurisprudence" created by the explosion of text messages and e-mail.[205]

a. *Reasonable Expectation of Privacy Inquiry*

The Ninth Circuit began its inquiry into the individual's reasonable expectation of privacy in text messages by looking at the Supreme Court's holdings in *Katz v. United States* and *Smith v. Maryland*, and noting that the *Katz* Court based its holding in part upon its desire to respect "the vital role that the public telephone ha[d] come to play in private communication."[206] The court proceeded to examine the distinction between content and non-content information that the Supreme Court applied to postal mail and telephone records, and that the Ninth Circuit had recently extended to the electronic realm through its decision in *United States v. Forrester*.[207] The court

---

200 *Quon*, 529 F.3d at 902.

201 *Id.* at 902-03.

202 *Id.* at 903.

203 *Id.* at 899.

204 *Id.*

205 *Id.* at 904.

206 *Quon*, 529 F.3d at 904 (quoting *Katz v. United States*, 389 U.S. 347, 352 (1967)) (internal quotation marks omitted).

207 512 F.3d 500 (9th Cir. 2008), *cert. denied sub nom.* Alba v. United States, 129 S. Ct. 249 (2008); *see Quon*, 529 F.3d at 904-05. In *Forrester*, the Ninth Circuit analogized e-mail to postal mail and held that, similar to postal mail, the contents of an e-mail may receive privacy protection; however, the *Forrester* court held that there is no reasonable expectation of privacy in non-content information. *Forrester*, 512 F.3d at 510-11. For a discussion of the distinction between content and non-content information, see *supra* note 85.

analogized text messages to postal mail and affirmed that individuals do not have a reasonable expectation of privacy in the non-content information used to "address" the text message.[208] However, the court held that, despite the fact that service providers are technologically capable of accessing text messages, individuals have a reasonable expectation of privacy in the contents of their text messages.[209] Applying this conclusion to the facts at hand, the Ninth Circuit held that Quon had reasonably expected that the messages he sent and received would remain private.[210]

b. *Reasonableness of the Search Inquiry*

The court observed that determining whether a search was reasonable under the Fourth Amendment requires examining "the totality of the circumstances . . . by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[211] A jury had determined that the purpose of the search was to ascertain whether the 25,000 character limit was sufficient for the SWAT team to conduct work-related communications.[212] The court found that this was a legitimate reason for conducting a search, but held that the scope of the search was unreasonable.[213] Declaring that "[t]here were a host of simple ways to verify the efficacy of the 25,000 character limit" that would not have violated Quon's constitutional rights, the court held that the city's search of his text messages "was excessively intrusive in light of the noninvestigatory object of the search."[214] Chief Scharf successfully raised a defense of qualified immunity, but the court held the city liable for its violation of Quon's Fourth Amendment rights.[215]

208 *Quon*, 529 F.3d at 905.

209 *Id.*

210 *Id.* at 906.

211 *Id.* at 903 (quoting United States v. Knights, 534 U.S. 112, 118-19 (2001)) (internal quotation marks omitted).

212 *Id.* at 908.

213 *Id.*

214 *Quon*, 529 F.3d at 909.

215 *Id.* at 910-11. As the Fourth Amendment applies only to actions taken by the government, Arch Wireless did not face constitutional claims. *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) ("The Fourth Amendment['s] . . . protection applies to governmental action.").

III. EXAMINING TEXT MESSAGES WITHIN A CONSTITUTIONAL FRAMEWORK

A. *Analyzing the Ninth Circuit's Decision*

In keeping with a string of previous missteps in applying the SCA,[216] the Ninth Circuit in *Quon* once again applied a sweeping analysis that misconstrued critical details of the SCA. The Ninth Circuit reversed the district court's determination of Arch Wireless's status under the SCA,[217] but in so doing overruled a decision that better accords with the text of the statute as well as with the prevailing interpretation of the statute and its legislative history. The court prefaced its analysis of the plaintiff's SCA claims with the statement that "[t]he nature of the services Arch Wireless offered to the city determines whether Arch Wireless is an ECS or an RCS."[218] This approach fails to account for the fact that, as contemplated by Congress, a service provider can offer multiple services to the same user and its classification under the statute will vary depending on which service is at issue.[219] Moreover, the same service can have aspects of both electronic communication and remote computing services, and the relevant inquiry then depends on the aspect of the service being examined.[220]

As the district court observed, the service Arch Wireless provided to the city had two distinct aspects: text-messaging, with storage incident to transmission, and long-term storage of the messages for archival and record-keeping purposes.[221] The Ninth Circuit bypassed these subtleties in its analysis and classified Arch Wireless as an ECS based on its conclusion that it primarily provided text-messaging services.[222]

The district court's decision evidences a more nuanced reading of the statute that better conforms to both Congress's intent in creating the SCA and the prevailing view as recognized by the government and commenta-

---

216 *See supra* Part I.C.3.

217 *Quon*, 529 F.3d at 903.

218 *Id.* at 900.

219 LAFAVE, CRIMINAL PROCEDURE, *supra* note 85, § 4.8(d) (explaining that network providers "cannot be classified [as an ECS or an RCS] . . . in the abstract" and "the question is the role of the provider with respect to that particular copy of the particular contents to be compelled").

220 *Id.* (noting that "different copies of a particular communication may be regulated by different rules at different times").

221 Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1137 (C.D. Cal. 2006), *aff'd in part, rev'd in part*, 529 F.3d 892 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

222 Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

tors.[223] The district court properly held that, under the SCA, Arch Wireless should not be held liable for disclosing the text message transcripts to the city of Ontario.[224] Although such a result may seem incongruous with Congress's desire to enact a statute designed to provide greater protections to stored communications, it harmonizes with the structure of the ECPA, which grants lesser protections to stored communications than to communications in transmission.[225]

The Ninth Circuit's analytical misstep was spotted by another federal district court construing the same statutory provision. In a surprising move,[226] the United States District Court for the Eastern District of Michigan opted to follow the reasoning of the vacated district court opinion rather than the Ninth Circuit's decision in construing the SCA.[227] The question presented in *Flagg v. City of Detroit* was whether a private plaintiff in a civil proceeding could lawfully compel the production of thirty-four city employees' text messages, including those of former Detroit mayor Kwame Kilpatrick.[228] The *Flagg* court examined both the district court and the Ninth Circuit's decisions in *Quon* and concluded that the district court had correctly applied the statute:

> [T]his Court finds the lower court's reasoning [in *Quon*] more persuasive, on a number of grounds. First, the Court reads the Ninth Circuit's decision in that case . . . as resting on a unitary approach, under which service providers contract with their customers to provide either an ECS or an RCS, but not both. Yet, the prohibitions against disclosure set forth in § 2702(a) focus on the specific type of service being provided (an ECS or an RCS) with regard to a particular communication, and do not turn upon the classification of the service provider or on broad notions of the service that this entity generally or predominantly provides. Thus, the Court is inclined to agree with the view of the district court in *Quon* that "Congress took a middle course" in enacting the SCA, under which a service provider . . . may be deemed to provide both an ECS and an RCS to the same customer.[229]

In applying the statute, the *Flagg* court followed the district court's reasoning and analyzed the issue from the perspective of determining the relevant characteristics of the service at issue in the case.[230]

---

223 *See supra* note 115 and accompanying text.

224 *Quon*, 445 F. Supp. 2d at 1129.

225 *Id.* at 1135 (observing that Congress "deliberately structured [the ECPA] to afford electronic communications in storage less protection than other forms of communication" (quoting Konop v. Haw. Airlines, Inc., 302 F.3d 868, 877 (9th Cir. 2002)) (internal quotation marks omitted)).

226 *See* Gordon, *supra* note 2 (characterizing the Eastern District of Michigan's decision to follow the District Court decision in *Quon* as "unusual").

227 *See* Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008). While the Ninth Circuit's decision was obviously not binding on the district court in Michigan, it was persuasive authority.

228 *Id.* at 348.

229 *Id.* at 362.

230 *Id.* at 362-63. The court determined that the service provider was an RCS and could disclose the text messages to the subscriber (i.e., the city of Detroit) without obtaining the consent of the author and recipient (i.e., Mayor Kilpatrick). *Id.* at 363.

B. *Effect of the Ninth Circuit's Decision*

Although the Ninth Circuit sidestepped both the language of the statute as well as the congressional intent, its aggressive reading of the SCA could be interpreted as an attempt to provide maximum protections for personal communications. Had it been allowed to stand, the district court's decision would have allowed wireless providers to disclose the contents of communications without requiring a warrant supported by probable cause.[231] Conversely, the Ninth Circuit's conclusion effectively requires a warrant supported by probable cause to obtain any text messages stored for less than 180 days.[232] The Ninth Circuit's objective of assertively protecting personal communications is further established by its holding on the constitutional question. Rather than limiting its discussion to Quon's reasonable expectation of privacy in his text messages (as the district court had), the Ninth Circuit took the opportunity to elaborate on the inherent characteristics of text messages that make them worthy of Fourth Amendment protection.[233] The court did not limit its inquiry to the workplace context, nor to the civil search context; instead, by holding that "users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider,"[234] it established a broad constitutional assurance of protection for text messages.[235]

The practical effect of this decision is threefold. First, it better harmonizes the Supreme Court's decision in *Katz* with the Court's decisions in the business records cases and illustrates that text messages are protected under the Supreme Court's Fourth Amendment jurisprudence. Second, it tacitly holds that several SCA provisions are unconstitutional, and restores the Fourth Amendment to its appropriate position as the first line of defense against unlawful intrusions into personal electronic communications. Third, it gives rise to an exclusionary remedy in the criminal context, a critical safeguard necessary to protect the individual and uphold the integrity of law enforcement investigations.

---

231 For a discussion of the implications of categorizing a wireless provider as an RCS, see *supra* Part I.C.

232 Jennifer Granick, *New Ninth Circuit Case Protects Text Message Privacy From Police and Employers*, ELECTRONIC FRONTIER FOUNDATION, June 18, 2008, http://www.eff.org/deeplinks/2008/06/new-ninth-circuit-case-protects-text-message-priva.

233 Quon v. Arch Wireless, 529 F.3d 892, 904-06 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

234 *Id.* at 905.

235 Note that the Ninth Circuit's decision applies equally to e-mail. *See id.* ("We see no meaningful difference between the e-mails . . . and the text messages . . . .").

1. The Ninth Circuit's Decision Accords with Supreme Court Jurisprudence

Courts construing Supreme Court jurisprudence in the context of electronic communications encounter a seemingly irreconcilable conflict: the Supreme Court has repeatedly held that Fourth Amendment protections are lost when an individual discloses information to a third party, but it has also established clear protections for the contents of personal communications in the cases of telephone conversations and postal mail.[236] At first glance, the Ninth Circuit's reasoning seems to conflict with the Supreme Court's Fourth Amendment jurisprudence, but upon closer examination, its decision in *Quon* reconciles the Court's purpose in *Katz* with its later decisions in the business records cases.

Congress passed the SCA in an era when stored electronic communications served business-oriented purposes.[237] In creating the SCA, Congress acted under the assumption that electronically stored business files would be exempt from constitutional protections under the business records exception established by *Smith v. Maryland* and *United States v. Miller*. This assumption no longer reflects the modern-day reality, in which individuals consistently use text messages for personal communications.[238] In deciding *Katz*, the Supreme Court faced a similar dilemma: the public telephone, once a novelty, had assumed a key role in the daily lives of many Americans.[239] There was no doubt that the public was objectively aware that its conversations were susceptible to eavesdropping,[240] but despite this public awareness of the phone's penetrability, the Court held that individuals were entitled to privacy in their conversations.[241] It reached this conclusion largely because of the "vital role that the public telephone ha[d] come to play in private communications,"[242] and because, as commentators have

---

236 *See supra* Part I.B.1.

237 Of the technologies contemplated by the SCA's drafters, most were used exclusively in the business context. *See* Electronic Communications Privacy Act of 1986, S. REP. No. 99-541, at 8-11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562-65 (examining the various technologies and highlighting the business-related usages of each); *see also* Mulligan, *supra* note 76, at 1557 ("In 1986 . . . commercial electronic mail services and commercial data processing centers were emerging, but both primarily served the business community.").

238 *See supra* notes 1-9 and accompanying text; *see also* Amicus Curiae Brief of Professor Orin S. Kerr in Support of the Appellant at 7, United States v. Bach, No. 02-1238 Criminal (8th Cir. 2002) [hereinafter Amicus Curiae Brief of Professor Orin S. Kerr] (observing that "the truth remains that Americans use e-mail just like they use the postal mail").

239 Katz v. United States, 389 U.S. 347, 352 (1967).

240 Freiwald, *supra* note 124, ¶ 28 ("In the several years preceding *Katz*, the public had learned of rampant illegal wiretapping from numerous influential books, scholarly articles, and newspaper accounts.").

241 *Katz*, 389 U.S. at 352.

242 *Id.*

noted, "any other result would [have been] destructive of society's ability to communicate."[243] The Court's decision was normative, as it established a reasonable expectation of privacy in phone conversations when there was no objective reason to believe the conversation was indeed private.[244] Regardless of the telephone's vulnerability to eavesdroppers, the Court found that the critical role the telephone played in modern communications entitled the user to expect that his calls would be private.[245]

Given the text message's role in the personal communications of nearly 270 million Americans,[246] it is evident that the text message has assumed a position similar to that of the phone booth in the mid-1960s. The *Katz* court's normative holding is equally applicable to text messages: despite the fact that service providers may in fact be able to view the messages, a user's reliance on text messages in modern communications entitles her to expect privacy in the messages she sends and receives. To hold otherwise would be to allow mere technicalities to defeat the purpose of the Fourth Amendment, an analytical error the Court scrupulously avoided in its decision in *Katz*.[247]

The significant factor distinguishing the business records cases from a case such as *Quon* is that, unlike stored text messages, each of the documents at issue in the business records cases was of "independent interest" to the business that received the documents from the individual.[248] The defendant in *Couch* disclosed her business records and tax information to her accountant for the purpose of preparing tax returns, and the accountant had a legal obligation to examine the contents of the records to avoid preparing a false return.[249] Similarly, the bank in *Miller* had an independent interest in viewing the contents of the defendant's checks and deposit slips in order to complete the transactions.[250] Moreover, the phone company in *Smith* required the defendant's dialed numbers to connect his phone calls and prop-

---

243 Freiwald, *supra* note 124, ¶ 29.

244 *Id.*

245 *Id.* ¶¶ 28, 29.

246 *See* sources cited *supra* note 2.

247 Freiwald, *supra* note 124, ¶ 32. Freiwald argues that "to conduct the appropriate analysis, a court must determine what users of modern electronic communications are 'entitled to believe' about those communications and whether those communications have assumed a vital role in our lives." *Id.* Freiwald elaborates:

> To deny constitutional protection to e-mail and other modern electronic communications information because of its vulnerability to interception would make the very mistake the Court avoided in *Katz*. Constitutional rights must constrain both abusive government practices and new technological tools that facilitate abuse. Government . . . may not [itself] constrain constitutional protections.

Id. (footnote omitted). Thus, she asserts that courts must play the key role of defining Fourth Amendment protections where new technologies create new opportunities for abuse. *Id.*

248 Mulligan, *supra* note 76, at 1579.

249 *Id.* at 325-26.

250 Mulligan, *supra* note 76, at 1579.

erly bill him.[251] None of these cases involved the contents of personal communications. Rather, "defendants conveyed information so that the recipient would do something with that information . . . . [T]he substance of the information at issue was not only relevant to the recipient, it was essential for the recipient to conduct the transactions in question."[252]

Conversely, a wireless service provider does not have any independent interest in the contents of the text messages that its users send, nor are the contents required to complete any service or transaction.[253] Because the contents of text messages are not of independent interest to the provider (i.e., the contents themselves are not critical to transmitting the message), they are more analogous to the phone conversations at issue in *Katz* than the financial records and numbers dialed at issue in the business records cases and should be protected accordingly.

In the two decades since the passage of the SCA, electronic communications have evolved to play an important role in society's personal communications, rather than simply business communications.[254] Courts today are in a position similar to that of the Court in *Katz*, when it faced the rise of a new technology to a place of prominence in personal communications,[255] and should take care to follow the Ninth Circuit in affording the contents of private communications a reasonable expectation of privacy.

2. Restoring the Fourth Amendment

Professor Orin Kerr articulated the effect of granting individuals a reasonable expectation of privacy in their electronic communications in an amicus curiae brief to the Eighth Circuit in which he stated that "a broad holding by this Court that the Fourth Amendment protects remotely stored files could undercut the constitutionality of several provisions of [the SCA]."[256] Similarly, in *Warshak*, a federal district court within the Sixth Circuit concluded that various provisions of the SCA "violate the Fourth Amendment of the United States Constitution to the extent they collectively authorize the ex parte issuance of search and seizure orders without a war-

---

251 *Id.*

252 Bellia, *supra* note 17, at 1403.

253 *See supra* Part I.A.

254 *See supra* notes 1-10 and accompanying text.

255 Katz v. United States, 389 U.S. 347, 352 (1967) (noting that "to read the Constitution more narrowly" by not protecting Katz's phone conversation "is to ignore the vital role that the public telephone has come to play in private communication").

256 Amicus Curiae Brief of Professor Orin S. Kerr, *supra* note 238, at 10. Professor Kerr elaborated by noting that "Congress chose not to protect all stored e-mails with a full warrant requirement. Instead, Congress opted to require law enforcement to obtain a search warrant to obtain some e-mails, but permitted lesser process such as an 'articulable facts' court order or even a subpoena to obtain other stored e-mails." *Id.*

rant and on less than a showing of a probable cause."[257] When the issue reached the Sixth Circuit on appeal, however, the court avoided the constitutional issue by finding that the plaintiff's claim was not ripe for review.[258]

Although the Sixth and Eighth Circuits sidestepped the Fourth Amendment question,[259] the Ninth Circuit squarely addressed the issue and granted constitutional protections in *Quon*.[260] The decision indicates that, within the circuit, law enforcement will be required to comply with the more stringent warrant requirements of the Fourth Amendment rather than the lax statutory requirements of the SCA and suggests that, to the extent that the SCA allows law enforcement to proceed under a standard lower than probable cause, it is unconstitutional.[261] By holding that users have a reasonable expectation of privacy in their text messages, the court restored the proper Fourth Amendment inquiry and protected text messages with the full force of the Constitution.[262] Within the Ninth Circuit, the statute will be relegated to a supporting status, and will be employed only where its provi-

---

257 *Id.* at *8. The district court confronted the constitutionality of the SCA in a case in which the FBI obtained a § 2703(d) order to compel production of the plaintiff's e-mails after satisfying a magistrate judge that the e-mails were relevant to an ongoing criminal investigation. *Id.* at *1-2. The FBI also succeeded in convincing the magistrate to delay notice to the plaintiff for ninety days, arguing that prior notice would jeopardize the investigation. *Id.* However, without any independent enforcement mechanism to force notification, the FBI delayed a full year before notifying the plaintiff of the searches it had conducted. *Id.* at *2. The plaintiff filed suit, arguing that the SCA's authorization of searches supported by less than probable cause violated the Fourth Amendment. *Id.* The district court found that the § 2703(d) standard of "relevancy" combined with the delayed notice provisions indicated a substantial likelihood of success on the merits of the constitutional claim, and enjoined the FBI from searching the plaintiff's e-mails through the use of a § 2703(d) order. *Id.* at *8.

258 Warshak v. United States, 532 F.3d 521, 526 (6th Cir. 2008). Judge Martin lamented in his dissent the majority's taking of "another step in the ongoing degradation of civil rights in the courts of this country" and lauded the district court's ruling that aspects of the SCA were unconstitutional, noting that even under such a decision, law enforcement would still be able to conduct the search by demonstrating probable cause. *Id.* at 537-38 (Martin, J., dissenting). Judge Martin continued:

> I can only imagine what our founding fathers would think of this decision. If I were to tell James Otis and John Adams that a citizen's private correspondence is now potentially subject to ex parte and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless.

Id. Observing that the practical effect of such a ruling would be that law enforcement would lose only one tool in its arsenal, the dissenting judge stressed that the minimal burden on law enforcement was not too high a price to pay when the alternative was a loss of constitutional rights. *Id.*

259 United States v. Bach, 400 F.3d 622, 627-28 (8th Cir. 2002) (avoiding the constitutional issue by finding that, regardless of whether protections applied, probable cause existed for the search).

260 *See supra* note 212 and accompanying text.

261 *See, e.g.*, Freiwald, *supra* note 124, ¶ 17 ("[T]he ECPA should certainly be vulnerable to constitutional challenge if it permits law enforcement agents to access rich electronic communications data in storage without first obtaining a probable cause warrant . . . ."); Bellia, *supra* note 17, at 1417 ("[T]he application of § 2703(b) to allow the government to compel production of electronic communications without a warrant will be unconstitutional in some circumstances.").

262 *See supra* note 217 and accompanying text.

sions do not conflict with the constitutional search requirements.[263] The decision in *Quon*, after over twenty years of uncertainty, returns the Fourth Amendment to its appropriate position as the first line of defense against unlawful intrusions into the personal communications of individuals.

3. The Exclusionary Remedy

Lastly, the Ninth Circuit's decision is of great importance because subjecting text messages to the standard constitutional inquiry protects unreasonably seized communications through an exclusionary remedy.[264] This is a key difference between the current statutory protections and the traditional constitutional search framework: while evidence obtained from a search that violates the Fourth Amendment will be suppressed at trial, evidence obtained from a search that violates the SCA will not.[265] As noted previously,[266] there are several doctrinal underpinnings to the exclusionary rule. Where the rule does not apply, the moral hazards it exists to ameliorate will flourish. Law enforcement has little incentive to properly adhere to the SCA's procedures when even unlawfully seized evidence will be admissible at trial, and courts become unwitting participants in this constitutional destabilization.[267] Moreover, the integrity of the criminal justice system is undermined when wrongfully-obtained evidence may be used to secure convictions.[268]

Furthermore, where searches are not limited by the contours of a search warrant requiring particularity of purpose and no exclusionary remedy exists to limit the use of questionably-obtained evidence at trial, there is nothing to impede law enforcement from securing information for one purpose and using it for another.[269] For instance, in *Quon*, the defendant police department seized Quon's text messages to determine whether they were personal or work-related, but another officer leading a corruption investigation asked to review them for evidence of Quon's involvement in the corruption.[270] Although the record is inconclusive as to whether the officer

---

263 For examples of situations where the SCA might be applied in place of the Constitution, see *infra* notes 277-78 and accompanying text.

264 *See supra* Part I.B.3.

265 *See supra* notes 77-82, 126-28 and accompanying text.

266 *See supra* Part I.B.3.

267 LAFAVE, SEARCH AND SEIZURE, *supra* note 41.

268 *Id.*

269 For instance, commentators have noted hypothetically that the government could obtain information about an individual for the purpose of combating terrorism but later use that information for the purposes of combating terrorism. *See* Solove, *supra* note 42, at 1112.

270 Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1127 (C.D. Cal. 2006), *aff'd in part, rev'd in part*, 529 F.3d 892 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

actually viewed the text messages,[271] the exchange illustrates the danger to personal liberty when communications seized for one purpose can easily become evidence in a criminal proceeding.

IV. APPLYING THE NINTH CIRCUIT'S APPROACH

Courts faced with these issues would do well to take note of the Ninth Circuit's faithful interpretation of the Fourth Amendment and apply similar reasoning in future cases. Despite the Ninth's Circuits misguided interpretation of the SCA, its decision on the constitutional issue properly established protections for personal communications. In order to properly follow and expand upon the Ninth Circuit's decision, courts will first need to ask whether a reasonable expectation of privacy exists. With regard to this question, courts should follow the Ninth Circuit in holding that the expectation of privacy in electronic communications is not diminished by the fact that the network provider has the technical capacity to view the contents of the message.[272] Second, courts must determine what procedures should be required to obtain those electronic communications in which the individual retains a privacy interest. In the civil context, this will require balancing the government's purpose in obtaining the information against the privacy interest to be invaded.[273] Just as the *Quon* court heavily weighted the individual's privacy interest in its calculus and determined that the routine workplace purpose was not sufficient to justify an intrusion of this nature,[274] future courts should adequately weigh the individual's privacy interest. In the criminal context, law enforcement will be required to obtain a warrant supported by probable cause unless a recognized exception, such as a search incident to arrest or exigent circumstances, applies.[275]

---

271 *Id.*

272 Quon v. Arch Wireless, 529 F.3d 892, 906 (9th Cir. 2008 *petitions for cert. filed*, 77 U.S.L.W. 3619 (U.S. Apr. 7, 2009) (No. 08-1332), 77 U.S.L.W. 3670 (U.S. May 29, 2009) (No. 08-1472).

273 *See* 79 C.J.S. *Searches* § 128 (2008) (explaining that under the "special needs" doctrine, when the government wishes to conduct a search for a "special need," such as enforcement of safety regulations, rather than to find evidence of a crime, the government must show "a legitimate and substantial governmental interest in conducting the search" and demonstrate that the "special governmental needs outweigh particular privacy interest[s]"); *see also* Camara v. Municipal Court, 387 U.S. 523, 535 (1967) ("Unlike the search pursuant to a criminal investigation, the inspection programs at issue here are aimed at securing city-wide compliance with minimum physical standards for private property . . . . In determining whether a particular inspection is reasonable . . . the need for the inspection must be weighed in terms of these reasonable goals of code enforcement.").

274 *Quon*, 529 F.3d at 908-09.

275 *See* JEROLD H. ISRAEL ET AL., CRIMINAL PROCEDURE AND THE CONSTITUTION 133 (2008). *But see* California v. Acevedo, 500 U.S. 565, 582 (1991) (Scalia, J., concurring) (pointing out that "the 'warrant requirement' ha[s] become so riddled with exceptions that it [is] basically unrecognizable" and cataloguing twenty-two exceptions to the warrant requirement).

However, questions remain even after this landmark decision, and the Supreme Court will likely need to examine the subject before any consensus emerges regarding these gray areas. First, and most notably, the nature of the network provider's interest in the messages remains unclear. The Ninth Circuit's approach in *Quon* addressed the situation of compelled disclosure in the case of network providers,[276] but this approach would not apply to a situation in which the network provider approaches law enforcement hoping to turn over some of its users' messages in order to prevent or prosecute a crime. Such situations should be treated with great skepticism by courts, as law enforcement may use "voluntary" disclosure as a way to bypass the constitutionally required procedures.[277] However, in the case of true voluntary disclosure, the Fourth Amendment likely would not bar the network provider from disclosing the information to law enforcement.[278] Here, the SCA fills a critical gap by establishing a set of procedures with which the network provider must comply in order to disclose messages.[279] Thus, in the case of voluntary disclosure, courts should look to the SCA, rather than the Fourth Amendment, to protect the individual's private communications.

Additionally, it is unclear what protections are due communications stored by private providers, such as employers or universities with proprie-

---

276 *See Quon*, 529 F.3d at 898 (detailing how law enforcement requested copies of the communications from the provider).

277 *See* Kerr, *A User's Guide to the Stored Communications Act*, *supra* note 93, at 1224-25 (noting that "the precise line between voluntary and compelled disclosure rules remains hazy" and giving practical examples of how law enforcement could suggest a network provider voluntarily disclose communications in order to be a "good citizen"); *see also* Solove, *supra* note 42, at 1098 ("[I]n times of crisis or when serious crimes are at issue, the incentives to disclose information to the government are quite significant. Companies . . . want to cooperate and help out.").

278 The practicalities of communications technology may lead to a framework in which network providers will be considered recipients of the message for some purposes but not for others. For instance, once a recipient receives a communication such as a letter from the sender, the recipient has a property interest in the letter and may do as she sees fit, including turning it over to law enforcement. Smith v. Maryland, 442 U.S. 735, 740 (1979) (holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"). This undoubtedly holds true in the case of intended recipients of e-mail (e.g., an individual who receives an e-mail from a friend detailing the friend's plans to commit a bank robbery could certainly inform police of the friend's plans). *See* United States v. White, 401 U.S. 745, 749 (1971). *Cf.* United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990) (holding that an individual did not have a legitimate expectation of privacy in a pager message after it was received by another pager and stressing that "when a person sends a message to a pager, he runs the risk that either the owner or someone in possession of the pager will disclose the contents of his message"). What remain unclear are the rights and responsibilities of an unintended recipient such as the network provider, who has the technological capability to view the contents of communications but is not the intended addressee. *Quon* resolves this question for the case of compelled disclosure (by holding that the network provider's technical capacity to view the message doesn't defeat the user's reasonable expectation of privacy, *Quon*, 529 F.3d at 905), but does not address the case of voluntary disclosure by the provider.

279 *See supra* Part I.C.

tary e-mail systems. The SCA explicitly exempts private providers from its compelled-disclosure provisions and only regulates private providers under the voluntary disclosure provisions.[280] Thus, where law enforcement seeks to compel the production of a message held by a private provider, any applicable protections must arise from the Constitution. The appropriate protection in this case remains an open question, but the same policy motives that weigh in favor of constitutional protections for text messages stored by commercial providers also weigh in favor of strong protections for communications stored by private providers.

Courts should be conscious of the critical role they play in ensuring the continued strength and vitality of the Fourth Amendment. Historically, the judiciary has been the primary force shaping the interpretation of the Fourth Amendment,[281] and many of the accepted Fourth Amendment doctrines, such as the exclusionary rule, were created by courts.[282] The judiciary has successfully preserved and guided the Fourth Amendment from an era in which professional police were non-existent to an age in which "armed, quasi-military, professional police forces" bear primary responsibility for crime control and prevention.[283] Congress has demonstrated its present inability to create a cohesive framework capable of granting the full protections due personal communications,[284] and courts should step forward to ensure that communications receive adequate protection.

CONCLUSION

Professor Laurence Tribe, speaking of the effect of cyberspace on the Constitution, once asked, "When the lines along which our Constitution is drawn warp or vanish, what happens to the Constitution itself?"[285] The parchment upon which our Constitution was inscribed has long since faded into obsolescence as a means of communication, and its modern equivalent, the electronic communication, faces an uncertain status in the courts. The statute designed to protect personal communications is outdated and fails to

280 LAFAVE, CRIMINAL PROCEDURE, *supra* note 85, § 4.8(a).

281 Swire, *supra* note 56, at 915-16.

282 Charles McC. Mathias, Jr., *The Exclusionary Rule Revisited*, 28 LOY. L. REV. 1, 7 (1982) ("This rule of evidence did not come from on high. It's man-made . . . ." (quoting *Hearings before the Attorney General's Task Force on Violent Crime*, June 3, 1981 (testimony of Judge Wilkey)), *cited in* LAFAVE, SEARCH AND SEIZURE, *supra* note 41, § 1.1(a).

283 LAFAVE, SEARCH AND SEIZURE, *supra* note 41, § 1.1(a) (internal citations omitted).

284 Freiwald, *supra* note 124, ¶ 34 (stating that Congress has "shown itself incapable of providing adequate protection by allowing the ECPA to fall out of touch with modern practices. . . . [W]hat the statute protects it does so weakly, and there is much it does not protect").

285 Laurence Tribe, Tyler Professor of Constitutional Law, Harvard Law Sch., Keynote Address at the First Conference on Computers, Freedom & Privacy: The Constitution in Cyberspace (Mar. 26, 1991).

provide the level of protection warranted under the Fourth Amendment. The Ninth Circuit recognized the dilemma facing modern courts and took a groundbreaking approach that restores the Fourth Amendment to its rightful position as the primary arbiter of privacy protections. By granting text messages a reasonable expectation of privacy, the *Quon* court leads the way to a constitutional framework that better accords with the *Katz* inquiry and provides greater protections in both the civil and criminal context. Future courts faced with similar questions would be wise to follow in the Ninth Circuit's footsteps and grant electronic communications the rights they are due under the Constitution.