William & Mary Law Review

Volume 53 (2011-2012)
Issue 5

Article 7

April 2012

Katz Cradle: Holding On to Fourth Amendment Parity in an Age of Evolving Electronic Communication

Christopher R. Brennan

NOTES

KATZ CRADLE: HOLDING ON TO FOURTH AMENDMENT PARITY IN AN AGE OF EVOLVING ELECTRONIC COMMUNICATION

TABLE OF CONTENTS

INTRODUCTION

> The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[1]

The Fourth Amendment provides for "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[2] As with many phrases of the Constitution, this right has become a font of considerable complexity as courts have expanded its reach to cover a wealth of interactions between the government and individuals.[3] Perhaps no other set of interactions better illustrates this complexity than the current laws and interpretations defining the Fourth Amendment's application to electronic forms of communication.[4] Despite the prevalence of electronic communication in the everyday interactions of the average American,[5] the current landscape of statutory authority and judicial interpretation on the government's ability to seize electronic communications can best be described as outdated and disjointed.[6]

Yet one could hardly fault legislative sloth and judicial trepidation given the breakneck pace that has characterized the last decade of technological innovation. E-mail has left the laboratories of college campuses for middle schoolers' iPhones. In a matter of a few years, Myspace rose and fell to Facebook's present dominance.[7] Twitter hashtags chart trends in real time. But beyond the pack-

---

1. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

2. U.S. CONST. amend. IV.

3. *See* Meredith N. Garagiola, Note, *When the Constable Behaves and the Courts Blunder: Expanding the Good-Faith Exception in the Wake of* Arizona v. Gant, 47 AM. CRIM. L. REV. 1285, 1305 (2010).

4. *See* Darla W. Jackson, *Protection of Privacy in the Search and Seizure of E-Mail: Is the United States Doomed to an Orwellian Future?*, 17 TEMP. ENVTL. L. & TECH. J. 97, 100-06 (1999).

5. For example, an estimated 247 billion e-mails were sent per day in 2009. Press Release, The Radicati Grp., Inc., The Radicati Group, Inc. Releases "Email Statistics Report, 2009-2013" (May 6, 2009), *available at* http://www.radicati.com/wp/wp-content/uploads/2009/05/e-mail-statistics-report-2009-pr.pdf.

6. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1396-97 (2004) (stating that provisions of the Stored Communications Act (SCA) "are becoming increasingly outdated and difficult to apply").

7. *See* Dawn C. Chmielewski & Jessica Guynn, *Myspace Layoffs Are Part of Broad Restructuring*, L.A. TIMES, Jan. 12, 2011, http://articles.latimes.com/2011/jan/12/business/la-fi-ct-myspace-20110112.

aging—an unending variety of ways that programmers can repack and reinvent the binary string of ones and zeros that now allows us to e-mail and video chat—the messages remain the same. People share news; they gossip. Secrets are told and confidences kept or broken. This Note stems from the simple belief that if the message remains the same, the Fourth Amendment should as well. Whether by letter, telephone, e-mail, or video, the Fourth Amendment should ensure parity between the mediums that transmit any given message.

Part I begins with a review of the Supreme Court's early constitutional jurisprudence on the intersection of government surveillance in communication and the Fourth Amendment. This review is centered on the Court's reasoning in *Katz v. United States*.[8] *Katz* was the genesis of contemporary thought on Fourth Amendment protections for the seizure of electronic communications. In *Katz*, the Court determined that the Fourth Amendment applied to the government's eavesdropping on a telephone call from a public pay phone, despite the lack of a physical "trespass" by the government.[9] The language in *Katz* stating the Fourth Amendment protects "people, not places" specifically rejects a property-based approach to Fourth Amendment analysis.[10] Likewise, the Court's statement that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected," supports the notion that the protections of the Fourth Amendment should not be applied relative to the technology used to communicate the message.[11] In the aftermath of its landmark decision in *Katz*, the Court narrowed the potential scope of its language in *United States v. Miller*[12] and *Smith v. Maryland* when involving business records or communications held by a third party.[13]

8. 389 U.S. 347 (1967).

9. *Id.* at 351-53.

10. *Id.* at 351.

11. *Id.* at 351-52; *see infra* notes 52-54 and accompanying text (discussing technology-neutral language in *Katz*).

12. 425 U.S. 435 (1976).

13. 442 U.S. 735 (1979).

Part II interjects Congress's attempt at statutory guidance via the Electronic Communications Privacy Act of 1986 (ECPA).[14] Unfortunately, the ECPA's assortment of procedural hurdles is based on arbitrary distinctions among content types and ultimately fails to adhere to the Supreme Court's guidance in *Katz*, *Miller*, and *Smith*.[15] Given these failings, the ECPA is an outdated framework in desperate need of meaningful modernization.

Addressing these failures, Part III suggests a simplified approach that rests upon a content/noncontent distinction. In distinguishing between content and noncontent, this Note formulates a "transactional relevance" test.[16] This test will allow for the evolution of technology while maintaining parity with the reasonable expectation of privacy test that the Court established in *Katz*. An important complement to the transactional relevance test is the dismissal of the arbitrary distinctions among content under the Stored Communications Act of the ECPA. The effect of the transactional relevance test is that warrant-level protections for content are maintained in accordance with the Supreme Court's guidance under *Katz* without regard to evolving technology.

I. THE FOUNDATIONS OF CONTEMPORARY FOURTH AMENDMENT ANALYSIS

When the Founders adopted the Fourth Amendment in 1791,[17] they could not have imagined, much less anticipated, a nation in which communications could instantaneously move from origin to destination. Yet this fact should have little moment in resolving the challenges posed by today's technology, as the Constitution has proven to be remarkably adaptive to the passage of time.[18] This Part

14. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

15. *See infra* Part II.

16. *See infra* Part III.

17. The Bill of Rights, consisting of the First Amendment through the Tenth Amendment, became effective upon ratification by Virginia on December 15, 1791. Parklane Hosiery Co. v. Shore, 439 U.S. 322, 343 (1979) (Rehnquist, J., dissenting).

18. For example, the Commerce Clause has proven an expansive tool in dealing with the exponential economic growth experienced since the nation's birth. *See, e.g.*, United States v. Lopez, 514 U.S. 549, 554-56 (1995). Similarly, the language of the Fourteenth Amendment has consistently been relied upon to extend the notions of due process and equal protection. *See,*

examines the Supreme Court's jurisprudence regarding Fourth Amendment protections for well-established communication mediums such as the first class postal letter, the telegraph, and the telephone. The Court's analysis of these early mediums merits a detailed review. Indeed, the cases addressing these "traditional" mediums establish important Fourth Amendment doctrines that can be applied through analogy to today's digital counterparts.[19]

A. Communication at the Founding: Ex Parte Jackson *and the Protection Afforded to Letters*

The only communication medium contemporaneous with the Fourth Amendment is the letter. The Fourth Amendment explicitly refers to "papers" when enumerating areas within its scope.[20] The Court first discussed the Fourth Amendment's protections for "papers" as a medium for communication by letter in a case from 1877, *Ex parte Jackson*.[21] The Court's ruling upheld a statute prohibiting the use of the postal system to circulate lottery materials, but in dictum the Court established the foundations of Fourth Amendment protections against warrantless searches of communications.[22] Writing for the Court, Justice Field stated that "[l]etters and sealed packages ... are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."[23] No law could empower the government, via its postal inspectors, to violate the protections afforded to the contents of sealed letters and packages by the Fourth Amendment.[24] To inspect

e.g., Griswold v. Connecticut, 381 U.S. 479, 481-85 (1965).

19. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112-13 (2009).

20. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

21. *Ex parte* Jackson, 96 U.S. 727, 732-33 (1877); *see* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 556-58 (2007).

22. *See* Desai, *supra* note 21, at 569.

23. *Ex parte Jackson*, 96 U.S. at 733.

24. *Id.* ("[A]ll regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the [F]ourth [A]mendment of the Constitution.").

sealed items in transit through the postal system, the government was required to procure a warrant based upon probable cause.[25]

The protections for sealed postal mail under *Ex parte Jackson* also carried two notable restrictions. First, the Court was clear to distinguish sealed mail, such as a letter, from mail that was left open to examination, such as a newspaper or printed pamphlet.[26] In subsequent cases and statutes, this content/envelope distinction became a dividing line when determining which communications, or what elements of a communication, the Fourth Amendment protects.[27] Second, the Court found that the Fourth Amendment certainly did not prevent an individual who received a package that contained a prohibited mailing from delivering that package to the government.[28] The recipient of a delivered communication is not restricted by any Fourth Amendment right of the sender. The termination of a sender's Fourth Amendment rights as to a delivered communication in the possession of another forms the underpinnings of the third-party exception.[29] Like the envelope/content distinction, expansive use of the third-party doctrine has played a critical role in distorting the protections afforded to electronic communications.[30]

---

25. *Id.* Interestingly, although Justice Field's opinion refers to "papers" as stated in the Fourth Amendment, constitutional scholars cannot find any evidence that the Framers intended for letters to be protected from warrantless searches while in the possession of the Postal Service. *See* Desai, *supra* note 21, at 575-77. Desai suggests that the true impetus for this protection stemmed from the longstanding statutory prohibitions against postal workers inspecting private correspondence. *Id.* at 577.

26. *Ex parte Jackson*, 96 U.S. at 733 ("[A] distinction is to be made between different kinds of mail matter,—between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined.").

27. For a detailed discussion of the development of the content/envelope distinction and its application to electronic communications, see Tokson, *supra* note 19, at 2113-18, 2123-54.

28. *Ex parte Jackson*, 96 U.S. at 735.

29. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."). Note, however, that in *Ex parte Jackson*, a sealed letter did not constitute a "revealed" communication because the third party—the government via the Postal Service—could not inspect a letter without a warrant. *Ex parte Jackson*, 96 U.S. at 733.

30. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121, 149.

B. Communication Evolves: Embracing the Telephone in Katz *and Justice Harlan's Reasonable Expectation of Privacy*

When the Court decided *Ex parte Jackson* in 1877, the telegraph was already widely deployed across the country after having played a critical role in communication during the Civil War.[31] The Supreme Court never addressed the Fourth Amendment's extension to telegraph transmissions,[32] instead leaving the issue to Congress and the lower courts.[33]

The telephone, as the telegraph's successor, first drew the Court's attention in *Olmstead v. United States*.[34] In *Olmstead*, federal prohibition officers wiretapped multiple phone lines in order to gather evidence regarding a conspiracy to violate the National Prohibition Act.[35] The officers inserted wiretaps in the phone lines at junctions outside the conspirators' property.[36] Roy Olmstead, the lead conspirator, and his coconspirators later argued that the wiretap amounted to search and seizure under the Fourth Amendment.[37]

The Court rejected Olmstead's argument on multiple grounds. First, the Court determined that the language of the Fourth Amendment dictated that a "search is to be of material things."[38] On this basis, the Court distinguished *Ex parte Jackson*.[39] Second, the Court reasoned that the "Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted."[40] Despite the telephone's existence in the fifty years preceding *Olmstead*, a majority of the Court was not prepared

---

31. DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 30 (1978), *available at* http://pirp.harvard.edu/pubs_pdf/seipp/seipp-p78-3.pdf.

32. Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 371 (2009).

33. *See generally* SEIPP, *supra* note 31, at 30-42 (describing the interplay between Congress, Western Union, and the lower courts in deciding the privacy of telegraph messages).

34. 277 U.S. 438 (1928).

35. *Id.* at 456-57.

36. *Id.*

37. *Id.* at 455.

38. *Id.* at 464.

39. *Id.* The Court also relied on the idea that Congress had monopolized the postal system and by statute prohibited postal workers from opening letters in their possession for transit. *Id.*

40. *Id.* at 465 (internal quotation marks omitted).

to extend the Fourth Amendment to cover the interception of electronic signals captured outside one's property.[41]

Almost forty years later, the Court revisited its ruling in *Katz v. United States*.[42] *Katz* presented a conceptually similar scenario to *Olmstead*: the defendant was convicted upon evidence obtained from an electronic listening and recording device attached to the exterior of a public pay phone.[43] The recording device captured the defendant transferring wagering information.[44] The Court of Appeals for the Ninth Circuit had affirmed the conviction based on the property theory expressed in *Olmstead*—the State did not physically trespass in the area occupied by the defendant.[45]

The Supreme Court's opinion, however, declined to continue the property-centric approach used in *Olmstead*.[46] Although *Katz* acknowledged the importance of the telephone in private communications,[47] the Court did not confine its language and analysis to the telephone booth. From the outset, the Court clarified that:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected*.[48]

According to the Court, Katz was "surely entitled" to privacy in the words he transmitted through the pay phone, and thus the recording of his conversation constituted a search and seizure under the Fourth Amendment.[49] Despite the importance of the Court's holding, the majority's opinion is sparse on guidance in understanding exactly why Katz was "surely entitled" to assume the privacy of his conversation. Following *Katz*, both the Court and scholars have

41. *Id.*
42. 389 U.S. 347 (1967).
43. *Id.* at 348.
44. *Id.*
45. *Id.* at 348-49.
46. *Id.* at 351; *see* Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 19 (2006).
47. *Katz*, 389 U.S. at 352.
48. *Id.* at 351-52 (emphasis added) (citations omitted).
49. *Id.* at 352.

looked to Justice Harlan's concurrence and its two-prong "reasonable expectation of privacy" test.[50] Under Justice Harlan's analysis of prior decisions, a search and seizure implicates the Fourth Amendment when "a person [exhibits] an actual (subjective) expectation of privacy and, second ... the expectation [is] one that society is prepared to recognize as 'reasonable.'"[51]

The majority's holding and Justice Harlan's reasonable expectation of privacy test are robust triggers for Fourth Amendment protection. First, the Court's language is technology-neutral.[52] In contrast to *Olmstead*,[53] there was no examination into the technology used to transmit the message because the Court no longer considered the Fourth Amendment's protections limited to physical objects.[54] Second, and in a related sense, Fourth Amendment protection existed even though a telephone service provider acted to transmit the message.[55] In *Katz*, the telephone provider functioned as the Postal Service did in *Ex parte Jackson*, and its role in the delivery of a communication did not erode the sender's expectation of privacy in the communication.[56] Despite the Court's generalized language, the Court subsequently restrained any overly broad

50. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (noting that Harlan's test is expressed in the majority's opinion as something that an individual "seeks to preserve ... as private," which is objectively "justifiable" (quoting *Katz*, 389 U.S. at 351, 353)); Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1591-92 (2010); Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 6-7 (2009). *But cf.* Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1382 (2008) (arguing that Justice Harlan's test distracted courts and befuddled the concept of "privacy" in the actual holding of *Katz*).

51. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

52. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 580 (2009) ("[T]elephone calls are protected because of the function they serve rather than the accident of the technology they use."). Indeed, Professor Kerr suggests that *Katz* requires a technologically neutral approach to the Fourth Amendment. *Id.*

53. Olmstead v. United States, 277 U.S. 438, 466 (1928) ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment.").

54. *Katz*, 389 U.S. at 353.

55. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 773 (2008).

56. Of course, this privacy is confined to the *contents* of the communication. As subsequent cases illustrate, noncontent information, such as the number dialed, is not considered within the scope of the Fourth Amendment. *See* discussion *infra* Part I.C (discussing *Smith v. United States* and *Miller v. United States*).

reading of *Katz*'s holding through reliance on the third-party doctrine.[57]

C. Contents in Context: Business Records and the Third-Party Doctrine

In *Katz*, the majority disavowed a strict focus on location or property and instead chose to focus on the expressed intent of the individual.[58] The Fourth Amendment protects information that an individual "seeks to preserve as private" and that society recognizes as reasonably entitled to privacy,[59] but information "knowingly expos[ed] to the public," regardless of location, is outside the Fourth Amendment's scope.[60] To be clear, the Court extended Fourth Amendment protections in *Ex parte Jackson* and *Katz* under factual scenarios that strictly involved the government intercepting the contents of a private communication.[61] Furthermore, in both cases the communication was in the possession of a third party solely for its delivery to the intended recipient.[62] When faced with noncontent information and information revealed to a third party in both *Miller* and *Smith*, the Court did not find a protected Fourth Amendment interest.

In *United States v. Miller*, the government acquired incriminating bank records associated with defendant Miller after serving a subpoena on Miller's banks.[63] The Court provided two reasons for denying Miller a Fourth Amendment interest in the bank records turned over due to the subpoena.[64] First, the Court found that the information conveyed was not the "private papers" of the defendant

---

57. *See* Smith v. Maryland, 442 U.S. 735, 743-45 (1979); United States v. Miller, 425 U.S. 435, 442-43 (1976); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1024-25 (2010).

58. 389 U.S. at 351-52.

59. *Id.*

60. *Id.* at 351.

61. In subsequent cases, the Court held that the Fourth Amendment does not apply to transactional business records. *See, e.g.*, *Miller*, 425 U.S. at 440.

62. With respect to the contents of the communication, the third parties—the U.S. Postal Service and a telephone company—were merely *mediums for transmitting* the messages. *See Katz,* 389 U.S. at 348; *Ex parte* Jackson, 96 U.S. 727, 732 (1877).

63. 425 U.S. at 437.

64. Kerr, *supra* note 52, at 569-70.

but rather constituted a "business record" of the bank.[65] An expectation of privacy could not exist with respect to information the bank used in commercial transactions.[66] Second, Miller had revealed the information to the bank—a third party—in conducting his finances.[67] Justice Powell wrote:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[68]

Miller demonstrates the restrictive nature of the objective prong in Justice Harlan's reasonable expectation of privacy test.[69] Regardless of whether Miller exhibited a belief that bank records were private communications, the Court deemed such an expectation unreasonable based on the records' transactional contents that Miller revealed in the ordinary course of his business with the bank.[70]

Three years later, the Court revisited its holding in *Miller* in the context of pen registers in *Smith v. Maryland*.[71] The pen register at issue in *Smith* employed a surveillance technique distinct from the wiretap analyzed in *Katz*.[72] The device was installed at the phone company's central office and recorded the numbers dialed from Smith's line but did not record the contents of any communication

---

65. *Miller*, 425 U.S. at 440.

66. *Id.* at 442 (finding that checks were not "confidential communications").

67. *Id.* at 441-43.

68. *Id.* at 443. Scholars differ on the import of the Court's holding on this point. *Compare* Bellia & Freiwald, *supra* note 30, at 148 ("[R]eading *Miller*'s 'assumption of risk' approach broadly creates undue tension with *Katz*."), *with* Sam Kamin, *The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 104 (2004) ("[T]he Court asked whether any other person has been given (or has gained) access to the information the government is seeking to obtain. If the answer is yes, the Court has held that the area simply is not protected by the Fourth Amendment.").

69. *See* Kerr, *supra* note 52, at 570-71.

70. *See* Tokson, *supra* note 19, at 2156.

71. 442 U.S. 735 (1979).

72. "A pen register is a mechanical device that records the numbers dialed on a telephone.... It does not overhear oral communications and does not indicate whether calls are actually completed." *Id.* at 736 n.1 (citation omitted).

on the line.[73] As in *Katz*, the government did not seek a warrant or court order to install the pen register, and Smith challenged the search and seizure of his call information as a violation of the Fourth Amendment.[74]

Smith's holding, which denied Fourth Amendment protections to pen register surveillance, demonstrated the interplay of the Court's jurisprudence on Fourth Amendment protections for communications from *Ex parte Jackson* through *Katz* and *Miller*.[75] Applying *Katz*, the *Smith* Court recognized the distinction between the contents of the private communications captured in *Katz* and the "limited capabilities" of the pen register used in *Smith*.[76] The Court's analysis harkened back to the content/envelope distinction referenced in *Ex parte Jackson*.[77] This distinction also weighed on the reasonable expectation of privacy test under *Katz*.[78] The Court found, from a normative view, that a phone company's routine use of subscriber phone records rendered any subjective expectation of privacy for dialed numbers highly unlikely.[79] Drawing from *Miller*, the Court found that Smith's privacy expectation was not objectively reasonable to society.[80] As with bank records in *Miller*, Smith conveyed the numbers he dialed to the phone company in the ordinary course of his business with the phone company.[81] In doing so, Smith "assumed the risk" that the information he revealed to the telephone company's equipment would be conveyed to government authorities.[82]

The Court's holding on this basis is of particular importance to electronic communications such as e-mail or instant messaging. *Smith* posited that information conveyed to a third party in the

73. *Id.* at 737, 741.

74. *Id.* at 737.

75. *See* Kerr, *supra* note 57, at 1023-25.

76. *Smith*, 442 U.S. at 741-42.

77. *See* Kerr, *supra* note 57, at 1023-25.

78. *See* Tokson, *supra* note 19, at 2155 ("[N]umerous courts and commentators have read *Smith* as holding that the content/noncontent distinction is crucial to determining whether an individual has a reasonable expectation of privacy.").

79. *Smith*, 442 U.S. at 742-43; *see* Tokson, *supra* note 19, at 2156.

80. *Smith*, 442 U.S. at 743-45.

81. *Id.*; *see* Tokson, *supra* note 19, at 2156-57 (stating that *Smith* implicitly extended the third-party doctrine discussed in *Miller* to transactions with third parties in which the communication was solely intended for another private party).

82. *Smith*, 442 U.S. at 743-45.

normal course of business was "revealed" regardless of whether that information was actually conveyed to a person or an electronic device.[83] In this respect, the Court maintained the technology-neutral approach it had adopted in *Katz*.[84] Regardless of the technology, *Katz* did not inquire into the specifics of the medium used to transfer the contents of a confidential communication,[85] and *Miller* and *Smith* likewise did not afford protection to noncontent information revealed to a third party in the normal course of its business, even when that information is revealed solely to electronic, automated systems.[86] Shifting from Supreme Court precedent to statutory authority, Part II will discuss how Congress has muddied the constitutional waters by enacting legislation governing electronic communications that largely ignores the holdings of *Katz* and its progeny.

II. CONGRESS INTERVENES: THE ELECTRONIC COMMUNICATIONS PROTECTION ACT

The ECPA currently provides the statutory framework for government surveillance of all electronic communications—from telephone wiretaps and pen registers to e-mail and today's emerging technologies.[87] Congress enacted the ECPA as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the original Wiretap Act.[88] The ECPA restructured the original Wiretap Act, which protected only voice communications from interception, into three parts.[89] Title I of the ECPA contains the updated Federal Wiretap Act, which encompasses the interception of wire, oral, and electronic communications.[90] Title II, the Stored Communications Act, outlines the protections afforded to informa-

83. *See id.* at 744; *see also* Tokson, *supra* note 19, at 2157. When addressing *Smith*'s applicability to Internet communications, Tokson criticizes the Court's "overlapping rationales" as failing to identify which basis was central to the Court's holding. *Id.* at 2156-57.

84. *See supra* notes 49-54 and accompanying text.

85. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

86. *See* Kerr, *supra* note 52, at 570; Tokson, *supra* note 19, at 2157.

87. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *see* Tokson, *supra* note 19, at 2117-18.

88. Pub. L. No. 90-351, 82 Stat. 197; *see* S. REP. NO. 90-1097 (1968).

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

90. 18 U.S.C. §§ 2510-2522 (2006); *see* Oyama, *supra* note 89, at 499.

tion in electronic storage and transactional records related to this information.[91] Title III contains the Pen Register Act, which covers any "device or process" used to capture noncontent information concerning the "dialing, routing, addressing, or signaling" of an electronic communication.[92]

Part I of this Note addressed the constitutional guidance that existed at the enactment of the ECPA. Part II now provides a brief synopsis of the relevant sections of the ECPA, particularly the Stored Communications Act. Congress itself has recognized the need for reforming the ECPA, for these statutes were enacted at a time when no one could have anticipated the evolution of communication possibilities via the Internet and mobile broadband.[93] In short, the ECPA offers a myriad of procedural requirements and degrees of protection for different forms and elements of electronic communications.[94] The provisions of the Stored Communications Act (SCA) are particularly significant. As opposed to the heightened protections that the Wiretap Act affords to the interception of a comprehensive range of communications, the SCA creates arbitrary distinctions that do not align with current communication mediums and data-retention practices.[95]

A. The Federal Wiretap Act

Congress expanded the scope of the Federal Wiretap Act under Title I of the ECPA to recognize the alternative means by which electronic communications might be intercepted.[96] The Act makes it illegal to "intentionally intercept[] ... any wire, oral, or electronic communication."[97] To this end, "intercept" is described as the "acquisition of the contents of any wire, electronic, or oral communi-

91. 18 U.S.C. §§ 2701-2712; *see* Oyama, *supra* note 89, at 499.

92. 18 U.S.C. §§ 3121-3127; *see* Tokson, *supra* note 19, at 2120 (describing the history of the Pen Register Act and its amendment by the USA PATRIOT Act); Oyama, *supra* note 89, at 499.

93. *See infra* Part III (describing the recent congressional hearings on reforming the ECPA).

94. *See* Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages,* 32 HASTINGS COMM. & ENT. L.J. 365, 367-68 (2010).

95. *See* Tokson, *supra* note 19, at 2121.

96. *See* Salter, *supra* note 94, at 373.

97. 18 U.S.C. § 2511(1)(a).

cation through the use of any electronic, mechanical, or other device."[98] The Act's definitions function to provide broad coverage for the content of any conceivable form of electronic communication while in transit.[99] The Wiretap Act, however, will apply to *only* interception that is contemporaneous with transmission.[100]

In e-mail and other current electronic communication technologies, however, storage is practically simultaneous with transmission.[101] Under the current ECPA framework, the courts and scholars remain confused as to the proper boundaries of the Wiretap Act and the SCA for e-mail and other similar communications that are "stored" incidental to their transmission at multiple locations before the communication reaches its intended destination.[102] Given the changes proposed in Part III, it is both beyond the scope of this Note and unnecessary to thoroughly document the morass that currently exists in determining whether an e-mail is in storage or in transit as the communication travels along the Internet's electronic pathways.[103] For the purposes of this Note, it is sufficient to assume that the seizure of an e-mail that has reached its destination is classified as "electronic storage" and would invoke the SCA rather than the Wiretap Act.[104] Viewed from the perspective of government surveillance, the Wiretap Act is a prospective investigation tool.[105] When the government obtains an electronic wiretap, it seeks the seizure of real-time transmissions that have not reached their final

98. *Id.* § 2510(4).

99. Salter, *supra* note 94, at 371 (discussing protections "applicable to wiretap surveillance of communications in transmission" as opposed to stored communications).

100. Tokson, *supra* note 19, at 2119.

101. *See* Salter, *supra* note 94, at 382-93 (documenting the guiding case law on the issue of when an electronic communication is considered stored or in transmission under the ECPA).

102. *See id.*

103. *See id.* at 382.

104. *See* 18 U.S.C. § 2510(17) (2006) (defining "electronic storage" as communications stored incidental to communication and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication").

105. *See* Paul K. Ohm, *Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1600 (2004) ("[A] classic substantive distinction in the law is that Title III, the Wiretap Act, governs prospective surveillance, meaning the contemporaneous interception of electronic communications, while the SCA governs access to static, historical information." (footnotes omitted)).

destinations because at the time the government seeks a wiretap order, these transmissions do not yet exist.[106]

Because a wiretap allows the government access to the contents of all prospective communications, it carries the highest level of protection among electronic communication surveillance techniques.[107] To legally impose a wiretap, the government must obtain what is known as a "super" warrant.[108] The requirements of a super warrant exceed those of a traditional lawful search and seizure.[109] In order to issue a wiretap order, a judge must find, upon a sworn statement of facts from a law enforcement officer, the following:

> (a) [T]here is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in [the Wiretap Act];
>
> (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; [and]
>
> (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[110]

In addition to these heightened requirements for obtaining a wiretap order, the Act also provides a comprehensive suppression remedy for evidence seized under an unlawful wiretap.[111] The Wiretap Act sets the current maximum for protections afforded to the contents of electronic communications and therefore offers a proper starting point for assessing the treatment of stored electronic communications under the SCA.[112]

---

106. Because the relevant evidence has not been transmitted, government agents will need to perform, at the minimum, a cursory examination of *all* incoming communications to determine their potential relevance.

107. *See* Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 290 (2008).

108. Orin S. Kerr, *Internet Surveillance After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 621 (2003).

109. *See* Salter, *supra* note 94, at 373.

110. 18 U.S.C. § 2518 (1), (3) (2006).

111. *See* Salter, *supra* note 94, at 375-76. The SCA lacks an equivalent suppression remedy for criminal proceedings. *Id.*

112. *See* Tokson, *supra* note 19, at 2121.

B. The Stored Communication Act

In contrast to the prospective nature of a wiretap, government surveillance by means of seizing communications under the SCA implies that these communications already exist in electronic storage at a given location, regardless of whether that location represents the messages' final destination. Seizure pursuant to the SCA is retrospective in the nature of the contents seized under the statute.[113] The SCA governs the accessibility of "stored wire and electronic communications and transactional records."[114] Subchapters of the SCA include prohibitions against unauthorized access of electronic communications[115] as well as restraints on a storage provider's ability to disclose the contents of its users' communications.[116] For government surveillance purposes, however, the principal provision of the SCA is 18 U.S.C. § 2703, which provides the procedures through which a government entity may require the disclosure by service providers of stored communications and transactional records.[117]

Section 2703 subdivides the compelled disclosure of stored communications and transactional records into a procedural hierarchy that results in varying levels of protection.[118] Subsection (a) first operates to distinguish between the content of messages in electronic storage for 180 days or less and messages stored for more than 180 days.[119] Among these types of content, the former is afforded ordinary probable cause warrant-level protection, as opposed to the "super" requirements for a wiretap.[120] The latter, however, only requires one of the three available options in subsection (b): a search warrant as in subsection (a); an administrative subpoena; or

---

113. The operative word here is *contents*. Certainly, the noncontent information recorded by electronic pen registers is prospective in nature. *See In re* United States for an Order: Authorizing the Installation & Use of a Pen Register & Tap & Trace Device, 622 F. Supp. 2d 411, 413 (S.D. Tex. 2007); *see also* Tokson, *supra* note 19, at 2118-21.

114. 18 U.S.C. ch. 121.

115. *Id.* § 2701.

116. *Id.* § 2702.

117. *Id.* § 2703; *see* Warshak v. United States, 490 F.3d 455, 462 (6th Cir. 2007), *vacated*, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007) (ordering rehearing en banc).

118. *See* Bellia & Freiwald, *supra* note 30, at 126-27.

119. 18 U.S.C. § 2703(a).

120. *See Warshak*, 490 F.3d at 461-62.

a court order.[121] If the government obtains a warrant, it does not have to provide notice to the user whose communications are disclosed,[122] but prior notice is required for an administrative subpoena or court order.[123]

The notice distinction is premised on the lesser standard required to obtain an administrative subpoena or court order.[124] A court order merely requires "specific and articulable facts showing that there are reasonable grounds to believe that ... [the communications or records] are relevant and material to an ongoing criminal investigation."[125] This is a lesser standard than probable cause.[126] In addition, the requirement that the notice be "prior" notice is not absolute. Under § 2705, notice may be delayed by up to ninety days if the government can demonstrate that notice would have an "adverse result."[127] In effect, § 2703 operates to allow the government to obtain the content of any e-mail stored by a service provider for more than 180 days and to delay notice of this government action without ever requiring a showing of probable cause—the standard explicitly set forth in the Fourth Amendment.[128]

When the government seeks noncontent information, the SCA sets procedural requirements at a bare minimum.[129] Under § 2703(c), the government may obtain the following user information with a subpoena:

> (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
> (A) name;
> (B) address;

121. *Id.* at 462; *see* 18 U.S.C. § 2703(a)-(b).

122. 18 U.S.C. § 2703(b)(1)(A).

123. *Id.* § 2703(b)(1)(B).

124. *See* Bellia & Freiwald, *supra* note 30, at 127-28.

125. 18 U.S.C. § 2703(d).

126. *See* Warshak v. United States, 490 F.3d 455, 463 (6th Cir. 2007).

127. 18 U.S.C. § 2705(a)(1)(A). An "adverse result" may be any of the following: "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." *Id.* § 2705(a)(2)(A)-(E). In addition, the government may obtain an additional ninety-day extension if it can demonstrate the continued potential for an adverse result. *Id.* § 2705(a)(1)(A).

128. *See id.* § 2703.

129. Tokson, *supra* note 19, at 2122.

> (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).[130]

Furthermore, the government is not required to provide notice to the subscriber when someone requests this information.[131] Outside of the enumerated items above, the government may request any other noncontent records through a court order under § 2703(d) or a warrant.[132] An example of this type of record for electronic communications is the header information from e-mails.[133] Again, notice is not required.[134]

III. RESTORING PARITY: A TECHNOLOGY-NEUTRAL APPROACH FOR ELECTRONIC COMMUNICATIONS IN ACCORDANCE WITH *KATZ*, *MILLER*, AND *SMITH*

It is hardly novel to suggest that the ECPA, and the courts' application of Fourth Amendment principles to electronic communications, demand reform. In May 2010, the House of Representatives's Subcommittee on the Constitution, Civil Rights, and Civil Liberties began a series of hearings focused on reforms to the ECPA.[135] Representative Nadler, Chairman of the Subcommittee, posed the following question to the panel of experts who testified at the hearing: "[I]n what ways have ... [recent technologies] potentially subverted one of the original and central goals of [the] ECPA, which was to preserve 'a fair balance between the privacy expectations of

130. 18 U.S.C. § 2703(c)(2)(A)-(F).

131. *Id.* § 2703(c)(3).

132. *Id.* § 2703(c)(1)(A)-(B).

133. Tokson, *supra* note 19, at 2122. The header of an e-mail contains the routing information for the message. *See id.* at 2127.

134. 18 U.S.C. § 2703(c)(3).

135. *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 1 (2010) [hereinafter *ECPA Hearing*].

citizens and the legitimate needs of law enforcement?'"[136] These hearings signify that Congress is aware of the pressing need to revisit a body of statutory law that was designed for a "technological environment as far removed from our own as that of 1986 was from the day Alexander Graham Bell said, 'Mr. Watson, come here. I need you.' in the first telephone call 110 years earlier."[137] Accordingly, the relevant issue is not the need for reform, but rather the shape these reforms should take. This Note argues that the overall objective should be a statutory framework that allows courts to apply the Supreme Court's jurisprudence in *Katz*, *Miller*, and *Smith* without regard to the medium or technology used to effectuate the message. In essence, the ECPA's successor should ensure Fourth Amendment parity between the telephone and all other communication mediums.

In shaping the following recommendations, insistence on simplicity is paramount. This insistence conforms with the Supreme Court's guidance on the Fourth Amendment and benefits all parties involved—courts, citizens, and law enforcement.[138] First, a simple framework, devoid of complex distinctions and protection hierarchies, will allow for consistent and efficient application by the federal judges who must review law enforcement requests for wiretaps and compelled disclosures on a daily basis in an ever-changing technological landscape.[139] Second, simple guidelines are more likely to conform with the subjective prong of the reasonable expectation of privacy test because the subjective privacy expectations of citizens are more likely to align with a statutory framework that avoids arbitrary distinctions.[140] Third, law enforcement officers will

136. *Id.* at 2 (statement of Rep. Jerrold Nadler).

137. *Id.* at 1.

138. *See* Arizona v. Roberson, 486 U.S. 675, 681-82 (1988) (describing the virtues of bright-line rules that provide "clear and unequivocal" guidelines to law enforcement (internal quotation marks omitted)); Oliver v. United States, 466 U.S. 170, 181-82 (1984) ("This Court repeatedly has acknowledged the difficulties created for courts, police, and citizens by an ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances. The ad hoc approach not only makes it difficult for the policeman to discern the scope of his authority; it also creates a danger that constitutional rights will be arbitrarily and inequitably enforced." (citations omitted)).

139. *See* 18 U.S.C. § 2516(1) (requiring a federal judge to grant an order authorizing the use of a wiretap).

140. For example, the SCA affords considerably less protection to e-mails that are stored for more than 180 days. *See id.* § 2703(a). Presently, Google's Internet-based e-mail service,

be less likely to unintentionally violate clear and consistent guidelines.[141]

A. The Transactional Relevance Test: A Technology-Neutral Definition for Noncontent

In *Ex parte Jackson*, the Court distinguished between the contents of a sealed letter and the exposed information visible on its envelope.[142] When faced with the interception of the contents of a telephone communication in *Katz*, the Court declared that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[143] Subsequently in *Miller* and *Smith*, the Court clarified that the Fourth Amendment would not apply to transactional information, such as bank records and dialed telephone numbers, revealed to a third party in the ordinary course of business.[144] This line of cases supports a distinction in Fourth Amendment protections between content and noncontent information.[145]

In accordance with this distinction, the seizure of communication content should require a probable cause search warrant regardless of the technology. Noncontent information may be obtained by a lesser standard, such as a subpoena or court order.[146] This framework has gained widespread approval among scholars and technol-

---

Gmail, offers users over seven gigabytes of free e-mail storage and suggests that users archive rather than delete messages. *See* Gmail Help Center, *Archiving vs. Deleting?*, GOOGLE, http://mail.google.com/support/bin/answer.py?hl=en&answer=32608 (last updated Dec. 7, 2011). As a result, Gmail users are highly unlikely to harbor a different expectation of privacy for their older messages as opposed to more recent e-mails. *See* Bellia & Freiwald, *supra* note 30, at 162.

141. *See Roberson*, 486 U.S. at 681-82.

142. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

143. Katz v. United States, 389 U.S. 347, 351-52 (1967).

144. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

145. *See, e.g.*, Bellia & Freiwald, *supra* note 30, at 173 (advocating for a content/noncontent distinction); Kerr, *supra* note 57, at 1018 (advocating again for a content/noncontent distinction); Tokson, *supra* note 19, at 2112 ("[T]he distinction is firmly established in communications surveillance law.").

146. *See, e.g.*, Kerr *supra* note 57, at 1018 ("[N]on-content information should not trigger the Fourth Amendment.").

ogy professionals.[147] Yet this proposal says very little, for the crux of this argument is really about how one defines content and, inversely, noncontent. As the following discussion demonstrates, scholars' views on this issue are wide-ranging.[148] Drawing from this pool of arguments and the Supreme Court's jurisprudence, this Note proposes a new "transactional relevance" test for separating content from noncontent across all communication mediums—present and future.

Given the present statutory morass, several notable scholars have attempted to devise a suitable model for understanding the Fourth Amendment in a digital world. Renowned Fourth Amendment scholar Orin S. Kerr, for instance, crafted a definition for content and noncontent via analogy to the physical world and an inside/outside distinction.[149] Professor Kerr argued that in the physical world, activities that occur "out in the open" are exposed to the public and government surveillance.[150] In contrast, activities in enclosed spaces are not visible to the public, and government surveillance of these inside activities requires a search warrant.[151] In the electronic world, the content/noncontent distinction must "mirror the traditional distinction between inside and outside."[152] In a world without any means of communication other than face-to-face conversation, the identities, location, and time of communication would

147. *See, e.g.*, *ECPA Hearing*, *supra* note 135, at 34-35. At the House of Representatives's Subcommittee on the Constitution, Civil Rights, and Civil Liberties's first hearing on ECPA reform, every witness supported a content/noncontent distinction. *See id.* at 18 (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology) ("Congress should extend the traditional warrant standard to our personal communications, private documents and highly sensitive information like mobile hacking data. Other less sensitive data should be available with a subpoena."); *id.* at 33 (statement of Albert Gidari) ("Service providers want clarity and bright line rules."); *id.* at 34 (statement of Orin S. Kerr, Professor, The George Washington University School of Law) ("[I]t may be helpful to think about two different kinds of data that communication providers may have. One category is content communication.... And then there is lots of non-content information."); *id.* at 55 (statement of Annmarie Levins, Associate General Counsel, Microsoft) ("I think that in fact if you are talking about content, people expect that what they would have on their hard drive, and in their personal hard drive, should be protected in the same way."). *But see* Slobogin, *supra* note 50, at 1588 (arguing that Fourth Amendment protections "ought to be roughly proportionate to the invasiveness of the search").

148. *See infra* text accompanying notes 149-62.

149. Kerr, *supra* note 57, at 1009.

150. *Id.* at 1010.

151. *Id.* at 1010-11.

152. *Id.* at 1009.

be public information.[153] This is outside information. However, assuming the conversation was not "out in the open," the content of the conversation would be inside information.[154] By analogy, in an electronic world, the Fourth Amendment would not protect the users' identities and logs of their messages, but it would protect the contents of their confidential communications.[155]

Kerr's analogy boasts a logical appeal, but it ultimately lacks practical usefulness. Kerr admits that an inside/outside analogy fails to give concrete answers as to what constitutes noncontent in electronic communications.[156] Although the analogy is technology-neutral in its application,[157] judges applying such an analogy will likely arrive at inconsistent conclusions. It would certainly be a difficult task, for instance, to find a physical world analogy for metadata.[158]

In contrast to Kerr's analogy, Professor Tokson crafts a definition for content that "focuses on the semantic and/or common law definition of 'content,' presumably the relevant definition for the word as it is used in *Smith*."[159] Tokson suggests that the Court's opinion in *Smith* referred to "content" as defined by the Wiretap Act.[160] And under the Wiretap Act, content encompasses "any information concerning the substance, purport, or meaning of that communication."[161] Tokson finds this to be a broad definition, one that would encompass "URLs and other content-revealing routing information."[162]

---

153. *See id.* at 1018.

154. *See id.* at 1010, 1020.

155. *Id.* at 1021.

156. *Id.* at 1029 ("Every different Internet application generates its own data, and lines must be drawn to distinguish content from noncontent for each.").

157. *Id.* at 1015.

158. Metadata may be defined as "data that provides information about or documentation of other data managed within an application or environment." Adam K. Israel, Note, *To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery*, 60 ALA. L. REV. 469, 472 (2009) (citation omitted).

159. Tokson, *supra* note 19, at 2125.

160. *Id.* at 2126 (relying on *Smith*'s use of a prior decision that discussed how pen registers do not reveal the "purport" of telephone conversations).

161. 18 U.S.C. § 2510(8) (2006).

162. Tokson, *supra* note 19, at 2170.

Tokson's definition is certainly practical.[163] Its adherence to *Smith*, however, is questionable due to its finding that content includes "URLs and other content-revealing routing information."[164] Recall that *Smith* determined that dialed telephone numbers captured by a pen register were not protected by the Fourth Amendment.[165] The Court stated that the "petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business .... The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[166] The Court explicitly stated that automation of the switchboard did not affect its constitutional analysis.[167]

Based on this language, a URL is simply the Internet's equivalent of a phone number. No constitutional difference should exist between a URL that contains words relating to the content of a website visited and the scenario of a telephone user who asks the operator to connect him to the town doctor. Both convey information for the use of the third party in its ordinary course of business. The only difference is automation, a distinction that *Smith* rejects.

As an alternative to the distinctions offered by Kerr and Tokson, this Note suggests a "transactional relevance" test for distinguishing between content and noncontent. This test asks whether the information a user submitted *is relevant to the transaction with the third party in its ordinary course of business*. In other words, would different information alter the transaction from the third party's point of view? If so, the information is *not* content.

In a straightforward example, consider the body of an e-mail message. From the perspective of the third-party service provider, the substance of the information contained in the body of an e-mail is entirely irrelevant. The service provider merely transmits this information to its intended recipient.[168] A user could alter every

163. Tokson applies this definition to various elements of electronic communications. *See id.* at 2127-39 (applying the broad definition of content to URLs and search terms).

164. *See id.* at 2170.

165. Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

166. *Id.* at 744.

167. *Id.* at 745.

168. This example is straightforward only to the extent that it is simplistic. Whether a message says "Hello" or "Goodbye" should be of no relevance to the service provider in

single character in the message, and the transaction would remain entirely unaltered from the perspective of the service provider.[169] Likewise, the subject field of an e-mail is content. In a more difficult example, consider the case of a content-revealing URL such as http://law.wm.edu/academics/gradingpolicy. This address certainly reveals some degree of the substantive content of the website. As discussed *supra*, Tokson would consider this URL to constitute content, and the government would thus need a warrant in order to access records showing that the user accessed this link under his framework.[170] The transactional relevance test, on the other hand, would unquestionably label this information as noncontent. Altering the URL would certainly change the transaction from the service provider's perspective, just as dialing a different number or asking to connect to a different person would make a material difference to a switchboard operator.

Using the transactional relevance test provides multiple benefits. First, it renders the analysis entirely technology-neutral. Regardless of future developments in communication technology, the question remains the same: Does the information alter the transaction from the third party's perspective? With good reason, Professor Kerr considers a technology-neutral solution vital for adapting the Fourth Amendment to electronic communications.[171] Unlike the inside/outside analogy, however, the transactional relevance test avoids requiring judges to mentally transport an iPhone back to the Founding. Most importantly, the transactional relevance test maintains parity between electronic communications and the Court's jurisprudence in *Katz*, *Miller*, and *Smith*. The test answers *Katz*'s question of whether information has been "knowingly expose[d] to the public" in accordance with the Court's guidance in *Miller* and

completing the transaction. But more complex, real-world scenarios could complicate the matter. For example, the size of the message—an attribute affected by the message's content—is likely relevant to the transaction. This reality, however, should not convert a message's content into part of the transaction. The content of a two-page letter inside an envelope is just as safe as that of a single-page letter.

169. Note that any obligation that a service provider may have to scan messages for illegal content is outside the bounds of the transactional relevance test.

170. *See* Tokson, *supra* note 19, at 2170.

171. *See* Kerr, *supra* note 57, at 1015-17.

Smith.[172] A broader definition for content would actually, and arbitrarily, provide greater protection for an e-mail than a letter.

B. Assigning Protections Under the Transactional Relevance Test

Even with the proper distinction between content and noncontent, the transactional relevance test must resolve the issue of assigning protections. In accordance with *Katz*, content information would require a probable cause search warrant.[173] Unlike the current provisions of the SCA, this protection would apply for all content, transmitted under any medium, stored for any length of time.[174] The notice provisions of § 2703(b) would therefore be rendered irrelevant.[175] Following *Smith* and *Miller*, noncontent information would exist outside the protections of the Fourth Amendment, and the government could obtain this information by means of a subpoena or court order.[176] Notice would not be required.

The transactional relevance test would have little practical effect on the wiretap and its "super" warrant requirement. As a prospective surveillance tool, the Wiretap Act already encompasses the interception of contents from any conceivable electronic communication technology.[177] Rather, the transactional relevance test would ensure that the retrospective surveillance of the contents of any electronic communication medium would require a showing of probable cause.

CONCLUSION

By aligning warrant-level protections with the contents of stored electronic communications as determined by the transactional

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

173. *See id.* at 352, 358-59.

174. Even under the existing statutory framework, the distinction created by § 2703(b) is likely unconstitutional. *See* Kerr, *supra* note 57, at 1043-44 ("In the routine case, however, § 2703(b) is unconstitutional.").

175. 18 U.S.C. § 2703(b) (2006).

176. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979) (holding that "pen registers did not acquire the *contents* of communications," and therefore were not protected under the Fourth Amendment); United States v. Miller, 425 U.S. 435, 440-41 (1976) (noting that the subpoenaed papers were business papers of the bank, not private papers, making the subpoena valid).

177. 18 U.S.C. § 2510(12).

relevance test, Fourth Amendment protections can be maintained in accordance with the Supreme Court's guidance under *Katz* without regard to the evolving technological mechanisms we use to communicate. This approach adheres to the technology-neutral language implicit in the holdings of *Katz* and *Smith*.[178] Furthermore, parity premised on constitutional doctrine ensures that the objective side of Justice Harlan's reasonable expectations test neither lags nor outpaces the current technological landscape.

Christopher R. Brennan[*]

178. *See* Kerr, *supra* note 52, at 570; Tokson, *supra* note 19, at 2157.

* J.D. Candidate 2012, William & Mary School of Law; B.S. 2009, University of Pittsburgh. Many thanks to my parents for their endless encouragement and support, and to the *Law Review* staff and editorial board for their time and effort throughout this process.